frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 23 March 2023
DOI 10.3389/fenrg.2022.861321

OPEN ACCESS

EDITED BY
Suyang Zhou,
Southeast University, China

REVIEWED BY
Kaiwen Zhang,
École de technologie supérieure (ÉTS), Canada
Huaping Sun,
Jiangsu University, China

*CORRESPONDENCE
Qingqing Ji,
jiqingqing20b@ict.ac.cn
Xu Zhao,
zhaox@bjut.edu.cn

†These authors have contributed equally to this work

SPECIALTY SECTION
This article was submitted to Sustainable Energy Systems and Policies, a section of the journal Frontiers in Energy Research

RECEIVED 24 January 2022
ACCEPTED 15 November 2022
PUBLISHED 23 March 2023

CITATION
Ji Q, Hu C, Duan Q, Huang C and Zhao X (2023), Decentralized power grid fault traceability system based on internet of things and blockchain technology. *Front. Energy Res.* 10:861321. doi: 10.3389/fenrg.2022.861321

Decentralized power grid fault traceability system based on internet of things and blockchain technology

Qingqing Ji[1,2,3*†], Chunying Hu[4†], Qiao Duan[5], Chunli Huang[6] and Xu Zhao[6*]

[1]Faculty of Information Technology, Beijing University of Technology, Beijing, China, [2]University of Chinese Academy of Sciences, Beijing, China, [3]Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China, [4]Graduate School, Beijing University of Technology, Beijing, China, [5]Faculty of Humanities and Social Sciences, Beijing University of Technology, Beijing, China, [6]Faculty of Science, Beijing University of Technology, Beijing, China

With the economic and social development of China, the scale of the power grid continues to expand. Rapid location and diagnosis of power failures have become significant for China to maintain its stable development of power system. In recent years, the Internet of Things (IoT) based on 5G technology has been applied to power grid more widely. Meanwhile, given the fact that the blockchain is traceable and tamper-resistant, the combination of the blockchain and IoT is considered to locate power failures quickly and assist professional maintenance personnel to deduce the cause of failures, minimizing economic loss. With the foundation of IoT sensor node data, this paper designs a decentralized electronic certificate scheme based on blockchain and Interplanetary File System (IPFS) to collect data of each node of the power system and store it in the blockchain. The model of data sharding, storage and certificate optimizes the utilization of storage space of the blockchain, reducing the time required for system access to nodes. Traceability of data stored on blockchain data is employed to quickly and accurately trace faults of the power system, providing strong technical support for the safe and stable operation of China's power system.

KEYWORDS

blockchain, IPFS, internet of things, power failures, fault location

1 Introduction

As development in all walks of life in China accelerates, higher requirements have been placed on the safe operation of electric energy and the reliability of power supply. As a national energy industry, electric energy has always played a vital role in boosting economy and improving people's life. Therefore, the stable development of electric energy serves as an important guarantee for the economy and people's livelihood. With the continuous expansion of the scale of the power grid, when a complex one fails, it is often difficult for power dispatchers to identify the location of power system fault and the cause

of it in a short time, thus further aggravating the failure. With distributed power generation connected to the distribution network in recent years, the traditional single centralized power generation mode has been gradually developed to a centralized and distributed mode, which makes the fault diagnosis of the distribution network more and more complicated. Therefore, the research on rapid and accurate methods of power system fault location and diagnosis are of great significance to the stable operation of China's power system.

With the construction of power system advancing, the scale and structure of the power grid are becoming increasingly complex, and the correlation between different regions and different modules is getting far more closely. When a power failure occurs, the location of the faulty element turns out to be an important premise for inferring the cause of it. At this stage, many studies mainly rely on physical properties to work out the fault location, and methods based on high frequency impedance measurement are often used for phase-to-phase faults and ground faults in neutral-grounded systems (Jia et al., 2016; Santos et al., 2016). The fault location methods based on single-ended impedance and double-ended impedance have the characteristics of simple principle and low cost, but they are also easily affected by line impedance and the feeding power of distributed power in the system (Jia et al., 2013a; Jia et al., 2013b). In recent years, optimization algorithms have been gradually applied to fault location and diagnosis. The particle swarm optimization method can obtain the optimal solution through global solution for the fault of the distribution network with distributed generators (Peng-Fei and Xing, 2018); the heuristic algorithm can solve the fault of the distribution network with distributed generators, but the time required for the solution is difficult to grasp (Manassero et al., 2016). The fault location method of distribution network with distributed generators based on ant colony algorithm can improve the speed and accuracy of fault location by dividing the large-scale power grid into multiple independent areas. All of these optimization algorithms can locate faults in distribution network with distributed generators, but they all have the problem of large computational load and are easy to fall into local optimum. With the development of artificial intelligence, some scholars determine the location of single-line fault and three-phase fault by adopting neutral network (Rezaei and Haghifam, 2008). The fault location method based on radial basis function neural network can determine the exact type and location of the fault, but it requires a large amount of data, and the robustness of the training model is poor for the circuit parameters often change (Zayandehroodi et al., 2011).

The development of 5G technology provides a foundation for the application of IoT technology in the construction of power grids (Khalid, 2020). Widely applied in the fields of smart home (Wagner et al., 2016), smart transportation (Leal et al., 2014), smart agriculture (Singh et al., 2021) and smart grid, the IoT technology in the power grid also enables different modules in the power grid to realize information interaction and control functions (Poldrack and Poline, 2015). Blockchain technology appeared in 2008, and then it has been widely used in many fields due to its decentralization, security and reliability (Wang et al., 2019). At the same time, in order to make the blockchain technology widely promoted in more fields, some studies have explored the operation mechanism of smart contracts of blockchain, and designed a smart contract framework based on a new six-layer architecture (Ortu et al., 2019). After comparing multiple blockchain software systems and the corresponding systems developed in the traditional Java language, some studies find that the blockchain system is mainly composed of distributed computing, P2P network and encryption algorithms, and often faces fields related to certain security issues in data storage (Kan et al., 2018). In order to improve the transaction efficiency of blockchain throughput, some researchers innovatively propose a component-based blockchain framework to create a multi-link network for communication between blockchains, thereby greatly improving the blockchain throughput performance (Silvestre et al., 2020). With the development and maturity of blockchain technology, many scholars gradually apply it to power grids (Jc et al., 2021; Xie et al., 2021; Reijsbergen et al., 2022; Tan et al., 2022). Among them, grid transaction is one of the main areas with blockchain technology applied. The use of digital currency in energy transactions can improve the reliability and security of energy transactions as well as promote the reliability of power system mobilization (Liu et al., 2019; Du et al., 2021; Yang and Wang, 2021). Some scholars have also explored the security and stability of the blockchain system, laying the foundation for further development and utilization of the blockchain system (Picone et al., 2021; Sun et al., 2022). In addition, some scholars have discussed and studied the impact brought by emerging technologies on the energy industry, arguing that technology can bring great changes to it, and promote the rapid development of the energy industry (Sun et al., 2021; Ali et al., 2022; Gulzara et al., 2022).

In summary, the determination of existing power system faults mainly relies on the laws of classical physics. Though some scholars have started to introduce artificial intelligence into the solution of fault location in recent years, these methods are to a certain extent characterized by low accuracy and long time required, which are not conducive to the rapid determination of fault location. At this stage, the exploration of the combination of blockchain and electric power industry mostly focuses on electricity trading or electricity data storage. Data security and transaction reliability are enhanced with the application of tamper-resistant blockchain (Hakiri and Dezfouli, 2021; Sonthi et al., 2021). This paper uses blockchain technology to solve the problem of determination of fault location of power systems and designs the model of data sharding, storage and certificate to enhance the utilization of storage space of

blockchain, thus reducing the time required for system access to nodes. Therefore, quick location and confirmation of fault location of power system can be achieved by taking advantage of traceability of blockchain.

2 5G-based IoT power monitoring system

2.1 System requirements and overall architecture design

The 5G-based IoT power monitoring system needs to fulfill the following four requirements: operation status monitoring, data transmission and preprocessing, video monitoring and overall control. In order to better realize the monitoring of the power system, the system in this paper has the following objectives:

1) The structure of the power grid monitoring and control system. Multiple indicators of the power grid are monitored and sensing equipment is controlled by means of the combination of local client and cloud storage. At the same time, the monitoring data generated by the sensing equipment is stored in the IPFS network and the blockchain network after a series of processing, and the local computer room realizes data backup and interactive access.
2) Regular monitoring. In order to routinely monitor the power system, it is necessary to set the system to be able to collect data at regular intervals.
3) Device control. In the daily operation of the system, each sensing device usually needs to work normally. But in case of special circumstances, it is necessary to issue instructions to the sensor acquisition device so that its working state can be changed.
4) Data upload. Data serves as an important basis for early warning and positioning. Therefore, the system needs to be able to use the 5G network to upload various data collected by sensors in time to facilitate rapid diagnosis and analysis when faults occur.

Given the above, the framework of the 5G-based IoT power monitoring system in this paper is shown in Figure 1, in which various sensors are arranged at each device end of the power delivery network to form a sensor module; the sensor module regularly collects power grid data according to the system settings, and uploads it to the cloud through the 5G network; then the data backed up by the cloud is sent to the central control room for confirmation and processing; finally it achieves system management and interaction on the local server. When the data is processed in the cloud, it is partially stored in the cloud IPFS network system, and the data summary and information are stored in the blockchain network, which is convenient for quick traceability of subsequent power failures.

2.2 Key technology of the system

1) Data collection. The system needs to collect various indicator data of the power system operation, such as temperature, humidity, voltage, current, resistance, wind speed and other parameters that can affect the stable operation of the power delivery system.
2) Network transmission. In order to minimize the data delay and improve reliability and real-time capability of data transmission, the data is uploaded to the system *via* 5G, and the corresponding instructions of the system are also sent to each sensor node *via* the 5G network. 5G network can minimize the limitations of terrain factors and reduce the impact of network speed during data collection and transmission.
3) Data encryption and tracing. In order to ensure the authenticity and reliability of the data used for power network fault diagnosis, the system uses blockchain and IFPS technology to encrypt and store the data, and implement multiple verifications to improve the reliability of the system data.

3 Decentralized fault tracing and location method based on blockchain and IPFS

3.1 Key technology of blockchain and system architecture design

Linux Foundation launched the open source project Hyperledger in 2015 to promote the application of blockchain in digital transactions (Singh and Kumar, 2021). Its sub-project Fabric is developed and built by IBM, which is more suitable for the construction of consortium chains and can quickly build a blockchain network serving commodity tracing, supply chain and financial transactions (Baliga et al., 2018). The fault location and traceability system in this paper is divided into five parts, including user layer, application layer, data layer, blockchain layer and data storage layer. The system architecture is shown in Figure 2:

The system users include certificate nodes composed of various sensors in the power grid system, power grid operation companies, and system administrators. System administrators can monitor the system and manage each storage node. These different users and nodes jointly build the certificate alliance. The application layer is used to realize data certificate and system management, involving system module and certificate platform. The system module includes four modules, namely certificate management, account management, monitoring module and system management. The certificate management module includes multiple modules such as upload, download and verification. Power grid operation companies and system administrators can manage the system through the

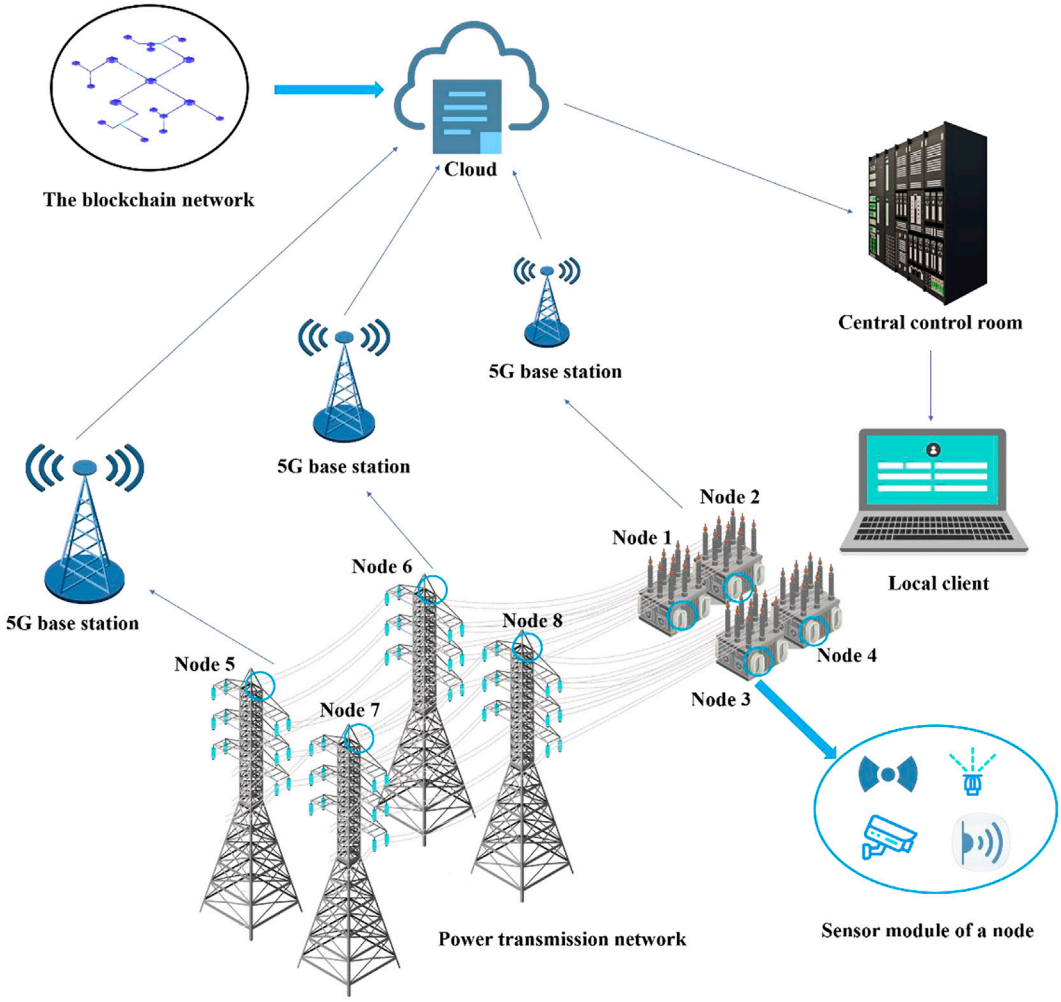

FIGURE 1
Framework of the 5G-based IoT power monitoring system.

above modules, so as to realize a variety of certificate operation functions. Each module of the certificate platform is connected to the system module upwards with the unified API interface, and downwardly connected with the underlying data, blockchain network and IPFS nodes and managed in a unified manner. The data layer stores user and administrator account, passwords and system data. The blockchain layer nodes include a certain number of blockchain nodes and corresponding smart contracts, which run on the docker cluster. The data storage layer consists of multiple IPFS nodes, and the system as a whole uses IPFS to test the network.

File storage layer is responsible for monitoring the operation and status and the blockchain system. Blockchain layer is responsible for data collection and storage in the operation of power system. Data layer is responsible for the storage of all kinds of data certificate on the blockchain. Application layer is responsible for download, verification and analysis of data on the blockchain. User layer grants corresponding permissions to system users with different identities to realize user interaction.

3.2 Interplanetary file system

Juan Benet launched InterPlanetary File System (IPFS) in May 2014. IPFS has the characteristics of content addressability, versioning, and peer-to-peer hypermedia. Its long-term development goal is to supplement or even replace the Hypertext Media Transfer Protocol (HTTP) to build a faster, safer and freer Internet era (Xu et al., 2018). The point-to-point network topology created by IPFS breaks the distribution relationship represented by HTTP, and uses files to generate unique hash identifiers for content addressing, which reduces space occupation costs. IPFS contains eight sub-protocol stacks, including identity layer, network layer, routing layer, switching

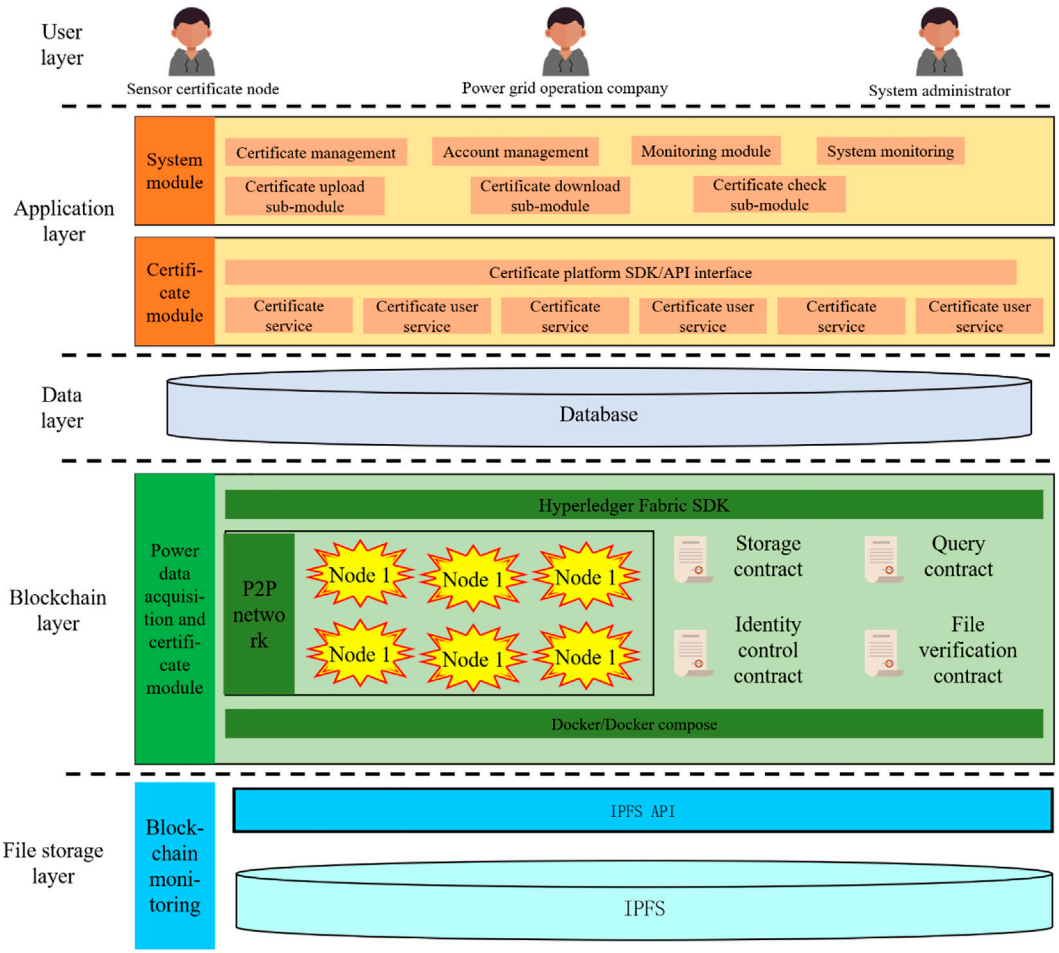

FIGURE 2
Architecture of decentralized fault traceability and location system based on blockchain and IPFS.

layer, object layer, file layer, naming layer, and application layer. Each protocol stack performs its own functions and cooperates with each other (Muralidharan and Ko, 2019).

3.3 The heuristic scheme of data sharding and storage with allocation

The storage and certificate on blockchain, and fault traceability and positioning system need to realize the functions of data storage, verification, download recovery, and data tracing and positioning. Data storage needs to encrypt and store the data content collected and transmitted by each IoT node in IPFS, and store the data summary and ancillary information in the blockchain. Certificate verification needs to compare and verify the data content stored in IPFS and the digital digest stored on the blockchain. The historical tracing of certificate includes related records of data modification and query, as well as retrospective search of past versions. Data recovery means that data information can be recovered to a certain extent after an abnormality occurs in the certificate verification, including the recovery of blockchain information and electronic data in IPFS. Data tracing and positioning can realize functions such as retrospective search of data, analysis of data content and upload of node information when a power system failure occurs. Hash function, also known as hash algorithm, can compress messages or data into digests, make the amount of data smaller, and fix the format of the data. In this paper, a relatively safe and reliable encryption algorithm SHA256 algorithm is used as the encryption algorithm of the system. The multiHash value is a self-describing hash, which combines the hash algorithm and the hash length in the form of a hash and uses base64 for encoding, thus having higher security than the hash function. In this paper the multiHash value is adopted as the encryption algorithm of digital digest.

Limited by factors such as the block size of the blockchain and system throughput, files are generally not stored on the blockchain. Therefore, in this fault traceability and location system, a Hash algorithm is used to extract the digital digest of the data stored in the certificate, and then the public key is used to asymmetrically encrypt it, and the encrypted result is stored in the blockchain; decentralized storage of data content is achieved through IPFS. When it is necessary to call the certificate data, it first takes out the ciphertext stored in the blockchain, decrypt it to obtain a digital digest. Then it obtains the content of the certificate data from IPFS according to the digital digest, perform Hash calculation on the certificate data again, and compare the calculation result with the digital digest stored in the blockchain. The obtained digital digest can help determine the uploading node of the certificate data, so as to locate the faulty node when the power system fails. The information stored in the certificate data can help professionals to infer the cause of the power failure to a certain extent. The certificate storage and fault traceability and location system need to be applied in four scenarios, including certificate and storage of electronic data, download of certificate data, verification of certificate data, and tracing of certificate nodes.

3.3.1 Electronic data certificate and data storage

The function of electronic data certificate and data storage needs to, when users upload the data and data information to be certificated, extract the data summary and perform operations such as encryption and transcoding, and then store the data summary and data information in the blockchain network, and upload the certificate data to the IPFS node for storage. The specific process of this function is shown in Figure 3. After logging in to the system, the user can obtain the corresponding

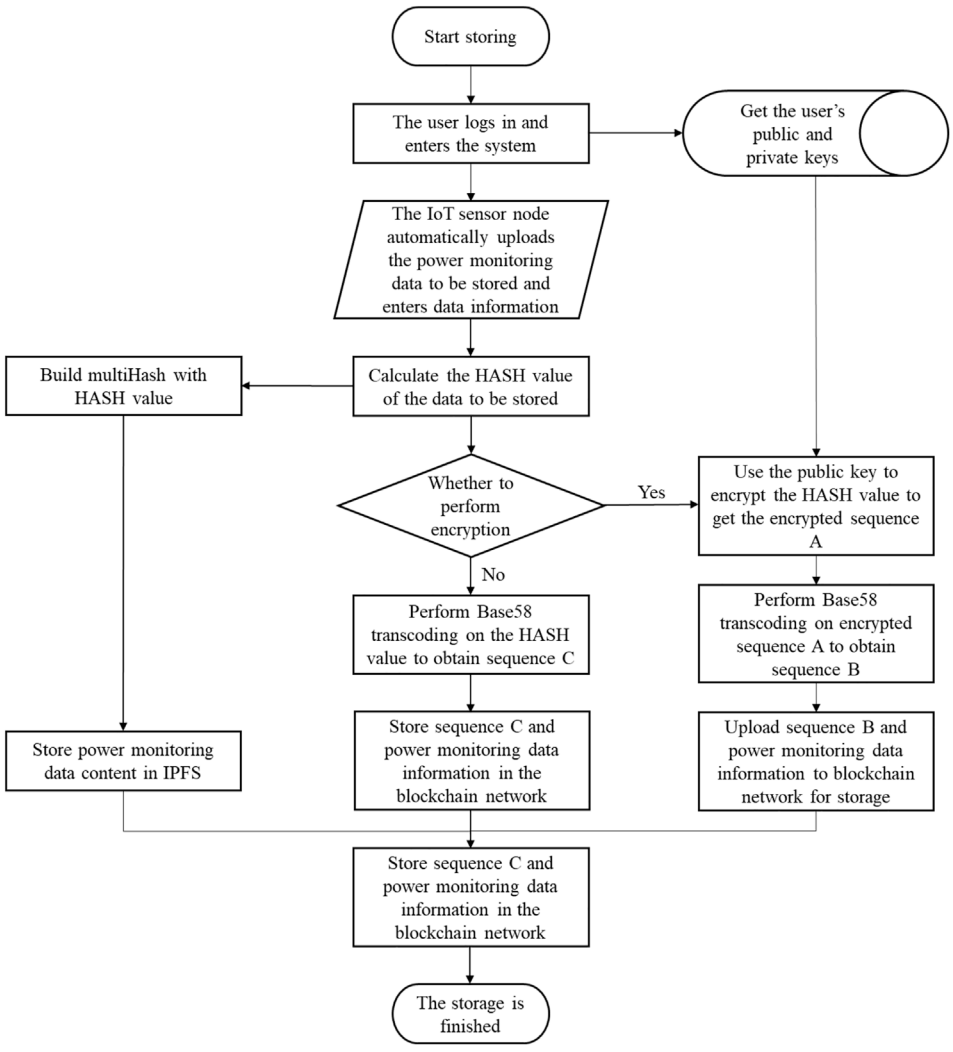

FIGURE 3
Flow chart of decentralized storage scheme for electronic data.

public key and private key, and then upload the electronic data and data information to be certificated. The system calculates the digital digest and uses it to construct the multiHash value, and stores the data in the IPFS network to realize the storage of the certificate data. In the certificate stage, the digital summary needs to be transcoded, and the transcoded digital digest and data information are stored in the blockchain. If the user chooses encrypted storage, the user needs to use the public key to store the digital digest. The encrypted storage method can protect the user's data privacy to a large extent, while the user can also choose non-encrypted storage according to their needs. Finally, the transcoded digital digest sequence is returned to the user who can use this sequence to download and search the stored data.

SHA256 algorithm serves as an important decision of the main cryptographic function on the blockchain, and plays a vital role in the construction of the blockchain (Wolrich et al., 2014). For block headers and transaction data, the integrity of the data is ensured through the SHA256 algorithm.

This paper utilizes the irreversibility of SHA256 algorithm, and the digital digest calculated by it is used to verify the authenticity and integrity of the certificated data. In order to ensure that the entire blockchain can quickly recover data after any node fails, this paper uses the characteristics of blockchain distributed ledgers to upload digital digest to the blockchain network for storage. At the same time, such an operation can also realize that when a small number of nodes in the system encounter an attack and data tampering occurs, the entire blockchain network will form an objection to the tampered data, thereby ensuring that the certificate data will not be tampered with. For the location of the node where an abnormal attack occurs, the Merkle Tree in the blockchain transaction data can be used to quickly locate it; when the power grid fails, the Merkle Tree can also be used to quickly trace the location of the faulty node. Each transaction in the blockchain is digitally signed with the user's private key, which strongly binds the user's identity, transaction and digital digest, thereby ensuring the authenticity of the identity of the user and the uniqueness of each data node in the power grid system. The time stamp is used to record the time of the certificate in the block, which can ensure the authenticity of the certificate. The power grid data files stored in IPFS network can avoid the risks of easy loss, easy copying, and easy tampering brought about by the centralized storage method. Therefore, blockchain technology and IPFS technology effectively ensure the authenticity, integrity and traceability of certificate information, digital digest and certificate data.

3.3.2 The model of data sharding, storage and certificate

In the blockchain system, as the number of transactions grows, the storage cost of individual nodes increases. Therefore, insufficient scalability that occurs during the use of the blockchain system needs a solution in a timely manner. In this paper, optimal block allocation is proposed based on the consensus unit so as to improve the scalability of blockchain.

A cluster of nodes organized by several nodes is called a consensus unit in the blockchain system. Traditionally, each node needs to perform blockchain data maintenance independently when storing data. But in a consensus unit, all nodes participate in the maintenance of data together, and all the blockchain data is distributed to the nodes in the unit for storage, thus significantly reducing the storage pressure on a single node. In this paper, all nodes in the consensus unit store the header information of all blocks. The purpose is to ensure that nodes can verify whether the acquired blocks are legal and valid. Figure 4 illustrates a small-scale consensus unit. The nodes mentioned in this chapter generally refer to the nodes where the consensus unit exists.

In this paper, the goal of data sharding and storage is to minimize the communication cost generated by each node in the consensus unit for querying blocks that have not been stored. A total of x blocks are allocated to a consensus unit with y nodes. b_i represents the i th block on the blockchain, where $i \in \{1, 2, \cdots, n\}$, and s_i represents the size of the data in the i th block. In a consensus unit, N_j is used to represent the j th node, where $j \in \{1, 2, \cdots, m\}$, and l_j represents the size of the storage capacity that the j th node has. At this point if a copy of the complete blockchain is to be stored in a consensus unit, it must satisfy:

$$\sum_{j=1}^{m} l_j \geq \sum_{j=1}^{n} s_i \tag{1}$$

In Figure 4, for example, there are four nodes in this consensus unit. Blocks b_2, b_3 and b_5 are stored in Node N_1, which needs to access b_1 and b_4. Therefore, when node N_1

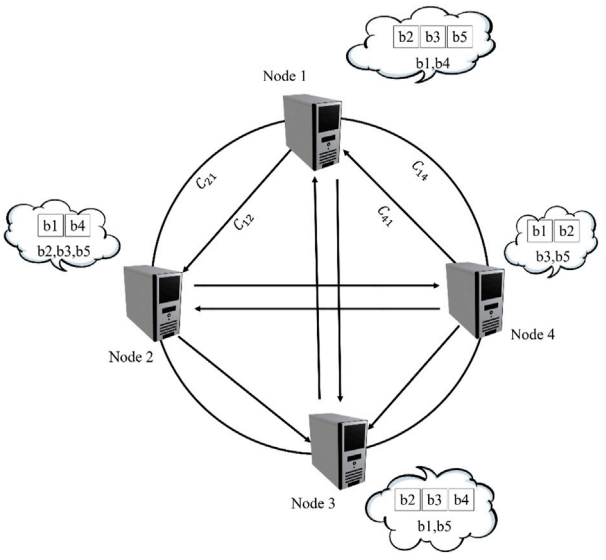

FIGURE 4
The model of storage of the consensus unit.

queries data in b_1, it needs to obtain data stored in b_1 from node N_2 or N_4. In this case, communication cost will be generated. In this paper, the communication cost required by node N_k to transmit unit data to node N_k is denoted as c_{jk}. The probability distribution of node N_j accessing each block is $ACP_j = \{p_{1j}, p_{2j}, \cdots, p_{ij}, \cdots, p_{nj}\}$. p_{ij} represents the probability of node N_j accessing block b_i. In practical application scenarios, nodes often only query data in some blocks frequently and rarely access data in other blocks. Therefore, it is believed that nodes only access a part of the blocks, and the probability of nodes accessing other blocks is 0. Consequently, the ratio between the number of blocks accessed by node N_j and the overall number of blocks is denoted as rat_j.

In this paper, the matrix $X(n^*m)$ is used to represent the allocation result. x_{ij} represents the elements in the i th row and j th column of matrix X. There are only two values in this case. $x_{ij} = 1$ indicates that block b_i is allocated to node N_j, otherwise $x_{ij} = 0$.

At this time, the minimum communication cost required by node N_j to query data on block b_i is $C_j^i = \min\{c_{ki}{}^* s_i\}, k \epsilon R(b_i)$ after the allocation. The overall query cost in the consensus unit is:

$$C_{\text{total}} = \sum_{j=1}^{m} \sum_{i=1}^{n} p_{ij} \min\left\{c_{ki} * s_i\right\}, \quad k \epsilon R(b_i) \tag{2}$$

The symbolic parameters used in this section and to be used later are summarized in Table 1.

To ensure that the consensus unit can have all the blocks on the blockchain after allocation, this paper divides the allocation into two steps. Step 1: Prepare a complete set of data containing all the data on the blockchain for allocation and storage in the nodes. The consensus unit can have a complete set of data information on the blockchain after allocation. Step 2: Allocate the remaining storage space in the consensus unit again until all nodes in the consensus unit have no remaining space to store any of the blocks so as to further reduce the communication cost.

Allocation of the first step can be denoted as the following:

$$\min_X \sum_{i,j} \left(x_{ij} * \sum_{k=1}^{m} p_{ik} s_i c_{jk} \right) \tag{3}$$

$$s.t. \sum_{i=0}^{n} s_i x_{ij} \le l_j, \quad j = 1, 2, \cdots, m \tag{4}$$

$$\sum_{j=1}^{m} x_{ij} = 1, \quad i = 1, 2, \cdots, n, \; x_{ij} \in \{0, 1\} \tag{5}$$

In this paper, the problem of allocation is transformed into a solution of perfect matching for bipartite graph. The specific steps are as follows:

1) Since the problem involved in this paper does not apply to the constraints of integers, x_{ij} can be taken as a fraction between 0 and 1. At this time, the slack problem corresponding to the integer programming formed by the objective function and constraints is a linear programming problem. The fractional solution $x_{ij}^{'}$is yielded by solving the problem.

TABLE 1 Parameters.

Notation	Definition
b_i	The i th block on the blockchain
n	Block synthesis on the blockchain
s_i	Data size of the block b_i
N_j	The j th node in the consensus unit
m	Total number of nodes in the consensus unit
l_j	Storage capacity of the consensus unit N_j
c_{jk}	The communication cost required by node N_j to transmit unit data to node N_k
ACP_j	Probability distribution of node N_j accessing each block
X	Results of block allocation
$R(b_i)$	The set of all nodes in the block b_i after allocation
rat_j	Ratio of the number of blocks accessed by b_i to the total number of blocks
O	The set of nodes on the blockchain
Q_{o_n}	Aggregation of sensor indications of a node in the normal state of the system
$Q_{o_n c}$	Aggregation of sensor indications of a node in real-time situation of the system

2) Combine the fractional solution $x_{ij}^{'}$ to construct the bipartite graph $G = (B, (N, K))$. It can be concluded that there is a total of k_j blocks assigned to node N_j from the solution of the slack problem, so it is possible to divide node N_j into k_j constituent units. Such a representation is a division of a single node into multiple slots, which can express the same meaning of allocation. The left points of the figure represent the set of blocks $B = \{1, 2, 3, \cdots n\}$, and the right points of the figure represent the set of slots $(N, K) = \{(j, k) | j = 1, 2, \cdots, m; k = 1, \cdots, k_j\}$ where the size of each slot is 1. The fractional solution $x_{ij}^{'}$ obtained in the previous step is mapped to each side of the bipartite graph G. Figure 5 is an example of the mapping of the fractional solution.

In the figure, $b_{i(j,k)}$ represents the mapping solution $(k \in [0, n])$ of the left block b_i connecting slot (N_j, K) on the right. Therefore, $x_{ij}^{'}$needs to be transformed. The first node is taken as an example to illustrate the transformation relation:

If $\sum_{i=1}^{i^*} x_{i1} \le k$, and $\sum_{i=1}^{i^*-1} x_{i1} \ge k - 1$, the loose solution of the side $(i, (1, k))$ can be set as $b_{i(1,k)} = x_{i^*1}$ (the range of k is $[0, n]$);

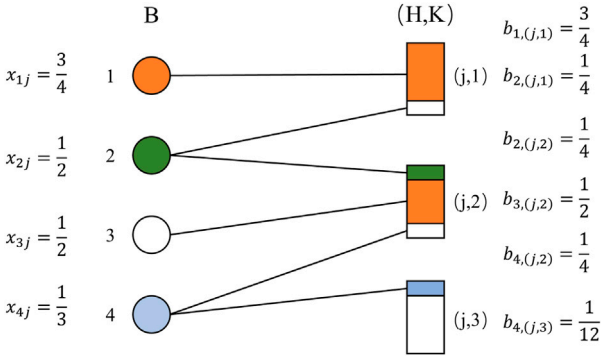

FIGURE 5
Mapping of the fractional solution in the bipartite graph.

If $\sum_{i=1}^{i^*} x_{i1} > k$, and $\sum_{i=1}^{i^*-1} x_{i1} < k-1$, the loose solution of the side $(i,(1,k))$ can be set as $k - \sum_{i=1}^{i^*-1} x_{i1}$, and the solution of the side $(i,(1,k))$ is set as $\sum_{i=1}^{i^*} x_{i1} - k$.

3) To obtain the solution of the perfect matching of the bipartite graph, the fractional solution of the side in the bipartite graph is converted into integer solutions of 0 and 1. The sides with the loose solution in the interval (0,1) are unsaturated sides, and the sides with the loose solution of 0 and 1 are saturated sides. After all the unsaturated sides are converted to saturated sides without the increase of the target value, each left vertex representing the block set is mapped to the right vertex representing the node set through a unique saturated side. It forms an injective mapping, which proves to be a perfect matching of the left in this case. There are two other scenarios that need to be considered:

When the unsaturated side cycle exists, the unsaturated sides are alternately numbered 0 and 1, The fractional solution of the unsaturated sides numbered 1 is increased by a numerically minimal constant 10^{-10}, and the fractional solution of the unsaturated sides numbered 0 is decreased by the same value. As long as this constant is small enough, it will not conflict with constraints. Since the objective function is a linear function, the adjacent sides are iterated successively in the direction that the objective value does not increase until the fractional solution of a side numbered 1 is equal to 1 or the fractional solution of a side numbered 0 is equal to 0.

When there is no cycle of unsaturated sides, the longest path whose starting or ending point is a vertex is chosen, and the sides on this path are alternately numbered 0 and 1. The fractional solution of the unsaturated sides numbered 1 is increased by the numerically minimal constant 10^{-10} successively along the direction of the path, and the fractional solution of the unsaturated sides numbered 0 is decreased by the same value successively until the fractional solution of a side numbered 1 is equal to 1 or a fractional solution of a side numbered 0 is equal to 0.

For the redistribution of some blocks in the second step, this paper adopts greedy algorithm to solve the problem based on the results of the first step. Firstly, the greedy criterion is formulated for the allocation, and its weight function is as follows:

$$f(i,j) = \begin{cases} \sum_{k=1}^{m} p_{ik} s_i c_{jk}, & l_j \geq s_i \\ \infty, & l_j < s_i, or\ x_{ij} = 1 \end{cases} \tag{6}$$

In the above equation, when the corresponding node of the block has been determined and the remaining storage space of the node is not enough for a block, the weight value needs to be set to infinity. In other cases, the weight value is equal to the communication cost generated by the node in the unit to query the block b_i after the block b_i is allocated to the node N_j. Based on the existing allocation, the remaining storage space of the consensus unit is calculated. Then the communication cost C_i generated by the node querying the block b_i after the first allocation step is calculated. The difference θ_i is defined as follows:

$$\theta_i = C_i - f(i, j^*) \tag{7}$$

θ_i represents the communication cost difference between allocated and pre-allocated nodes querying block b_i. The larger the value is, the more cost can be saved by allocating block b_i to node N_{j^*}. After the weight value is calculated from Eq. 6, the corresponding subscript j^* with the smallest weight value and i^* with the largest cost difference $\theta_i^{j'}$ are taken out to complete the task of allocating block b_i to node N_{j^*}. At this time, $x_{i^*j^*} = 1$. Then the remaining space, various weights and cost differences are calculated continually, and the second step is repeated until the nodes in the consensus unit do not have enough remaining storage space for any blocks. This concludes the description of the data storage module.

3.4 The model of power fault tracing and location

3.4.1 Download of data certificate

Fundamentally, the judgement of power system faults starts with power data, and then monitor whether there are abnormal values in the system, so as to screen them. Download of data certificate mainly realizes the download of the sequence of electronic data and data information that has been certificated, and its flow chart is shown in Figure 6. The user can input in the blockchain network or directly use the smart contract to query the storage sequence, which can realize the function of querying the storage information of the corresponding storage data in the blockchain network. Since

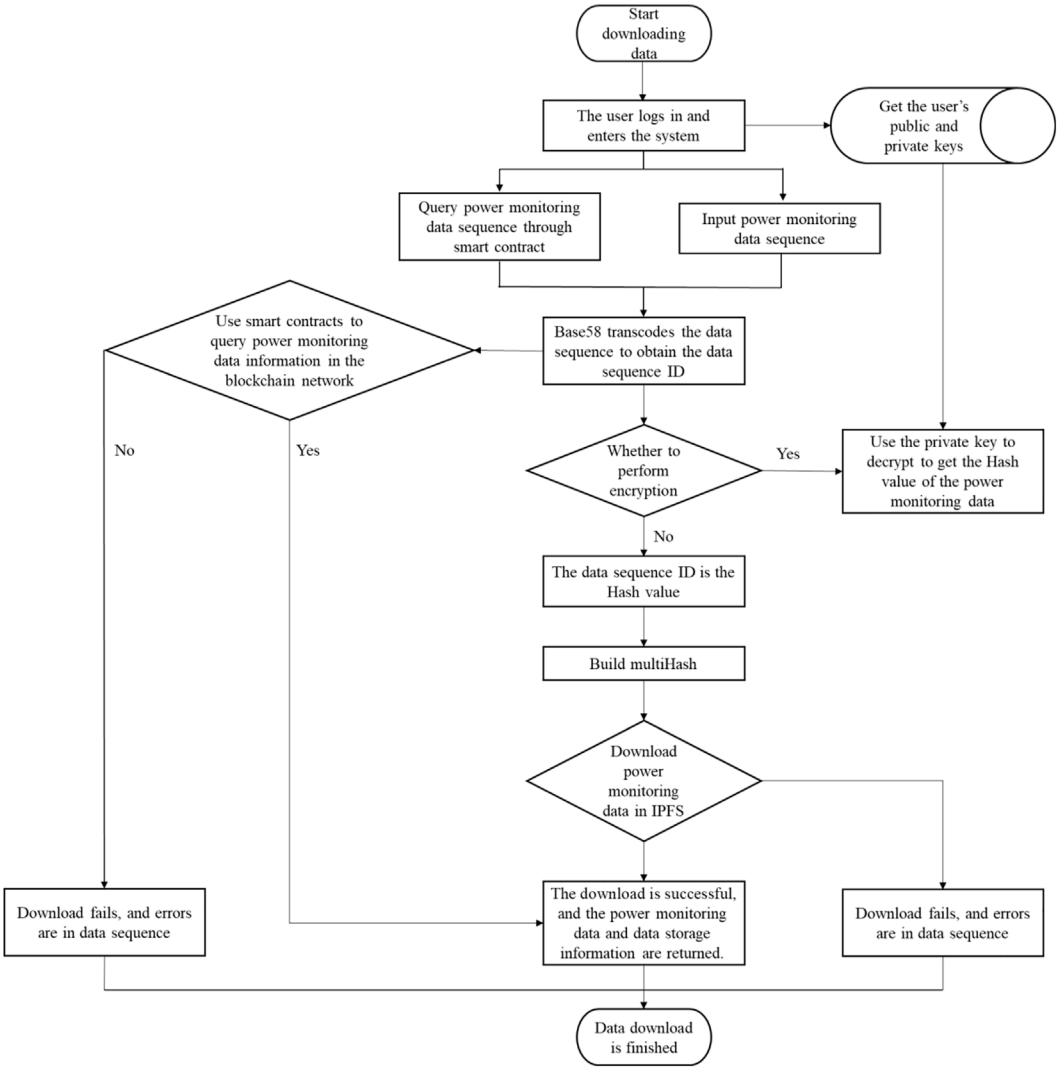

FIGURE 6
Flow chart of downloading scheme for storage and certificate of electronic data in power monitoring system.

the data certificate is stored in the IPFS network, downloading it requires first obtaining its digital digest. The parsing of the digital digest requires Base58 transcoding the data sequence first. If the data is encrypted, it needs to be decrypted with the user's private key to obtain the digital digest of the data, and then use the digital digest to construct the corresponding multiHash value. After the value is set, the corresponding certificate data can be downloaded in the IPFS network. When the certificate sequence cannot be queried in the blockchain network for its corresponding data information or the corresponding data cannot be downloaded in the IPFS network, it indicates that the sequence is invalid, that is, the corresponding data certificate and information cannot be found. When an emergency failure occurs in the power grid, after the faulty node is confirmed, the data certificate of the corresponding node can be downloaded, and the professional staff can assist in judging the cause of the power grid failure and take measures.

3.4.2 Verification of electronic data certificate

When the power grid fails, it needs to judge the cause of the accident according to the existing data in a short time and take measures quickly. Verification of electronic data certificate can provide the information and attribution of the data after uploading the electronic data, and prove the authenticity and integrity of it. The process of verification of electronic data certificate is shown in Figure 7. After entering the system, the user uploads the electronic data that needs to be verified to the system. It first calculates the digital digest of the data, then constructs multiHash, and downloads the electronic data in

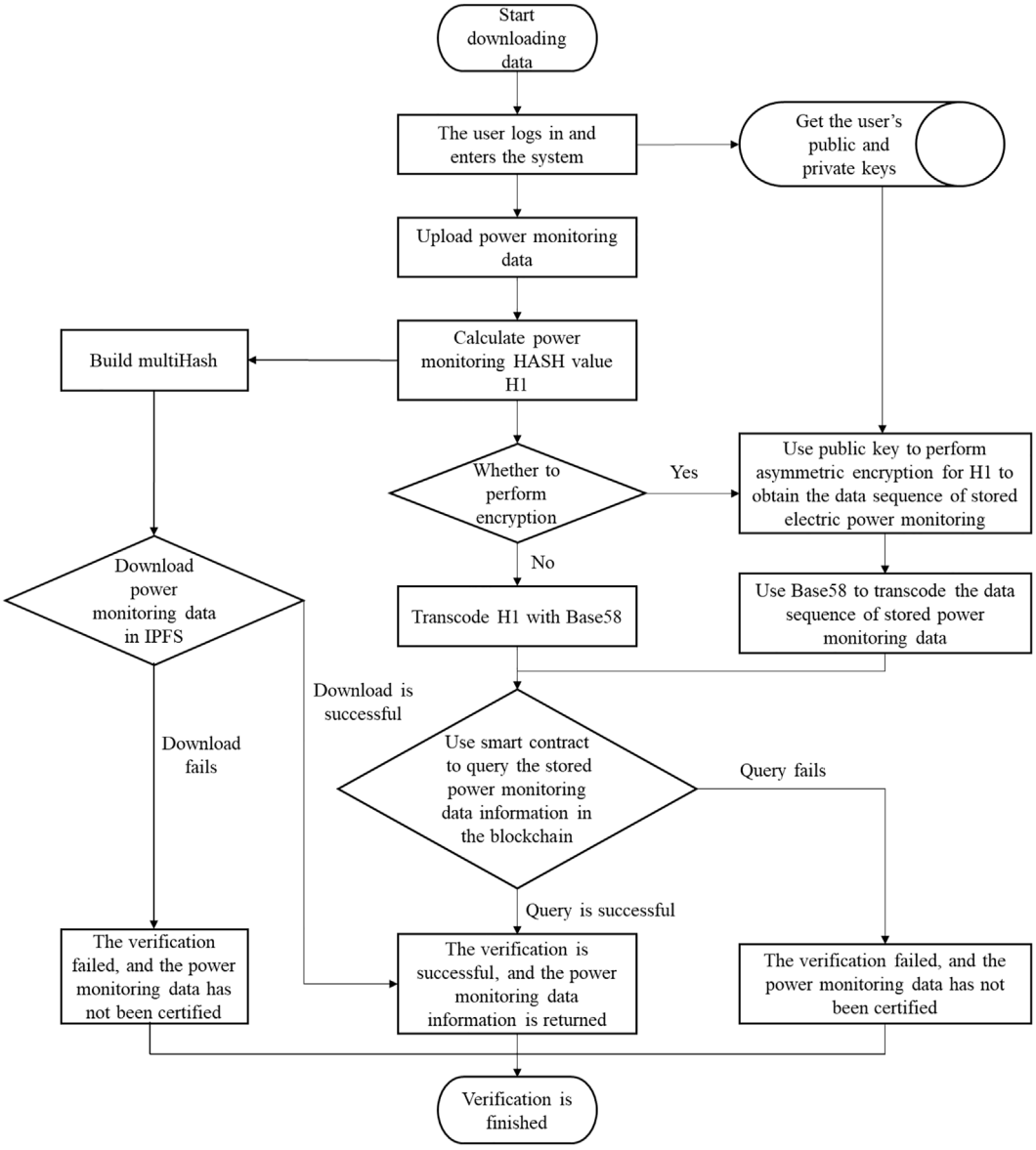

FIGURE 7
Flow chart of verification scheme for electronic data certificate.

the IPFS network. It also requires querying the certificate information in the blockchain network in combination with the situation of data encryption and certificate. If the electronic data can be downloaded in the IPFS network, and the corresponding certificate information exists in the blockchain, it means that the verification is passed, and the certificate information of the data is returned at this time; if the electronic data cannot be downloaded in the IPFS network, and the certificate information of the electronic data cannot be queried in the blockchain network, it means that the uploaded data has not been stored or has been tampered with, and the certificate information cannot be returned.

3.4.3 Fault tracing of power system

After the system completes the download and verification of data certificate, it can judge the operation of the power system. First of all, in the normal and stable operation of the power system, each node on the blockchain constitutes a node set $O = \{o_1, o_2, \cdots, o_n\}$, and all indicators of power monitored by each sensor node of the power grid are in normal state. At this time, the set of indicators of power system of a sensor node is $Q_{o_n} = \{[q_1 - m_1, q_1 + m_1], [q_2 - m_2, q_2 + m_2], \cdots, [q_n - m_n, q_n + m_n]\}$, where m refers to the value of a sensor floating up and down under normal conditions. The indicators of power system collected by a sensor

TABLE 2 Indicator test of IoT monitoring data transmission performance.

Performance	Indicator	Performance	Indicator
Time of data uploaded to the cloud	1800–2100 ms	Success rate of transmission reservation	99.3%
Data throughput	3–4M/s	Accuracy of data transmission	99.9%

node constitute the real-time collection of indicators of power system $Q_{o_nc} = \{q_1, q_2, \cdots, q_n\}$. Through the comparison of Q_{o_n} and Q_{o_nc}, quick and accurate judgement about the operation state of the power grid can be made. If the system is abnormal, traceability of blockchain data is adopted to quickly and accurately locate faults, so as to ensure stable and reliable operation of the power system.

Compared with the judgement and analysis of fault location of long-distance power transmission system by physical method at present, this method can locate the fault and analyze the cause of it more quickly and accurately. It helps the operation department of the power system to make a quick decision, so as to reduce the loss caused by power failure.

4 System effect test

This paper first runs the IoT power monitoring system based on 5G sensors, and tests its data transmission rate and accuracy. The data collection interval is set to 10 min, and the transmission work is carried out precisely after the collection is completed. After 4 h of testing, the following test results are obtained:

It can be seen from the test results that the successful processing time of each reservation is within 2s, which can fully meet the transmission and storage of monitoring data of the power system. At the same time, the accuracy of data transmission in the experiment reaches 99.9%, which can greatly ensure authenticity and reliability of the data in the blockchain. However, due to the factors such as the backward areas of 5G signal development represented by the wild and mountainous areas, the success rate of data transmission reservation is 99.3%. But, after the second request, the success rate of data transmission reservation can reach more than 99.9%, which can ensure that the monitoring data of power grid operation is uploaded to the cloud in a timely and effective manner. The relevant test results are shown in Table 2.

To facilitate the testing of the system, the IPFS node is deployed in the cloud server with the configuration shown in Table 3.

In Hyperledger Fabric system, the resource usage of node components is one of the main factors that determine the system performance when the world state is updated. The test results of some nodes are shown in Table 4.

The test results show that the memory usage of node components is about 200MB, the CPU usage is about 60%, and the disk writes is about 50 MB when the world state is updated. The query performance of the system plays a vital role in the quick fault location for the system. This paper also carries out corresponding tests on the query performance of the system, and the test results are shown in Table 5.

It can be seen from the test results that average memory usage, average CPU usage and disk writes of the node components in the query state are mostly consistent with the results of updated world state.

The decentralized electronic certificate system based on blockchain and IPFS developed in this paper has undergone account system, certificate management function, certificate alliance function, blockchain data query, consensus mechanism, node management, throughput, security, reliability and maintainability testing. The test results of more than 30 test points in 10 major items are in line with the expected results, and all functions can operate normally. Data sharing is one of the characteristics and advantages of the blockchain system. The sharing performance of the designed system has been tested. The network nodes in the alliance chain can automatically synchronize transaction data, which is significant for the stability and reliability of the power delivery system. The sharing efficiency and transmission performance of the system are the key factors to maintain the reliable operation of the system. Therefore, corresponding tests are conducted and the results are as follows:

The designed system consortium chain nodes can perform block consensus more than 120 times within an hour, process nearly 500 messages concurrently, and provide feedback at a high speed. It can be seen from the actual test results in Figures 8, 9 that the system can meet the actual needs of data storage, state monitoring and fault traceability of power networks.

TABLE 3 The system test environment.

Item	Configuration
CPU	Dual core
Memory	16 GB
Operating system	Ubuntu 18.04
Main software environment	Hyperledger Fabric 1.5.1 Golang 13.1 Docker 19.03 IPFS 0.4.23

TABLE 4 Resource usage with updated world state.

Node components	Average memory usage (MB)	Average CPU usage	Disk writes) (MB)
Peer1node	175.9	61.32	51.2
Peer2 node	264.3	63.86	51.2
Peer3 node	187.4	61.97	51.2
Peer4 node	190.6	62.01	51.2

TABLE 5 Resource usage of performing query.

Node components	Average memory usage (MB)	Average CPU usage	Disk writes (MB)
Peer1 node	197.3	60.98	0
Peer2 node	276.3	62.43	0
Peer3 node	192.7	61.61	0
Peer4 node	203.5	62.99	0

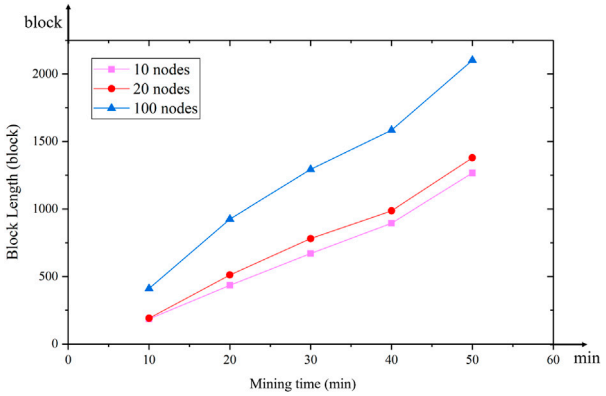

FIGURE 8
Mining speed test of nodes.

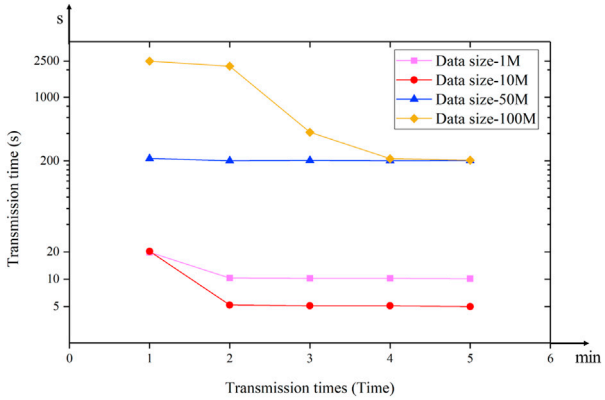

FIGURE 9
Transmission speed test.

5 Conclusion

This paper analyzes the application status of IoT and blockchain technology in the power supply system. Given the characteristics of blockchain technology, it puts forward the requirements of electronic certificate and traceability applied in power grid fault location and diagnosis, demonstrating the significance of decentralized power fault traceability system. Combined with IoT, a multi-sensor monitoring system for power system with the application of IoT is proposed. A decentralized power system fault traceability and location scheme based on blockchain and IPFS distributed storage is put forward. In this scheme, the model of data sharding, storage and certificate is designed to improve the storage efficiency of the blockchain system and optimize the system operation process, reducing the time required for storage and certificate. Finally, the system performance is tested, and it is found that the system can basically meet the actual use requirements, and can realize the rapid traceability and location of power system faults.

In the future, further research work on improving the data access performance between different data nodes in the system will be carried out, so that the data generated by the sensors in the power system can be uploaded to the system faster. (Zhang et al., 2020; Bulatov et al., 2021; Gupta et al., 2021); (Moudoud et al., 2022).

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Author contributions

QJ, CYH, and QD conducted the back ground research of the project. QJ, CYH, and XZ proposed the methodology of the project. QJ, CYH, CLH, and XZ completed the main theory and simulationcontent. QD and CLH carried out the index calculation and comparison of the scheme. QJ, CYH, and QD completed the writing of the paper. Thework was supported by the fund of XZ.

Funding

This work was supported by the National Natural Science Foundation of China (grant numbers: 11801019).

Acknowledgments

The authors would like to thank the referees and editors for their very helpful and constructive comments, which have significantly improved the quality of this paper.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Ali, I., Sun, H., Gulzara, T., Ali, H., Baz, K., Mahmood, H., et al. (2022). Asymmetric impact of coal and gas on carbon dioxide emission in six Asian countries: Using asymmetric and non-linear approach. *J. Clean. Prod.* 367, 132934. [J]. doi:10.1016/j.jclepro.2022.132934

Baliga, A., Solanki, N., Verekar, S., Pednekar, A., Kamat, P., and Chatterjee, S. (2018). "Performance characterization of hyperledger fabric," (Zug, 65–74.*2018 crypto valley conference on blockchain technology (CVCBT).*

Bulatov, Y. N., Kryukov, A. V., Suslov, L. V., and Cherepanov, A. V. (2021). Timely determination of static stability margins in power supply systems equipped with distributed generation installations. *Mater. Sci.* 25. [J].

Du, X., Qi, Y., Chen, B., Shan, B., and Liu, X. (2021). The integration of blockchain technology and smart grid: Framework and application. *Math. Problems Eng.* 2021, 1–12. [J]. doi:10.1155/2021/9956385

Gulzara, T., Sun, H., Ali, I., Pasha, A. A., Khan, M. S., Rahman, M. M., et al. (2022). Influence of green technology, green energy consumption, energy efficiency, trade, economic development and FDI on climate change in South Asia. *Sci. Rep.* 12 (1), 16376. [J]. doi:10.1038/s41598-022-20432-z

Gupta, S., Kumar, N., Srivastava, L., Malik, H., Pliego Marugan, A., and Garcia Marquez, F. P. (2021). A hybrid jaya–powell's pattern search algorithm for multi-objective optimal power flow incorporating distributed generation. *Energies* 14, 2831. [J]. doi:10.3390/en14102831

Hakiri, A., and Dezfouli, B. (2021). Towards a blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks.USA *SDN-NFV Sec.*

Jc, A., Wq, B., Jie, M. A., Xu, C., Zhou, G., Ding, H., et al. (2021). Evaluation index system of blockchain technology feasibility towards power material supply chain. *Energy Rep.* 7, 968–978. [J]. doi:10.1016/j.egyr.2021.09.176

Jia, K., Bi, T., Ren, Z., Thomas, D. W. P., and Sumner, M. (2016). High frequency impedance based fault location in distribution system with DGs. *IEEE Trans. Smart Grid* 9 (99), 807–816. [J]. doi:10.1109/tsg.2016.2566673

Jia, K., Thomas, D., and Sumner, M. (2013). A new single-ended fault-location scheme for utilization in an integrated power system. *IEEE Trans. Power Deliv.* 28 (1), 38–46. [J]. doi:10.1109/tpwrd.2012.2215346

Jia, K., Thomas, W. P., and Sumner, M. (2013). A new double-ended fault-location scheme for utilization in integrated power systems. *IEEE Trans. Power Deliv.* 28 (2), 594–603. [J]. doi:10.1109/tpwrd.2013.2238560

Kan, L., Wei, Y., Hafiz Muhammad, A., Siyuan, W., Linchao, G., and Kai, H. (2018). "A multiple blockchains architecture on inter-blockchain communication," Lisbon: QRS-C, 139–145.*2018 IEEE international conference on software quality, reliability and security companion*

Khalid, L. (2020). Internet of Things (IoT). *Software Architecture for Business.* Singapore: Springer[M].

Leal, A. G., Santiago, A., Miyake, M. Y., Noda, M. K., and Avanco, L., (2014). "Integrated environment for testing IoT and RFID technologies applied on intelligent transportation system in Brazilian scenarios," in *Ieee rfid Brazil 2014.* Sao Paulo, Brazil: IEEE. [C].

Liu, Y., Ji, Q., Zheng, Q., Wu, H., Wang, Z., and Xiong, G., (2019). "Security assessment of a partially decentralized blockchain system," in 2019 IEEE international conference on service operations and logistics, and informatics (SOLI). Zhengzhou, China: IEEE. [C].

Manassero, G., Santo, S. D., and Souto, L. (2016). Heuristic method for fault location in distribution feeders with the presence of distributed generation. *IEEE Trans. Smart Grid*, 8, 1–10. [J].

Moudoud, H., Cherkaoui, S., and Khoukhi, L. (2022). "An IoT blockchain architecture using oracles and smart contracts: The use-case of a food supply chain," Istanbul, Turkey. [C].*2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC).*

Muralidharan, S., and Ko, H. (2019). "An InterPlanetary file system (IPFS) based IoT framework," (Las Vegas, NV, USA, 1–2.*2019 IEEE international conference on consumer electronics (ICCE).*

Ortu, M., Orrú, M., and Destefanis, G. (2019). "On comparing software quality metrics of traditional vs blockchain-oriented software: An empirical study," (Hangzhou, China, 32–37.*2019 IEEE international workshop on blockchain oriented software engineering (IWBOSE).*

Peng-Fei, X. U., and Xing, R. Z. (2018). Fault location of distribution network with distributed power supply by particle swarm optimization algorithm. *Chin. J. Power Sources.* [J] 42 (4), 591–592+600.

Picone, M., Cirani, S., and Veltri, L. (2021). Blockchain security and privacy for the Internet of Things. *Sensors* 21 (3), 892. [J]. doi:10.3390/s21030892

Poldrack, R. A., and Poline, J. B. (2015). The publication and reproducibility challenges of shared data. *Trends Cognitive Sci.* 19 (2), 59–61. [J]. doi:10.1016/j.tics.2014.11.008

Reijsbergen, D., Maw, A., Venugopalan, S., Yang, D., Dinh, T. T. A., and Zhou, J., (2022). "Protecting the integrity of IoT sensor data and firmware with A feather-light blockchain nfrastructure," in 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China. [C].

Rezaei, N., and Haghifam, M. R. (2008). Protection scheme for a distribution system with distributed generation using neural networks. *Int. J. Electr. Power & Energy Syst.* 30 (4), 235–241. [J]. doi:10.1016/j.ijepes.2007.07.006

Santos, W. C., Lopes, F. V., Brito, N., and Souza, B. A. (2016). High impedance fault identification on distribution networks. *IEEE Trans. Power Deliv.* 32 (1), 23–32. [J]. doi:10.1109/tpwrd.2016.2548942

Silvestre, M., Gallo, P., Guerrero, J. M., Musca, R., Riva Sanseverino, E., Sciume, G., et al. (2020). Blockchain for power systems: Current trends and future applications. *Renew. Sustain. Energy Rev.* 119, 109585. [J]. doi:10.1016/j.rser.2019.109585

Singh, S. K., and Kumar, S. (2021). Blockchain technology: Introduction, integration and security issues with IoT. *arXiv*. Available at: https://arxiv.org/abs/2101.10921.

Singh, U., Rizwan, M., Alaraj, M., and Alsaidan, I. (2021). A machine learning-based gradient boosting regression approach for wind power production forecasting: A step towards smart grid environments. *Energies* 14, 5196. [J]. doi:10.3390/en14165196

Sonthi, V. K., Nagarajan, S., Vbmkm, M., Giridhar, K., and Mohan, V. M., (2021). *Imminent threat with authentication methods for AI data using blockchain security*. Singapore: Springer [M].

Sun, H., Edziah, B. K., Kporsu, A. K., Sarkodie, S. A., and Taghizadeh-Hesary, F. (2021). Energy efficiency: The role of technological innovation and knowledge spillover. *Technol. Forecast. Soc. Change* 167, 120659. doi:10.1016/j.techfore.2021.120659

Sun, H., Edziah, B., Sun, C., and Kporsu, A. K. (2022). Institutional quality and its spatial spillover effects on energy efficiency. [J]. *Socio-Economic Plan. Sci.*, 83.

Tan, W., Li, L., Zhou, Z., Yan, Y., Zhang, T., Zhang, Z., et al. (2022). Blockchain-based distributed power transaction mechanism considering credit management. *Energy Rep.* 8, 565–572. [J]. doi:10.1016/j.egyr.2022.02.240

Wagner, M., Jeroen, L., Dennis, G., Olaf, W., and Sebastian, S., (2016). "Integrating vehicular data into smart home IoT systems using eclipse vorto," in *Workshop on vehicular information services for the Internet of Things*. Montreal, QC, Canada: IEEE. [C].

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., and Wang, F. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man. Cybern. Syst.* 49, 2266–2277. doi:10.1109/tsmc.2019.2895123

Wolrich, G. M., Yap, K. S., Guilford, J. D., Gopal, V., and Gulle, S. M., (2014). Instruction set for message scheduling of SHA256 algorithm. UK: Patent Scope, GB2520858A.

Xie, Y. S., Lee, Y., Chang, X., Yin, X., and Zheng, H. (2021). Research on the transaction mode and mechanism of grid-side shared energy storage market based on blockchain. *Energy Rep.*8.

Xu, Q., Song, Z., Mong Goh, R. S., and Li, Y. (2018). "Building an ethereum and IPFS-based decentralized social network system," (Singapore, 1–6.*2018 IEEE 24th international conference on parallel and distributed systems (ICPADS)*.

Yang, Q., and Wang, H. (2021). Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain. *IEEE Internet Things J.* 8, 11463–11475. [J]. doi:10.1109/jiot.2021.3051323

Zayandehroodi, H., Mohamed, A., Shareef, H., and Mohammadjafari, M., (2011). "Determining exact fault location in a distribution network in presence of DGs using RBF neural networks," in IEEE international conference on information reuse & integration. Las Vegas, NV, United States: IEEE. [C].

Zhang, J., Li, H., Shan, D., Kim, K., and Gong, P. (2020). "A dynamical network fault setting approach for joint power grid simulation," in 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea (South). [C].