Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8533219, 10 pages
https://doi.org/10.1155/2022/8533219

Research Article

Application of Blockchain Technology in Electric Vehicle Charging Piles Based on Electricity Internet of Things

Haitao Liu,[1] Zhipeng Lv ,[1] Zhenhao Song,[1] Shan Zhou,[1] Wenlong Liu,[1] and Mu Fang[2]

[1]State Grid Shanghai Energy Interconnection Research Institute Co., Ltd., Pudong New District, Shanghai 201203, China
[2]State Grid Shangdong Electric Power Company, Jinan 250003, China

Correspondence should be addressed to Zhipeng Lv; 220202927@seu.edu.cn

Received 2 June 2022; Revised 27 July 2022; Accepted 16 August 2022; Published 31 August 2022

Academic Editor: Chia-Huei Wu

With the continuous development of urban intelligence, as traffic, power grids, and electric vehicles are new ideas to solve energy shortages and air control problems, they have received widespread attention from the society and strong support from the government. The charging pile is a key hub for data exchange and has typical characteristics of IoT terminals. However, the guidance of the grid connection of electric vehicles is not standardized, and the security and stability of the power grid will inevitably be affected. The blockchain has the characteristics that data is difficult to tamper with and decentralized. Based on these two characteristics, the information recorded by the blockchain is more authentic and reliable. This paper is aimed at realizing the global unified identification and management of large terminal equipment based on ubiquitous power Internet of Things equipment with the help of blockchain technology and at providing safe, efficient, and stable online management services for a large number of devices in the ubiquitous power Internet of Things. In this paper, we analyze the application possibility of blockchain technology in the current electricity market and apply blockchain technology to the electricity market to solve the drawbacks of the electricity market, as well as adding blockchain analytics to the renewable energy electricity market. The experimental data analysis shows that with the increase of the length of the blockchain, the blocking time of the new area increases correspondingly, but the overall performance declines slightly, so this scheme can meet the practical needs of a large number of concurrent access terminals in the ubiquitous power Internet of Things. It can be seen that the successful application of blockchain technology based on the power Internet of Things in electric vehicle charging piles has greatly improved work efficiency.

1. Introduction

Along with the rapid growth of the smart grid and the rise of the Internet of Things and blockchain, the combination of the three has become one of the development directions of the future power industry. If the choice of Internet 10 years ago is to take the bullet train, now choose "block chain + Internet of things" is to take the rocket, the Internet of everything is the future development trend, for example, our most common home smart system enables us to use a mobile phone to remotely control all the electrical appliances in the home. With the rapid development of technology, the evolution of the Internet of things, which is based on the Internet, has been accelerated. At present, the Internet is being connected to several billion devices worldwide. The power Internet of Things is the application of the Internet of Things in the smart grid. It is the result of the development of information and communication technology to a certain stage. It will effectively integrate communication infrastructure resources and power system infrastructure resources and improve the level of power system informatization and facility utilization.

As a key measure to deal with the energy crisis and environmental governance, electric vehicles have received much attention and strong support from society and the government. Electric vehicles are a new type of deployable load that can either receive power from the grid through charging or release power to the grid, depending on the characteristics of their own mobile storage loads. If EVs are not guided in an orderly manner, they will bring a series of challenges to the safe and stable operation of the grid, including increasing the peak-to-valley load difference, affecting power quality, and reducing the reliability and economy of the distribution network. In view of this, this paper combines blockchain technology and IoT to further address these challenges in power distribution.

The Internet of Things is based on computers and a large number of electronic devices. It promotes the rapid development of the global information industry and brings great opportunities and challenges to people's lives. Therefore, its security problem is more and more prominent. First, the physical security problems are brought by mass device nodes, among the large number of equipment knots accessed by the IoT, a problem with the security of any one node can become a gap that affects overall IoT security. Second, weak authentication control leads to unauthorized illegal access, insufficient identity authentication, poor access control, and other problems, which may lead to uncontrolled device data and access rights. Finally, diversified data transmission modes bring security problems of data transmission. IoT devices use various wireless transmission methods in message transfer, and the data transmitted are very easily taken away or disturbed and interfered by the attackers [1]. The decentralized, distrustful, and tamper-proof characteristics of blockchain ensure the security and authenticity of the grid in the transaction, reconciliation, information transfer, and closing process, while reducing regulatory costs and improving operational efficiency.

The application advantages of blockchain technology have attracted much attention in the field of information technology, and scholars from all over the world have carried out research on its application trend. Abdullah and Faizal reviewed the cryptographic methods used in the blockchain sector in the current industrial revolution (industry 4.0). This implementation of cryptographic solutions is now widely used as a solution to cyber security issues, including the simplification. The review document shows that blockchain technology has great potential not only for financial services technical industries and manufacture but also for the public sector, healthcare, and the media industry. The document details how blockchain can be applied to different areas of technology to provide more security as well as protection from vulnerability attacks and abuse without having to delegate to a second person. However, the use of blockchain in various industries is helping to transform the industry [2]. Yermack assesses the prospective effects of the changes upon regulators, corporate investors, and the other various groups engaged with company management. Blockchain offers less expensive, greater liquidity, better records, and ownership transparency that could significantly change the power balance between each of this groups [3]. Dinh et al. first investigated the state of the technology, focusing on the private blockchain (where all parties are certified). Dinh et al. analyze productive as well as study-based applications in the context of its systems in four different layers: distributed ledgers, codes, consent protocols, and smart contracts. BLOCKBENCH, the framework for understanding the performance of private blockchains under data processing workloads for benchmarking, is introduced. Dinh et al. comprehensively evaluated three major blockbench-based blockchain systems, namely, Ethereum, parity, and hyperledger structures [4].

Blockchain and IoT can be applied to electric vehicle charging management. An et al. propose a location privacy protected online (LoPrO) scheme that can allocate electricity and charging stations in a microgrid to electric vehicles when energy supply is limited [5]. Kaur et al. propose an edge cloud framework in which cooperation between cloud and edge devices is implemented to make intelligent decisions related to electric vehicle charging and discharging, while achieving the expected balance of supply and demand [6]. The abovementioned scholars have studied the relevant application principles of blockchain technology, mostly in the financial field, but lack of reflection in the practical application of smart grid.

In order to solve the challenges brought by the electric vehicle power distribution problem, this paper proposes a safe and intelligent management method based on the ubiquitous Internet of Things combined with blockchain technology, which will be able to effectively solve the problem of a large number of electric vehicles connected. The advantages of IoT and blockchain technology in unified identification and data fusion are expected to realize IoT power terminal equipment management and provide safe, efficient, and stable online management of massive equipment.

2. Proposed Method

2.1. Unified Identification of Ubiquitous Power Internet of Things Communication Devices

2.1.1. Introduction to Blockchain. The earliest descriptive description of blockchain is that the concept of bitcoin was first proposed, and blockchain, as the core technology of bitcoin, came into being. However, the definition of blockchain has not yet been clearly proposed and is only used to record the accounting history of bitcoin transactions. Although blockchain technology was first proposed in 2008, it has only recently gained widespread attention. Blockchain is essentially a distributed ledger technology based on asymmetric encryption that records transactions only after they are checked through a common mechanism for all nodes on the blockchain [7]. This technology is supported by cryptography technology, and any number of nodes in the participating system records the information into the chain sequence block by hash cryptography algorithm. Each node has a fair position, can participate in the transaction authentication, and guarantees the authenticity and reliability of the transaction and cannot be tampered with by the encryption algorithm [8, 9]. Since each shareholder can confirm and reward the new blockchain according to the consensus mechanism, without the participation of the third party arbitration, the blockchain can be regarded as a decentralized distributed ledger. Core advantage is the ability to block chain of decentralization, at the same time be able to use data encryption, extensions, such as distributed consensus means, in the absence of mutual trust in the distributed system implementation, coordination, and cooperation, thus to

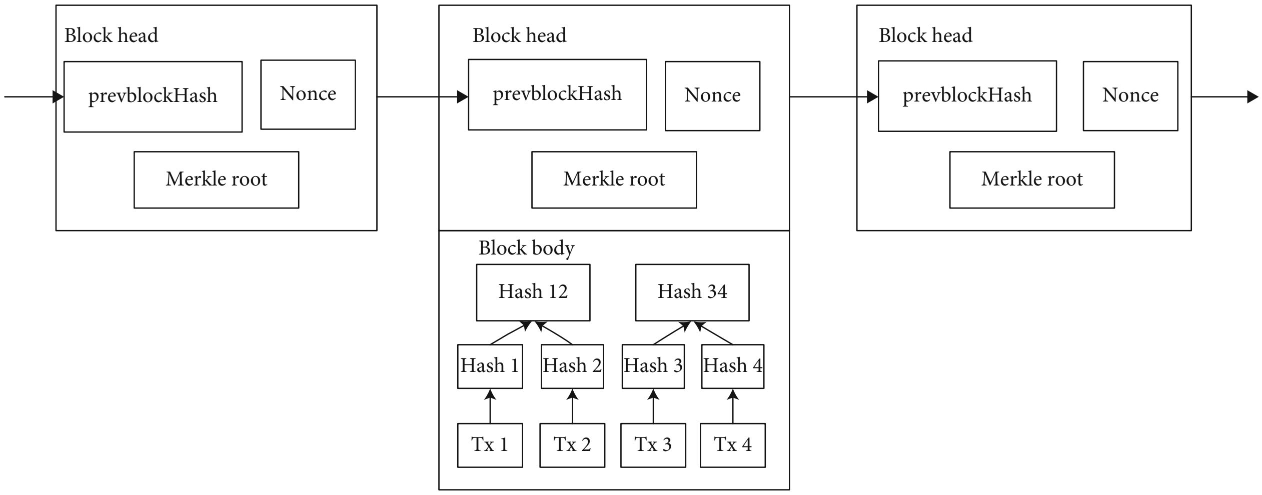

Figure 1: Schematic diagram of blockchain data structure.

solve the problem of high cost of centralized institutions are widespread, low efficiency, and data reserve uneasy congruent provides solutions [10].

Blockchain can provide disintermediation between digital asset publishers, app developers and consumers, and decoupling functions related to asset management, such as issuance, transaction processing, ensuring the security of users' funds, and establishing user identity. For example, on Ethereum, digital assets are released through smart contracts, with an estimated market value of over 10 billion yuan and still increasing. This trend indicates that more offline assets will be transferred to blockchain in the future, and blockchain assets will directly enter the asset allocation table of the middle class, with an increasing proportion [11].

2.1.2. Blockchain Structure. In order to realize the tamperability of data, blockchain introduces the chain structure with block as unit. In the case of bitcoin, each block consists of a block and a block. A block contains many transactions that have occurred since the previous block. The size contains the front block hash, random number, Merkle root, and so on. The hash value is the ID of the file, but it is stricter than the ID. Merkle root is used in blockchain to maintain the integrity and immutability of ledger verification data [12]. As shown in Figure 1, the blockchain data structure is described.

2.1.3. Features of Blockchain Technology

(1) Decentralization and Detrust. In the blockchain system, the entire network is not arbitrated by a third party, and an open and transparent set of encryption mathematical algorithms is used to enable the nodes in the entire system to automatically and securely conduct transactions without trust. The rights are equal between any individual nodes, with no impairment or failure of any of them affecting operation on the whole network.

(2) Nontampering. Blockchain data is open source, and each participant can copy a complete data from the interface. However, only if more than 51% of the nodes reached consensus in the control system can the data be tampered.

(3) Open and Transparent, Collective Maintenance. While the privacy of accounts processed in blockchain is encrypted, the rest of the data is public and open to all. Any participant can view it through a public interface, and each participant can participate in maintenance.

2.2. Use Blockchain to Solve Problems in Data Flow

2.2.1. Registration of Digital Assets. Digital asset registration is a prerequisite for the flow of assets on the blockchain. It is a challenge for assets to maintain the uniqueness of the whole network while ensuring that they cannot be tampered with. Many blockchains have previously implemented smart contracts, which define certain assets to be issued within the contract code. In a production environment, asset transfer is performed by running contract code through a virtual machine. However, there is a problem that in the process of user operation, if it directly targets the contract address, contract token and contract binary code, etc., it will not know the specific asset to be marked, nor can it mark the components of the asset [13, 14]. In the process of design thought about two solutions: offline state, the globally unique identifier (GUID) is by the kind of card, timestamp, and CPU data; the algorithm generated binary digital identifier length is 128, under the condition of effective, it is a little repeated strings, but in the current scenario, the GUID is unable to meet demand, it is just a series of irregular character, cannot record the actual properties of the assets, like COINS address at the same time, also read not friendly, and not easily to remember. In addition, GUID is not scalable enough to meet the additional attributes and regulatory requirements in the future, so it will not be a good choice. Online status defined a resource, it is easy to think of the DNS domain name system, the domain name system will be the host name resolves to IP address, using a global, hierarchical distributed database system, each domain name can be defined as a these resources are independent, but Internet

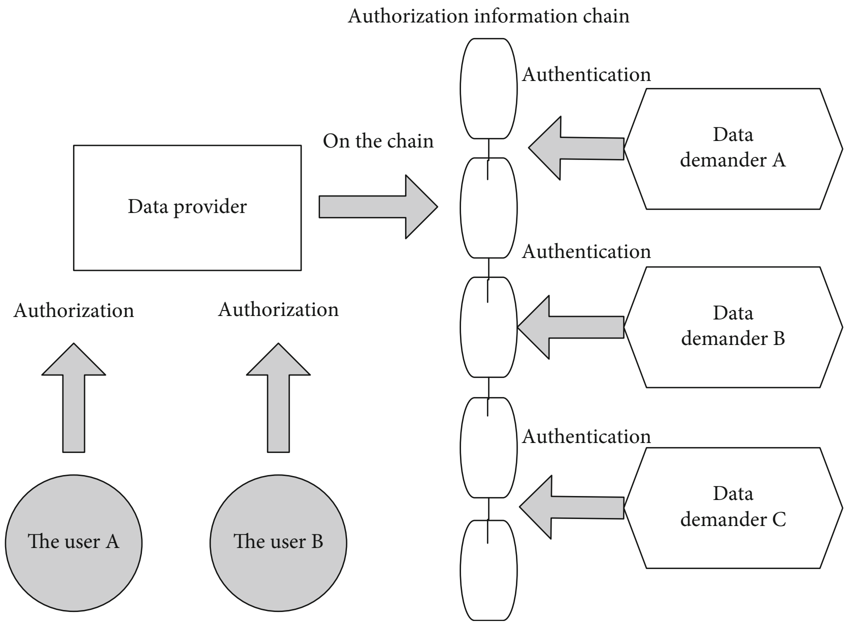

Figure 2: Schematic diagram of blockchain mode of data transaction user authorization depository.

sources are distributed autonomous systems, DNS is not autonomous system, and there are still some inherent defect [15].

ODIN is an open system for independently identifying a data content index and exchanging it in a web-based context. It follows the URI (Uniform Resource Identifier) specification and provides a scalable framework for independent, open, secure, and trusted data content management and intellectual property management for blockchain-based digital assets [16]. The owner of each ODIN identifier corresponds to a pair of asymmetric cryptography public as well as patient keys, which allows the independently published digital components to be signed by the private key, and the public key can be used to verify the individual receiving the industrial data contents to ensure that the received data is trusted and will not be tampered with. Combined with multilevel blockchain combinations such as Bitcoin, the ODIN identifier identifies any data content object uniquely with an index of open access, so as to accurately identify and extract the data content object. Once the ODIN identifier is generated, it is permanent and does not change as the owner or storage address of the data content object it identifies changes, and subsequent maintenance costs are low [17].

It is based on the description of the asset, we choose multilevel blockchain system integration tag, if we choose it in power IoT device as the parent ODIN prefix, the PKK:/351474.434/asset/DCS is to register the DCS this asset category of assets in the terminal equipment height 351474, and 434 deals in the DCS of attributes can be described using the JSON format data. Once the data is written, it represents the successful registration of the asset, and the ownership of the asset is determined by the private key of the account in the current ODIN system. Hierarchical control of the private key can make the hierarchy and management authority of the asset clearer. If the asset needs to change the property, it can also republish the new asset through the private key [18, 19]. Compared to the original chain into UTXO asset attributes, including design ASSET_UID fields, compared to the original chain itself as secondary or tertiary index sign, the definition of assets can be compared to the original chain to ensure that the entire network is unified, namely, after any registration on other block chain assets, once the implementation of this agreement access can be moved to trade than the original chain and circulation and solved many assets in different chains, possible fraud risk [20].

After the system registers the assets, the original chain will be through the internal API interface than the original chain asset details of the query. At the same time, a complete set of search engine can be realized on the agreement, and the details of digital assets can be inquired in different blockchains of the whole network, which is convenient for those who are in the know to inquire. Such a decentric marking protocol as PPK can solve the problem of repeated definition of cross-chain assets, and at the same time, it can reduce system risks due to the combination of multiple blockchain implementations [21].

By 2020, the number of connected devices in the world will reach 50 billion, and the amount of data generated by the Internet of Things will reach 4.4zb. The security and consistency of device data are facing severe challenges. Therefore, we proposed a new device solution and stored data through the blockchain technology. Through the blockchain technology, key issues in authorization, data source, and data flow can exist. Improve and implement new trade circulation methods, such as smart contracts [22].

In this case, the data is deleted from the original usage scenario, and the usage purpose is changed. With the gradual understanding of the value of data resources and the increasingly perfect industrial chain structure of big data, the demand for data circulation in China is increasingly urgent [23, 24].

Table 1: Basic feature information of data flow in blockchain mode.

The data flow	The data made by	Provide room to be authorized autonomously	Trading back
Intelligent contract	Classification management	Privacy protection	Automated trading
Data is stored	Trading based model	Blockchain structure	Asymmetric encryption
Consensus mechanism	PBFT/RBFT and other byzantine fault-tolerant classes are absolutely consistent consensus algorithms		
The network exchange	CA certification	Special access	Peer-to-peer networks

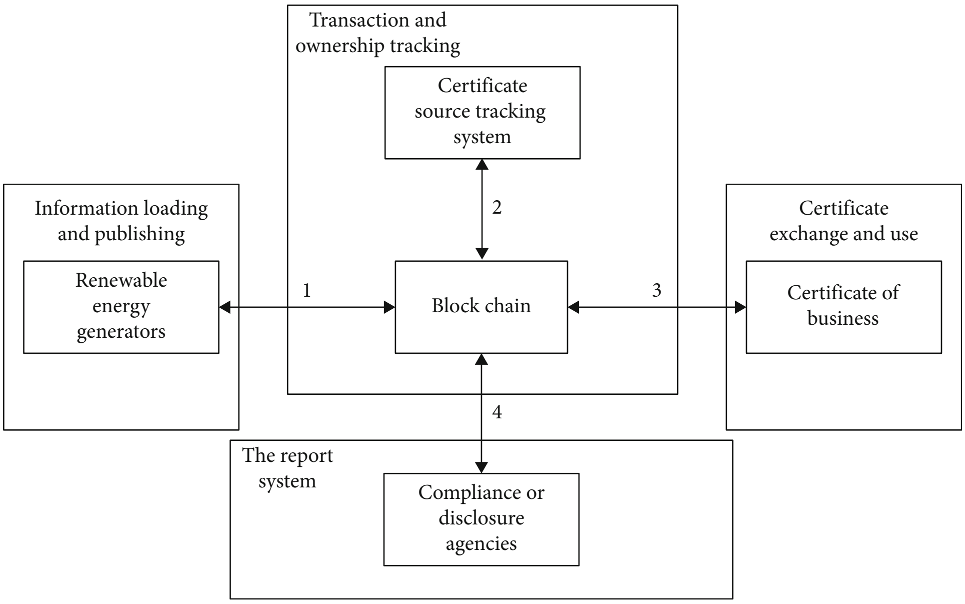
Transaction and ownership tracking
Certificate source tracking system
2
Information loading and publishing
Renewable energy generators
1
Block chain
3
Certificate exchange and use
Certificate of business
4
The report system
Compliance or disclosure agencies

Figure 3: Blockchain + renewable energy market.

2.2.2. Data Circulation. In traditional mode, the authorized store can be tampered with at will and has no credibility. Each application and data source company needs to sign a separate agreement because of the corresponding liability determination terms. In addition, querying authorization records requires the development of a separate interface that is often ignored and difficult for users to join and exit due to authorization and business process bindings [25]. The development of blockchain technology has made new breakthroughs in this field. In the blockchain mode, the complete authorization and authentication process is shown in Figure 2 and Table 1.

2.3. Power Grid System Based on Blockchain. The development of the energy Internet and the transformation of electric propulsion will change the identity of consumers. And combined with blockchain technology and communication technology, it can be promoted among millions of participants at the same time to ensure the security of transactions and payments. The distributed energy blockchain can directly provide renewable energy to users, realize local output, reduce transmission loss, and achieve "zero marginal cost in society. Take renewable energy as an example to illustrate the impact of blockchain technology on the power market.

The certification body then manually issues renewable energy “certificates” from the database, which middlemen use to connect buyers and sellers to complete the transaction. The whole transaction process takes a long time; there are many human factors, process, and other problems involved in the process; there are many shortcomings. However, with the addition of blockchain technology, the steps are reduced a lot, making the market more concise [26].

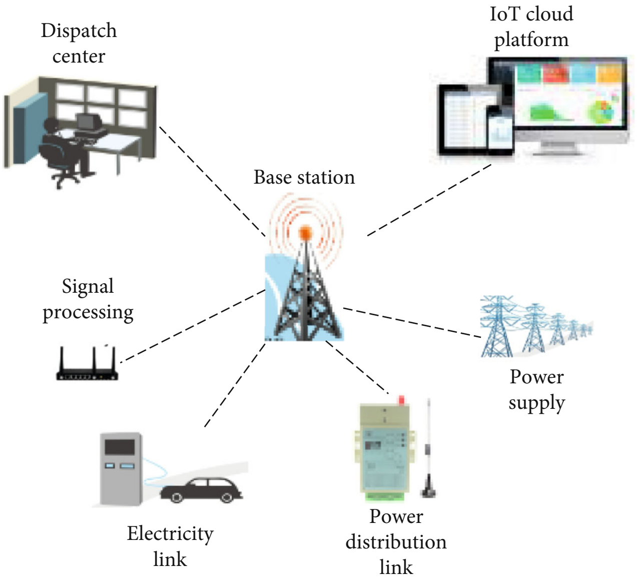

Figure 4: Power IoT device structure.

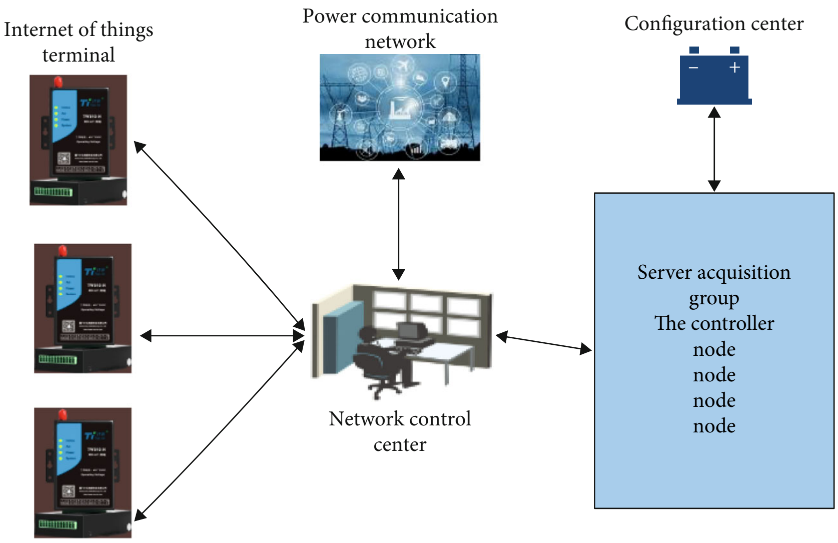

Figure 5: Simulation system architecture.

As shown in Figure 3, blockchain technology application in renewable energy markets, electricity meters will be directly connected to the blockchain, chain blocks at the same time as a public books will bring together all the data information, replaced the previous data manual transmission, the process of decentralization, and tamper-resistant features of block chain to ensure the data security and market transparency. All participants perform their duties according to the information stored in the blockchain, automating most of the processes in the current system, while eliminating some tedious intermediate links and making it easier for more users to enter the market.

The power grid equipment is established through the above technical methods. The structure of the power network equipment is shown in Figure 4.

3. Experiments

Electric vehicles are characterized by their random and volatile access to the grid. If their charging demand can be modeled based on historical statistics, it can provide important guidance for the subsequent development of a reasonable charging and discharging scheduling strategy. In this paper, we combine electrical IoT with blockchain technology to further explore a blockchain-based authentication scheme for electrical IoT access.

3.1. Experimental Background. A federated chain is a consortium or industry-managed blockchain of several institutions in which data is secure and can only be read, modified, or accessed by that institution. For example, from the perspective of commercial use, due to the small number of nodes, fast processing speed, and low transaction costs, the alliance chain is easy to establish a connection relationship with enterprises, and the country is also actively promoting it, which is widely used. The application groups are mainly banks, insurance, securities, enterprise groups, and enterprise groups. The typical feature of the alliance chain is that each node usually has a corresponding entity and can only join or exit the system with the approval of the alliance. Access rights and permissions are set to ensure the security of the system. The consensus process in a federated chain is controlled by preselected nodes and is a type of blockchain between a private chain and a publicly owned chain.

These features of federated chains are particularly well suited for the ubiquitous power IoT industrial ecosystem. A leading federated chain development platform is Hyperledger Fabric, a Hyperledger Project led by the Linux Foundation and contributed by Digital Asset and IBM. It uses Docker container technology to run smart contracts called chain code and provides a modular architecture to run nodes, chain code (smart contracts), configurable protocol services, and membership services.

3.2. Experimental Design. Power IoT systems are industrial applications. Therefore, we are building an experimental environment with a federated chain based on Hyperledger Fabric. Hyperledger Fabric's vision is to create a transparent, secure, and decentralized enterprise-grade blockchain solution. The experimental environment is a computing cluster consisting of five workstations. Each workstation is equipped with an inteli7-7700hqcpu with a main frequency of 2.80 GHz, 16 GB ddriii memory, and a 256 GB SSD hard disk. The operating system is CentOS7, running a Docker container-level virtualization system that emulates a P2P blockchain network. The container orchestration tool is Kubernetes 1.9; one of the five workstations is the cluster manager and the other four are compute nodes.

The IoT endpoints consist of a Raspberry Pi and a tablet. The Raspberry Pi is version 3b and is configured as a broadcom BCM283780SOC with an integrated 4-core armcortex-a5364-bit CPU, 1.4 GHz, and 1 GB lpddr2sdram. The tablet smart device is powered by Huawei M5 platform, Kirin 960ARM architecture chip, 4 main frequency, and integrated 2.4 G processing core, 4 GB RAM, and 64 GB memory [27].

The simulation system consists of client software running on the ubiquitous power IoT terminal, ubiquitous power IoT gateway software, and ubiquitous power IoT

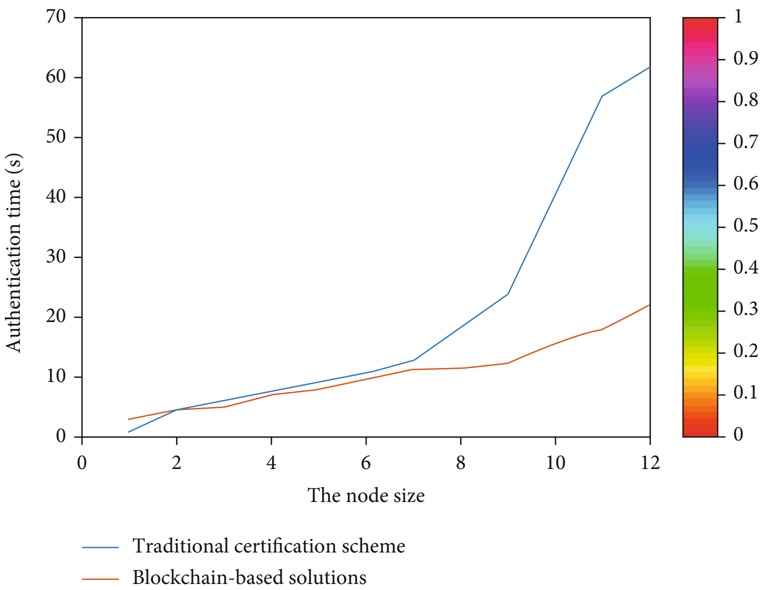

FIGURE 6: Certification efficiency curve.

terminal trust configuration software. The ubiquitous power Internet of Things is a smart service system that fully applies modern information technologies such as mobile Internet and artificial intelligence around all aspects of the power system and has the characteristics of comprehensive status perception, efficient information processing, and convenient and flexible application. The architecture of the emulation system is shown in Figure 5. The ubiquitous power IoT gateway is located in a computing cluster, and the ubiquitous power IoT endpoints are connected to the business network and authentication server cluster via a network controller.

Build the overall architecture based on the simulation system, determine the connection of input and output data of each test system based on the purpose of full power performance, and realize the synchronization of the power simulation system with the help of the clock synchronization system, the long-distance intelligent I/O interface system, and the intelligent gateway system, interconnection, to achieve integrated simulation.

4. Discussion

4.1. Time Required for Blockchain Technology to Access the Internet of Things in Power

4.1.1. Comparison between Traditional Scheme and Blockchain Scheme Based on Information Communication. Figure 6 shows the time taken by a trusted recipient of the ubiquitous power IoT endpoint from request to completion. The comparison curve is the time under centralized control of a traditional private key center. All data are averages of 10 experiments. The data results show that under the traditional centralized access authentication scheme, the authentication center's computational and network overhead increase as the number of IoT endpoints increases. When the number of endpoints increased by more than 10, the completion time increased significantly. Although it also showed an upward trend before, it was not more than 20, but when the number of endpoints exceeded 10, the completion time exceeded 60 in one fell swoop, leading to a decrease in authentication efficiency, which is directly reflected in a rapid increase in authentication time. Whereas blockchain-based authentication is a distributed approach with multiple layers of authentication, and blockchain-

TABLE 2: Impact of group size on certification efficiency.

Authentication group threshold t	Authentication time/s
$t = 3$	5.7
$t = 5$	9
$t = 7$	11.8

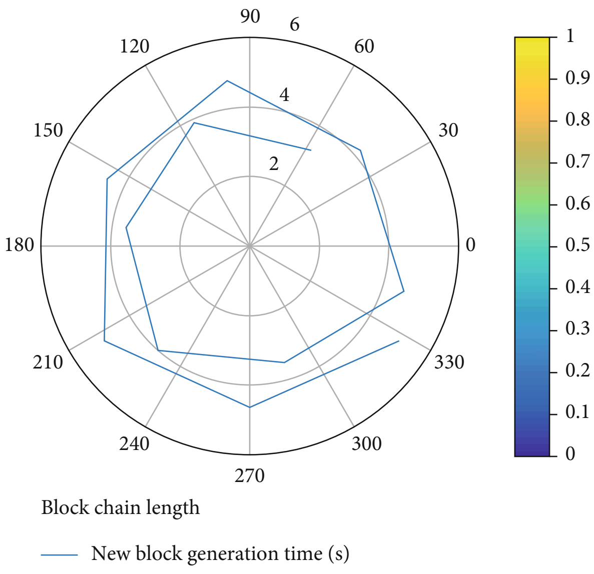

FIGURE 7: Block generation curve.

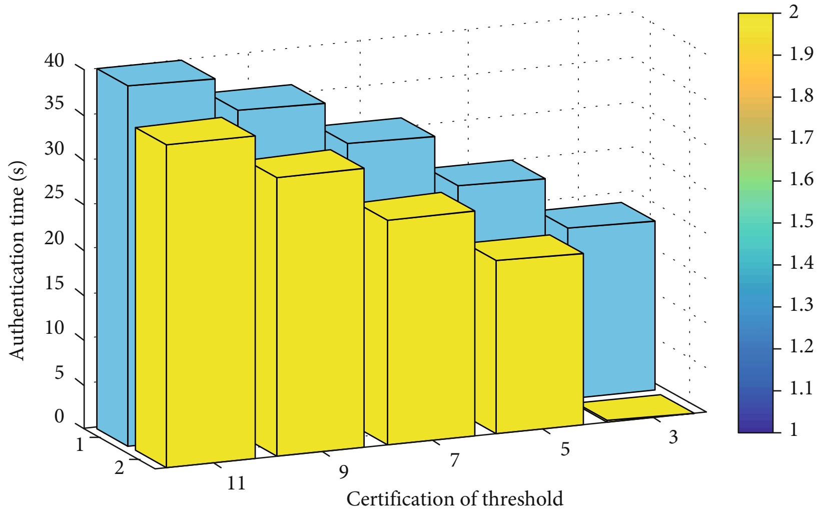

Figure 8: The effect of group size on authentication efficiency.

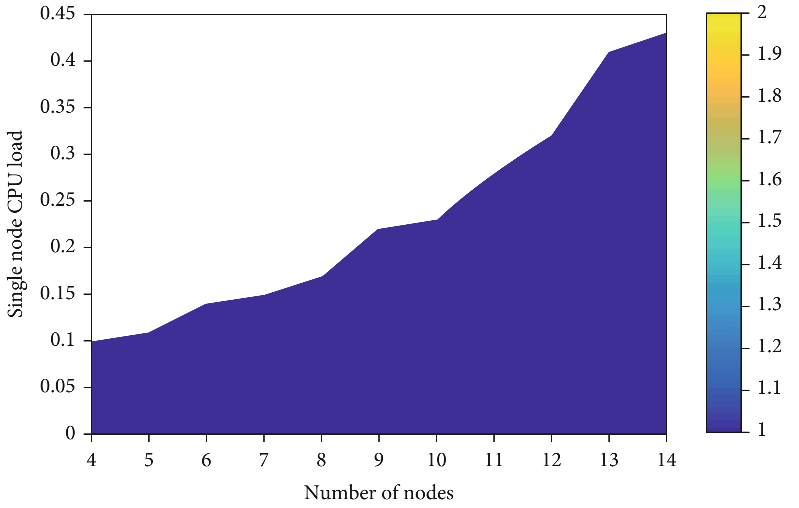

Figure 9: The CPU capacity with concurrent requests.

based solutions work by breaking the problem into many small parts that are distributed to multiple computers for processing. This can save the overall computing time and greatly improve the computing efficiency.

4.1.2. The Effect of the Size of the Accreditation Group on the Efficiency of the Accreditation. Table 2 shows the size of the same Internet of things node. The comparison of the authentication time of the threshold values of the authentication group is under 3, 5, and 7, respectively. It can be clearly seen that as the authentication threshold increases, the authentication time also increases.

Figure 7 illustrates a correlation of the new block generation duration with the size of the existing blockchain. The data shows that as the length of the blockchain increases, the new block generation of time increases accordingly, but the overall performance does not degrade significantly.

4.2. Analysis of the Influence of the Experimental Group on the Certification Efficiency. Figure 8 compares the authentication time of authentication group nodes with different thresholds for the same size of IoT nodes. Figure 9 shows how the CPU load on a single node increases with the number of nodes picked up simultaneously due to the elastic scheduling algorithm of Kubernetes. Resilient deep learning can be achieved by implementing the Kubernetes native framework and invoking TensorFlow 2.0. The so-called Kubernetes-native refers to the program that calls the Kubernetes API to start and stop processes. Kubernetes is an open source for managing containerized applications on multiple hosts in a cloud platform. Its goal is to make deploying containerized applications simple and efficient.

In blockchain applications, the number of simultaneous blocks is an important metric for blockchain applications. Analysis of simulated data shows that as the length of the blockchain increases, the time to generate a new block increases accordingly, but the overall performance does not degrade significantly. Authentication efficiency shows an upward trend when t increases from 9 to 11. Authentication efficiency shows an upward trend when t increases from 9 to 11. Thus, the proposed approach is applicable to the ubiquitous power IoT with a large number of concurrent access endpoints.

5. Conclusions

The introduction of a blockchain-based collaborative transaction model for EV charging and discharging is significant for the grid, charging companies and EV owners. In the case of the grid, storing transaction data in blockchain technology will eliminate inequalities in information exchange between charging operators and the power system and facilitate analysis of EV driving and charging-related data by industry associations and related companies. In the case of cluster control centers, establishing a transaction mechanism based on blockchain technology and allocating EV charging and discharging rights in a market-based manner within the cluster could make it even better.

Trust in IoT endpoints is an important factor that limits the security and reliability of power systems. In this paper, we apply decentralized distributed trust of blockchain to the ubiquitous trust of IoT end devices and propose a practical scheme compared with the traditional centralized key scheme. The scheme is based on the verifiability of blockchain and avoids the system overhead of running decryption algorithms during the verification process. Simulation experiments on the superledger platform confirm that the authentication efficiency is significantly improved compared with the traditional centralized authentication scheme.

Currently, blockchain technology is still facing many issues and challenges in integrating into grid construction, such as the scalability of the blockchain, for example, COINS and Ethernet public chains currently only handle 7 to 30 units per transaction can, if the world's power consumption and production facilities are digitized, depending on the next unit level, it needs to be able to handle millions of computational power per second. This is something that blockchain technology is currently unable to achieve. Next, further research is needed to integrate blockchain technology into the construction of power grids and promote smart grids.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was supported by Science and Technology Projects of State Grid Corporation of China "Research on Distribution Network Configuration and Control System Construction Technology Supporting High Proportion of Distributed Resources" (project no: 5100-202155291A-0-0-00).

References

[1] Z. Lv, L. Qiao, K. Cai, and Q. Wang, "Big data analysis technology for electric vehicle networks in smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1807–1816, 2021.

[2] R. S. Abdullah and M. A. Faizal, "Block chain: cryptographic method in fourth industrial revolution," *International Journal of Computer Network and Information Security*, vol. 10, no. 11, pp. 9–17, 2018.

[3] D. Yermack, "Corporate governance and blockchains," *Social Science Electronic Publishing*, vol. 21, no. 1, article rfw074, 2017.

[4] T. T. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: a data processing view of blockchain systems," *IEEE Transactions on Knowledge & Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[5] D. An, Q. Yang, W. Yu, D. Li, and W. Zhao, "LoPrO: location privacy-preserving online auction scheme for electric vehicles joint bidding and charging," *Future Generation Computer Systems*, vol. 107, no. 7, pp. 394–407, 2020.

[6] K. Kaur, S. Garg, G. Kaddoum, S. H. Ahmed, and M. Atiquzzaman, "Demand-response management using a fleet of electric vehicles: an opportunistic-SDN-based edge-cloud framework for smart grids," *IEEE Network*, vol. 33, no. 5, pp. 46–53, 2019.

[7] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications," *International Journal of e-Collaboration (IJeC)*, vol. 16, no. 1, pp. 16–32, 2020.

[8] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering & Applications*, vol. 9, no. 10, pp. 533–546, 2016.

[9] A. A. Umarovich, V. N. Gennadyevna, and A. O. Vladimirovna, "Block chain and financial controlling in the system of technological provision of large corporations' economic security," *European Research Studies*, vol. 20, no. 3, pp. 3–12, 2017.

[10] W. Meng, E. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," *IEEE Access*, vol. 6, no. 1, pp. 10179–10188, 2018.

[11] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science Research & Development*, vol. 33, no. 1-2, pp. 207–214, 2018.

[12] M. Saracevic and N. Wang, "New model of sustainable supply chain finance based on blockchain technology," *American Journal of Business and Operations Research*, vol. 3, no. 2, pp. 61–76, 2021.

[13] Y. Wang, Y. Liu, C. Wang et al., "Storage-less and converter-less photovoltaic energy harvesting with maximum power point tracking for internet of things," *IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems*, vol. 35, no. 2, pp. 173–186, 2016.

[14] A. Nikoukar, S. Raza, A. Poole, M. Gunes, and B. Dezfouli, "Low-power wireless for the internet of things: standards and applications," *IEEE Access*, vol. 6, pp. 67893–67926, 2018.

[15] M. Mačiulienė, “Power through things: following traces of collective intelligence in internet of things,” *Social Technologies*, vol. 4, no. 1, pp. 168–178, 2014.

[16] C. Iozzio, “Power to the internet of things,” *Scientific American*, vol. 311, no. 6, p. 30, 2014.

[17] C. Fangxiao and W. Xu, “Vehicle power battery monitoring system based on internet of things,” *Journal of Jilin University*, vol. 32, no. 3, pp. 275–279, 2014.

[18] C. Zhaoa, J. Liub, and F. Shenc, “Low power CMOS power amplifier design for RFID and the internet of things,” *Computers & Electrical Engineering*, vol. 52, pp. 157–170, 2016.

[19] L. Hua, Z. Junguo, and L. Fantao, “Internet of things technology and its applications in smart grid,” *Telkomnika Indonesian Journal of Electrical Engineering*, vol. 12, no. 2, pp. 940–946, 2013.

[20] N. Tang, S. Mao, Y. Wang, and R. M. Nelms, “Solar power generation forecasting with a LASSO-based approach,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1090–1099, 2018.

[21] U. R. Efobi, B. V. Tanankem, and S. A. Asongu, “Female economic participation with information and communication technology advancement: evidence from sub-Saharan Africa,” *South African Journal of Economics*, vol. 86, no. 2, pp. 231–246, 2018.

[22] S. E. Wildevuur and L. W. Simonse, “Information and communication technology-enabled person-centered care for the "big five" chronic conditions: scoping review,” *Journal of Medical Internet Research*, vol. 17, no. 3, article e77, 2015.

[23] O. B. Akan, H. Ramezani, T. Khan, N. A. Abbasi, and M. Kuscu, “Fundamentals of molecular information and communication science,” *Proceedings of the IEEE*, vol. 105, no. 2, pp. 306–318, 2017.

[24] K. Kauppi, M. Välimäki, H. M. Hätönen et al., “Information and communication technology based prompting for treatment compliance for people with serious mental illness,” *Cochrane Database of Systematic Reviews*, vol. 6, no. 6, article CD009960, 2014.

[25] W. Bank, “The little data book on information and communication technology 2010,” *World Bank Publications*, vol. 29, no. 5, pp. 449–458, 2014.

[26] Q. Liang, S. Dang, B. Shihada, M.-S. Alouini, R. Nowak, and Z. Lv, “Can blockchain link the future?,” *Digital Communications and Networks*, 2021.

[27] Z. Lv and A. K. Singh, “Big data analysis of internet of things system,” *ACM Transactions on Internet Technology*, vol. 21, no. 2, pp. 1–15, 2021.