EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Blockchain-based IoT device identification and management in 5G smart grid

Dong Wang[*], Huanjuan Wang and Yuchen Fu

*Correspondence: wangdong@sgec.sgcc.com.cn
State Grid Electronic Commerce Co., Ltd. State Grid Blockchain Technology Co., Ltd., Beijing, China

Abstract

This work investigates the unified coding and identification of smart grid IoT devices, as more and more IoT devices in smart grid need to be managed and controlled. We combine blockchain technology with 5G MEC to realize the connection of massive power IoT devices at the edge of 5G network. Due to blockchain's distributed storage and credibility, it is used to identify and register IoT devices in smart grid, ensuring the reliability and accuracy of smart grid IoT devices management. In this paper, we propose a hybrid blockchain mechanism based on 5G MEC smart grid, where both public blockchain and private blockchain are deployed on the MEC gateway/server. To facilitate the data searching and extracting, we endeavor to build a blockchain explorer indexed by IoT device identifier. After that, we study the typical consensus algorithms in the blockchain such as PoW, PoS, DPoS, PDFT, and discuss their feasibility in the hybrid blockchain. Finally, we analyzed and compared the performance of different consensus algorithms from the perspective of average computing time and average time to agreement.

Keywords: Smart grid, IoT device identification, 5G MEC, Blockchain, Consensus algorithm

1 Introduction

The fifth-generation mobile communication technology (5G) can flexibly meet the specific needs of services in different scenarios and will bring various innovative applications to vertical industries, driving social economic efficiency improvements and cost reductions [1, 2]. 5G integrates with the Internet of Things (IoTs), big data, cloud computing, edge computing, blockchain, and artificial intelligence. It is bringing unprecedented momentum to the digital transformation of industry, economy and society.

Smart grid is a new development trend of traditional power system [3], which fuses together modern advanced information and communication technology (ICT), Internet of Things (IoTs), artificial intelligence (AI), control technology, etc., to realize the communications of power system. Furthermore, a ubiquitous intelligent power IoTs can be realized that can fully perceive the system status and efficiently process information.

Smart grid will focus on the end-to-end links of power generation, transmission, transformation, power distribution, and electricity consumption, to carry out intelligent and informatized upgrades [4]. The key requirements of smart grid communication networks include ultra-low latency (millisecond level), high isolation (complete isolation from other 5G vertical industries), high reliability (99.999%), and massive access (ten million terminals) etc. [5]. It requires the deployment of edge computing services on the 5G base station side. As a result, 5G multi-access edge computing technology (MEC) can be used to realize the connection of massive power equipment, the collection of various power data (video, pictures, sensor data, etc.) [6], local unloading and processing, intelligent judgment and fault location, and fault recovery from minutes to seconds. Smart grids are facing new challenges and opportunities during development and construction.

In recent years, blockchain has achieved initial success in application fields such as trade finance and industrial Internet [7]. With the rise of smart grid, the application of blockchain in smart grid has attracted a lot of attention. Recently, researchers have done a lot of work on the security, privacy and trust issues of smart grids [8]-[17]. For example, [8, 9] described the application of blockchain in the energy Internet and a series of problems brought about by it are discussed. An overview of the microgrid blockchain investigation and related projects is given in [14]. On the basis of [12, 15]-[17] further studied the blockchain-based peer-to-peer energy transaction and used it for distributed energy dispatch. [10] introduced a survey of smart grid blockchain applications and new frameworks. In [11], typical use cases of blockchain in energy applications are described, such as distributed energy transactions, smart microgrids, smart power distribution, and smart power consumption. Blockchain provides a non-centralized trust mechanism, which is suitable for distributed energy operations. [13] introduced some major blockchain platforms and research projects in the smart grid, and analyzed the potential advantages of blockchain applications in smart energy systems.

Blockchain and 5G are both new technologies, and the huge potential of the combination of the two have become increasingly prominent. 5G drives the massive adoption of smart devices, which means that blockchain will have more data than ever before, and these data will greatly promote the globalization of technology. Blockchain will be able to provide stable tracking, traceability and distributed point-to-point transaction functions for trillions of commodities around the world. Blockchain technology can just make up for the shortcomings of 5G's poor privacy and security, lack of trust in virtual transactions, and inadequate property rights protection. The decentralization of blockchain, the transaction information privacy protection, the anti-tampering of historical records, and traceability will effectively promote the development of 5G networks and new business models. 5G can guarantee the integrity, comprehensiveness, and speed of traceable data transmission. Blockchain can guarantee the trustworthiness of traceable data. The integration of 5G and blockchain will promote the rapid development of various vertical industries in different fields.

5G MEC provides the required cloud computing functions and IT service environment at the edge of the 5G network for application developers and content service providers. Decentralized edge computing based on blockchain technology will have more advantages in data security, identity authentication, privacy protection, etc. [18], thereby inspiring and promoting the large-scale deployment of MEC application scenarios.

Information searching in blockchain is currently an open challenge, since the desired piece of information may be scattered and no indexed. To overcome this difficulty, we propose to build a blockchain explorer to facilitate the information localization and extraction of smart grid IoT devices. The IoT device identifier will serve as the index of blockchain explorer to search for the desired information using specific domain terms. From this respect, IoT device identification is pivotal to the blockchain-based smart grid equipment management.

In this paper, we combine blockchain technology with 5G EC to realize the connection of massive power IoT services at the edge of 5G network and investigates the unified coding. In the life cycle management of smart grid equipment, smart grid equipment coding plays an indispensable role. In the relevant database of equipment asset management, intelligent online monitoring, power inspection, fault repair and other subsystems, the smart grid equipment code is the only index to realize various database operations. In the establishment of a unified database for smart grid, standardized smart grid device coding and identification will become crucial.

Blockchain-Specific Challenges and Directions are as follows.

(1) Throughput

The throughput of the blockchain is usually closely related to the number of transactions per unit time and the time of each transaction. Currently, most popular blockchain applications (such as Bitcoin) have low throughput, so there are some challenges in real-time transactions and micropayments. However, in the smart grid scenario, various energy transactions such as smart power distribution and smart power consumption will often occur, and the amount of data may be large. Therefore, it is necessary to solve the transaction problem of the blockchain in the case of high throughput on the basis of the existing blockchain technologies, and provide the possibility for the implementation of the blockchain in the smart grid.

(2) Consensus Mechanisms

The current popular consensus mechanisms are generally only suitable for a single blockchain application, and the performance of the consensus mechanisms are related to the specific requirements of different applications. PoW is a popular consensus mechanism currently, which has rich trading rules. However, this consensus mechanism requires more computing resources when confirming transactions, resulting in the consumption of a large amount of energy, which is a big challenge for resource-constrained smart grid edge devices. Therefore, in view of the specific scenarios and performance requirements of the smart grid, improving the existing consensus mechanism or developing a new consensus mechanism is an inevitable requirement for the application of blockchain in the smart grid.

(3) Security

Blockchain technology helps to build a decentralized, immutable, and highly reliable system. But the premise is that the platform of the block application must be absolutely secure and trustworthy. In smart grid applications based on blockchain technology, the introduction of a smart contract mechanism can improve the security of the smart grid application platform and realize automatic transactions such as electric energy and electricity bills.

The reminder of this paper is organized as follows. In Sect. 2, we introduced the need and importance of IoT device identification in smart grid, and the current status of smart grid device coding was presented. In Sect. 3, we introduced the blockchain technology into the smart grid IoT device management. Based on the 5G MEC network architecture, we proposed a hybrid blockchain-based smart grid IoT device management mechanism. Section 4 proposed the consensus algorithm of hybrid blockchain, and Sect. 5 analyzed the performance of different consensus algorithms in smart grid applications.

2 Related work to IoT device identification in smart grid

2.1 Smart grid

Smart grid is a new generation power system with many characteristics, including highly informatization, automation, and interaction, etc. [19]. It can improve the reliability of grid power supply, promote energy saving and emission reduction, and realize the maximization of grid benefit and social benefit. It represents the future development direction of the power system.

The construction of smart grid emphasizes the interconnection of massive IoT devices and the transmission of information. As a smart grid infrastructure, 5G MEC is responsible for information collection and local offloading in all aspects of smart grid, and provides safe, reliable, and efficient information transmission channels for various energy service platforms to promote the overall efficient and coordinated operation of the power system.

2.2 IoT device identification

The IoT device identifier can uniquely identify a single entity or a type of entity and is used to identify the device in the system. At the same time, the various data contents in the IoTs system also need to develop a unified identifier to realize the information interaction and sharing. Using blockchain technology, encryption technology and security algorithms can be used to protect digital identities, thereby building a more secure and convenient digital identity authentication system for IoTs.

The role of IoT device identifiers is not only to indicate their identity characteristics, but also to assist the search and discovery of IoT devices. Therefore, when formulating a unified identification system for IoT devices, it is necessary to fully consider the huge volume of IoT devices in cross-system and cross-platform situations, as well as the diversity of types, and ensure that the devices can be quickly and accurately searched.

2.3 Smart grid equipment identification

In the life cycle management of smart grid equipment, smart grid equipment coding plays an indispensable role. In the relevant database of equipment asset management, intelligent online monitoring, power inspection, fault repair and other subsystems, the smart grid equipment code is the only index to realize various database operations. In the establishment of a unified database for smart grid, standardized smart grid device coding and identification will become crucial as shown in Fig. 1.

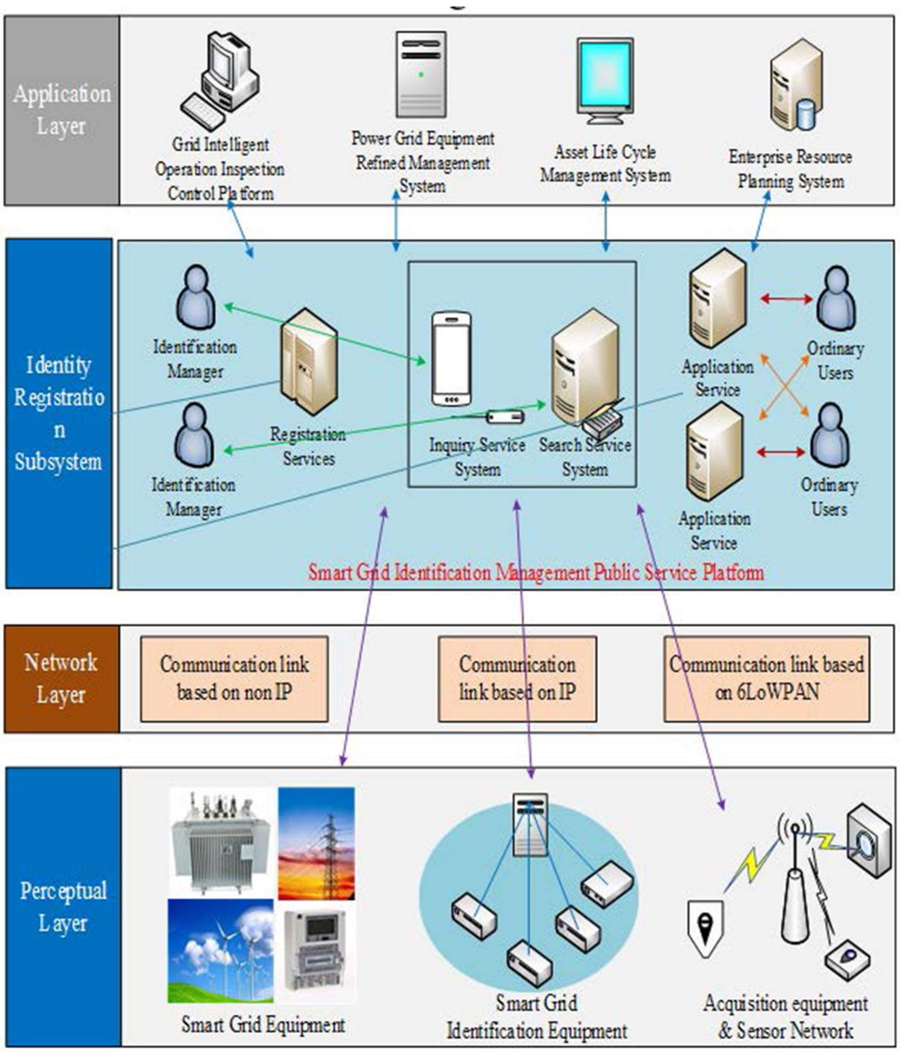
Application Layer
Grid Intelligent Operation Inspection Control Platform
Power Grid Equipment Refined Management System
Asset Life Cycle Management System
Enterprise Resource Planning System
Identity Registration Subsystem
Identification Manager
Registration Services
Identification Manager
Inquiry Service System
Search Service System
Application Service
Ordinary Users
Application Service
Ordinary Users
Smart Grid Identification Management Public Service Platform
Network Layer
Communication link based on non IP
Communication link based on IP
Communication link based on 6LoWPAN
Perceptual Layer
Smart Grid Equipment
Smart Grid Identification Equipment
Acquisition equipment & Sensor Network

Fig. 1 Smart grid equipment identification platform; Instructions for Smart grid equipment identification platform

The complete link of the smart grid includes power generation, transmission, distribution, energy storage and power consumption. The application of modern information technology and automatic control technology can realize the two-way exchange of information from power generation to power consumption, and realize the maximum benefit of the grid and social benefits. In the whole process, hundreds of millions of devices are interconnected between power generation, transmission and distribution, which requires to carefully code these devices to ensure the accuracy of device identification and control.

2.4 Status quo of smart grid equipment coding

In the process of smart grid construction, there are various coding schemes, but no unified standard yet. At present, the traditional international power equipment coding schemes [20] include: British CCC coding system, 1kks power plant identification system, French EDF coding system, China National Grid power equipment code, China power plant equipment identification system coding standard, and China Southern Power Grid equipment information Classification code, etc.

Currently, there are three main problems with smart grid device coding. First of all, different units, different types of professional equipment and different systems have their own coding schemes, which cannot achieve cross-platform and cross-system information sharing and interoperability. Secondly, the formulation of the coding scheme lacks a unified standard, the formulation rules are not compatible, and it is impossible to extend the existing coding scheme. Finally, the existing coding scheme mainly encodes the equipment on the service link, and the coverage is not comprehensive, but it has not yet covered the equipment on the control link such as power generation and transmission of smart grid.

Therefore, the current smart grid equipment management has basic coding standardization problems. Non-standard equipment coding is not conducive to the positioning and traceability of equipment management and maintenance, and it is not conducive to information transmission and system interaction among smart grid devices. It will inevitably lead to information isolation, fail to meet the development needs of smart grid, and fail to complete the smart grid industry chain. Standardized device coding can realize data sharing and reduce costs. It can not only provide basic guarantee for the interconnection of energy flow and information flow of the smart grid, but also has practical urgent needs and engineering application value.

2.5 Unified coding and identification standard system

The construction of the smart grid equipment coding standard system includes many fields, such as equipment coding classification and identification technology, equipment entire life cycle management platform, information sharing and information support platform, etc. Therefore, it is necessary to analyze specific application requirements from a cross-industry, cross-enterprise, and cross-system perspective. Under this premise, we formulate standard design principles, improve existing equipment coding and marking schemes, and build a set of unified coding and Identification standard system.

When building a unified coding and marking standard system for smart grid devices, the following principles should generally be followed. First of all, it is necessary to realize the unique identification and unified identification of the equipment code. In all links of the smart grid equipment cycle, the equipment coding must realize "one object, one identification," which is the only legal identity for the operation and management of smart grid equipment. At the same time, it only needs to modify rather than overthrow the existing equipment coding and identification schemes, and is widely compatible with multiple existing coding schemes, and gradually realize the final unification of the standard. Moreover, considering the rapid growth of smart grid devices, the standard must be flexible and expandable, and a sufficient number of expandable equipment codes must be guaranteed to meet the coding requirements of new services and new equipment in the future. Finally, convenience and practicality are also a principle that must be followed in standard formulation. The equipment coding mark and identification system must not only provide services such as unified registration, distribution, application, analysis, and cancellation of coding marks, but also have the ability to identify devices quickly and accurately, and support the remote control of power equipment through equipment codes.

As a result, following the above principles, we designed a basic framework of a unified coding and identification standard system for smart grid devices as shown in Fig. 2. The framework includes a core system composed of coding–identification–transmission–analysis–applications and a support system composed of management technology standards, while considering the impact of management, technology and standards on the intelligent unified coding and identification system. Unified IoT device identifier can be used to index the database or blockchain to build an efficient searching engine.

IoT business platform built using blockchain technology is a "decentralized" business platform. Various IoT entities (for example, IoT devices, IoT servers and gateways, end-user devices, etc.) cooperate with each other in a "decentralized" mode. The IoT blockchain supports smart contracts. Some typical IoT services can be presented and executed through smart contracts, such as identifying IoT devices and online processing IoT data.

Despite the wide variety and number of IoT devices, most devices are not always active, and even some devices are rarely active. IoT devices can deploy smart contracts on the IoT blockchain to automatically manage the registration, update, authentication, access, and data processing of IoT devices. IoT devices can register or update their status information on the IoT blockchain when they are activated or when their status changes. IoT business can search for registered IoT devices information through IoTs blockchain. For IoT devices that are deactivated or limited in capacity, they can be indirectly connected to the IoT blockchain through IoT gateways.

The cost of traditional IoT solutions is relatively high, and the computing and storage resources of IoT cloud servers are relatively high, and the energy consumption is also high. Combining the blockchain and IoTs, with the help of the "decentralization" of the blockchain, a highly adaptable and secure distributed mechanism can be created for the simple connection of millions of devices. Blockchain technology can provide

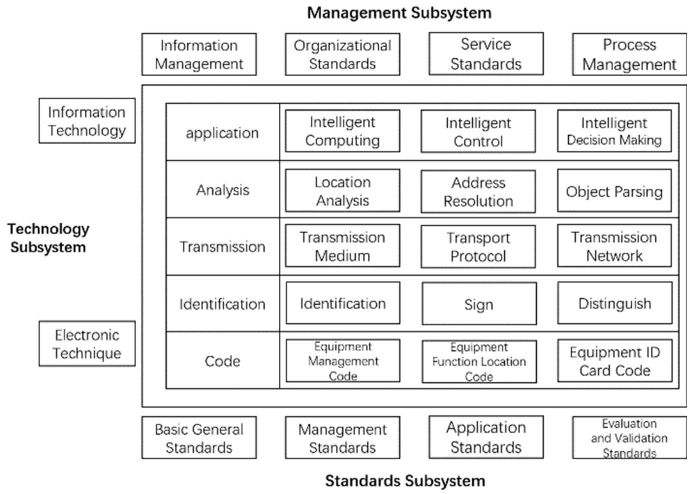

Fig. 2 Framework of unified coding and identification system; Description of o Framework of unified coding and identification system

point-to-point direct interconnection for IoTs to transmit data, making full use of the computing power, storage capacity and bandwidth of hundreds of millions of idle devices distributed in different locations for transaction processing, significantly reducing the cost of calculation and storage, thereby greatly reducing the energy consumption brought by the IoT cloud server in the "centralized" mode.

Moreover, blockchain technology superimposed with smart contracts can turn each smart device into an independent network node that can be self-regulated. These nodes can manage their own various resources (including computing, storage, energy resources, etc.) based on pre-installed rules, thereby further saving a lot of equipment maintenance costs and energy consumption, and extending the survival time of IoT devices.

3 Methods

This section mainly introduces the system architecture and management method of 5G MEC blockchain-based smart grid IoT.

3.1 Building blocks for future IoT device management: blockchain and 5G MEC

The 5G-based smart grid application is currently in its infancy. In the future, power companies should work with telecom operators and communication equipment manufacturers to lead the standardization of technologies in the power communication field, promote the generalization of power communication terminal modules, and build a support platform for communication business management to support smart grids Sustainable development.

Considering the deep integration with the 5G network, we will concentrate on the research of unified coding and identification technology for smart grid devices. At the same time, combined with blockchain and mobile edge computing, we will construct a public management platform to register and manage the asset information of smart grid equipment by using the unified coding and identification standards. In other words, we propose to move the system in Fig. 2 to the blockchain for extra reliability and security.

Smart grid is a new development trend of traditional power system, which fuses together modern advanced technology [21], such as IoTs, blockchain, and 5G mobile edge computing (MEC). Furthermore, a ubiquitous intelligent power IoTs can be realized that can fully perceive the system status and efficiently process information. Blockchain and 5G MEC are both new technologies, and the huge potential of the combination of the two have become increasingly prominent.

3.2 Hybrid blockchain system for smart grid

5G drives the massive adoption of smart devices in the smart grid, which means that blockchain will have more data than ever before, and these data will greatly promote the globalization of smart grid technology. Blockchain technology can just make up for the shortcomings of 5G's poor privacy and security, lack of trust in virtual transactions, and inadequate property rights protection. The decentralization of blockchain, the transaction information, the privacy protection and the anti-tampering of historical records in the smart grid will effectively promote the development of 5G networks in smart grid.

Blockchain can automate various transaction processes and can significantly reduce labor costs and transaction time. For example, IBM uses blockchain technology to solve the problems faced by temporary labor contracts, and has developed corresponding invoice reconciliation products to deal with invoice problems caused by temporary labor. Reconciliation through the digital ledger can not only ensure the compliance of payment terms, eliminate disputes arising from invoices, but also reduce the cost of reconciling invoices and shorten the work cycle. As a shared digital ledger for recording transactions, blockchain technology has brought fresh air to the business world.

A blockchain system contains multiple components [22], including network, consensus, application and meta-application layers in the blockchain system. The functions of these layers are briefly described as follows.

(a) Meta application layer. It is mainly to cover the application layer and combine blockchain with other applications in Fig. 3.

(b) Application layer. It is the semantic interpretation of blockchain system, and its key function is to develop blockchain solutions for different applications and industries. An example of semantic interpretation is to define cryptocurrency and then establish a protocol for how to exchange the currency between different entities.

(c) Consensus layer. It mainly supports the distributed consensus mechanism of the blockchain system. This layer is used to verify the correctness of each blockchain,

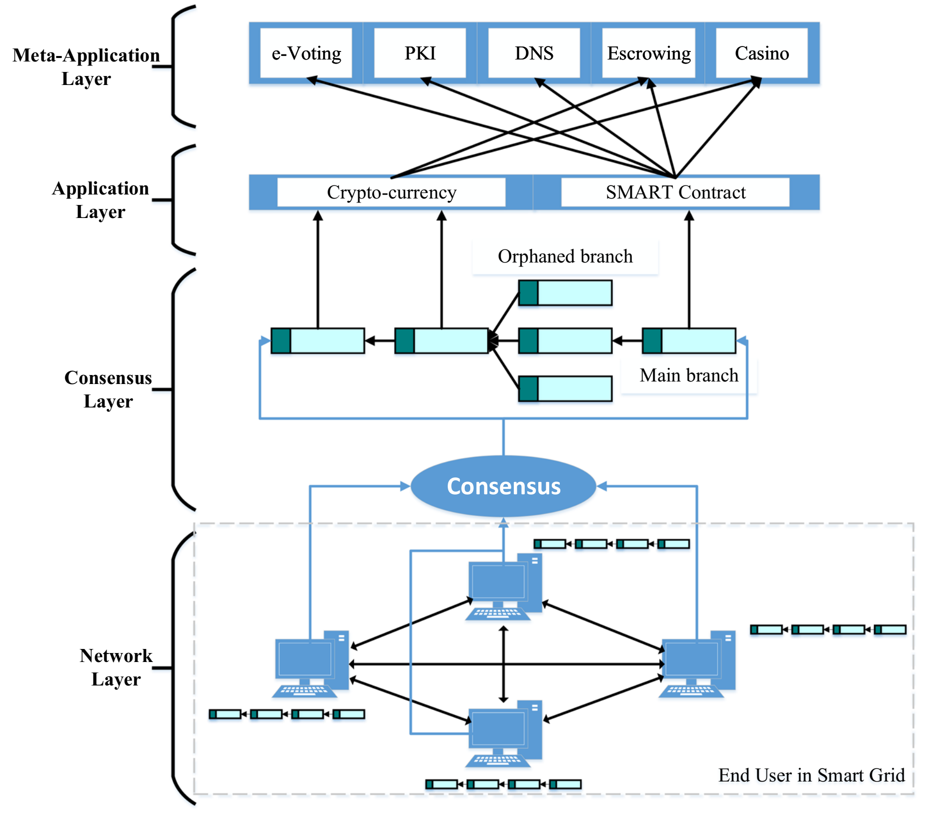

Fig. 3 Blockchain Layers; Illustration of the Blockchain Layers

determine the order of the blockchain, and finally achieve the consistency required by the system.

(d) Network layer. It is mainly responsible for adding blockchain chains, updating and exchanging information on blockchain chains and other functions.

Blockchain can be divided into three types, including public, private, and consortium blockchain.

(a) *Public Blockchain.* The public blockchain is a blockchain that anyone in the world can freely read, submit transactions and participate in the mining process. However, all nodes can participate in the consensus process, and there is a transaction confirmation waiting time, which results in low transaction throughput. Worse, its transaction information is transparent to the public, which is not conducive to protecting privacy.

(b) *Private Blockchain.* The right to write in a private blockchain is reserved by a person or organization. This allows them to realize their personal wishes while keeping certain transaction information private. It can be considered a centralized network with the above-mentioned shortcomings.

(c) Consortium Blockchain. The consortium blockchain is partially decentralized and is jointly established by multiple organizations. Only some authorized nodes participate in the consensus, which improves the efficiency of the consensus and the entire transaction. The charging node adds the data that needs to be verified to the corresponding blockchain and stores it permanently to support query at any time. The conditions for selecting blockchain nodes are richer hardware resources or better operating environment, which can improve the execution efficiency of the system and ensure the security of the system.

The single blockchain architecture will result in the information data masking between different organizations. And the hybrid blockchain architecture adopted in the smart grid will promote the communication between different organizations. As shown in Fig. 4 each organization in the hybrid blockchain builds its own private blockchain, independent of each other. When data interaction occurs between different organizations, it is up to the organization itself to choose the data stored in its own private blockchain, compress and upload it to the consortium blockchain. The hybrid blockchain is multi-centralized, combining the low trust of the public blockchain with the single high trust of the private blockchain. It inherits the advantages of centralization and alleviate the problem of monopoly.

Similar to search engines in the Internet (such as google), it requires a blockchain browser to find the interested data. In our work, we use the IoT device identifier as an index to build a blockchain browser to search for the desired blockchain data.

3.3 5G MEC and blockchain

With large bandwidth, large connections, and low latency as outstanding technical features [23], 5G can flexibly meet the specific needs of services in smart grid, driving social economic efficiency improvements and cost reductions. MEC technology provides the

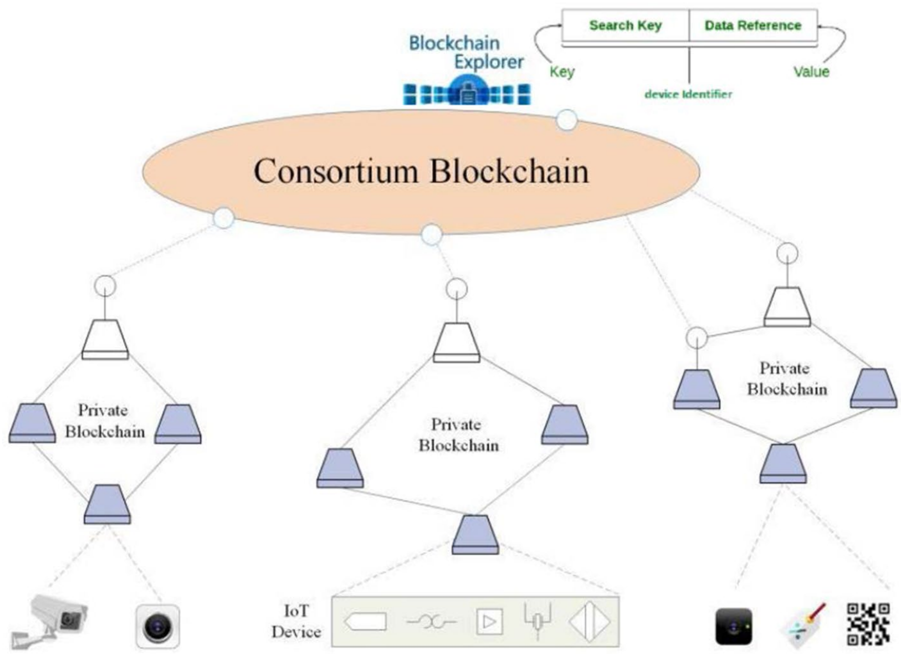

Fig. 4 Hybrid Blockchain Architecture; Illustration of the Hybrid Blockchain Architecture

required cloud computing functions at the edge of the 5G network for application developers and content service providers. Decentralized edge computing based on blockchain technology will have more advantages in data security, identity authentication, privacy protection, etc., thereby inspiring and promoting the large-scale deployment of MEC application scenarios. In actual deployment, the blockchain platform or application can be deployed on the MEC server to provide blockchain capabilities support for different application scenarios.

The network architecture of MEC enables computation to be completed at the edge of mobile network and achieve cloud side collaboration. The main benefit of MEC is to reduce congestion on mobile networks, which will play an important role in reducing 5 g network latency. By making the data closer to the end user and transmitting the data stream to the user terminal more directly, such low delay communication can be realized.

The application of blockchain technology to the mobile edge computing infrastructure (BMEC) will help solve the access and management of various devices in the smart grid, as well as the local data offloading [24]. In the case of limited computing resources, BMEC realizes the distributed deployment of various resources to ensure the traceability of transaction data. Through the distributed deployment of the BMEC server, the management of IoT devices in the blockchain and the storage of IoT device information and data can be easily realized.

In the BMEC model, the blockchain node is deployed in the MEC server, and the mobile device accesses the nearest MEC server and executes the blockchain consensus process. Lightweight blockchain nodes can also be deployed in specific mobile devices. In Fig. 5, each edge server runs a copy of the blockchain, which reduces the resource

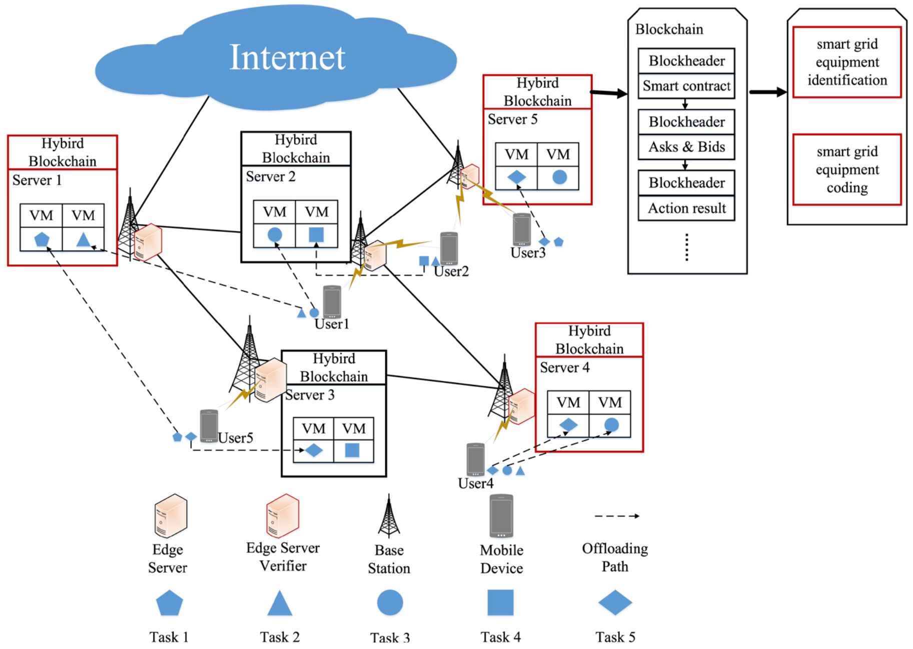

Fig. 5 A typical blockchain-driven cross-server resource allocation architecture in MEC; Illustration of A typical blockchain-driven cross-server resource allocation architecture in MEC

requirements for mobile devices, and is particularly suitable for mobile devices with limited resources.

As shown in Fig. 6, this BMEC framework contains three layers, namely users, edge networks (heterogeneous wireless networks with MEC) and blockchain. In the BMEC system, 5G MEC server acts as a dual gateway, acting as the gateway between the private and consortium blockchains in the hybrid blockchain to realize the data interaction and information transfer between different organizations, and acting as the gateway between the enterprise network and core network to realize the network interconnection. The blockchain is used as an overlay system to provide management and control functions for the underlying MEC system.

3.4 Study on hybrid blockchain consensus algorithms

Blockchain system is a distributed system. When the traditional single node architecture evolves into distributed system, the first problem is to ensure the consistency. If the distributed system can't guarantee the consistency of processing results, the business systems built on it will not work normally. Consistency is the most basic and important problem of blockchain system [25]. If the distributed system can achieve "consistency", it can present a perfect and scalable "virtual node", which has better performance and stability than physical nodes. Consensus describes the process of reaching an agreement on a certain state among multiple nodes in a distributed system. Different consensus mechanisms can meet the needs of different degrees of consensus. The following parts of this section analyze the performance of several consensus algorithms, including PoW, PoS, DPoS and PDFT.

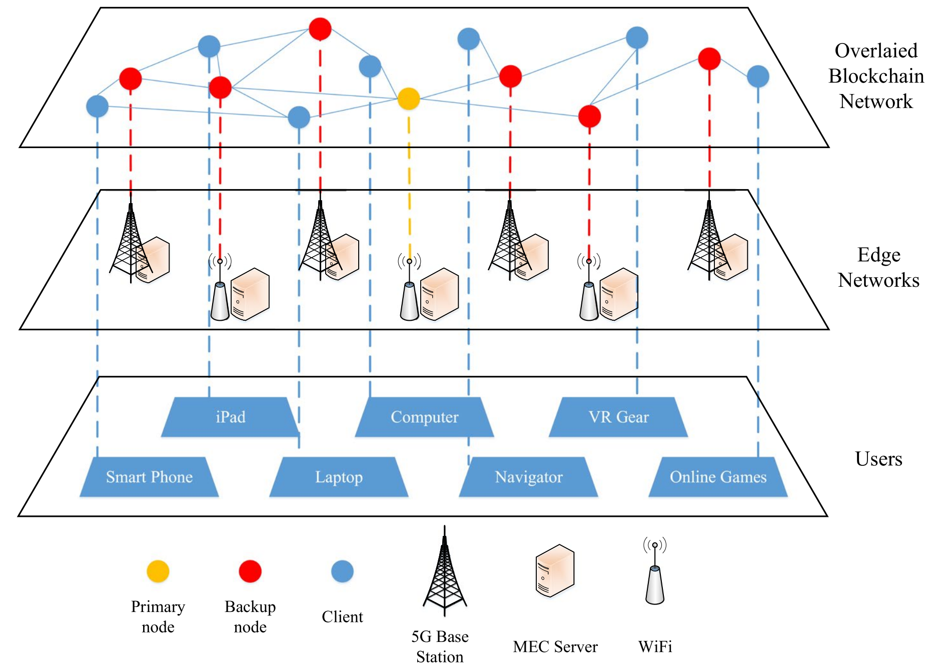

Fig. 6 BMEC in the heterogeneous wireless networks; Illustration of the BMEC in the heterogeneous wireless networks

3.5 PoW

Generally, the whole process of monitoring work is very inefficient, but it is a very efficient way to verify the results of the work to prove that the corresponding workload has been completed. Proof of work (PoW) is simply a proof that you have done a certain amount of work. In the blockchain, the pow consensus algorithm mainly determines who accounts by calculating the difficulty value. The workload of pow refers to the solution of the equation. Whoever gets the solution of the equation first has the right to account. Except for the first block, the hash value of each block is related to the hash value of the previous block and the random number generated. There is no fixed solution to the equation, so we can only keep trying. This way of solving the equation is called hash collision. The more times the collision is, the more difficult it will be to solve the equation. A typical application of pow is bitcoin.

3.6 PoS

However, PoW is not without defects. In addition to consuming a lot of energy, another problem of pow is that its value loop must pass through external input. In other words, the safety of using PoW is not directly related to users, but through the medium of miners. So PoS was proposed in [2]. The assumption of PoS is that the security of currency with PoS is directly related to the user, thus eliminating the medium of miners. When the PoS publishes a message, it is necessary to pay the price for the simple proof of ownership. And ownership means that if you cheat and damage the security of the system, your rights and interests will be damaged, which makes you pay a price in disguise. Compared with pow, PoS can greatly reduce energy consumption, and block generation rate is greatly accelerated, so the time to complete transaction verification is greatly reduced.

3.7 DPoS

The principle of DPoS is the same as that of PoS, but some representatives are selected [26]. The difference with PoS is that the owner of the equity elects a number of agents, which are verified and accounted for by the agent. In other words, becoming an agent equals to having more rights and interests. The election process should try to ensure that the equity owners can ultimately control the whole network, because once the network problems, the equity owners will lose the most. Stakeholders vote to generate agents, which is an excellent mining mechanism. Decentralization means that each shareholder has influence according to its shareholding ratio, and the result of 51% shareholders' voting will be irreversible and binding. The challenge is to achieve 51% approval through a timely and efficient approach. In the DPoS mechanism, the number of nodes participating in verification and billing is greatly reduced, consensus verification is effectively guaranteed, and processing efficiency is higher. However, the disadvantage is that the whole mining mechanism still relies on tokens, and many industrial applications of blockchain do not need tokens.

3.8 PBFT

Practical Byzantine Fault Tolerance (PBFT) [27] improves the performance of system fault tolerance. In PBFT algorithm, at most one third of Byzantine nodes in the system can be tolerated, that is, if more than two thirds of the nodes are normal, the whole system can work normally. In recent years, PBFT algorithm as a consensus protocol has been widely used in blockchain applications. PBFT needs to run three basic protocols, including conformance protocol, validation protocol and view replacement protocol. The conformance protocol is the core, mainly including the following stages: Request, prepare, prepare, submit, reply. In theory, PBFT consensus is more effective than workload proof in terms of consistency. Under the PBFT mechanism, the transaction is completed once and cannot be changed (that is, without multiple confirmations). When the transaction volume is not too large, a higher transaction verification speed can be achieved. In addition, PBFT has a small amount of calculation and low energy consumption (Fig. 7).

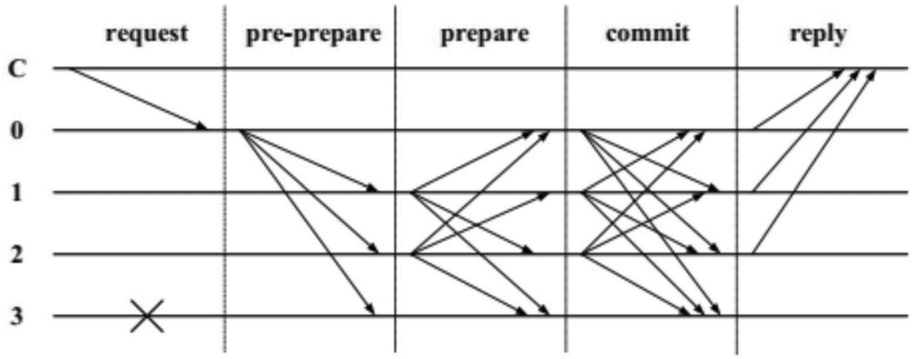

Fig. 7 PBFT algorithm flow; Illustration of the process of PBFT algorithm flow

Table 1 Performance comparison of consensus algorithms

	PoW	PoS	DPoS	PBFT
Applicable Form	public	public	public	consortium
Degree of decentralization	complete	complete	complete	incomplete
Accounting nodes	Whole network	Whole network	Elect	Dynamic decision
Response time	10 min	1 min	3 s	1 s
Throughput capacity	7TPS(Bitcoin)		Above 300TPS	Above 1000TPS
Fault tolerance rate	49%	49%	10/21	33%(m/3 m + 1)

3.9 Hybrid mechanism

For any public blockchain chain, its underlying architecture needs a consensus mechanism to specify how nodes compete for bookkeeping. At present, the most popular ones are PoW, PoS, DPoS, PBFT. Their speed, security and centralization degree are different, as shown in Table 1. For each public chain project adopting a single consensus mechanism, speed, security and centralization cannot be achieved at the same time. Hybrid consensus refers to the application of two or more consensus mechanisms in the underlying architecture of the same blockchain. Reasonable use of mixed consensus can make up for the defects of low efficiency, loss of security protection or sacrifice of centralization degree caused by single consensus mechanism.

For example, in order to take advantage of BFT class consensus, fast final confirmation and high throughput, one method is to combine BFT class with public chain class algorithm, and introduce BFT class consensus into public chain business scenarios. The combination of BFT and PoS absorbs their respective advantages. It is a multi-round PoS algorithm and can tolerate Byzantine behavior between nodes. Generally, within the scope of cap theorem, BFT PoS algorithm tends to be consistent in availability when network partition occurs.

For example, the hybrid PoW-PoS protocol has the same security as the PoW algorithm, but discards its disadvantages. Two different types of blocks can be created in the same blockchain: PoW and PoS blocks. The miner is responsible for creating the PoW block, and the mint is responsible for creating the PoS block. The miners/minters compete with each other, and when they find a valid PoW/PoS block, they broadcast to the network and expect to be verified by other nodes.

4 Experimental results and discussions

This section shows the performance comparison of different consensus algorithms extended from [28]. Table 1 articulates the specific performance comparison of mainstream blockchain consensus algorithms.

The average time shown in Fig. 8 includes the time taken by the algorithm to calculate all messages and the time to transmit them. The average time is in milliseconds, sending 320 bytes of packets per millisecond. As can be seen, the time required by three consistency algorithms is very short in general with PoW being the worst case. Figure 9 reveals it is generally short regarding the time for all nodes participating in the consensus algorithm to reach an agreement. Wireless communication model is designed for better and more accurate research on wireless communication. However, the time for

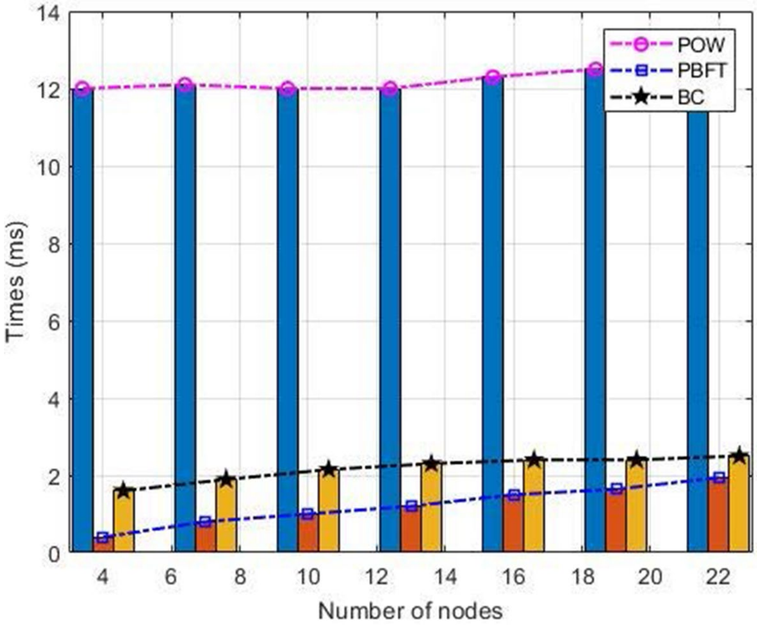

Fig. 8 Average computing time; Illustration of the Average computing time

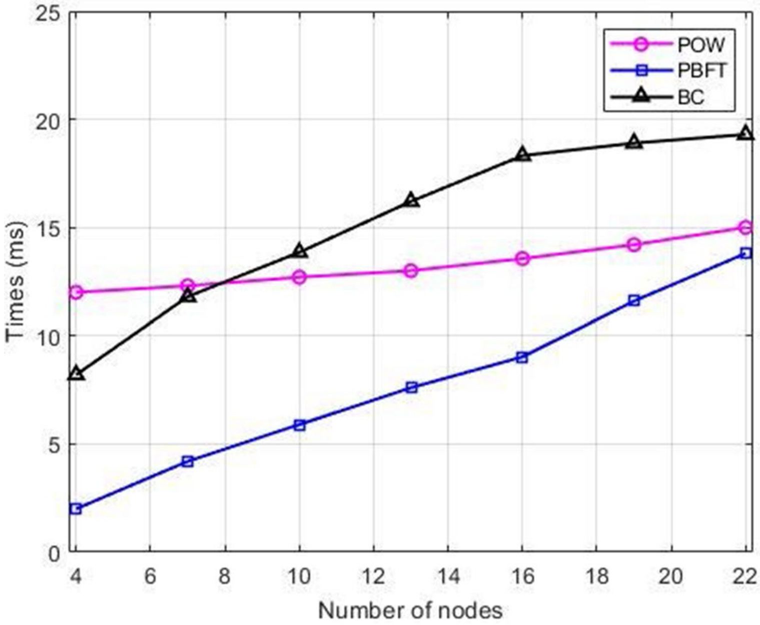

Fig. 9 Average time to agreement; Illustration of the Average time to agreement

different models to reach consensus is different. UDGM wireless communication model only needs a few milliseconds to reach a consensus, while MRM model takes hundreds of milliseconds to reach a consensus. Figure 9 shows that the average consensus time of

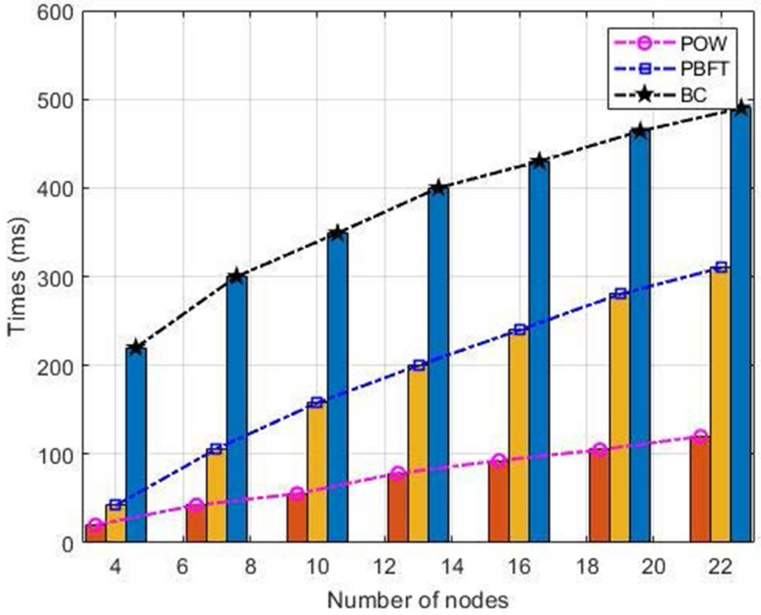

Fig. 10 Average time to agreement (MRM); Illustration of the Average time to agreement (MRM)

BC algorithm in wireless media is longer, while the average consensus time of improved PoW and PBFT in UDGM and MRM media is shorter.

Figure 10 shows the performance of a consensus protocol for transaction throughput, network scale scalability, and applicability to licensed or unauthorized blockchains. Using thousands of TPS protocols to implement BFT style block termination mechanism, hundreds of networks can meet this mechanism. At the same time, because the communication lines of the public network are shared by the public users, the protocol of large-scale public network is mainly non privilege protocol, and the block termination mechanism which only realizes probability termination is adopted. In the blockchain scenario, finality means that once submitted to the blockchain, all well-formed blocks will not be revoked. For security reasons, their transaction throughput is typically 100 TPS. Although the protocols in Fig. 10 show good scalability, their security has always been questioned.

As for the applicability of licensed or unlicensed blockchain, a stable agreement with consensus group participating in control and identification is the key to ensure the applicability of licensed blockchain. We have been fortunate to experiment with many new blockchain protocols or tools, including PBFT, honey badger BFT, Poa BFT and RPCA. In contrast, the protocols used by large-scale unauthorized blockchains include Nakamoto, Nakamoto ghost, chain-based PoS, etc. However, due to the need to rely on the electoral mechanism to maintain a stable consensus group, in order to better realize public supervision, the identities of them may be publicly supervised. The DAG protocol is suitable for the unauthorized network because the purpose of protocol design is to expand the number of participants, which is consistent with the design purpose of the unauthorized network.

5 Conclusions

Smart grid is the most promising vertical industry application of 5G. This paper integrated blockchain technology into 5G MEC-based smart grid to solve the coding and identification problems of massive smart grid IoT devices. In the life cycle management of smart grid equipment, unified smart grid equipment coding or identification can serve as the index of blockchain explorer for data searching and extracting. Because blockchain has the characteristics of decentralization, distribution, credibility, and traceability, this paper proposed a hybrid blockchain mechanism for the identification and registration of IoT devices in smart grid. This hybrid mechanism is deployed on the MEC server, which acts as both a gateway for the public chain and a gateway for the private chain. Furthermore, as the basic technology in blockchain, we studied a number of consensus algorithms, and discussed their suitability for the hybrid blockchain. Finally, the performances of these consensus algorithms are analyzed and compared.

Abbreviations

5G: Fifth-generation mobile communication technology; IoTs: Internet of Things; MEC: Multi-access edge computing technology; PoW: Proof of work; PoS: Proof of Stake; DPoS: Delegated proof of Stake; ICT: Information and communication technology; AI: Artificial intelligence; BMEC: Blockchain-based mobile edge computing; PBFT: Practical Byzantine fault tolerance.

Acknowledgements

The authors thank the anonymous reviewers and editors for their efforts in valuable comments and suggestions.

Authors' contributions

D.W. contributed the central idea, analyzed most of the data, and wrote the initial draft of the paper. H.W. and Y.F. contributed the idea for the simulation experiment and provided constructive suggestions. All authors read and approved the final manuscript.

Funding

This research was funded by The State Grid Science and Technology Project, Research on Key Technologies and Application of Internet of Things Identification Resolution in Power Industry grant number 5700-202019182A-0-0-00.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 9 November 2020 Accepted: 24 March 2021
Published online: 17 May 2021

References

1. M. Fan, X. Zhang, Consortium blockchain based data aggregation and regulation mechanism for smart grid. IEEE Access **7**, 35929–35940 (2019)
2. S. Zhang, J. Lee, A group signature and authentication scheme for blockchain-based mobile-edge computing. IEEE Internet Things J. **7**(5), 4557–4565 (May 2020)
3. Y. Li, B. Hu, An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain. IEEE Trans Smart Grid **11**(3), 2627–2637 (May 2020)
4. W. Sun, J. Liu, Y. Yue and P. Wang, Joint resource allocation and incentive design for blockchain-based mobile edge computing, in IEEE Transactions on Wireless Communications, https://doi.org/10.1109/TWC.2020.2999721.
5. J. Feng, F. Richard Yu, Q. Pei, X. Chu, J. Du and L. Zhu, Cooperative Computation Offloading and Resource Allocation for Blockchain-Enabled Mobile-Edge Computing: A Deep Reinforcement Learning Approach, in *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6214–6228, July 2020.
6. Y. Liu, F.R. Yu, X. Li, H. Ji, V.C.M. Leung, Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing. IEEE Trans. Veh. Technol. **68**(11), 11169–11185 (Nov. 2019)
7. F. Guo, F.R. Yu, H. Zhang, H. Ji, M. Liu, V.C.M. Leung, Adaptive Resource Allocation in Future Wireless Networks With Blockchain and Mobile Edge Computing. IEEE Trans. Wireless Commun. **19**(3), 1689–1703 (2020)

8. J. Wu, N. Tran, Application of blockchain technology in sustain- able energy systems: An overview. Sustainability **10**(9), 3067 (2018)
9. Y. Cao, Energy internet blockchain technology, in The Energy Internet. Elsevier, 2019, pp. 45–64.
10. A. S. Musleh, G. Yao, and S. Muyeen, Blockchain applications in smart grid–review and frameworks, IEEE Access, vol. 7, pp. 86 746– 86 757, 2019.
11. M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. Mc- Callum, and A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019.
12. N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu, X. Du, M. Guizani, When energy trading meets blockchain in electrical power system: The state of the art. Appl. Sci. **9**(8), 1561 (2019)
13. N.U. Hassan, C. Yuen, D. Niyato, Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions. IEEE Ind. Electron. Mag. **13**(4), 106–118 (2019)
14. A. Goranovic´, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, Blockchain applications in microgrids an overview of cur- rent projects and concepts, in IECON 2017–43rd Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2017, pp. 6153–6158.
15. P. Siano, G. De Marco, A. Rola´n, and V. Loia, A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets, IEEE Systems Journal, vol. 13, no. 3, pp. 3454–3466, 2019.
16. M. Troncia, M. Galici, M. Mureddu, E. Ghiani, F. Pilo, Distributed ledger technologies for peer-to-peer local markets in distribution net- works. Energies **12**(17), 3249 (2019)
17. A. Ahl, M. Yarime, K. Tanaka, D. Sagawa, Review of blockchain- based distributed energy: Implications for institutional development. Renew. Sustain. Energy Rev. **107**, 200–211 (2019)
18. Y. Hao, Y. Li, X. Dong, L. Fang, P. Chen, Performance analysis of consensus algorithm in private blockchain, IEEE Intell Vehicl Symp IV. Changshu **2018**, 280–285 (2018). https://doi.org/10.1109/IVS.2018.8500557
19. Z. Cui et al., A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Trans. Serv. Comput. **13**(2), 241–251 (2020)
20. K. Lei, M. Du, J. Huang and T. Jin, Groupchain: towards a scalable public blockchain in fog computing of IoT services computing, IEEE Trans Serv Comput **13**(2), 252–262 (1 March-April 2020).
21. M. Zhaofeng, W. Xiaochang, D.K. Jain, H. Khan, G. Hongmin, W. Zhen, A blockchain-based trusted data management scheme in edge computing. IEEE Trans. Industr. Inf. **16**(3), 2013–2021 (March 2020)
22. H. Paik, X. Xu, H.M.N.D. Bandara, S.U. Lee, S.K. Lo, Analysis of data management in blockchain-based systems: from architecture to governance. IEEE Access **7**, 186091–186107 (2019)
23. H. Xu, L. Zhang, Y. Liu, B. Cao, RAFT based wireless blockchain networks in the presence of malicious jamming. IEEE Wireless Commun Lett **9**(6), 817–821 (June 2020)
24. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang, Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybernet Syst **49**(11), 2266–2277 (Nov. 2019)
25. Editorial: Blockchain in Industrial IoT Applications: Security and Privacy Advances, Challenges, and Opportunities, in *IEEE Transactions on Industrial Informatics*, 16(6), 4119–4121 (June 2020)
26. D. Sikeridis, A. Bidram, M. Devetsikiotis, M.J. Reno, "A blockchain-based mechanism for secure data exchange in smart grid protection systems,", , IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). Las Vegas, NV, USA **2020**, 1–6 (2020). https://doi.org/10.1109/CCNC46108.2020.9045368
27. J. Wang, L. Wu, K.R. Choo, D. He, Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Trans. Industr. Inf. **16**(3), 1984–1992 (March 2020)
28. S. Zoican, M. Vochin, R. Zoican and D. Galatchi, Blockchain and consensus algorithms in internet of things, 2018 International Symposium on Electronics and Telecommunications (ISETC 2018), pp. 1–4, Timisoara.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.