Hindawi
Security and Communication Networks
Volume 2021, Article ID 9501572, 20 pages
https://doi.org/10.1155/2021/9501572

Research Article

Smart Grid Nontechnical Loss Detection Based on Power Gateway Consortium Blockchain

Xudong He, Jian Wang, Jiqiang Liu, Enze Yuan, Kailun Wang, and Zhen Han

Beijing Jiaotong University, Beijing, China

Correspondence should be addressed to Jian Wang; wangjian@bjtu.edu.cn

Received 17 June 2021; Revised 5 August 2021; Accepted 27 September 2021; Published 14 October 2021

Academic Editor: Yinghui Zhang

The rapid development of the smart grid brings convenience to human beings. It enables users to know the real-time power supply capacity, the power quality, and the electricity price fluctuation of the grid. However, there are still some threats in the smart grid, which increase all kinds of expenses in the grid and cause great trouble to energy distribution. Among them, the man-made nontechnical loss (NTL) problem is particularly prominent. Recently, there are also some NTL detection programs. However, most of the schemes need huge amounts of supporting data and high labor costs. As a result, the NTL problem has not been well solved. In order to better avoid these risks, problems such as tampering of smart meter energy data, bypassing the smart meter directly connected to the grid, and imbalance between revenue and expenditure of the smart grid are tackled, and the threat scene of NTL is constructed. A hierarchical grid gateway blockchain is proposed and designed, and a new decentralized management MDMS system is constructed. The intelligent contract combined with the elliptic curve encryption technology is used to detect the storage and the acquisition of power data, and the detection of NTL problems is realized. At the same time, it has a certain ability to resist attacks such as replay, monitoring, and tampering. We tested the time consumption and throughput of this method on Hyperledger Fabric. At the same time, eight indexes of other methods proposed in the literature are compared. This method has a good effect.

1. Introduction

The concept of smart grid was put forward in 2003, and the "Smart Grid Technology Forum" was established by the European Union in 2005. The smart grid is essentially a modern transmission network. It uses information and communication technology to adjust the production, transmission, and distribution of electric power [1], to achieve the purpose of saving energy, reducing loss, and enhancing the reliability of the power grid. The smart grid can realize the two-way communication of information the services [2, 3]. The smart meter in the smart grid not only has the basic measurement function but also has more abundant functions, such as communication function. In order to adapt to the use of modern smart grid and new energy, it is also equipped with a storage module and a calculation module, which can store electricity consumption information and the two-way ladder rate metering function, and also provides a control interface that can be remotely controlled, as well as intelligent functions such as electricity theft prevention. In the smart grid, Advanced Metering Infrastructure (AMI) system is used for intelligent management. AMI system is mainly composed of smart meter, communication system and equipment, and Meter Database Management System (MDMS).

While the smart grid brings advantages, for example, intelligent power grid management, it is also faced with extremely serious threats, which are mainly divided into natural threats and man-made threats. Among the many threats, the most common is that power thieves or power users deceive power companies through a series of ways and then bring nontechnical loss to the entire smart grid. NTL refers to the remaining part of the loss of power transmission and distribution that cannot be explained by technology after excluding TL. Abnormal electricity consumption behaviors such as electricity theft are the main cause of NTL

[4]. According to statistics, in countries such as India, Brazil, China, and the United States, the loss of power supply caused by power theft is more than 25%. In recent years, not only is the phenomenon of electricity theft becoming more and more serious, but also the electricity theft methods used by electricity theft users are more and more various, and means of electricity theft are becoming more and more sophisticated. In addition to the traditional power theft methods, such as the undervoltage method and undercurrent method [5], there are also high-tech methods of electricity thefts, such as strong magnetic interferences, power thefts from high-frequency power supply, and network attacks on intelligent meters or data centers [6]. The behavior of electricity thefts is becoming more and more technically sophisticated. It can be seen that, in the past, the means that users relied on to steal electricity, such as destroying traditional electricity meters or private power lines, have been transformed into attacks on smart meters through digital storage technology and network communication technology [7]. The attack is to reduce the corresponding time power consumption or directly return it to zero through data tampering, in order to reduce the electricity bill payable.

In the operation of the power grid, nontechnical losses will cause a large number of energy and economic losses, and the uncertainty of power theft behavior will directly affect the load supply and demand balance of the power grid and interfere with the stability of the power system. Therefore, it is of great practical significance to analyze power consumption data and to detect electricity theft behavior [8]. In response to the aforementioned nontechnical power loss problem, much related work has been done which can be divided into the following three categories: (1) Physical detection solutions include the use of physical solutions to prevent and detect electricity theft. These physical solutions include routine inspections, sensor monitoring, camera monitoring, and drone monitoring. (2) The NTL fraud detector based on machine learning algorithms mainly uses machine learning technology to establish a detection model to identity electricity theft. However, the training dataset of the nontechnical power loss detection model requires power experts to mark the attack data in the power dataset; thus, the cost is high. In addition, because the power theft against smart grids will bring huge economic benefits to attackers, the diversity of related attack behaviors increases. The feature extraction becomes more and more difficult, and the inaccuracy of features directly leads to the high accuracy of detection models. The reduction in magnitude has led to huge economic losses in the power system. (3) Based on the comparison method, this kind of scheme usually adopts a safe and reliable central instrument to measure the abnormal situation and compare it with other suspicious instruments. These schemes are usually lightweight and flexible, but existing schemes can only detect NTL fraud with small datasets.

Therefore, even if there are some detection schemes for NTL attacks, we still need to explore other more effective solutions. The study is aimed at the NTL problem in the smart grid and develop a detection plan from the MDMS in the AMI system. We designed a smart grid NTL problem protection scheme based on the power gateway consortium blockchain. The scheme can solve the problems such as the difficulty of state detection of smart meters, the difficulty of smart meter access authentication, and the insecurity of hierarchical management of power transactions. We use power data and meter status data to detect NTL. It has a good detection effect on smart meter data tampering and power theft caused by users directly connected to the power grid. It is used to solve the problems caused by NTL in the smart grid.

The main contributions of this paper are as follows:

(1) The scheme proposed in this paper can effectively resist replay attacks, surveillance attacks, man-in-the-middle attacks, and witch attacks.

(2) This paper stores the electric energy information and the state of the smart meter in the MDMS system, and adopts the storage mode of the edge network blockchain to store the user's smart meter status and the user payment information, which is used for NTL audit and accountability.

(3) This paper proposes the NTL threat scenario, which detects NTL based on the edge network blockchain, and uses the blockchain technology to ensure that the data cannot be tampered with. The detection method does not rely on a large amount of data to train the model but on smaller user power consumption data.

The rest of the paper consists of the following sections. Section 2 introduces the related research work of blockchain technology and the NTL detection technology. Section 3 proposes a smart grid NTL detection scheme based on the power network association chain, including the overall structure, client registration, and data encryption and decryption transmission. Section 4 demonstrates the experiment and the experimental results as well as the comparison. Section 5 analyzes the security and threat scenarios of the overall scheme. Section 6 gives the research results and discussion.

2. Related Work

This section will summarize the existing work; we first summarize the related work of NTL detection in smart grid, then investigate the important role of blockchain technology in the smart grid, and finally summarize the related detection technology of blockchain to illustrate the feasibility of smart grid NTL detection scheme based on the gateway blockchain.

2.1. Smart Grid NTL Detection. Nowadays, with the development of smart, integrated, and interconnected power grids, to achieve the goal of reliability, security, and cost-effectiveness of the power grid and to prevent the occurrence of power theft incidents, the NTL detection technology and related research are gradually developing. Leite et al. [9] proposed a strategy for detecting nontechnical losses using a multivariate control chart, which establishes a reliable area

to monitor the measured variance. After detecting the nontechnical loss, the pathfinding program based on the algorithm can find the consumption point of the nontechnical loss. Jeyaraj et al. [10] put forward a multidimensional deep learning algorithm to learn and classify nonperiodical electricity and then can detect user theft of electricity from the periodic load curve. The weekly load pattern and daily load pattern are both processed as 2D power data samples. Saeed et al. [11] suggested an efficient classification method based on the BoostingC5.0 decision tree to detect nontechnical losses in electric utilities. First, extract data features from the dataset to distinguish honest from fraudulent customers. Afterward, Pearson's chi-square feature selection algorithm is used to select the most relevant feature among the extracted features. Finally, use the BoostedC5.0 decision tree (DT) algorithm to classify honest consumers and fraudsters based on the results of the selected functions. Viegas et al. [12] mentioned a clustering-based method to detect power theft. By clustering the collected data, typical consumer behavior prototypes can be extracted. If the distance between a new data sample and a typical consumer prototype is too large, the distance-based novelty detection framework will classify it as vicious data. Okino Otuoze et al. [13] put forward a power theft detection framework based on a general predictive algorithm. The framework uses universal anomaly detection (UAD) based on the Lempel-Ziv universal compression algorithm, which can realize real-time detection in the smart grid environment. It detects anomalies by monitoring many network parameters, including monitoring energy consumption data, the change rate of energy consumption data, and date stamps as well as time stamps. Blazakis et al. [14] introduced an adaptive neuro-fuzzy inference system (ANFIS) for power theft detection. The results show that if the technology is correctly applied, it can achieve a high detection success rate in the case of fraudulent activities caused by unauthorized energy use.

Given the NTL problem in the smart grid, the above detection methods have played a certain role, but a few of them require a large amount of data, and the calculation method is complex. It poses a serious threat to the privacy and security of power-related data. We explore new technologies to solve the NTL problem by investigating the application of blockchain in the smart grid.

2.2. Application of Blockchain in Smart Grid. In the smart grid system, various network transpositions require a large amount of data sharing and exchanges between gateways. At the same time, information exchanges between power suppliers and individual consumers are also very frequent; therefore if the power system encounters network security threats, it will cause huge losses. Blockchain technology has the characteristics of decentralization, openness, transparency, and nontamperability; realizes the collaborative trust and concerted actions between multiple subjects; and is widely used in the construction of smart grids. Gai et al. [15] suggested an alliance blockchain method to solve the privacy leakage problem of energy transaction users in smart grids without restricting transaction functions. This method also can detect the relationship between it and other information (such as physical location and energy usage) by mining various energy transaction volumes. Guan et al. [16] put forward a blockchain-based smart grid data aggregation privacy protection scheme, which divides users into different groups, and each group has a private blockchain to record the data of its members. The scheme uses pseudonyms to hide the identity of users. Each user can create multiple pseudonyms and associate their data with different pseudonyms. However, this scheme also only conducts a single-dimensional data collection, and the user power data in the same area is transmitted in plain text, posing a great security risk. Pop et al. [17] used blockchain technology to design a demand-side response model for distributed management of energy networks. The model uses tamper-proof blockchain technology to store energy consumption data collected from the IoT smart meter. At the same time, the automatically executed smart contract defines the expected energy loss of each producer and each consumer in a programmatic way and then realizes it. In order to match the production and demand of the smart grid. Gao et al. [18] put forward a smart grid monitoring method based on a secure sovereign blockchain and also implemented a smart contract. The contract executes the established procedures and then provides a network-based trusted system. The system proved to be very effective because users can monitor how the electricity is used, and it also provides a platform that no one needs to manipulate.

Through the investigation of related work, there are many applications of blockchain technology in the smart grid, less research working on NTL detection and, some problems such as information sharing; thus, we also investigate the scheme of abnormal problem detection of blockchain in our paper.

2.3. Smart Grid Combined with Blockchain-Related Work. Blockchain technology is also used in the industrial Internet of things scenarios [19]. In response to the problem of abnormality detection in the smart grid, the blockchain can realize the cooperative trust between different information interaction parts through "smart contracts" and efficiently detect abnormal situations.

Li et al. [20] mentioned a blockchain-based method for detecting abnormal electricity consumption in smart grids, aiming to use sensor processing, smart meter readings, machine learning, and blockchain to accurately and timely detect electricity consumption abnormality.

Signorini et al. [21] proposed a blockchain-based anomaly detection method (BAD). BAD is a complete framework that relies on several components that utilize its core blockchain metadata to collect potentially malicious activities. BAD avoids any central point of failure and can prevent malware from deleting or changing its own traces.

Golomb et al. [22] mentioned a lightweight framework CIoTA, which uses the concept of blockchain to perform distributed and collaborative anomaly detection on devices

with limited resources. Through the consensus between proof and IoT devices, CIoTA uses the blockchain to gradually update the reliable anomaly detection model.

Casado-Vara et al. [23] suggested a new system for detecting fraud based on blockchain. The blockchain is used to store the data of the distribution network monitored by the WSN and apply the created clustering algorithm to detect fraud. Whenever the blockchain grows, the stored data is more secure. Therefore, the power company can check the stored blockchain data. It is proved that blockchain technology has a certain effect on abnormal problem detection.

Through the above research and analysis, it is found that, with the development of the smart grid, the interaction between power suppliers and users becomes more convenient. At the same time, due to the application of various intelligent devices and the generation of corresponding massive data and information, problems such as Internet security and power theft continue to appear in the power grid system. Aiming for the problem of NTL, several scholars have also proposed a detection scheme, but the scheme has some problems, such as the large demand for data and the need for data concentration. Moreover, data privacy and security cannot be guaranteed and are high labor costs. Therefore, combined with the blockchain technology, this paper proposes a smart grid power theft detection model based on the power network association chain, which gives full play to the dispersion, openness, transparency, and tamper-proof of the blockchain technology, and applies it to the smart grid NTL detection problem.

3. Smart Grid NTL Detection Based on Power Gateway Consortium Blockchain

Through the investigation of related work, we found that the smart grid has problems of NTL caused by the tampering of the electricity data of the smart meter at the home network layer, NTL caused by bypassing the smart meter and directly connected to the grid network, and difficulty in detecting the imbalance of smart grid revenue and expenditure. Based on the edge of the smart grid network, we designed a smart grid NTL problem protection program based on the power gateway blockchain. We first introduced the smart grid gateway consortium blockchain structure and described the threat model scenarios of NTL in the smart grid. Finally, a smart grid NTL detection model and detection method based on the power gateway consortium blockchain are proposed in Section3.3. In the detection method, the smart meter registration, online data storage and query, data structure, consensus, and detection process are introduced in detail.

3.1. Smart Grid Gateway Consortium Blockchain Structure. The smart grid gateway consortium blockchain structure consists of two parts, including the power infrastructure network and the power communication network. The power communication network includes three levels: wide-area network (WAN), local area network (LAN), and home network (HAN). The WAN consortium blockchain network consists of LAN power gateways, and each LAN power gateway node includes multiple LAN consortium blockchain networks. The LAN consortium blockchain network is composed of HAN power gateways, and each HAN power gateway node includes multiple HAN networks. The specific structure is shown in Figure 1.

Definition 1. Power infrastructure network.

The basic network of power facilities includes the basic equipment in the traditional power grid, such as power generation facility, power transmission stations, and substation/distribution stations. After generating electricity from the power generation facility, the process of voltage boosting, transmission, and the step-down is carried out, and finally, the electricity is sold to the users by the distribution station. It provides a guarantee for the production, transmission, and use of electric energy.

Definition 2. Electric power communication network.

The electric power communication network is composed of three types of network structures, including HAN, LAN, and WAN. Each layer of the network structure includes power gateway equipment for data aggregation and network communication as shown in Table 1.

The blockchain structure of HAN, LAN and WAN, grid gateway, and smart meter in the power communication network is shown in Figure 2.

The electric power communication network is divided into HAN, LAN, and WAN according to the communication range from small to large. The three are inclusive ($\mathrm{HAN} \subset \mathrm{LAN} \subset \mathrm{WAN}$). Among them, the HAN network includes HAN power gateways, smart meters, and various home electrical equipment. Electrical equipment gathers power consumption information in smart meters, which are connected to the HAN power gateway. Here, we define multiple HAN networks as $\mathrm{HAN}_1, \mathrm{HAN}_2 \ldots \mathrm{HAN}_N$. LAN network is composed of multiple HAN networks, namely, $\mathrm{LAN} = \{\mathrm{HAN}_1 \cup \mathrm{HAN}_2 \ldots \mathrm{HAN}_N\}$. In the LAN network, the HAN power gateway is used as a node to form a LAN network consortium blockchain. Similarly, the WAN network consists of multiple LAN networks, namely, $\mathrm{WAN} = \{\mathrm{LAN}_1 \cup \mathrm{LAN}_2 \ldots \mathrm{LAN}_N\}$. In the WAN network, the LAN power gateway is used as a node to form a WAN network consortium blockchain.

3.2. Threat Scenario. The user is the smallest unit in the smart grid scenario and is divided into malicious users and normal users. The malicious user is the core threat that causes nontechnical power loss in the smart grid. Based on the behavior and distribution characteristics of malicious users, this paper divides the threats of malicious users into three categories: active malicious user threats, passive malicious user threats, and group malicious user threats. The specific scenarios of the three different threats will be introduced one by one as follows:

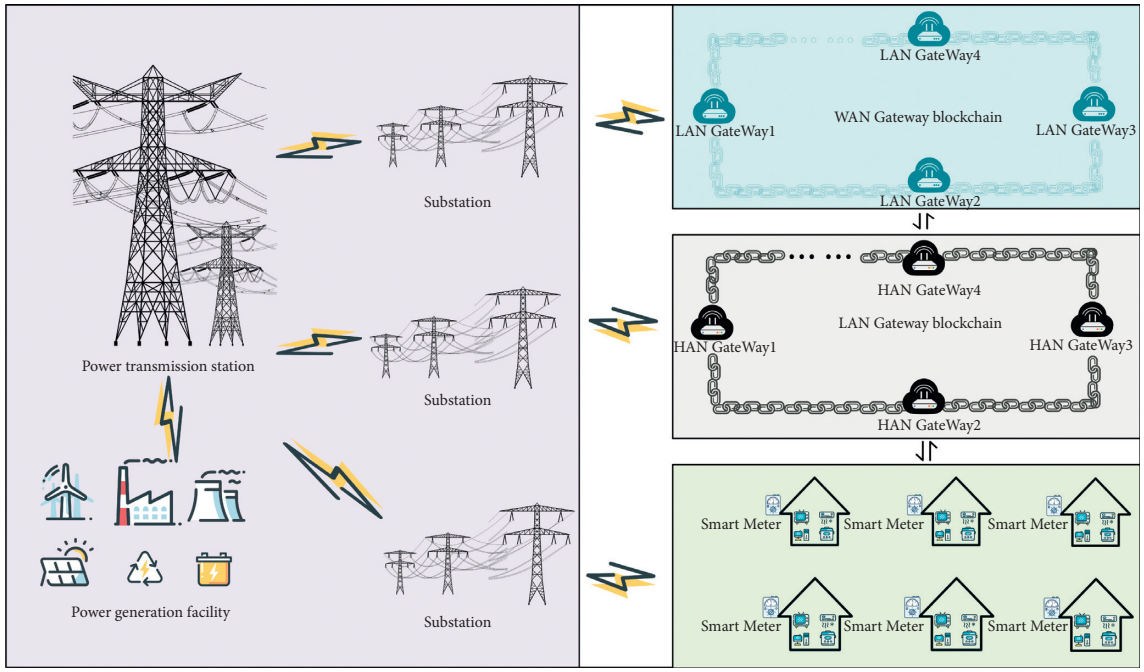

Figure 1: Smart grid gateway consortium blockchain structure.

Table 1: Interpretation of key nouns.

Name	Description
Power gateway	There are different types of gateways in different network structures. The HAN network includes HAN power gateway equipment and smart meter equipment; the LAN network includes the LAN power gateway equipment; and the WAN network includes the WAN power gateway equipment.
HAN network	Devices in a home area network (HAN) share resources through public communication networks (such as Ethernet) or wireless connections (such as WIFI, Bluetooth low energy, ZigBee, and IEEE 802.15.4). The smart meter of each home local area network is used as the entrance and exit of electric energy control, and the electricity consumption in the home network is collected and controlled through the smart meter.
LAN network	The local area network (LAN) is larger than the HAN network communication range from the perspective of network information communication. The LAN network is an alliance blockchain composed of HAN power gateways, which can store data. In the LAN consortium blockchain network, the HAN power gateway node collects and stores information from the smart meters in HAN.
WAN network	From the perspective of network communication, the wide-area network (WAN) has a larger communication range than LAN. In the wide-area network, the power gateway in the LAN is used as a node to form an alliance blockchain. The LAN power gateway in the WAN consortium blockchain network completes data collection and storage in the LAN network.

Active Malicious User Threat. Active malicious users are malicious users with intermittent power theft from the perspective of behavior characteristics. This type of user will perform normal charging behaviors and also conduct power theft behavior. From the perspective of distribution characteristics, this type of user does not have obvious geographic clustering and is usually mixed with normal users.

Passive Malicious User Threat. The distribution characteristics of passive malicious users and active malicious users are the same, but the behavior characteristics are different, which is mainly reflected in the passive malicious users not performing charging behavior.

Threats of Group Malicious Users. The harm of group malicious users to the smart grid is extremely serious. The most distinctive feature is that malicious users gather in the same area, and the behaviors of malicious users are complex and diverse, for example, active malicious users are mixed with passive malicious users.

3.3. Smart Grid NTL Detection Model Based on Power Gateway Consortium Blockchain. In the proposed detection method, the overall structure and concept, intelligent meter registration, online data storage and query, data structure, consensus, and detection process are introduced in detail in the following subsections.

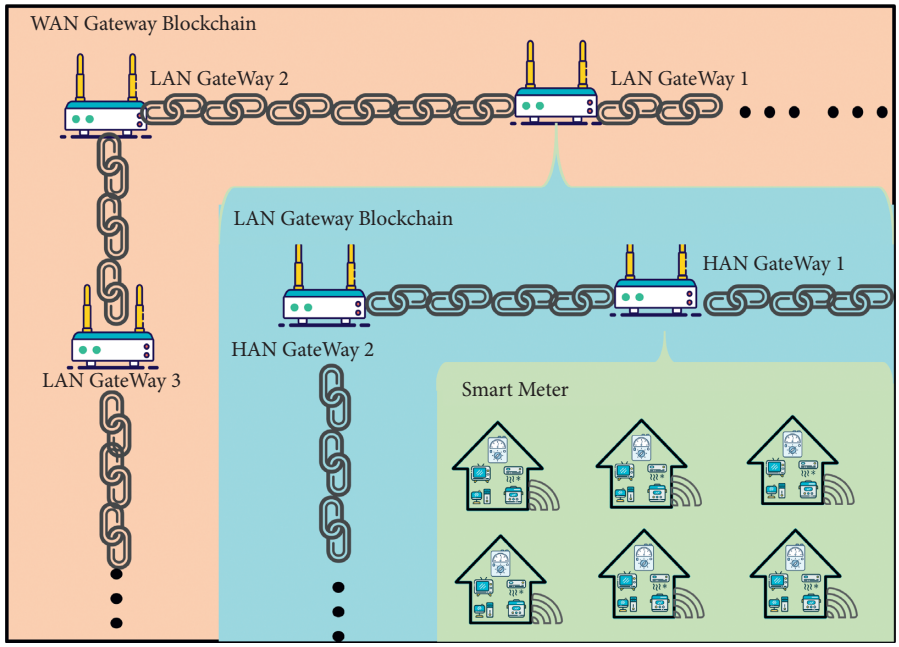

Figure 2: Blockchain structure of power communication network.

3.3.1. Overall structure and Concept of the Detection Method. Logically speaking, each layer of the power communication network contains the MDMS system. Based on the MDMS storage and detection mechanism, a smart grid NTL detection model based on the power gateway consortium blockchain is proposed. The structure of the detection model is shown in Figure 3.

The overall power communication network model includes three parts: the blockchain network, the power gateway, and the smart meter. The communication network includes three network domains, home network, local area network, and wide-area network. The local area network and the wide-area network contain alliance blockchains, which are, respectively, LAN network consortium blockchain and WAN network consortium blockchain. The WAN network consortium blockchain and the LAN network consortium blockchain combine MDMS to manage and control the data of power gateway devices and smart meters, including two parts: device information data and hierarchical power information data.

Equipment Information Collection Task Business. The WAN network consortium blockchain and the LAN network consortium blockchain are combined with the MDMS system to store and manage device information on the chain. The LAN network consortium blockchain forms the MDMS system through the HAN power gateway node to provide device information data query and storage services. The LAN network consortium blockchain collects the state information of the smart meter through the power gateway and stores it in the LAN network consortium blockchain. Similarly, the LAN power gateway is a node of the WAN network consortium blockchain and stores the device status information of the LAN gateway in the WAN network consortium blockchain.

Hierarchical Power Information Collection Task. WAN network consortium blockchain and the LAN network consortium blockchain combine with the MDMS system to store and manage hierarchical power information on the chain. The hierarchical power information includes user payment information, smart meter power information, HAN power gateway power information, and LAN power gateway power information. Among them, the user payment information and power information are uploaded to the LAN network alliance blockchain storage management through the smart meter and the HAN power gateway node power information through the HAN power gateway node. The LAN power gateway power information is stored and managed in the WAN network consortium blockchain through the LAN power gateway node.

Block Structure. The block structure includes the block head and the block body. The block header includes a block identification number, a block size, a timestamp, an address number, and a Merkle root. The block includes equipment information, power information, and source address (smart meter ID, power gateway ID). The specific block structure is shown in Figure 4.

Data Content. The data in the WAN network consortium blockchain includes WAN network layer input power, LAN power gateway ID, timestamp, LAN power gateway equipment power consumption, and device status. The data in the LAN network consortium blockchain includes HAN power gateway output power, HAN power gateway ID, timestamp (including power purchase time, transaction processing time, and power start reading time), smart meter ID, household name, remaining power, purchase power and purchase time, smart meter public, and private key pairs.

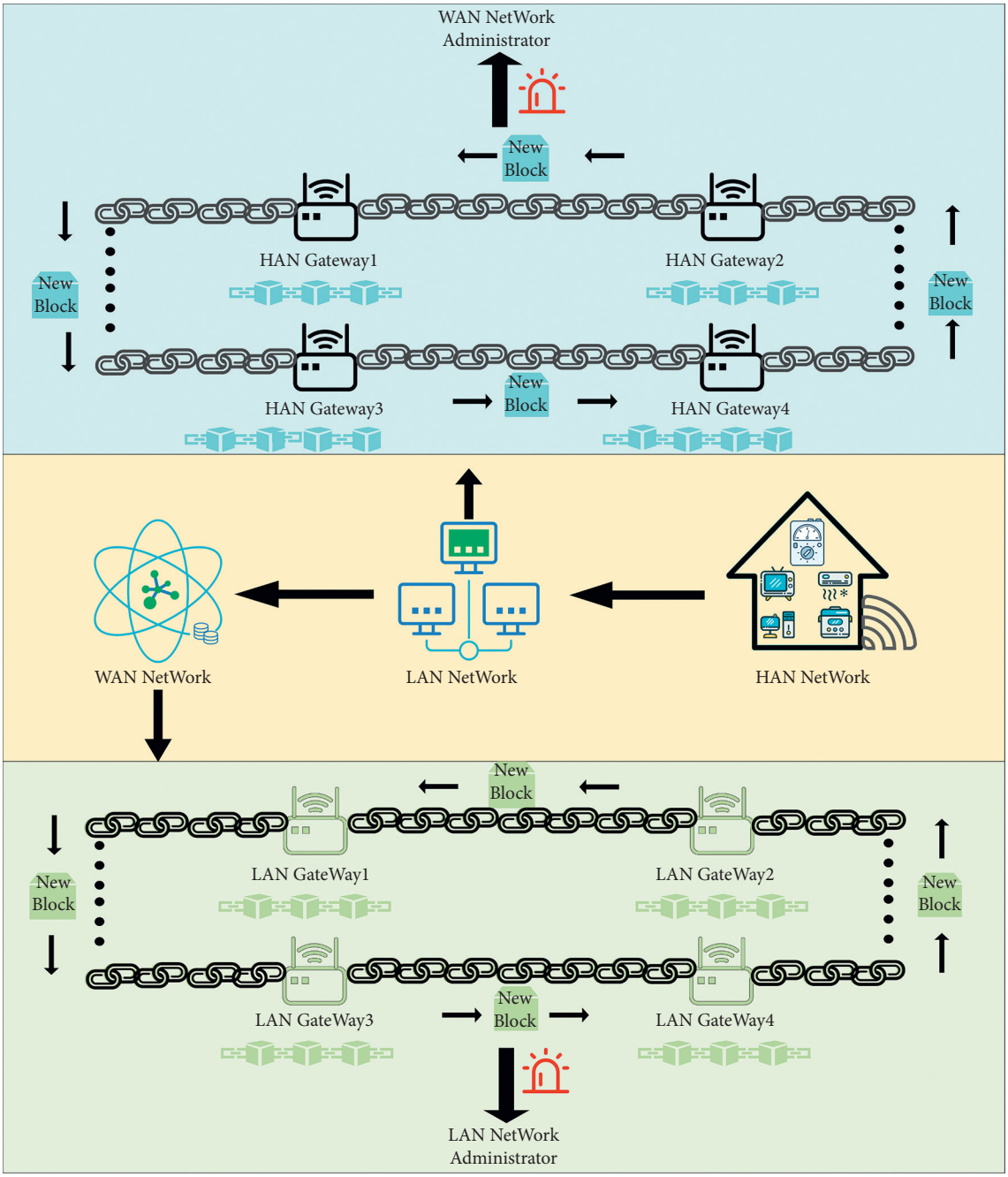

Figure 3: Smart grid NTL detection model based on power gateway consortium blockchain.

Raft Consensus. In Fabric, the orderer service based on Raft replaces the previous Kafka orderer service. Generally, a Raft cluster includes $2N+1$ orderer nodes, allowing N faulty serves in the network. In raft, each node can only be in one of three states [24, 25]:

Follower: in the initial situation, all nodes are followers
Leader: responsible for processing client requests and ensuring that all followers have the same data records
Candidate: candidates will initiate elections to compete for leaders

Under certain conditions, the state of a node can be transformed. In the initial situation, all nodes are followers. Since there is no message from the leader within a period of time, the follower will automatically transform into a candidate and initiate a vote. After receiving votes from most nodes, the node will transform into a leader, accept and respond to requests from clients. For example, when the leader receives an information storage request from the client (HAN Gateways) in the LAN alliance chain, the leader will broadcast this request to the followers. A response will be sent if the follower receives the request successfully. When the leader receives responses from more than half of

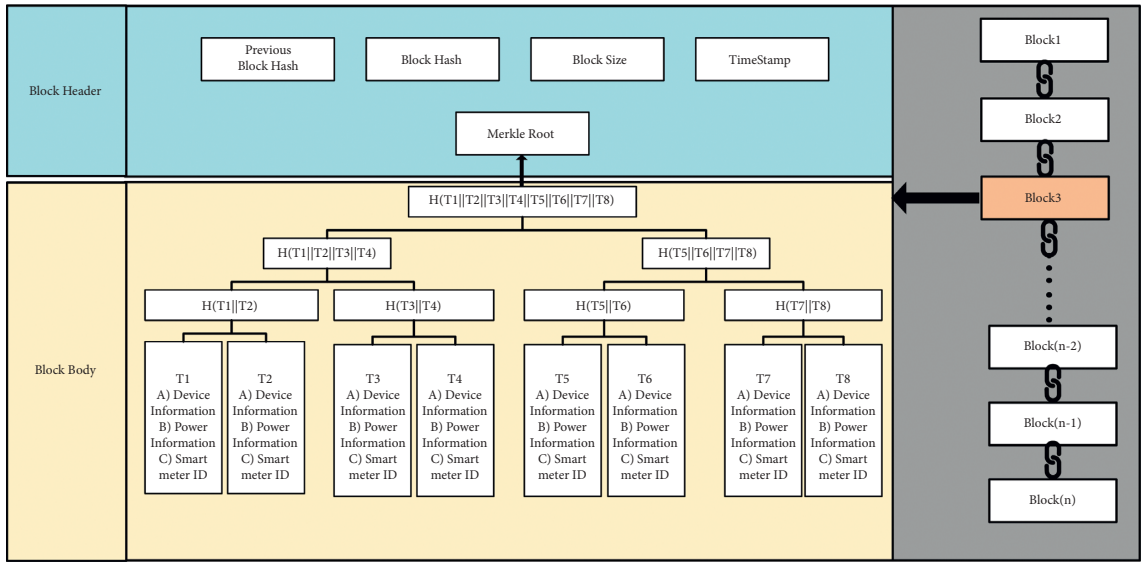

Figure 4: Structure of block data.

the nodes, it will submit the request locally and broadcast all followers to execute the request. The follower accepts and verifies whether the request is legal; after that, the request will be packaged to generate a block, broadcast to all HAN Gateways, and written into the local ledger.

The overall structure takes the form of an alliance blockchain, which is a special blockchain, based on a certain number of preselected authentication nodes. The consensus algorithm of the blockchain is performed by these preselected nodes instead of all the nodes in the whole network, which can greatly reduce the network overhead. In the power grid system, different regions can be regarded as different alliances, so that they can be autonomously managed, and the information can be shared within the scope. The power consumption statistics equipment (smart meter) in the power grid is detected by HAN and LAN power gateway, and the monitoring data are collected and stored. As the real-time detection and audit consume much calculation and storage, a conditional trigger is used to detect the behavior trigger. The introduction of the threat model triggers the detection mechanism when the following methods are employed in the NTL problem detection process of the smart grid.

3.3.2. Initialization and Registration

Assumption 1. The power blockchain gateway is trusted. The audit terminals in the MDMS system deployed by the alliance chain are also trusted.

Assumption 2. The smart meter is semitrusted, and the user is not trusted. The communication channel between the intelligent meter and the power gateway is not completely secure.

Assumption 1 specifies that the gateway of the power blockchain is trustworthy. The power gateway generates certificates and private keys for the intelligent watt-hour meter. This information is stored in the power gateway to ensure that the information is secure and will not be stolen or tampered with. As the audit client in the federation chain MDMS, the audit terminal is also credible, which makes the audit results accurate.

For Assumption 2, the smart meter is a semitrusted entity; it will not actively tamper with and steal information but will be subject to passive attacks. Users are untrusted by default, and such entities are highly aggressive.

The symbols and descriptions used in the whole process are shown in Table 2. The low-power encryption scheme is very important in the Internet of things [26, 27]. The key process of the model is as follows:

System Initialization. The symbol definitions used in the detection method are shown in Table 2.

The system selects an elliptic curve E: $y^2 = x^3 + ax + b \pmod{n}$. The generator is P, and the following three hash function operations are selected. H_1: $\{0,1\}* \longrightarrow G$; H_2: $\{0,1\}* \longrightarrow \{0,1\}*$; H_3: $G \longrightarrow \{0,1\}*$. The private key of the power gateway is α and its public key is $p_a = \alpha * P$.

Smart Meter Information Registration Process. HAN network users request access to smart meters from HAN power gateway nodes through the communication network. Access is allowed if authentication is passed, and access is denied if the authentication fails. The HAN power gateway combines the information of smart meter and house number to generate the unique identification number in the current HAN network. All the smart meter identification number information in the HAN network is stored in the HAN gateway. When the NTL occurs, the HAN gateway can be responsible for the smart meter with NTL problems according to the identification number information. Since the smart meter as a client needs to sign when it needs to submit to blockchain request to the HAN gateway, the HAN gateway needs to generate a public and private key pair for the smart meter and send

Table 2: Notations used in this paper.

Symbol	Description
P	Generator
E	Elliptic curve
(α, p_a)	Private key and public key of power gateway
SM_{id}	ID of smart meter
Q_{SM}	Certificate of smart meter
$PSK_{SM_{id}}$	Private key of smart meter
(r_a, y_a)	One-time password power gateway private key, public key
(r_s, Y_s)	One-time password smart meter private key, public key
M	Data uploaded by smart meter
T_i	Time stamp
H_1, H_2, H_3	Hash operation
(r_b, y_b)	Audit client's private key, public key

the private key to the smart meter for signature. The specific process is shown in Figure 5.

The smart meter has a unique ID for SMid, for the power gateway to issue a certificate for it, as follows:

Step 1: smart meter generates random number k_i as its private key, $k_i \in [1, n-1]$

Step 2: smart meter sends (k_i, SM_{id}) to power gateway for the later generation of certificates

Step 3: the power gateway calculates its certificate $Q_{sm} = \alpha * k_i * P$, to further update its private key to $PSK_{SM_{id}} = \alpha * k_i + H_3(Q_{sm}) * \alpha$

Step 4: the power gateway will return $(Q_{sm}, PSK_{SM_{id}}, t_i)$ to the smart meter is $(certificate, privatekey, timestamp)$

3.3.3. Data Storage and Query Process. The nodes of the LAN network consortium blockchain and WAN network consortium blockchain are in the HAN power gateway and the LAN power gateway, respectively, and they are responsible for the client to submit data information to the blockchain. The process is shown in Figure 6.

The smart meter signs and uploads the data, and the process is mainly divided into four steps: one-time password generation, message signature, identity verification, and message verification.

In order to ensure the security of the data, the one-time password is used every time the smart meter uploads the data, and the generation process is as follows:

Step 1: the power gateway generates a random number r_a and sends it to the smart meter

Step 2: the smart meter randomly selects r_s as its private key and calculates its public key as $y_s = r_a * r_s * Q_{SM}$

Step 3: the power gateway uses its private key α to generate a public key of $y_a = H_2(r_a) \oplus H_3(\alpha * y_s)$

As the smart meter is a semitrusted entity, when generating the public key, the public key value is determined by both the power gateway and the smart meter.

The smart meter signature process for uploading data:

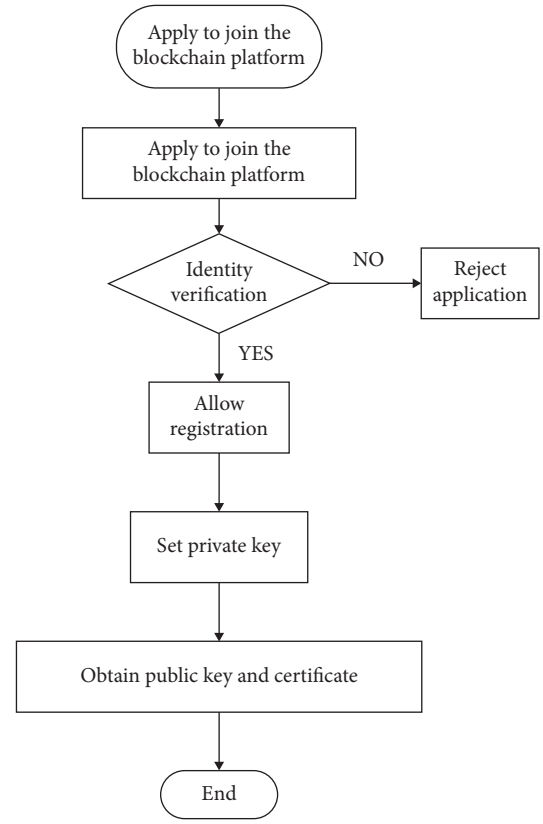

Figure 5: Smart meter information registration process.

Step 1: firstly, the private key $PSK_{SM_{id}}$ issued by the power gateway node is used to sign the uploaded data: $sign(M) = H_2(M, SM_{id}, y_s, t_i) * r_s + PSK_{SM_{id}}$.

Step 2: the smart meter will upload the data $msg = (SM_{id}, sign(M), y_s, M, t_i, Q_{sm}, \backslash\backslash H_2(r_a))$ to the power gateway. It is easy to verify the identity of the smart meter. If the transmission channel is eavesdropped or tampered with, the power gateway can determine whether the message has been tampered with according to the signature $\text{sign}(M)$.

The authentication process of the power gateway to the smart meter is as follows:

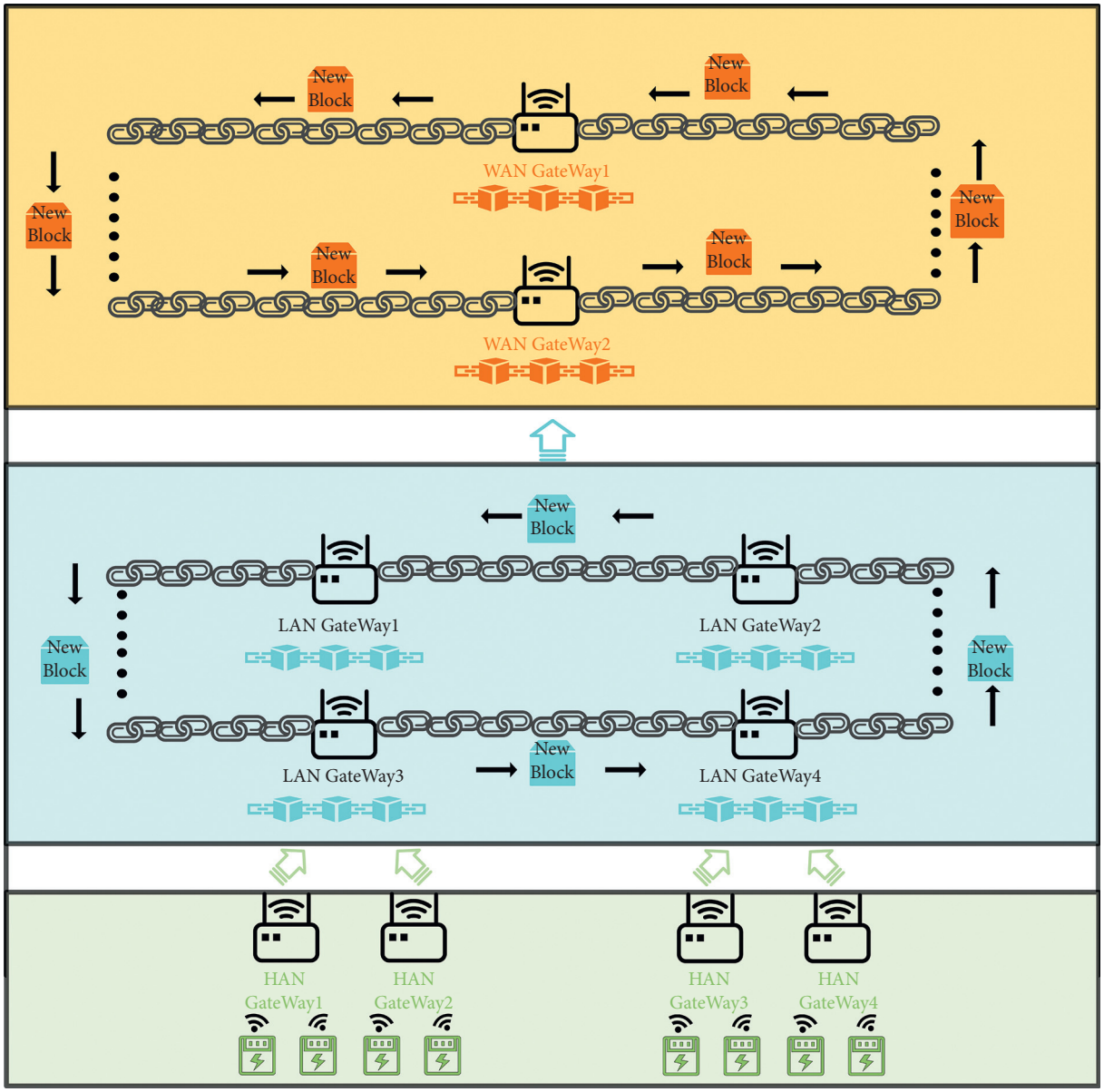

Figure 6: Data block generation process.

In the case that the Q_{sm} verification is passed, to prevent the certificate from being eavesdropped on by an adversary, further judge $H_2(r_a) = y_a \oplus H_3(\alpha * y_s)$. It ensures that the message cannot be tampered with.

The power gateway verifies the message sent by the intelligent meter as follows:

First, calculate the $h_1 = H_2(M, SM_{id}, y_s, t_i) * r_s$; $h_2 = H_3(Q_{sm})$. Determine whether the equation $sign(M) * P = h_1 * y_s + Q_{sm} + h_2 * p_a$ is true, and if so, receive the message.

The verification principle is as follows:

$$\begin{aligned} sign(M) * P &= \left(H_2(M, SM_{id}, y_s, t_i) * r_s + PSK_{SM_{id}}\right) * P \\ &= h_1 * y_s + \alpha * k_i * P + h_2 * P \\ &= h_1 * y_s + Q_{sm} + h_2 * p_a. \end{aligned} \tag{1}$$

The above is a single message authentication process. If batch message processing is carried out and the number of messages is assumed to be n, the verification process is as follows:

$$\begin{aligned} SP &= \sum_{i=1}^{n} sign_i(M_i) * P \\ &= \sum_{i=1}^{n} \left(h_1 + PSK_{SM_{id}}\right) * P \\ &= \sum_{i=1}^{n} h_1 * P + \sum_{i=1}^{n} [\alpha * k_i + H_3(Q_{SM} * \alpha)] * P \\ &= \sum_{i=1}^{n} h_1 * P + \sum_{i=1}^{n} Q_{sm} + \sum_{i=1}^{n} h_2 * p_a. \end{aligned} \tag{2}$$

The HAN power gateway node stores the collected smart meter data (HAN network layer data) on the LAN network consortium blockchain, and the LAN power gateway node stores the aggregated LAN network layer data on the WAN network consortium blockchain. The data is stored in an encrypted manner, and the way the data is stored on the blockchain and obtained is shown in Figure 7.

After obtaining the data, the power gateway node encrypts the data through the encryption algorithm, stores it on the chain, and decrypts the query in the process of detection and audit.

The audit client audits the data uploaded by the smart meter, and the process is as follows: as the audit client and the power gateway are trusted entities, both parties can use the original elliptic curve encryption algorithm when transmitting data:

Step 1: the audit client chooses the private key as r_b; then, its public key is $y_b = r_b * P$

Step 2: the power gateway hashes the data m to be audited: $M = H_1(m)$, randomly generates r, and calculates the point $R = r * P$

Step 3: the power gateway calculates $C = M + r * y_b$ and returns the (C, R) to the auditor

Step 4: fter the audit client gets the ciphertext C, calculate the plaintext $M = C - r * y_b = C - r * r_b * P = C - R * r_b$ and audit it

3.3.4. NTL Detection Method. The HAN user initiates the power purchase on the platform, and the user sends the verification information $HANPurchaseInfo = \{UserID, SMID, Purchaseamount, TimeStamp\}$ to the platform for verification. After the verification is passed, the audit contract of the detection mechanism is triggered, as shown in Figure 8.

The steps for the audit contract are as follows and the process is shown in Algorithm 1:

Step 1: HAN tests the connectivity of the smart meter (obtaining the meter status data), performs Step 2 if the test is successful, and issue an alarm to the auditor if the test fails.

Step 2: the HAN gateway node sends a request for information collection to the smart meter of the power buyer.

Step 3: if the smart meter receives the request information, it responds to the request of the HAN gateway node and transmits the $HANsm = \{SMID, UserID, Remaining\ Electricity\}$ information to the HAN power gateway node.

Step 4: the HAN power gateway node obtains the $HAN\ gw = \{SMID, UserID, CurrentTime,\ the user's\ last\ power\ purchase\ time\ (Tlast), after\ the\ electricity\ purchase\ (Elast)\}$ information, which is compared and fused with the HANsm information. We calculate the difference between the (*Elast*) and the remaining power of the watt-hour meter after the last power purchase and compare it with the output electricity of the HAN gateway (the electricity information between the last purchase time and the current purchase time). We judge whether the charging users and other users under the current HAN power gateway node have abnormal power consumption.

Step 5: After the verification is passed, $HANgw1 = \{SMID, UserID, CurrentTime, PurchaseTime,\ after\ purchased\ electricity\ (ATE)\}$ is packaged and uploaded. At the same time, the platform will send the purchased electricity to the smart meter of the family.

(1) NTL Detection Method for HAN Network. Aiming for the problem of passive malicious user detection, a HAN network NTL detection method is proposed based on The NTL detection method. Every once in a while, the HAN gateway will query the data on the chain, request the data of the smart meter, then calculate the theoretical power consumption of each smart meter under the current HAN network, and after that compare it with the actual output power EOutput of each user's HAN gateway. If the actual output power is greater than the theoretical power consumption, the user is considered to be a passive malicious user. The process is shown in Algorithm 2.

(2) NTL Detection Method for LAN Network. The WAN network layer regularly audits LAN users following the audit rules. The WAN network initiates a regular audit of the power output of the LAN power gateway to audit whether the WAN input and the LAN output are balanced. According to the audit results, it is to judge whether the LAN group users have NTL problems. The process is shown in Algorithm 3.

After the WAN network carries out the connectivity test to the gateway node (obtains the equipment state data), every interval T triggers the audit contract; in other words, it carries out the query about the WAN gateway node information stored in the LAN consortium blockchain. The input power data of the WAN network is obtained and compared with the LAN node data to determine whether there is a problem with LAN group user NTL. If there is a problem, the auditor is alerted.

4. Experimental Simulation

We have carried out experiments on the proposed smart grid NTL detection scheme based on the power network association chain and simulated the data winding and the detection process of the LAN alliance chain, including HAN users (smart meter), the alliance chain composed of the HAN gateway, and the detection client. The structure of the experiment is shown in Figure 9.

4.1. Experimental Environment. The Docker is used to simulate peers on the blockchain to verify our scheme. The OS used is Ubuntu 18.04, and the version of the Hyperledger Fabric is 2.3.0. More details for the experimental environment are listed in Table 3.

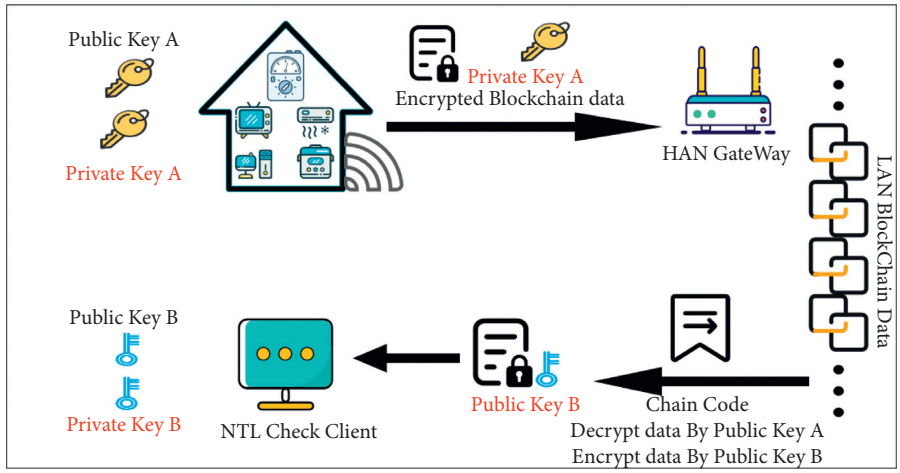

Figure 7: Data storage and acquisition process.

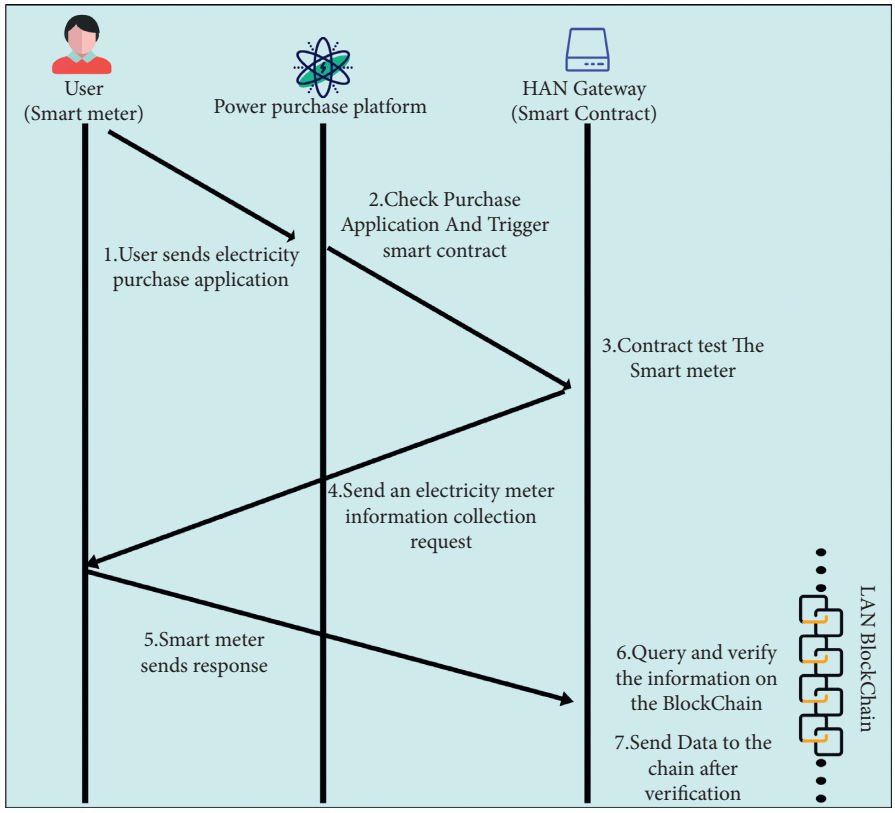

Figure 8: NTL detection method.

For the LAN alliance chain, the blockchain network consists of two Orgs, each of which has fifteen peers (HAN Gateways). The peer0 of each Org serves as the anchor node of its own Org and is responsible for the communication between organizations. There is one channel in the network; all peers will install the chain code and join the channel.

4.2. Experimental Result. The main steps of the experiment include the creation and maintenance of the channel, the development, and the use of the chain code. The administrator is responsible for adding HAN Gateways and LAN Gateways to their corresponding channels, developing and deploying chain code, and fulfilling other requirements. The blockchain network function test and the Smart Grid data interaction function test are shown in Tables 4 and 5, which mainly include storing and querying the gateway power date.

We tested a network with two Orgs, and four HAN Gateways per Org. The test results are shown in Figures 10 and 11. The results show that the processing capacity of the LAN blockchain network reaches the peak when four HAN Gateways initiate transactions at the same time.

Input: HANpurchaseInfo = {UserID, SMID, Purchase amount, TimeStamp}
Output: Audit Result
(1) **function** NTL(HANpurchaseInfo)
(2) get the state of the Smart Meter
(3) **if** State = offline **then**
(4) **return** Send warning to Auditors
(5) **else**
(6) Send request to the corresponding Smart Meter
(7) get HANsm = {SMID, UserID, SOC} sent from Smart Meter
(8) get HANgw = {SMID, UserID, Current Time, Tlast,Elast} from HAN
(9) **if** (Elast-SOC)-E_Output > threshold **then**
(10) **return** Send warning to Auditors
(11) **else**
(12) Purchasing Time = TimeStamp
(13) SOC = SOC + Purchase amount
(14) send HANgw1 = {SMID, UserID, Current Time, Purchasing Time, ATE} to BlockChain
(15) send update to user's smart meter
(16) **return** Normal
(17) **end if**
(18) **end if**
(19) **end function**

Algorithm 1: Contract for audit.

Input: TIME INTERVAL
Output: Analysis Result
(1) **function** NTL FOR HAN
(2) **if** Current Time-Last Time = TIME INTERVAL **then**
(3) **for** $i = 0 \longrightarrow n$ **do**
(4) get HANsm = {SMID, UserID, SOC} sent from $User_i$'s Smart Meter
(5) get HANgw = {SMID, UserID, Current Time, Tlast,Elast} from HAN
(6) E_Theoretical_Consumption = Elast-SOC
(7) get E_Output from HAN
(8) **if** E_Output > E_Theoretical_Consumption **then**
(9) Send warning to Auditors
(10) **end if**
(11) **end for**
(12) **return** over
(13) **end if**
(14) **return** waiting
(15) **end function**

Algorithm 2: NTL for HAN.

Instead of controlling the peers, join the channel one by one; we join all the peers into the channel at the same time and then control the number of peers that initiate transactions at the same time.

In the LAN alliance chain, different numbers of HAN Gateways initiate transactions at the same time for different total transactions. The results include the time consumption and throughput referring to the number of transactions that can be processed per second. Figure 12 shows the relationship between the time required to complete the transaction and the number of HAN Gateways needed to initiate the transaction. Figure 13 shows the relationship between the throughput and the number of HAN Gateways needed to initiate the transaction at the same time. It can be seen that, with the increase in the number of HAN Gateways participating in the transaction, the processing capacity of the LAN alliance chain network continues to increase and eventually stabilizes. When three HAN Gateways initiate transactions at the same time, the maximum processing capacity of the LAN network is achieved. It can be seen that, in application, we only need a small number of nodes to make full use of the blockchain network; thus, we can save our costs.

It is worth noting that the throughput of the blockchain is affected by many factors, including but not limited to system architecture, hardware, and consensus algorithm.

Input: TIME INTERVAL
Output: Analysis Result
(1) **function** NTL FOR LAN
(2) get the state of LAN
(3) **if** State = offline **then**
(4) **return** Send warning to Auditors
(5) **else**
(6) **if** Current Time-Last Time = TIME INTERVAL **then**
(7) **for** $i = 0 \longrightarrow n$ **do**
(8) get LAN1 = {LANID, SOC} sent from LAN_i
(9) get LAN2 = {LANID, Elast} from WAN
(10) E_Theoretical_Consumption = Elast-ATE
(11) get E_Output from WAN
(12) **if** E_Output > E_Theoretical_Consumption **then**
(13) Send warning to Auditors
(14) **end if**
(15) **end for**
(16) **return** over
(17) **end if**
(18) **return** waiting
(19) **end if**
(20) **end function**

Algorithm 3: NTL for LAN.

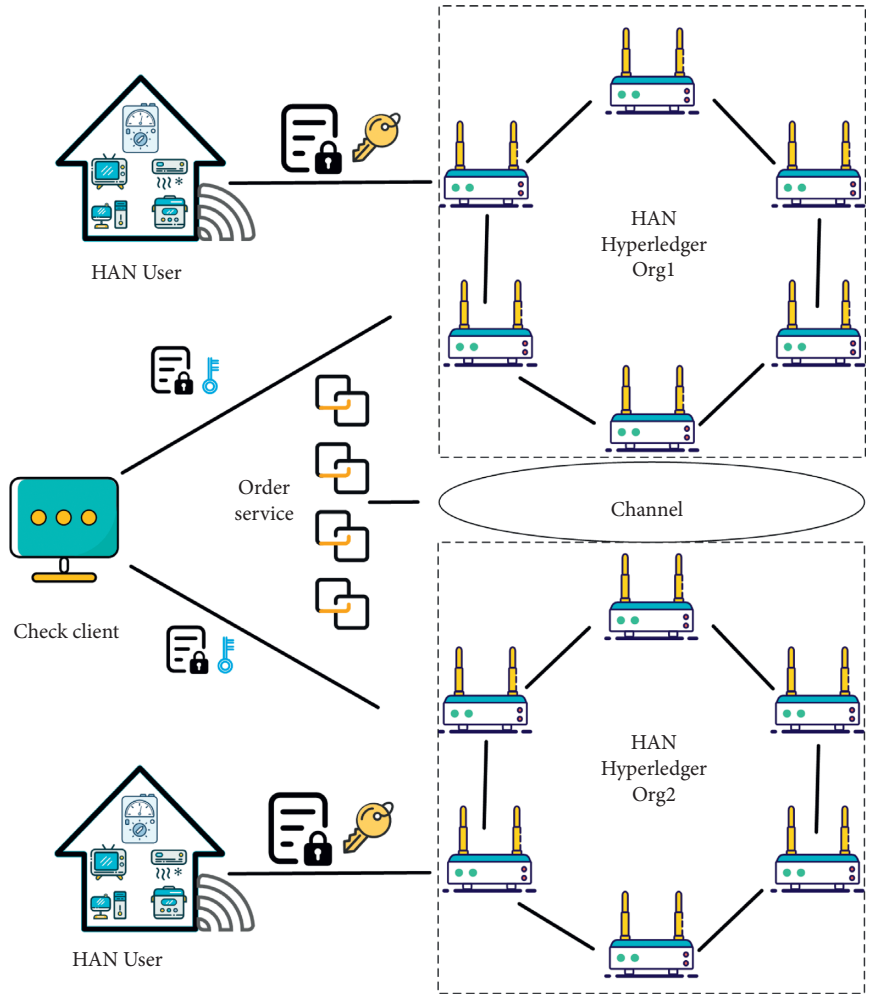

Figure 9: Experimental environment.

Table 3: Experimental environment.

Tools	Version	Function
Ubuntu	18.04	The operating system
Hyperledger Fabric	2.3.0	An open-source alliance chain framework for generating blockchain network
Docker	19.03.6	Used to simulate peers in blockchain
Docker-compose	1.17.1	Manage container
Go	1.15.7	Develop chain code (smart contract)

Table 4: Blockchain network function test.

Function	Explanation	Result
Create channel	Create channels for LAN or WAN alliance chain	Success
Join channel	Add HAN Gateways and LAN Gateways to their corresponding channels	Success
Deploy chain code	Install chain code on the channel	Success
Invoke chain code	Execute the function defined on the chain code	Success

Table 5: Blockchain network function test.

Function	Explanation	Result
Power data storage	Upload power data to blockchain	Success
Power data query	Query the power data from blockchain	Success

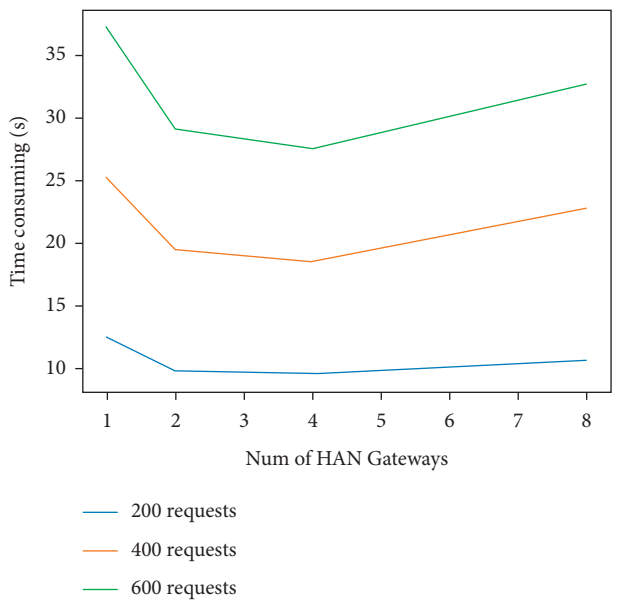

Figure 10: Time consumption for different numbers of transactions and HAN Gateways (four nodes).

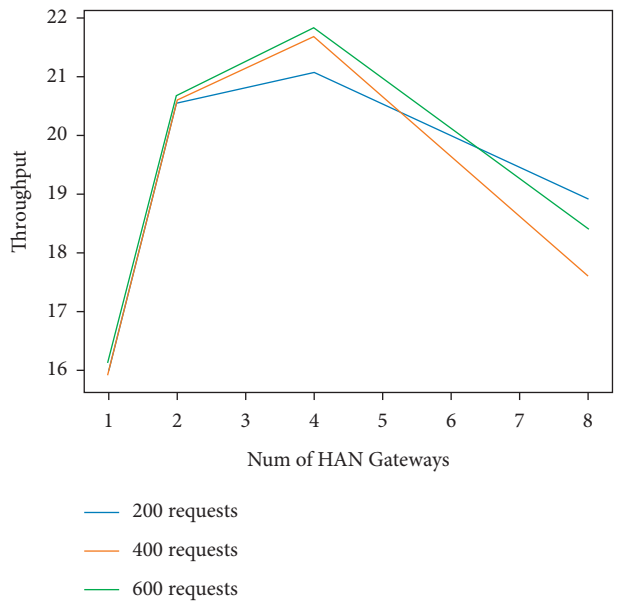

Figure 11: Throughput for different numbers of transactions and HAN Gateways (four nodes).

The number of peers needs to be appropriately set according to the application of the scenario.

To further verify the feasibility of the scheme, the dataset [28] from Smart Energy Informatics Lab was selected. The dataset consists of electricity consumption data (December 2016 to January 2018) from a high-rise residential building inside the IIT Bombay campus. Each apartment is instrumented with a smart meter. For privacy reasons, the name of apartments are kept anonymous and are replaced by numbers. The date is downsampled at 1-hour granularity. It includes apartment ID, timestamp, voltage, and energy consumption.

The results are as shown in Figures 14 and 15, similar to previous results, the processing capacity of the LAN alliance chain network continues to increase and eventually stabilizes with the increase in the number of HAN Gateways participating in the transaction.

To our best, only one similar paper is found. Khalid et al. [29] tried to combine the IoT device with blockchain to eliminate nontechnical loss. The IoT devices are deployed at

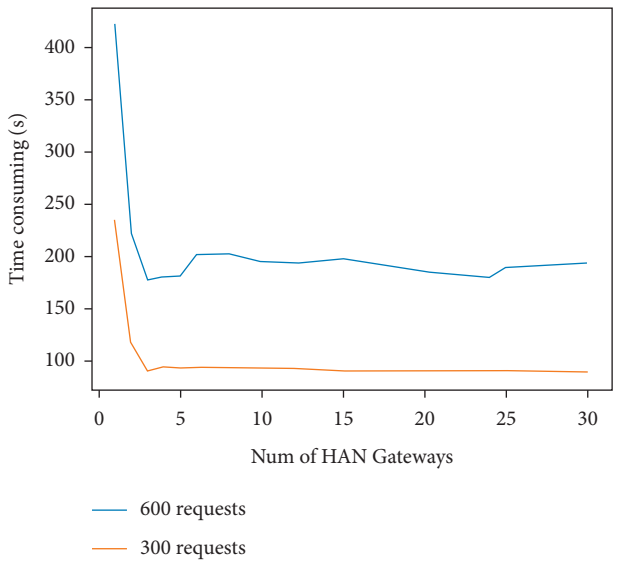

Figure 12: Time consumed for different numbers of transactions and HAN Gateways (fifteen nodes).

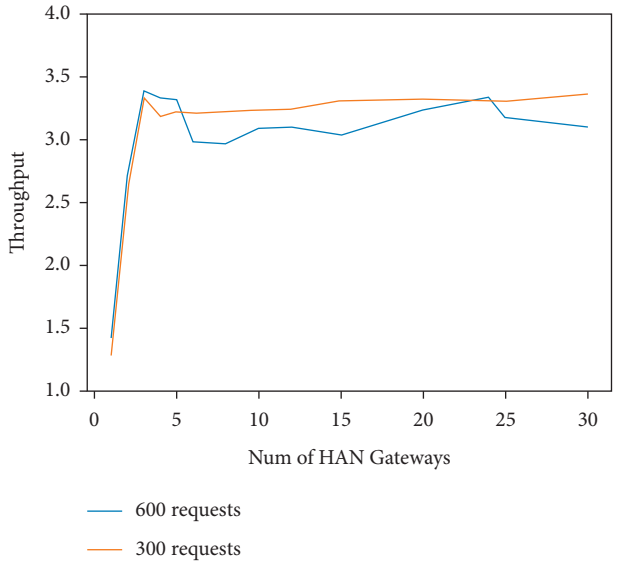

Figure 13: Throughput for different numbers of transactions and HAN Gateways (fifteen nodes).

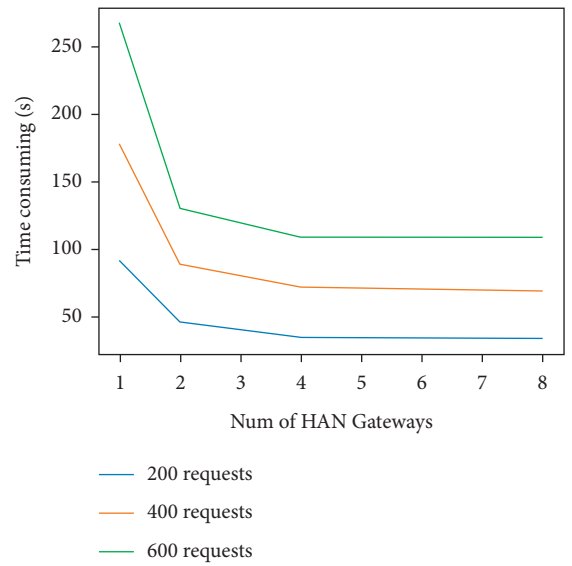

Figure 14: Time consumed for different numbers of transactions and HAN Gateways (four nodes).

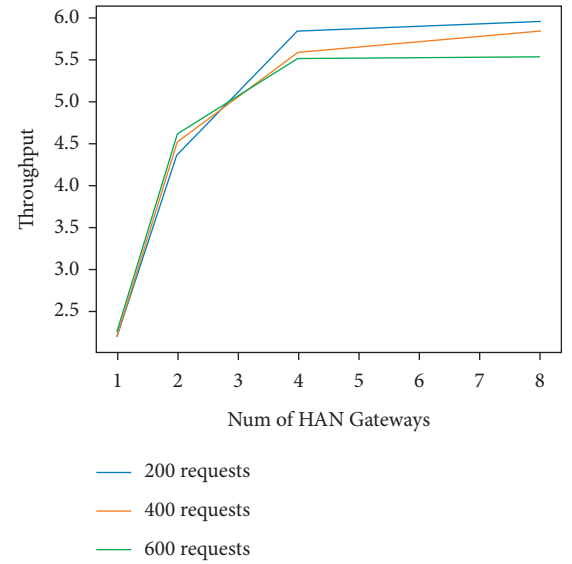

Figure 15: Throughput for different numbers of transactions and HAN Gateways (four nodes).

the key point of the power system to detect electricity production and consumption. The nontechnical loss is detected by calculating the difference between production and consumption. Ethereum is used to verify this scheme finally.

For consumers of different sizes, Sana designed different solutions. Private chains, alliance chains, and public chains are used to target large-scale, medium-scale, and small-scale consumers, respectively. This indeed improves the throughput of the blockchain, but there is little improvement in NTL detection. The scheme proposed in our work is based on Fabric which also is known as alliance chain. Although the private chain has a high throughput, the peers in the private chain are required to be mutually trustworthy, which is impossible in the actual situation. Compared with the private chain, the alliance chain is more in line with the actual situation. This is because the nodes in the alliance chain only need to be semitrusted between others. However, this paper only offers the results of the successful execution of smart contracts and blockchain; it does not offer the performance results.

What is more, large-scale IoT devices are needed to be installed to find specific users who stole electricity which will result in high costs. However, the hierarchical structure proposed in our paper allow us to locate users who stole electricity more conveniently and flexibly based on existing power supply equipment. By analyzing the data from different HANs and LANs in their respective

blockchain networks, we can effectively solve the problems of single-user power theft and group user power theft.

4.3. Qualitative Analysis of the Results. In this section, we will discuss the differences between the design scheme of this paper and other existing schemes in each index dimension, which mainly includes the following eight index dimensions. The first dimension is the detection effectiveness of NTL, and the second dimension is to judge whether it has the characteristics of decentralization, which can avoid the single point of failure and other problems. The third dimension is the data tamper-proof; because this paper uses the blockchain structure, it has the antitamper ability of data. The fourth dimension is the intelligent detection capability, which mainly examines whether the detection scheme can be carried out without the need for manual table lookup, to reduce the labor cost. All the detection processes in this paper can be automatically carried out by the intelligent contract; thus, there is no need for any manual table lookup. The fifth dimension is the ability of information sharing, which mainly refers to the ability of data sharing between nodes. In this paper, due to the use of blockchain mechanism, different nodes achieve data consistency through the consensus mechanism. The sixth dimension is the confidentiality of the data. All the upper-chain information in this paper is ciphertext so that the data can be effectively protected. The seventh dimension is the traceability and auditability of the data; because all the power equipment information and the power purchase information are stored on the chain, the power purchase behavior can be traced back and audited. The eighth dimension is independent of audit data; because the detection process in this paper is to trigger intelligent contracts for detection, there is no need to train datasets for learning; thus, it is not dependent on large audit data.

Based on the eight indicators previously pointed out earlier, our work is compared with other existing works, and the results are shown in Table 6.

5. Security Analysis

In this section, the security of the proposed method is analyzed from the aspects of smart meter information initialization, data authentication, block verification, and threat scenario.

5.1. Smart Meter Information Initialization. The smart meter, as a client, needs to be signed when submitting a chain request to the HAN gateway; therefore, the HAN gateway needs to generate a public-private key pair for the smart meter and send the private key to the smart meter as a signature. The HAN gateway uses a hash algorithm and a random number generator to generate public and private key pairs. Although the random number generator is built randomly by man, it can be exploited by attackers. The hash algorithm provides a more secure method. The SM public key information is a blockchain created based on the Merkle tree and timestamp using a hash function and is stored in the HAN gateway to keep it safe during the initialization phase of the smart meter.

5.2. Data Authentication Security. The data is stored on the permissioned blockchain through encryption. After the HAN gateway obtains the smart meter data, it encrypts the user's meter data through an encryption algorithm and stores it on the blockchain. When SM communicates with the HAN gateway, they create a secure session and update the private key pairs at intervals of time t. When the HAN gateway initiates a request and receives a message encrypted with the private key by the SM, as the leader, it uses the SM public key to verify the signature of the encrypted data. The authentication security and the integrity of data transmission are ensured by means of private key pairs verification.

5.3. Block Verification Security. The security of block verification in the scheme is guaranteed by the Raft algorithm. The MDMS in the designed smart grid is a distributed system, in which the failure of a single gateway is an independent event. Assume that there are n HAN Gateways in a LAN alliance chain, where the number of faulty nodes is f. As the election of the leader is based on voting in raft, we need to ensure that the number of normal nodes is greater than the faulty nodes to guarantee the voting process. Therefore, we need $n - f > f$, which leads to $n > 2f$. Then, we need to ensure that there are at least $2f + 1$ nodes in the system to ensure the security of the distributed system.

5.4. Security Analysis of Threat Scenario

(1) Active Malicious User Threat Analysis. As the active malicious user will carry out the charging behavior, it will trigger the NTL detection method mentioned above. After the request of the active malicious user passes the platform verification and the active malicious user's electricity meter passes the subsequent connectivity test, the HAN gateway will collect the information from the user's smart meter HAMsm: smart meter ID, UserID, remaining power (ERemain), and then the HAN gateway will query the information on the chain to obtain the user's last charging information HANgw: $\{smartmeterID,\ UserID,\ currenttime,\ user's\ last\ purchase\ time\ (Tlast),\ after\ the\ meter\ (ELast)\}$. Combined with HANsm, the difference between the quantity of (ELast) and the remaining power of the meter after the last purchase is calculated to get the theoretical power consumption E_Theoretical_Consumption = (ELast-ERemain) and compared with the actual output of the HAN gateway (electricity information between the last purchase time and the current purchase time).

Since the active malicious user has the behavior of stealing electricity, the E_Output is greater than E_Theoretical_Consumption, and the difference between the two

Table 6: Comparison between the proposed method and other related methods.

Metric	[9]	[6]	[30]	[11]	[31]	[20]	Our method
Detection of NTL	Yes	Yes	Yes	Yes	No	Yes	Yes
Decentralization	No	No	No	No	Yes	Yes	Yes
Data tamperproof	No	No	No	No	Yes	Yes	Yes
Intelligent detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Information sharing	No	No	No	No	Yes	Yes	Yes
Data confidentiality	No	No	No	No	No	No	Yes
Data traceability and audit	No	No	No	No	Yes	Yes	Yes
Nonaudit data reliance	Yes	Yes	No	No	Yes	Yes	Yes

represents the malicious degree of the malicious user. The more the number of power theft, the higher the malicious degree. At this time, an alarm of electricity theft will be made to the LAN power network administrator and be dealt with according to the degree of malice.

(2) Passive Malicious User Threat Analysis. Passive malicious users do not charge, so regular NTL detection methods cannot be triggered. However, this paper introduces the NTL detection method of the HAN network, and every once in a while, the HAN gateway will query the data on the chain, request the data of the smart meter, then calculate the theoretical power consumption E_Theoretical_Consumption, of each smart meter under the current HAN network, and compare it with the actual output power E_Output of each user's HAN gateway. If the actual output power is greater than the theoretical power consumption, the user is considered to be a passive malicious user. And because the HAN network node in this paper separately maintains the blockchain data structure for each user, compared with maintaining a blockchain data structure, the query data amount of this scheme is smaller; thus, it is more efficient.

(3) Group Malicious User Threat Analysis. At present, the LAN network NTL detection method and the HAN network NTL detection method proposed in this paper can effectively solve the threat of malicious users of this group. The difference between the LAN network NTL detection method and the HAN network NTL detection method mainly lies in the different content of the blockchain data. The block data of the LAN network chain records the power purchase information in the unit of the user, while the block data of the WAN network chain records the power purchase information in the unit of the region, and each LAN power gateway represents an area. Therefore, the group of malicious users can be classified as the different malicious area.

6. Conclusion

In this paper, we propose a smart grid NTL problem detection scheme based on the power gateway blockchain to solve the NTL problem in the smart grid system. Our scheme divides the communication network domains such as HAN, LAN, and WAN in the smart grid. A hierarchical power grid gateway blockchain is proposed and designed, and a decentralized management MDMS system is constructed. Without the support of a large amount of data, the intelligent contract combined with encryption technology is used to store and query the power data, and the detection of NTL problems is realized. First of all, the overall structure of the consortium blockchain of the smart grid gateway is described. Secondly, the threat scenarios of NTL problems in the smart grid are analyzed. Finally, a smart grid NTL detection model based on the power grid association consortium blockchain is proposed. The model uses the edge network blockchain to store the state information of smart meter, power gateway, and related power data. In the model, the data situation in the smart grid, and the data winding and query process in the smart grid are described in detail. The trigger mechanism and the detailed detection flow of the NTL detection method are introduced, and a smart contract is written to ensure the safe and reliable operation of the detection scheme. It has a certain ability to resist attacks such as replay, monitoring, and tampering. It is worth noting that the throughput and the consumed time of the blockchain are affected by many factors. The number of peers needs to be reasonably set according to the application in the scenario. After testing the performance of the scheme, it is proved that it is theoretically feasible. In the future, we will expand our work to optimize the efficiency of the consensus algorithm and to refine the trigger conditions of the detection mechanism to improve the practical feasibility of the scheme.

Data Availability

The dataset used in this manuscript belongs to synthetic data. The synthetic data used to support the findings of this study are available from the corresponding author upon request. There are no restrictions on access to the synthetic datasets.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Fundamental Research Funds for the Central Universities (2019YJS033) in China.

References

[1] K. Yu, K. Shibata, T. Tokutake et al., "A lightweight ledger-based points transfer system for application-oriented LPWAN," in *Proceedings of the 2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, pp. 1972–1978, IEEE, Chengdu, China, December 2020.

[2] L. Chen, S. Suo, X. Kuang, Y. Cao, and W. Tao, "Secure ubiquitous wireless communication solution for power distribution internet of things in smart grid," in *Proceedings of the IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, pp. 780–784, IEEE, Guangzhou, China, December 2021.

[3] Y. Zhang, J. Zou, and R. Guo, "Efficient privacy-preserving authentication for V2G networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1366–1378, 2021.

[4] J. L. Viegas, P. R. Esteves, R. Melício, V. M. F. Mendes, and S. M. Vieira, "Solutions for detection of non-technical losses in the electricity grid: A review," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 1256–1268, 2017.

[5] Y. Li, Q. Wang, D. Zhang, X. Sun, and X. Xu, "Research and application of electricity anti-stealing system based on neural network," in *Proceedings of the 2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, pp. 1039–1043, 2016.

[6] V. B. Krishna, K. Lee, G. A. Weaver, R. K. Iyer, and W. H. Sanders, "F-DETA: a framework for detecting electricity theft attacks in smart grids," in *Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016*, pp. 407–418, IEEE Computer Society, Toulouse, France, June 2016.

[7] S.E. McLaughlin, D. Podkuiko, and P.D. McDaniel, "Energy Theft in the Advanced Metering Infrastructure," in *Critical Information Infrastructures Security, 4th International Workshop, CRITIS 2009, Bonn, Germany, September 30–October 2, 2009. Revised Papers; Rome (Lecture Notes in Computer Science)*, R. E. Bloomfield, Ed., vol. 6027, pp. 176–187, Springer, 2009.

[8] J. Dou, X. Liu, J. Lu, D. Wu, and X. Wang, "Research on electricity anti-stealing method based on power consumption information acquisition and big data," *Electrical Measurement and Instrumentation*, pp. 60–67, 2018.

[9] J. B. Leite and J. R. S. Mantovani, "Detecting and Locating Non-Technical Losses in Modern Distribution Networks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1023–1032, 2018.

[10] P.R. Jeyaraj, E. Nadar, A.C. Kathiresan, and S.P. Asokan, "Smart grid security enhancement by detection and classification of non-technical losses employing deep learning algorithm," *International Transactions on Electrical Energy Systems*, 2020.

[11] M.S. Saeed, M.W. Mustafa, U.U. Sheikh, T.A. Jumani, I. Khan, and S. Atawne, "An efficient boosted C5.0 decision-tree-based classification approach for detecting non-technical losses in power utilities," *Energies*, vol. 13, 2020.

[12] J. L. Viegas, P. R. Esteves, and S. M. Vieira, "Clustering-based novelty detection for identification of non-technical losses," *International Journal of Electrical Power & Energy Systems*, vol. 101, pp. 301–310, 2018.

[13] A. Okino Otuoze, M. Wazir Mustafa, I. Ebianga Sofimieari et al., "Electricity theft detection framework based on universal prediction algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 2, pp. 758–768, 2019.

[14] K. V. Blazakis, T. N. Kapetanakis, and G. S. Stavrakakis, "Effective Electricity Theft Detection in Power Distribution Grids Using an Adaptive Neuro Fuzzy Inference System," *Energies*, vol. 13, no. 12, p. 3110, 2020.

[15] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.

[16] Z. Guan, G. Si, X. Zhang et al., "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[17] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids," *Sensors*, vol. 18, no. 2, p. 162, 2018.

[18] J. Gao, K. O. Asamoah, E. B. Sifah et al., "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[19] K.P. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE transactions on industrial informatics*, 2021.

[20] M. Li, K. Zhang, J. Liu, H. Gong, and Z. Zhang, "Blockchain-based anomaly detection of electricity consumption in smart grids," *Pattern Recognition Letters*, vol. 138, pp. 476–482, 2020.

[21] M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro, "BAD: A Blockchain Anomaly Detection Solution," *IEEE Access*, vol. 8, pp. 173481–173490, 2020.

[22] T. Golomb, Y. Mirsky, and Y. Elovici, "CIoTA: Collaborative IoT Anomaly Detection via Blockchain," 2018, https://arxiv.org/pdf/1803.03807.pdf.

[23] R. Casado-Vara, J. Prieto, J. M. Corchado et al., "How Blockchain Could Improve Fraud Detection in Power Distribution Grid," in *International Joint Conference SOCO'18-CISIS'18-ICEUTE'18-San Sebastián, Spain, June 6-8, 2018, Proceedings, Advances in Intelligent Systems and Computing*, J.A. Sáez, H. Quintián, and E. Corchado, Eds., vol. 771, pp. 67–76, Springer, Berlin, Germany, 2018.

[24] F. Jamil, N. Iqbal, Imran, S. Ahmad, and D. Kim, "Peer-to-Peer Energy Trading Mechanism Based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid," *IEEE Access*, vol. 9, pp. 39193–39217, 2021.

[25] J. Abdella, Z. Tari, A. Anwar, A. Mahmood, and F. Han, "An Architecture and Performance Evaluation of Blockchain-based Peer-to-Peer Energy Trading," *IEEE Transactions on Smart Grid*, 2021.

[26] F. Khan, H. Li, Y. Zhang, H. Abbas, and T. Yaqoob, "Efficient attribute-based encryption with repeated attributes optimization," *International Journal of Information Security*, vol. 20, no. 3, pp. 431–444, 2021.

[27] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," *Peer-to-Peer Networking and Applications*, pp. 1–13, 2020.

[28] P.M. Mammen, H. Kumar, K. Ramamritham, and H. Rashid, "Want to reduce energy consumption, whom should we call?" *Proceedings of the Ninth International Conference on Future Energy Systems*, pp. 12–20, 2018.

[29] S. Khalid, A. Maqbool, T. Rana, and A. Naheed, "A Blockchain-Based Solution to Control Power Losses in Pakistan," *Arabian Journal for Science & Engineering*, p. 45, Springer Science & Business Media BV, 2020.

[30] Z. A. Khan, M. Adil, N. Javaid, M. N. Saqib, M. Shafiq, and J.-G. Choi, "Electricity theft detection using supervised learning techniques on smart meter data," *Sustainability*, vol. 12, no. 19, p. 8023, 2020.

[31] 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 Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2019.