Received November 10, 2019, accepted November 21, 2019, date of publication December 2, 2019,
date of current version December 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2957211

Blockchain-Based Distributed Energy Trading in Energy Internet: An SDN Approach

XIN LU[1], LINGYUN SHI[1], ZHENYU CHEN[1], XUNFENG FAN[1], ZHITAO GUAN[1], (Member, IEEE), XIAOJIANG DU[2], (Fellow, IEEE), AND MOHSEN GUIZANI[3], (Fellow, IEEE)

[1]School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China
[2]Department of Computer and Information Science, Temple University, Philadelphia, PA 19122, USA
[3]Department of Computer Science and Engineering, Qatar University, Doha 2713, Qatar

Corresponding author: Zhitao Guan (guan@ncepu.edu.cn)

This work was supported in part by the Beijing Natural Science Foundation under Grant 4182060, in part by the National Natural Science Foundation of China under Grant 61972148, and in part by the Fundamental Research Funds for the Central Universities under Grant 2019MS020.

ABSTRACT The new network paradigm of Software Defined Networking (SDN) has been widely adopted. Due to its inherent advantages, SDN has been widely used in various network fields such as data centers, WAN, enterprise, Optical Networks and energy Internet. Among them, SDN-based energy Internet systems are receiving more and more attention. But at the same time, some problems and challenges are gradually becoming more prominent. The SDN-based energy Internet is a distributed architecture for renewable energy, so the traditional centralized electric energy trading model will no longer apply. The blockchain has been rapidly developed and applied in various domains by virtue of its decentralization, coordinated autonomy, and non-tamperability. We propose an SDN-based energy Internet distributed energy trading scheme supported by blockchain technology. The proposed scheme achieves a reasonable match of the transaction objects under the premise of protecting privacy. Finally, we conducted a comprehensive, systematic security and applicability analysis of the proposed solution, further confirming that the system meets our design goals.

INDEX TERMS Software defined networking (SDN), energy Internet, blockchain, privacy-preserving.

I. INTRODUCTION

With the continuous expansion of the network scale and the rapid growth of Internet traffic, the demand for traffic has been expanding, and various new services have emerged, increasing the cost of network operation and maintenance. Software defined network (SDN) is a new type of network innovation architecture. By separating the control plane of the network device from the data plane, it realizes flexible control of network traffic and provides a good platform for innovation of core networks and applications [1], [2]. SDN is one of the hottest and most promising technologies in the current networking arena. In view of the huge development potential of SDN, the academic community has deeply researched the key technologies of the data layer and the control layer, and successfully applied SDN to various domains such as enterprise networks and data centers. Today, a new network paradigm for SDN has been widely adopted [3], [4].

In order to cope with the energy crisis, renewable energy such as solar energy, wind energy and bioenergy are highly valued by countries all over the world. However, renewable energy has the characteristics of geographical dispersion, discontinuous production, randomness, volatility and uncontrollability. The centralized and unified management of traditional power networks is difficult to adapt to the requirements of large-scale utilization of renewable energy. In order to solve the problem of efficient use of renewable energy, energy Internet provides a feasible technical solution. Energy Internet understands that it is a combination of advanced power electronics technology, information technology and intelligent management technology. It interconnects a large number of new power network nodes consisting of distributed energy harvesting devices, distributed energy storage devices and various types of loads to realize an energy-to-peer exchange and shared network of two-way flow of energy. At the same

The associate editor coordinating the review of this manuscript and approving it for publication was Al-Sakib Khan Pathan.

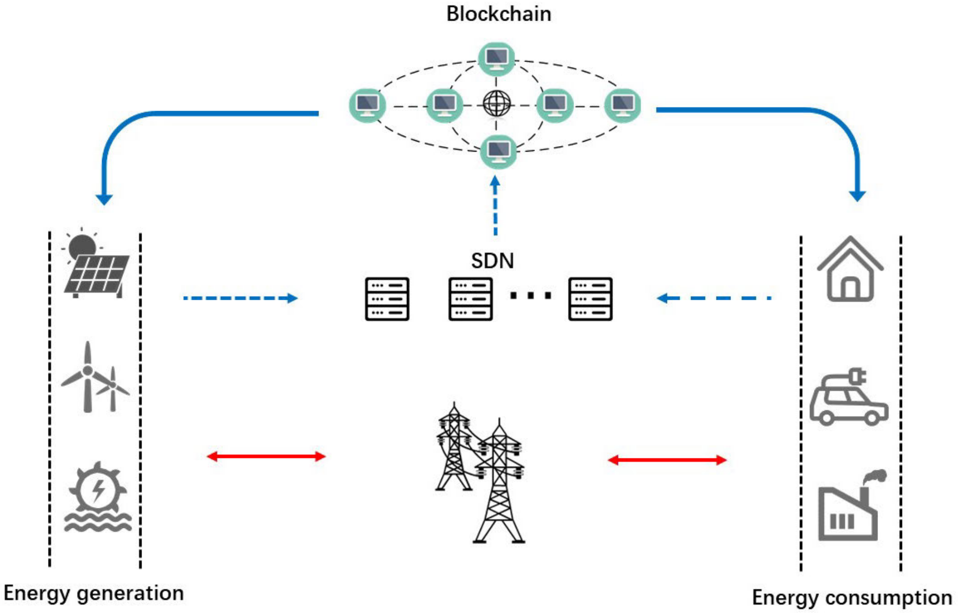


FIGURE 1. System model.

time, the energy Internet has five characteristics of renewable, distributed, interconnected, open and intelligent, which provides new possibilities and challenges for the traditional centralized energy model.

In the intelligent construction of energy Internet, an efficient communication system would be essential, i.e., a networked system and infrastructure with fast reliable information flow capability, and support for good system observability and controllability. Such communication systems would facilitate the energy Internet to achieve secure, reliable, and secure power and information exchange. Therefore, SDN has an immense potential in playing a significant role in managing the overall network and communication entities for the future energy Internet systems. As shown in Figure 1, the concept and method of the SDN are applied to the energy Internet to realize the separation of part or all of the operation, control and management of the energy Internet. This separation will greatly change the structure and operation of the traditional energy Internet, making the energy Internet more flexible. But at the same time, the SDN-based energy Internet revolution has brought some difficulties and challenges. First, in a distributed energy Internet architecture, the sheer volume of data makes it difficult for centralized systems to meet demand. Second, the security and privacy-preserving of distributed systems is difficult to solve.

As the underlying support technology of Bitcoin, the blockchain has gradually attracted everyone's attention and has developed rapidly due to its technological advantages. Blockchain is a new application mode of computer technology such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm. The blockchain uses cryptographic methods to generate data blocks that ensure the security and integrity of the transaction data. The blockchain has been applied in many domains such as finance, industry, and public services by virtue of its decentralization, openness, independence, anonymity, and security.

With its unique technical advantages, blockchain technology perfectly solves the difficulties and challenges of energy trading in the above SDN-based energy Internet. There are already some blockchain-based energy trading schemes, but most of these schemes only satisfy data integrity, and there are few researches on trading matching under the premise of ensuring data security and privacy-preserving. Combining blockchain technology with SDN-based energy Internet, we propose a distributed energy trading scheme based on SDN-based energy Internet background supported by blockchain technology. Our scheme enables secure, reliable and efficient trading of electrical energy in a distributed environment. Our innovations are as follows:

1. We propose an SDN-based energy Internet trading scheme supported by blockchain technology. The scheme realizes distributed trusted energy trading while ensuring data integrity and system security.
2. We design a new transaction matching method, introducing the manager node to achieve intelligent matching of trading users in black box. This design improves the transaction success rate while achieving user Privacy-preserving.
3. We conduct a comprehensive and detailed security analysis of the system, which fully prove the applicability and security of the system from different aspects.

The chapters of the paper are organized as follows. In the section 2, we will introduce the related work. In the section 3, we will describe the model and goals of the system in detail. In the section 4, the details of the modules and algorithms of the scheme will be explained. An analysis of the security and applicability of the system will be given in section 5. Section 6 concludes the paper.

II. RELATED WORK

Today, due to its inherent advantages, SDN has been widely used in various network domains, including data center, WAN, enterprise, optical network, underwater sensor network (UWSN), energy Internet (EI) and smart grid (SG). There have been many researches on the protocols and algorithms of SDN itself. Kim and Feamster use SDN to improve common network management and configuration tasks across a variety of different types of networks [1]. Cui shows that SDN can improve the performance of big data applications [2], and solve several questions prevailing with big data applications. Wu proposes a network functions virtualization approach based on SDN [3]. Zhang et al. propose StEERING, a scalable framework based on SDN and OpenFlow protocol [5]. Chen et al. investigate the problem of task offloading in ultra-dense network with the idea of SDN [6]. In the application of SDN, Blenk et al. made a comprehensive investigation and research on the management hypervisors for SDN networks [7]. Zhu et al. propose a privacy-preserving cross-domain attack detection scheme based on SDN [8]. Huang exploits SDN to optimize network management and introduce software defined energy harvesting IoT [9]. Wan et al. propose a new concept for industrial environments based on SDN [10].

EI as a new power generation, develops a vision of evolution of smart grids into the Internet, and has aroused global concern once proposed. In terms of EI architecture design, Dong et al. take electricity as an example to present some key assumptions and requirements for constructing the EI [11]. Cao and Yang propose a new concept of EI as an Internet-based solution to energy problems [12]. Wang et al. introduce a representative EI architecture [13], and then they propose a stability evaluation model in the EI to maintain stable and healthy environment of energy network [14]. Sani et al. propose a framework for EI network security based on the IoT [15]. Reference [16] propose a fault-tolerant and energy-efficient continuous data protection system. Su et al. propose a novel framework for a deregulated electricity market to enable EI in a residential distribution system [17]. From the current research on EI, we can conclude that EI architecture design is very complete and has high security and practicality.

In addition, because SDN plays an important role in the future smart grid system and has great potential, the SDN-based energy Internet has gradually attracted attention. Zhong et al. propose an SDEI architecture based on SDN method adopted in EI to enhance t EI [18]. Zhang et al. research communication network architecture of EI based on SDN [19]. It is not difficult to see that SDN has been widely applied in EI, and related research is also increasing.

As the most promising technology, blockchain has been applied in many domains such as security and privacy [20], [21], Internet of Things, finance, public service, key management [22], searchable encryption [23] and so on. In terms of privacy preserving, Zyskind et al. implement a protocol that turns a blockchain into an automated access-control manager to ensure users own and control their data [24]. Hawk, a blockchain model of cryptography and privacy-preserving Smart Contracts is presented, that retains transactional privacy from the public's view [25]. And Hu et al. use blockchain to construct a privacy-protected search scheme without worrying about potential wrongdoings of a malicious server [26]. In the domain of IoT, Christidis and Devetsikiotis move blockchain into the IoT domain [27], and describe a blockchain-IoT combination. Dorri et al. propose a new secure, private and lightweight architecture for IoT [28], based on blockchain technology, then the approach is exemplified in a smart home setting [29]. Oscar proposes a fully distributed access control system for IoT based on blockchain [30]. In addition, there are some other aspects of research that deserve our attention. Zhu et al. propose the CBDM, a controllable blockchain data management mode [31]. Guan et al. propose a secure and efficient energy trading scheme in IIoT-enabled energy internet based on blockchain [32]. Richter et al. evaluat the current maturity of the local electricity market based on blockchain [33].

Moreover, combining blockchain with energy trading is a potential research area. Wang et al. classify, summarize and study the existing energy trading schemes based on the blockchain [34]. Gai et al. present a consortium blockchain-oriented approach to solve the problem of privacy leakage in energy trading [35]. Aitzhan and Svetinovic use blockchain technology to slove the problem of providing transaction security in decentralized smart grid energy trading [36]. Li et al. epropose energy blockchain, a secure energy trading system based on blockchain [37]. Guan et al. propose EFFECT, an aggregation scheme with authentication in smart grid [38]. Besides, the blockchain has solved the difficult problems in the domain of EI with its unique technological advantages. For example, Yang et al. present the potential application of the blockchain technology in future EI operation [39]. Tai et al. propose a method of electricity trading management based on blockchain [40]. Wu et al. design Block Static Storage, a new blockchain storage mode based on EI [41]. From the above research, we can find that the combination of blockchain and energy trading has matured.

III. MODELS AND GOALS

In this section, we will introduce the model architecture of the system and the expected goals of the system implementation.

A. SYSTEM MODEL

As shown in Figure 2, the system builds a distributed energy trading model based on blockchain. It is not difficult to see from Figure 2. Our system consists of different entities. The following is an introduction to different entities:

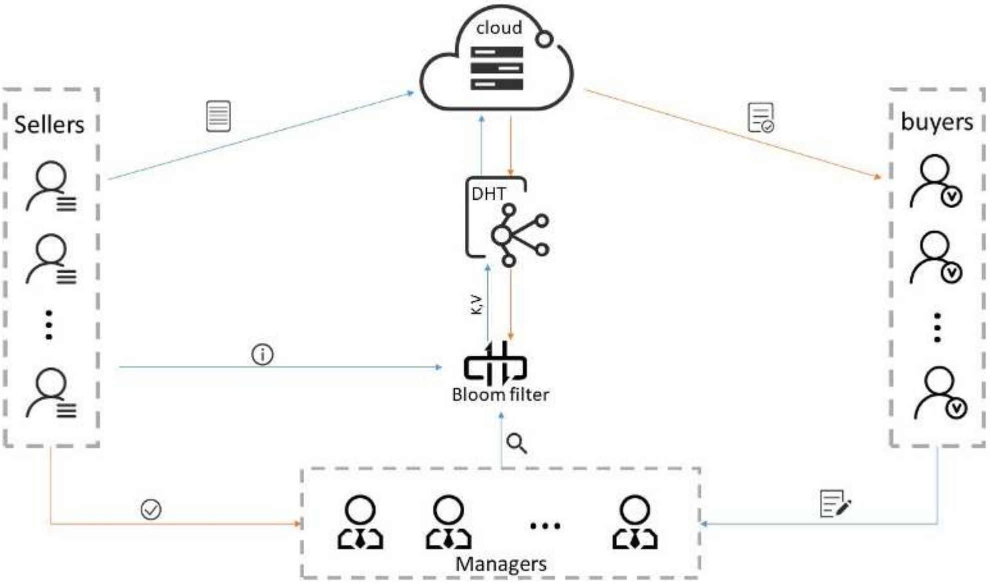


FIGURE 2. Illustration of energy trading in energy internet.

1. *Seller node*: In the distributed context of the energy Internet, users use different forms to generate electricity and sell it.
2. *Buyer node*: Electric energy users can participate in distributed energy trading as a buyer node to purchase the sold electricity.
3. *Manager node*: The manager node is a role we abstracted out. These nodes are selected from the common nodes participating in the energy trading and assist in completing the transaction.
4. *Bloom filter*: The SDN-based energy Internet generates a large amount of data and judges whether or not the target data exists from the huge information is difficult to implement in the blockchain scenario. Therefore, we use the Bloom filter to screen the electrical energy information.
5. *DHT*: Through the characteristics of the fast convergence of the distributed hash table (DHT), the location information of the data stored in the cloud is found, and the system operation efficiency is improved.

Our system is divided into three modules: electricity sales, electricity purchase, and matching. In the electricity sale module, the seller nodes generate electrical energy through the distributed power generating device and store them in the energy storage device while recording the complete electricity information in the cloud storage. Subsequently, the seller node performs a hash operation to reset the Bloom filter, and then stores the hash value in the DHT to find the location information in the cloud storage, thereby improving the search efficiency. In the electricity purchase module, the buyer node sends the demand information to the manager node and waits for the matching transaction object. In the matching module, the manager node intelligently matches the transaction object and finally completes the transaction by comparing the sales information and the purchase demand by an algorithm.

B. ADVERSARIAL MODEL

The SDN-based energy Internet requires a secure, trusted, and robust distributed trading environment. In traditional distributed systems, it is difficult to achieve data security in the context of big data, and data integrity and authenticity are difficult to guarantee. Secondly, the number of user nodes in the distributed architecture is huge, and it is difficult to achieve mutual trust between nodes. If there are malicious nodes in the system to conduct network attacks, system security cannot be guaranteed.

C. DESIGN GOALS

We propose that the SDN-based energy Internet transaction model supported by blockchain technology meets the following objectives:

1. The system can meet the needs of distributed trading scenarios and can efficiently process large amounts of transaction data. At the same time, the system needs to have strong security and robustness to defend against attacks and achieve long-term, stable and secure operation.
2. The system realizes the intelligent transaction object matching, so that the user does not need to find a suitable transaction object in a huge amount of messages, and improves the transaction success rate of the system.
3. Privacy-preserving is achieved throughout the transaction. Users can’t get other people’s electrical energy information during the transaction process, ensuring fair trade without leaking privacy.

IV. OUR SCHEME

A. SYSTEM INITIALIZATION

Our scheme is to use the DHT network as the platform to conduct electricity transaction between seller nodes and buyer nodes, so we need to establish the DHT network and update the power generation information files regularly to upload to it.

1) ESTABLISH THE NETWORK

We select Kademlia technology to establish the DHT network, which is based on unique XOR algorithm for distance measurement. Kademlia establishes a new DHT topology, which improves the speed of routing query greatly compared with other algorithms. The DHT network based on Kademlia is a tree structure. All nodes are treated as leaves of a binary tree and have a 160-bit ID value as a marker. It can converge to locate specific nodes quickly. Pointers pointing to cloud physical storage locations are stored in nodes. Through the DHT network, we can efficiently store and search the generation information files provided by the seller nodes, audit and filter the seller nodes, so as to conduct electricity trading.

2) UPDATE POWER GENERATION INFORMATION

Electric energy generated by power generation equipment is stored in energy storage equipment by smart meters, and data information of power generation attributes is generated. Seller nodes collect data information and generate generation information files regularly to upload to the DHT network. The process is as follows:

Step 1: Seller nodes form generation information file f by collecting generation attribute data by smart meters, including power generation quantity, time, speed, unit price and so on.

Step 2: Use f as the input of hash *function* $H(f)$ to obtain the fixed-length string k. We can use k as an alias for generation information file, which denotes the location of the file f in the DHT network.

Step 3: Set up Bloom filter to record file location information. Firstly, we initialize the Bloom filter, each value of the Bloom filter array is initialized to 0. Secondly, we set up the Bloom filter. Nations related to Bloom filter settings are presented in table.1

TABLE 1. Nations in bloom filter settings.

Acronym	Descriptions
f	Generation information file
$H_i(i=1,2...n)$	Hash function
$e_i(i=1,2...n)$	Random number
$p_i(i=1,2...n)$	Fixed-length string
$E_i(i=1,2...n)$	The value on the bit of the Bloom filter
$Bloom\_Filter$	Bloom filter array

we use hash functions $H_i(f)$ (i = 1, 2...n) to hash f to get p_i as index, which denotes the location information of the Bloom filter array:

$$p_i = H_i(f)\ (\mathrm{i} = 1, 2...n)$$

Among the n positions corresponding to the n indexes in the Bloom filter array, non-zero positions regard their present values as the random numbers, the first of the other zero positions is k and the others are generated by the random number generator. We use $e_i(i = 1, 2...n)$ to represent the ith random number and perform the following operations:

$$\begin{aligned} E_1 &= e_1 \\ E_2 &= E_1 \oplus e_2 \\ E_3 &= E_1 \oplus E_2 \oplus e_3 \\ &\ldots\ldots \\ E_k &= E_1 \oplus E_2 \oplus E_3 \oplus \ldots\ldots \oplus e_k \\ &\ldots\ldots \\ E_n &= E_1 \oplus E_2 \oplus E_3 \oplus \ldots\ldots \oplus E_k \oplus \ldots\ldots e_n \end{aligned}$$

Then, the n positions of Bloom filter array are assigned with E_i(i = 1, 2...n) to complete initialization. we show the detailed algorithm in table.2.

TABLE 2. Set up bloom filter.

```
Algorithm1 Set up Bloom Filter
Input: $f$ , $k$
$Bloom\_Filter \leftarrow 0$
$p_i = H_i(f)$
for var 1 to $n$ by $i$ do
    if $Bloom\_Filter[p_i] = 0$ then
        if $Bloom\_Filter[p_i]$ is the first zero position then
            $Bloom\_Filter[p_i] \leftarrow k$
        else
            $Bloom\_Filter[p_i] \leftarrow$ random number
        end if
    end if
    $e_i \leftarrow Bloom\_Filter[p_i]$
end
$E_1 \leftarrow e_1$
for var 2 to $n$ by $i$ do
    $E_i \leftarrow E_1 \oplus ... \oplus E_{i-1} \oplus e_i$
end
$Bloom\_Filter[p_i] \leftarrow E_i$
```

Step 4: Upload k to the DHT network. Find n nodes closest to k on the DHT network and broadcast new resource information to these nodes. Node k stores the pointer to physical storage locations in the cloud.

B. USER PURCHASE APPLICATION

When buyer nodes have electricity demand, they need to draw up electricity purchase contract and submit it to the DHT network for audit. All the qualified seller nodes are screened out by the DHT network.

1) DRAW UP PURCHASE CONTRACT

Buyer nodes draw up purchase contracts, which include the conditions required by the buyer nodes, such as generation capacity, unit price, threshold, compensation for breach of contract and so on.

2) AUDIT CONTRACT

In order to prevent malicious attackers sending a large number of contracts causing network congestion, buyer nodes send the prepared contracts to DHT network for audit.

3) SCREEN SELLER NODES

After confirming that the power purchase contract provided by the buyer nodes is all right, the DHT network screens out all eligible seller nodes according to the purchase contract. The process is as follows:

Step 1: The DHT network calls generation information files f of seller nodes.

Step 2: Restore position information k through Bloom filter. We use hash functions $H_i(f)$ (i = 1, 2...n) to hash to get n fixed-length strings as indexes. Then, we can determine n positions of Bloom filter array based on indexes, and get the return value $E_i(i = 1, 2...n)$ to perform the following operations:

$$k = E_1 \oplus E_2 \oplus E_3 \oplus \ldots\ldots \oplus E_n$$

If the result is empty, it indicates that the file does not exist and the seller nodes will be eliminated directly, otherwise the file storage pointer k will be obtained. We show the detailed algorithm in table.3.

TABLE 3. **Calculate the value of *k*.**

```
Algorithm2  Calculate the value of $k$
Input: $f$
Output: $k$
$p_i \leftarrow H_i(f)$
$E_i \leftarrow Bloom\_Fliter[p_i]$
$k \leftarrow E_1 \oplus E_2 \oplus E_3 \oplus \cdots\cdots \oplus E_n$
if $k = NULL$ then
    return to 1
else
    return to $k$
end if
```

Step 3: The DHT network searches the corresponding position according to the obtained k, where the pointer pointing to the cloud is stored. Then, the DHT network returns the pointer.

Step 4: Locate the actual physical storage location of the generation information file according to the pointer, obtain and return the file.

Step 5: The DHT network obtains power generation information by returning files, and screens all eligible seller nodes according to contract requirements.

C. TRANSACTION MATCHING

In this part, managers have received information which have passed the Bloom filter. The amount of information may be huge. Not all sales information meets the needs of consumers. Therefore, further classification needs to be continued.

We assume that there are $n(n \geq 1)$ seller information that have passed the Bloom filter. Assume $S = \{s_1, s_2, \ldots s_n\}$ is the set of indices for these seller information. What we need to do is to choose up to τ index as the ultimate choice for buyer nodes, where τ is determined by managers. In addition, use s_i^j to represent the $j-th$ attribute of the $i-th$ index information, where $i = \{x | 1 \leq x \leq k, x \in N\}$ and j depend on the number of attributes. Assume $A = \{a_1, a_2 \ldots a_m\}$ is the set of indices for these attributes. Here we give some attributes:

1. *Electric quantity*: How much electricity is sold by the sellers.
2. *Price*: How much per KWH.
3. *Time*: The time when the sales information was uploaded to DHT.
4. *Credit*: Integration of information such as adequacy of power supply and punctuality of power supply.
5. *Region*: Refers to the area where electricity is generated, usually taking into account the loss of long-distance transmission.

In order to facilitate the implementation of the algorithm, the value of the above attributes in the sales information is fixed.

For a buyer node b, he has requirements for certain attributes. We call the buyer's requirements for these attribute constraints. Constraints can be divided into two kinds. Equal constraints are called hard constraints and unequal constraints are called soft constraints. Soft constraints can be divided into three categories:

1. buyer nodes require that the larger the attribute value is, the better it is, such as credibility, which is called benefit constraint.
2. buyer nodes require that the smaller the attribute value is, the better it is, such as the price of electricity, which is called cost constraint.
3. buyer nodes don't require this attribute very much, they just need to be in a certain interval, which is called interval constraint. Assume c_i^j is the critical value of j attribute constraints (cost constraints or benefit constraints) of buyer node b to seller nodes (i.e. index) s_i, while the interval constraints are $[c_{i1}^j, c_{i2}^j]$. Buyer's emphasis on different attributes is determined by different weighting coefficients. Buyer's weighting coefficients for different attributes a are w_a, and the sum of all weighting coefficients is 1, i.e. $\sum_{a \in A} w_a = 1, w_a \geq 0$.

Assume when the buyer requests DHT, he will explain a series of information in the contract, including various constraints, which are accepted by the trading platform, and then matched by the trading intermediary according to the buyer's requirements. The biggest principle of matching is to maximize the matching degree between the sellers and the buyers. In order to establish the mathematical model of transaction matching more simply, the concept definition of matching degree and its calculation method are given.

Concept 1: For hard constraints, they must be satisfied $c_i^j = s_i^j$.

Concept 2: For benefits constraints, they must be satisfied $c_i^j \le s_i^j$.

Concept 3: For cost constraints, they must be satisfied $c_i^j \ge s_i^j$.

Concept 4: For interval constraints, they must be satisfied $c_{i1}^j \le s_i^j \le c_{i2}^j$.

Assume $0 \le \alpha_i^j \le 1$, α_i^j defined as the matching degree between buyer nodes and seller nodes i under attribute j. $s_{max}^j, s_{min}^j \in A^j$, where A^j is a collection of all attributes j. Then the matching degree satisfies the following conditions: for any constraint, if it does not satisfy the concepts above, then the matching degree is 0. Otherwise, for hard constraints and interval constraints, the matching degree is 1. For benefits constraints and cost constraints, the formula for calculating the matching degree is as follows:

$$\alpha_i^j = (\frac{s_i^j - s_{min}^i + \varepsilon}{s_{max}^j - s_{min}^j + \varepsilon})^t, \quad \alpha_i^j = (\frac{s_i^j - s_{min}^i + \varepsilon}{s_{max}^j - s_{min}^j + \varepsilon})^{1/t}$$

$$\text{where } t = \frac{c_i^k + (\frac{s_{max}^j + s_{min}^j}{2})}{s_{max}^j + s_{min}^j}, \varepsilon = \frac{s_{min}^j}{2}.$$

According to the above description of transaction matching, the definition of matching degree and the calculation method under different constraints, we can get a comprehensive matching degree between buyers and sellers:

$$\alpha_i = \sum_{j \in A} \alpha_i^j w_j$$

In the latter discussion we will use queues, where the node of the queue is a structure type. There are three member variables in the structure. Among them, *Comp_match_degree* is used to record the comprehensive matching, $*$ *index* is used to record the index, and $*$ *next* is used to point to the next node.

At this time, we can match the buyer node according to the comprehensive matching degree. The specific methods are as follows:

First, initialize an empty queue q. In the case that S is not empty, keep taking element s_i of S and calculate the comprehensive matching degree α_i between s_i and buyer node, then create a node to record information and join the queue q. Second, when S is empty, sort q. The sorting method is based on the comprehensive matching degree. The higher the matching degree, the higher the position of the nodes in front of the queue. Once some nodes have the same matching degree, they are arranged according to the sequence of the time when the information is uploaded to the DHT network. Finally, return the first τ nodes information to buyer node. At this point, the matching process is finished. The algorithm gives matching information to one buyer node. If it needs to match multiple buyer nodes, it only needs to run the program repeatedly. The algorithm is given in Table 4.

TABLE 4. **Matching algorithm.**

Algorithm3 Matching algorithm

Input: S, τ

Output: matching information

```
Init queue $q$ and $p$
$q.next \leftarrow p$
for (i = 0; i < n; i++)
    Calculate $\alpha_i$ of $s_i$
    Create $a$
    $a.Comp\_match\_degree \leftarrow \alpha_i$
    $a.index \leftarrow s_i$
    $a.next \leftarrow null$
    $p.next \leftarrow a$
    $p \leftarrow a$
sort $q$
for (i = 0; i < $\tau$; i++)
    $p \leftarrow q.next$
    Print $p$
    $p \leftarrow p.next$
```

1) TRANSACTION MATCHING

Transaction confirmation becomes easier when transaction matching is done. At this very moment, buyer node will get τ matching results. Buyer can choose one or more sellers to reach an agreement based on the matching results. When the buyer and the sellers reach an agreement, the newly formed power purchase contract will be deployed into the blockchain after all user nodes verify that it is legitimate. At this point, the whole process of selling electricity is over.

V. SECURITY AND APPLICABILITY ANALYSIS

In this section, we will discuss the security and applicability of the system. In terms of security, we conduct a comprehensive analysis of our system from three aspects: data security, algorithm security and privacy-preservation. And then, we will discuss the applicability of the system.

A. SECURITY ANALYSIS

1) DATA SECURITY

Traditional energy trading systems are not suitable for distributed trading of new energy due to low efficiency, high cost and poor data security. So, in this system, we use blockchain technology as the framework to improve system efficiency and ensure data security. Blockchain technology has the advantages that traditional trading platforms do not have, and blockchain can help us solve problems that appear in traditional trading platforms. Blockchain technology is decentralized to ensure rapid decision making in trading systems. At the same time, in the blockchain system, the information recorded on the chain cannot be tampered and the information is traceable, ensuring the integrity of the information [42]. In this system, we use blockchain technology to solve the shortcomings of the traditional trading platform.

2) ALGORITHM SECURITY

A hash table is a data structure that associates KEY and VALUE with a hash algorithm. The appearance of hash table makes it easy for people to query information. However, the hash table has its own problems. If the hash table is stored in a certain machine, the security and integrity of the stored information will be threatened. So, in this paper, we use a distributed hash table to store relevant information. The distributed hash table divides the entire hash table into sections, each of which is maintained by different nodes. At the same time, each part of the hash table is maintained by multiple nodes to ensure the integrity of the information. Since each part of the hash table is maintained by multiple nodes, it can prevent a node from maliciously tampering with the saved information, thereby protecting the security of the information.

The Bloom filter is a probabilistic data structure with high space utilization. The Bloom filter uses different hash functions to determine if an element is present in the record. This article uses the Bloom filter to quickly find out if the information matches. At the same time, the Bloom filter does not store the information itself, and the node cannot obtain relevant information through the Bloom filter, thus ensuring the security of the information.

The Bloom filter has the possibility of a hash collision. As the recorded data gradually increases, the possibility of a hash collision increases. This will cause the algorithm to determine that a record exists, but it does not exist. If this happens, the system will return a result that does not match the expected result. In the actual system, the returned result is judged, and if the matching result is satisfied, the result is returned and further matching is performed. Although the Bloom filter will have a hash collision, it will not affect the overall security of the system, and will not return irrelevant information to the node, protecting the privacy of unrelated users.

3) PRIVACY-PRESERVING

The system adopts the method of anonymous transaction, and the two parties cannot know the transaction object before the transaction parties finally reach an agreement. Regardless of whether the buyer node uploads the demand, or the seller node sells the purchase information, the other nodes cannot know the information about the buyer node or the seller node. Before the transaction is reached, whether it is an inquiry or a matching operation, the relevant information of the transaction user cannot be known in the process. Anonymous transactions ensure that the user's privacy cannot be obtained by other nodes.

In the system, all data is stored in the cloud. The Bloom filter does not store specific data, while the distributed hash table stores only address pointers to data in the cloud. Nodes can store relevant information in the cloud, but cannot access data stored in the cloud. Only when the transaction is matched and succeeded can the node obtain information from the cloud for further matching. The system stores data in the cloud, and nodes cannot directly access it, thus protecting the privacy of users.

The system as a whole is a black box transaction process. Neither the buyer nor the seller knows the matching process, and the buyer node and the seller node can only know the final transaction result. Both parties to the transaction cannot obtain the information stored in the cloud, and only when the information that matches successfully can be returned for further matching during the matching process. The black box transaction process protects the user's privacy [43], [44], and the user does not need to understand the running process of the entire system, which improves the system's applicability [45].

B. APPLICABILITY ANALYSIS

With the development of blockchain technology, the application of blockchain has become more and more extensive. At present, blockchain technology has not only existed in Bitcoin, but blockchain technology has been applied in various fields. Blockchain has been applied in the fields of finance, Internet of Things, and public services. In [29], privacy is protected by using blockchain technology to manage personal information. In [27], blockchain technology is used in the Internet of Things. Blockchain technology realizes the sharing of information and resources and ensures the privacy of users by means of authentication. In [46], a privacy protection search scheme for malicious servers was designed by using blockchain technology. In [26], blockchain was used to design a threshold system for use in the Internet of Things. Blockchain technology has been widely applied and provided a new direction in the development of various fields.

Blockchain technology is not only in the theoretical stage, but also applied in many practical systems. For instance, Brooklyn microgrid was developed in 2016. The system was the first blockchain-based energy trading platform. Utilizing the advantages of the blockchain, the Sunchain platform created using fabric provides a distributed solar trading system. Pylon network with blockchain technology built in Spain with full data privacy protection. With the continuous development of blockchain technology, more practical systems of blockchain will emerge and provide a better distributed platform.

In summary, our proposed SDN energy Internet trading system based on blockchain technology is applicable.

VI. CONCLUSION

This paper mainly proposes an SDN-based energy Internet trading scheme supported by blockchain technology, which realizes secure, efficient and intelligent distributed energy trading. The scheme designed a reasonable matching algorithm for trading users under the premise of ensuring privacy, which further improved the trading success rate. Finally, we conducted a comprehensive security analysis and practical analysis of the system, which fully verified the security and practical application value of the system.

Although our scheme implements blockchain-based secure and trusted distributed computing in SDN, there are still some shortcomings that we deserve to continue research. The amount of data generated by distributed systems based on SDN will be very large, which puts high demands on the efficiency and processing power of the system. At the same time, the technical characteristics of the traditional blockchain determine that it requires a lot of computational overhead and thus the system is inefficient. In the future, we can conduct in-depth research on the technical bottlenecks of blockchain scalability, consensus algorithms, security, etc. in order to be better applied in SDN.

REFERENCES

[1] H. Kim and N. Feamster, "Improving network management with software defined networking," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 114–119, Feb. 2013.

[2] L. Cui, F. R. Yu, and Q. Yan, "When big data meets software-defined networking: SDN for big data and big data for SDN," *IEEE Netw.*, vol. 30, no. 1, pp. 58–65, Jan./Feb. 2016.

[3] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, and M. Wang, "Fog-computing-enabled cognitive network function virtualization for an information-centric future Internet," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 48–54, Jul. 2019.

[4] Q. Zhang, H. Gong, X. Zhang, C. Liang, and Y.-A. Tan, "A sensitive network jitter measurement for covert timing channels over interactive traffic," *Multimedia Tools Appl.*, vol. 78, no. 3, pp. 3493–3509, 2019.

[5] Y. Zhang, N. Beheshti, L. Beliveau, G. Lefebvre, R. Manghirmalani, R. Mishra, R. Patney, M. Shirazipour, R. Subrahmaniam, C. Truchan, and M. Tatipamula, "StEERING: A software-defined Networking for Inline Service Chaining," in *Proc. 21st IEEE Int. Conf. Netw. Protocols (ICNP)*, Goettingen, Germany, Oct. 2013, pp. 1–10.

[6] M. Chen and Y. Hao, "Task offloading for mobile edge computing in software defined ultra-dense network," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 587–597, Mar. 2018.

[7] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on network virtualization hypervisors for software defined networking," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 655–685, 1st Quart., 2016.

[8] L. Zhu, X. Tang, M. Shen, X. Du, and M. Guizani, "Privacy-preserving DDoS attack detection using cross-domain traffic in software defined networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 628–643, Mar. 2018.

[9] X. Huang, R. Yu, J. Kang, Z. Xia, and Y. Zhang, "Software defined networking for energy harvesting Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1389–1399, Jun. 2018.

[10] J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, and A. Vasilakos, "Software-defined industrial Internet of Things in the context of industry 4.0," *IEEE Sensors J.*, vol. 16, no. 20, pp. 7373–7380, Oct. 2016.

[11] Z. Dong, J. Zhao, F. Wen, and Y. Xue, "From smart grid to energy Internet:Basic concept and research framework," *Automat. Electr. Power Syst.*,vol. 38, no. 15, pp. 1–11, 2014.

[12] J. Cao and M. Yang, "Energy Internet—Towards smart grid 2.0," in *Proc. 4th Int. Conf. Netw. Distrib. Comput.*, Los Angeles, CA, USA, Dec. 2013, pp. 105–110.

[13] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, Y. Xiang, and J. Wu, "A survey on energy Internet: Architecture, approach, and emerging technologies," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2403–2416, Sep. 2018.

[14] K. Wang, H. Li, Y. Feng, and G. Tian, "Big data analytics for system stability evaluation strategy in the energy Internet," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1969–1978, Aug. 2017.

[15] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Dong, "Cyber security framework for Internet of Things-based Energy Internet," *Future Gener. Comput. Syst.*, vol. 93, pp. 849–859, Apr. 2019.

[16] X. Yu, Y.-A. Tan, Z. Sun, J. Liu, C. Liang, and Q. Zhan, "A fault-tolerant and energy-efficient continuous data protection system," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 8, pp. 2945–2954, 2018.

[17] W. Su and A. Q. Huang, "Proposing a electricity market framework for the energy Internet," in *Proc. IEEE Power Energy Soc. General Meeting*, Vancouver, BC, Canada, Jul. 2013, pp. 1–5.

[18] W. Zhong, R. Yu, S. Xie, Y. Zhang, and D. H. K. Tsang, "Software defined networking for flexible and green energy Internet," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 68–75, Dec. 2016.

[19] G. Zhang, L. Su, Y. Wang, X. Liu, and J. Li, "Research on communication network architecture of energy Internet based on SDN," in *Proc. IEEE Workshop Adv. Res. Technol. Ind. Appl. (WARTIA)*, Ottawa, ON, USA, Sep. 2014, pp. 316–319.

[20] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "ASAP: An anonymous smart-parking and payment scheme in vehicular networks," *IEEE Trans. Dependable Secure Comput.*, to be published.

[21] L. Zhu, C. Zhang, C. Xu, X. Du, R. Xu, K. Sharif, and M. Guizani, "PRIF: A privacy-preserving interest-based forwarding scheme for social Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2457–2466, Aug. 2018.

[22] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 24–34, Jan. 2007.

[23] Z. Guan, X. Liu, L. Wu, J. Wu, R. Xu, J. Zhang, and Y. Li, "Cross-lingual multi-keyword rank search with semantic extension over encrypted data," *Inf. Sci.*, vol. 99, p. 1, Nov. 2019.

[24] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184.

[25] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2016, pp. 839–858.

[26] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization," in *Proc. IEEE Conf. Comput. Commun.*, Honolulu, HI, USA, Apr. 2018, pp. 792–800.

[27] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[28] A. Dorri, S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," Aug. 2016, *arXiv:1608.05187*. [Online]. Available: https://arxiv.org/abs/1608.05187

[29] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The Case Study of A Smart Home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

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

[31] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Gener. Comput. Syst.*, vol. 91, pp. 527–535, Feb. 2019.

[32] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, and M. Guizani, "Towards secure and efficient energy trading in IIoT-enabled energy Internet: A blockchain approach," *Future Gener. Comput. Syst.*, vol. 99, p. 1, Oct. 2019.

[33] B. Richter, E. Mengelkamp, and C. Weinhardt, "Maturity of blockchain technology in local electricity markets," in *Proc. 15th Int. Conf. Eur. Energy Market (EEM)*, Lodz, Poland, Jun. 2018, pp. 1–6.

[34] N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu, X. Du, and M. Guizani, "When energy trading meets blockchain in electrical power system: The state of the art," *Appl. Sci.*, vol. 9, no. 8, p. 1561, Apr. 2019.

[35] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.

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

[37] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[38] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Sci. CHINA Inf. Sci.*, vol. 62, no. 3, p. 2103, Mar. 2019.

[39] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao, and C. Lin, "Applying blockchain technology to decentralized operation in future energy Internet," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI)*, Beijing, China, Nov. 2017, pp. 1–5.

[40] X. Tai, H. Sun, and Q. Guo, "Electricity transactions and congestion management based on blockchain in energy Internet," *Power Syst. Technol.*, vol. 40, pp. 3630–3638, Dec. 2016.

[41] L. Wu, K. Meng, S. Xu, S. Li, M. Ding, and Y. Suo, "Democratic centralism: A hybrid blockchain architecture and its applications in energy Internet," in *Proc. IEEE Int. Conf. Energy Internet (ICEI)*, Beijing, China, Apr. 2017, pp. 176–181.

[42] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun. Mag.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.

[43] X. Gao, Y. Tan, H. Jiang, Q. Zhang, and X. Kuang, "Boosting targeted black-box attacks via ensemble substitute training and linear augmentation," *Appl. Sci.*, vol. 9, no. 11, p. 2286, Jun. 2019, doi:10.3390/app9112286.

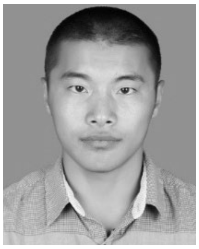
[44] Y. Xue, Y.-A. Tan, C. Liang, Y. Li, J. Zheng, and Q. Zhang, "RootAgency: A digital signature-based root privilege management agency for cloud terminal devices," *Inf. Sci.*, vol. 444, pp. 36–50, May 2018.

[45] Y. Li, S. Yao, K. Yang, Y.-A. Tan, and Q. Zhang, "A high-imperceptibility and histogram-shifting data hiding scheme for JPEG images," *IEEE Access*, vol. 7, pp. 73573–73582, 2019.

[46] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

XIN LU received the B.Eng. degree from North China Electric Power University, in 2017, where he is currently pursuing the master's degree with the School of Control and Computer Engineering. His current research interests include smart grid security and cloud security.

LINGYUN SHI received the B.Eng. degree from Beijing Technology and Business University, in 2019. She is currently pursuing the master's degree with the School of Control and Computer Engineering, North China Electric Power University. Her current research interest includes smart grid security.



ZHENYU CHEN received the B.Eng. degree from North China Electric Power University, in 2019, where he is currently pursuing the master's degree with the School of Control and Computer Engineering. His current research interest includes smart grid security.

XUNFENG FAN received the B.Eng. degree from North China Electric Power University, in 2019, where he is currently pursuing the master's degree with the School of Control and Computer Engineering. His current research interest includes smart grid security.

ZHITAO GUAN (M'13) received the B.Eng. and Ph.D. degrees in computer application from the Beijing Institute of Technology, China, in 2002 and 2008, respectively. He is currently an Associate Professor with the School of Control and Computer Engineering, North China Electric Power University. His current research interests include smart grid security, wireless security, and cloud security. He has authored over 60 peer-reviewed journals and conference papers in these areas.

XIAOJIANG DU (M'04–SM'09–F'20) received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, in 2002 and 2003, respectively. He was an Assistant Professor with the Department of Computer Science, North Dakota State University, from August 2004 and July 2009, where he received the Excellence in Research Award, in May 2009. He is currently a Professor with the Department of Computer and Information Sciences, Temple University. His research interests include security, wireless networks, and computer networks and systems. He has published over 200 journals and conference papers in these areas. He is a Life Member of ACM.

MOHSEN GUIZANI (S'85–M'89–SM'99–F'09) received the B.S. (Hons.) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor with the Computer Science and Engineering Department, Qatar University, Qatar. Previously, he served in different academic and administrative positions at the University of Idaho, Western Michigan University, University of West Florida, University of Missouri-Kansas City, University of Colorado Boulder, and Syracuse University. He is the author of nine books and more than 500 publications in refereed journals and conferences. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is a Senior Member of ACM. He is currently the Editor-in-Chief of the *IEEE Network Magazine*, serves on the editorial boards of several international technical journals.