IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 3, 2019, accepted March 12, 2019, date of publication March 15, 2019, date of current version April 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2905298

Consortium Blockchain Based Data Aggregation and Regulation Mechanism for Smart Grid

MOCHAN FAN AND XIAOHONG ZHANG
School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, China
Corresponding author: Xiaohong Zhang (xiaohongzh@263.net)

This work was supported in part by the National Natural Science Foundation of China under Grant 61763017 and Grant 51665019, in part by the Scientific Research Plan Projects of the Jiangxi Education Department under Grant GJJ150621, in part by the Natural Science Foundation of Jiangxi Province under Grant 20161BAB202053 and Grant 20161BAB206145, and in part by the Innovation Fund for Graduate Students in Jiangxi Province under Grant YC2017-S302.

ABSTRACT Flexible regulation of smart grid is vital for grid operation. This paper proposes a smart grid data aggregation and regulation mechanism based on consortium blockchain, and its signcryption algorithm can be applied to multidimensional data acquisition and multiple receivers in the consortium blockchain. In the process of regulation, the control center, the grid operator, and the equipment supplier receive fixed-height blocks from the blockchain and obtain plaintext from the decryption. Each receiver analyzes the multidimensional data and formulates corresponding control policies for individual users. Grid operators implement user power regulation by feedback on smart contracts. The security analysis and performance comparison show that the proposed scheme has advantages in computing and communication costs while meeting security requirements for confidentiality and data integrity.

INDEX TERMS Consortium blockchain, smart contract, smart grid, signcryption.

I. INTRODUCTION

Blockchain is the underlying technology of the digital cryptocurrency system represented by Bitcoin. It isdecentralized, tamper-proof and permanent, and can achieve peer-to-peer transactions that are independent of any third party. Blockchain can implement trusted transactions in untrusted distributed systems through cryptographic algorithms, timestamps, and distributed consensus. Coordination among the nodes in the blockchain solves problems of high cost, low efficiency, and insecure data storage that are common in centralized organizations [1]. Legitimate data or transactions in the chain will be permanently recorded in the blockchain, and the Merkle root [2], [3] of the transaction can verify whether the transaction data in the block header and block has been tampered with. The hash value of the former block can be used to verify whether all blocks before the block and up to the Genesis block have been tampered with. Relying on the hash of the previous block, all blocks are interlinked. If any block is tampered, all subsequent block hash changes will be triggered. Therefore, the block and all previous blocks can be downloaded from an untrusted node, and verified whether any block has been modified [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Enamul Haque.

There is no current industry recognized blockchain definition, and various studies define blockchains from narrow and broad senses [1]. In a narrow sense, a blockchain is an untampered and unforgeable decentralized shared ledger that combines data blocks in a chronological manner into specific data structures cryptographically. It can safely store simple, sequential and verifiable data in the system. Generalized blockchain technology is a new decentralization framework and distributed computing paradigm that uses encrypted chain block structure to verify and store data, distributed node consensus algorithm to generate and update data, and automated scripting code (smart contract) to program and operate data. Blockchain has considerable potential economic, political, humanitarian, and legal benefits, because control transfers to participants rather than being centralized [5].

Smart grid are the next generation of power grids, integrating current information networks and information systems into the new grid system along with traditional energy networks, which offers better controllability and observability, and solves problems of low energy utilization rate, poor interaction, and difficulty of security and stability analysis of traditional power grids [6]. Currently, various smart terminals and smart meters have been widely used in smart grid. Users can have two-way interaction between the smart

meter and the power company, and can know their own power consumption and electricity prices in time. Depending on the user's electricity information, the power company makes corresponding distribution and real-time pricing adjustments [7], [8].

However, several challenges remain in current smart grid. Firstly, the user's power information may be stolen by attackers when it is transmitted to the control center (CC), which leads to the leakage of user's privacy information. Therefore, it is necessary to ensure the security of user's power data during transmission. Secondly, the data in power grid is stored and shared by reliable central nodes. This centralized data storage method faces security problems such as single point failure of the central node and malicious tampering of data. Therefore, it is urgent to design a safe and reliable decentralized data storage method. Finally, there are hundreds of millions of power equipments in the grid, which are difficult to supervise and require high real-time performance. Therefore, it is necessary to optimize the supervision mechanism of smart grid in order to improve management efficiency and operation cost.

In order to ensure the security of power data during communication, some researches have proposed aggregation schemes, including multidimensional [9], [10] and single-dimensional [11]–[15] data aggregation. These schemes all adopted the semantically secure Paillier encryption algorithm to decrypt the ciphertext and produce the corresponding plaintext. However, the computational cost of the Paillier algorithm is large, which increases the computational burden of the smart meter. Guan et al. [13] proposed a device-oriented anonymous privacy-protection scheme with authenticating data aggregation applications, which supports multi-authority to manage smart devices locally. Xue *et al.* [14] proposed a privacy-preserving service outsourcing scheme for real-time pricing demand response in smart grid with fault tolerance and flexible customer enrollment and revocation. Li *et al.* [15] proposed a multisubset aggregation scheme for smart grid, which can aggregate users' electricity data in different ranges, while guaranteeing the privacy of individual users. Guan *et al.* [16] proposed a data acquisition scheme based on ciphertext policy attribute encryption. The data is divided into blocks and encrypted with its corresponding access subtree in sequence to process data encryption and data transmission in parallel. Li *et al.* [17] proposed a smart grid prepayment system, which is operated by the trading market operated by the control center to respond to the dynamic needs of users. Almost all of the above schemes are centralized structures, so there is a security risk of single point of failure. These schemes are difficult to achieve accurate feedback, or the feedback function is too single.

Considering the characteristics of decentralization and distributed storage of blockchain, it can solve the problems of centralization and inaccurate feedback in traditional smart grid schemes. Nowadays, many studies [18]–[23] have applied blockchain to smart grid to solve the above challenges. Pop *et al.* [18] proposed a decentralized management model of demand response programs in smart energy grids. The model could be used to match energy demand and production at smart grid level. Gao *et al.* [19] proposed a grid monitoring model that allowed users to monitor power usage without requiring third-party management and achieve efficient operation of the grid system through smart contracts. Wu *et al.* [20] proposed a secure data storage and sharing system (DSCB) based on consortium blockchain in smart grid. The DSCB system solves the information security problems such as single point failure and deliberate tampering of data caused by centralized storage mode. However, it is too succinct to describe how the data is encrypted, and there is no reasonable overhead analysis. Liang *et al.* [21] designed a new, distributed blockchain-based protection framework to enhance the self-defensive capability of modern power systems against cyber-attacks. They presented a discussion on how blockchain technology can be used to enhance the robustness and security of the power grid. Aitzhan and Svetinovic [22] proposed a scheme to improve security and privacy of distributed energy transactions through multi-signature, blockchain, and anonymous message Streams. Guan *et al.* [23] presented a privacy-preserving and data aggregation scheme based on the blockchain to preserve user's privacy in smart grid. However, this scheme only studied single-dimensional data aggregation and users' power data is transmitted in plaintext form in groups, which has great security risks.

The above schemes solve the problems of the smart grid in varying degrees, but there are still many shortcomings. Distinct from the existing literature, this paper proposes a consortium blockchain based data aggregation and regulation mechanism for smart grid (CBSG). The primary contribution of the paper can be summarized as follows:

1) The CBSG establishes a flexible power data monitoring and management architecture, which solves the problems of low data aggregation efficiency, large computational complexity, and difficulty in accurate feedback, realizes the functions of key user monitoring, anti-stealing management and data repair.
2) The CBSG achieves accurate feedback to single users through smart contracts. The tamper-proof, transparent and permanent features of blockchain technology enable efficient and safe operation of smart grid.
3) We develop a novelty approach that can be applied to multidimensional data acquisition and multiple receivers.
4) We demonstrate that the CBSG meets the various security requirements for power aggregation and regulation. We also show the proposed algorithm can achieve significant advantages in terms of computation and communication overhead for multidimensional data and multi-receiver modes.

The remainder of this paper is organized as follows. Section II introduces blockchain concepts and signcryption algorithms, and Section III details the proposed design model.

Sections IV and V provide the multidimensional data aggregation algorithm and receiver feedback modules, respectively. Section VI evaluates the proposed scheme's security and performance, and Section VII concludes the paper.

II. BLOCKCHAIN AND ENCRYPTION ALGORITHMS

This section explains the blockchain and encryption algorithms employed in the proposed scheme. We describe the blockchain and its application in various fields, and introduce encryption algorithms to ensure safe operation.

A. BLOCKCHAIN

Blockchain technology originated from a digital currency called bitcoin proposed by Nakamoto [24]. Bitcoin enabled mutually distrusting nodes to pay directly without requiring authoritative third party management. Subsequently, Vitalik Buterin proposed the Ethereum blockchain [25]. In contrast to the Bitcoin blockchain, Ethereum's built-in digital currency was ether, and the Merkle tree used the Merkle Patricia tree [26]. When validating a new block, the Merkle Patricia tree does not need to recalculate the entire tree, but only needs to calculate the account state that has changed in the new block. Branches with no changes in status can be directly referenced. Ethereum also provided Turing complete programming language to write smart contracts [27], enabling smart contracts on the blockchain. Smart contracts are a series of rules written on the blockchain in the form of code. When triggered, the nodes in the chain automatically execute the contract at the same time. Before the preset gas is exhausted, no institution or individual can force it to terminate.

Blockchain has been applied to many fields, particularly for internet of things (IoT), helping IoT to evolve into the chain of things (CoT) [28]. Emergence of blockchain has brought consensus mechanism and distributed networks to IoT. Consensus mechanism solved the problem of how to coordinate between billions of devices and reinforces IoT security.

Currently, many studies have combined IoT with blockchain [29]–[32]. Dorri *et al.* [29] proposed a blockchain for IoT security and privacy, using a smart home as a representative case-study. Khan and Salah [30] considered major IoT security issues and discussed how blockchain could be a key enabler to solve many of these security problems. Christidis and Devetsikiotis [31] reviewed blockchains and smart contracts for IoT, and showed that the blockchain-IoT combination was powerful and could enable significant transformations across several industries, paving the way for new business models and distributed applications. Sharma *et al.* [32] proposed a blockchain based distributed cloud architecture with software defined networking (SDN) enabled controller fog nodes at the edge of the network to meet the required design principles. Based on the decentralized nature of distributed ledgers, blockchain facilitates security and decentralization of transactions among multiple parties in the IoT.

Previous studies have also considered blockchain topics in many other fields. Dagher *et al.* [33] proposed a privacy preserving framework for access control and interoperability of electronic health records and Xia *et al.* [34] enabled trustless medical data sharing among cloud service providers using blockchain. Chen [35] proposed a Takagi-Sugeno fuzzy cognitive map artificial neural network as a traceability chain algorithm. A numerical example of the proposed algorithm in blockchain mining was evaluated and an optimized decisions experiment analyzed. Huang *et al.* [36] presented a security model for electric vehicle and charging pile management based on a blockchain ecosystem.

The various studies of blockchain applications have established that blockchain promotes transparency and efficiency in multi-party transactions, enhances security and mutual trust, and reduces fraud. The proposed scheme includes a large number of smart meters, with a limited number of nodes capable of data aggregation and analysis. Thus, it is inappropriate to adopt a private blockchain with only one node for consensus or a public blockchain where any node can participate in the consensus. Therefore, we applied the consortium blockchain for smart grid power aggregation and regulation.

B. BILINEAR PAIRING

Consider cyclic additive groups G_1 and G_2 with big prime order q, and P as the G_1 generator. Let there be a non-degenerate and efficient computability bilinear mapping [37], [38] $e : G_1 \times G_1 \rightarrow G_2$ with the following properties.

- Bilinearity: $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$ for all $P_1, P_2 \in G_1, a, b \in Z_q^*$.
- Non-degeneracy: for all $P_1, P_2 \in G_1, e(P_1, P_2) \neq 1$.
- Computability: the bilinear pair function $e(P_1, P_2)$ is computable with an efficient algorithm for all $P_1, P_2 \in G_1$.

C. HYBRID SIGNCRYPTION SCHEME

The hybrid signcryption scheme comprises four algorithms: system parameters setup (Setup), key generation (KeyGen), hybrid signcryption (Hsign), and non-hybrid signcryption (UnHSign). The concept model for the anonymous hybrid signcryption scheme with multi-receiver (multi-message) based on identity [39] is as follows.

- Initialization: Select security parameter k; calculate the corresponding system public parameter, *Params*, and master key, x; keep x secret and expose *Params* public. We can express this as $(Params, x) \leftarrow Setup(1^k)$.
- KeyGen: Enter the user identity, *ID*, and output the public and private keys (PK_{ID}, SK_{ID}) corresponding to *ID*. We can express this as $(PK_{ID}, SK_{ID}) \leftarrow KeyGen(Params, ID, x)$.
- Hsign: Enter the message, M, to be encrypted; sender identity, $ID_S = \{S_1, S_2, \ldots, S_n\} (i = 1, 2, \ldots n$, and receiver identity set, $ID_R = \{R_1, R_2, \ldots, R_m\} (j = 1, 2, \ldots, m$; and output the corresponding signcryption

ciphertext, δ. We can express this as $\delta \leftarrow HSign(Params, M, ID_S, ID_R)$.

- UnHSign. Enter δ; receiver's identity, $R_j, j = 1, 2, \ldots, m$ and its private key x_{R_j}; and output the corresponding plaintext, M. We can express this as $M \leftarrow UnHSign(Params, \delta, R_j, x_{R_j})$.

III. PROPOSED DESIGN MODEL

This section describes the overall structure of the proposed CBSG and explains the various entities. CBSG uses the consortium blockchain to construct a multidimensional data aggregation and regulation mechanism for smart grid, as shown in Figure. 1. The mechanism can aggregate multidimensional data and send it to multiple receivers simultaneously, and consists of a consortium blockchain, smart meter, multi-receiver, etc. Detailed descriptions of each entity are provided below.

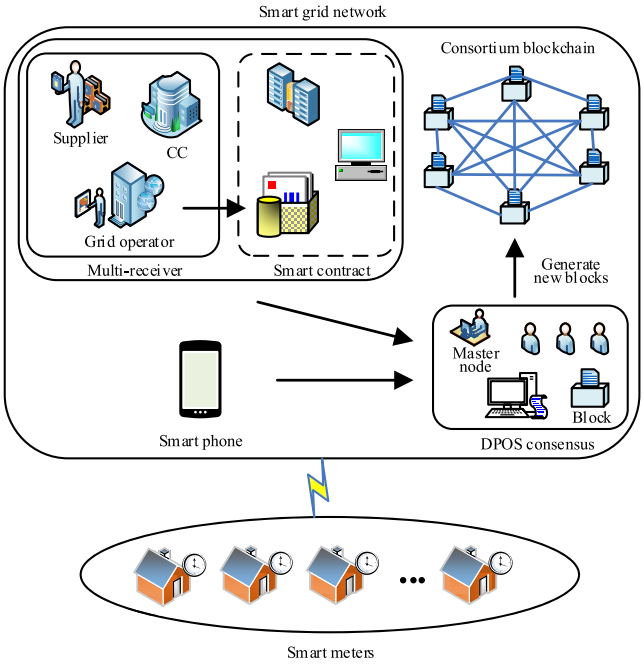

FIGURE 1. CBSG system model.

A. CONSORTIUM BLOCKCHAIN

We adopt the consortium blockchain for CBSG, where only pre-selected nodes can participate in consensus and generate blocks, i.e., not all nodes participate in consensus. This greatly reduces communication overhead and network load. When the accounting node views the data to be validated during its accounting period, it packages them and adds them to the newly generated block. Once the data is verified, it will be permanently stored in the blockchain and can be queried. Pre-selecting nodes with appropriate qualifications (better hardware, better operating environment) and using them to verify data and generate blocks improves system execution efficiency and ensure system security.

B. DELEGATED PROOF OF STAKE CONSENSUS MECHANISM

The consortium blockchain proposed for CBSG uses the delegated proof of stake (DPOS) [40] consensus mechanism to complete verification and recording of information. First, 101 accounting nodes were pre-selected according to their qualifications. These accounting nodes take turns to act as the master node for accounting. When data aggregation and regulation are released in the consortium blockchain, the current master node packages and generates new blocks. The accounting node can also record the user's fine-grained ciphertext in the blockchain, which is convenient for the single-user regulation of the receivers. When a new block is generated, the current accounting node must verify that the previous master node has successfully generated the block. If any accounting node misses the corresponding blocks, they are removed from the list of accounting nodes. In CBSG, users can post and query information on the blockchain, but do not participate in consensus or accounting.

C. SMART METER

Smart meters are installed on the user side for multidimensional data collection, such as user power consumption and real time monitoring information (e.g. temperature and humidity). When a smart meter is produced, a unique identity ID is registered in the blockchain, and the meter and data receiver are registered in the blockchain when they are used. Smart meters send multidimensional data to the nearest pre-selected accounting node, which may change in each round. This scheme eliminates the building area network gateway (BG) and the wide area network gateway (WG) and reduces system communication overhead. The smart meter realizes flexible power regulation by executing the feedback smart contract set by the receiver and the user's mobile phone.

D. SMART CONTRACT

After the grid operator decrypts and analyses the multidimensional data received, it develops corresponding feedback policies for each user. We implement policy feedback using smart contracts. Users can also set up smart contracts to control devices in real time. The appropriate smart contract is executed automatically when the trigger condition is reached. Each user adjusts the operation of their equipment according to the smart contract to realize efficient equipment operation. The feedback smart contract is designed specifically for each user by the receiver, reducing the network burden for the smart grid system and improving execution efficiency.

E. MULTI-RECEIVER

The proposed CBSG signcryption algorithm can be applied to the multi-receiver system model. Multiple receivers considered include CC, grid operators, equipment suppliers, etc. Each receiver obtains corresponding data from the multidimensional data, and the receiver analyzes the obtained data and formulates corresponding feedback smart contracts for

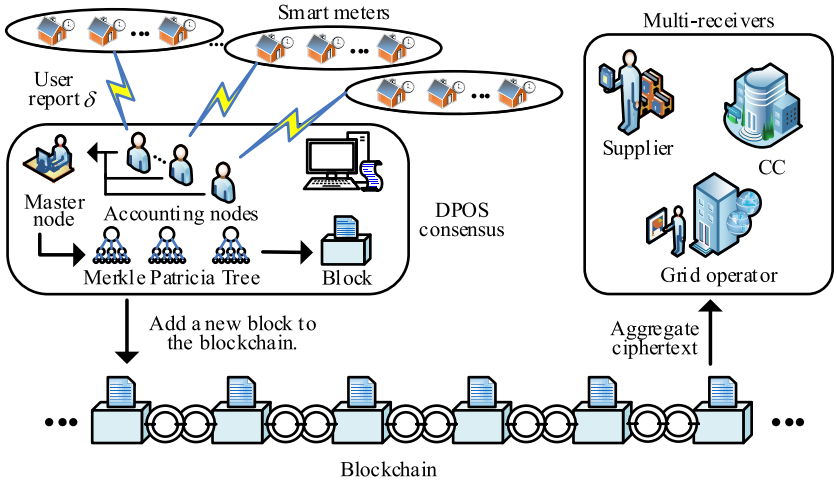

FIGURE 2. Smart grid data aggregation architecture.

each user. After receiving the smart contract, the smart meter adjusts power consumption according to the contract and reports the contract change to the user's mobile phone.

1) THE CC

The CC uses blockchain's permanent and tamper-proof to realize recording, management, and storage of power data. Implementation of this function only needs to construct the corresponding management smart contract without human intervention, avoiding errors caused by human operation and human tampering with data, and improving efficiency and security of data management and query. By analyzing the multidimensional data, the CC can realize key user monitoring, anti-theft management, and data recovery. When the user is suspected of illegal behavior, the CC can cooperate with the grid operator to manage the user accordingly. When the equipment supplier stops providing equipment maintenance services, equipment is monitored and repaired by the CC. The CC is also responsible for initializing the signcryption algorithm, generating partial private keys for receivers, such as smart meters and grid operators.

2) THE GRID OPERATOR

The grid operator is mainly responsible for transmission, distribution, and sales of electricity in their region. Regardless of fluctuations in power producers and demand, grid operators need to ensure real time matching between production and demand. The grid operator obtains user power consumption data in real time and uses a smart contract that can be triggered automatically for feedback. This reduces pressure on the grid due to electrical load during peak hours, and improves reliability and service level of the power supply.

3) THE EQUIPMENT SUPPLIER

The equipment supplier obtains equipment operation data from the multidimensional data, and achieves real-time equipment monitoring and prediction by analyzing the equipment operational state. When the equipment fails, the supplier can quickly identify the fault point to achieve efficient maintenance. This will improve the utilization rate of power grid equipment, ensuring secure and economic operation of the power grid, and reducing and delaying investment in power grid construction.

F. THE SMART PHONE

When the smart meter receives the feedback smart contract, it sends feedback policy messages to the user's smart phone. Users can obtain real time information regarding power supply capacity, power quality, price, and blackouts, and arrange use of their electrical appliances accordingly. Users can also set operational policy smart contracts for each power device through the smart contract client on the smart phone. The smart meter will also optimize current power usage according to the smart contract set by the user.

IV. DATA AGGREGATION

This paper proposes a smart grid data aggregation and regulation mechanism based on consortium blockchain. Figure 2 shows the basic design architecture.

A. INITIALIZATION

The initialization algorithm is executed by the CC with specific operations as follows.

1. Consider cyclic group G_1 and G_2 with big prime order q, and P as the G_1 generator. Given a bilinear pairing, let $Enc(K, \cdot)$ and $Dec(K, \cdot)$ be symmetric encryption and decryption algorithms, respectively, with key space κ. Define 4 secure hash functions: $H_1, H_2 : \{0,1\}^* \rightarrow Z_q^*$, $H_3 : \{0,1\}^* \rightarrow G_1$, and $H_4 : G_1 \times G_2 \rightarrow \kappa$, where $\{0,1\}^*$ represents a set of bit strings of arbitrary length.

2. Define the index function $f_{Index} : ID \rightarrow Z_q^*$ that maps ID to Z_q^*. The f_{Index} enables receivers, such as CC, grid operators,

and equipment suppliers, to accurately locate corresponding ciphertext from the ciphertext set, i.e., a subscript of the $f_{Index}(ID)$ generation parameter.

3. Select the master key, $x \in Z_q^*$; randomly; calculate the system public key, $Y_{Pub} = xP$; and publish the system parameters $\{P, q, G_1, G_2, e, Y_{Pub}, H_1, H_2, H_3, H_4, f_{Index}, Enc, Dec\}$.

B. KEY GENERATION

Suppose there are n users in the entire area; m receivers, including CC; S_i users in the area, $i = 1, 2, \ldots n$; and R_j user data receivers, $j = 1, 2, \ldots, m$. The process of generating each entity key is as follows.

1) PARTIAL PRIVATE KEY EXTRACTION

When a new smart meter is produced, a unique identity, ID, is registered in the consortium blockchain. As soon as they are used, the meter and receiver register in the consortium blockchain accordingly. Grid operators and suppliers also register their IDs in the consortium blockchain, and any private information such as user and receiver locations cannot be checked by ID. The CC checks all smart meters and receivers IDs in the blockchain, and calculates the partial private keys for S_i and R_j after verification.

- Select a random number, $r_i \in Z_q^*$; calculate $\alpha_i = r_i P$, $\eta_i = H_1(ID_{Si} \parallel \alpha_i)$, $h_i = r_i + \eta_i x$; and send partical private key h_i secretly to S_i, α_i as part of the S_i public key.
- Select a random number $r_j \in Z_q^*$; calculate $\alpha_j = r_j P$, $\eta_j = H_1(ID_{Rj} \parallel \alpha_j)$, $h_j = r_j + \eta_j x$; and send h_j secret to R_j, α_j as part of the R_j public key.

2) USERS, RECEIVERS KEY GENERATION

The S_i and R_j, other than the CC, randomly select $x_{Si}, x_{Rj} \in Z_q^*$ as a secret value, respectively, with corresponding private keys (h_i, x_{Si}) and (h_j, x_{Rj}). Calculate $Y_{S_i} = x_{Si} P$, $Y_{Rj} = x_{Rj} P$, and use (Y_{S_i}, α_i) and (Y_{R_j}, α_j) as public keys and publish them in the consortium blockchain.

C. DATA SIGNCRYPTION

Let the multidimensional smart meter data $M = \{M_1, \ldots, M_v\}$ be the data set to be encrypted, with data dimension v; $ID_{Si} = \{ID_{S1}, ID_{S2}, \ldots, ID_{Sn}\}$ be the set of smart meter identity, and $ID_{Rj} = \{ID_{R1}, ID_{R2}, \ldots, ID_{Rm}\}$ be the receiver's identity set. The specific signcryption operation is as follows.

1. Knowing the identity set of smart meter, a secret random number, $d \in Z_q^*$, is chosen to calculate $D = dP$. After calculation, d is erased safely.
2. For each receiver R_j, $j = 1, 2, \ldots, m$, after calculating the index $J_{Rj} = f_{Index}(R_j)$, we calculate $U_{J_{Rj}} = e(dY_{Pub}, Y_{Rj})$ separately, and the data encapsulation key $K_{J_{Rj}} = H_4(U_{J_{Rj}}, D)$.

The ciphertext $\omega_{J_{Rj}} = Enc(K_{J_{Rj}}, M_{J_{Rj}})$ is calculated and the ciphertext set $\omega = \{\omega_{J_{R1}}, \ldots, \omega_{J_{Rm}}\}$ is generated. In order to reduce the computational overhead, we adopt the aggregate signature scheme proposed in [41]. The signature algorithm goes as follows.

- Compute $\beta_i = H_2(\omega \parallel ID_{Si} \parallel Y_{S_i} \parallel \alpha_i \parallel Y_{Pub} \parallel D)$ and $Q = H_3(Y_{Pub})$.
- Select random number w_i and calculate $W_i = w_i P$.
- Calculate $T_i = (\beta_i x_{S_i} + h_i + w_i)Q$ and use $\sigma_i = (T_i, W_i)$ as the signature of S_i for ciphertext ω.
- Finally, package the ciphertext and signature into the user report

$$\delta = \langle \omega \parallel ID_{Si} \parallel mID_{Rj} \parallel T_t \parallel D \parallel \sigma_i \rangle, \tag{1}$$

which are sent to the nearest pre-selected accounting node, where T_t is the current timestamp to prevent replay attack.

D. VERIFY CIPHERTEXT LEGALITY

After receiving the user report, each pre-selected accounting node first performs aggregation signature verification on the user report. Accept that the multidimensional data has not been tampered or forged if and only if

$$\begin{cases} T = \sum_{i=1}^{n} T_i \\ W = \sum_{i=1}^{n} W_i \\ e(P, T) = e(Q, \sum_{i=1}^{n} (\beta_i Y_{si} + \alpha_i + \eta_i Y_{Pub}) + W) \end{cases}. \tag{2}$$

At the same time, Equation (2) also verifies the validity of the key parameter D. Each pre-selected accounting node locates the ciphertext $\omega_{J_{Rj}}$ accurately from the user ciphertext set by ciphertext index J_{Rj}. The ciphertext is classified and summated according to the different receivers. The master node record the aggregation message and D into the new block. The new block is broadcast and each node adds it to the respective blockchain.

E. DATA RECOVERY

The receiver queries the blocks with the height L in the blockchain, and obtains the aggregate data and D of each accounting node. Verify that T_t matches the timestamp encapsulated by the block header.

After the cc calculates $U_{J_{CC}} = e(DY_{Pub}, x)$ and $K_{J_{CC}} = H_4(U_{J_{CC}}, D)$, the aggregation ciphertext is decrypted $M_{J_{CC}} = Dec(K_{J_{CC}}, \omega_{J_{CC}})$, and then the corresponding user power data is obtained. Data recovery of the grid operators and suppliers are the same as CC, and are not be repeated here.

This scheme uses the consortium blockchain and the hybrid signcryption algorithm to realize multidimensional data aggregation and send it to multi-receivers. the aggregation method of classification summation enables each receiver to directly locate the information sent to itself in the multidimensional data. it promotes efficient analysis of user power data by each receiver, and realizes flexible power regulation.

V. DATA MONITORING

This section describes the processing after each receiver decrypts the data. After receiving blocks with height L in the consortium blockchain, the receivers use their private keys to decrypt the corresponding data, analyze them, and use the smart contract to generate power control policies for each user. After the receivers release the smart contract in the consortium blockchain, the current master node packages the contracts and adds them to the new block.

A. CENTRAL CONTROL DATA MANAGEMENT

In CBSG, the CC manages power data storage, and has anti-theft functions. Users of stolen electricity are mainly high voltage users with large electrical consumption. To identify illegal users with high supply and low meters and high supply and high counts, three phase voltage and current are obtained from ciphertext for pretreatment and dimension reduction, and then voltage and current scatter plots are constructed. Then the CC adds them to the list of suspected power theft. In subsequent data acquisition and processing, users in the candidate list are emphatically analyzed to realize key monitoring of power theft. In the event of an illegal act, the CC may cooperate with the grid operator to take additional disciplinary measures against the user.

After the CC completes data processing, the packet is encrypted and published to the consortium blockchain, as shown in Figure. 3. The current master node in the chain encapsulates the viewed packets and adds them to the newly generated block. Prior to this, the current master node must verify that the previous block was successfully generated. Once a message has been added to the blockchain, it cannot be tampered with and is permanent. When unscheduled smart meter outage causes data disorder or omission, the data can be recovered by the CC to ensure normal operation of the smart grid. When equipment passes its warranty period, operation monitoring and diagnosis is realized by CC.

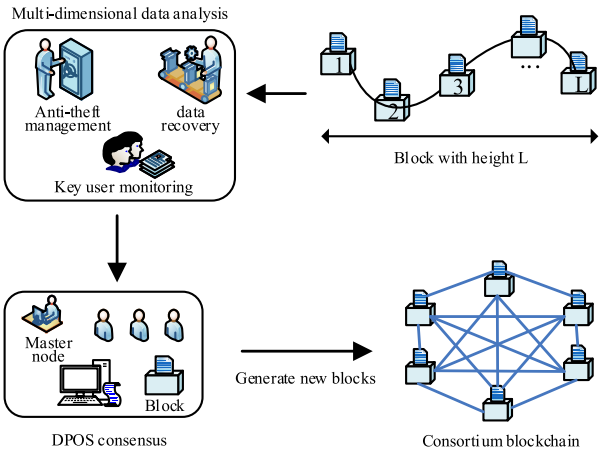

FIGURE 3. CC logic structure diagram.

B. GRID OPERATOR SMART CONTRACT

The grid operator decrypts the aggregated data to obtain the user's power consumption, and analyzes it to ensure that power supply matches power consumption in the area. Real time analysis of power consumption data enables the problem of excessive power load during peak periods to be solved.

The grid operator develops a feedback smart contract for each user, which regulates their electricity consumption and payment, as shown in algorithm 1. When decrypting the user's electricity data, the grid operator first checks whether the data has been tampered with, and generates an alarm on the smart meter side if it has been tampered. When user power consumption exceeds the preset threshold, the smart meter transforms into power saving mode. When the power data is conventional value, each appliance operates as usual. In the payment function, grid operators check user remaining electricity charges and execute corresponding smart contracts. When prepayment is insufficient or in arrears, the smart meter triggers the smart contract, sending a message to the user's smart phone to inform the user to pay the electricity bill. When the user is seriously in arrears, the smart meter will

Algorithm 1 The Grid Operator Smart Contract

```
Contract GridOperatorFeedback {
  public meter_value; threshold_value; electricity_bill;
    abnormality; normality; meter_prepaid; lack; arrears;
    serious arrears;
  address public GridOperator;
  address public meter;
  function consumption() {
  case meter_value of
  case1: meter_value == abnormality
  Output "meter || GridOperator || Data has been tampered
with, please re-upload";
  case2: meter_value >= threshold_value
  Output "meter || GridOperator || Excessive power con-
sumption, transfer to power saving mode";
  Case3: meter_value == normality
  Output "meter || GridOperator || Smart meter runs as
usual";
  end case }
  function cost() {
  if meter_prepaid == lack then
  Output "meter || GridOperator || Insufficient prepay-
ment, notify users to pay electricity bills";
  else if electricity_bill == arrears then
  Output "meter || GridOperator || Please pay the electric-
ity fee";
  else if electricity_bill == serious arrears then
  Output "meter || GridOperator || Forced trip";
  else{Report the latest electricity price;}}
  end if
  }
}
```

trip to force the user to pay the electricity bill. The feedback smart contract also informs the user of the latest electricity price in time, so the user can adjust power usage themselves.

C. EQUIPMENT SUPPLIER

The equipment supplier obtains information, such as equipment operating status data and fault reports, from the consortium blockchain. They determine factors that have the greatest impact on safe operation by analyzing the different equipment operating states, and then targeted measures are taken. The proposed CBSG scheme realizes real time equipment monitoring and prediction to ensure the safe operation, dividing the equipment operating state into normal, alarm, emergency, outage, and repair states, as shown in Figure. 4.

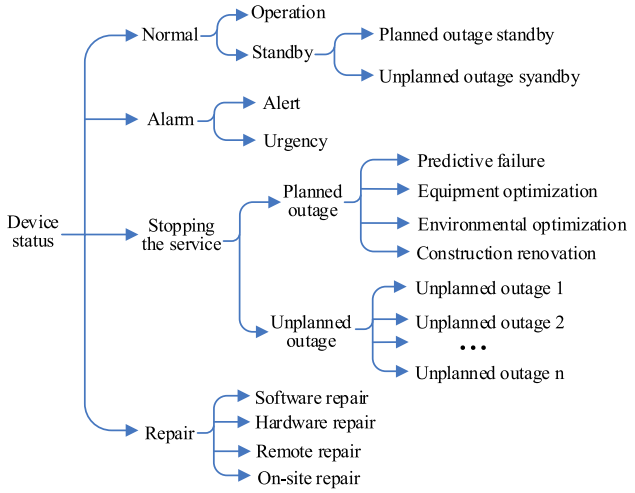

FIGURE 4. Device status classification.

When a fault occurs, the power equipment timely reports fault information to the supplier, including equipment *ID*, fault location, fault type, event number, fault time, etc., which is helps to guide technical personnel to correctly assess the required maintenance mode. For example, software upgrades, etc., can be remotely maintained within the consortium blockchain, thus eliminating geographical restrictions and saving equipment repair time; whereas in the case of hardware failure, etc., engineers can accurately locate the fault for on-site maintenance, and check the problematic part in a targeted manner, rather than relying on speculation and experience. This will significantly reduce equipment management and maintenance costs, improving energy efficiency.

The supplier also needs to summarize power equipment operating status, particularly alarm and unplanned outage status. The equipment supplier through the statistical analysis of alarm conditions, outage frequency, outage time, and failure percentage for each device, ultimately providing reliable equipment failure prediction. After analyzing and processing equipment status and fault data, the supplier node publishes the information in ciphertext in the consortium blockchain, which is verified by the current master node and added to the new block.

VI. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

This section analyzes CBSG security compared with the four schemes described above [9]–[12].

A. SECURITY ANALYSIS

Property 1: In the signcryption process, private key exchange is not performed between the user and the receiver, and the receivers can calculate the decryption key using their private key, i.e.,

Proof:

$$\begin{aligned} e(DY_{Pub}, x_{Rj}) &= e(dPY_{Pub}, x_{Rj}) \\ &= e(dY_{Pub}, x_{Rj}P) \\ &= e(dY_{Pub}, Y_{Rj}), \end{aligned} \tag{3}$$

hence

$$U_{J_{Rj}} = e(dY_{Pub}, Y_{Rj}) = e(DY_{Pub}, x_{Rj}), \tag{4}$$

and the receiver can calculate the data encapsulation key, $K_{J_{Rj}} = H_4(U_{J_{Rj}}, D)$, correctly.

Property 2: The aggregate signature verification process is correct.

Proof:

$$\begin{aligned} e(P, T) &= e(P, \sum_{i=1}^{n} T_i) \\ &= e(P, \sum_{i=1}^{n} (\beta_i x_{s_i} + h_i + w_i)Q) \\ &= e(Q, \sum_{i=1}^{n} (\beta_i x_{s_i} + (r_i + \eta_i x) + w_i)P) \\ &= e(Q, \sum_{i=1}^{n} (\beta_i x_{s_i} P + \alpha_i + \eta_i xP + w_i P) \\ &= e(Q, \sum_{i=1}^{n} (\beta_i Y_{s_i} + \alpha_i + \eta_i Y_{Pub}) + W), \end{aligned} \tag{5}$$

hence $e(P, T) = e(Q, \sum_{i=1}^{n} (\beta_i Y_{s_i} + \alpha_i + \eta_i Y_{Pub}) + W)$, the verificati-onon process is correct.

Property 3: The proposed scheme provides confidentialit-y of the data from smart meters to the receivers.

Proof: An attacker could monitor the communication channel, but each user calculates the ciphertext index $J_{Rj} = f_{Index}(R_j)$ and the corresponding data encapsulation key $K_{J_{Rj}} = H_4(U_{J_{Rj}}, D)$ for each receiver before publishing the multidimensional data, so the data transmitted in the channel is the encrypted ciphertext set $\omega = \{\omega_{J_{R1}}, \ldots, \omega_{J_{Rm}}\}$. The $K_{J_{Rj}}$ is calculated by a hash function with unidirectional, anti-collision and avalanche effects. It is not feasible for an attacker to calculate $K_{J_{Rj}}$ without knowing $(U_{J_{Rj}}, D)$.

In the process of multidimensional data aggregation, key transmission is not required. Even if the attacker intercepts the ciphertext, the corresponding plaintext cannot be

decrypted. At the same time, the aggregated data records in the consortium blockchain can guarantee the confidentiality of the data.

Property 4: The proposed scheme provides aggregation data integrity.

Proof: This scheme is based on the consortium blockchain, where the data of each node is recorded by the current master node in the untamable and permanent blockchain. Therefore, once a new block is generated, integrity of the data it contains can be guaranteed. Blockchain has the characteristics of decentralization and distributed storage. It is almost impossible for a malicious node to tamper with data only if it successfully attacks 51% of the legitimate nodes.

At the same time, we employ the signature algorithm based on the computational Diffie-Hellman (CDH) problem [42] to sign the data when publishing multidimensional data. When the equation $e(P,T) = e(Q, \sum_{i=1}^{n} (\beta_i Y_{s_i} + \alpha_i + \eta_i Y_{Pub}) + W)$ is established, signature verification is effective, that is, data is not tampered with during transmission, which resists forgery attacks and ensures data integrity in transmission.

Property 5: The proposed scheme provides non-repudiation of data aggregation and regulation.

Proof: According to [41], in random oracle mode, the probability ε' that challenger can successfully solve CDH problem by attacker is $\varepsilon' \geq \varepsilon(1-(q_E/q_E+1)^n)(q_E/q_E+1)^{q_E+q_s}$, ε is the probability that attacker can forge signature successfully, q_E and q_s are the times of executing part of private key inquiry and signature inquiry respectively. Therefore, the signature is unforgeable, which ensures the non-repudiation of the aggregated data.

When each node publishes information in the consortium blockchain and performs bidirectional interaction with its unique *ID*, the receiver can only obtain power consumption data corresponding to that *ID*, and user privacy information corresponding to the *ID* is unknown. Once the interaction information is recorded in the consortium blockchain, it cannot be changed. The node can check the previous interaction information through the merkle tree, so the scheme is non-repudiational.

B. PERFORMANCE ANALYSIS

The CBSG signcryption mechanism collects multidimensional data and sends it to multiple receivers that individually decrypt the ciphertext index to obtain the corresponding plaintext. The CC, power grid operators, and equipment suppliers process the multidimensional data to realize intelligent control of the smart grid. The CC can realize anti-theft management, key user monitoring, and data recovery by analyzing the user data, and record the processed data in the consortium blockchain to realize efficient management of power data. The blockchain is permanent, hence data is permanently stored in the blockchain. Grid operators formulate feedback smart contracts depending on user's analyzed power consumption data. Through smart contracts, power control for individual user is realized. Equipment suppliers monitor operational status to ensure normal operation of power equipment, saving network construction costs.

Table 1 compares the proposed CBSG scheme functionality with common schemes proposed in previous studies. The CBSG scheme offers significant advantages over all the current schemes.

TABLE 1. Functionality for the proposed CBSG and comparison schemes.

Functionality \ Ref.	[9]	[10]	[11]	[12]	CBSG
Confidentiality	Y	Y	Y	Y	Y
Data integrity	Y	Y	Y	Y	Y
Multi-dimensional data	Y	Y	N	N	Y
Multi-receiver	N	N	N	N	Y
Efficient data management	N	N	N	N	Y
Single-user feedback	Y	Y	N	N	Y
Data permanence	N	N	N	N	Y

Compared with traditional schemes, CBGS can aggregate multidimensional data and send it to multiple receivers at the same time. This scheme uses blockchain to achieve multi-receiver. Each receiver designs different smart grid management policies by using smart contracts, realizes user precise feedback, key user monitoring and other functions, and ensures the real-time performance of the grid, thus realizing decentralized and flexible monitoring of the grid. Further more, storage of power data and regulation policies through blockchain ensures that these data can be permanently stored and tampered-proof.

C. COMPUTATION OVERHEAD

Current smart grid data collection systems mostly adopt first (BG) and second (WG) level gateway aggregation. Table 2 compares computational overhead between CBSG and the four aggregation schemes described above. Multiple receivers, such as the CC, grid operator, and suppliers, are uniformly represented by CC. For convenience, C_p denotes bilinear pairings, C_m denotes multiplication on G_1, C_{eZ} is an exponent operation on $Z_{N^2}^*$, and C_{eT} is an exponential operation on G_2. Experiments were performed with the cpabe-0.10 [43] library on a 3.0 GHz processor and a 2 GB memory machine. These four operations consume 12.1, 0.7, 6.8, and 2.9 ms, respectively [10].

Since the computing power and storage capacity of smart meters are limited, we assume that the meter can collect 10 data types. The multidimensional data of the user in this scheme is summed by each pre-selected accounting node and recorded in the blockchain by master node. The receivers obtain data with height L from the blockchain, eliminating multi-level gateway aggregation. In Table 2, we combine the computation cost of signature verification with the computation cost of CC. Computational overhead for the multiplication operation on $Z_{N^2}^*$ is negligible compared with

TABLE 2. Computational costs for the proposed CBSG and comparison schemes.

Ref.	User	BG	WG	CC
[9]	$(v+1)C_{eZ}+2C_m$	$2C_p+C_{eZ}+2C_m$	$2C_p+2C_m$	$2C_p+3(l-1)C_m$
[10]	$2C_m+(v+1)C_{eZ}$ $+2C_p+2C_{eT}$	$5C_p+2C_m$	—	$\lvert f_{Index}\rvert C_m+C_{eZ}$
[11]	$2C_p+2C_{eZ}+C_m$	$(n+4)C_p+C_m$	$(t+5)C_p+2C_m$	$2C_p+lC_{eZ}+$ $C_{eT}+3C_m$
[12]	$2C_m+2C_{eZ}$	$3t+2C_m$	—	$3C_p+C_{eT}$
CBSG	C_p+2C_m	—	—	$3C_p$

exponential and bilinear pair operations on $Z_{N^2}^*$; multiplication negligible compared with exponential on G_2; and bilinear pairing, exponential operation, and decrypting the total power consumption of gateways at all levels can be neglected.

Since CBSG can achieve multidimensional data aggregation, whereas schemes [11], [12] only aggregate one-dimensional data, we only compare computational costs for [9] and [10]. Figures 5 and 6 compare computational cost to aggregate multidimensional data, and total amount of BG-WG-CC computations, respectively.

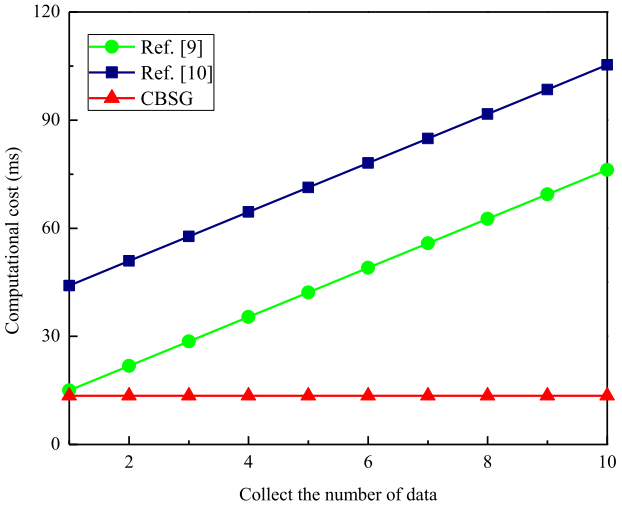

FIGURE 5. Calculational cost comparison at users.

Computational overhead for schemes [9], [10] increase linearly with increasing number of data types collected. However, [9] only studied data from User-CC aggregation, and CC-User feedback was not considered. CBSG user calculation overhead was constant, i.e., it does not increase with increasing number of data types collected. Thus, overall computational overhead for CBSG was significantly less than other schemes. Although [11] and [12] only aggregate one-dimensional data, v-dimensional data can be aggregated by v repeats, but this is computationally expensive and unsuitable for multidimensional data aggregation with smart grid.

Computational overhead of [9] increased linearly with increasing number of BGs (Fig. 6), indicating no advantage compared with CBSG. CBSG computational complexity

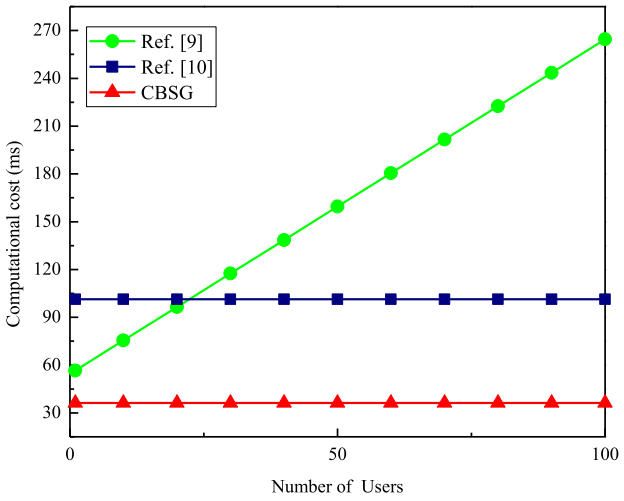

FIGURE 6. Comparison of remaining calculation costs.

does not increase with increasing users, which also make the scheme advantageous for practical applications. Although [10] also satisfies this characteristic, its computational cost for BG and CC is larger than for CBSG. Thus, CBSG advantages increase with increasing number of users.

D. COMMUNICATION OVERHEAD

This section analyzes communication overhead between users and receivers of the proposed CBSG and compares it with the [9] and [10] schemes, as shown in Table 3. Since [9] has a secondary gateway, its communication overhead includes: User-to-BG, BG-to-WG, and WG-to-CC; and [10] includes: User-to-BG and BG-to-CC.

TABLE 3. Communication overheads for the proposed CBSG and comparison schemes.

Ref. [9]	
User-to-BG	$\lvert\delta_{11}\rvert = n(\lvert\omega_{ijk}\rvert + 2\lvert ID\rvert + \lvert T_t\rvert + \lvert G_1\rvert)$
BG-to-WG	$\lvert\delta_{12}\rvert = t(\lvert\omega_{ij}\rvert + 2\lvert ID\rvert + \lvert T_t\rvert + \lvert G_1\rvert)$
WG-to-CC	$\lvert\delta_{13}\rvert = l(\lvert\omega_i\rvert + 2\lvert ID\rvert + \lvert T_t\rvert + \lvert G_1\rvert)$
User-to-CC	$\lvert\delta_1\rvert = (n+7)(2048+96+160)$
Ref. [10]	
User-to-BG	$\lvert\delta_{21}\rvert = n(\lvert\omega_{ik}\rvert + 2\lvert ID\rvert + \lvert T_t\rvert + 2\lvert G_1\rvert)$
BG-to-CC	$\lvert\delta_{22}\rvert = t(\lvert\omega_i\rvert + 2\lvert ID\rvert + \lvert T_t\rvert + 2\lvert G_1\rvert)$
User-to-CC	$\lvert\delta_2\rvert = (n+4)(2048+96+320)$
CBSG	
User-to-DPOS	$\lvert\delta\rvert = n(\lvert\omega\rvert + \lvert ID_{Si}\rvert + m\lvert ID_{Rj}\rvert + \lvert T_t\rvert + 3\lvert G_1\rvert)$

The user reporting phase first generates ciphertext and signature $\{\omega, \sigma_i\}$, together with user and receiver

IDs, and timestamp, T_t, to form the user report $\delta = \langle \omega \parallel ID_{Si} \parallel mID_{Rj} \parallel T_t \parallel D \parallel \sigma_i \rangle$ to accounting node. In Table 3 we use DPOS to indicate the accounting node. CBSG ciphertext uses symmetric encryption, and $|ID|$, $|T_t|$ are 32 bit, $|G_1|$ is 160 bit. Therefore, the communication overhead reported by each user in this scheme is $|\delta| = (|\omega| + |ID_{Si}| + m|ID_{Rj}| + |T_t| + 3|G_1|)$, that is, $|\delta| = (32m + 672)$, where $m = 3$ is the number of receivers. Since CBSG has no BG or WG gateway, the user reporting communication overhead is the final communication overhead. Since [9] and [10] use Paillier encryption, N is 1024 bit. The communication overhead between the user and the BG in [9] and [10] is $|\delta_{11}| = (|\omega_{ijk}| + 2|ID| + |T_t| + |G_1|)$ and $|\delta_{21}| = (|\omega_{ik}| + 2|ID| + |T_t| + 2|G_1|)$, respectively; and the communication overhead of BG-WG and WG-CC in [9] is $|\delta_{12}| = t(|\omega_{ij}| + 2|ID| + |T_t| + |G_1|)$ and $|\delta_{13}| = l(|\omega_i| + 2|ID| + |T_t| + |G_1|)$ respectively. Since [10] has only a first-level gateway, the communication overhead for BG-CC is $|\delta_{22}| = t(|\omega_i| + 2|ID| + |T_t| + 2|G_1|)$.

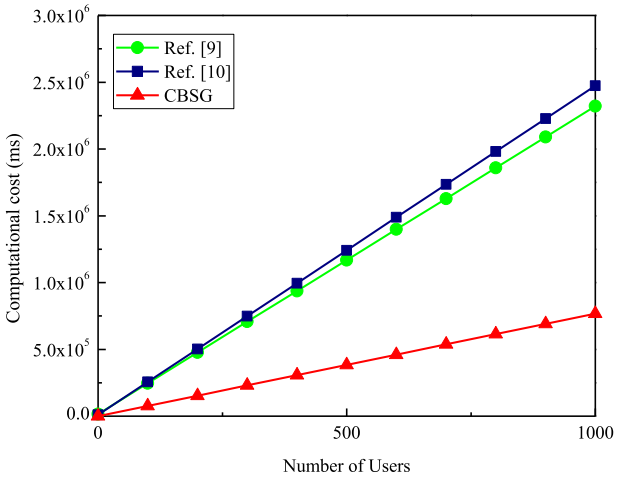

FIGURE 7. Communication overhead.

Figure 7 compares communication overheads for the cases $WG = 3$, and $BG = 4$. Communication overhead for [9] and [10] increases with increasing number of users, whereas the proposed CBSG scheme has significantly lower and slow increasing overhead.

The proposed CBSG scheme was based on the consortium blockchain and adopted the DPOS consensus. In contrast with the consensus of all nodes in public blockchains, CBSG only allows 101 preselected nodes to participate in the consensus, and generates new blocks in turn. In the feedback stage, CBSG realizes power management for a single user by designing feedback smart contracts, which are automatically executed when the trigger condition is reached, greatly reducing computational complexity and communication resources. CBSG can collect multidimensional data and achieve multi-party reception, for limited cost, hence meets practical application requirements and is very suitable for smart grid.

E. CONSORTIUM BLOCKCHAIN DELAY

In intelligent metering infrastructure, each meter measures multidimensional data and sends it to the consortium blockchain regularly, usually for 9 minutes [44]. The DPOS consensus adopted in this scheme can generate new blocks in 2 seconds [45]. Each block is about 12s, which can be confirmed eventually (after 6-10 confirmations), and the cycle of a complete 101 blocks is only about 3.367 minutes. Compared with the Proof of Work (PoW) mechanism 10 minutes to generate a block, 1 hour confirmation block, DPOS consensus greatly improved the confirmation speed. When the pre-selected node misses the block due to computational instability, computer downtime or maliciousness, it will be removed in the next round of elections. There is no large-scale and high-frequency broadcast in this scheme. There is no or little delay in this scheme during the aggregation phase.

In the management phase, each receiver realizes real-time regulation of the smart grid through smart contracts. The receiver sets regulation smart contracts for the grid operation status and user power consumption, which encapsulates a number of predefined status and conversion rules, triggers the execution of the contract, and responds to specific scenarios. When the trigger condition is reached, the smart contract is executed automatically. The proposed scheme uses computer language instead of cumbersome execution steps in the grid regulation process to realize real-time monitoring of the smart grid.

VII. CONCLUSION

This paper uses the consortium blockchain to achieve smart grid data aggregation and flexible regulation. Security analysis showed that CBSG meets all the various security requirements for power aggregation and regulation. Performance comparison verified that CBSG exhibited significant advantages in terms of computation and communication overhead for multi-user, multidimensional data and multi-recipient modes.

REFERENCES

[1] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future trends," *Acta Autom. Sinica*, vol. 42, no. 4, pp. 481–494, 2016.
[2] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. DBLP*, Oakland, CA, USA, Apr. 1980, pp. 122–134.
[3] M. Szydlo, "Merkle tree traversal in log space and time," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2004, pp. 541–554.
[4] Q. F. Shao, C. Q. Jin, Z. Zhang, W. N. Qian, and A. Zhou, "Blockchain: Architecture and research progress," *Chin. J. Comput.*, vol. 41, no. 5, pp. 969–988, Nov. 2018.
[5] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015, pp. 53–66.
[6] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: A survey," *IEEE Netw.*, vol. 28, no. 1, pp. 24–32, Jan. 2014.
[7] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.
[8] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.
[9] H. Zhou, J. Chen, Y. Y. Zhang, and L. J. Dang, "A multidimensional data aggregation scheme in multilevel network in smart grid," *J. Cryptologic Res.*, vol. 4, no. 2, pp. 114–132, Sep. 2017.

[10] X. Y. Liu *et al.*, "Data aggregation and access control method for communication system of smart grid," *Autom. Electr. Power Syst.*, vol. 40, no. 14, pp. 135–144, Jul. 2016.
[11] H. Shen and M. W. Zhang, "A privacy-preserving multilevel users' electricity consumption aggregation and control scheme in smart grids," *J. Cryptologic Res.*, vol. 3, no. 2, pp. 171–191, Feb. 2016.
[12] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2053–2064, Aug. 2014.
[13] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.
[14] K. Xue *et al.*, "PPSO: A privacy-preserving service outsourcing scheme for real-time pricing demand response in smart grid," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2870873.
[15] S. Li, K. Xue, Q. Yang, and P. Hong, "PPMA: Privacy-preserving multi-subset data aggregation in smart grid," *IEEE Trans. Ind. Inf.*, vol. 14, no. 2, pp. 462–471, Feb. 2018.
[16] Z. Guan, J. Li, L. Wu, Y. Zhang, J. Wu, and X. Du, "Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1934–1944, Dec. 2017.
[17] S. Li, X. Zhang, K. Xue, L. Zhou, and H. Yue, "Privacy-preserving prepayment based power request and trading in smart grid," *China Commun.*, vol. 15, no. 4, pp. 14–27, Apr. 2018.
[18] C. Pop *et al.*, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, p. 162, Jan. 2018.
[19] J. Gao *et al.*, "GridMonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, Mar. 2018.
[20] Z. Q. Wu *et al.*, "Secure data storage and sharing system based on consortium blockchain in smart grid," *J. Comput. Appl.*, vol. 10, pp. 2742–2747, Jun. 2017.
[21] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2018.2819663.
[22] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
[23] Z. Guan *et al.*, "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.
[24] Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[25] Ethereum White Paper. *A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: Nov. 12, 2015. [Online]. Available: https://github.com/ethereum/wiki/wiki/WhitePaper/
[26] D. R. Morrison, "Patricia—Practical algorithm to retrieve information coded in alphanumeric," *J. ACM*, vol. 15, no. 4, pp. 514–534, 1968.
[27] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.
[28] Q. M. Huang, "Blockchain and IoT-building the world on the chain," *Gold Card Project*, vol. 10, pp. 71–73, Oct. 2016.
[29] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE PerCom Workshops*, Mar. 2017, pp. 618–623.
[30] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst*, vol. 82, pp. 395–411, May 2018.
[31] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[32] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IOT," *IEEE Access*, vol. 6, pp. 115–124, May 2016.
[33] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.
[34] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
[35] R.-Y. Chen, "A traceability chain algorithm for artificial neural networks using T–S fuzzy cognitive maps in blockchain," *Future Gener. Comput. Syst.*, vol. 80, pp. 198–210, Mar. 2018.
[36] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, Mar. 2018.
[37] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2001, pp. 213–229.
[38] A. Joux, "A one round protocol for tripartite Diffie–Hellman," in *Proc. ANTS*, Berlin, Germany, 2000, pp. 385–393.
[39] Y. W. Zhou, B. Yang, and Q. L. Wang, "Anonymous hybrid signcryption scheme with multi-receiver (multi-message) based on identity," *J. Softw.*, vol. 29, no. 2, pp. 442–455, Apr. 2018.
[40] D. Larimer. (2014). *Delegated Proof-of-Stake White Paper*. [Online]. Available: https://bitfarm.io/
[41] Y. Xu *et al.*, "A provably secure and compact certificateless aggregate signature scheme," *Acta Electronica Sinica*, vol. 44, no. 8, pp. 1845–1850, Aug. 2016.
[42] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 62–73.
[43] J. Bethencourt. (2018). *Advanced Crypto Software Collection: The CPABE Toolkit*. [Online]. Available:http://acsc.cs.utexas.edu/cpabe/
[44] F. Benhamouda, M. Joye, and B. Libert, "A new framework for privacy-preserving aggregation of time-series data," *ACM Trans. Inf. Syst Secur.*, vol. 18, no. 3, p. 21, Apr. 2016.
[45] T. Y. Song *et al.*, "Comparison of blockchain consensus algorithm," *Comput. Appl. Softw.*, vol. 35, no. 8, pp. 1–8, Aug. 2018.

MOCHAN FAN received the B.S. degree in electronics and information engineering from the Suzhou University of Science and Technology, Jiangsu, China. She is currently pursuing the M.S. degree in electronics and communication engineering with the Jiangxi University of Science and Technology, Jiangxi, China. Her current research interests include blockchain technology and information security.

XIAOHONG ZHANG received the B.S. degree in physics from Jiangxi Normal University, Jiangxi, China, in 1988, the M.S. degree in optical information processing from the Chinese Academy of Sciences, Changchun Institute of Optical Precision Machinery, China, in 1993, and the Ph.D. degree in control theory and control engineering from the University of Science and Technology Beijing (USTB), in 2006, and the Postdoctoral degree in science of command from the Beijing University of Posts and Telecommunications (BUPT), in 2009. She was a Visiting Scholar with the University of California, Berkeley, CA, USA, from 2014 to 2015. She is currently a Full Professor with the School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China. Her main research interests include blockchain technology, information security, nonlinear dynamics, and wireless sensor networks.