Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Blockchain Based Data Monitoring and Sharing Approach for Smart Grids

YANHAN YANG[1], MINGZHE LIU*[1], QIN ZHOU[1], HELEN ZHOU[2], and RUILI WANG[3]

[1]State Key Laboratory of Geohazard Prevention and Geoenvironment Protection, Chengdu University of Technology, Sichuan 610059, China
[2]School of Engineering, Manukau Institute of Technology, Auckland, New Zealand
[3]School of Natural and Computational Sciences, Massey University, Auckland, New Zealand

Corresponding author: Mingzhe Liu (e-mail: liumz@cdut.edu.cn).

ABSTRACT With the development of science and technology, human beings cannot live without electricity. The introduction of smart grid systems brings new ideas to break the shackle of existing electricity systems. This paper proposes a mechanism with data monitoring and sharing capabilities based on the consortium blockchain, realizing comprehensive monitoring of smart devices, and promoting the effective sharing of electrical data in smart grids. When a smart device is out of order, the smart contract connected to it will be triggered, and the users can check the running status through the smart phone. This approach allows nodes in the consortium blockchain to request transactions, using the prepaid payment smart contract with time-lock script to protect the consumer right of request nodes. In addition, we use a (t,n) -threshold secret sharing scheme to realize multiparty sharing of electrical data. Paillier encryption arithmetic is used to guarantee the confidentiality of messages in node transaction.

INDEX TERMS Consortium blockchain, Data sharing, Smart contract, Smart grids.

I. INTRODUCTION

The continuous progress of science and technology has led to the change of the way of life around the world. Use of electricity has been a breakthrough for the development of new technologies [1]. Smart grids are improving the existing power system to make it more efficient and reliable, and provide more intelligent services for the users who are connected to it [2]. Smart grids balance energy demand and grid energy production for delivering flexible services and appropriately financial settlement, under the form of adaptation of energy demand profiles, to all stakeholders involved in the market [3], [4].

The smart home communicates with the smart grid by logging and sending data to the smart grid through smart meters or other smart devices. In a smart grid system, the real-time data is uploaded to the grid system through the Internet to conduct bill settlement for users. The data which belongs to the personal privacy of users transferred via the Internet can be compromised when it falls into the hands of malicious actors [5]-[7]. Users usually receive a monthly bill from the vendor, which does not contain any details of the purchase or suggestions. In a traditional grid system, data acquisition base stations mainly adopt local and self-management methods [8], resulting in substandard operation of power generation and transmission, and such losses are about 20%-30% of the total capacity [9].

In recent years, many solutions have been proposed to address the problems arising from smart grids. Umar *et al.* [10] proposed a method to process efficiency of smart grid by improving the automation and monitoring capabilities of smart grid infrastructure. A distributed architecture is applied to the smart home. The smart gateway inside the smart home manages the sensors in the smart home.

Sebnem *et al.* [11] proposed a smart grid data management model based on the characteristics of cloud computing. The model aims to provide a platform for flexible collaboration across organizational boundaries of network operators and energy service providers. Smart grids have a huge amount of information, and the cloud computing model can meet the requirements of collaborative and intensive data computing as well as multiparty data sharing.

Guan *et al.* [12] proposed a privacy-preserving and efficient data aggregation scheme to prevent attackers from analyzing the user’s electricity consumption profile from adversaries. Users are divided into different groups, and the privacy of group members is protected by private blockchain.

Zhang *et al.* [13] proposed a blockchain based secure equipment diagnosis mechanism of smart grids. In case of equipment problems, a diagnosis can be requested in the consortium blockchain. The aim of their paper is to propose a double auction mechanism, which can bring fast, convenient and safe device diagnosis to users.

The increasingly complex interaction among different energy entities calls for a secure, efficient, and robust cyber infrastructure [14]. As an emerging distributed computing technology, blockchain provides a secure environment to support such interaction. The public blockchain generally requires all nodes in the network to synchronize information, and the efficiency of transaction largely depends on the processing capacity of a single node. These can easily lead to serious network congestion in blockchain. On the basis of the above, we propose the consortium blockchain mechanism to help users monitor the operation of smart home appliances and support data sharing in smart grids among multiple sharing parties.

In our scheme, based on the combination of smart grids and consortium blockchain, a data monitoring and sharing mechanism (DMSM) can be realized. To ensure no falsifying of blockchain and the privacy-preserving of users, the data transmitted to the smart grid needs to be hashed and the data hash value is stored in the blockchain. In addition, we connect smart devices with smart contracts, so that the smart grid can send notifications to users through their smart phones. Users can apply to the processing node to disclose the details of their personal bills through their personal ID . Finally, the electrical data in the smart grid is encrypted and sent to the cloud. We use the (t,n) -threshold secret sharing scheme to share the key and promote the data sharing nodes to jointly maintain the security in the cloud. This paper is organized as follows. Section II introduces the basic concept of blockchain and some algorithms. Section III details the framework and layering of the proposed mechanism. Section IV constructs some operational details, including the prepaid payment smart contract and the data storage policy. Section V introduces the implementation process of equipment monitoring, user's request and data sharing. Section VI analyzes the security of the scheme and section VII concludes the paper.

II. PRELIMINARY

A. BLOCKCHAIN

Blockchain was first proposed in 2008 by a scholar using the alias "satoshi nakamoto" in "Bitcoin: A Peer-to-Peer Electronic Cash System", which is a data structure used to record the account history of bitcoin transactions [15]. In essence, blockchain is a point-to-point distributed network and a distributed database technology. It packs data into blocks, in the order in which transactions occur, and then connects the blocks in a chain. The blockchain has the characteristics of decentralization, anonymity, programmability and trustworthiness. Blockchain defines credit in a mathematical way, thus replacing the traditional centralized system based on central trust and adopting the distributed node trust mechanism. Depending on the timestamp in the blockchain, each block in the blockchain adds a time dimension that becomes traceable. When transactions occur in the smart grid, other nodes in the consortium blockchain also see the interaction information. After the new block is mined and formed, the temporary information will be replaced by the new block and the hash value will be generated [16].

According to different participants, blockchain can be roughly divided into public blockchain, consortium blockchain and private blockchain [17]. Information is fully disclosed in the public blockchain, and anyone can maintain the blockchain and extract information from it. Because of these characteristics of the public blockchain, the public blockchain requires all nodes in the network to synchronize information, resulting in network congestion. That does not apply to our scheme. In addition, a closed private chain is obviously not appropriate. Therefore, we adopt the consortium blockchain in the proposed scheme.

B. BONEH-LYNN-SHACHAM SHORT SIGNATURE SCHEME

Boneh-Lynn-Shacham (BLS) Short Signature Scheme is based on the computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves, and it is also a typical bilinear pairing scheme [18]. Let G' be a cyclic additive group generated by G , whose order is a big prime q , and G'' be a cyclic multiplicative group with the same order q [19], [20]. The $e:G'\times G'\to G''$ satisfies the following properties:

Bilinearity. $e(aG,bQ)=e(G,Q)^{ab}$ for all $G,Q\in G'$, $a,b\in Z_q$.

A hash function can be defined as $h:\{0,1\}^*\to G'^*$, which the security analysis views as a random oracle [21]. Given G' and G'' are cyclic additive groups.

Key generation. Given a bilinear pairing $e:G'\times G'\to G''$, and pick random $\rho\in Z_q^*$ as the secret key and compute $\rho\cdot G$ as the public key.

Signature. Given the plaintext $m\in G'$ and compute $h(m)=M^*$. Then, $\rho\cdot M^*$ is the signature sig .

Verification. If $e(\rho\cdot G,M)=e(G,sig)$, it proves that the signature can be verified. Otherwise fail.

C. THE PAILLIER CRYPTOSYSTM

In 1999, Paillier proposed a novel computational problem, namely the Composite Residuosity Class Problem, and its applications to public-key cryptography [22]-[24].

Encryption. The first step in encrypting information using the Paillier encryption algorithm is to create a public key. Two large primes can be chosen as p and q . And then

$$n=p\cdot q \tag{1}$$

Choosing $g\in Z_{n^2}^*$ and a random nonzero integer $r\in Z_n^*$, and the public key is $pk=(n,g)$. The plaintext is $m\in Z_n$, and

$$M=g^m r^n \bmod n^2 \tag{2}$$

Decryption. The lcm is the least common multiple, and

$$\lambda(n)=lcm\left[(p-1)\cdot(q-1)\right] \tag{3}$$

A safety parameter k of the same length as p and q can be chosen, and

$$L(u)=(u-1)/n \tag{4}$$
$$L(g^{\lambda(n)} \bmod n^2)=k \tag{5}$$
$$\mu=k^{-1} \bmod n \tag{6}$$

Based on the private key $sk=(\lambda,\mu)$, the plaintext m can be calculated as

$$m=L(M^{\lambda(n)} \bmod n^2)\cdot\mu \bmod n \tag{7}$$

D. FELDMAN VERIFIABLE SECRET SHARING SCHEME

Shamir and Blakley firstly proposed a (t,n) -threshold secret sharing scheme [25], [26], and then Feldman proposed a verifiable secret sharing (VSS) scheme [27] in order to solve the honesty problem of the distributor and participant members.

After the private key is calculated, it is divided into a group of key $(sk_1,sk_2,...,sk_i)$, which are randomly distributed to n data sharing nodes and each member's key is promised. sk_i is the key of s_i, and the correctness of sk_i can be verified after s_i receives sk_i. In n share holder members, any t valid members can cooperate to reconstruct the private key. This means that one party wants to decrypt the ciphertext, at least $(t-1)$ keys of other parties are needed to be aggregated.

III. DESIGN FORMULATION

In the proposed scheme, users monitor smart devices through smart contracts and smart phones. Users can request personal transactions in the consortium blockchain. The encrypted data in the smart grid is uploaded to the cloud, and the encrypted data can be shared with data sharing nodes through key sharing.

A. PREPARATORY WORK

Table 1 lists definitions of all symbols used in this paper.

TABLE 1. Symbols used in this paper.

Symbol	Definition
C	Set of consortium blockchain nodes
U	Set of user nodes
S	Set of data sharing nodes
P	Set of processing nodes
D	Set of device nodes
M	Encryption message for nodes
ρ	Private key for nodes
R	Relevant file for nodes
m	Message for nodes
ID	Identifier for nodes
σ	Signature for nodes
$Timestamp$	Timestamp
CID	Identifier for requests
M^*	Hash value of m

B. MECHANISM DESIGN

Figure 1 shows the general architecture of our proposed solution. The following is a detailed description of the architecture.

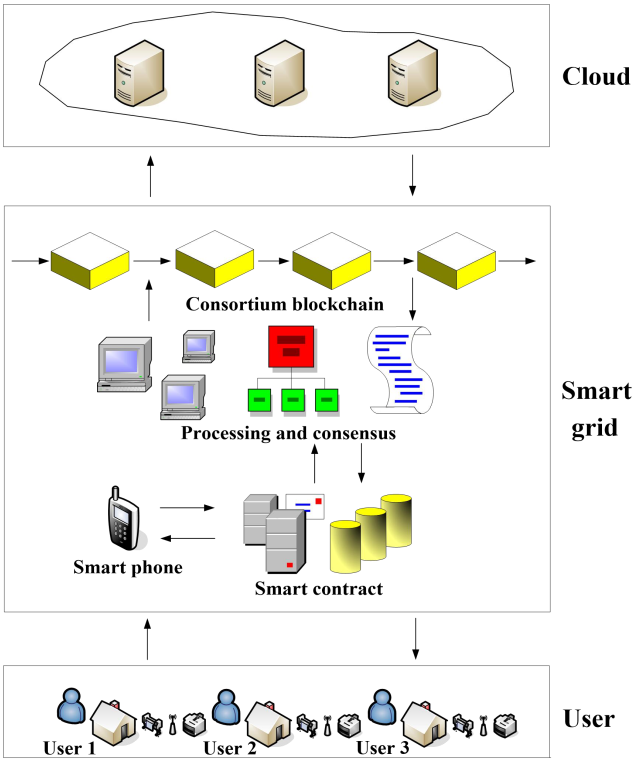

FIGURE 1. Data monitoring and sharing mechanism structure.

Consortium blockchain node is a node in consortium blockchain network, expressed as c, and a set of nodes as $C=\{c_1,c_2,\ldots,c_n\}$, $c_i\in C$. Each node has a unique identifier ID that identifies the node.

Electrical entities, including residential residents, schools and companies, can be user nodes. As the owner of smart devices, users will receive notifications about the status of smart devices bound to smart contracts through their mobile phones and make corresponding policy adjustments according to the notifications. A set of user nodes are referred to as $U=\{u_1,u_2,\ldots,u_n\}$, $u_i\in U$, $U\subseteq C$.

Processing nodes are geographically divided, and each region has processing nodes dedicated to managing local user nodes. The user node can only request transactions from the local processing node. A set of processing nodes are referred to as $P=\{p_1,p_2,\ldots,p_n\}$, $p_i \in P$, $P \subseteq C$.

Device nodes are smart devices in the consortium blockchain, such as smart meters for household use. The device node ID_{d_i} is also registered on the consortium blockchain. A set of device nodes are referred to as $D=\{d_1,d_2,\ldots,d_n\}$, $d_i \in D$, $D \subseteq C$.

Vendors or other entities that require electrical data for research can be data sharing nodes. In order to share electrical data preferably, the encrypted electrical data is stored in the cloud. The data sharing node ID_{s_i} is registered on the consortium blockchain. A set of data sharing nodes are referred to as $S=\{s_1,s_2,\ldots,s_n\}$, $s_i \in S$, $S \subseteq C$.

C. BLOCK STRUCTURE

As shown in Fig. 2, the data in the consortium blockchain is stored in the block, and each data block contains a block header and a block body. Each block header quotes the previous block header's hash and is stored in linked list to establish the connection between blocks. The block body includes the number of transactions in the current block and all transaction records generated during the verified block creation process [28].

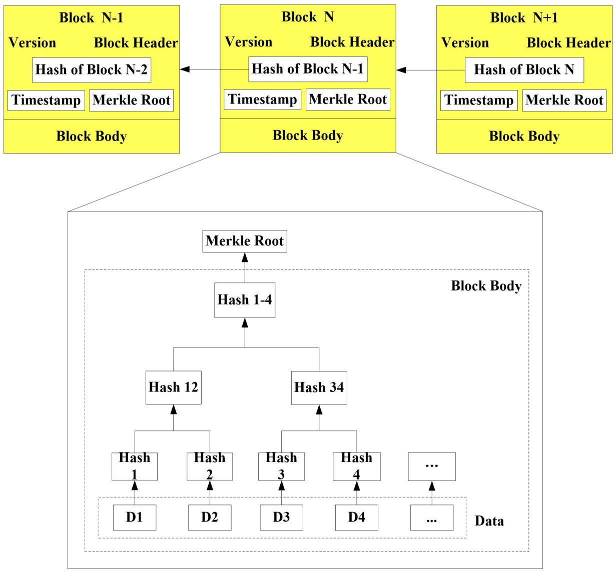

FIGURE 2. Block structure.

SHA-256 hash algorithm is used in our proposed scheme. The output sequence is of fixed length 2^{256}, regardless of the input sequence length [29]. For the hash function, even small changes in the input can make a big difference in the output.

IV. DATA STORAGE AND PREPAID PAYMENT TRANSACTION

We set up the prepaid payment smart contract for transactions between the request node and the processing node. In the smart grid, the data is huge and complex, so we need to consider how to store data reasonably and save space.

A. DATA STORAGE

Electrical data is transmitted in the smart grid, and p_i processes electrical data within its jurisdiction. The main task of p_i is to hash, store and upload the electrical data as follows:

1. Let $h:\{0,1\}^* \rightarrow \{0,1\}^l$ be a cryptographic hash function SHA-256. For the electrical data to be encrypted, p_i first generates $M^* = h(h(m))$.

2. p_i uses encryption parameters (n_{p_i}, g_{p_i}) to encryption m as $M_{p_i} = E(m) = g_{p_i}^m \cdot r^{n_{p_i}} \bmod n_{p_i}^{\ 2}$.

3. p_i sends M_{p_i} and M^* together to the cloud for storage.

4. Then, the consensus node creates a package from it that contains p_i's unique identity ID_{p_i} for the valid transaction and the hash value M^* for electrical data. The packet is then processed and converted into a block, which is verified and attached to the consortium blockchain.

B. PREPAID PAYMENT SMART CONTRACT

In the proposed blockchain-based smart grid, users are free to make requests that include the disclosure of electricity consumption of consumer bills and other legitimate transactions within the smart grid regulations. Data sharing nodes in the consortium blockchain can also request freely according to their own data sharing requirements. But before making the request, the request node needs to go through the process shown in Fig. 3. In this section, we assume that the request node is a user node to illustrate the operation, and the data sharing node operation is the same in the actual process.

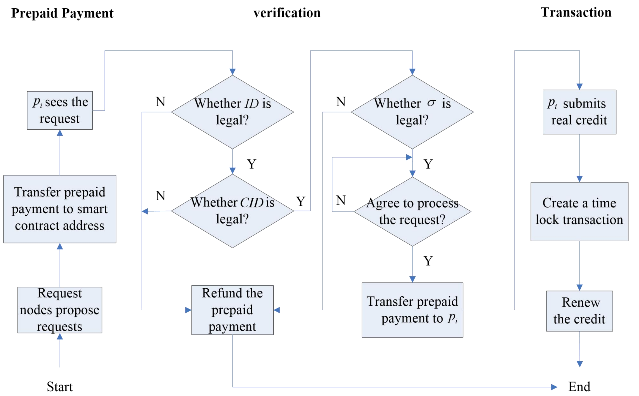
Prepaid Payment
verification
Transaction
p_i sees the request
Transfer prepaid payment to smart contract address
Request nodes propose requests
Start
N
Whether ID is legal?
Y
N
Whether CID is legal?
Y
Refund the prepaid payment
N
Whether σ is legal?
Y
N
Agree to process the request?
Y
Transfer prepaid payment to p_i
p_i submits real credit
Create a time lock transaction
Renew the credit
End

FIGURE 3. Prepaid payment smart contract.

Prepaid payment includes three steps:

a. The node needs to transfer the prepaid payment to the smart contract address before making the individual.

b. request. The type and price of requests are specified by the energy center that provides the data support.

c. The request node encrypts his message into M and signs it with the personal private key. Then, the message is packaged as R and sent to p_i.

Validation also includes three steps:

a. p_i immediately verifies the ID after receiving R. If the ID is valid, p_i goes to the next step. Otherwise, p_i sends the information and prepaid payment back to the requester.

b. After validating the ID, p_i continues to validate CID. CID represents the type of the request and is generated based on the request content of the user node. If CID is not of the smart grid specified type, the information and the prepaid payment will be sent back to the requester and the process will be terminated.

c. p_i finally verifies the BLS short signature of the request node. Verified by the following calculation:

$$e(G,\sigma)=e(\rho\cdot G,h(R)) \tag{8}$$

If the equation is true, it is verified and fails otherwise. p_i determines whether to immediately respond to the request.

Transaction includes following steps:

After p_i accepts the request, the prepaid payment in the smart contract address will be transferred to p_i's address. p_i also needs to submit its real credit to the smart contract. After that, p_i and the request node jointly create a payment transaction that contains the prepaid payment. While p_i is processing the request, perhaps the network suddenly crashes or drops the line. So we use the time-lock script shown in Fig. 4 to make a full refund to the request node.

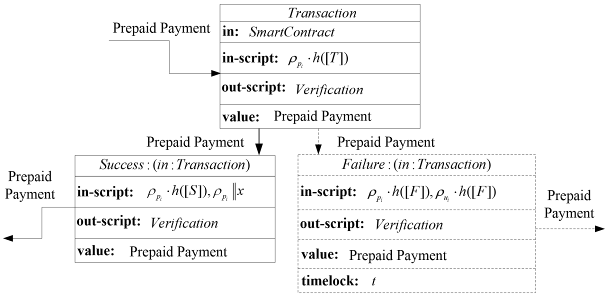

FIGURE 4. Time-lock transaction.

The time-lock script is also used in [30], but their main aim is to prevent either side of the deal from breaking the rules. The main purpose of us is to ensure that the requester can receive the result within a time limit T. The transaction creation process is as follows:

a. p_i and u_i exchange a secret factor such that $C=h(\rho_{p_i}\|x)$.

b. p_i sends $C=h(\rho_{p_i}\|x)$ and $c=\rho_{p_i}\|x$ to u_i.

c. p_i creates $Transaction$ and posts it on the consortium blockchain.

d. p_i creates the body of $Failure$ with time-lock set to a time T, and sends it to u_i with signature.

e. u_i completes $Failure$ with his own signature on the body.

p_i opens $Transaction$ and one will get the prepaid payment as long as the request content is sent to u_i within time T. If p_i does not provide the corresponding service within time T, p_i will lose the prepaid payment. The setting of time-lock can urge p_i to provide service for the requester as soon as possible. To some extent, time-lock script protects the interests of the requesting node. After that, p_i updates the credit value according to the transaction result. If the request is completed within time T, the credit value goes up and down otherwise. All nodes in the consortium blockchain can see the credit value of p_i.

V. IMPLEMENTATION OF DATA MONITORING AND SHARING MECHANISM

As mentioned above, the proposed mechanism is divided into three parts as notification about smart devices, request of user nodes, and data sharing.

In order to make the mechanism of our design more specific, we set up five smart devices based on Hyperledger Fabric, and set one host as the cloud. Each device node is built by the same Raspberry PI hardware, and we deploy our smart contract on the Linux system, and the five smart devices are all access to the same network. The following Fig. 5 shows the test network and the server environment.

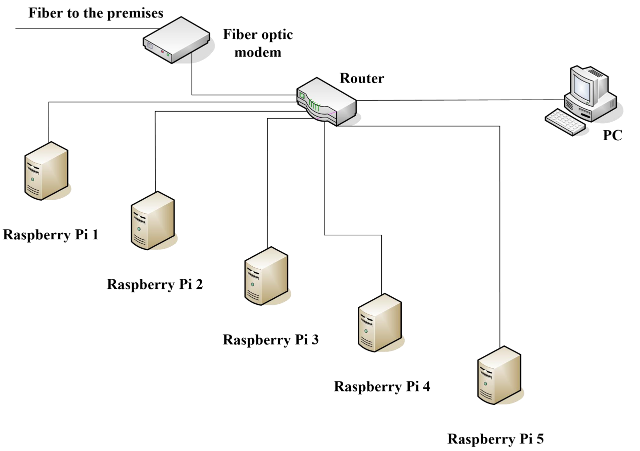

FIGURE 5. Test network and server environment.

A. NOTIFICATION ABOUT SMART DEVICES

We connect smart contracts with smart devices, establish equipment policies, and monitor the operation of smart devices. The smart contract is located on the consortium blockchain, and the execution process will not be changed due to other factors after the contract is triggered. This ability to express logic in open, trusted and verifiable peer-to-peer systems provide an opportunity for individual users and groups to delegate some of their activities to the blockchain [31]. All data transmission is conducted under the joint monitoring of the consortium blockchain to increase the reliability of electrical data in the smart grid.

After the user successfully installs the smart device, the smart device connects to the smart contract and registers the ID_{d_i} in the blockchain. As shown in Algorithm 1, the status of smart devices can be divided into startup and shutdown, mainly focusing on whether the operation of devices is stable. A smart contract can be triggered if a device runs at too high

Algorithm 1 Notification Smart Contract

```
Class ContractNotificationRule{
public deviceID;
public low.threshold;
public high.threshold;
public device.power;
public device.temperature;
public key;
function comment(){
if device.power >= high.threshold then
    comment == "The power of the device with"-deviceID-"is too high";
else if device.power <= low.threshold then
    comment == "The power of the device with"-deviceID-"is too low";
else {comment == "The device with"-deviceID-"is in operation";}
end if
function encrypt(key, signature){retrieve key;
encrypt comment();}
function main(){
if device.temperature >= temperature.warning then
    comment == "The temperature of the device with"-deviceID-"is too high";
    encrypt(key);
else{return null;}
end if
if device.power > 0 then
encrypt(key);
else{comment == "The device with"-deviceID-"has been shut down";}
end if
```

or too low power. Besides, device temperature is also the focus of our attention, once the device temperature exceeds the warning value will also trigger the smart contract. The smart contract uses its private key to encrypt the report and send it to the smart grid network. Users can receive the report of the smart device on the smart contract client through their smart phone, and the smart contract client is responsible for the deployment and adjustment of the smart contract.

We switched the five devices on and off a hundred times, and sent notification transactions with high temperature, and counted the blockchain processing delay and resource consumption (CPU and memory consumption) of each notification transaction in the whole 100 network monitoring in the Raspberry Pi. The figure below describes the delay distribution of all notification transactions in the network. It can be seen from the Fig. 6 that it takes about one second to add a single notification transaction to the public ledger (the sum of the consumption of both consensus and storage delays), and the resource distribution in the network is relatively uniform and stable.

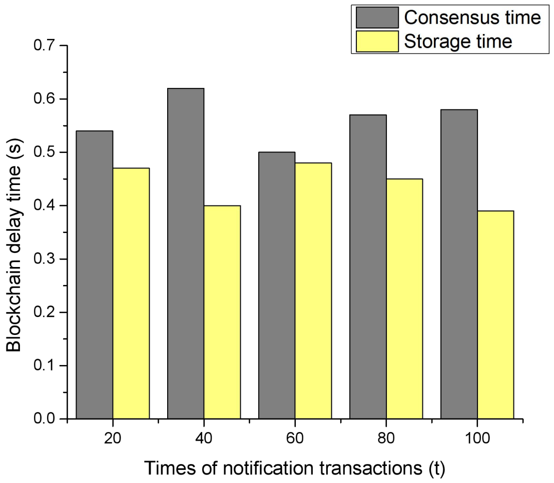

FIGURE 6. Delay time of notification transactions.

B. REQUESTS OF USER NODES

In our proposed blockchain based smart grid, users are allowed to make personal requests. The transaction could be a request for details about this month's bills or advice for better household electricity. The energy center needs to set up the prepaid payment to avoid too many invalid requests leading to system network congestion. Figure 7 illustrates the specific process of user request, and details are as follows:

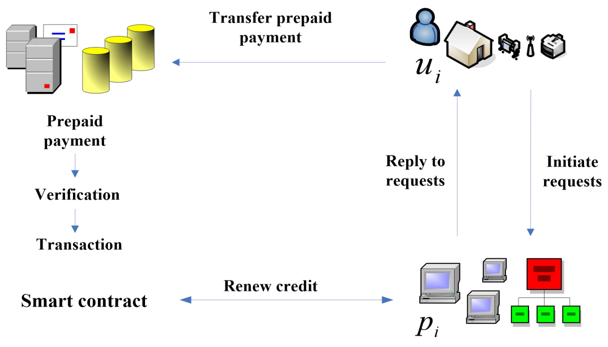

FIGURE 7. Request procedure of user nodes.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2952687, IEEE Access

1. The user node, u_i, uses p_i encryption parameters (n_{p_i}, g_{p_i}) to encrypt request details m_{u_i}, generating ciphertext $M_{u_i} = E(m_{u_i}) = g_{p_i}^{m_{u_i}} r^{n_{p_i}} \bmod n_{p_i}{}^2$ with corresponding BLS signature $\sigma_{u_i} = \rho_{u_i} \cdot h(M_{u_i} \| ID_{u_i} \| ID_{p_i} \| CID_{u_i} \| Timestamp)$. CID_{u_i} is the content identifier generated by u_i from the requested content.

2. u_i forwards $R_{u_i} = \{M_{u_i} \| ID_{u_i} \| ID_{p_i} \| CID_{u_i} \| Timestamp\}$ to p_i, where $Timestamp$ is the current timestamp. u_i transfers the prepaid payment to the smart contract address. The prepaid payment smart contract is executed according to the scenario described in IV B. p_i verifies the authenticity of u_i's BLS signature.

3. If the above conditions are all satisfied, p_i extracts the request information $m_{u_i} = D(M_{u_i}) = L(M_{u_i}{}^{\lambda_{p_i}} \bmod n_{p_i}{}^2) \cdot \mu_{p_i} \bmod n_{p_i}$ using $(\lambda_{p_i}, \mu_{p_i})$. Depending on m_{u_i}, p_i obtains the corresponding response, m_{p_i}, from the smart grid database.

4. p_i encrypts m_{p_i} using the u_i encryption parameters (n_{u_i}, g_{u_i}), generating ciphertext $M_{p_i} = E(m_{p_i}) = g_{u_i}^{m_{p_i}} r^{n_{u_i}} \bmod n_{u_i}{}^2$ and signature $\sigma_{p_i} = \rho_{p_i} \cdot h(M_{p_i} \| ID_{u_i} \| ID_{p_i} \| Timestamp)$ with ρ_{p_i} (the private key for p_i), and forwards $R_{p_i} = \{M_{p_i} \| ID_{u_i} \| ID_{p_i} \| Timestamp\}$ to u_i.

5. No matter whether p_i is sent to u_i in time T, the time-lock transaction will be executed automatically as soon as the time is up. The result of the transaction is either that p_i successfully gets the prepaid payment or the transaction fails and the prepaid payment is transferred to the address of u_i. Regardless of the outcome, the prepaid payment smart contract will refresh the credit value for p_i, which will be submitted for further evaluation in the next transaction.

C. DATA SHARING

Data sharing nodes are allowed to broadcast sharing requests and then share electrical data with our proposed smart grid. As shown in Fig. 8, after s_i broadcasts the request, it needs to transfer the prepaid payment for application to the data sharing smart contract and request to get a form of p_i that is willing to provide the data sharing service. Details are as follows:

Prepaid payment for application. s_i broadcasts the request and transfers the prepaid payment for application to the data sharing smart contract address. Note that the request for s_i broadcasts should carefully describe the conditions under which they want the electrical data, such as time or location.

Response. After p_i sees the news broadcast by s_i, it first verifies whether the ID_{s_i} of s_i is legal. If ID_{s_i} is not verified, the data sharing smart contract will send the prepaid payment for application back to s_i. Otherwise, p_i should consider whether to agree to the data sharing request, and if p_i decides to respond, it will transfer one's current credit value to the data sharing smart contract.

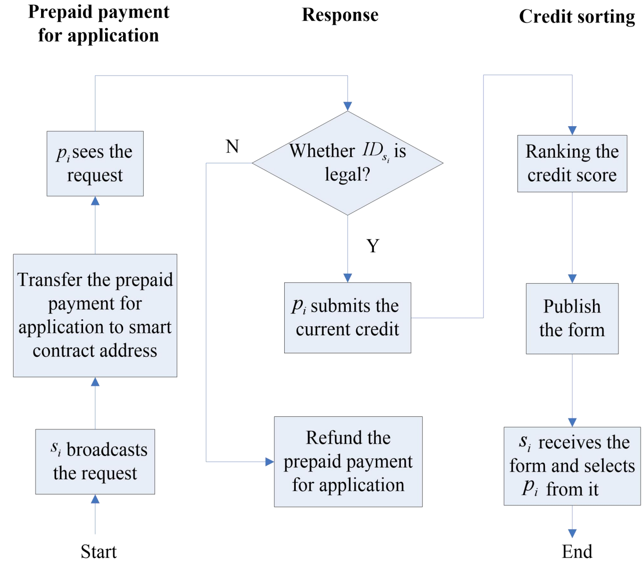
Prepaid payment for application
Response
Credit sorting
p_i sees the request
N
Whether ID_{s_i} is legal?
Ranking the credit score
Y
Transfer the prepaid payment for application to smart contract address
p_i submits the current credit
Publish the form
s_i broadcasts the request
Refund the prepaid payment for application
s_i receives the form and selects p_i from it
Start
End

FIGURE 8. Data sharing in smart contract.

Credit sorting. The data sharing smart contract sorts the processing nodes that have submitted the current credit and it creates a form that uses the credit score to sort from high to low. The form is exposed to all consortium blockchain members and the node is selected by s_i in the form. If the credit value of p_i is too low, it may not be selected by s_i.

After s_i selects p_i, s_i can apply to p_i for sharing electrical data. Note that s_i can request electrical data from multiple p_i, and different p_i only represents processing nodes in different regions. Figure 9 shows the process of s_i requesting sharing as follows:

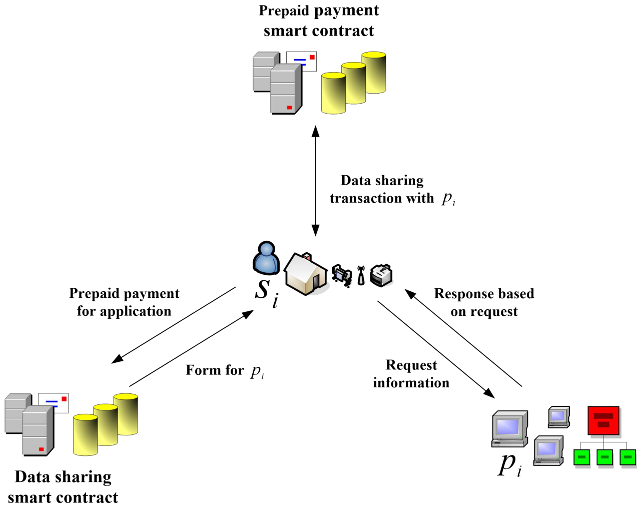
Prepaid payment smart contract
Data sharing transaction with p_i
s_i
Prepaid payment for application
Response based on request
Form for p_i
Request information
Data sharing smart contract
p_i

FIGURE 9. Request procedure of data sharing nodes.

1. s_i is executed according to the prepaid payment smart contract scheme described in IV B. s_i uses p_i encryption parameters (n_{p_i}, g_{p_i}) to encrypt request details m_{s_i}, generating ciphertext $M_{s_i} = E(m_{s_i}) = g_{p_i}^{m_{s_i}} r^{n_{p_i}} \bmod n_{p_i}{}^2$ with corresponding BLS signature $\sigma_{s_i} = \rho_{s_i} \cdot h(M_{s_i} \| ID_{s_i} \| ID_{p_i} \| CID_{s_i} \| Timestamp)$. s_i describes a group of data sharing nodes in m_{s_i}. The total number of n members of the group, including s_i, is denoted as $S(|S| = n)$. CID_{s_i} is the content identifier generated by s_i from the requested content.

2. p_i verifies the authenticity of s_i's BLS signature. Only the above conditions are all satisfied, p_i extracts the request information $D(M_{s_i}) = m_{s_i} = L(M_{s_i}{}^{\lambda_{p_i}} \bmod n_{p_i}{}^2) \cdot \mu_{p_i} \bmod n_{p_i}$ using $(\lambda_{p_i}, \mu_{p_i})$. Depending on m_{s_i}, p_i creates the time-lock transaction with s_i.

3. According to the request of s_i, the key is randomly distributed to a group of data sharing nodes including s_i in the manner of D in II. It is also necessary to verify these nodes before issuing the keys.

4. If all members of this group get the key before the time required by the time-lock script, p_i can get the prepaid payment. Otherwise, the transaction fails and the prepaid payment will be refund to s_i.

5. The prepaid payment smart contract will return a credit value for p_i based on the outcome of the transaction.

The cloud provides reading and writing interactions with the consortium blockchain. If s_i has successfully traded with p_i, the encrypted electrical data requested by s_i and its corresponding hash value will be sent to the group of data sharing nodes. The encrypted electrical data can be decrypted accurately only if more than t members cooperate with one another. After decryption, the electrical data can be compared with the hash value recorded in the consortium blockchain to confirm the authenticity of the shared data.

Similarly, we simulated 100 times of prepaid payment transactions and account inquiry transactions in the blockchain network of our five smart devices. Figure 10 below describes the time cost.

As can be seen from Fig. 10, after 100 times of prepaid payment transactions simulation, the time cost tends to be stable, and the prepaid payment can be completed within two seconds to meet the actual demand. In addition, with the increase of ledger space, query time is also within the acceptable range.

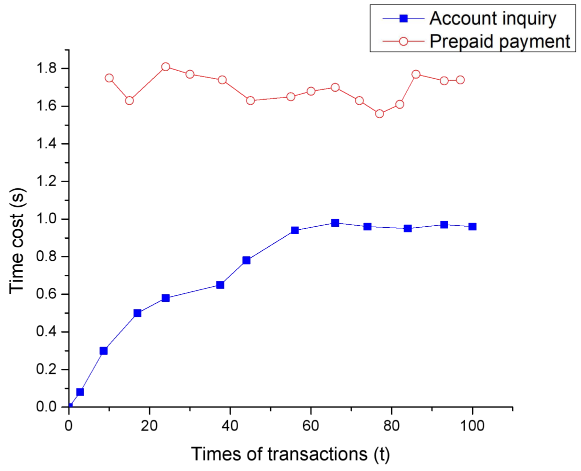

FIGURE 10. Time cost of prepaid payment transactions and account inquiry transactions.

VI. MECHANIEM COMPARISON AND SAFETY ANALSIS

In this section we discuss the security of proposed mechanism and compared it with the existing smart grid mechanism.

A. MECHANISM COMPARISON

Our scheme is established in the consortium blockchain. The hash storage of transaction information and electrical data is verified and cannot be tampered after being recorded in the consortium blockchain. Therefore, our blockchain based DMSM is tamper-proofing. The request node must first make a prepaid payment or the smart contract will not process the request. Unverifiable identifiers and signatures are discarded immediately after the request is made. Our scheme can effectively prevent malicious requests. This mechanism also has the function of preventing malicious requests effectively.

By making a user request, the user node can perform a data audit. Data auditing which refers to data users being able to check personal electricity usage details. Smart grids also have an obligation to explain the details of users' bills in detail, and should even provide users with safer and more scientific advice on electricity consumption. In addition, users can monitor the operation of smart devices by binding them to smart contracts to prevent accidents.

Data sharing node requests electrical data sharing and exposed to the whole network. Smart grid users are well aware of data sharing node requests and processing node responses. Transactions between data sharing nodes and processing nodes are also recorded in the consortium blockchain. Therefore, the data management in this paper is visual, users can clearly know where personal data and source.

TABLE 2. **Comparison between proposed mechanism and other related mechanisms.**

	[9]	[10]	[11]	[12]	DMSM
Blockchain-Based	N	N	Y	Y	Y
Tamperproof	N	N	Y	Y	Y
Prevent malicious requests	Y	Y	Y	Y	Y
Data auditing	N	N	N	N	Y
Electricity monitoring	N	N	N	N	Y
Data sharing	Y	Y	N	N	Y
Visual data management	N	N	N	Y	Y

B. SAFETY ANALYSIS

1) INTERACTIVE SAFETY

In this paper, the interaction between nodes uses Paillier encryption algorithm to encrypt the plaintext to be sent. When messages passed between nodes are intercepted, the attacker cannot infer any relevant information about the plaintext sent by the node. Only the opposing node with the decryption parameters can decrypt the message. In this way, the message confidentiality between nodes is guaranteed when they interact with each other.

Each node in the consortium blockchain has its own unique legal ID , and each node generates their own BLS short signature when information occurs on the chain. Because of the private key owned by different nodes, the different signature is generated. During node interaction, if the signature verification is not successful, the information interaction will be interrupted immediately.

2) BLOCKCHAIN NETWORK SAFETY

(1) No trusted center authority

With the support of blockchain technology, our scheme is carried out without a trusted authority. In the consortium blockchain, no third-party trusted central authority, and all nodes are involved in maintaining a tamper-proofing ledger. In the data sharing scheme, the processing nodes distribute the key randomly to the data sharing nodes and promise a verifiable result. The data sharing node can verify its own key. The whole process does not rely on a trusted third-party authority to make our solution more convenient and reliable.

(2) Node identity protection

All nodes in the consortium blockchain are authenticated and have a unique ID before registration, but the attacker cannot identify this ID . If the ID is intercepted by the attacker, the attacker cannot get any valid information from it. Only the processing nodes can recognize the ID of other nodes. In addition, the ID only represents the identity of the node but does not reveal any transaction information, running status or valid whereabouts of the node.

(3) Data security

The cloud holds encrypted electrical data and its hash value, while the consortium blockchain only keeps the transaction records and electrical data hash. The cloud has the right to read the transaction information in the blockchain, and only the data sharing node with a successful transaction is allowed to download the ciphertext, and cannot download the data beyond the permission. No data sharing node has complete decryption parameters and cannot decrypt the ciphertext alone until any t valid members have taken out their keys to calculate the decryption parameters. The hash value of electrical data can be compared with the record in blockchain or cloud to ensure the authenticity of the data.

(4) Malicious requests

In our scheme, both user nodes and data sharing nodes can make request transactions with identification. When they make the transaction, they use their legal ID and attach their unique BLS signature to the request. The attacker may make multiple malicious requests, resulting in network congestion and unresponsive nodes. However, we specify that the node request first needs to transfer the prepaid payment to the smart contract address, and then the ID and signature must be verified. If any of these links fail, the current request is immediately discarded. This greatly saves network resources and effectively avoids network congestion caused by malicious requests.

(5) Information cannot be falsified

The hash value of electrical data is stored in the cloud, it can be used to quickly match the corresponding data or to compare with the hash value stored in the blockchain to determine the authenticity of the data. The hash value stored in the consortium blockchain cannot be tampered with unless the attacker controls more than 50% of the bookkeeper nodes in the network.

VII. CONCLUSION

Smart grids are being more widely deployed, inevitably requiring intelligent services and multiplatform data sharing. This paper proposes the DMSM based on consortium blockchain. It realizes the monitoring of smart devices by users and the multiparty sharing of electrical data, and users can request a wide range of services from the smart grid. The whole process uses BLS short signature and Paillier encryption algorithm to ensure the confidentiality of node interaction. By connecting the smart contract to the smart device, users can view the running report of the smart device in the smart phone. The request transaction adopts the prepaid payment smart contract, in which the time-lock script guarantees consumer’s rights and interests of the requesting node within the specified time. Data sharing nodes and processing nodes are mutually selected each other to share data through the data sharing smart contract. Discussed has shown that, in comparison to existing related mechanism, our mechanism is more suitable for the application of smart grids in data monitoring and sharing. The security analysis has proven that our data monitoring and sharing mechanism meets the requirements of privacy protection and security management of smart grids.

REFERENCES

[1] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," *IEEE Access,* vol. 6, no. 99, pp. 9917-9925, Feb. 2018.

[2] M. Fan, and X. H. Zhang, "Consortium Blockchain Based Data Aggregation and Regulation Mechanism for Smart Grid," *IEEE Access*, vol. 7, pp. 35929-35940, Mar. 2019.

[3] P. Claudia, C. Tudor, A. Marcel, A. Ionut, S. Ioan, and B. Massimo, "Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids," *Sensors*, vol. 18, no. 1, pp. 162. Jan. 2018.

[4] T. Y. Zhang, H. Pota, C. C. Chu, and R. Gadh, "Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency," *Appl. Energ.*, vol. 226, pp. 582-594, Sep. 2018.

[5] M. Tome, P. Nardelli, and H. Alves, "Long-range Low-power Wireless Networks and Sampling Strategies in Electricity Metering," *IEEE Ind. Electron.*, vol. 66, no. 2, pp. 1629-1637, Feb. 2018.

[6] J. Beyea, "The Smart Electricity Grid and Scientific Research," *Science*, vol. 328, no. 5981, pp. 979-980, May. 2010.

[7] X. Jiang, M. Z. Liu , C. Yang, Y. H. Liu and R. L. Wang, "A Blockchain-Based Authentication Protocol for WLAN Mesh Security Access Scheme," *CMC-Comput Mater Con*, vol. 58, no. 1, Jan. 2019.

[8] M. M. Eissa, "Developing wide area phase plane primary protection scheme "WA4PS" for complex smart grid system," *Int. J. Elec. Power*, vol. 99, pp. 203-213, Jul. 2018.

[9] N. Shaukat, S. M. Ali, C. A. Mehmood, B. Khana, M. Jawadb, U. Farida, Z. Ullaha, S. M. Anwarc, and M. Majid, "A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid," *Renew. Sust. Energ. Rev.*, vol. 81, pp. 1453-1475, Jan. 2017.

[10] U. Ahsan and A. Bais, "Distributed Smart Home Architecture for Data Handling in Smart Grid," *CJElCE*, vol. 41, no. 1, pp. 17-27, Winter. 2018.

[11] S. Rusitschka, K. Eger, and C. Gerdes, "Smart Grid Data Cloud: A Model for Utilizing Cloud Computing in the Smart Grid Domain," in *Proc. IEEE SmartGridComm*, NIST, MD, USA, 2010, pp. 483-488.

[12] Z. T. Guan, G. L. Si, X. S. Zhang, L. F. Wu, N. Guizani, X. J. Du, and Y. L. Ma, "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp.82-88, Jul. 2018.

[13] X. H. Zhang, and M. Fan, "Blockchain Based Secure Equipment Diagnosis Mechanism of Smart Grid," *IEEE Access*, vol. 6, no. 99, pp. 66165-66177, Jul. 2018.

[14] A. Facchini, "Distributed energy resources: Planning for the future," *Nat. Energy*, vol. 2, pp. 17129, Jul. 2017.

[15] S. Nakamoto, (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*, [Online] Available https://bitcoin.org/bitcoin.pdf

[16] K. Saito, and H. Yamada, "What's So Different about Blockchain? -Blockchain is a Probabilistic State Machine," in *Proc. IEEE ICDCS*, Nara, Japan, 2016, pp. 168-175.

[17] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain or not blockchain: That is the Question," *IT Prof.*, vol. 20, no. 2, pp. 62-74, Mar. 2018.

[18] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing" in *Proc. ASIACRYPT*, Heidelberg, BER, GER, 2001, vol. 2248, pp. 514-532.

[19] D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Cryptology-CRYPTO*, Heidelberg, BER, GER, 2001, vol. 2139, pp. 213-229.

[20] F. Zhang, R. Safavinaini, and W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications," in *Proc. PKC*, Singapore, 2004, vol. 2947, no. 39, pp. 277-290.

[21] M. Bellare, and P. Rogaway, "The Exact Security of Digital Signatures: How to Sign with RSA and Rabin," in *Proc. EUROCRYPT*, Heidelberg, BER, GER, 1996, vol. 1070, pp. 339-416.

[22] R. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 2, pp. 96-99, 1978.

[23] B. K. Zheng, L. H. Zhu, M. Shen, F. Gao, C. Zhang, Y. D. Li, and J. Yang, "Scalable and Privacy-Preserving Data Sharing Based on Blockchain," *J. Comput. Sci. Technol.*, vol. 33, no. 3, pp. 557-567, May. 2018.

[24] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances Cryptology-Eurocrypt*, Prague, Czech Republic, 1999, vol. 547, no. 1, pp. 223-238.

[25] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612-613, 2011.

[26] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS*, 1979, New York, USA, 1979, pp. 313-317.

[27] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Proc. ASFCS*, 1987, pp.427-438.

[28] F. Tschorsch, and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Commun. Surv. Tut.*, vol. 18, no. 3, pp. 2084-2123, Third Quarter. 2016.

[29] Y. Yang, F. Chen, X. Zhang, J. Yu, and P. Zhang, "Research on the Hash Function Structures and its Application," *Wireless Pers. Commun.*, vol. 94, no. 4, pp. 2969-2985, Jun. 2016.

[30] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Fair Two-Party Computations via Bitcoin Deposits," in *Proc. 18th FC*, 2014, vol. 8438, pp. 105-121.

[31] L. Thomas, Y. Zhou, C. Long, J. Z. Wu, and N. Jenkins, "A general form of smart contract for decentralized energy systems management," *Nature Energy*, vol. 4, pp. 140-149, Jan. 2017.

YANHAN YANG received her B.Sc. in Measurement, Control Technology and Instrumentation from Sichuan University of Science and Engineering, Sichuan, China, in 2016. She is studying for her master's degree in Instrument, Meter Engineering, Chengdu University of Technology, Sichuan, China. Her research interests include blockchain encryption, smart contract, data privacy and smart grid.

MINGZHE LIU received his M.Sc. in Computer Science from Massey University, New Zealand, in 2006; as well as PhD in Computer Science from Massey University, New Zealand, in 2010. He is currently a Professor and the Head of College of Information Science and Technology, Chengdu University of Technology, China. His research interests include intelligent information processing, information security, and system control, etc.

QIN ZHOU received her B.Sc. in Building Electrical and Intelligent major from Hunan University of Arts and Science, Changde, China. She is studying for her master's degree in Instrument, Meter Engineering, Chengdu University of Technology, Sichuan, China. Her research interests include blockchain, cloud storage and data privacy.

HELEN ZHOU is currently a senior lecturer in Mechatronics at the School of Engineering, Manukau Institute of Technology, New Zealand. She received a Ph.D. in Computer Science from the School of Computer Science and Informatics, National University of Ireland, Dublin in 2005. Her main research interests include mobile and wireless GIS, Biomedical Engineering Systems and Applied Health Informatics.

RUILI WANG received the Ph.D. degree in computer science from Dublin City University, Dublin, Ireland. He is currently a Professor with the School of Natural and Computational Sciences, Massey University, Auckland, New Zealand, where he is the Director of the Centre of Language and Speech Processing. His current research interests include speed processing, language processing, image processing, data mining, and intelligent systems.