Power Blockchain Guarantee Mechanism Based on Trusted Computing

Yong Yan[1], Tianhong Su[2(✉)], Shaoyong Guo[2], and Song Kang[2]

[1] Electric Power Research Institute of State Grid Zhejiang Electric Power Company, Hangzhou 310009, China
[2] Beijing University of Posts and Telecommunications, Beijing 100876, China
sutianhong@bupt.edu.cn

Abstract. The power Internet of Things is an effective way to solve the inefficiency of traditional Internet of Things services in the era of big data. However, as the power Internet of Things is full of sensitive data, how to ensure the security of the information transmission and exchange process is an urgent problem in the power Internet of Things system. This paper combines the characteristics of blockchain and power Internet of Things to propose a power blockchain guarantee mechanism based on trusted computing for the above problems. The decentralized technology of the blockchain provides a reliable solution to the massive data and high concurrency problems in the power Internet of Things. The trusted platform module is added to the blockchain node server to ensure the credibility of the server operating environment. At the collection layer, the system designs an algorithm for real-time monitoring of malicious collection terminals based on reputation, which prevents malicious terminals from publishing malicious data. At the same time, the system detects the visitor's access authority through integrity certification and access policy verification, ensuring the credibility of the access terminal, maintaining the safe and reliable operation of the power blockchain system in all aspects, and protecting the private data in the power blockchain.

Keywords: Trusted computing · Blockchain · Privacy protection

1 Introduction

The concept of the Internet of Things was first proposed in 1999 by Professor Ashton of the Auto-ID Center. The Internet of Things is a giant network that uses the Internet as an information carrier to collect information about monitored objects in real time through information sensing equipment, and realize communication between people and things, and things and things. With the continuous development of the Internet of Things in smart cities, smart transportation and other fields, it has brought great convenience to people's lives. According to Gartner's report, the IoT market will grow to 5.8 billion endpoints by the end of 2020. There is a huge amount of private information in the Internet of Things. For example, wearable devices record the health of people, Internet of Vehicles systems record the daily trajectory of users, and user privacy data recorded

X. Sun et al. (Eds.): ICAIS 2021, LNCS 12737, pp. 488–501, 2021.
https://doi.org/10.1007/978-3-030-78612-0_39

in the Internet of Things. These private information will be recorded in the data center. if the central server is attacked by malicious users and causes privacy leakage, it will have an incalculable impact. Therefore, traditional IoT central nodes are faced with multiple challenges of high-concurrency and massive data processing against multiple attacks. Therefore, traditional IoT central nodes are faced with multiple challenges of high concurrent processing and malicious user attacks.

In the era of big data, massive high-concurrency data exchanges have brought great challenges to traditional networks with data centers as the computing core. The drawbacks of the traditional "collection + centralized" power service model are gradually emerging.There are many kinds of data in the traditional power service. Data collection and data status monitoring will consume huge human and financial resources, which cannot meet the demand of current power grid development. The power Internet of Things has become the first choice for improving the efficiency of power services and reducing costs. In 2019, the State Grid proposed the concept of ubiquitous power Internet of Things, aiming to provide a more efficient and flexible power Internet of Things.

Reliability and controllability are the top priorities for the development of the power Internet of Things system. It is necessary to ensure the service efficiency of the system under high concurrency and the security of user privacy. Therefore, it is necessary to ensure the security of collection, deployment, network and other aspects.

The power blockchain provides a reliable solution to the problem of excessive central pressure under the high concurrency of the power Internet of Things system, but the risk of privacy leakage still exists in the blockchain system working in the open environment. This paper proposed a power blockchain guarantee mechanism based on trusted computing that combines the advantages of the current power blockchain to jointly maintain the safe operation of the power blockchain system and the security of sensitive information in the system from the hardware and software levels, The system guarantees the credibility of the operating environment of the blockchain node through the TPM chip, and guarantees the credibility of the collection terminal and the collected information through the contract.

2 Key Concept

2.1 Trusted Computing

With the rise of emerging Internet computing models such as the Internet of Things and cloud computing, it has brought extremely serious security problems while facilitating people's lives. Trusted computing emerged as an effective solution.

Hardware-based trusted computing is an active defense technology. By adding a root of trust to the computing system and establishing the operating environment for isolated execution, and the trust relationship is extended from the bottom layer to the upper layer applications, thereby realizing hardware-based active protection. Trust means that the entity always proceeds towards the predetermined target result in a predetermined manner. The Trusted Computing Group (TCG) released the TPM2.0 specification in 2015, which further increased the authorization level and became an ISO/IEC standard.

2.2 Blockchain

Different from traditional centralized database, blockchain is in essence a decentralized distributed database technology. It maintains a chain structure of data blocks among participating nodes and maintains continuously growing and non-tamper able data records based on cryptography.

Each block can be logically divided into a block header and a block body. Each block is connected in series by the hash value of the block header, and each block header is associated with all transactions in the block through the Merkle root. The blockchain will synchronize transaction information to the entire network, and each client stores the latest transaction information, forming a decentralized storage method. When some nodes fail, it will not affect the operation of the entire system.

Consensus mechanism is the soul of blockchain. It is the core technology for blockchain to solve trust problem with decentralized idea. Its purpose is to maintain the consistency of blockchain system. The most common consensus mechanism is Proof of Work (PoW). Miners need to use their own computing power to calculate a hash problem, PoW mechanism is to use the solution of the problem to prove the credibility of the data, so that nodes get the right to keep accounts. This problem is computationally difficult but easy to verify. When a blockchain node wants to create a block, it must solve the problem and then broadcast it to other nodes. All nodes in the blockchain system will take the longest chain as the main chain of the system to complete the system consensus.

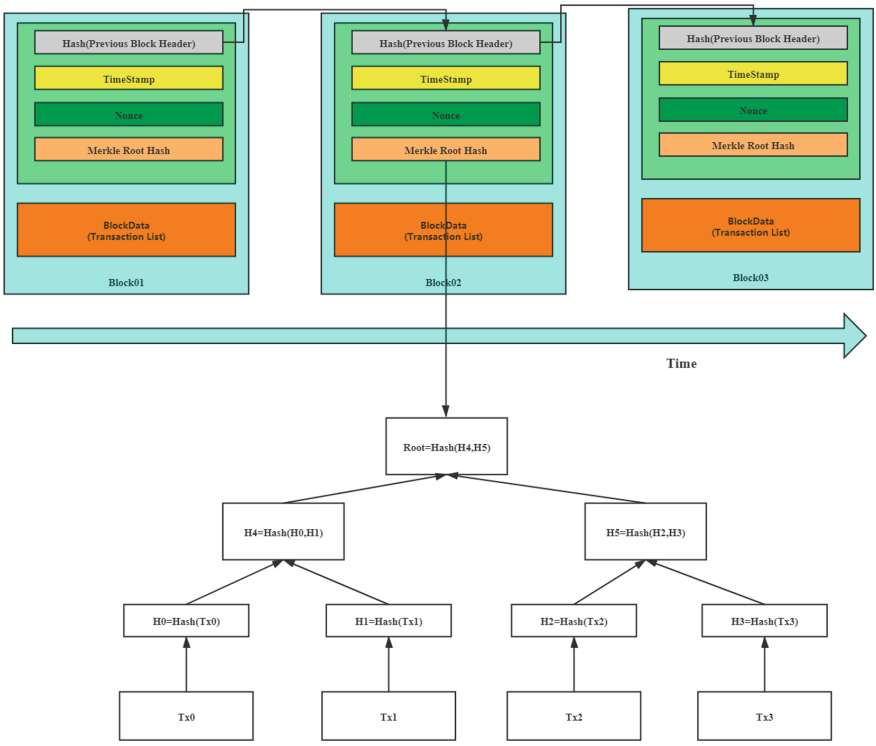

Fig. 1. Blockchain structure

A smart contract is composed of transaction processing and a state machine. It is a set of rules that are executed automatically by a computer system and needs to be jointly formulated by multiple participants. Smart contracts can make a set of complex and conditionally controlled rules execute in a pre-defined order. The smart contract defines trigger conditions. When the trigger conditions are met, the smart contract can be in the blockchain without human participation. The results of execution can be published in the blockchain network and added to the blockchain through the consensus mechanism. The bytecode of the smart contract is stored in each blockchain node, and the failure of one node does not affect the overall operation of the system. The scheduling process of the smart contract is also recorded and traceable by the blockchain, ensuring the safe operation of the smart contract (Fig. 1).

3 Related Works

The traditional Internet of Things system adopts the mode of central server-client terminal and connects to the Internet of Things devices through cloud computing. Due to the limitation of storage capacity of server and transmission bandwidth, it is easy to cause server paralysis under the scenario of high concurrency of mass terminals. Data centralization also brings security risks to user privacy. The decentralization, traceability and anti-tampering of the blockchain provide solutions to the hidden dangers of the Internet of Things [1]. However, as the blockchain works in an open environment and is vulnerable to malicious attacks. How to integrate the blockchain with the Internet of Things efficiently under the premise of ensuring privacy security has become a hot research topic at present.

Reference [2] proposes a scheme to guarantee the privacy of the Internet of Things based on block chain, which uses blockchain to solve the access control problem of distributed Internet of Things. Reference [3] uses the decentralization, non-tampering, and smart contract characteristics of the blockchain to combine blockchain technology and access control to design a smart contract-based access control system for the Internet of Things. Ding et al. proposed an attribute-based access control method for the Internet of Things, which simplifies the access control protocol of Internet of Things devices by storing attribute data through the blockchain and avoids illegal data tampering [4]. Liu proposed a blockchain-based distributed trusted network connection architecture (B-TNC), which builds a trusted blockchain network based on hardware [5]. Town Crier is an authenticated data feed scheme that uses Intel SGX as a trusted execution environment and uses trusted computing technology to ensure the credibility of external data used by smart contracts [6]. Zhang proposed a consensus mechanism based on integrity proofs to execute transactions, execute smart contracts, and protect sensitive data [7].

In summary, although blockchain IoT devices can be used to store access control strategies to ensure that access control can be traced and decision results cannot be tampered with, the privacy data protection and the efficiency of smart contract execution in blockchain are important factors that prevent the combination of the Internet of Things and the blockchain. Although the security of smart contracts can be enhanced by adding trusted computing technology, there are still limitations in security and efficiency. The Town Crier solution is only for external data and cannot guarantee the security of the

smart contract execution environment. The blockchain body based on integrity proof weakens the decentralized characteristics of the blockchain, and there are still hidden dangers in high concurrency scenarios.

Based on the characteristics of power system service, this paper combines the power blockchain with trusted computing technology and proposed a trusted power blockchain system through Access Service Chain, Log Service Chain and Remote Proof Chain. The Access Service Chain (ASC) is a blockchain composed of multiple Certificate Authority (CA) and a high-performance trusted CA server. The trusted server has enough storage and computing power to support the operation of the system. The trusted server takes the TPM chip as the trust root, which can establish the trusted system [8] from the CPU instructions and execution links, build the trusted operating environment during the server operation, filter the illegal access, and dynamically defend the server in real time during the operation process. Log Service Chain (LSC) is a block Chain composed of high-performance trusted servers, which also integrates TPM as the trust root, and designs a malicious sensor detection scheme to monitor the security status of sensors in real time. Remote Proof Chain (ROC) records the link relationship between the TPM public and the TPM chip, which can provide remote proof and remote authentication functions to ensure the authenticity of the TPM and its key information. Through the integration of trusted computing and power blockchain, this paper jointly guarantees the credibility of the collection terminal and server in the power blockchain from both hardware and software aspects, ensuring the security of the privacy data of each user and the security of the smart contract execution environment in each blockchain node.

4 System Architecture

The decentralization characteristic of blockchain has made it very promising in the context of massive data such as the Internet of Things. The blockchain has been widely used in the Internet of Vehicles, smart home and other Internet of Things scenarios. This system combines power blockchain with trusted computing technology to maintain the security of the blockchain network and the security of private data in the blockchain node while ensuring the service efficiency of power blockchain.

The overall architecture of the power blockchain system based on trusted computing includes three blockchains, namely the access service chain, the log service chain, and the remote proof chain. Compared with the traditional blockchain, this system adds a trusted chip to each blockchain node, so that each blockchain node has strong identity authentication. The system creates a credible power Internet of Things working environment through trusted chips and malicious node detection mechanisms. The system requires that the access terminal contains a trusted chip, and the visitor needs to go through the double test of the access strategy and integrity certification when entering the network, which prevents malicious terminals from illegally accessing system resources and ensures the credibility of the network terminal.

The TPM chip integrates multiple cryptographic algorithms, encapsulates keys, and can provide multiple trusted computing functions, such as measuring platform integrity, verifying integrity information, encrypting sensitive messages, and signing. These functions can be implemented inside the TPM chip, separated from other parts of the system,

so malicious code that tampered with the system cannot affect the execution environment inside the TPM.

TPM Remote Authentication: The system sets that all terminals requesting access to the system need to contain a TPM chip, and the signature verification key in each TPM chip is bound to the TPM chip and stored in a trusted third party (remote proof chain). The remote proof chain can verify the authenticity of the key.

TPM integrity measurement process is as follows:

When the system is initialized, TPM will perform a static integrity measurement on the system and generate an integrity value before all applications run. When the application starts to run, the integrity measurement program measures the running status of each application and module at the top and stores the generated integrity measurement value in the trusted register (PCR) in the TPM. Since PCR cannot be obtained from outside, the integrity value in PCR is considered safe. In order to verify the integrity measurement value, TPM records the PCR log, which records all the steps in the integrity measurement process. The verifier can quickly calculate the PCR value from the log and compare it with the original value to verify the legitimacy of the integrity certification process.

TPM can also provide remote integrity certification. The TPM contains a dedicated integrity message signature and signature verification key pair, which can be certified by the TPM authority. Because the key is stored in the hardware, the security of the key generation process is guaranteed. At the same time, external malicious users cannot steal the private key information in the hardware, which preventing signature forgery. The process of remote integrity certification is as follows:

The requester extracts the log information of the integrity measurement and signs it with the signature key to provide the verifier with the signed message.

$$ISM = Sign_{Isk}\left(M_{Log}, Pval\right) \tag{1}$$

In the message, ISM is the signed message, Isk is the signature key, *MLog* is the partial integrity message in the TPM log, and Pval is the integrity measurement value of the requester. To ensure the real-time performance of the message, the requester needs to attach the timestamp information, and the final message sent is {*ISM*,Ts}.

After receiving the message, the verifier first verifies whether the message is real-time according to its own clock information, and the system sets a timeout threshold T_{res}. If $T - Ts < T_{res}$, is satisfied, the verifier starts the verification.

$$M_{Log}, Pval = Ver_{Ivk}(ISM) \tag{2}$$

Ivk is the verification key. The verifier uses the integrity verification module (IVM) to re- verify the integrity of the log message M_{Log} of the log requester.

$$Pval' = IVM\left(M_{Log}\right) \tag{3}$$

Compare whether $Pval'$ is consistent with the received *Pval*. If they are consistent, the verification is successful, otherwise the verification fails (Fig. 2).

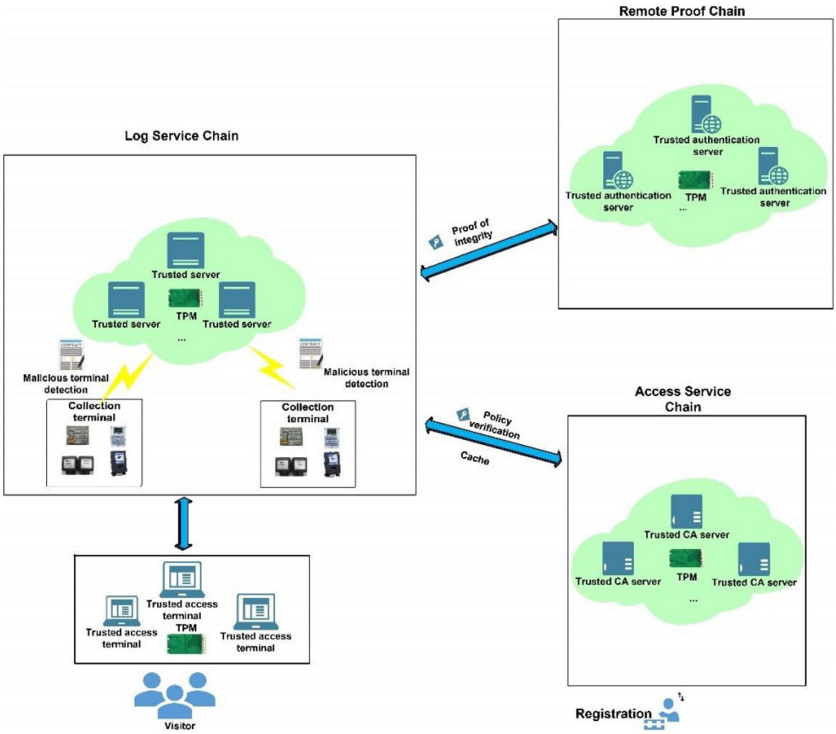

Fig. 2. System architecture

4.1 System Initialization

The system default asymmetric encryption algorithm is ECC algorithm, symmetric encryption algorithm is 128-bit AES algorithm, and signature algorithm is 256-bit ECDSA algorithm.

1) Each trusted server in the access service chain, log service chain and remote proof chain generates its own public and private key pair through the trusted chip and stores the public key information in the blockchain.
2) The access service chain selects nodes randomly to generate a blockchain master key pair (*ASCMPUK*, *ASCMPrK*) and synchronizes to the blockchain network. The log service chain and the remote proof chain respectively generate key pairs in the same way.(*LSCMPUK*, *LSCMPrK*, *ROCMPUK*, *ROCMPrK*).
3) ASC needs to set the parameter L = (p, a, b, G, n) for the system to determine the elliptic curve E in the finite field GF(p). It is used to systematically encrypt communications.
4) ASC negotiates the session key with ROC and LSC.

Since the efficiency of symmetric encryption is much higher than that of asymmetric encryption, the communication between blockchains adopts symmetric encryption,

which requires the exchange of keys before communication. The key negotiation process between ASC and LSC is as follows:

1) The access service chain selects the leader node, and the TPM of the leader node generates a random number A, Basic Key, and the timestamp information, which are encrypted with the private key *ASCMPrK* and sent to LSC. The randomness of A is guaranteed by timestamp information and TPM identification information.
2) LSC uses the ASC public key to verify the validity of the message after receiving the message. After successful verification, LSC stores the Basic Key, random number A, and generates random number B in the same way. and sends B to ASC after encryption with private key LSC_{MPrK}.
3) After receiving the message from LSC, ASC uses the public key *LSCMPUK* of LSC to decrypt the message and obtain the random number B. ASC uses TPM to combine random numbers A, B and Basic Key to generate the session key *SKAL*. At the same time, the session key is used to encrypt the negotiated message and send it to LSC.
4) LSC combines the random numbers A, B and Basic Key to generate the session key$SKAL'$ using the same algorithm. After receiving the ASC message, LSC uses $SKAL'$ to decrypt the message. If the decryption is successful, the key negotiation is completed. The LSC feeds back a message that the session key negotiation is successful to the ASC.
5) After ASC receives the message, the negotiation is completed.

The negotiation process between ASC and ROC is consistent with the above process.

4.2 User Registration

The terminal which the user used to access the IoT contains a TPM chip that can be verified on the remote proof chain. The TPM can provide functions such as secure storage, integrity measurement, and trusted password services.

1) The user encrypts the personal identity certificate and TPM public key information (*UTpmpuk*) with the ASC public key and sends it to the ASC.ASC examines user information and sends a remote public key verification request to a trusted TPM verification third party after successful review.
2) After the ROC receives the verification request, it will verify whether the public key is trustworthy, and the result will be signed with the master private key (*Rmprik*) and feed back to the ASC. To verify the real-time nature of the message, a timestamp information will be added after the message. The final message sent is Msg = $\{Sign_{roc}, Ts_{roc}\}$ Ts_{roc} is the timestamp information.

$$\mathrm{Res}_{\mathrm{u}} = Ver_{TPM}\left(UTpm_{puk}\right) \tag{4}$$

$$\mathrm{Res}_{\mathrm{u}} = Ver_{TPM}\left(UTpm_{puk}\right) \tag{5}$$

3) After receiving the feedback result, the ASC verifies the real-time performance of the received message through its own timestamp information Ts_{ASC}, and discards the message if the message times out.

ASC uses the ROC public key to verify the ROC signature. If the verification is successful, it can prove that the user terminal contains a trusted TPM chip.

$$Res_{uASC} = Ver_{R_{mpub}}(sign_{roc}) \tag{6}$$

4) The system recognizes that the registered terminal is credible, and the TPM chip in the leader node generates a random number A by combining user identity information, and generates a credible key based on the random number A.

$$U_{pub}, U_{pri} = Gen(A) \tag{7}$$

After the user key is generated, the leader node generates a random integrity evidence (RIE) for the user to detect the integrity of the user's communication. The leader node signs the key and integrity evidence with its own private key (LN_{pri}) and then publishes them to the blockchain network.

5) After receiving the signature message of the leader node, other nodes of the blockchain verify the authenticity of the signature. After a certain number of nodes are successfully verified, the user key can be determined to be valid.
6) ASC sends the key information to users through secure channels.

A legal device owner can grant other legal users access to their own devices, ASC writes authorization rules into the blockchain to provide LSC with legal access policy authentication.

4.3 Malicious Node Detection

The system uses a combination of hardware and software to ensure the credibility of the operating environment of the power Internet of Things collection equipment. LSC adopts a malicious node detection technology based on smart contracts to conduct real-time credibility evaluation of terminals, and promptly investigate terminals with low credibility values to maintain the credibility of the system operating environment.

The structure of the smart contract is SC-ASC = (LS, ES, Sen, θ, P, σ, Loc, Time).

LS is the leading trusted server, responsible for issuing smart contracts. ES is the contract execution server, Sen is the collection terminals to be detected, σ is the evaluation index (PLR, MDR, CDR, HBRT), P is the credit score, and σ is the threshold. Loc is the position of the node to be detected.

The detailed process of malicious node detection is as follows:

ES first checks the timestamp information that detects whether the message forwarded by the terminal is out of date. And if the message is out of date, it will be dropped. The system records the number of timeout messages of each node. At the same time, the system sets the threshold σ_T. If the ratio exceeds the initial threshold σ_T, the node is directly judged as a malicious node. Then LS detects the location information in the message. If the location information is severely distorted, it directly determines that the current communication is malicious communication, records and discards the malicious data packet. The system also sets the threshold σLoc, when the ratio of the node's distorted location message exceeds the initial threshold σ_{Loc} in a certain period of time, the node is directly determined as a malicious node.

After verifying the time stamp information and location information, the system preliminarily determines that the current communication is normal communication, and then the system continues to receive data packets and calculates the credible score value of the current communication. The calculation standards are as follows:

Packet Loss Rate: Since malicious nodes and unreliable links will increase the node's packet loss rate, the packet loss rate can be used as one of the criteria for measuring malicious nodes.

$$PLR = 1 - \left(\frac{n_{recv}}{n_{send}}\right) \tag{8}$$

n_{recv} is the number of successfully received data packets, and nsend is the number of all the data packets sent in the current time interval.

Message Delay Rate: S Since malicious nodes will increase the delay when processing data, in order to ensure that the received data is valid, the system records the time taken by the current collection terminal from collecting data to forwarding data, and at the same time sets the time interval Td to calculate the message delay rate.

$$MDR = \begin{cases} (T_{sensor}/T_d) & T_{sensor} < T_d \\ 1 & T_{sensor}{}^3 T_d \end{cases} \tag{9}$$

Communication Delay Rate: The response time of malicious nodes is longer than that of normal nodes. The system records the complete time from when the node to be detected receives the request to when the requester receives the response within a certain time interval. This delay is mainly for the messages on the communication link.

$$\text{CDR} = (\text{T}_{hd} + \text{T}_{td})/\text{T}_e \tag{10}$$

$$\text{T}_{td} = Ms/Nb + Pd/ts \tag{11}$$

Thd is the processing time, *Ttd* is the propagation time of message, Ms is the current size of message, Nb is the bandwidth of network, pd is the propagation distance, ts is the propagation speed, and *Te* is the preset time interval.

Historical behavior: Malicious nodes often communicate continuously within a certain interval. T The system calculates the ratio of malicious information to normal information of the node in a certain time interval as one of the reference standards for reputation value.

$$\text{HBR}_\text{T} = \text{Num}_\text{MB}/(\text{Num}_\text{NB} + \text{Num}_\text{MB}) \tag{12}$$

NumMB represents the number of malicious communications, *NumNB* is the number of normal communications, and T is the time interval.

The current communication score (Communication Score, CS) of the node is:

$$CS = \lambda_1 * PLR + \lambda_2 * MDR + \lambda_3 * CDR + \lambda_4 HBR_T \tag{13}$$

The ratio of each factor can be adjusted according to different scenarios, and it needs to satisfy $\lambda 1 + \lambda 2 + \lambda 3 + \lambda 4 = 1$. The system sets the threshold K. If $\text{CS} \leq \text{K}$, the current communication is normal communication, otherwise it is malicious communication.

The total communication reputation P of the node to be detected is determined by the number of malicious communications (*NMB*) and the number of normal communications (*NNB*).

$$P = \frac{e^{N_{NB}}}{e^{N_{NB}} + e^{N_{MB}} + 1} \tag{14}$$

The system sets the threshold σ. The collection terminal is recorded as a malicious terminal when $P \leq \sigma$. LS announces the information of malicious nodes to the entire network through the consensus mechanism and removes it from the trusted network.

4.4 Remote Access Policy Verification Mechanism

The Internet of Things has high requirements for the real-time nature of messages. The traditional blockchain uses a proof-of-work mechanism (PoW). Since the blockchain works in a completely open environment, the only way for an attacker to control the blockchain is to occupy with more than 51% of the entire network's computing power, and the cost of an attack is too high. What's more, the PoW mechanism requires a lot of computing power, which cannot meet the requirements in the power Internet of Things scenario. The server containing the TPM chip has a strong identity certificate that cannot be forged. The system has established a trusted verification chain (TVC) in the ASC that is specifically responsible for verification. Since each node in TVC is highly credible, the system can randomly assign accounting nodes without using the traditional consensus mechanism of proof-of-work, which improves the efficiency of the system. This paper designs a trusted verification mechanism based on a trusted server in the log record chain to efficiently verify user access rights and improve the system operating efficiency.

The system sets a parameter N. N is the number of trusted servers that need to participate in the verification, which can be adjusted according to different scenarios. N is set to 12 in this paper. To ensure the efficiency of verification, the TVC stores the cache of the verification strategy in the ASC.

The process of TVC trusted verification is as follows:

1) Randomly select a verification node from N nodes to establish communication with visitors. For example, assume that node 1 is selected
2) Set node 2 as the TVC accounting node at this time. Node 2 anonymizes the visitor's integrity information and verifies the authenticity of the integrity information with the ROC. If the ROC verification is unsuccessful, it rejects the visitor's access request. If successful, continue to step 3.
3) Node 2 verifies whether there are the visitor's access strategy and integrity evidence from the ASC cache. If the visitor's information does not exist in the cache, step 4 is executed. If it exists, go to step 5.
4) Node 2 requests ASC to update the cached data, and then queries again whether there is visitor's information in the blockchain, if it exists, execute step 5, if it still does not exist, then reject the visitor's access request.
5) Node 2 verifies whether the integrity evidence in the blockchain is the same as the evidence provided by the visitor. If they are the same, it proves that the information has not been modified, otherwise the verification fails.

6) Node 2 determines whether the visitor's access request meets the requirements according to the access policy in the ASC, and writes the judgment result into the blockchain system.
7) Node 2 returns the verification result to the visitor, and writes the verification process into the blockchain system for other verification nodes to check.

The Power Internet of Things is the application of the Internet of Things in the smart grid. The power system is realized the interconnection of everything in the power system and human- computer interaction with a smart service system with comprehensive status perception, efficient information processing, and convenient and flexible applications through the data collection, authority control, and status monitoring of key links in the power grid system such as power generation, transmission, transformation, distribution, and power consumption.

Through the data acquisition, access control, condition monitoring in the grid system's power generation, transmission, substation, power distribution process, power IoT realized the interconnection between all things in each step of the power system, human-computer interaction. Power IoT is an intelligence system which has the characteristics of state comprehensive perception, efficient information processing and convenient and flexible application.

The data collected by various smart meters in ASC is stored in the ASC blockchain. The trusted server can verify the reputation value of each terminal in real time, avoiding malicious terminals from uploading malicious data. The specific operation process of the trusted power Internet of Things system based on the blockchain is as follows:

1) If the visitor A wants to access the data in the power Internet of Things, the visitor terminal collects its own integrity status information through the TPM integrity collection module, The integrity status information, the requested access resource information (*Requ*), and RIE obtained at registration are packaged and encrypted with the private key and sent to the TVC.

TVC queries the visitor's public key information through the ASC cache and decrypts the visitor's request packet.

TVC randomly selects nodes to verify the visitor's access strategy and integrity through the trusted remote verification strategy, to determine whether the access terminal is credible and whether the access terminal has the legal access rights to the requested data.

If the verification is passed, LSC randomly selects the lead node to record the visitor's access behavior, and obtains the electricity data information requested by the visitor in the blockchain, uses the private key of blockchain to sign, and then uses the visitor's public key to encrypt the message and send to the visitors.

After receiving the message, the visitor uses his own private key to decrypt the message, and uses the blockchain public key to verify the authenticity of the source of the message.

The use of trusted computing combined with the power blockchain greatly reduces the risk of the paralysis of the central server and the leakage of privacy under high concurrency situations. The system separates each permission into different blockchains,

solving the problem of excessive centralization of strategic decision-making in the traditional power blockchain system. Through trusted computing, the security of each blockchain server operating environment, power blockchain collection terminal, and power blockchain access terminal is guaranteed, which is more in line with the actual network operating environment.

5 Analysis

Anti-eavesdropping Attack: An eavesdropping attack means the attacker monitors the communication channel between the two parties to obtain unencrypted sensitive data from both parties. Although it will not affect the normal operation of the system, it will lead to the leakage of user privacy and cause serious consequences. The communication between the user and the blockchain is encrypted communication, which ensures that the information will not be eavesdropped by unauthorized users.

Anti-replay Attack: A replay attack refers to a malicious node republishing data packets in the previous system to the system, causing system performance degradation. This system includes timestamp information in all communication processes, and both parties in communication receive messages After that, first verify whether the difference between the synchronized clock information and the time stamp is less than the threshold THR, and only when the time difference is within the allowable range, the message is considered as a valid message.

Anti-witch Attack: A witch attack means that a single node has multiple identities and disrupts network behavior. Since the identities of users and blockchain nodes in the system are protected by trust, malicious nodes cannot forge identities.

Decentralized and Traceable: The system integrates each permission into three blockchains and greatly reduces the pressure on the central server by using the decentralized nature of the blockchain. At the same time, all operations in the blockchain will be recorded. It can be traced at any time, avoiding the problem that the traditional central server cannot supervise, and enhancing the user trust.

6 Summary

In the primary stage of power Internet of Things research, how to ensure the service efficiency of massive data under the high concurrency and the security of private data in the Internet of Things is particularly important. The power blockchain guarantee mechanism proposed in this paper combined the advantages of the trusted computing and the power blockchain, which not only removes the serious centralization problems of traditional power Internet of Things, but also guarantees the security of each blockchain node server through trusted computing. It solves the defect that blockchain nodes are vulnerable to be attacked in the open environment. Through remote integrity verification and policy verification, the system guarantees the security of networked terminals. At the same time, a reputation-based malicious node detection scheme is designed at the collection layer to monitor the status of each collection terminal in real time. It will find

malicious terminals in time and remove the suspect terminals with low reputation from the network to guarantee the authenticity of the collection terminal and the information collected by the terminal. In summary, the power blockchain guarantee mechanism based on trusted computing greatly improves the security of system operation while ensuring the efficiency of power services.

Acknowledgment. This work is supported by Science and Technology Project of STATE GRID ZHEJIANG ELECTRIC POWER CO., LTD. (5211DS200002).

References

1. He, Z.Y., Duan, T.T., Zhang, Y., Zhang, H.W., Sun, Y.: The application and challenges of blockchain technology in the internet of things. J. Appl. Sci. **38**(01), 22–33 (2020)
2. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha, Á., Serrhini, M., Felgueiras, C. (eds.) Europe and MENA Cooperation Advances in Information and Communication Technologies. Advances in Intelligent Systems and Computing, vol. 520, pp. 523–533. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-46568-5_53
3. Zhang, J.H., Cui, B., Li, R., Shi, J.S.: Access control system of internet of things based on smart contract[J]. Comput. Eng. **47**(4), 21–31 (2021). https://doi.org/10.19678/j.issn.1000-3428.0058302
4. Ding, S., Cao, J., Li, C.: A novel attribute-based access control scheme using blockchain for IoT. IEEE Access **7**, 38431–38441 (2019)
5. Liu, M.D., Shi, Y.J., Chen, Z.N.: Distributed trusted network connection architecture based on blockchain. J. Softw. **30**(8), 2314–2336 (2019)
6. Zhang, C., Truxen, A.: Trusted computing enhanced blockchain (2020). https://arxiv.org/abs/1904.08335
7. Zhang, F., Cecchetti, E., Croman, K.: Town crier: an authenticated data feed for smart contracts. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, pp. 270–282 (2016)
8. Huang, J.H., Shen, C.X.: TPCM active defense trusted server platform design. J. Zhengzhou Univ. (Sci. Ed.) **51**(03), 1–6 (2019)