Hindawi
Mobile Information Systems
Volume 2021, Article ID 7397926, 13 pages
https://doi.org/10.1155/2021/7397926

*Research Article*

# Blockchain-Enhanced Fair and Efficient Energy Trading in Industrial Internet of Things

**Jianwen Hu**,[1,2] **Yuling Chen**,[1,2] **Xiaojun Ren**,[3] **Yixian Yang**,[4] **Xiaobin Qian**,[5] **and Xiaomei Yu**[6]

[1]*College of Computer Science and Technology, Guizhou University, Guiyang 550000, China*
[2]*State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550000, China*
[3]*Blockchain Laboratory of Agricultural Vegetables, Weifang University of Science and Technology, Weifang 261000, China*
[4]*School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100000, China*
[5]*Guizhou CoVision Science & Technology Co. Ltd, Guiyang 550000, China*
[6]*School of Information Science and Engineering, Shandong Normal University, Jinan 250000, China*

Correspondence should be addressed to Yuling Chen; ylchen3@gzu.edu.cn

Received 1 September 2021; Revised 26 September 2021; Accepted 29 October 2021; Published 17 November 2021

Academic Editor: Xuyun Zhang



As the technical support of the industrial Internet of Things, blockchain technology has been widely used in energy trading, data transactions, and Internet of Vehicles. However, most of the existing energy trading models only address the transaction security and transaction privacy issues that arise in the energy trading process, ignoring the fairness of resource allocation and transaction equity in the trading process. In order to tackle those problems, an energy trading scheme called HO-TRAD is proposed in this paper to improve the efficiency of model trading while ensuring the fairness of energy trading. We propose a new trading strategy in the HO-TRAD energy trading scheme that guarantees fairness in the allocation of trading resources by introducing an entity's active reputation value. Use smart contracts to achieve transparency and ensure fairness in the transaction process. Based on the identity verification foundation of the consortium chain, the scheme enhances the existing PBFT consensus algorithm and improves the efficiency of model transactions. The experimental simulation indicates that the scheme requires less transaction time and has higher transaction fairness and security.

## 1. Introduction

As the core solution to realize Industry 4.0 [1], industrial Internet of Things (IoT) has become the focus of academic circles. With the development of the Internet of Things technology, the intelligent characteristics of the Internet of Things have also gained considerable growth. Nevertheless, due to the continuous innovation of industrial technology, the demand for industrial energy is increasing day by day, and how to ensure the energy supply of in IoT has become a hot research point. To overcome these problems, smart grid [2], vehicle energy Internet [3, 4], and virtual power plan [5] have been proposed successively.

However, a majority of existing energy trading schemes are centralized; there is a possibility for the occurrence of single point of failure since a third party is allowed to serve as a controller to manage or control all transaction and registration information. The reason is that energy nodes must rely on a central entity to handle energy distribution, resource allocation, entity registration, and authentication [6, 7], which may bring some potential security issues.

The security of transactions and user privacy issues have been a concern in industrial IoT energy trading [8, 9]. Attackers may bypass user authentication mechanism [10, 11], disrupt energy trading central to collect transaction user data, and perform privacy analysis of the acquired

transaction data to extract sensitive user information. Therefore, most existing research focuses on the security and privacy of industrial IoT energy transactions [12–14], while ignoring the fairness of energy transactions in industrial IoT. In the process of energy trading, high-quality trading resources will inevitably lead to vicious trading competition, and unfair trading resource allocation will certainly reduce the trading quality of the system. In addition, in the traditional PBFT consensus model, each round of consensus requires screening master nodes. This greatly wastes system resources, reduces the efficiency of the trading system, and limits the future development of industrial IoT energy trading [15, 16].

To address the abovementioned issues, we design a consortium blockchain-based energy trading scheme called HO-TRAD, which takes advantage of the decentralized feature of consortium chain and conducts an in-depth investigation of the fairness and efficiency of energy trading under the condition of ensuring the security and privacy of IoT energy trading. In the HO-TRAD scheme, the active reputation value of energy trading entities is adopted to ensure the fairness of trading resource allocation. The system will allocate resources based on the active reputation value of trading entities, when energy trading nodes compete for limited trading resources. In conjunction with the smart contract, a transaction reward and punishment mechanism is proposed to ensure the fairness of the transaction process. In the event of fraud or termination of a transaction, the smart contract will activate the transaction reward and punishment mechanism. Depending on the circumstances of the energy transaction, the entity that breaks the transaction will be punished, while the other trading entity will be rewarded for complying with the rules of the transaction.

In a nutshell, our contributions are as follows:

(1) We propose an energy trading solution called HO-TRAD to better regulate the process of energy trading in the industrial IoT in an open and transparent way. We establish a consortium blockchain to store all energy transaction information to ensure the verifiability of transaction data. A new smart contract is proposed to replace the traditional trading model to ensure the fairness and transparency of the trading process.

(2) The system records the active reputation value of the trading subjects within the management scope, and when there are multiple trading subjects competing for the same trading resource, the system will allocate resources based on the active reputation value of the trading subjects, which improves the resource fairness of energy trading.

(3) In the HO-TRAD scheme, we improve the traditional BPFT consensus algorithm by replacing the original master node selection system with the designated master node approach, which reduces the resource consumption of the consensus algorithm and improves the consensus efficiency.

(4) The security analysis and experimental simulation of this scheme from multiple perspectives show that the proposed scheme can effectively improve the trading efficiency of energy trading entities and guarantee the fairness of energy trading and the privacy of trading data.

The remaining of this article is organized as follows: We discuss the technology and method of energy trading in IoT in Section 2. The design of the energy trading model for IoT with blockchain is presented in Section 3, followed by a security analysis and performance evaluation in Section 4. Finally, Section 5 concludes this article.

## 2. Technology and Method of Energy Trading in IoT

*2.1. Blockchain Technology.* Since the blockchain technology was proposed in 2008, after a long development, it has already had a relatively perfect technical system [17–20]. According to different task scenarios and user needs, blockchains can be broadly classified into three categories: public blockchain, private blockchain, and consortium blockchain. The combination of blockchain and industrial IoT broadens the use scenarios of data and fosters the security use of data [21–24]. In the public chain, firstly, because of the decentralized feature, there is no central node to protect and maintain the system, so the consensus of every transaction in the public chain requires the participation of all nodes in the whole network, and this consensus method will certainly reduce the transaction efficiency of the system. Secondly, each node on the public chain can freely join and exit the network, making the system unable to distinguish between honest nodes and malicious nodes. Finally, after the malicious node receives punishment as predicted, the malicious nodes will quit the system and rejoin with a new identity, and there is no way to truly guarantee the security of the system. In the private chain, the participating entities are fixed before the system operates, which has higher transaction rate and privacy assurance. Nevertheless, because the participating entities are fixed in advance, private chain is not suitable for industrial IoT energy trading scenarios. In consortium chain, all entities are not allowed to access the system unless they are authorized by the certificate authority. In addition, the nodes in consortium chain are divided into two categories: full nodes have complete transaction information, while light nodes only keep their own relevant information, which satisfies the needs of different types of entities. Therefore, this paper adopts consortium chain to construct the industrial IoT energy trading network. Blockchain, as a term used in the field of information technology, is essentially a shared, transparent database. It guarantees the fairness and security of transactions through smart contracts and digital signatures.

*2.1.1. Smart Contracts.* Smart contracts are digitally defined protocols. Unlike traditional paper contracts, they combine

the trigger conditions and execution of a contract into a single atomic operation. Smart contracts are deployed on the blockchain, where the content of the contract is open, transparent, and tamper-proof. The transaction entities can transact securely in an environment of distrust.

*2.1.2. Digital Signatures.* The digital signature, as an authentication mechanism of the blockchain, has two functions. On the one hand, it verifies the sender of the message and confirms the origin of the message. Because of the uniqueness of the private secret key, other entities cannot forge the signature. On the other hand, digital signatures can verify the integrity of the message and guarantee the complete consistency of the sender's message through the digital digest technique and the collision resistance of the hash function.

*2.2. Elliptic Curve Code.* Elliptic curve cipher is recognized as the most secure encryption algorithm for a given length of secret key; it is profoundly influencing the technological development of industrial IoT such as intelligent monitoring [25], data flow management [26], and data prediction [27]. Elliptic curve cipher is a public key encryption algorithm based on the elliptic curve. It is extremely difficult to solve $K$ with known base point $G$ and multiples of base point $KG$ on the elliptic curve, which is a discrete logarithm problem based on the elliptic curve, where $K$ is used as the user's private key and $KG$ is used as the user's public key. The principle of the encryption algorithm for elliptic curves is as follows: Suppose the user's private key and public key are $K$ and $KG$, respectively, and in encrypted communication, the encrypting party chooses a random number $r$ to convert the message $M$ into a ciphertext by

$$C = \{rG, M + rKG\}. \tag{1}$$

The decryption method is

$$M + rKG - K(rG) = M + r(KG) - K(rG) = M. \tag{2}$$

When using elliptic curve cipher for signature, first choose the random number $r$ and calculate the point $rG(x, y)$. Subsequently, $s = (h + kx)/r$ is calculated based on the random number $r$, the hash value $h$ of the message $M$, and the private key $k$. After the calculation is completed, the message $M$ and the signature $\{rG, s\}$ are sent to the receiver.

The signature verification method is

$$\frac{hG}{s} + \frac{xKG}{S} = \frac{(h + xK)G}{S} = \frac{r(h + xK)G}{h + xK} = rG. \tag{3}$$

*2.3. Methods in Energy Trading.* Some works have proposed to optimize industrial IoT energy trading for the past few years.

*2.3.1. Privacy in Energy Trading.* The authors in [28] first propose the application of blockchain technology to the industrial IoT distributed energy trading scenario. The authors in [29] propose a scheme called DePET, which enables reliable transactions between EVs and energy nodes within a short processing delay. This scheme uses a k-anonymity approach to construct joint requests hiding location information and creates clock regions based on undirected graphs, making it impossible for an attacker to distinguish the user's real location information, and experimental results show that the scheme can effectively protect the location privacy of transacting entities. In [3], a local vehicle-to-vehicle (V2V) energy trading architecture based on fog computing is proposed. In [2], a federated blockchain-oriented approach is proposed to address the privacy leakage problem without limiting the transaction functionality. In [30], a decentralized auction strategy for microgrid energy trading, DEAL, is proposed, which effectively protects the privacy of auction participants by using the Laplacian index. Experiments show that the scheme can prevent the data privacy of trading entities from being compromised under different auction scenarios.

*2.3.2. Security in Energy Trading.* For the security of industrial IoT energy transactions, the authors in [31] proposed a blockchain-based electricity trading (B-ET) ecosystem and designed a smart contract to ensure that transactions are conducted safely and reliably. Reference [32] constructed a partially decentralized power trading system based on consortium BC, and the scheme improves the stability, economy, and security of grid operation by optimizing the charging and discharging states at each time period. Qualitative security and privacy analysis shows that the scheme helps to improve the security and privacy of power trading. Reference [33] combined blockchain, edge computing, and contract theory to propose a secure and efficient V2G energy trading framework for CPS. The authors in [34] proposed an algorithm that can be implemented in a distributed manner by trading partners to enable energy trading.

*2.3.3. Fairness in Energy Trading.* In response to transaction fraud as well as transaction fairness issues that arise in industrial IoT energy transactions. The authors in reference [35] proposed a blockchain-based energy trading scheme. The scheme is designed with a time-commitment based mechanism to ensure fairness in the energy trading process. The experimental results show that the scheme can improve the fairness of transactions while ensuring the privacy and security of users. The literature [36] analyzed the transaction security and transaction fairness under a large number of known attack patterns using multiple-signature mechanism, and the scheme has higher security and fairness compared to the traditional approach.

Combining the analysis of existing literature, we find that most of the current solutions focus on how to ensure the privacy of energy transactions in industrial IoT and the security of transactions, and there is a lack of research on energy and transaction efficiency and transaction fairness. Hence, there is an urgent need to design an energy trading scheme that takes into account the efficiency and fairness of energy trading in the industrial Internet of Things.

## 3. Design of the Energy Trading Model for IoT with Blockchain

In the HO-TRAD solution, the system nodes are divided into edge user nodes, a limited number of local energy aggregators, and a certificate authentication central. The energy transactions of the system will be performed by the consensus of the local aggregators, which greatly reduces the time required for consensus and increases the transaction throughput of the trading system. On the one hand, the transaction entities of the consortium chain need to be audited by the certificate authentication central before entering the existing consortium chain system; this access mechanism ensures the security of the system nodes. On the other hand, for the transaction entities, there is no need to store all historical transactions, which reduces the resource consumption of user nodes. The industrial IoT energy trading system does not require any transaction fees when the consortium blockchain is chosen for transactions. Compared with the transaction fees of the public chain, the consortium blockchain is obviously an unavailable benefit for small transactions of scattered users.

*3.1. System Architecture.* The system model of HO-TRAD is shown in Figure 1.

The entities in the model are divided into three main parts, namely, energy trading entity (ETE), local aggregators (LAs), and certificate authority (CA), and the functions of these entities are as follows:

(1) ETE: In this scheme, energy trading entities are divided into two major categories, energy buyers and energy sellers, and ETEs trade in a P2P manner. The same ETE can switch between being an energy seller, being an energy buyer, or being idle, depending on the current demand of the self-generation.

(2) LA: The LA is responsible for statistical information and trade matching of traded energy in the region.

(3) CA: The CA is a reliable authority that supervises the transaction data of the scheme and initializes the transaction model. In addition, all LAs as well as ETEs in the model are unified at the CA for authentication before they can obtain legal identity and public-private key pairs.

ETEs can both publish their own demand information and query the existing transaction information on the consortium chain, and after querying the transaction information they need, they can match the transaction with the central node, while buyers or sellers can request the central node to match the transaction. ETEs can monitor each other's posted information; if any illegal information is found, the publisher will be banned and disqualified from trading.

*3.2. System Interaction.* In the HO-TRAD scheme, the transaction information of the system is encrypted and uploaded by the LA, and the specific transaction information is not available to ETEs other than those participating in the transaction, ensuring the privacy of ETEs. In addition, LA will allocate resources based on the active reputation value of ETEs to ensure the fairness of energy transactions. The interaction flow of the scheme can be divided into four modules: entity registration, energy matching, energy trading, and energy consensus, as shown in Figure 2.

*3.2.1. Entity Registration.* When an ETE applies to join the trading system, the ETE needs to submit its entity information to the CA, which will issue a digital certificate to the ETE after reviewing the entity's qualification.

$$\begin{aligned} \text{APPLY} &= \{UID \| TIME \| LA\}, \\ \text{CER} &= \{UID \| \text{TIME} \| \| PK \| RES\}. \end{aligned} \tag{4}$$

*APPLY* is the application information, *CER* is the digital certificate issued by CA, *UID* is the ID of ETEs, *TIME* is the application registration time of ETEs, and *PK* is the public key of ETEs. *RES* is the result of system audit $RES \in \{0, 1\}$, where 1 means that the node is allowed to join the trading system if the audit is passed, and 0 means that the node is not allowed to join the trading system if the audit is not passed. After receiving the information submitted by the user, the CA generates a public-private key pair for the user using the system's elliptic cipher curve (ECC). The CA then transmits the generated public-private key pair to the applicant node by encrypting it with its own private key and signs the user's identity token, and other ETEs can verify the CA's signature to determine the user's identity token.

*3.2.2. Energy Matching.* After accessing the trading system, ETEs are required to publish their public key information and download the transaction data of the recent period within the LA management scope they belong to. When ETEs need to sell or buy energy, they need to broadcast their transaction requirements and attach their signatures to the broadcast message. The broadcasted message should contain the ID of the ETE, the transaction demand, the request time, and its own signature. When the entity has already obtained a transaction match or needs to cancel this transaction, it should broadcast a message again that the transaction needs to be canceled and add its own signature to the message in the broadcast.

$$\begin{aligned} REQ &= \{UID \| DEN \| TIME \| SIGN\}, \\ REV &= \{UID \| REQ \| SIGN\}. \end{aligned} \tag{5}$$

In the above equation, *UID* denotes the identity *ID* of the transacting entity, *DEN* represents the energy demand of the transacting entity, and *SIGN* is the entity signature for the source of the information on the blockchain.

ETEs can view each other's posted trade information; after finding a trade requirement that matches their own, they can make a trade matching request to the LAs. After receiving a trade match request from ETEs, LAs need to check the eligibility of ETEs to trade, including the amount of energy owned by ETEs and the amount of

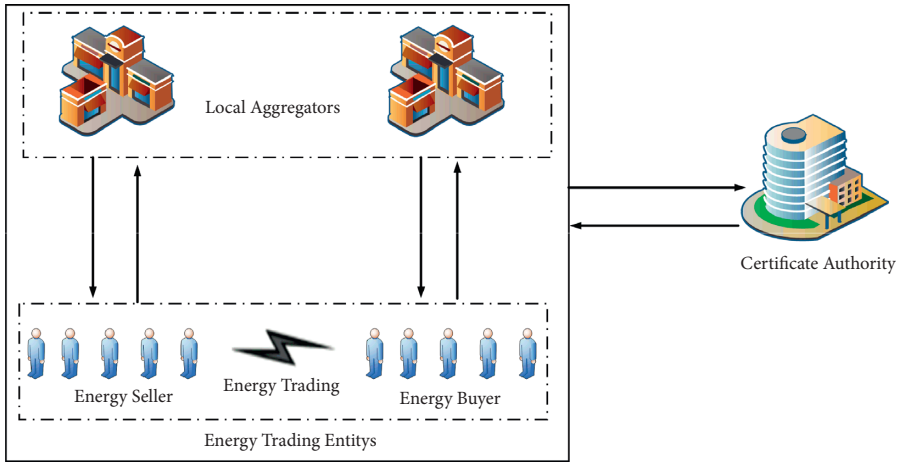


Figure 1: Scheme interaction flow diagram.

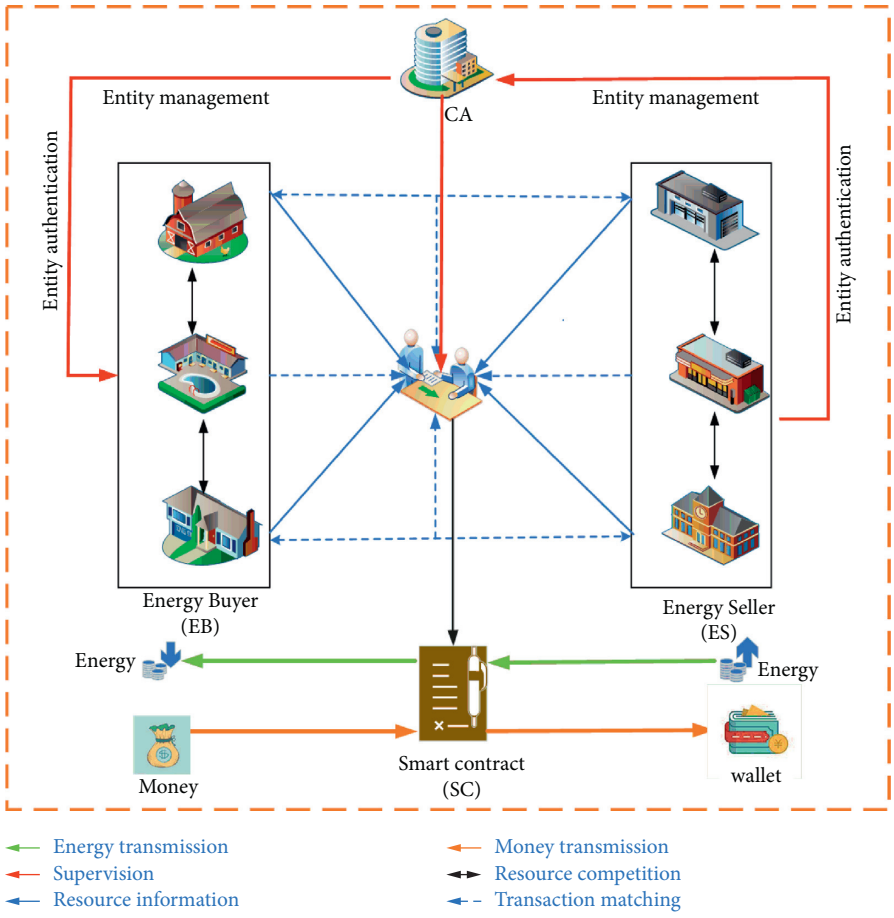


Figure 2: Scheme interaction flow diagram.

funds. After confirming the trading eligibility that ETEs have, LAs will match trading entities for energy transactions. After the entity transaction matching is completed, LAs will record the buyer user's ID, seller user's ID, transaction time, transaction wallet, and coin quantity.

$$CON = \{UID_1 || UID_2 || TIME \| WALLT_1 || WALLT_2 || QUA\}. \quad (6)$$

In this formula, *WAL* denotes the wallet of the trading entity, since the same energy trading entity may have more than one trading wallet, which is recorded to facilitate the verification of the transaction information, and *QUA* denotes the transaction amount of this trading.

*3.2.3. Energy Trading.* LA records the transaction information and then transfers the entire transaction to the smart contract for execution. The smart contract locks the deposit corresponding to the transaction entity's wallet based on the amount of this transaction. After the transaction amount is locked, the trading entity will not have the right to do anything with the frozen portion of the amount until this transaction is closed. ETEs may make multiple energy transactions at the same time. When a transaction match is made, the ETEs' account will be frozen for the corresponding portion of the amount, and although this transaction is not made, the ETEs' account balance shall be reduced by the corresponding amount in the following physical transaction. After a deal is matched, ETEs are required to pay 10% of the total transaction amount as a transaction deposit. If one party wants to terminate the deal after the deal is matched or fails to complete the transaction step by the agreed time, they need to pay their deposit to the other party as compensation. If the transaction is successfully completed, the locked amount in the energy buyer's account will be transferred to the energy seller's account through the smart contract, and if any unforeseen circumstances cause the transaction to fail, the locked amount in the energy buyer's account will be unlocked and access to the amount will be restored. The transaction buyer needs to return a confirmation message after receiving the energy, and the smart contract will transfer the amount deducted in advance to the transaction seller's account after receiving this message. If the trading entity disagrees with the transaction process, the ETEs can send the disagreement back to the LA for a ruling. The system transaction flow is shown in Figure 3.

The process of implementing a smart contract is shown in Algorithm 1:

*3.2.4. Trading Consensus.* Considering the access mechanism of the consortium chain and the actual scenario of this scheme, the consensus efficiency can be improved by reducing the amount of participation of consensus nodes when the nodes do not do evil. Based on the above conditions, we make an improvement to the existing PBFT consensus scheme; the new consensus scheme is divided into two parts as follows.

(1) Selecting the master node: If the system master node is selected in ETEs, the master node may be different for each round of transactions, and the trading system needs to broadcast the master node information to other nodes within the scope of other systems, which will increase the communication overhead of the system. Since LAs are all trusted nodes authenticated at CA, selecting LAs as the master nodes of the system, having LAs participate in consensus in each round of transactions, and uploading the transaction information to the distributed ledger will enhance the communication efficiency of the system.

(2) Consensus process: The consensus process is carried out by the LA that initiated the transaction leading the rest of the LAs in the system, who package the transaction information and broadcast it in the system. In the consensus phase, LA packages this transaction information to other LAs, and LAs will broadcast the verification results along with the signatures to other auditing entities for checking after reviewing the transaction data. The audit message includes the audit entity ID, audit result, audit time, and entity signature.

$$OUT = \{UI\ D || RESULT || TIME \| SIGN\}. \quad (7)$$

LA counts the audit messages received; if it receives more than two-thirds of the number of participating entities agreeing to the message, LA will hash this transaction information and upload it to the blockchain ledger, while the frozen funds in the energy buyer's account will be unlocked and transferred to the energy seller's account. The consensus process is shown in Figure 4.

*3.3. Active Reputation Value.* When ETEs trade energy in the system, different trade sizes will have different impacts on ETEs; thus, we propose a trade impact factor to measure the degree of impact of different trades on the trading entity (capped at 1). The impact factor is calculated as

$$f = \left(\frac{M_i}{M_q}\right). \quad (8)$$

In the formula, $M_i$ is the current energy transaction amount and $M_q$ is the account balance of the entity before the energy trading.

In this scheme, we use the entity activity value to represent the recent active status of the ETEs. A high activity value of an ETE indicates that this entity has been actively trading in the system recently, and the entity will close the deal as soon as there is a successful match.

ETEs select the nearest LA after passing the CA audit, and the LA will give the entity an initial entity activity value of $P_0 = 10$ after receiving the entity information. The entity activity value of ETE will be counted and stored by LA, and it will be used as one of the reference criteria for the allocation of trading resources. The activity value is calculated as follows.

When an ETE completes an energy trading action, the entity's entity activity value is calculated and updated by the LA.

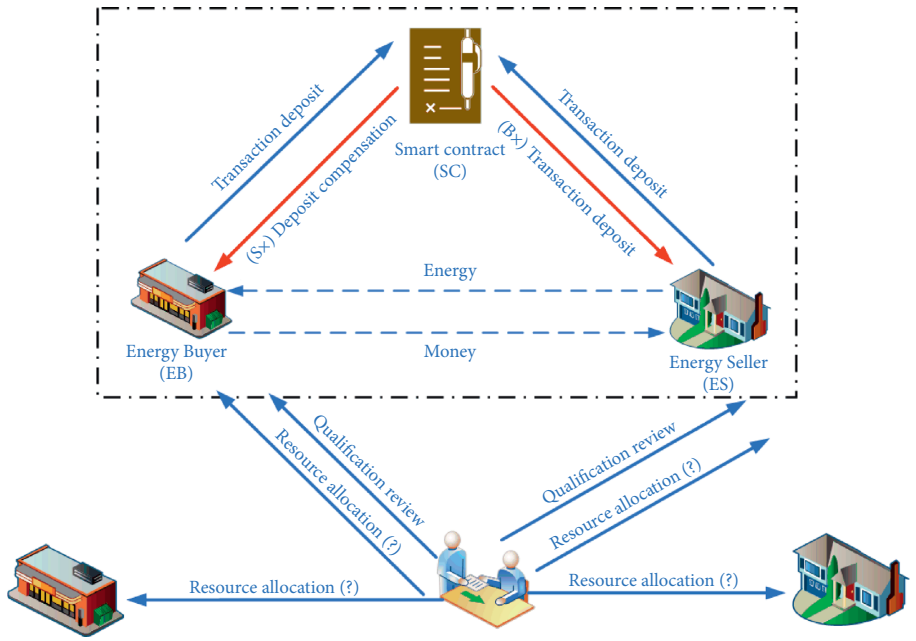


Figure 3: Scheme transaction diagram.

Input: seller's account $W_1$, buyer's account $W_2$, number of energy transactions $q$, amount of energy transaction M
Output: trading results
(1) Freezing of deposits $M_0 = 10\%M$
(2) Lock transaction balance $M_1 = 90\%M$
(3) if transaction down
(4) release seller($M_0$)
(5) $W_1 \leftarrow M_1 + M_0$
(6) else if transaction break
(7) if seller break
(8) $W_1 \leftarrow W_1 - M_0$
(9) $W_2 \leftarrow 2 * M_0$
(10) else if buyer break
(11) $W_2 \leftarrow W_2 - M_0$
(12) $W_1 \leftarrow 2 * M_0$
(13) end if

Algorithm 1: Energy trading contracts.

$$P_i = \log\left(P_{i-1}^f\right) + P_{i-1}. \tag{9}$$

When an ETE initiates an energy trade match after a period of no energy trade, the LA counts the length of silence of the trading entity and updates the entity's activity value for that ETE based on the length of silence (the lowest activity value is 0), where $T$ is the length of silence time (unit in days) and $\alpha$ is a random value chosen by LA ($\alpha$ is a descent parameter greater than 1 and less than 5).

$$P_i = P_{i-1} - e^T \cdot \sum_{i-\infty}^{i-1} \left(\frac{M_{i'}}{M_{q'}}\right). \tag{10}$$

Entity reputation value: We use entity reputation value to indicate the integrity of ETEs in energy trading. The entity reputation value indicates the integrity of ETE in energy trading, and an ETE with high reputation value is able to comply with the system trading rules in the energy trading. After the ETEs select LA, LA will initialize the ETEs' reputation value $C_0 = 20$. The reputation value of ETEs will change with the entity's trading practices.

When entity completes this transaction,

$$C_i = f^{(1/f)} + C_{i-1}. \tag{11}$$

When a trading entity violates trading rules or does not complete an energy transaction,

$$C_i = (1 - f) \cdot C_{i-1}. \tag{12}$$

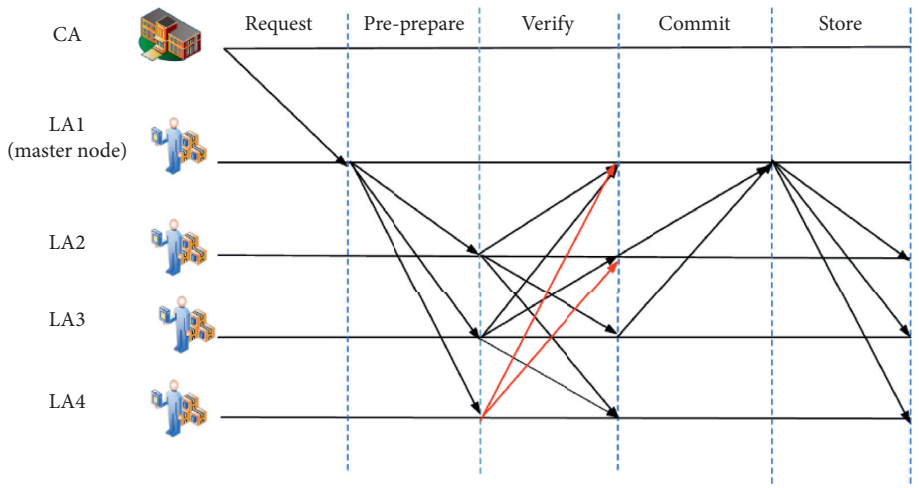


Figure 4: Consensus procedures.

In the energy trading system, ETEs post their trading requirements in the system in the form of signatures. There may be multiple ETEs requesting trade matching for the same trading resource. If the system randomly selects ETEs for matching, the fairness of the trade will be lost. To tackle this problem, this proposal proposes to handle the allocation of trading resources based on the active reputation value of ETE. In the case of multiple competitors competing for a uniform resource, the ETE with the highest active reputation value will be eligible to trade. If the ETEs have the same active value, the entity with the higher reputation value will be eligible to trade. The active reputation value of ETE is calculated as follows:

$$H_i = f^{\beta} \cdot \frac{P_i^{\delta} + C_i^{\delta}}{\delta\left(P_i + C_i\right)}. \tag{13}$$

In this equation, $\beta$ and $\delta$ are the regulating parameters of the system. When the active reputation value of EFE's rises or falls continuously, the system will adjust $\beta$ and $\delta$ so that the rate of change of the active reputation value decreases.

## 4. Simulation and Experiment Analysis

### 4.1. Security Analysis

*4.1.1. Authentication.* In the HO-TRAD scheme proposed in this paper, all ETEs and LAs are required to undergo the same authentication by CA before entering the trading system. CA generates public-private key pairs by means of prescribed elliptic curve ciphers and determines the uniqueness of ETE identity by assigning different public-private key pairs and CA certificates to each ETE. All information released by ETEs in HO-TRAD scheme needs to be signed by affiliated entities, and any information can be traced back to the issuer of the information. It is experimentally demonstrated that an attacking adversary performs an eavesdropping indistinguishable experiment under the condition of having access to the predictive machine model and succeeds in eavesdropping with a probability no greater than $1/2 + \vartheta$ ($\vartheta$ is a negligible function), which is statute to the mathematical problem, so the adversary will not be able to crack the authentication scheme.

*4.1.2. Privacy.* In this scheme, all information of entity authentication and entity transaction process is encrypted, and ETEs will attach their signatures to the released information to ensure the source and reliability of the message. When a transaction is reached, LA will hash the transaction information and upload it to the federation chain ledger, so that even if an adversary obtains the transaction ledger of the system, it cannot get the corresponding transaction information, which protects the privacy of the transaction.

*4.1.3. Resource Fairness.* When the system encounters the situation where multiple ETEs compete for the same trading resource, it is unfair to allocate the resources by random assignment. Therefore, in this scheme, LAs will measure the allocation of current trading resources based on the active reputation value of the trading entities in the system, and the entity with the highest active reputation value will get the ownership of the trading resources. If the active reputation value of an ETE remains high after an honest transaction, this ETE will always enjoy the right to allocate trading resources. Therefore, this proposal proposes that if ETEs do not trade for a period of time or behave dishonestly in the transaction, the active reputation value of the ETEs will be significantly reduced to ensure that ETEs enjoy a fair competition for trading resource .

*4.1.4. Trading Fairness.* When ETEs make an energy transaction, the LA checks the eligibility of both parties to the transaction, and when both parties are eligible to trade, the energy transaction is transferred to a smart contract for further execution. The smart contract will freeze the corresponding account funds in the trading account in advance before executing the trade, depending on the amount of this trade. During the execution of the contract, when one party violates the trading rules, the frozen amount of that ETE is forfeited and transferred to the other counterparty as compensation. When a

Table 1: Performance comparison.

| Property | BSeIn | BETS | DePET | FeneChain | HO-TRAD |
|---|---|---|---|---|---|
| Authentication | √ | × | √ | √ | √ |
| Privacy | × | × | √ | √ | √ |
| Resource fairness | × | × | × | × | √ |
| Trading fairness | × | × | × | √ | √ |
| Verifiability | √ | × | √ | √ | √ |

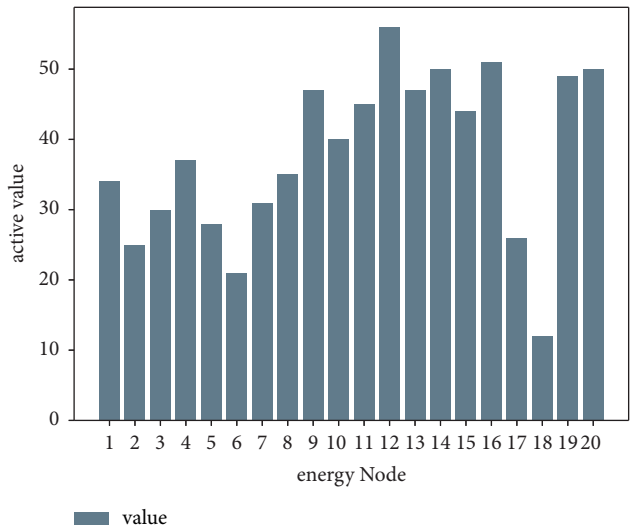


Figure 5: Energy trading entity activity.

transaction is successfully concluded, the corresponding funds in the transaction buyer's account will be deducted and transferred from the smart contract to the transaction seller's account when the transaction buyer confirms receipt of the energy, and the ETEs can refer to the LAs for adjudication if there are objections to the transaction.

*4.1.5. Verifiability.* In this scheme, all transaction records are accompanied by the signature of the node handling the transaction. If a malicious LA or an adversary changes the LA transaction data, CA can quickly check the source of the error and make changes based on the signature, and the unforgeability of the blockchain ensures the verifiability of the transaction data.

We compare HO-TRAD with existing works, and the results are shown in Table 1 where we can easily identify the differences in the solutions.

*4.2. Experiment Setting.* We instantiate the HO-TRAD on a laptop with 16.00 GB RAM running Windows 10 Home and PyCharm Community Edition and using an AMD Ryzen 5 4600H CPU@3.0GHz and NVIDIA GeForce GTX 1650 graphics card to run the experimental platform. We choose Hyperledger Fabric as the blockchain platform for the solution, obtain the public and private key pairs of transaction entities on the elliptic curve $y^2 = x^3 - x + 1$, and upload the transaction information hash to the blockchain through the hash function SHA256. Hyperledger Fabric is an experimental blockchain-based platform that allows the creation of consensus mechanisms that meet the needs of users.

*4.3. Results and Discussion.* For the IoT energy trading scheme proposed in this paper, the experiment will reflect the fairness of system resource allocation through the change of active reputation value of energy trading entities and illustrate the trading performance of the scheme through the transaction duration. The experiment passes the observation to collect the recent activity of trading entities and track and record the trading practices of trading entities. The experiment simulates 500 energy trading entities trading in the system and intercepts the recent entity parameters of twenty trading entities $\{U_1, U_2, U_3 \ldots\ldots U_{20}\}$ after the trading system has been running for a period of time. The entity activity values are shown in Figure 5, and the reputation values are shown in Figure 6. The initial entity parameters of these twenty trading entities are consistent, and the experiment records the entity parameters as an array and records the changed values in the array according to their trading practices. It is obvious in the figure that the entity parameters have changed significantly after the entity has been in the system for a period of time for its trading practices.

The experiment simulates the entity parameters under different scenarios based on the current entity values of the system, the entity activity value changes as shown in Figure 7, and the entity reputation value changes as shown in

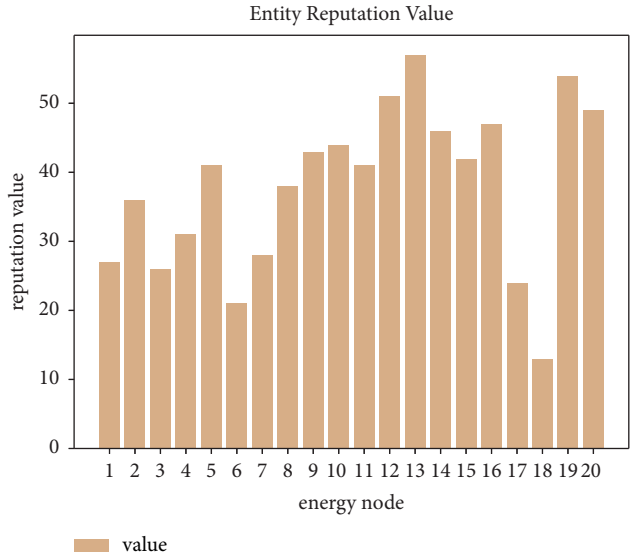


Figure 6: Energy trading entity reputation.

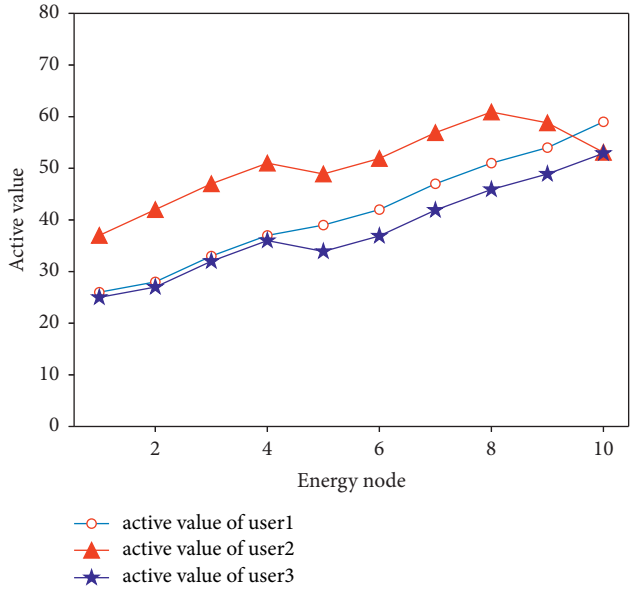


Figure 7: Change of ETE's activity value.

Figure 8. From the perspective of entity activity value, user 2 stopped trading for one day after the fourth transaction and terminated the transaction on the eighth day after resuming the transaction on the sixth day, and the rate of decrease of entity activity value was proportional to the length of transaction stoppage. User 1 maintains a very high level of transaction participation throughout the transaction period, so the entity activity value tends to increase. From the perspective of entity reputation value, user 1 and user 3 have maintained good trading practices, so the entity's reputation value is in a slow growth state, while user 2 did not comply with the trading rules during the fourth transaction, so the entity's reputation value dropped significantly. Figure 9 shows how the active reputation value of the entity varies with the entity's transaction practices.

Compared with the transaction efficiency proposed in [4], this paper specifies the consensus master node in the algorithmic consensus process of PBFT so that this scheme does not need to execute the attempted rotation protocol. In addition, due to the solidification of the consensus master node, the time spent in the view checking protocol in each consensus round is further reduced compared to the scheme proposed in [4]. For the sake of generality, the average latency of 200 transactions with different number of nodes is taken for comparative analysis. As can be seen in Figure 10, the transaction latency of this scheme is reduced by nearly 1/3 compared to that of [4], and the transaction performance of this scheme is more prominent when the number of consensus nodes increases.

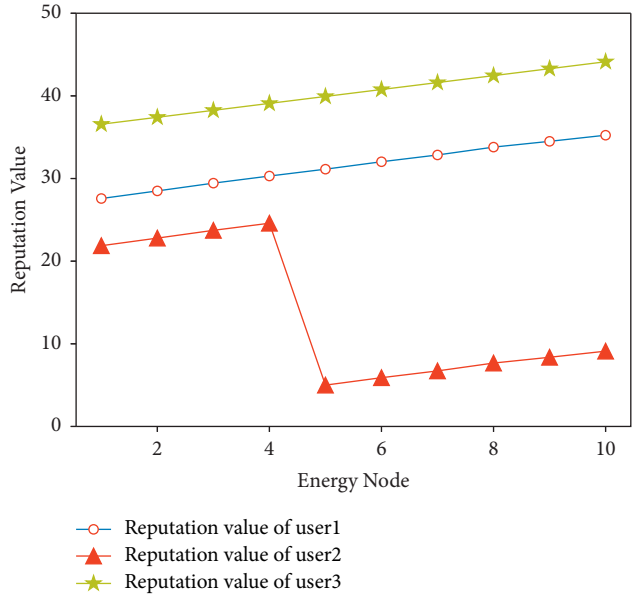


Figure 8: Change of ETE's reputation value.

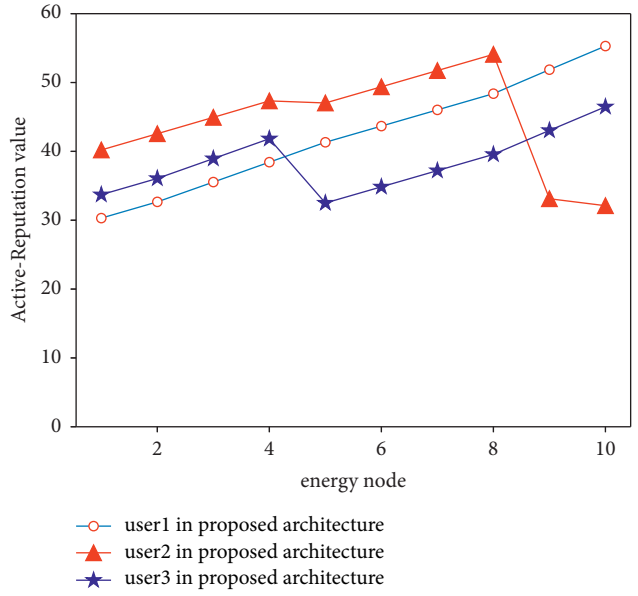


Figure 9: Change of ETE's active reputation value.

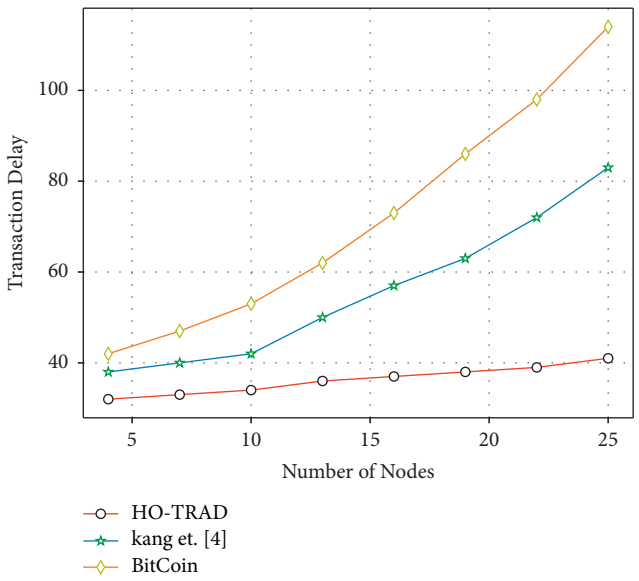


Figure 10: Energy transaction delay comparison.

## 5. Conclusions

In this paper, we propose HO-TRAD, a secure energy trading scheme based on consortium chain, to solve the problem of limited resource allocation and transaction fraud in energy trading. The model achieves privacy, unforgeability, and verifiability of energy trading data with the technical support of the consortium chain. The experimental results show that the scheme can effectively ensure the fairness of system trading and improve the system trading efficiency. This scheme is more consistent with the IoT energy trading scenario from the perspective of transaction fairness. However, the fairness of energy trading should be reflected not only in the allocation of trading resources, but also in the trading price, and we will use the game theory approach to solve the trading price problem in our future work.

## 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 no conflicts of interest.

## Acknowledgments

Our research work was funded by National Natural Science Foundation of China (Grant no. 61962009), Major Scientific and Technological Special Project of Guizhou Province (20183001), Science and Technology Support Plan of Guizhou Province ([2020]2Y011), and Talent project of Guizhou Big Data Academy Guizhou Provincial Key Laboratory of Public Big Data ([2018]01).

## References

[1] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[2] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.

[3] G. Sun, M. Dai, F. Zhang, H. Yu, X. Du, and M. Guizani, "Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7868–7882, 2020.

[4] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[5] S. Y. Altahir, X. Yan, and X. Liu, "A power sharing method for inverters in microgrid based on the virtual power and virtual impedance control," *in*, in *Proceedings of the 2017 11th IEEE International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG)*, pp. 151–156, Cadiz, Spain, April 2017.

[6] Z. Che, Y. Wang, J. Zhao, Y. Qiang, Y. Ma, and J. Liu, "A distributed energy trading authentication mechanism based on a consortium blockchain," *Energies*, vol. 12, no. 15, https://www.mdpi.com/1996-1073/12/15/2878 [Online]. Available:, 2019.

[7] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42–52, 2018, https://www.sciencedirect.com/science/article/pii/S1084804518301619 [Online]. Available:.

[8] H. Kou, H. Liu, Y. Duan et al., "Building trust/distrust relationships on signed social service network through privacy-aware link prediction process," *Applied Soft Computing*, vol. 100, 2021 https://www.sciencedirect.com/science/article/pii/S1568494620308802 Online]. Available:, Article ID 106942.

[9] S. Xu, X. Chen, and Y. He, "Evchain: an anonymous blockchain-based system for charging-connected electric vehicles," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 845–856, 2021.

[10] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: a distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[11] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and IoT environment," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2116–2123, 2021.

[12] Y. Wang, G. Yang, T. Li, F. Li, Y. Tian, and X. Yu, "Belief and fairness: a secure two-party protocol toward the view of entropy for iot devices," *Journal of Network and Computer Applications*, vol. 161, Article ID 102641, 2020.

[13] F. Li, D. Wang, Y. Wang et al., "Wireless communications and mobile computing blockchain-based trust management in distributed internet of things," *Wireless Communications and Mobile Computing*, vol. 2020, no. 5, pp. 1–12, Article ID 8864533, 2020.

[14] F. Li, R. Ge, H. Zhou, Y. Wang, Z. Liu, and X. Yu, "Tesia: a trusted efficient service evaluation model in Internet of things

based on improved aggregation signature," *Concurrency and Computation: Practice and Experience*, vol. 57, p. e5739, 2020.

[15] E. Jiang, L. Wang, and J. Wang, "Decomposition-based multi-objective optimization for energy-aware distributed hybrid flow shop scheduling with multiprocessor tasks," *Tsinghua Science and Technology*, vol. 26, no. 5, pp. 646–663, 2021.

[16] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, "New enhanced authentication protocol for internet of things," *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1–9, 2021.

[17] T. Li, Z. Wang, G. Yang, Y. Cui, Y. Chen, and X. Yu, "Semi-selfish mining based on hidden Markov decision process," *International Journal of Intelligent Systems*, vol. 36, no. 7, pp. 3596–3612, 2021, https://onlinelibrary.wiley.com/doi/abs/10.1002/int.22428 [Online]. Available:.

[18] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, and Y. Yang, "Is semi-selfish mining available without being detected?" *International Journal of Intelligent Systems*, vol. 55, 2021.

[19] T. Li, Y. Chen, Y. Wang et al., "Rational protocols and attacks in blockchain system," *Security and Communication Networks*, vol. 2020, 2020 https://doi.org/10.1155/2020/8839047, Article ID ,8839047.

[20] Y. Wang, G. Yang, A. Bracciali et al., "Incentive compatible and anti-compounding of wealth in proof-of-stake," *Information Sciences*, vol. 530, pp. 85–94, 2020.

[21] J. Mabrouki, M. Azrour, D. Dhiba, Y. Farhaoui, and S. E. Hajjaji, "Iot-based data logger for weather monitoring using arduino-based wireless sensor networks with remote graphical application and alerts," *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 25–32, 2021.

[22] F. Wang, H. Zhu, G. Srivastava, S. Li, M. R. Khosravi, and L. Qi, "Robust collaborative filtering recommendation with user-item-trust records," *IEEE Transactions on Computational Social Systems*, vol. 68, pp. 1–11, 2021.

[23] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "A source location privacy protection scheme based on sector phantom routing in wsns," *International Journal of Intelligent Systems*, vol. 10, 2019, https://onlinelibrary.wiley.com/doi/abs/10.1002/int.22666.

[24] A. Guezzaz, Y. Asimi, M. Azrour, and A. Asimi, "Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly detection," *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 18–24, 2021.

[25] J. Mabrouki, M. Azrour, G. Fattah, D. Dhiba, and S. E. Hajjaji, "Intelligent monitoring system for biogas detection based on the internet of things: mohammedia, Morocco city landfill case," *Big Data Mining and Analytics*, vol. 4, no. 1, 2021.

[26] D. Wei, H. Ning, F. Shi et al., "Dataflow management in the internet of things: sensing, control, and security," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 918–930, 2021.

[27] Y. Huo, J. Fan, Y. Wen, and R. Li, "A cross-layer cooperative jamming scheme for social internet of things," *Tsinghua Science and Technology*, vol. 26, no. 4, pp. 523–535, 2021.

[28] M. E. Peck and D. Wagman, ""Energy trading for fun and profit buy your neighbor's rooftop solar power or sell your own-it'll all be on a blockchain," *IEEE Spectrum*, vol. 54, no. 10, pp. 56–61, 2017.

[29] Y. Long, Y. Chen, W. Ren, H. Dou, and N. N. Xiong, "A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and k - anonymity," *IEEE Access*, vol. 8, p. 192, 2020.

[30] M. U. Hassan, M. H. Rehmani, and J. Chen, "Deal: differentially private auction for blockchain-based microgrids energy trading," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 263–275, 2020.

[31] J. Guo, X. Ding, and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2040–2050, 2021.

[32] Y. Li and B. Hu, "A consortium blockchain-enabled secure and privacy preserving optimized charging and discharging trading scheme for electric vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1968–1977, 2021.

[33] O. Samuel and N. Javaid, "A secure blockchain-based demurrage mechanism for energy trading in smart communities," *International Journal of Energy Research*, vol. 45, no. 1, pp. 297–315, 2019, https://onlinelibrary.wiley.com/doi/abs/10.1002/er.5424 [Online]. Available:.

[34] U. Amin, M. J. Hossain, W. Tushar, and K. Mahmud, "Energy trading in local electricity market with renewables-A contract theoretic approach," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 3717–3730, 2021.

[35] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6564–6574, 2020.

[36] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.