applied sciences

MDPI

Article

A Blockchain-Based Privacy-Preserving and Fair Data Transaction Model in IoT

Wei Zhou [1,2], De Zhang [1,*], Guangjie Han [3], Wenyin Zhu [2] and Xupeng Wang [1]

[1] School of Information and Control Engineering, Qingdao University of Technology, Qingdao 266520, China; zhouwei@qut.edu.cn (W.Z.); wxp1130@yeah.net (X.W.)
[2] Qingdao Haier Smart Technology R&D Co., Ltd., Qingdao 266101, China; zhuwenyin@haier.com
[3] College of Internet of Things Engineering, Hohai University, Changzhou 213022, China; hanguangjie@gmail.com
* Correspondence: zhangdeql@163.com; Tel.: +86-183-7517-9412

Abstract: The rapid development of the Internet of Things (IoT) has resulted in vast amounts of widely distributed data. Sharing these data can spur innovative advancements and enhance service quality. However, conventional data-sharing methods often involve third-party intermediaries, posing risks of single-point failures and privacy leaks. Moreover, these traditional sharing methods lack a secure transaction model to compensate for data sharing, which makes ensuring fair payment between data consumers and providers challenging. Blockchain, as a decentralized, secure, and trustworthy distributed ledger, offers a novel solution for data sharing. Nevertheless, since all nodes on the blockchain can access on-chain data, data privacy is inadequately protected, and traditional privacy-preserving methods like anonymization and generalization are ineffective against attackers with background knowledge. To address these issues, this paper proposes a decentralized, privacy-preserving, and fair data transaction model based on blockchain technology. We designed an adaptive local differential privacy algorithm, MDLDP, to protect the privacy of transaction data. Concurrently, verifiable encrypted signatures are employed to address the issue of fair payment during the data transaction process. This model proposes a committee structure to replace the individual arbitrator commonly seen in traditional verifiable encrypted signatures, thereby reducing potential collusion between dishonest traders and the arbitrator. The arbitration committee leverages threshold signature techniques to manage arbitration private keys. A full arbitration private key can only be collaboratively constructed by any arbitrary t members, ensuring the key's security. Theoretical analyses and experimental results reveal that, in comparison to existing approaches, our model delivers enhanced transactional security. Moreover, while guaranteeing data availability, MDLDP affords elevated privacy protection.

Keywords: blockchain; Internet of Things; data transaction; local differential privacy; verifiable encrypted signature

Citation: Zhou, W.; Zhang, D.; Han, G.; Zhu, W.; Wang, X. A Blockchain-Based Privacy-Preserving and Fair Data Transaction Model in IoT. *Appl. Sci.* **2023**, *13*, 12389. https://doi.org/10.3390/app132212389

Academic Editor: Gianluca Lax

Received: 19 October 2023
Revised: 13 November 2023
Accepted: 14 November 2023
Published: 16 November 2023

1. Introduction

With the widespread development and application of Internet of Things (IoT) technology, vast amounts of data from IoT sensors are collected, stored, and utilized [1]. Data from a single sensor often fails to meet the requirements of users. The true value of IoT lies in the sharing and comprehensive use of diverse sensing data. Data sharing promotes the distribution of data resources, elevating work efficiency and quality, while spurring innovative applications. For instance, in healthcare, data sharing can provide valuable records of patient treatments and physical examinations, assisting medical professionals in providing more targeted treatment plans [2]. In data markets, novel data transaction models have emerged that allow data owners to sell their information to consumers. Big data has evolved into a valuable asset [3].

However, the current IoT system architecture is based on client–server communication. IoT devices are connected to a central cloud server which is used to ensure the communication between devices and handle and store data. This centralized architecture may create a single point of failure. This may increase security and privacy risks. Therefore, it is necessary to adopt a new solution based on decentralized architecture [4]. Additionally, during data transactions, due to the inherent mistrust between data providers and consumers, the latter might delay or refuse payments after obtaining the data. Similarly, providers could withhold datasets after receiving compensation, making fair payments between parties hard to ensure. Given the aforementioned challenges in security, privacy preservation, and fair payment, many data owners are reluctant to provide their data to third-party trading platforms. The big data industry grapples with the challenge of "data islands". Hence, there is an imperative need to adopt a decentralized data-sharing framework and establish a secure, efficient data transaction model that ensures fair payment and safeguards data providers' privacy during transactions.

Blockchain, as a distributed ledger, embodies characteristics of decentralization, immutability, and auditability and is frequently employed to address security issues tied to traditional IoT systems [5]. Compared to conventional centralized IoT systems, a decentralized IoT system based on blockchain has several advantages: firstly, it achieves end-to-end communication without involving centralized servers, reducing single-point failure risks and bolstering fault tolerance; secondly, nodes on the blockchain can verify the integrity and identity information of data uploaded by other nodes, which can prevent malicious data tampering and ensure the security and consistency of the blockchain network; finally, blockchains store data and event logs in an immutable manner, giving blockchain-based IoT systems traceability and accountability.

Nevertheless, each node in the blockchain maintains a local backup of the entire blockchain to uphold the network's integrity. Given that all nodes have access to blockchain data, this backup mechanism has raised growing concerns about privacy. There's a potential risk of sensitive information being exposed. Traditional privacy-preserving techniques, such as anonymization and generalization, have proven inadequate when faced with attackers possessing background knowledge [6]. This inadequacy is evident from significant privacy leaks in datasets like AOL [7] and Netflix [8], leading to questions about the effectiveness of these methods in protecting user privacy. Differential privacy, which is a notable method to counter attackers with background knowledge, operates by adding random "noise" to datasets to ensure data privacy [9,10]. However, while differential privacy introduces "noise" to maintain privacy, it compromises data availability. Determining the right amount of "noise" to strike a balance between dataset availability and privacy remains a research challenge.

In the context of ensuring fair payment, verifiable encrypted signatures are commonly used to guarantee transaction fairness online. The concept of verifiable encrypted signatures was first introduced by ASOKAN [11] and involves three parties: the signer, the verifier, and a trusted third party (i.e., an arbitrator). The fundamental principle behind verifiable encrypted signatures is that the signer encrypts a conventional digital signature using the arbitrator's public key, thereby confirming that the ciphertext genuinely contains a standard signature. Any verifier can use the arbitrator's public key to verify its validity. Nevertheless, without the help of the signer or the arbitrator, it is impossible to extract a valid signature. The ordinary signature can only be recovered by the adjudicator from this encrypted signature. However, in such a situation, the impartiality and security of a single arbitrator cannot always be guaranteed. Dishonest traders might collude with the arbitrator to the detriment of the other party. Furthermore, if the arbitration node experiences a single-point failure, the potential loss of the arbitration private key could render the arbitration process unfeasible.

To address these challenges, this paper proposes a decentralized, privacy-preserving, and fair IoT data transaction model based on blockchain. We have developed an adaptive localized differential privacy algorithm, termed MDLDP (Multiple Disturbance of Local

Differential Privacy), which perturbs data prior to its integration into the blockchain, ensuring the protection of local data privacy. We also leverage verifiable encrypted signatures to ensure fairness during transactions. This model replaces the traditional single arbitrator, commonly found in conventional verifiable encrypted signatures, with an arbitration committee. The arbitration committee employs threshold signature techniques to manage arbitration private keys. Only by collaborating among any arbitrary set of t members can the reconstruction of the complete arbitration private key be achieved. Assuming that any t members act securely and honestly, the impartiality and security of the arbitration committee can be guaranteed. This setup precludes both the loss of arbitration private keys and the potential collusion between dishonest traders and arbitrators. Theoretical analysis and experimental results indicate that our model offers heightened transaction security compared to existing approaches. Additionally, the MDLDP algorithm not only ensures data availability but also provides augmented privacy protection.

2. Related Works

2.1. Blockchain and Differential Privacy

With the widespread adoption of blockchain technology, a secure and distributed ecosystem has been established for the Internet of Things (IoT). This technology is increasingly being utilized across diverse IoT sectors to build robust data-sharing solutions [12]. In the domain of Industrial IoT, the complexity of manufacturing processes increases due to the varied nature of the industries involved. As the final products frequently originate from multiple departments that span various sectors, concerns about privacy and security arise during cross-domain interactions. Singh et al. [13] presented a centralized cloud cross-domain data-sharing platform employing multiple security gateways. These gateways employ blockchain technology to upload information to a centralized cloud. When applications report malicious activities, the centralized cloud employs blockchain verification to validate the reports and subsequently impose penalties on the responsible parties. However, this approach cannot guarantee the impartiality and security of the centralized cloud. Lu et al. [14] designed a blockchain-empowered secure data-sharing architecture for distributed multiple parties. They formulate the data-sharing problem into a machine learning problem by incorporating privacy-preserved federated learning. The privacy of data is well maintained by sharing the data model instead of revealing the actual data. In the field of Medical IoT, Sabu et al. [15] proposed a model that combines blockchain with the Interplanetary File System (IPFS) to address privacy and security concerns associated with data sharing. This model provides restrictions and protective measures for users' personal data. The data in the IPFS is distributed among nodes, and using IPFS to store health records has the feature of tamper resistance. Nevertheless, this mechanism lacks effective protection for the raw data. Thantharate et al. [16] presented ZeroTrustBlock—a comprehensive blockchain-based framework for secure and private health data management that addresses limitations in mainstream health IT systems. The proposed architecture provides a decentralized medical record repository using a permissioned blockchain. Smart contracts enact fine-grained access policies tailored to patient consent. A hybrid on-chain and off-chain storage model balances transparency with confidentiality. Integration gateways enable interoperability with existing systems like EHRs and insurance platforms. In the field of smart transportation, Cui et al. [17] propose a secure and efficient data-sharing scheme among vehicles without the assistance of an RSU in IoV. They exploit consortium blockchain technology to achieve traceability and immutability of data-sharing records. The scheme prevents unauthorized data sharing and improves the security and privacy of the data-sharing process. To meet the requirements of vehicle speed, latency, and communication overhead in the actual environment of vehicle networking, Du et al. [18] modified the original PBFT consensus structure and designed an extensible double-layer PBFT consensus algorithm. In addition, a multi-weight subjective logic model CRMWSL for calculating reputation values was proposed to achieve accurate calculation of RSU node reputation values. Meanwhile, suitable nodes are elected into the committee

to participate in consensus according to their reputation values, which further reduces communication overhead and improves blockchain scalability. Miao et al. [2] advocated for data sharing through model sharing and introduced a secure mechanism called BP2P-FL, which utilizes peer-to-peer federated learning. By introducing blockchain into data sharing and recording every training process, data providers are able to provide high-quality data. To protect privacy, BP2P-FL uses differential privacy techniques to disturb the global data-sharing model, but this mechanism cannot guarantee privacy safety during the federated learning process. Fotiou et al. [10] proposed a data transaction model employing Local Differential Privacy (LDP) to safeguard data provider privacy and devised a blockchain-based solution to ensure fair exchange and immutable data logs. However, traditional LDP mechanisms cannot fit well with blockchain since the requirements of a fixed input range, large data volume, and using the same privacy budget, which are practically difficult in a decentralized environment. To address this, Zhang et al. [19] presented a novel local differential privacy mechanism to partition and perturb data, which does not mandate vast data volumes or fixed input ranges. By using an iteration approach to adaptively allocate the privacy budget for different perturbation procedures that minimize the total deviation of perturbed data and increase the data availability.

2.2. Fair Payment

In recent years, the big data transaction market has garnered significant attention from researchers. In data transactions, fair payment refers to the timely receipt of the agreed-upon dataset or compensation when both parties of the transaction comply with the transaction agreement in good faith [20]. Zhou et al. [21] proposed a distributed data vending framework based on blockchain by combining data embedding and similarity learning. They obtained the trade-off between data retrieval and leakage risk by indexing the data. Niu et al. [22] proposed TPDM, which integrates trust and privacy preserving in data markets by using homomorphic encryption and identity-based signatures. However, these mechanisms do not adequately address the fair payment issue between trading parties. Djuric et al. [23] propose the Fair Exchange Internet Payment Protocol (FEIPS) for the payment of physical goods. Although FEIPS has a strong emphasis on fair exchange, it still guarantees strong security properties, including confidentiality, data integrity, authentication, and non-repudiation. Goldfeder et al. [24] contemplated the fair payment problem when purchasing physical goods with cryptocurrencies and proposed a series of protocols. These protocols offer security and privacy and are compatible with blockchain-based cryptocurrencies like Bitcoin. Chen et al. [25] propose a fair exchange protocol for autonomous data sharing and describe a concrete implementation framework based on BTC. The concrete framework is designed based on BVM smart contract scripts. Nevertheless, these protocols all rely on trusted third parties. Kurtulmus et al. [26] established a protocol using blockchain technology, wherein participants do not need mutual trust. Users can employ their datasets to train machine learning models and obtain rewards. However, this protocol lacks effective protection for local data. Wang et al. [27] propose an auditable fair payment and physical asset delivery protocol based on smart contracts. In view of the phenomenon of goods being switched, the way of "pre-verification" is added. In addition, this plan designs a complete return process for the first time, providing a better service experience and higher efficiency for consumers. Zhao et al. [28] propose a new blockchain-based fair data trading protocol in the big data market, to enhance the privacy, availability, and fairness of data trading. The advantage of blockchain infrastructures is removing the single-point failure of the big data market. They enhance the anonymity of data providers and extend DAPS to data trading for fairness. At the same time, they use similarity learning to enhance the availability of trading data.

3. Background Knowledge

3.1. Blockchain

Blockchain is a peer-to-peer network comprised of multiple participating nodes. It can be regarded as a distributed ledger characterized by decentralization, tamper-resistance, non-forgery, and traceability. Transaction information is recorded in block structures that include timestamps, and each block contains a pointer to its predecessor. The blockchain is maintained collaboratively by all participating nodes, with its consistency ensured via consensus algorithms. Depending on the access rules, blockchains can be categorized into public blockchains and consortium blockchains. In public blockchains, the number of participating nodes is not fixed, and they have the freedom to join or exit at will. For consortium blockchains, only users who have undergone identity verification and received authorization are permitted to join.

3.2. Local Differential Privacy

Traditional data privacy protection techniques, such as k-anonymity [29] and generalization [30], lack universal applicability due to their absence of a strong mathematical foundation to define data privacy and data loss. Moreover, they are ineffective against attackers armed with background knowledge. The emergence of differential privacy [31–33] has effectively addressed this issue. This model is a robust privacy protection technique based on mathematical theory. Differential privacy is unconcerned with an attacker's background knowledge, even if the attacker possesses information on all records except one, that single record's privacy remains uncompromised. Local differential privacy is a distributed variant of differential privacy that allows each user to locally perturb the raw data to protect privacy before uploading it. It is defined as follows [34]:

Definition 1 (ε-Local Differential Privacy): *If there exists a randomized algorithm M, for any two distinct tuples v_i and v_i' in dataset D and any potential output $y \in Y$ (Y being the output domain of M), that satisfies*

$$\Pr[M(v_i)Y] \leq e^{\varepsilon} \times \Pr\left[M\left(v_i'\right)Y\right], \tag{1}$$

then the randomized algorithm M is said to satisfy ε-local differential privacy. Here, Pr[•] indicates the probability of the output result. ε is referred to as the privacy budget, which represents the level of data privacy protection. The smaller its value, the closer the probabilities over adjacent datasets, and the higher the level of data privacy protection.

A commonly employed technique to realize local differential privacy is the randomized response mechanism [35]. The principle behind this mechanism is that when users respond to sensitive Boolean questions, they answer truthfully with probability *P* and oppositely with a probability of 1-*P*. Local differential privacy is built on a rigorous mathematical foundation that ensures data privacy protection even when the attacker has maximum background knowledge.

3.3. Verifiable Encrypted Signature

The basic principle of verifiable encrypted signatures is as follows [36]: Data consumers encrypt the arbitrator's digital signature using their public key and verify if the signature truly exists in the ciphertext. Anyone can validate the validity of the signature via the arbitrator's provided public key. In the case of disputes, arbitrators can use their private keys to decrypt encrypted signatures and prevent traders from maliciously withholding digital signatures. Verifiable encrypted signatures effectively ensure fairness in online transactions and protect both parties from potential losses. The verifiable encrypted signature protocol comprises the following eight algorithms:

(1) $Setup(1^{\lambda}) \rightarrow pp$: Generates the open parameter *pp* by giving the parameter λ.

(2) $AdjKeyGen(pp) \rightarrow (APK, ASK)$: By disclosing the parameters pp, generate the arbiter's key pair (APK, ASK).
(3) $KeyGen(pp, APK) \rightarrow (pk_i, sk_i)$: Generating signer i by disclosing the parameters pp and the arbiter's public key APK of the key pair (pk_i, sk_i).
(4) $Sign(pp, sk_i, m) \rightarrow \sigma_i$: By disclosing the parameters pp, private key sk_i and message m, generating signer i of the digital signature σ_i.
(5) $Verify(pp, pk_i, m) \rightarrow 0/1$: Verify the validity of the digital signature σ_i by disclosing the parameters pp, public key pk_i and message m. If the algorithm outputs 1 it means that the signature is valid and outputs 0 it means that the signature is invalid.
(6) $VESSign(sk_i, m, APK) \rightarrow \sigma_i^{VES}$: Generate a verifiable encrypted signature σ_i^{VES} by utilizing the private key sk_i, message m, and the arbiter's public key APK.
(7) $VESVerify(pk_i, m, APK, \sigma_i^{VES}) \rightarrow 0/1$: By public key pk_i, message m, arbiter public key APK as well as the verifiable encrypted signature σ_i^{VES}, verifying the validity of the verifiable encrypted signature σ_i^{VES}. If the algorithm outputs 1, the cryptographic signature can be verified as valid, while an output of 0 indicates that it is invalid.
(8) $Adj(pk_i, APK, ASK, m, \sigma_i^{VES})\sigma_i$: By public key pk_i, APK, the private key of the arbiter ASK, message m and a verifiable encrypted signature σ_i^{VES} to obtain the digital signature σ_i.

3.4. Threshold Signature

In 1987, Yvo Desmedt first introduced the concept of threshold signatures [37]. The threshold signature mechanism allows any t signatories out of r to sign a message. However, if the number of signatories is less than t, a valid signature cannot be generated. The scheme is described as follows [38]:

Let Z be a finite field, and q be a large prime number in that field. c_i (where $i = 1, 2, \ldots, r$) represent the r participants. A $t-1$ degree polynomial is randomly selected as:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \ mod \ q, \tag{2}$$

where $a_i \in Z(q)$ (for $i = 1, 2, \ldots, t-1$). Compute $s_i = f(x_i)$ for $i = 1, 2, \ldots, r$, and send s_i as a secret share to participant c_i. Using any t sub-keys, the secret can be reconstructed such that:

$$s = f(0) = \sum_{i=1}^{t} s_i \prod_{l=1, l \neq i}^{t} \frac{-x_i}{x_i - x_l} \ mod \ q, \tag{3}$$

4. System Model

This section introduces our proposed blockchain-based security, privacy-preserving, and fair data transaction model.

4.1. System Overview

In the model, data is perturbed using local differential privacy before the transaction to protect data privacy, and verifiable encrypted signatures are used to ensure the fairness of the transaction. An arbitration committee is established to replace the traditional single arbitrator, with the intention of preventing potential collusion between dishonest parties and the arbitrator during the transaction. The system assumes that IoT devices are programmable and can implement local differential privacy. The model views IoT devices as nodes in the blockchain, which can effectively prevent single-point failures. It also securely records information about data disturbances and transactions in an immutable manner to ensure the traceability of transactions.

The system overview is illustrated in Figure 1. As depicted in Figure 1, the system primarily consists of four components: data consumers, data providers, the arbitration committee, and the blockchain. Specifically, data consumers issue data transaction requests. Data nodes that meet the requirements and are interested can apply to become data providers for a given transaction. After the application is approved, the data provider will

consider their privacy and reward needs to determine their privacy budget and perturb their local data preparation for transactions. The transaction employs verifiable encrypted signatures to sign the transaction agreement, with the arbitration public key synthesized by a random subset of t members from the arbitration committee. Ultimately, the blockchain records transactional information, including data perturbations, to facilitate traceability. Further details on each component of the model will be explained below.

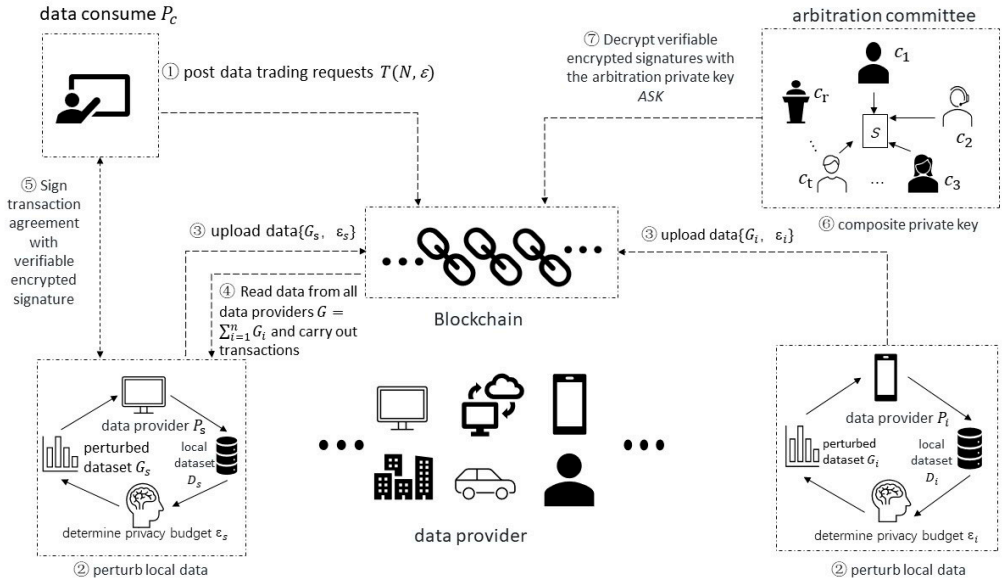


Figure 1. Blockchain-based privacy-preserving fair IoT data transaction model.

(1) Data Consumers: Based on their specific needs, they issue a data trading request. Data consumers may need to ensure the size of transaction data due to statistical and other business needs. Meanwhile, the smaller the privacy budget of differential privacy, the lower the availability of transaction data. Therefore, the minimum data volume and minimum privacy budget are specified in the data transaction request. Subsequently, they make a payment that serves as a deposit to prevent any malicious behavior on their part. Data nodes that meet the criteria of the consumer's request and are interested in it can apply to participate in this data transaction. Ultimately, a transaction agreement is signed using a verifiable encrypted signature, after which they obtain the dataset, now distorted with noise, and paid compensation.

(2) Data Providers: Refers to nodes that meet the demands of the data consumers and successfully partake in the data transaction. These providers aspire to earn compensation from the current data transaction. However, they might be unable to meet the data volume requirements of the data consumer individually due to limitations in their storage or limited data resources. When data providers apply to join a transaction, they must declare their own data size. If the cumulative data size of all the providers does not meet the consumer's needs, the transaction is then canceled. Similarly, to prevent malicious behavior, data providers must also pay a deposit when applying to participate in the transaction.

(3) Arbitration Committee: This committee is selected through mutual consultation between both trading parties and is exclusively valid for the current transaction. Committee members are also required to pay a deposit to prevent malicious behavior, such as delaying or refusing arbitration. At the same time, in order to motivate committee members, they will receive rewards after completing the arbitration on time, which come from both parties involved in the transaction that require arbitration. The number of members, r, in the committee adheres to the rule $t < r \leq 2t - 1$. After the committee's formation, each member receives a secret share s_i of the arbitration private key, distributed by the key management entity. If any abnormality occurs

during the transaction process, such as one party exhibiting dishonest behavior and refusing to use its private key to decrypt a verifiable encrypted signature, any member of the committee can jointly rebuild the arbitration private key, decrypt it, and extract the digital signature. As long as any t members within the committee are honest and secure, it ensures the fairness of the arbitration committee and the security of the private key.

(4) Blockchain: Consortium blockchains, as a specific type of blockchain, possess access controls, comply with the requirement of reviewing user settings, and maintain a relatively stable set of participating nodes. The system employs the consortium blockchain as a distributed environment required for data trading between data consumers and providers. Throughout the data trading process, all participating entities collaboratively maintain the blockchain ledger. Failures or departures of individual nodes will not disrupt the entire data transaction process, thereby enhancing the robustness of the data trading market. Furthermore, due to the blockchain's inherent attributes of transparency, immutability, and traceability, transaction details and the reputation evaluations of participants are logged onto the blockchain. Nodes with malicious behaviors are penalized, enhancing the model's security and fairness.

4.2. Threats and Security Goals

The system assumes the data provided by the data providers is genuine. These nodes have undergone rigorous review before joining and aim to achieve a successful transaction with a high-quality noisy dataset. However, they could potentially face challenges related to privacy, security, or fair reward. The following discusses the threats faced by the system and the security goals achieved in responding to these threats.

Threat 1: Privacy leakage of data providers. The information offered by data providers could pose severe adverse consequences, such as the exposure of sensitive details (names, addresses, phone numbers, social accounts, etc.). Malicious entities may use this information to pose threats to users' personal safety and assets. In addition to personal information, other data provided can also be used for data analysis to reveal preferences, interests, behaviors, etc. This may have adverse effects, such as dynamic pricing based on big data.

Security Goal 1: Privacy protection of local data. Throughout the data transaction process, without voluntarily disclosing their local data, data providers will not compromise the privacy of sensitive data. No data provider can directly or indirectly access the real data information of other data providers during the cooperative transaction process. Data providers use local differential privacy to perturb sensitive data before uploading it, rather than sending plaintext, which ensures that no one can infer the provider's local data information from the perturbed dataset.

Threat 2: The erroneous behavior of participants. Mainly including three types of incorrect behavior: (1) data providers deceitfully report a larger data size to garner more compensation while providing a smaller actual size; (2) after receiving payment, the data provider intentionally fails to send the perturbed dataset, which will result in direct losses for the data consumer; (3) after obtaining the perturbed dataset, data consumers intentionally withhold payments, which will result in direct losses for the data provider.

Security Goal 2: Fair protection of reward for data providers. The system weighs a data provider's reward based on three key aspects: (1) size of the local data size, which remains unchanged after perturbation. (2) Privacy budget: a smaller privacy budget means higher privacy protection and lower data availability, which means less reward, and vice versa. (3) Credibility value: only by diligently participating in data perturbation and trading more data size can providers elevate their credibility score, with those erring seeing a reduction. High credibility ensures more rewards. Additionally, the system also implements punitive measures. Providers who misbehave will be fined and honest providers will be compensated.

Security Goal 3: Secure transactions. The transaction process utilizes the verifiable encrypted signature technology. Both parties first agree on the transaction terms. Following

this, the data consumer signs the agreement using a verifiable encrypted signature, which anyone can verify for validity. Once the signature's validity is confirmed, the data provider furnishes the perturbed dataset. After receiving this dataset, the data consumer uses their private key to extract their signature, completing the transaction. If the data consumer cheats and refuses to use their key, the data provider can appeal to the arbitration committee for decryption and penalize the deceitful party.

4.3. Workflow

Table 1 enumerates and explains the relevant symbols:

Table 1. Description of symbols.

Symbol	Description
P_s, P_c	data providers and data consumers engaged in transactions
N	minimum data volume required by P_c
ε	minimum privacy budget required by P_c
P_i	the i-th data provider
D_i, d_i	The local raw dataset of P_i,the size of the datasetD_i
ε_i	The privacy budget of P_i
L_i, l_i	The private dataset of P_i , the size of the dataset of L_i
G_i	The perturbed dataset of P_i
α_i	The privacy protection level of L_i
n	the number of data providers
APK	arbitration public key for verifiable encrypted signatures
(pk_c, sk_c)	The public key and private key for encrypting and decrypting signatures by P_c
$intersect(X, Y)$	function to determine the number of common elements between sets X and Y

Based on processes ① to ⑦ in Figure 1, the workflow of the system mainly includes four stages: initialization, local data perturbation, data transaction, and arbitration.

Initialization stage: Data consumers issue a data transaction request T (N, ε) to the blockchain and deposit a fee as collateral (as in Process ①). Data nodes can apply based on their computational capacity and data resource conditions. Nodes approved for the task become data providers for this transaction and also contribute a fee as a deposit. During the application process, data node i states its local data size d_i. If the final total data size $\sum_{i=1}^{n} d_i$ is less than N, the task is aborted. The specific approval method can be through offline negotiations, which is beyond the paper's primary focus. Nodes not involved in the transaction can propose to form an arbitration committee with data consumers and providers. Members of the arbitration committee must gain mutual consent from both transaction parties.

Local data perturbation stage: Firstly, the data provider P_i clarifies that the dataset D_i they are about to use for transactions and the privacy dataset L_i they want to focus on protecting belong to D_i. Then, based on their own situation, they balance the privacy protection of data and the transaction rewards they want to obtain to determine their respective privacy budget ε_i. The privacy budget ε_i cannot be less than the minimum privacy budget ε required by data consumers P_c. Due to the characteristics of differential privacy technology, the larger the privacy budget, the higher the data availability, and the greater the rewards obtained, but the weaker the privacy protection. Conversely, the smaller the privacy budget, the better the privacy protection, but the lower the data availability, and the fewer transaction rewards obtained. Next, the data provider P_i utilizes

the algorithm MDLDP to locally perturb dataset D_i to obtain perturbed dataset G_i for transaction (as shown in process ②). In order to achieve better privacy protection for L_i, i.e., a greater degree of privacy protection α_i, the algorithm MDLDP requires multiple random perturbations to select one of the best results. Due to the unchanged privacy budget ε_i, the overall availability of dataset G_i has not decreased. Finally, the data provider P_i uploads the perturbed dataset G_i and privacy budget ε_i and other information to the blockchain for transaction (as in process ③). The MDLDP algorithm is as follows (Algorithm 1):

Algorithm 1. The MDLDP Algorithm

Input: D_i, ε_i, L_i
Output: G_i, α_i
Create array *indice* [L_i] for storing the index of dataset L_i;
Create array *indice* [G_{ij}] storing the index of the perturbed data in dataset G_{ij};
$p_i = \exp\{\varepsilon_i\}/(\exp\{\varepsilon_i\} + d_i - 1)$;
for j 1 to h by 1 // independent perturbations of the original dataset D_i h times
for z 1 to d_i by 1 // Randomly perturb each element in dataset D_i with probability $1 - p_i$
if rand() < p_i
g_{ijz} = value$_{ijz}$; // value$_{ijz}$ refers to the true value in D_i, g_{ijz} is an element in G_{ij}
else
g_{ijz} = rand(D_i)/value$_{ijz}$;
end
Obtaining perturbed dataset G_{ij};
$\alpha_{ij} = intersect\left(indice\left[G_{ij}\right], indice[L_i]\right)/l_i$; // Calculate degree of privacy protection α_{ij} to evaluate the effectiveness of this perturbation
end
Take α_{ij} the result of the largest perturbation as G_i and α_i;
return G_i, α_i.

Data transaction stage: Initially, the data provider P_s aggregates all data from providers (as in Process ④) and negotiates with data consumer P_c regarding fees and data sharing, primarily encompassing reward details. Following this, P_c and P_s generate their respective key pairs (pk_c, sk_c) and (pk_s, sk_s) using the public key APK. P_c generates his true signature σ_i based on $Sign(pp, sk_c, m)$. P_c then produces a verifiable encrypted signature σ_c^{VES} using $VESSign(sk_c, m, APK)$ to sign the transaction agreement. Anyone can validate the validity of the signature via the arbitrator's provided public key APK. But without the help of the P_c or the arbitration committee, it is impossible to extract the true signature σ_i. Once the agreement is signed and validated, P_s delivers the perturbed data set $G = \sum_{i=1}^{n} G_i$ to P_c. After confirming the G dataset, P_s decrypts the encrypted signature σ_c^{VES} using its private key sk_c and extracts the true signature σ_i to validate the agreement and complete the transaction (as in Process ⑤).

Arbitration stage: If P_c acts deceitfully during the transaction, refusing to decrypt the encrypted signature σ_c^{VES} to extract the true signature σ_i to complete the agreement, i.e., paying compensation. Data providers P_s can seek assistance from arbitration committees. any t members within the arbitration committee can utilize Equation (3) to reconstruct the arbitration private key ASK (as in Process ⑥). Based on the characteristics of verifiable encrypted signature technology, the private key ASK can directly extract the true signature σ_i of data consumer P_c from the encrypted signature σ_c^{VES} (as in Process ⑦). Forcing data consumer P_c to execute agreements to pay compensation. Dishonest trading behavior will result in the confiscation of margin as compensation for honest traders and arbitrators.

5. Verifiable Encrypted Signature

To facilitate fair transactions and safeguard both transaction parties' legitimate rights, this paper introduces a verifiable encrypted signature protocol. Traditional verifiable encrypted signature protocols assume a single and neutral arbitrator [39], but such an arbitrator may experience a single point of failure or cheating behavior. To address this issue, we merge the verifiable encrypted signature with the threshold signature, replacing

the traditional arbitrator with a committee. Every committee member holds a secret share s_i, and any t members can reconstruct the arbitration private key. The verifiable encrypted signature protocol is detailed below:

Setup: enter the security parameter λ, choose two large primes of length λ/2, and compute the product of these two large primes N. Choose a random element in the group $Z^*_{\Phi(N)}$, and compute the element s such that $se = 1 \ mod \ \Phi(N)$. The system public key is (N, e). The corresponding private key is (N, s), according to Equation (2), s is divided into r parts, held by r members of the arbitration committee. When arbitration is needed, any t members can use Equation (3) to reconstruct s and decrypt the corresponding verifiable encrypted signature.

KeyGen: The data provider P_s randomly selects $g_1 Z^*_{\Phi(N)}$, and selects $x_s\{0,1\}^\lambda$, calculates $g = {g_1}^2 \ mod \ N$, $y_s = g^{x_s} \ mod \ N$. The data consumer P_c selects the element $x_c \in \{0,1\}^\lambda$ and computes $y_c = g^{x_c} \ mod \ N$. The public key for P_s is y_s, with a private key $sk_s = x_s$. The public key for P_c is y_c, with a private key $sk_c = x_c$.

Sign: outputs the transaction protocol Tx, P_c computes a signature

$$\sigma_c = H(Tx)^s \ mod \ N.$$

Verify: taking as input the transaction agreement Tx, signature σ_c and the system public key (N, e). Verify whether the

$${\sigma_c}^e = H(Tx)^s \ mod \ N.$$

If the equation holds, output 1, indicating that the signature σ_c is valid, otherwise output 0, indicating that the signature is invalid.

PreSign: P_c select the element $r \in \{0,1\}^\lambda$, and calculate $y_r = g^r mod \ N$ and also calculate the secret factor $u = y_s^{x_c} mod \ N$ and $m' = u^e H(Tx) mod \ N$. P_s Calculate the secret factor $u' = y_v^{x_s} mod \ N$, and verify whether $m' = u'^e H(Tx) mod \ N$.

VESSign: P_c selects an element t from the set $t \in \{0,1\}^\lambda$, and calculates $\sigma' = m'^{2s} y_c^r mod \ N$, $y_e = y_s^e mod \ N$, $y_{er} = y_s^r mod \ N$, $y_t = g^t mod \ N$, $y_{et} = y_e^t mod \ N$, $c = H(m', y_{er}, y_r, y_e, g, y_{et}, y_t)$. P_c then computes $z = t - rc$, and outputs the verifiable encrypted signature $\sigma_c^{VES} = (\sigma', c, z)$.

VESVer: Given the system's public key (N, e), P_c's public key pk_c, P_s's public key pk_s, and the parameters g, m', y_r, as well as the verifiable encrypted signature σ_c^{VES}, computes $w_{er} = \sigma'^e m'^{-2} \ mod \ N$, $y'_e = y_s^e mod \ N$,$w_{er} = y_e'^z w_{er}^c \ mod \ N$, $w_t = g_z y_r^c$ and

$$c' = H(m', w_{er}, y_r, y'_e, g, w_{et}, w_t)$$

If $c = c'$, then output 1, indicating that the verifiable encrypted signature σ_c^{VES} valid. Otherwise, output 0, indicating that the signature is invalid.

VESExt: given the output σ', y_r, u', P_s compute $\sigma_s = \sigma' \left(y_r^{x_c}\right)^{-1} u'^{-2} mod N$.

Assume that $2\alpha + e\beta = 1$, then $H(Tx)^d = \sigma_s^\alpha H(Tx)^\beta \ mod \ N$, P_s extracts σ_c from σ_s.

6. Security Analysis

6.1. Privacy Protection

We use a lemma to prove that the model can protect the privacy of data providers P_i.

Lemma 1: *If the data provider P_i does not leak data locally, the proposed model ensures the privacy and security of the data provider.*

Proof. The data provider P_i determines the dataset D_i used for the transaction before the transaction and determines the privacy budget ε_i based on privacy protection and compensation needs. Then, the algorithm MDLDP is used to perturb dataset D_i to obtain G_i. Finally, upload the privacy budget ε_i and perturbed dataset G_i to the blockchain for

transaction. The entire process is conducted locally, so this model can ensure the privacy and security of the data provider P_i. □

6.2. Fairness Assurance

The system's transaction mechanism and financial incentive structure guarantee fairness for data providers. This mechanism will prevent malicious behavior by data providers and encourage them to actively provide perturbed datasets. Data providers must pay a fee as a deposit when registering for a transaction. The size of the provided data and the privacy budget serve as bases for reward, both correlating positively with the reward. In addition to transaction rewards, data providers can earn bonuses tied to their reputation score. Only by actively and honestly providing data can they enhance their credibility. High-credibility data providers will receive more rewards. The system enforces penalties: dishonest data providers will be fined, with deductions made from their initial deposit, compensating honest data providers in the process.

6.3. Transactional Security

Lemma 2: *If any t members of the arbitration committee are honest, then the verifiable encrypted signature protocol proposed in this paper achieves fair payment.*

Proof. There are only four situations in the transaction process: (1) both parties are honest; (2) The data provider P_s is honest, while the data consumer P_c is dishonest; (3) Data consumers P_c are honest, while data providers P_s are dishonest; (4) Both parties in the transaction are dishonest. □

Situation (1). The data provider P_s will provide the data $G = \sum_{i=1}^{n} G_i$ honestly, and the data consumer P_c will also pay the compensation honestly, which is fair to both parties.

Situation (2). The data provider P_s and the data consumer P_c have negotiated an agreement regarding payment of compensation. The data provider P_s provides the data G after verifying the verifiable encrypted signature σ_c^{VES} of the data consumer P_c, and the data consumer P_c refuses to decrypt the encrypted signature σ_c^{VES} after obtaining the dataset G. Any t members of the arbitration committee will collaborate to generate the arbitration private key ASK, which can directly decrypt the encrypted signature σ_c^{VES} to make the payment agreement effective. The implementation of the agreement will be resolved by law. Ensuring fairness.

Situation (3). The data provider P_s and data consumer P_c negotiate a payment agreement, and the data consumer P_c performs a verifiable encrypted signature σ_c^{VES} on the payment agreement, but the data provider P_s refuses to provide the dataset G. The probability of a data provider P_s successfully cracking an encrypted signature without a private key to defraud a reward is negligible. Meanwhile, due to the number of committee members $t < r \leq 2t - 1$, and t members being honest, it is impossible for t dishonest members to collude with data providers P_s, and dishonest data providers P_s cannot receive any rewards. Ensuring fairness.

Situation (4). The data provider P_s will not provide the data honestly, and the data consumer P_c will not make the payment honestly. Both parties have no losses, but both parties will be deducted the deposit due to malicious behavior, which is fair to both parties.

7. Experiments

This section describes the experimental environment for the algorithm MDLDP and evaluates it from the perspectives of privacy protection, data availability, and time cost.

7.1. Experimental Setup

To assess the MDLDP algorithm, experiments were conducted on the real-world dataset "Air Quality" [40]. The dataset consists of 9358 instances recorded by five metal

oxide chemical sensor arrays embedded in air quality chemical multisensory devices. These devices are located on the ground in a heavily polluted area of Italy, with a recorded duration from March 2004 to February 2005. These data, provided by certified reference analyzers from the same region, represent hourly average concentrations of ground-level pollutants such as carbon monoxide, non-methane hydrocarbons, benzene, total nitrogen oxides, and nitrogen dioxide. For comparison, this article randomly selected 500 data from non-methane hydrocarbons, except for missing values. This article uses the MATLAB platform for simulation experiments. All experimental programs are written in the MATLAB R2018b platform using the MATLAB language, and the experimental hardware environment is Intel (R) Core (TM)i3-7100U, equipped with a CPU @ 2.40 GHz and 8 GB RAM, running on the Windows 10 operating system. The equipment comes from Qingdao, China, and the manufacturer is Lenovo Company.

This article uses privacy protection degree α to evaluate the privacy protection effect of algorithm MDLDP. G_j represents the perturbed dataset obtained by the data provider after the j-th perturbed of the original dataset D. L represents the privacy dataset of the data provider, which is a part of the original dataset D. $\Delta(L, G_j)$ represents the number of perturbed data in the privacy dataset L after the j-th perturbed, l represents the amount of data in dataset L. $\frac{\Delta(L,G_j)}{l}$ represents the proportion of perturbed data in the privacy dataset L, which is the degree of protection for the privacy dataset. According to the MDLDP algorithm, the data provider needs to perform h random perturbations on the dataset and select the result with the maximum degree of protection. In addition, due to the randomness of differential privacy, w privacy protection degrees will be generated in the experiment, and their average value will be taken as the final result.

$$\alpha_k = \max_{j=1,2,\ldots,h} \frac{\Delta(L, G_j)}{l}, \tag{4}$$

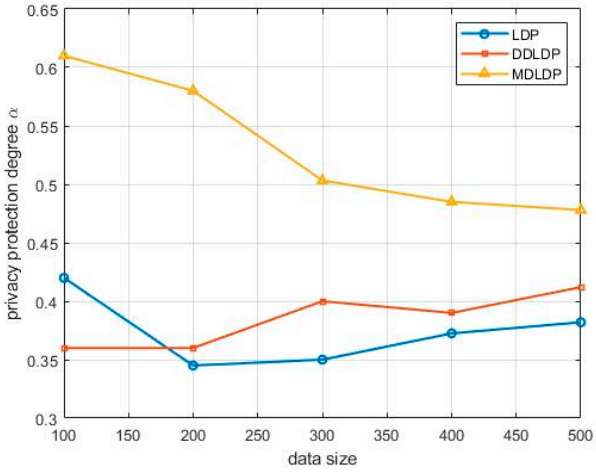
$$\alpha = \frac{1}{w} \sum_{k=1}^{w} \alpha_k. \tag{5}$$

In this paper, we use the commonly used method of mean square error (*MSE*) to evaluate the data availability of the algorithm, such as [41]. Among them, $(a_1, a_2, \cdots, a_n)$ denotes the real data in the Original dataset D, $(a'_1, a'_2, \cdots, a'_n)$ represents the data in the perturbed dataset G.

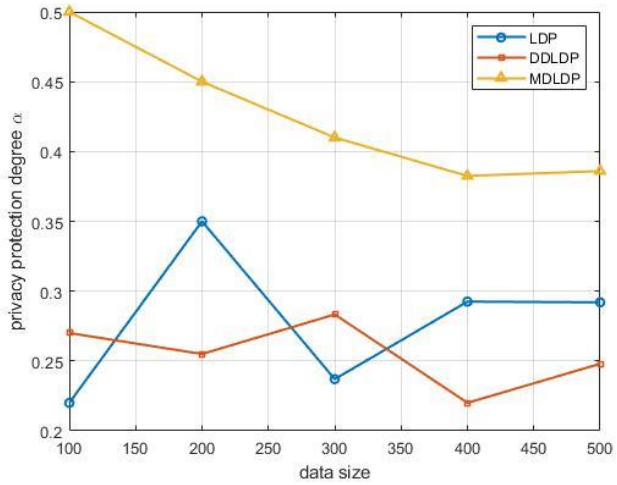
$$MSE = \frac{1}{n} \sum_{i=1}^{n} (a'_i - a_i)^2. \tag{6}$$

7.2. Experimental Analysis

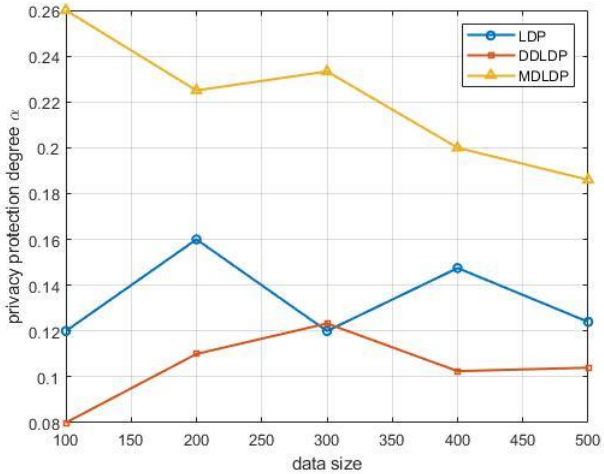
In the work of using local differential privacy technology to protect user privacy, most of them use other implementation mechanisms such as Laplace, while the use of random perturbation mechanisms is relatively rare. Therefore, this article chose the traditional LDP algorithm [42] and DDLDP [43] as a comparison, both of which use random perturbation mechanisms. To ensure a fair comparison, five data groups identical in size to [43] were chosen, with sizes of 100, 200, 300, 400, and 500, respectively. Three different privacy budgets were selected: $\varepsilon = 0.5$, $\varepsilon = 1.0$, and $\varepsilon = 2.0$. Figure 2 shows the privacy protection degree under different data sizes for the three algorithms. To prevent randomly inconsistent results, we chose $w = 10$ and calculated the average of 10 instances. Moreover, the experiment randomly selected 10% of the data size from the original set D as private data L.



(**a**) Privacy budget $\varepsilon = 0.5$



(**b**) Privacy budget $\varepsilon = 1.0$



(**c**) Privacy budget $\varepsilon = 2.0$

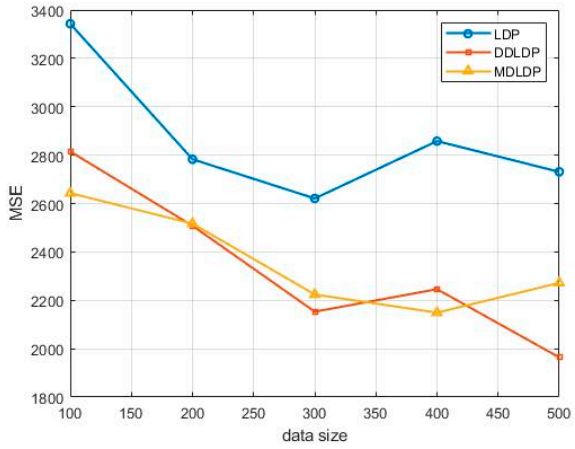
Figure 2. Privacy-preserving degrees of private dataset with different data sizes.

According to Equations (4) and (5), we obtained the privacy protection degrees of three algorithms under different privacy budgets and data sizes. As shown in Figure 2, under three different privacy budgets, the privacy protection of the MDLDP method is generally higher than that of the other two comparison methods. This indicates that the MDLDP

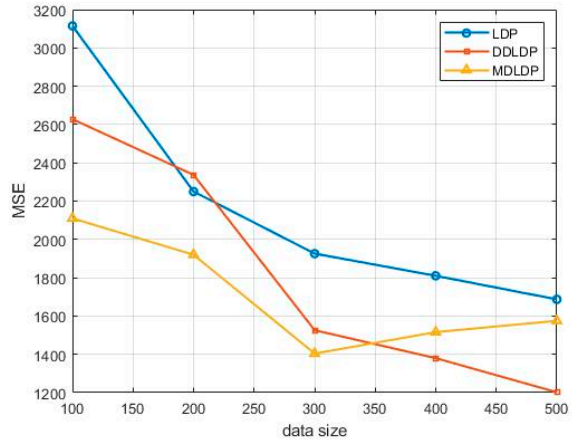
method can better and more accurately protect the privacy dataset L. As the amount of data increases, the degree of privacy protection α slightly decreases and eventually stabilizes.

According to Equation (6), we obtained the mean square error (MSE) of three algorithms under different privacy budgets and data sizes. From Figure 3, it can be observed that under varying privacy budgets and data sizes, the traditional LDP method exhibits a slightly larger mean squared error, indicating its relatively lower data availability. The mean squared error of the MDLDP method is close to that of the DDLDP method, suggesting that both methods offer better data availability. In conjunction with Figure 2, it can be concluded that the MDLDP method not only offers superior privacy protection but also ensures great data availability. This is because under the same privacy budget, the MDLDP method tends to protect private datasets and relatively reduces the protection of non-private data.

Figure 4 depicts the perturbation time of the three algorithms at different data sizes. As the data size increases, the fluctuation in perturbation time for all three algorithms remains within a certain range, with these fluctuations being related to the randomness of differential privacy. When the data size is constant, the perturbation time for each algorithm under different privacy budgets is roughly equivalent, which aligns with the characteristics of differential privacy. As can be observed from Figure 4, the time consumed by the MDLDP algorithm is approximately on par with the DDLDP algorithm, both of which are slightly longer than that of the LDP algorithm. But compared to better privacy protection, these limited excess time consumption are acceptable. Due to the fact that time consumption does not significantly change with changes in privacy budget or data volume, the MDLDP method has good practicality.

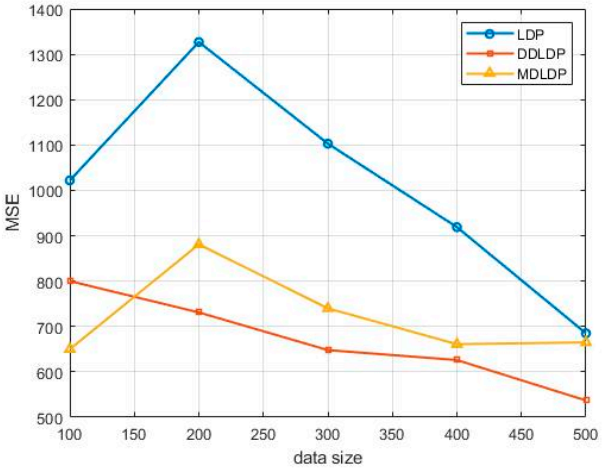


(**a**) Privacy budget $\varepsilon = 0.5$



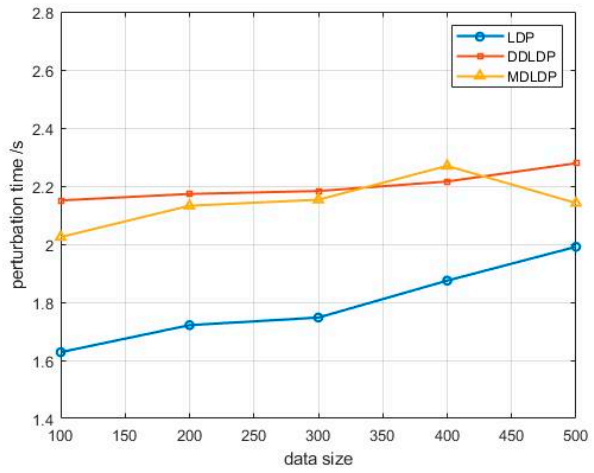
(**b**) Privacy budget $\varepsilon = 1.0$

Figure 3. *Cont.*

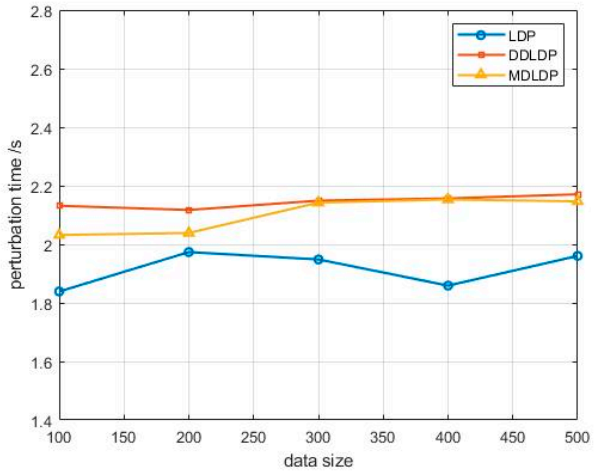


(**c**) Privacy budget ε = 2.0

Figure 3. Mean Square Error with different data sizes.

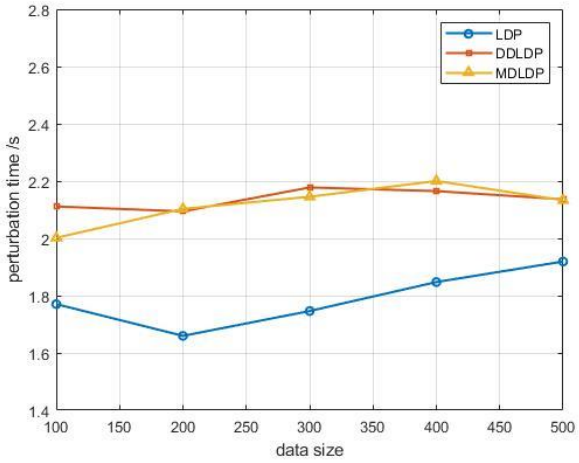


(**a**) Privacy budget ε = 0.5



(**b**) Privacy budget ε = 1.0

Figure 4. *Cont.*



(**c**) Privacy budget $\varepsilon = 2.0$

Figure 4. Time consumption for perturbing different data sizes.

8. Conclusions and Future Works

This paper introduces a decentralized, privacy-preserving, and fair data transaction model based on blockchain technology. The model safeguards the privacy of local data by designing an adaptive local differential privacy algorithm, MDLDP, and ensures fair data transactions using verifiable encrypted signatures. Instead of the traditional single arbitrator found in conventional verifiable encrypted signatures, the proposed model introduces a committee. Through threshold signature technology, the arbitration private key is divided and managed by the committee members. In the event of transaction disputes, any t members of the committee can collaborate to reconstruct the arbitration private key for arbitration. Theoretical analysis shows that our method can effectively protect the privacy of data providers, ensure fair transaction markets, and safeguard the security of arbitration private keys, preventing the theft or loss of arbitration private keys due to single-point failures. In addition, this method also prevents collusion between dishonest traders and arbitrators and achieves fair payment in transactions. We evaluated the MDLDP algorithm on a real-world dataset. Compared with existing methods, although the MDLDP algorithm has slightly more time consumption than the method with the lowest time consumption, it has better privacy protection and can more accurately protect users' privacy datasets. Meanwhile, this method will not reduce data availability. Due to the fact that time consumption does not significantly change with changes in privacy budget or data volume, the limited excess time consumption of the MDLDP method is acceptable and has good practicality.

However, although we conducted simulation experiments using MATLAB, there is a lack of specific implementation details on real blockchain platforms, such as node registration and approval, consensus algorithms, transactions, and data storage. We plan to further validate the model on specific blockchain platforms such as Hyperledger in the future. The model proposed in this article assumes that honest data providers provide effective and high-quality data. How to verify data quality and ensure data validity is a problem that needs to be solved in the future. In addition, it is also a valuable study that high availability and low latency access may be required for IoT systems.

Author Contributions: Conceptualization, W.Z. (Wei Zhou) and D.Z.; methodology, D.Z.; software, D.Z. and G.H.; validation, W.Z. (Wei Zhou), D.Z. and W.Z. (Wenyin Zhu); formal analysis, D.Z.; investigation, X.W. and W.Z. (Wenyin Zhu); resources, X.W.; data curation, D.Z. and W.Z. (Wenyin Zhu); writing—original draft preparation, D.Z.; writing—review and editing, W.Z. (Wei Zhou) and G.H.; visualization, X.W.; supervision, W.Z. (Wei Zhou); project administration, W.Z. (Wei Zhou); funding acquisition, W.Z. (Wei Zhou). All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China under Grant Numbers 61502262 and 62001262.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Publicly available datasets were analyzed in this study. This data can be found here: (https://archive.ics.uci.edu/dataset/360/air+quality, accessed on 31 July 2023).

Conflicts of Interest: Authors Wei Zhou and Wenyin Zhu were employed by the company Qingdao Haier Smart Technology R&D Co., Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Liang, F.; Yu, W.; An, D.; Yang, Q.; Fu, X.; Zhao, W. A survey on big data market: Pricing, trading and protection. *IEEE Access* **2018**, *6*, 15132–15154. [CrossRef]
2. Miao, Q.; Lin, H.; Hu, J.; Wang, X. An intelligent and privacy-enhanced data sharing strategy for blockchain-empowered Internet of Things. *Digit. Commun. Netw.* **2022**, *8*, 636–643. [CrossRef]
3. Jung, T.; Li, X.Y.; Huang, W.; Qian, J.; Chen, L.; Han, J.; Hou, J.; Su, C. Accounttrade: Accountable protocols for big data trading against dishonest consumers. In Proceedings of the IEEE Conference on Computer Communications (IEEE INFOCOM 2017), Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.
4. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egypt. Inform. J.* **2022**, *23*, 329–343. [CrossRef]
5. Bhushan, B.; Sinha, P.; Sagayam, K.M.; Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Comput. Electr. Eng.* **2021**, *90*, 106897. [CrossRef]
6. Chen, S.; Fu, A.; Shen, J.; Yu, S.; Wang, H.; Sun, H. RNN-DP: A new differential privacy scheme base on Recurrent Neural Network for Dynamic trajectory privacy protection. *J. Netw. Comput. Appl.* **2020**, *168*, 102736. [CrossRef]
7. Barbaro, M.; Zeller, T.; Hansell, S. A face is exposed for AOL searcher no. 4417749. *New York Times*, 9 August 2006.
8. Narayanan, A.; Shmatikov, V. Robust de-anonymization of large sparse datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP 2008), Oakland, CA, USA, 18–21 May 2008; pp. 111–125.
9. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating noise to sensitivity in private data analysis. In Proceedings of the Theory of Cryptography: Third Theory of Cryptography Conference (TCC 2006), New York, NY, USA, 4–7 March 2006; Springer Springer: Berlin/Heidelberg, Germany, 2006; pp. 265–284.
10. Fotiou, N.; Pittaras, I.; Siris, V.A.; Polyzos, G.C.; Anton, P. A privacy-preserving statistics marketplace using local differential privacy and blockchain: An application to smart-grid measurements sharing. *Blockchain Res. Appl.* **2021**, *2*, 100022. [CrossRef]
11. Asokan, N.; Schunter, M.; Waidner, M. Optimistic protocols for fair exchange. In Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, 1–4 April 1997; pp. 7–17.
12. Bhushan, B.; Sahoo, C.; Sinha, P.; Khamparia, A. Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. *Wirel. Netw.* **2021**, *27*, 55–90. [CrossRef]
13. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Cross-domain secure data sharing using blockchain for industrial IoT. *J. Parallel Distrib. Comput.* **2021**, *156*, 176–184. [CrossRef]
14. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
15. Sabu, S.; Ramalingam, H.M.; Vishaka, M.; Swapna, H.R.; Hegde, S. Implementation of a Secure and privacy-aware E-Health record and IoT data Sharing using Blockchain. *Glob. Transit. Proc.* **2021**, *2*, 429–433. [CrossRef]
16. Thantharate, P.; Thantharate, A. ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. *Big Data Cogn. Comput.* **2023**, *7*, 165. [CrossRef]
17. Cui, J.; Ouyang, F.; Ying, Z.; Wei, L.; Zhong, H. Secure and efficient data sharing among vehicles based on consortium blockchain. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 8857–8867. [CrossRef]
18. Du, Z.; Zhang, J.; Fu, Y.; Huang, M.; Liu, L.; Li, Y. A Scalable and Trust-Value-Based Consensus Algorithm for Internet of Vehicles. *Appl. Sci.* **2023**, *13*, 10663. [CrossRef]
19. Zhang, K.; Tian, J.; Xiao, H.; Zhao, Y.; Zhao, W.; Chen, J. A numerical splitting and adaptive privacy budget-allocation-based LDP mechanism for privacy preservation in blockchain-powered IoT. *IEEE Internet Things J.* **2022**, *10*, 6733–6741. [CrossRef]
20. Hong, L.; Zhang, K.; Gong, J.; Qian, H. Blockchain-Based Fair Payment for ABE with Outsourced Decryption. *Peer Peer Netw. Appl.* **2023**, *16*, 312–327. [CrossRef]

21. Zhou, J.; Tang, F.; Zhu, H.; Nan, N.; Zhou, Z. Distributed data vending on blockchain. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1100–1107.
22. Niu, C.; Zheng, Z.; Wu, F.; Gao, X.; Chen, G. Trading data in good faith: Integrating truthfulness and privacy preservation in data markets. In Proceedings of the 2017 IEEE 33rd International Conference on Data Engineering (ICDE), San Diego, CA, USA, 19–22 April 2017; pp. 223–226.
23. Djuric, Z.; Gasevic, D. FEIPS: A secure fair-exchange payment system for internet transactions. *Comput. J.* **2015**, *58*, 2537–2556. [CrossRef]
24. Goldfeder, S.; Bonneau, J.; Gennaro, R.; Narayanan, A. Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin. In Proceedings of the Financial Cryptography and Data Security: 21st International Conference (FC 2017), Sliema, Malta, 3–7 April 2017; Revised Selected Papers 21. Springer International Publishing: Berlin/Heidelberg, Germany, 2017; pp. 321–339.
25. Chen, Y.; Guo, J.; Li, C.; Ren, W. FaDe: A blockchain-based fair data exchange scheme for big data sharing. *Future Internet* **2019**, *11*, 225. [CrossRef]
26. Kurtulmus, A.B.; Daniel, K. Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain. *arXiv* **2018**, arXiv:1802.10185.
27. Wang, S.; Tang, X.; Zhang, Y.; Chen, J. Auditable protocols for fair payment and physical asset delivery based on smart contracts. *IEEE Access* **2019**, *7*, 109439–109453. [CrossRef]
28. Zhao, Y.; Yu, Y.; Li, Y.; Han, G.; Du, X. Machine learning based privacy-preserving fair data trading in big data market. *Inf. Sci.* **2019**, *478*, 449–460. [CrossRef]
29. Sweeney, L. k-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl. Based Syst.* **2002**, *10*, 557–570. [CrossRef]
30. Fung BC, M.; Wang, K.; Philip, S.Y. Anonymizing classification data for privacy preservation. *IEEE Trans. Knowl. Data Eng.* **2007**, *19*, 711–725. [CrossRef]
31. Dwork, C. Differential privacy: A survey of results. In Proceedings of the International Conference on Theory and Applications of Models of Computation, Xi'an, China, 25–29 April 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 1–19.
32. Dwork, C. Differential privacy. In Proceedings of the International Colloquium on Automata, Languages, and Programming, Venice, Italy, 10–14 July 2006; Springer: Berlin/Heidelberg, Germany, 2006; pp. 1–12.
33. Dwork, C.; Lei, J. Differential privacy and robust statistics. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May–2 June 2009; pp. 371–380.
34. Wang, T.; Zhang, X.; Feng, J.; Yang, X. A comprehensive survey on local differential privacy toward data statistics and analysis. *Sensors* **2020**, *20*, 7030. [CrossRef] [PubMed]
35. Warner, S.L. Randomized response: A survey technique for eliminating evasive answer bias. *J. Am. Stat. Assoc.* **1965**, *60*, 63–69. [CrossRef] [PubMed]
36. Gu, C.; Zhu, Y. An id-based verifiable encrypted signature scheme based on Hess's scheme. In Proceedings of the International Conference on Information Security and Cryptology, Santa Barbara, CA, USA, 14–18 August 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 42–52.
37. Desmedt, Y. Society and group oriented cryptography: A new concept. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 16–20 August 1987; Springer: Berlin/Heidelberg, Germany, 1987; pp. 120–127.
38. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
39. Li, D.; Chen, R.; Wan, Q.; Guan, Z.; Li, S.; Xie, M.; Su, J.; Liu, J. Intelligent and Fair IoV Charging Service Based on Blockchain with Cross-Area Consensus. *IEEE Trans. Intell. Transp. Syst.* **2023**. [CrossRef]
40. Vito, S. Air Quality. *UCI Mach. Learn. Repos.* **2016**. [CrossRef]
41. Li, M.; Zeng, Y.; Guo, Y.; Guo, Y. A movie recommendation system based on differential privacy protection. *Secur. Commun. Netw.* **2020**, *2020*, 6611463. [CrossRef]
42. Fanti, G.; Pihur, V.; Erlingsson, Ú. Building a RAPPOR with the unknown: Privacy-preserving learning of associations and data dictionaries. *arXiv* **2015**, arXiv:1503.01214. [CrossRef]
43. Sun, Z.; Wang, Y.; Cai, Z.; Liu, T.; Tong, X.; Jiang, N. A two-stage privacy protection mechanism based on blockchain in mobile crowdsourcing. *Int. J. Intell. Syst.* **2021**, *36*, 2058–2080. [CrossRef]