IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 6, 2018, accepted July 10, 2018, date of publication July 24, 2018, date of current version November 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2856807

Blockchain-Based Secure Equipment Diagnosis Mechanism of Smart Grid

XIAOHONG ZHANG AND MOCHAN FAN
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 Jiangxi Education Department under Grant GJJ150621, in part by the Natural Science Foundation of Jiangxi Province under Grant 20161BAB202053 and Grant20161BAB206145, and in part by the Innovation Fund for Graduate Students in Jiangxi Province under Grant YC2017-S302.

ABSTRACT The smart terminal and grid protection devices play a very important role in the safe operation of the smart grid. Traditional maintenance and renewal of the center node wastes a lot of manpower and material resources and have huge safety implications. This paper proposes a safety equipment diagnosis mechanism based on consortium blockchain technology to realize more efficient, convenient, and secure device maintenance. When a device has problems or notices improper operation, it can make a device diagnosis request in the consortium blockchain network, and receive a diagnosis response from a vendor or non-original supplier nodes. This scheme designs a decentralized safety equipment diagnosis smart contract, combining response node bid price and credit, and applies a multi-dimensional reverse auction mechanism to determine bid node and transaction price. After a smart device diagnosed, the relevant message will be packaged and sent to a smartphone, which can use the client to set up the smart contract of equipment operation policy. Paillier encryption arithmetic can be used to ensure device diagnosis mechanism safety. The proposed scheme is guaranteed not to reveal sensitive information in the process of device interaction.

INDEX TERMS Consortium blockchain, equipment diagnosis, hash function, smart contract.

I. INTRODUCTION

Smart grids are integrated network systems composed of advanced communication and information technology. They have good controllability and can realize optimal power transmission and distribution between suppliers and users, solving traditional power grid problems of poor interaction, low energy utilization, and difficult safety analysis. These prominent advantages mean they have become the new trend for power grid construction, also bringing significant social benefits [1]–[3].

Smart grids mainly include intelligent substations, relay protection devices, smart meters, intelligent interactive terminals, etc., and the smart devices play a very important role. Equipment malfunction or abnormal operation can greatly influence safe and stable power system operation. The most common maintenance method at present when smart equipment does not work properly is that enterprise technicians go to the equipment in the field for diagnosis and repair, which is inefficient, consumes significant manpower and material resources, and user satisfaction is generally poor. Thus, traditional diagnosis and maintenance methods no longer meet societal needs, and new approaches are urgently required.

Several previous studies have considered methods to effectively improve intelligent equipment maintenance efficiency. Jamshidi *et al*. [4] proposed a risk prioritization framework to select the best maintenance strategy for medical devices, increasing high risk equipment availability. Markov outage models have been applied to condition based maintenance [5], analyzing three maintenance mode characteristics: complete, incomplete, and minimum maintenance. Subsequently, a time varying outage model to cover various maintenance modes was designed [6], based on a cloud platform, to solve reliability and fault diagnosis accuracy problems for substation equipment. A remote online diagnosis system for smart grid protection devices was developed [7] using mature 4G mobile communication technology. However, all previous studies considered a trusted central node monitoring all equipment updates and maintenance. If the central node was attacked or otherwise compromised, all data could be tampered or deleted, with consequentially serious safety problems for the whole system.

Some recent studies have applied blockchain technology with Internet of Things (IoT) equipment to solve safety interaction problems. Blockchain openness and transparency

mitigate malicious attack or tampering. Embedded device firmware version and update schemes have been proposed using blockchain technology [8] to address device safety firmware update problems. The proposed scheme verified embedded device firmware was the latest version, forbidding tampering.

A framework that integrated blockchain technology with smart devices was proposed [9] to provide a secure interaction platform and thereby ensure efficient and optimal use of available resources, while simultaneously providing better customer services. Reference [10] also presented an Ethereum blockchain platform, which by running Turing Complete code on the Ethereum to achieve an efficient and safe management for the IoT devices. However, since traditional public blockchain requires all network nodes to synchronize the information on the distributed storage chain, this will lead to network congestion.

Therefore, we propose a consortium blockchain based on Ethereum, focusing on real-time interaction device diagnosis, and developed a new safety equipment diagnosis mechanism. The proposed scheme does not require all nodes to participate in the consensus, avoiding network congestion.

Devices and diagnosis nodes are registered on the blockchain by their *ID* alone. When power protection devices, smart meters, or other electrical terminals fail or exhibit abnormal operation, they request diagnosis in the Ethereum network as failure nodes. If they are still within their warranty period, they are eligible for free diagnosis and service. When the failure node is outside the warranty period, original vendor nodes and non-original supplier nodes submit their price and credit to participate in bidding to diagnose the node. To this end, we design the decentralized safety equipment diagnosis smart contract (DSC), which decides the successful bidder according to their tendered price and credit. It is an auction mechanism that is approved by all nodes in the blockchain. The previous literatures also introduced some auction mechanisms [11]–[14], but they are centralized and not adaptive to our scheme. Once the deal is decided, a smart contract is executed automatically, which prevents any party from denying it. This also solves the double payment problems by the centralized system. Every interaction can be broadcasted in the Ethereum network and temporarily stored in node buffer pools. These interactions can be registered in a new block by preselected bookkeeper nodes. We adopted the consortium blockchain, which pre-selects nodes to participate in bookkeeping without involving all the nodes.

The proposed scheme realizes more efficient, convenient, and secure smart grid device maintenance. When grid protection devices, smart meters, or other electrical terminals require version update, this can be remotely diagnosed and actioned through the Ethereum network. The scheme breaks regional restrictions and saves maintenance time. Users would probably be unaware of device failures before receiving maintenance messages. During on-site maintenance, engineers can accurately check the specific problem part, rather than relying on experience or speculation, further reducing managing and testing costs for smart terminals or smart grid protection devices, promoting resource efficiency.

Section II introduces blockchain concepts and encryption algorithms, and Section III details the proposed safety equipment diagnosis mechanism. Section IV constructs the smart contract diagnostic mechanism, including equipment control and decentralized safety diagnosis policies. Section V introduces the diagnosis mechanism between original vendor and non-original supplier nodes after equipment failure. Section VI evaluates the proposed scheme safety and performance, and Section VII concludes the paper.

II. BLOCKCHAIN AND ENCRYPTION ALGORITHMS

A. BLOCKCHAIN

Blockchain was proposed by Nakamoto [15] in 2008 as a public ledger to record bitcoin transactions without requiring the third party. The blockchain has the characteristics of decentralization, time-series data, collective maintenance, programmability, security and trustworthiness. Blockchain has considerable potential economic, political, humanitarian, and legal benefits, because control transfers to participants rather than being centralized [16]. Blockchain uses asymmetric cryptography to encrypt plaintext, hence it can defend against strong computing external attack with the help of a consensus algorithm for the distributed network nodes, ensuring data reliability and tamper resistance [17].

When a smart device interaction occurs, interaction information will be seen by other nodes in the Ethereum consortium blockchain, and is stored in their own temporary information pool. After a miner creates a new block, interaction information can be removed from the temporary information pool, replaced by this new block, and prove legality by computing a two-Hash. For bitcoin blockchain, a deal is considered acknowledged and irreversible after six blocks. However, core developers believe that 120 blocks [18] will adequately protect networks, with no remaining threat by a potentially longer blockchain. The improvement scheme of bitcoin was developed in 2014 [19], and every bitcoin transaction can attach a message with no more than 40 bytes. In contrast, Ethereum, first proposed by Buterin in 2013 [20], can write unlimited data. The significantly shorter transaction time, about 12 seconds, means transaction confirmation is significantly faster than bitcoin. Therefore, the Ethereum blockchain was the best choice for the current application.

A closed private blockchain would be inappropriate since the system starts with the failure node requesting diagnosis, and participants are not limited to one vendor or one non-original supplier. Only vendors and qualified non-original suppliers are eligible to participate. The mechanism has a low requirement for anonymity and a high requirement for the speed of protection. Therefore, consortium blockchain is the most appropriate blockchain. Users, vendors and non-original suppliers are members of the consortium blockchain. The number of consortium blockchain bookkeeper pre-selection

node could be configured according to the Ethereum network scale.

Original vendor and non-original supplier nodes are treated equally in the proposed consortium blockchain. They can all be set as bookkeeper pre-selection nodes according to network scale. We adopted the cross fault tolerance (XFT) consensus algorithm [21], it considers that it is difficult for malicious nodes to control the entire network and bookkeeper pre-selection nodes at the same time, and then simplifies the Byzantine fault tolerance (BFT) message pattern.

B. BILINEAR PAIRING

Consider cyclic additive group G_1 and G_2 of big prime order q, selecting P as G_1 generator. Let there be a non-degenerate and efficient computability bilinear mapping [22], [23] $e : G_1 \times G_1 \to G_2$ 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 $P_1, P_2 \in G_1$.

A bilinear mapping that satisfies these properties is called a permissible bilinear mapping. This paper proposes safety equipment diagnosis mechanisms relied on some difficult problems [24].

C. BONEH-LYNN-SHACHAM SHORT SIGNATURE SCHEME

The Boneh-Lynn-Shacham (BLS) short signature [25] is a typical bilinear pairing-based scheme, which consists of key generation, signature, and verification. Given G_1 and G_2 are cyclic additive groups, we define a secure hash function $H : \{0, 1\}^* \to G_1^*$, where $\{0, 1\}^*$ represents a set of bit strings of arbitrary length, '$\cdot$' as the following multiple operation.

- Key generation. Given a bilinear pairing $e : G_1 \times G_1 \to G_2$, select random $x \in Z_q^*$ as the private key, sk, with corresponding public key $pk = xP$.
- Signature. Suppose $M \in G_1$ is the plaintext to be signed, then the signature of M can be expressed as

$$\sigma = x \cdot H(M). \tag{1}$$

- Verification. Compute $e(P, \sigma)$ and $e(pk, H(M))$ separately, and test for equality. If

$$e(P, \sigma) = e(pk, H(M)), \tag{2}$$

then verify the signature, otherwise fail.

D. THE PAILLIER CRYPTOSYSTEM

The Paillier encryption algorithm [26] is an additively homomorphic encryption, consisting of key generation, encryption, and decryption. Paillier encryption safety depends on the decisional composite residuosity assumption, which provides semantic security [26], [27].

- Key generation. Given a safety parameter κ, we select two large primes p and q, where p, q, and κ are the same length, and

$$N = pq, \quad \lambda = lcm(p - 1, q - 1) \tag{3}$$

where lcm is the least common multiple, and

$$L(u) = (u - 1)/N. \tag{4}$$

Choosing $g \in Z_{N^2}^*$ as the generator,

$$\mu = \left(L\left(g^{\lambda} \bmod N^2\right)\right)^{-1} \bmod N, \tag{5}$$

where N is an RSA coefficient. Hence, $pk = (N, g)$ is the public key, and the corresponding private key is $sk = (\lambda, \mu)$.

- Encryption. For all messages $M \in Z_N$, random select $r \in Z_N^*$, and obtain ciphertext

$$C = E(M) = g^M \cdot r^N \bmod N^2 \tag{6}$$

- Decryption. Given the ciphertext $C \in Z_{N^2}^*$, decryption is defined as

$$M = D(C) = L(C^{\lambda} \bmod N^2) \cdot \mu \bmod N. \tag{7}$$

In this paper, we use the BLS short signature based on bilinear pairing and the Paillier cryptosystem to ensure the security of the diagnostic interaction.

III. PROPOSED SAFETY EQUIPMENT DIAGNOSIS MECHANISM

The proposed safety equipment diagnosis mechanism can identify that a smart device is exhibiting failure or abnormal operation, and can be used as a failure node to request the diagnosis service in the Ethereum consortium blockchain.

A. PREPARATORY WORK

The diagnosis node can be original vendor or non-original supplier, and failure node generates a message sent to a smartphone after diagnosis. Non-original supplier includes indirect vendors (e.g. Siemens for Samsung is a non-original supplier) and qualified community diagnosis depots. When failing devices are within their warranty period, diagnostic services are free from the original vendors. Original vendors or non-original suppliers can submit their bid and credit to the DSC once the failure node is outside warranty. The smart contract system could adopt [13] based on the credit and bidding price of the bidding node, and designs a multi-dimensional reverse auction mechanism to determine the successful bidding node and transaction price. However, before offering a bid, diagnosis nodes are required to assess if they can diagnose the problem, and whether they are willing to provide service depending on the failure node's device mode and credit. The diagnosis nodes chooses the maintenance mode at the close of bidding, considering remote or on-site repair options.

Table 1 lists all symbols and definitions of this paper which will be used in the scheme description.

TABLE 1. Symbols used in this paper.

Symbol	Definition
B	Set of blockchain nodes
K	Set of normal nodes
V	Set of vendor nodes
NV	Set of Non-original supplier nodes
S	device of type k_i
Y_{ki}	Public key for k_i
Y_{vi}	Public key for v_i
x_{vi}	Private key for v_i
ID_{ki}	Identifier for k_i
ID_{vi}	Identifier for v_i
M_{ki}	Fault message for k_i
M'_{ki}	maintenance policy for k_i
R_{ki}	Relevant file for M_{ki}
$Cred_{ki}$	Credit for k_i
$Cred_{vi}$	Credit for v_i
n_c	Maximum or minimum credit values for cutting
w_i	Suspicious index
d_i	Coupons of last round of bidding failure nodes
R_i	Ranking price of bidding node
T	Timestamp
t_{ki}	Maintenance time for k_i
$Spot_{ki}$	Maintenance place for k_i
σ_{ki}	Signature for k_i
σ_{vi}	Signature for v_i
σ_{nvi}	Signature for nv_i
C_{ki}	Encryption message for k_i
C_{vi}	Encryption message for v_i
C_{nvi}	Encryption message for nv_i
P_i	Bid price by diagnosis node i
$P_{i\min}$	Minimum maintenance price
$P_{i\max}$	Maximum maintenance price
Rep_{vi}	Maintenance team with vender nodes

B. MECHANISM DESIGN

Figure 1 shows the proposed scheme structure, with detailed parameters as follows.

- Blockchain node. A blockchain node is a node in blockchain network, expressed as B, and a set of nodes as $B = \{b_1, b_2, \ldots, b_n\}$, $b_i \in B$. All blockchain node IDs can be registered on the blockchain and are available to all nodes.
- Ordinary node. An ordinary node is a smart device in the consortium blockchain, sending running conditions to and receiving regulation policy from a mobile phone app at regular intervals. The node adjusts its running conditions, and self-regulates by sensing failure diagnosis to the Ethereum consortium blockchain. A set of ordinary nodes are referred to as $K = \{k_1, k_2, \ldots, k_n\}$, $k_i \in K, K \subset B$. Every ordinary node's ID_{k_i} is registered on the blockchain available to all nodes.
- Original vendor node. Equipment brands correspond to different vendors, e.g. Cisco switches and routers belong to Cisco, Samsung smart devices to Samsung, etc. The original vendor node has first-hand information about their devices, and can be set consortium blockchain primary nodes depending on the network scale. A set of vendor nodes are referred to $V = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V, V \subset B$.
- Non-original supplier node. Non-original suppliers include indirect vendors and qualified community diagnosis depots, they can obtain the diagnostic right of the faulty device in the form of bidding. A set of non-original supplier nodes are referred to as $NV = \{nv_1, nv_2, \ldots, nv_n\}, nv_i \in NV, NV \subset B$.
- Smartphone. Devices are connected to smartphones through wireless networks, and regularly receive policy regulation from the smartphone. When a device fault is diagnosed, the diagnostic message is sent to the smartphone, which includes who finish diagnosis of the failure device, what maintenance has already occurred, payment information, etc. In the proposed system the smartphone accepts the message through the app, and establishes the equipment policy smart contract, realizing flexible equipment operation policies. For example, set the highest limit power for the electronic device. Once the power consumption of the device reaches the upper limit, it will automatically enter the power saving mode.

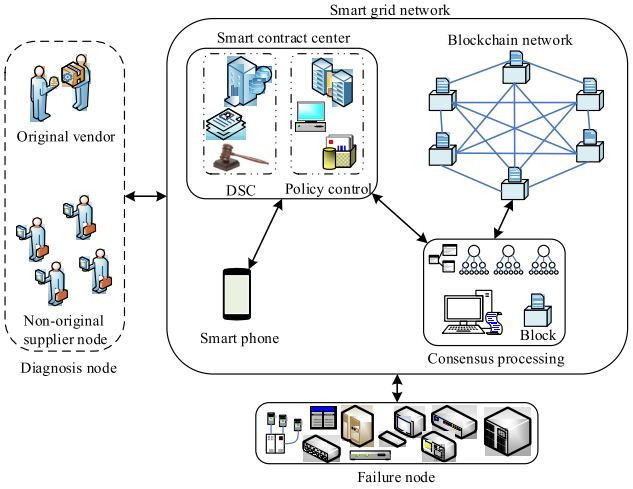

FIGURE 1. Secure equipment diagnosis structure.

C. SCHEME FLOW DIAGRAM

Figure 2 shows the proposed scheme. A malfunctioning device (failure node) broadcasts a diagnosis request on the Ethereum consortium blockchain, and original vendor and non-original supplier nodes are considered diagnosis nodes if they offer to provide diagnosis services for the request.

Different response processes apply depending on the failure devices being within the warranty period or not. Free diagnosis is available if the failure node is within the warranty period. The node must still transfer the digital currency of Ethereum (ETH) to the DSC to prevent fake requests. After diagnosis, the deposit will be returned to failure nodes.

If the failure node is out of warranty, diagnosis priority is assigned by bidding. Original vendor nodes v_i, and

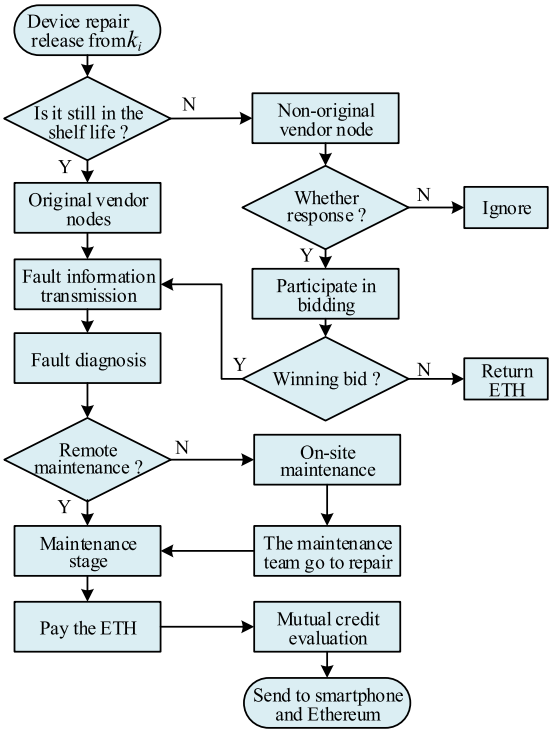

FIGURE 2. Secure equipment diagnosis flow.

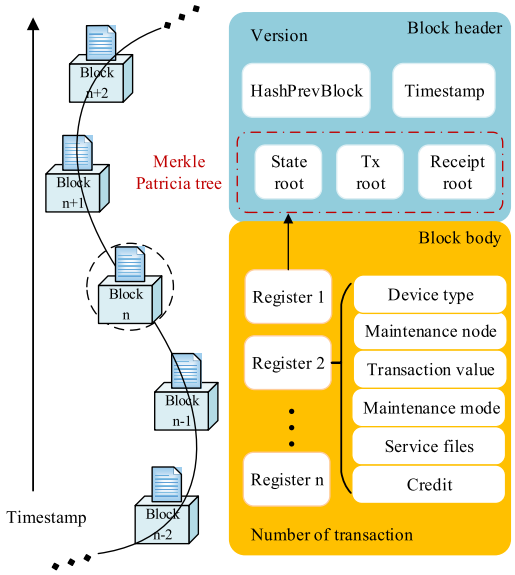

FIGURE 3. Diagnostic mechanism block structure.

non-original supplier nodes nv_i, compete fairly. They submit their bid and credit to DSC, and also transfer ETH to DSC to prevent malicious bidding.

D. DIAGNOSTIC MECHANISM BLOCK STRUCTURE

Each block quotes the previous block header's hash and is stored in linked list to establish the connection between blocks, forming the blockchain [28]. The block structure adopted in proposed scheme includes a block header and block body.

Unlike the bitcoin blockchain, Ethereum uses the Merkle Patricia tree [29]. Each Ethereum block head contains three Merkle trees, corresponding to three object types: state, transaction (Tx), and receipt root, as shown in Figure 3 dark red dotted line. The state tree records state changes of the nodes in the consortium blockchain, increased or reduced account balance of related nodes after a diagnosis interaction, execution state of the smart contract, whether a node exists in the consortium blockchain, etc. The transaction tree contains diagnostic information in the chain, and determines whether interaction information exists in the transaction tree. The receipt tree records receipts for the transaction execution log.

The block body is composed of the hash of diagnosing information, including device type, dis node, transaction value, maintenance mode, service details, and credit, as follows.

- Device type. The smart device type requesting service, such as air-conditioning, street lamps, etc. This helps diagnosis nodes to identify if the requesting device is in self-diagnosing areas, and convenient for adopting corresponding maintenance policies.
- Diagnosis node. Any node that reacts when the failure node sends a request for diagnosis.
- Transaction value: The cost of an equipment diagnosis. There is no charge for diagnosis (and repair) if the device is diagnosed by the original vendor and is still under warranty. Otherwise, the price will be determined by DSC subsequent to bidding by many nodes.
- Maintenance mode: Shows the specific repair type: Remote or on-site maintenance.
- Service files: Includes the requesting node *ID*, response node *ID*, failures types, diagnosis time, etc.
- Credit: After equipment service, failure and diagnosis nodes evaluate each other's response, etc. The final credit is calculated by trimmed mean [30]. The credit assists failure and diagnosis nodes to assess whether to accept or provide diagnosis, respectively. If a failure node's credit is below a diagnosis node's threshold, they will refuse to provide service for it.

We use the symmetric trimmed mean to calculate node reputations. Suppose the original vendor node has n historical credit $\{Cred_{v_{i1}}, Cred_{v_{i2}}, \ldots Cred_{v_{in}}\}$. Then the pruning value for selection is α, and the highest or lowest credit for clipping is

$$n_c = \left[\frac{\alpha}{100} \cdot \frac{n}{2}\right], \tag{8}$$

and the original vendor node credit is

$$Cred_{v_i} = \frac{\sum_{j=n_c+1}^{n-n_c} Cred_{v_{ij}}}{n - 2n_c}. \tag{9}$$

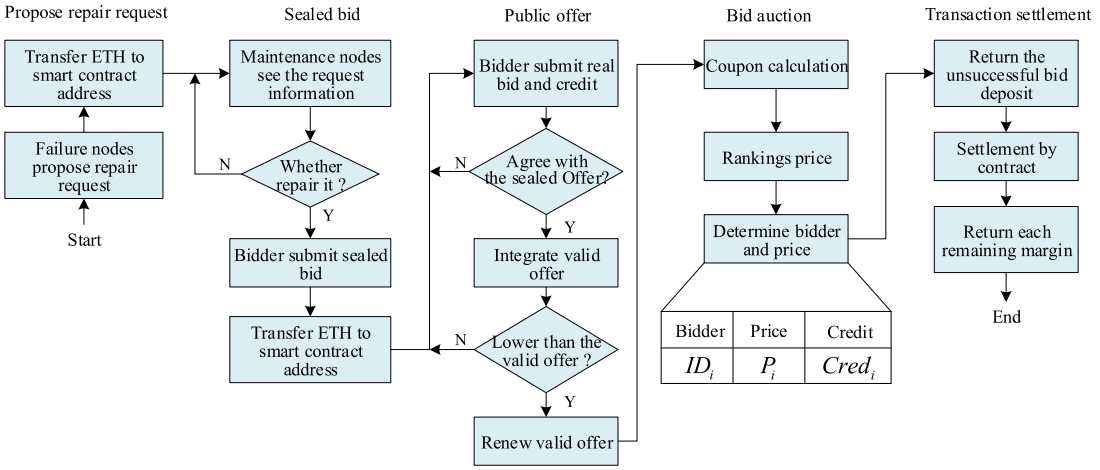

FIGURE 4. Decentralized safety equipment diagnosis smart contrac.

E. ALGORITHM INTERACTIVITY

When the failure node interacts with the diagnostic node, we use the Paillier encryption algorithm to encrypt and decrypt the mutual information. The Paillier algorithm is semantical safe and can effectively guarantee the confidentiality of the data. The goal of BLS short signature based on the bilinear pairing is to ensure data unforgeability and non-repudiation. In Section V we will specifically describe the use of these cryptographic algorithms. Diagnosing interaction information and smart contract, which will be recorded on the blockchain after verification in the chain of preselected consortium bookkeeper nodes, can be reviewed in the Merkle Patricia tree. Any irregularities can be promptly checked and corrected.

IV. SMART CONTRACT FOR DIAGNOSIS

This paper considers a large number of power protection devices, smart meters, other electrical terminals, smartphones, original vendors, and non-original suppliers. To facilitate establishment and management of smart contracts in the consortium blockchain, we need to design a smart contract client that all smart devices and other participants in the consortium blockchain can use. Therefore, we mainly focus on equipment control policy and the DSC.

A. EQUIPMENT CONTROL POLICY SMART CONTRACT

The smartphone regularly receives operation reports from the equipment and makes corresponding operation policy adjustments. Thus, smartphones establish smart contracts for equipment policy regulation through the smart contract client. Control policy smart contracts encapsulate smartphone and controlled device identities; predefined state and transformation rules; triggering contract execution, such as arriving at a specific time or a specific event, etc.; and responding to specific situations [17]. After policy control smart contract completion is released in the consortium blockchain, the preselected blockchain bookkeeper node packages and verifies the regulatory smart contracts, and the bookkeeper node with account access registers the packaged smart contracts into specific blockchain blocks.

The client regularly checks the state of contract execution, including the states, transactions, and trigger conditions in each contract. When a state reaches a trigger condition, it is removed from the blockchain and pushed to the queue for verification by bookkeeper nodes [31], realizing flexible adjustment of device operating policy.

B. DECENTRALIZED SAFETY EQUIPMENT DIAGNOSIS SMART CONTRACT

The proposed DSC is based on a distributed multilateral transaction smart contract [14], i.e., a smart contract tender system. Proposed diagnosis node bidding prices should conform to market trends for the device type. The price should be within $P_{i\min} < P_i < P_{i\max}$, where $P_{i\min}$ and $P_{i\max}$ represent the maximum and minimum maintenance price of a device when it is maintained, to prevents diagnosis nodes raising diagnosis prices. Figure 4 shows DSC process.

- Payment guarantee. When power protection devices, smart meters, and other electrical terminals broadcast a diagnosis request information on the Ethereum consortium blockchain, it needs to dispense ETH to DSC address as deposit to prevent false requesting, where ETH is the digital currency of Ethereum. The respond diagnosis nodes also pay ETH to the smart contract address as a deposit to prevent false bidding.
- Sealed bid. Diagnosis nodes assess their capability depending on the failure node device type. If they are capable and willing to provide diagnosis service they can bid for it, and the bid price remains confidential during the sealed bid period. Diagnosis nodes use hash encryption to present $H(P_i, Cred_i)$ as a sealed bid.
- Public offer. After the sealed bid period, bidders provide their real cost P_i and credit $Cred_i$ in the allotted time, and the smart contract verifies that these match $H(P_i, Cred_i)$.

An offer is valid if they match and void otherwise. When a new quotation is lower than the maximum price of the present effective quotation, the quotation is verified and updated as valid.

- Bid auction. To gain more income, some nodes may conspire to bid low for several auction rounds, winning the bids. Eventually other bidders withdraw from the bidding mechanism, and the collusion nodes can control the auction mechanism. They then raise bid prices to increase their income, without the regulating influence of other bidders, increasing diagnosis costs. Therefore, the k-means [13], [32] algorithm is used police price conspiracy and ensure auction fairness.
  a. Bidding prices for n diagnosis nodes are clustered, and r bidding prices are selected as centroid, $r \ll n$.
  b. The price difference between remaining bids and each centroid is calculated and the bid classified into the nearest centroid class. Then the mean of each cluster is recalculated (central object).
  c. Cycle (b) until each cluster does not change.
  d. If the central price of a class is lower than the mean value of all class center prices, bidding nodes in this class are suspected of collusion. All bidding nodes in these classes are recorded.
  e. After consecutive iterations, if a bidding node frequency in suspect classes exceeds a predetermined threshold, the suspect index w_i plus one, i denotes a bidding node, and the initial value of w_i is zero:

$$w_i = w_i + 1 \tag{10}$$

Based on the bidding price and its credit, a multi-dimensional reverse auction mechanism is designed, in order to ensure the reliable bidding nodes continue to participate in the diagnosis of bidding.

When a bidder fails in the bidding, he can gain coupons to increase their probability of winning subsequent auctions, the rule of coupons is as follow:

$$d_i = \begin{cases} d_i + \beta(Cred_i - e^{w_i}), & \text{Failed bid} \\ 0, & \text{Successful bid,} \end{cases} \tag{11}$$

where d_i represents the coupon value for bidder i, and β represents the total amount of coupons. Hence, when a bidder fails a previous auction, d_i is refresh with increment, which is the difference between the reputation value $Cred_i$ and the exponent of the suspect index w_i and weights with the total virtual coupon β. Nodes with high credit and low suspicion get more coupons, increasing their probability of winning subsequent auctions. If a node won the previous auction or withdrew from process midway, coupon value is zero.

Define a ranking price O_i, P_i for the actual bidding price. The proposed DSC determines the final bidder using,

$$O_i = P_i - d_i \tag{12}$$

where we select the lowest ranking price, O_i, as the winning bid. Thus, bidding node coupons improve their ranking prices, increasing their likelihood of winning an auction. The actual node quotation is the diagnosis price once the winning node is determined.

- Transaction settlement. After determining the winning node, the DSC returns all deposit of the unmarked nodes, and returns respective surplus guarantees according to the agreed-upon price.

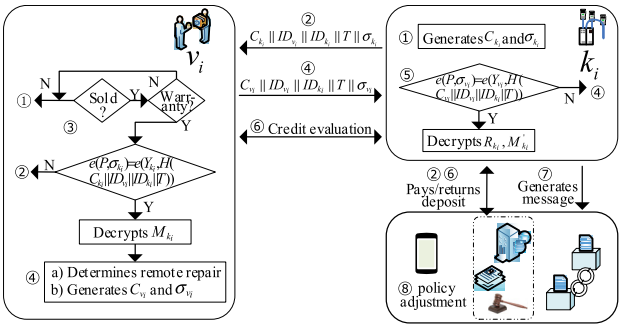

FIGURE 5. Remote maintenance procedure during the warranty period (RMW).

V. IMPLEMENTATION OF SAFETY EQUIPMENT DIAGNOSIS MECHANISM

As discussed earlier, the proposed scheme can be divided into free diagnosis by original vendor nodes when the device is within the warranty period and diagnosis by original vendor or non-original supplier nodes otherwise. Nodes receive diagnosis rights through the DSC. Once the diagnosis node is assigned, repair processes can be either remote or on-site.

A. DIAGNOSIS WITHIN WARRANTY PERIOD

Power protection devices, smart meters, etc. can take advantage of free diagnosis provided by the original vendor nodes if they are within their warranty period. Remote or on-site maintenance is then decided depending on the diagnosed fault. For example, physical damage repair must be performed on-site, but firmware updates can be remotely actioned through the consortium blockchain.

Various parameters are exchanged within the consortium blockchain: failure node k_i send ID_{k_i}, Y_{k_i}, and (g_{k_i}, r_{k_i}) to the original vendor node, v_i; and v_i sends ID_{v_i}, Y_{v_i}, and (g_{v_i}, r_{v_i}) to k_i. Since these details are confidential, they must be transmitted by secure channels.

1) REMOTE MAINTENANCE

Figure 5 shows the remote maintenance procedure during the warranty period (RMW), with details as follows.

1. The failure node, k_i, uses vendor node (v_i) encryption parameters (g_{v_i}, r_{v_i}) to encrypt failure details: trouble spot, failure performance, etc., generating ciphertext $C_{k_i} = E(M_{k_i}) = g_{v_i}^{M_{k_i}} \cdot r_{v_i}^{N} \bmod N^2$ with corresponding signature $\sigma_{k_i} = x_{k_i} H(C_{k_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T)$.
2. k_i forwards $C_{k_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T \parallel \sigma_{k_i}$ to the vendor node, v_i, where T is the current timestamp to prevent replay attack. Failure nodes dispense ETH to the DSC to prevent false requests.
3. v_i receives the message, it first inquires the state tree of the Merkel Patricia tree in the blockchain to verify whether the device is sold by itself and the current status of the device is still in the warranty period. If the above conditions are all satisfied, the BLS short signature based on bilinear pairing is used to verify whether the message sent by k_i has been falsified or forged. If $e(P, \sigma_{k_i}) = e(Y_{k_i}, H(C_{k_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T))$ validation was successful, otherwise verification fails and the protocol terminates. After validation v_i extracts the device failure details $M_{k_i} = D(C_{k_i}) = L(C_{k_i}^{\lambda} \bmod N^2) \cdot \mu \bmod N$ using decryption key (λ, μ).
4. Depending on M_{k_i}, v_i diagnoses the device requires remote maintenance, and obtains the corresponding repair policy file, R_{k_i}, from the database. v_i then encrypts R_{k_i} using the k_i encryption parameters (g_{k_i}, r_{k_i}), generating ciphertext $C_{v_i} = E\left(R_{k_i}\right) = g_{k_i}^{R_{k_i}} \cdot r_{k_i}^{N} \bmod N^2$ and signature $\sigma_{v_i} = x_{v_i} H(C_{v_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T)$ with x_{v_i}(the private key for v_i), and forwards $C_{v_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T \parallel \sigma_{v_i}$ to k_i.
5. k_i validates the message from v_i, verifying the origin and the data was not tampered or forged, i.e., if $e(P, \sigma_{v_i}) = e(Y_{v_i}, H(C_{v_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T))$ then validation was successful and fails otherwise. If validation succeeds k_i decrypts the message, extracts R_{k_i} and hence M'_{k_i}, and repairs the smart device following M'_{k_i}.
6. k_i and v_i assess each other and provide corresponding credits. Consortium blockchain nodes renew their credit following the trimmed mean method in Part B of Section III, and the failure node's deposit is be returned through the DSC.
7. k_i packages maintenance information and credit evaluation of both parties, and forwards to the smartphone and Ethereum consortium blockchain. A bookkeeper node adds the details to the newly generated blockchain after verification. Once the message was add to the blockchain, it will be permanently stored on the blockchain.
8. The smartphone adjusts the appropriate smart contract policy using the smart contract client and publishes it to the consortium blockchain. The smart contract client periodically checks the status of contract execution. If something reaches the trigger condition, it will be taken out of the consortium blockchain, and the policy control smart contract will be automatically executed, so as to realize the timely policy adjustment of smart devices.

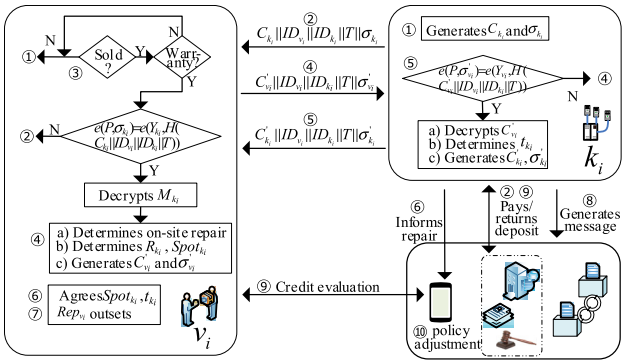

FIGURE 6. On-site maintenance procedure during the warranty period (SMW).

2) ON-SITE MAINTENANCE

Figure 6 shows the on-site maintenance procedure during the warranty period (SMW), with details as follows.

1. Failure node k_i, encrypts the fault message using v_i encryption parameters (g_{v_i}, r_{v_i}), including trouble spot, failure performance, etc., generating ciphertext $C_{k_i} = E(M_{k_i}) = g_{v_i}^{M_{k_i}} \cdot r_{v_i}^{N} \bmod N^2$, and corresponding signature $\sigma_{k_i} = x_{k_i} H(C_{k_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T)$.
2. k_i sends $C_{k_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T \parallel \sigma_{k_i}$ to v_i, where T is the current timestamp to prevent replay attack, and dispenses ETH to the DSC as deposit to prevent false requesting.
3. The v_i verifies in the consortium blockchain state tree that the device was sold by itself and can provide free services for it. Afterwards the BLS short signature based on bilinear pairing is used to verify whether the message sent by k_i has been falsified or forged. If $e(P, \sigma_{k_i}) = e(Y_{k_i}, H(C_{k_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T))$ validation was successful and fails otherwise. If validation succeeds, v_i extracts device failure information $M_{k_i} = D(C_{k_i}) = L(C_{k_i}^{\lambda} \bmod N^2) \cdot \mu \bmod N$ using decryption key (λ, μ).
4. Depending on M_{k_i}, v_i diagnoses physical damage or other requirements for on-site repair; obtains the corresponding repair policy file, R_{k_i}, from the database; determines the maintenance location, $Spot_{k_i}$; encrypts $C'_{v_i} = E\left(Spot_{k_i}\right) = g_{k_i}^{Spot_{k_i}} \cdot r_{k_i}^{N} \bmod N^2$ signed with x_{v_i}; and generates $\sigma'_{v_i} = x_{v_i} H(C'_{v_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T)$. Finally, v_i sends $C'_{v_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T \parallel \sigma'_{v_i}$ to k_i.
5. The k_i validates the message to ensure it come from v_i and the data was not tampered or forged, i.e., if $e(P, \sigma'_{v_i}) = e(Y_{v_i}, H(C'_{v_i} \parallel ID_{v_i} \parallel ID_{k_i} \parallel T))$ validation was successful, and fails otherwise. If validation succeeds, k_i decrypts the message to obtain $Spot_{k_i}$; decides a maintenance time, t_{k_i}; encrypts the details as C'_{k_i}, generates σ'_{k_i}, and sends these to v_i.

6. The v_i validates the message, then decrypts it to obtain t_{k_i}. If there is no objection, v_i informs $ID_{k_i} \parallel M_{k_i} \parallel R_{k_i} \parallel Sport_{k_i} \parallel t_{k_i} \parallel T$ to their maintenance crews, Rep_{v_i}, and the maintenance crews prepare repair tools. If the parties disagree with $Spot_{k_i}$, t_{k_i} they can consult through the available time window. k_i sends the diagnosis messages to the smartphone with equipment fault, repair location, repair time, etc., details
7. At the negotiated time, Rep_{v_i} goes to the device site and instigates repair.
8. The k_i reports maintenance information to the smartphone after completion, including the maintenance time.
9. Smartphone (as k_i agent), and v_i assess each other and notify the corresponding credits to consortium blockchain. Blockchain nodes renew their credit using the trimmed mean method in Part B of Section III. The failure node's deposit is then returned by the DSC. The Smartphone sends the maintenance message to Ethereum. The preselected bookkeeper node in the consortium blockchain stores the received interaction information in its own buffer pool. After the consensus verification, the message is added to the newly generated block.
10. The smartphone adjusts the appropriate smart contract policy using the smart contract client. The bookkeeper node with account access registers the policy control smart contracts with specific blocks of the blockchain. Thus, policy adjustment is automatically triggered once appropriate conditions are achieved. After each smart contract is executed, a receipt will be generated in the receipt tree of the blockchain, which facilitates the query of the completion of the smart contract later.

B. DIAGNOSIS BEYOND WARRANTY

When power protection devices, smart meters, etc., request diagnosis beyond their warranty period, other nodes in the consortium blockchain will see the request information. The original vendor and non-original supplier nodes submit bid applications to the DSC in Part B of Section IV, which determines the successful bidder and price as detailed in Section IV. Just as for the within warranty period case, repairs are divided into requiring remote or on-site maintenance. We consider the case where a non-original supplier node wins the auction to describe diagnosis details, but the original vendor case follows similarly.

1) REMOTE MAINTENANCE

Figure 7 shows the remote maintenance procedure outside warranty period (ROW), with details as follows.

1. Failure node k_i forwards a request message including Y_{k_i}, ID_{k_i}, S, $Cred_{k_i}$ to the DSC, and dispenses ETH to the DSC to prevent false requests.
2. After each diagnostic node in the consortium blockchain checks k_i's diagnosis request, it verifies in the status tree whether k_i is a registered node in the chain and judges it is true and valid. The diagnosis node obtains k_i's device mode S, determines the diagnosis is within their capabilities, consider k_i credit $Cred_{k_i}$, and decides if they are willing to provide diagnosis services.
3. The nv_i sends bid price and their $Cred_{nv_i}$ to the smart contract tender system for consideration and dispenses ETH to the DSC to prevent false bidding. If the bid is judged to be a malicious attempt to disrupt normal bidding or other behavior, their deposit will not be returned.
4. The DSC determines the successful bidder and price as detailed in Section IV, and publishes the outcome to Ethereum network. For demonstration purposes, we assume the winning node is nv_i.
5. After bidding, nv_i and k_i exchange the successful bidder and failure nodes exchange necessary parameters including identity, public key Y_{nv_i}, and encryption parameters (g_{nv_i}, r_{nv_i}) and (g_{k_i}, r_{k_i}) using a secure channel.
6. The nv_i and k_i interact (***stage I***), to realize safety diagnosis following similar process to RMW steps (1)–(5).
7. Once the maintenance is successfully completed, the DSC automatically arranges payment to nv_i at the agreed price, and returns any remaining bidding deposits. If nv_i and k_i fail to perform the smart contract, the defaulter's deposit will not be returned.
8. The k_i and nv_i assess each other and notify the corresponding credits to consortium blockchain. Consortium blockchain nodes renew their credit using the trimmed mean method in Part B of Section III.
9. The k_i packages maintenance information, credit evaluation for both parties, and payments and forwards to the smartphone and Ethereum. After verification, these details are added to the blockchain by the bookkeeper node.
10. The smartphone adjusts the appropriate smart contract policy using the smart contract client and publishes it to the consortium blockchain. The client will check the execution status of each contract regularly. If the

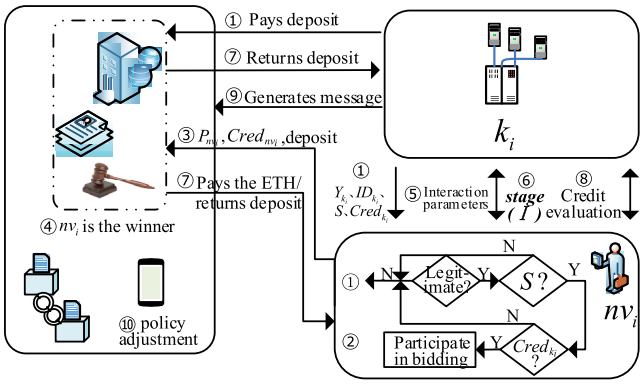

FIGURE 7. Remote maintenance procedure outside warranty period (ROW).

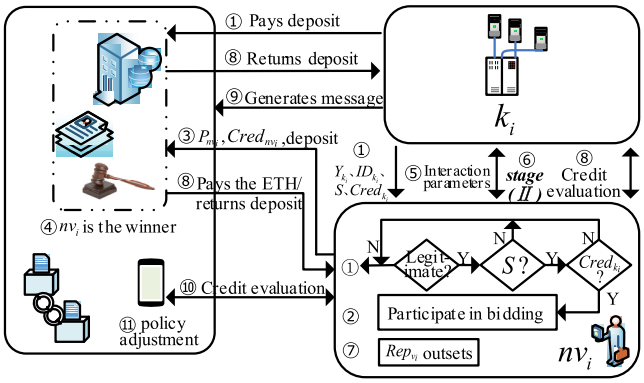

FIGURE 8. On-site maintenance procedure outside the warranty period (SOW).

execution condition is satisfied, the contract will be pushed to the queue to be verified. Thus, policy adjustment is automatically triggered once appropriate conditions are achieved. After the smart contract is executed, it is categorized in the blockchain's receipt tree.

2) ON-SITE MAINTENANCE

Figure 8 shows the on-site maintenance procedure outside the warranty period (SOW), with details as follows.

1. Failure node k_i deliveries a request message including Y_{k_i}, ID_{k_i}, S, $Cred_{k_i}$ to the DSC, and dispenses ETH to the DSC to prevent false requests.
2. A diagnosis node nv_i in consortium blockchain finds the diagnosis request of the fault node k_i, it will verify whether k_i is a valid node in the chain through the state tree root. If k_i is a valid node in the consortium blockchain, checks its device mode S to determine if the device is in its own maintenance scope, that is, whether it has the ability to diagnose the device. At the same time, the in-chain diagnostic node can verify whether the $Cred_{k_i}$ submitted by the requesting node k_i is true and valid in the state tree, and determine to provide diagnosis services or not.
3. The nv_i sends the bid price and $Cred_{nv_i}$ to the smart contract tender system for consideration and dispenses ETH to the DSC to prevent false bidding. nv_i also pays a certain margin (deposit) to prevent malicious bidding. If the bid is assessed as malicious bid, attempting to disrupt the normal bidding mechanism or other behavior, the deposit will not be returned.
4. The DSC determines the successful bidder and price as detailed in Section IV, returns the deposits for unsuccessful nodes, and publishes the result to Ethereum network. For demonstration purposes, we assume the winning node is nv_i.
5. After bidding, nv_i and k_i exchange the successful bidder and failure nodes exchange necessary parameters including identity, public key Y_{nv_i}, and encryption parameters (g_{nv_i}, r_{nv_i}) and (g_{k_i}, r_{k_i}) using a secure channel.
6. nv_i and k_i interact (***stage II***), to realize safety diagnosis following similar process to SMW steps (1)–(6).
7. At the negotiated time, Rep_{v_i} goes to the device site and instigates repair.
8. Once the maintenance is successfully completed, the DSC automatically arranges payment to nv_i at the agreed price automatic, and returns any remaining bidding deposits. If nv_i and k_i fail to fail to perform the smart contract, the defaulter's deposit will not be returned.
9. k_i also reports maintenance information to the smartphone, let it to master the maintenance information in time.
10. Smartphone and nv_i assess each other and notify the corresponding credits to consortium blockchain. Consortium blockchain nodes renew their credit using the trimmed mean method. The smartphone publishes the maintenance message to Ethereum. A bookkeeper node adds the details to blockchain after verification. The nodes can query in the transaction tree of the consortium blockchain whether the diagnostic interaction is in a specific block.
11. The smartphone adjusts the appropriate smart contract policy using the smart contract client and publishes it to the consortium blockchain. Thus, policy adjustment is automatically triggered once appropriate conditions are achieved.

VI. SAFETY ANALYSIS AND PERFORMANCE EVALUATION

In this section we discuss the security of the designed DSC and compare it with the existing auction mechanism. Then, we made a detailed analysis of the security and performance of the proposed scheme, which included communication overhead and computational overhead.

A. THE DSC DISCUSSION

DSC allows the nodes in the chain to issue diagnostic requests and participate in bidding decentralized. Information occurs at each node on the chain, and be stored in the blockchain permanently after consensus verification. Therefore, the auction mechanism is tamper-proofing. The requesting node and the bidding node on the blockchain platform are undeniable for any messages posted on the chain, and the mechanism can solve the "double spending" problem. The DSC in this paper is multidimensional which means it not only pays attention to price bidding, but also takes the credibility value of each node into consideration. By introducing coupons and ranking prices, bidding determines the diagnostic nodes with low prices and good service quality.

1) DSC RELATED ALGORITHM

The request issued by the fault node is visible to the in-chain diagnostic node. The diagnostic node can judge whether to participate in the bidding based on the device type of the

TABLE 2. Comparison between DSC and other related mechanisms.

	[11]	[12]	[13]	[14]	DSC
Blockchain-Based	N	N	N	Y	Y
Tamperproof and non-repudiation	Y	N	N	Y	Y
Multidimensionality	N	N	Y	N	Y
Dynamic and distance participation	Y	Y	Y	Y	Y
Bidding confidentiality	Y	Y	N	Y	Y
Anti-collusion	N	N	Y	N	Y
Prevent malicious bidding	N	Y	Y	Y	Y
Identity management	Y	N	N	N	Y

failure node and its credit. Thus it will realize dynamic participation and remote bidding. During the submitting quotations phase, if bidding price and credit are submitted directly, those information are visible to all nodes in the chain, which may cause subsequent diagnostic nodes to drive down prices maliciously to obtain diagnostic rights when participating in bidding. To solve this problem, the mechanism divides bid submission into two stages: sealed bid and public offer. In this way, the confidentiality of bidding can be achieved. The auction mechanism we designed can prevent the bidding node collusion attack by the K-means clustering algorithm and ensure the fairness of the bidding mechanism.

2) DSC ADVANTAGE

The DSC in this paper can effectively prevent malicious bids and false requests, which is achieved by paying ETH as a deposit. The amount of ETH is very large. If there is any breach of contract, the deposit will not be returned. Therefore, there will be no breach of contract by all nodes due to the deposit. This mechanism also has the function of identity management. Unlike the bitcoin blockchain, this paper designs a consortium blockchain based on Ethereum. The identity management of each node can be achieved through the Ethereum Merkle Patricia tree. In the Patricia Tree's state tree, we can query whether each node is a valid node in the chain and its status. Moreover, the computation overhead of our auction mechanism is very small, and we only require light weight hash calculation and coupon calculation in bidding.

3) MECHANISM COMPARISON

Table 2 compares our DSC's function with literature [11]–[14] presented in this paper. To sum up, this scheme is superior to other four schemes in terms of functionality and safety, and it is more suitable for smart grid equipment diagnostic bid auction.

B. SAFETY ANALYSIS

We analyzed the security of the proposed scheme in terms of diagnosis interactions and Ethereum consortium blockchain.

1) MAINTENANCE INTERACTIVE SAFETY

a: Confidentiality of interactive messages

We adopt Paillier encryption to provide transaction safety between failure and diagnosis nodes. Attackers cannot obtain any information about fault messages or diagnosis strategies, even if messages between nodes were hacked. Thus, interactive message confidentiality is assured.

b: Data unforgeability

All nodes use their private keys to sign any messages before sending. Receiving nodes use the sender's public key to verify the message. The proposed scheme adopts the BLS signature based on the computational Diffie-Hellman problem [24] to ensure an attacker cannot forge a new signature by wiretapping the original signature. Operational safety using Paillier encryption arithmetic and BLS signature technology has been proved previously [33], [34].

2) ETHEREUM BLOCKCHAIN NETWORK SAFETY

a: Exclusive diagnosis mechanism

Smart devices can only be registered in consortium blockchain by their legal *ID*. When a failure node sends diagnosis request, the response node ensures it is a legitimate consortium blockchain member by verifying its *ID*. Should any unregistered nodes manage to enter the network, any messages from them will be discarded. Thus, the proposed scheme conserves communication resources as well as preventing potential attacks.

b: Node identity protection

All ordinary nodes in the proposed scheme have a unique *ID* provided by the vendor, which is used as their communication identity for any interaction. Only the vendor node knows which smart device the identity corresponds to, and they do not reveal the identity of their production equipment. Hence, failure nodes and non-original supplier nodes do not know each other's real identity. If attackers or curious legal nodes obtain another node's identity, they cannot obtain the node owner, spot, device type, running status or other information.

c: False claims and malicious bids

The proposed DSC prevents false requests by requiring failure nodes to pay a deposit when issuing a diagnosis request. This also avoids network congestion caused by the repeated diagnosis requests from conquered or curious nodes intended to waste network resources. The deposit also ensures the failure node has the capacity to pay.

Diagnosis nodes also pays a deposit to the DSC when they responds to a diagnosis request. This effectively prevents malicious bidding and guarantees smooth bidding. Once maintenance is completed, the bidding mechanism deducts the ETH from the request nodes and pays the diagnosis node automatically. Thus, payment arrears are eliminated.

TABLE 3. Diagnostic mode communication overhead.

Pattern	Node	Unicast	Broadcast
RMW	k_i	3	1
	v_i	2	0
	Smartphone	0	0
SMW	k_i	4	0
	v_i	2	0
	Smartphone	1	1
ROW	k_i	5	1
	nv_i	2	0
	Smartphone	0	0
SOW	k_i	6	0
	nv_i	3	0
	Smartphone	1	1

TABLE 4. Diagnostic mode computation overhead.

Pattern	Node	Computation	Computation cost
RMW	k_i	3 × exponent arithmetic, 1 ×multiplication operation, 1 × bilinear pairing	$6T_E + 2T_M + 2T_P$
	v_i	3 × exponent arithmetic, 1 ×multiplication operation, 1 × bilinear pairing	
SMW	k_i	5 × exponent arithmetic, 2 ×multiplication operation, 1 × bilinear pairing	$9T_E + 3T_M + 3T_P$
	v_i	4 × exponent arithmetic, 1 ×multiplication operation, 2 × bilinear pairings	
ROW	k_i	3 × exponent arithmetic, 1 ×multiplication operation, 1 × bilinear pairing	$6T_E + 2T_M + 2T_P$
	nv_i	3 × exponent arithmetic, 1 ×multiplication operation, 1 × bilinear pairing	
SOW	k_i	5 × exponent arithmetic, 2 ×multiplication operation, 1 × bilinear pairing	$9T_E + 3T_M + 3T_P$
	nv_i	4 × exponent arithmetic, 1 ×multiplication operation, 2 × bilinear pairing	

d: Data theft prevention

Failure information sent to a diagnosis node includes current equipment performance, possible fault point, device type, credit, etc. These data are not confidential, and the diagnosis node cannot obtain equipment operation rules or owner behavior data.

e: Information cannot be falsified

Diagnosis interaction and bidding data are verified by consortium blockchain bookkeeper nodes. Once verified, the data are permanently recorded in Ethereum network. This prevents data tampering and forgery while ensuring real and effective data. If a node forged a higher credit to obtain superior diagnosis service or increase their bid success rate, the false data would be seen by other bookkeeper nodes. The node would need to control more than 50% of the bookkeeper nodes, to successfully forge data.

The proposed scheme adopts the XFT consensus algorithm, which simplifies the BFT message pattern. If there are f malicious bookkeeper nodes, then we only need $n \geq 2f + 1$ valid bookkeeper nodes to data tampering. If every node had 50% probability of becoming malicious, data tampering success rate is only $1/2^{f+1}$ [21]. For examples, suppose there are 100 bookkeeper nodes, with 50% probability of becoming malicious. Then 50 bookkeeper nodes must be simultaneously controlled to successfully manipulate data, i.e., the probability of successful attack $= 1/2^{50} \approx 8.9 \times 10^{-16}$.

C. PERFORMANCE EVALUTION

We analyze the proposed scheme's performance with regard to communication and computation overhead.

1) COMMUNICATION OVERHEAD

The proposed scheme's communication overhead includes interactions between fault and diagnosis nodes, and node interactions with ETH.

In RMW, k_i unicasts failure information to v_i; package the corresponding diagnosis message then forward it to the smartphone and broadcast it to Ethereum network; and forward the credit evaluations. Thus, there are three unicast and one broadcast communication. The v_i unicasts diagnosis information to k_i, and provides credit evaluation of k_i. Thus, there are two unicast communications. Table 3 summarizes the communication overhead for the four maintenance modes. Unicast transmission is the dominant mode, with very limited broadcast transmissions in all cases.

2) COMPUTATION OVERHEAD

The proposed scheme's computational cost arises mainly from calculating the Paillier exponential (T_E), multiplication in signature algorithm (T_M), and bilinear pairs (T_P). Other calculations, such as Paillier multiplication may be neglected. Table 4 shows calculation overhead for each maintenance mode.

VII. CONCLUSION

Smart grids are being more widely deployed, inevitably requiring smart device maintenance, including power protection devices, smart meters, and other electrical terminals diagnosis. This paper proposes a safety equipment diagnosis mechanism based on Ethereum blockchain technology to realize safe automatic fault diagnosis. Smartphones can be notified of equipment operating conditions in real-time, and interactively manage device policy. Paillier encryption and BLS short signatures are based on bilinear pairs ensure message transmission security. The proposed security equipment diagnosis mechanism explicitly considers devices within or outside their warranty period, and the proposed DSC structure and detailed processes are explained and visualized in flow charts. A multi-dimensional reverse auction mechanism combining bidder price and credit determines

successful bidder nodes and transaction price. The proposed system eliminates payment repudiation, and ensures that high quality nodes continue are recognized and preferred in bidding. Discussed have shown that, in comparison to existing related mechanism, DSC offers significant improvements in terms of security and various performance. Security analysis has proven that the safety equipment diagnosis mechanism based on Ethereum blockchain meets the requirements for diagnosing interactive security and privacy protection. Blockchain applications for equipment maintenance have enormous potential. Future research objectives include reducing communication and calculation overheads, and improving scalability.

REFERENCES

[1] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," *Future Gener. Comput. Syst.*, vol. 28, no. 2, pp. 391–404, Feb. 2012.

[2] G. W. Arnold, "Challenges and opportunities in smart grid: A position article," *Proc. IEEE*, vol. 99, no. 6, pp. 922–927, Jun. 2011.

[3] 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.

[4] A. Jamshidi, S. A. Rahimi, D. Ait-Kadi, and A. Ruiz, "A comprehensive fuzzy risk-based maintenance framework for prioritization of medical devices," *Appl. Soft Comput.*, vol. 32, pp. 322–334, Jul. 2015.

[5] G. Ji, B. Zhang, S. Liu, W. Wu, and W. Jiang, "A time-varying component outage model for power system condition-based maintenance," *Proc. CSEE*, vol. 33, no. 25, pp. 139–146, Sep. 2013.

[6] Y.-Y. Wang, Y.-N. Cai, and C. Wang, "Intelligent diagnosis system for substation equipment based on cloud platform," *High Voltage Eng.*, vol. 41, no. 12, pp. 3895–3901, Dec. 2015.

[7] Z.-G. Wang *et al.*, "Research on remote diagnosis system of smart grid protection device," *Power Syst. Protection Control.*, vol. 45, no. 20, pp. 86–91, Oct. 2017.

[8] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, Mar. 2017.

[9] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. HPCC-SmartCity-DSS*, Sydney, NSW, Australia, 2016, pp. 1392–1393.

[10] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. ICACT*, Bongpyeong, South Korea, Feb. 2017, pp. 464–467.

[11] G. Liu, J.-Z. Zhang, and S.-C. Xie, "Multiparty quantum english auction scheme using single photons as message carrier," *Int. J. Theor. Phys.*, vol. 57, no. 3, pp. 756–763, Nov. 2018.

[12] H. Shajaiah, A. Abdelhadi, and C. Clancy, "Secure power scheduling auction for smart grids using homomorphic encryption," in *Proc. IEEE BigData*, Boston, MA, USA, Dec. 2017, pp. 4507–4512.

[13] J. Li, X.-W. Wang, and R. Liu, "User reputation-based participatory incentive mechanism in social and community intelligence systems," *J. Frontiers Comput. Sci. Technol.*, vol. 9, no. 12, pp. 1471–1482, Nov. 2015.

[14] J. Ping, S. Chen, N. Zhang, L. Yao, and Z. Yan, "Decentralized transactive mechanism in distribution network based on smart contract," *Proc. CSEE*, vol. 37, no. 13, pp. 3682–3690, Jul. 2017.

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

[16] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, Inc., 2015, pp. 53–66.

[17] 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.

[18] D. Larimer. (2014). *Delegated Proof-of-Stake*. [Online]. Available: https://www.bitfarm.io/

[19] G. Andresen. (2014). *Bitcoin Improvement Proposals*. [Online]. Available: https://www.github.com/bitcoin/bips/

[20] Ethereum. *A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: Nov. 12, 2015. [Online]. Available: https://github.com/ethereum/wiki/wiki/WhitePaper/

[21] S. Liu, P. Viotti, C. Cachin, V. Quéma, and M. Vukolić, "XFT: Practical Fault Tolerance beyond Crashes," in *Proc. 12th USENIX Symp. Oper. Syst. Design Implement. (OSDI)*, 2016, pp. 485–500.

[22] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 2001, pp. 213–229.

[23] A. Jou, "A one round protocol for tripartite Diffie–Hellman," in *Proc. ANTS*, Heidelberg, Germany, 2000, pp. 385–393.

[24] F. Bao, R. H. Deng, and H. Zhu, "Variations of diffie-hellman problem," in *Proc. ICICS*, Heidelberg, Germany, 2003, pp. 301–312.

[25] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, 2004.

[26] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Eurocrypt*, vol. 547, 1999, pp. 223–238.

[27] O. Baudron, P.-A. Fouque, D. Pointcheval, G. Poupard, and J. Stern, "Practical multi-candidate election system," in *Proc. 20th ACM Symp. PODC*, New York, NY, USA, 2001, pp. 274–283.

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

[29] D. R. Morrison, "PATRICIA—Practical algorithm to retrieve information coded in alphanumeric," *J. ACM*, vol. 15, no. 4, pp. 514–534, 1968.

[30] D. C. Hoaglin, F. Mosteller, and J. W. Tukey, *Understanding Robust and Exploratory Data Analysis*. New York, NY, USA: Wiley, 1983, pp. 1333–1336.

[31] J. Cai, S. Li, L. Tang, and B. Fan, "Blockchain based energy trading in energy Internet," *Electr. Power Construction*, vol. 38, no. 9, pp. 24–31, Sep. 2017.

[32] G. Gan and M. K.-P. Ng, "k-means clustering with outlier removal," *Pattern Recognit. Lett.*, vol. 90, pp. 8–14, Apr. 2017.

[33] D. Kempe, J. Kleinberg, and É. Tardos, "Maximizing the spread of influence through a social network," in *Proc. KDD*, New York, NY, USA, 2003, pp. 137–146.

[34] S. Asur, S. Parthasarathy, and D. Ucar, "An event-based framework for characterizing the evolutionary behavior of interaction graphs," *ACM Trans. Knowl. Discovery Data*, vol. 3, no. 4, Nov. 2009, Art. no. 16.

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, the Ph.D. degree in control theory and control engineering from the University of Science and Technology Beijing, in 2006, and the Post-Doctoral degree in science of command from the Beijing University of Posts and Telecommunications in 2009. She was a Visiting Scholar with the University of California at Berkeley, Berkeley, 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 are blockchain technology, information security, nonlinear dynamics, and wireless sensor network.

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 includes blockchain technology and information security.