Electrical Power and Energy Systems 148 (2023) 108933

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Blockchain-based dynamic energy management mode for distributed energy system with high penetration of renewable energy

Longze Wang [a], Siyu Jiang [a], Yuyao Shi [b], Xinxin Du [b], Yuxin Xiao [b], Yiyi Ma [a], Xinxing Yi [a], Yan Zhang [b,c], Meicheng Li [a,*]

[a] State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources, School of New Energy, North China Electric Power University, Beijing 102206, China
[b] School of Economics and Management, North China Electric Power University, Beijing 102206, China
[c] Beijing Key Laboratory of New Energy and Low-Carbon Development, Beijing 102206, China

ARTICLE INFO

Keywords:
Energy management
Distributed energy
Blockchain
Consensus mechanism
Encryption algorithm

ABSTRACT

The emerging blockchain technology is one of the most feasible solutions to decentralized and autonomous energy management in distributed energy systems (DESs). However, with the increase of renewable energy penetration in the DES, blockchain nodes will generate massive calculation tasks and cause high delay in energy trading. In this paper, we propose a dynamic energy management mode, which is tailored for the DES with high penetration of renewable energy. Firstly, a novel consensus mechanism is established by the proof of energy contribution. Particularly, the energy contribution value characterizes the credible transaction, emission reduction, demand response and system operation contribution of energy prosumers. Secondly, the model inversion process of blockchain SM2 encryption algorithm is simplified by using the verification data of nodes with high energy contribution, so as to improve the computation ability of the DES. Finally, an actual energy blockchain project with 300 renewable energy prosumers is analyzed as an example. The case study shows that this work can reduce the network delay to less than 2000 ms, which is more than double the operation efficiency of the energy trading in Ethereum. Moreover, by calculating the network delay under different conditions, it is concluded that the number of committee nodes has a greater impact on operational efficiency than the number of transactions in the new block and the total number of nodes.

1. Introduction

The greenhouse effect has become one of the most pressing problems in the world. According to the report of Special Report on Global 1.5 °C Temperature Rise released by IPCC, only by achieving global carbon neutralization in the middle of the 21st century can the extreme harm caused by climate change be mitigated [1]. Under this background, the DES represented by gas-fired electricity (GE), solar energy and wind energy is playing more important roles in energy structure to solve the conflict between energy saving and emission reduction [2]. A DES is usually a complex physical structure composed of multiple energy prosumers [3], and has high renewable energy penetration [4].

A number of energy management modes have been proposed for DESs to improve the permeability and utilization efficiency of renewable energy [5,6]. The conventional centralized management modes reported several drawbacks due to a high cost of communication from the central controller to all single equipment and these methods also pose the risk of single-point failures [7]. Moreover, often the existing decentralized energy management strategies are unable to realize the mutual trust of multiple stakeholders and plug-and-play of energy equipment [8]. With the rise of digital technology, the distributed information interaction of blockchain has stimulated new vitality for the energy management of DESs [9,10].

Blockchain has the characteristics of decentralization, openness and transparency, which would become a key breakthrough in the next round of technological innovation. However, blockchain technology has not been widely used due to hurdles in economics, policy and regulatory aspects. In terms of economics, the blockchain distributed data structure has brought more huge data storage capacity requirements, and

* Corresponding author.
E-mail addresses: 51102710@ncepu.edu.cn (L. Wang), 120202211047@ncepu.edu.cn (S. Jiang), 120212206082@ncepu.edu.cn (Y. Shi), 120202206172@ncepu.edu.cn (X. Du), 120212206094@ncepu.edu.cn (Y. Xiao), 120212211018@ncepu.edu.cn (Y. Ma), 120222211084@ncepu.edu.cn (X. Yi), zhangyan8698@ncepu.edu.cn (Y. Zhang), mcli@ncepu.edu.cn (M. Li).

https://doi.org/10.1016/j.ijepes.2022.108933
Received 14 June 2022; Received in revised form 22 November 2022; Accepted 27 December 2022

Nomenclature

Acronyms

DES	distributed energy system
GE	gas-fired electricity
PoEC	proof of energy contribution
NBFT	non-byzantine fault tolerance
BFT	byzantine fault tolerance
PoW	proof of work
PoS	proof of stake
DPoS	delegated proof of stake
pBFT	practical byzantine fault tolerance
dBFT	delegate byzantine fault tolerance
PV	photovoltaic
WPP	wind power plant
GPP	gas power plant
CNS	committee node subgroup
DPC	data preservation contribution
DAC	data authorization contribution
OC	online contribution
DCC	data communication contribution
CTC	credible transaction contribution
ERC	emission reduction contribution
DRC	demand response contribution
EIC	energy interaction contribution
IEC	integrated energy contribution

Variables and Parameters

C_m	committee node m
ED	energy data in a consensus
n	total quantity of committee nodes
t	minimum of committee nodes in a consensus
$t^{'}$	actual quantity of committee nodes in a consensus
$K_{C_i}^{public}$	public key of committee node i
$K_{C_i}^{private}$	private key of committee node i
Δt	upper limit of the time to deploy or execute an energy smart contract
$t_{current}$	the time to deploy or execute an energy smart contract in the current consensus
$t_{contract}^{deadline}$	deadline of the time to deploy or execute an energy smart contract
sig	digital signature from CNS
Key	secret key from CNS
α_1	duration of data information recovery
α_2	duration of the data preservation interval
ΔT	time difference in data preservation
T_{now}	current data preservation time
T_{last}	lats data preservation time
kr	influence factor of the data authorization
QA	quantity of data authorization
QDP	quantity of the data preservation
α_3	online time coefficient
$T_{lastblock}$	timestamp of the last consensus block completed
$T_{addtime}$	timestamp of the node joining the DES
$T_{offline}$	off-line time of the node
α_4	reward/punishment factor for *DCC*
$CTC_{i,t}^{supplier}$	*CTC* of energy supplier i in time t
$CTC_{j,t}^{user}$	*CTC* of energy user j in time t
$Q_{i,j,t}^{actual}$	actual quantity of energy interaction between i and j in time t
$Q_{i,j,t}^{contract}$	smart contract quantity of energy interaction between i and j in time t
α_5	reward factor of energy supplier or user for *CTC*
α_6	coefficient of energy supplier for *ERC*
α_7	reward factor of energy user j for *DRC*
e_n	pollutant quantity of per unit energy supplier n emitted
p_n	environmental treatment punishment of unit quantity n emitted
$Q_{j,t}^{rse}$	energy demand response quantity of user j in time t
α_8	reward/punishment factor for *ESC*
$k^{supplier}$	paid fund coefficient of energy suppliers
k^{user}	paid fund coefficient of energy users
$F_{i,t}^{supplier}$	paid fund of energy supplier i in time t
$F_{j,t}^{user}$	paid fund of energy user j in time t
F_t^{total}	total fund of DES operation
k^{token}	token coefficient for paid f und
Tok_t^{total}	total volume of token in time t
$Tok_{i,t}^{re,com}$	token reward volume of committee node i in time t
p	public key of SM2 signature algorithm
d	random number
G	base point of SM2 signature algorithm
E_p	elliptic curve equation
M	energy message
Z_A	hash value
$e, e^{'}$	hash summary
$r, s, \alpha, \beta, \alpha^{'}, \beta^{'}$	signature parameters
P_w	hash password
d_1 and d_2	random numbers
$X_1, X_1^{'} Y_1, Y_1^{'}$	elliptic curve point
M''	forged replaced message
N_{tot}	total number of energy nodes
N_{com}	number of committee nodes
γ	number of transactions in each block

correspondingly more resource consumption problems [11]. Real-time synchronization of complete data by each node would generate a large amount of redundant data, which makes the blockchain economically inefficient for large-scale industrial applications [12]. In terms of policy, the decentralized characteristic of blockchain has a significant anti control tendency, which makes the application of blockchain technology by most governments still in the exploration period [13]. In terms of regulatory, the complete concealment of personal information by blockchain technology may lead to criminal activities escaping from the perspective of supervision [14]. Meanwhile, the blockchain smart contract means "code is a rule", and the legality and supervision mode of this rule are still unclear [15]. These problems have brought hurdles to the development and application of blockchain technology.

The world's first energy blockchain was born in Brooklyn, New York, USA. The solar power generation on the roofs of five households was sold directly to five other nearby households through the blockchain network [16]. Since the distributed energy management strategy is consistent with the decentralized information interaction mode of blockchain, more and more scholars pay attention to blockchain-based energy management for DESs [17,18]. For example, an integrated blockchain-based energy management platform was designed that optimizes energy flows in a microgrid whilst implementing a bilateral trading mechanism. This platform is being tested using a dataset from a real prosumer community in Amsterdam and has demonstrated to have certain technical advantages [19]. Several original bidding strategies for multi-energy trading based on a blockchain network were proposed,

which facilitated the comprehensive utilization of renewable energy through free trading and real-time price [20]. In terms of energy system security, a provably secure authenticated keyless scheme was designed for energy systems. This scheme can improve the reliability of certification and non-repudiation with blockchain technology [21]. To enhance the applicability of trading markets, a universal framework for a blockchain platform was proposed that enables peer-to-peer energy trading in the retail electricity market. This study further demonstrates the technical advantages of blockchain for distributed energy management [22].

In the past 5 years, a lot of scholars around the world have devoted themselves to the research and practice of energy blockchain. However, interestingly, there has no indication of the scale implementation of blockchain-based energy management mode in the actual energy market. The main reason is that the existing blockchain-based energy management mode cannot adapt to the DES with high penetration of renewable energy, and it is embodied in the following three aspects.

(1) The existing energy blockchain technology mainly guarantees the atomicity of asset interaction by means of electronic cryptocurrency deployment [23]. Due to the fact that DES contains massive calculation tasks such as frequency, voltage and power, the traditional blockchain architecture cannot be directly applied to complex energy management scenarios.
(2) The mainstream blockchain consensus mechanisms are designed for financial transactions and currency circulation. Different from the financial trading platform, energy management needs to consider power balance, renewable energy consumption, carbon and pollutant reduction, etc. It is necessary to establish a consensus mechanism for energy blockchains that are consistent with energy interaction characteristics.
(3) With the increase in renewable energy penetration, energy management mode requires a second-level response to cope with the power generation uncertainty. The existing blockchain encryption algorithms focus on ensuring data security and rarely pay attention to operational efficiency. However, the network delay could affect the system reliability and renewable energy consumption.

In this paper, we propose a dynamic energy management mode based on blockchain to address these gaps. This mode includes a novel consensus mechanism that is custom-tailored for DESs and an optimized encryption algorithm that can improve operational efficiency. The main contributions of this paper are summarized below.

Consensus mechanism: The credible transaction, emission reduction, demand response and system operation contribution of energy prosumers are dynamically characterized as the energy contribution value, and the proof of energy contribution (PoEC) consensus mechanism is established. The PoEC consensus mechanism conforms to the operation characteristic of DESs, and introduces the token incentive to ensure the enthusiasm of prosumers to participate in consensus.

Encryption algorithm: The model inversion process of blockchain SM2 encryption algorithm is optimized by using consensus node group whose energy contribution value exceeds the threshold to verify and transmit energy data. The optimized SM2 encryption algorithm simplifies the key management execution process, and thus improves the data communication efficiency of the DES.

Feasibility analysis: The validity, anti-falsification and security of the dynamic energy management mode for energy blockchain are analyzed. The simulation test of the Brooklyn energy blockchain project verifies that the proposed mode can reduce the network delay to less than 2000 ms, which is more than double the operation efficiency of the energy trading system in Ethereum. Moreover, the influencing factors of energy blockchain operation efficiency are analyzed.

The rest of the paper is organized as follows: Section 2 presents the background of state-of-the-art research on consensus mechanism and encryption algorithm of blockchain. The system framework is presented in Section 3. Section 4 explains the PoEC consensus mechanism and Section 5 introduces the optimized SM2 encryption algorithm. Section 6 verifies the proposed mode based on theoretical analysis. Section 7 simulates the operational efficiency through a case study. Finally, conclusions are drawn in Section 8.

2. Background

2.1. Consensus mechanism

Since all states of blockchain are recorded in the global accounts, the consensus mechanism is the mechanism for selecting the accounting nodes in the blockchain network, and the mechanism for ensuring the correct consistency of the accounting data in the whole network [24]. The existing consensus mechanisms are mainly divided into non-byzantine fault tolerance (NBFT) and byzantine fault tolerance (BFT). NBFT consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS), etc. BFT consensus mechanisms include practical byzantine fault tolerance (pBFT) and delegate byzantine fault tolerance (dBFT), etc.

PoW can be found in the Hash cash proof of work developed to limit denial of service attacks on Internet resources [25]. It was initially used for Bitcoin's underlying architecture and can verify that the specified workload has been completed by reviewing the work results. This simple consensus mechanism can ensure the legitimacy and robustness of the entire blockchain system. The advantage of the PoW consensus mechanism is that the higher decentralization, nodes plug-and-play and the cost of damaging the system are huge. The disadvantage is the low trading efficiency, and bringing a lot of resource waste through computing power competition [26].

In order to reduce the computational difficulty, PoS consensus mechanism combines the number and holding time of virtual tokens held by nodes to form a comprehensive index. The higher this index, the lower the difficulty of node calculation [27]. PoS reduces the computational threshold for nodes with more tokens and increases the probability of generating new blocks. This consensus mechanism reduces the threshold of node performance, shortens the time to reach consensus, but reduces the degree of system decentralization [28].

The DPoS consensus mechanism generates a block by some agents, which are selected by each node. The selection mode does not depend on calculation and Token, but on reputation. Therefore, dishonest agents will be voted out to improve the credibility of consensus information. This deterministic selection of block producers allows very fast confirmation times, and improve the consistency efficiency of the whole network data [29,30]. However, this consensus mechanism sacrifices the decentralized model and theoretically increases the possibility of blockchain networks being manipulated [31].

The pBFT consensus mechanism was proposed by Castro and Liskov in 1999 to solve the problem of low efficiency in the original BFT algorithm [32]. It reduces the complexity of the algorithm from exponential level to polynomial level, which makes BFT algorithm feasible in practical system applications. Firstly, the client sends a request call service operation to the main node, and then the main node broadcasts the other copies of the request. All copies execute the request and send the result back to the client. The client needs to wait for $f + 1$ different replica nodes to return the same result as the final result of the whole operation. The difference of dBFT consensus mechanism is the whole blockchain network is divided into consensus nodes and ordinary nodes, and consensus nodes are agents selected by ordinary nodes [33]. The consensus efficiency of pBFT and dBFT is high. The pBFT and dBFT can deal with high-frequency trading volume, and basically meet the requirements of commercial real-time processing. The defect is that one-third of the accounting nodes stop working, the system will not be able to run normally [34].

Proof of activity (PoA) is not an independent consensus algorithm,

but a hybrid algorithm of PoW and PoS. In the PoA consensus mechanism, there can be an unlimited number of nodes, but the number of verifiers is limited. The node mainly synchronizes the blockchain ledger information, while the verifier is responsible for verifying transactions and packaging blocks. Due to the limited number of verifiers, the PoA consensus mechanism is more efficient and scalable than the PoW.

In view of the complex physical structure and special operation requirements of the energy system, some scholars have designed blockchain consensus algorithms for the energy system. The Green PoW proof mechanism proposed in Ref. [35] alleviates the low efficiency of the PoW consensus algorithm by selecting a few miners to mine the next block. Ref. [36] designed a network cooperation mechanism for reaching agreements based on the regional multi-energy aggregation model of virtual power plants. This consensus mechanism could reduce internal energy dispatching decision-making time in virtual power plants. A Proof of Benefit consensus mechanism is used in the local power market, which achieves power demand side response through benefit incentive [37]. Ref. [38] proposed a proof of credit protocol, in which credit and tokens are used to encourage nodes to cache and transmit more content in honest behavior. These efforts aim to improve the applicability of the consensus algorithm in the energy system by simplifying the consensus verification process or using incentive strategies.

The existing blockchain consensus mechanism cannot take into account decentralization, security and scalability at the same time, and can only choose the appropriate consensus mechanism according to different application scenarios [39,40]. For example, PoW is relatively prominent in security and decentralization, which is suitable for high-value payment applications, and DPoS has the higher efficiency, but it is only suitable for commercial applications that require less decentralization. Therefore, according to different application fields and technical goals, such as the energy system, it is necessary to design a proper blockchain consensus mechanism suitable for energy management.

2.2. Encryption algorithm of blockchain

Encryption algorithms are the plaintext file or data according to some algorithm processing, in order to ensure that the data is not illegally stolen and read [41]. They can be divided into symmetric encryption and asymmetric encryption. Blockchain network mainly uses asymmetric encryption technology, which requires two kinds of keys, public key and private key [42]. Existing blockchain encryption algorithms mainly include three categories: hash algorithm, zero knowledge proof and elliptic curve algorithm.

The hash algorithm maps a binary value of any length into a shorter, fixed-length binary value, which is called a Hash. A hash is a unique and extremely compact numerical representation of distributed data. The hash algorithm is a one-way cipher system, that is, an irreversible mapping from plaintext to ciphertext, only the encryption process and no decryption process [43,44]. Decentralized computation can be realized because of the determinacy and efficiency of this algorithm, and the security of the blockchain network is improved to a certain extent [45]. However, the hash algorithm needs to consume a lot of computing power, and network delay is high, so it is mainly used in virtual currency transactions such as Bitcoin [46].

The zero knowledge proof is the certifier cannot provide any useful information to verify messages, but can make the verifier believe that an argument is correct [47]. This algorithm has two parties, which are called the certifier and the verifier. The two parties follow an agreement and interact with each other, and ultimately the verifier will come to a conclusion about whether the verifier knows or has a certain message. The zero knowledge proof encryption algorithm has certain advantages in the privacy protection of participating nodes [48]. However, due to the complexity of this encryption algorithm, it is rarely applied to energy systems with complex physical structures.

Based on elliptic curve mathematics, elliptic curve cryptography relies on the difficulty of the elliptic curve discrete logarithm problem [49]. The short key length of this algorithm makes it advantageous to save network broadband and node storage. Moreover, all nodes can select different curves in the same underlying domain, so that all users can perform domain operations using the same operation [50]. A reliable encryption algorithm is a necessary guarantee for the security of the energy blockchain business. Ref. [51] proposed a private key storage algorithm based on image information hiding and verified that this algorithm can improve the robustness of the energy blockchain system. Aiming at the vulnerability of public blockchain networks, Ref. [52] proposed an identity-based encryption algorithm. This algorithm does not need the public key certificate to reduce energy consumption and improve security. Ref. [23] improved the RSA encryption algorithm to achieve secure data communication between multiple microgrids. These researches mainly focus on using encryption algorithms to enhance the security of energy data. However, it is worth noting that energy scheduling and interaction require a second level response. In particular, the volatility of renewable energy has put forward higher requirements for the data interaction efficiency of the energy system. Therefore, the design of a secure and efficient encryption algorithm is also a concern of energy blockchain technology.

SM2 is an elliptic curve algorithm used in China, which includes digital signatures, key exchange, public key encryption and other features. Compared with traditional algorithms such as RSA, this algorithm has higher security, faster computing speed, smaller storage space and lower broadband requirements [53]. The SM2 encryption algorithm is widely used in industrial blockchain systems, but it is still possible to optimize according to different application scenarios [54]. Beyond the state-of-the-art, in this work, we propose an optimized SM2 encryption algorithm for DESs that can improve system operation efficiency.

2.3. Conclusions and objectives

To summarize, the mechanism research on the energy blockchain system remains a gap since the optimized consensus mechanism and encryption algorithm may be absent. The existing consensus mechanism selects consensus nodes mainly considering the computing power, virtual token and reputation, but does not combine the operation characteristics and requirements of DESs. For example, the evaluation and selection of consensus nodes do not consider power balance, power generation efficiency, demand response and carbon emissions. In addition, the research on the operation efficiency of energy blockchain is insufficient. For the high penetration of renewable energy, it is urgent to develop blockchain encryption algorithm with lower network latency to achieve efficient scheduling of energy systems.

To address existing technical deficiencies, we propose a novel blockchain-based energy management mode. This mode not only proposes a consensus mechanism to dynamically select consensus nodes according to the energy contribution of each prosumer, but it also aims to make data efficient interaction through an optimized SM2 encryption algorithm. The idea organization and main procedures of this work are shown in Fig. 1.

3. System framework

Energy management based on blockchain can organically integrate DESs with digital technologies [55]. In this study, the proposed energy management system is divided into three layers, namely the physical layer, blockchain mechanism layer and application layer. The lower layer provides an interface to the upper layer that realizes the real-time dissemination of information in these architecture levels. The upper layer sends application requirements or information interaction instructions to realize the efficient operation of the DES. The hierarchical framework is shown in Fig. 2.

The physical layer is the basis of the energy management system, which includes five main parts: electricity production, utilization,

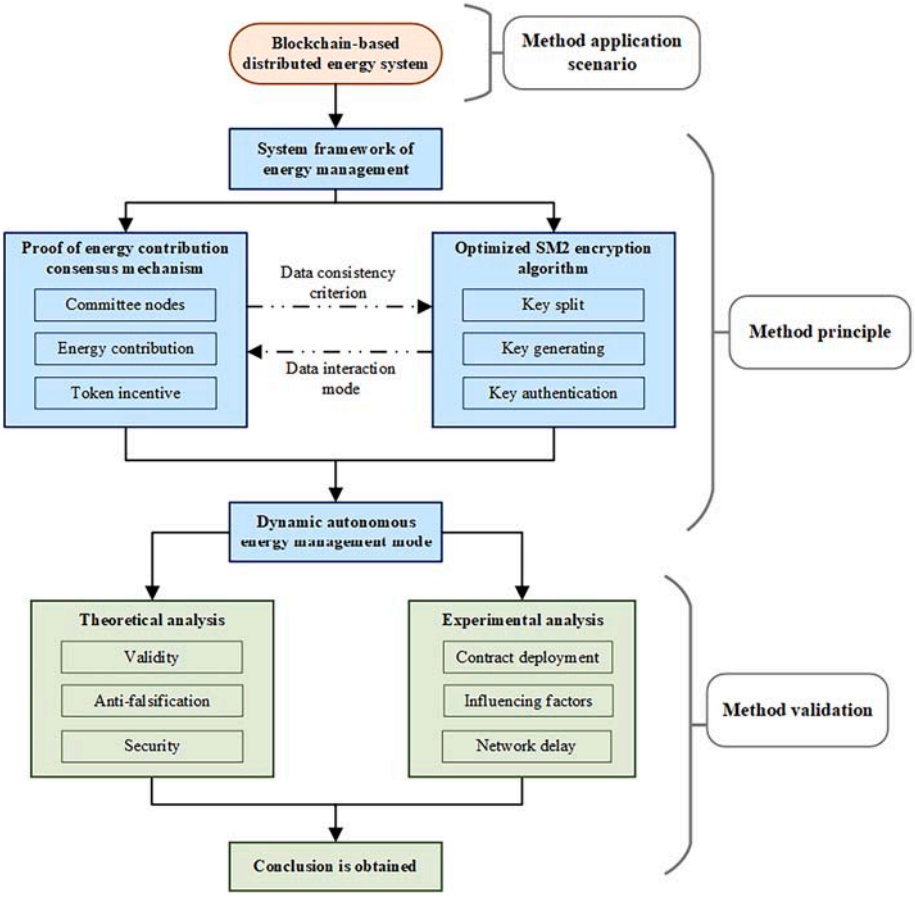

Fig. 1. Idea organization and main procedures of this work.

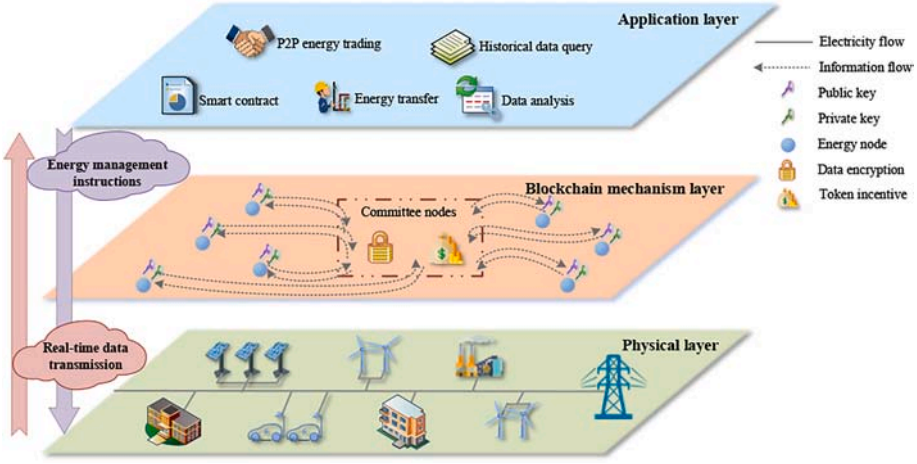

Fig. 2. Hierarchical framework of the blockchain-based energy management system.

transmission/distribution, metering and communication. Electricity production equipment is dominated by renewable energy, such as distributed photovoltaic (PV) and wind power plant (WPP), and also includes gas power plant (GPP) to ensure the stability of the regional power supply. Electricity utilization equipment includes all power consumption equipment in residents, commerce and industry, and electricity consumption is calculated according to the measurement standards of the Internet of Things. Electricity transmission/distribution facilities mainly refer to the distribution network, which can transmit electric energy from the producer to the utilization equipment. Electricity metering generally refers to smart meters. The smart meter is responsible for measuring and collecting the user 's consumption information. After a short period of storage and simple processing, it is collected into the wide area network in the form of encrypted data packets through the neighborhood. The wide area network is responsible for the communication function of the system. It generally adopts wireless 4G public network, and wireless 4G private network or 5G network can be used where conditions permit. The designed consensus mechanism and asymmetric encryption algorithm are integrated into the blockchain mechanism layer. The application layer is used to

provide transaction entry for participants and managers. These applications could include P2P energy trading, energy transfer, data analysis, smart contract and historical data query.

In a typical P2P trading scenario of the DES, market players include electricity producers, suppliers, consumers and electricity-selling enterprises. Electricity producers are mainly renewable energy producers such as PV and WPP, while electricity consumers are all kinds of users who actively participate in the distributed electricity market. The commodity of P2P energy trading is electricity. This study does not consider the transaction of heat load, cooling load, coal and other energy sources. The market organization and commodity trading process include 7 main steps:

Step 1: In t slot, seller A creates t + 1 slot transaction order information in the energy management system, and digitally signs the created order information.

Step 2: The system submits the order information and signature information to the smart contract gateway, and the smart contract gateway calls the identity certificate to verify the signature information of seller A.

Step 3: If the verification of signature A is passed, verify the saleable electricity quantity of seller A in time slot t + 1. Otherwise, the transaction request of seller A is ignored.

Step 4: After the verification of electricity sales passes, call the P2P trading module to create an order block and record the information in the blockchain system.

Step 5: Buyer B finds the order information to be confirmed by itself through the P2P trading module, and confirms it through digital signature.

Step 6: If the signature is verified, the transaction voucher and order block information are generated. Meanwhile, bilateral account information is updated and recorded in the energy management system. Otherwise, the transaction order is ignored.

Step 7: Perform power dispatching in t + 1 timeslot according to the trading protocol of t timeslot, and conduct the commodity trading process of t + 2 timeslot according to steps 1–6.

The energy management system indicates the transaction power and transaction amount through the blockchain smart contract. When the smart contract is triggered, the traded commodity, i.e. electricity, can be delivered in a short time, and the corresponding settlement is automatically executed immediately. This market organization ensures that the interests of all parties would not be damaged, and some extent avoid the cumbersome process of centralized settlement.

The energy management system can be divided into six computer modules that include consensus mechanism module, configuration module, storage module, energy trading module, block validation module and data transfer module. The functional module structure is shown in Fig. 3.

The system startup needs to read the first batch of committee lists and consensus mechanism parameters in the configuration module. When the committee nodes receive the transaction sent by prosumers in the blockchain network, it is necessary to verify the trading demand. After a validation can be added to the energy trading module, the trading module according to preset conditions for energy trading match. Prosumers who reach the transaction deploy smart contracts based on the parameters, and execute these contracts in the energy trading module. The energy trading module needs to build a relationship between the contract sender and the contract address in the storage module and record the address of the contract sender in the candidate list. After a trading complete, the system updates the energy contribution values of each prosumer.

In the consensus mechanism module, it enters the new block generation process after the current block generation. Firstly, reading the trading behavior of the relevant prosumers in the storage module. Secondly, the system adds a timestamp, weight calculation and incentive calculation. Finally, after the historical block information is added, the counter is waiting to complete the instruction. When the counter timing is completed, the block is transmitted to the whole network through the data transfer module.

The block validation module not only verifies the block header information received in the data transfer module, but also verifies the

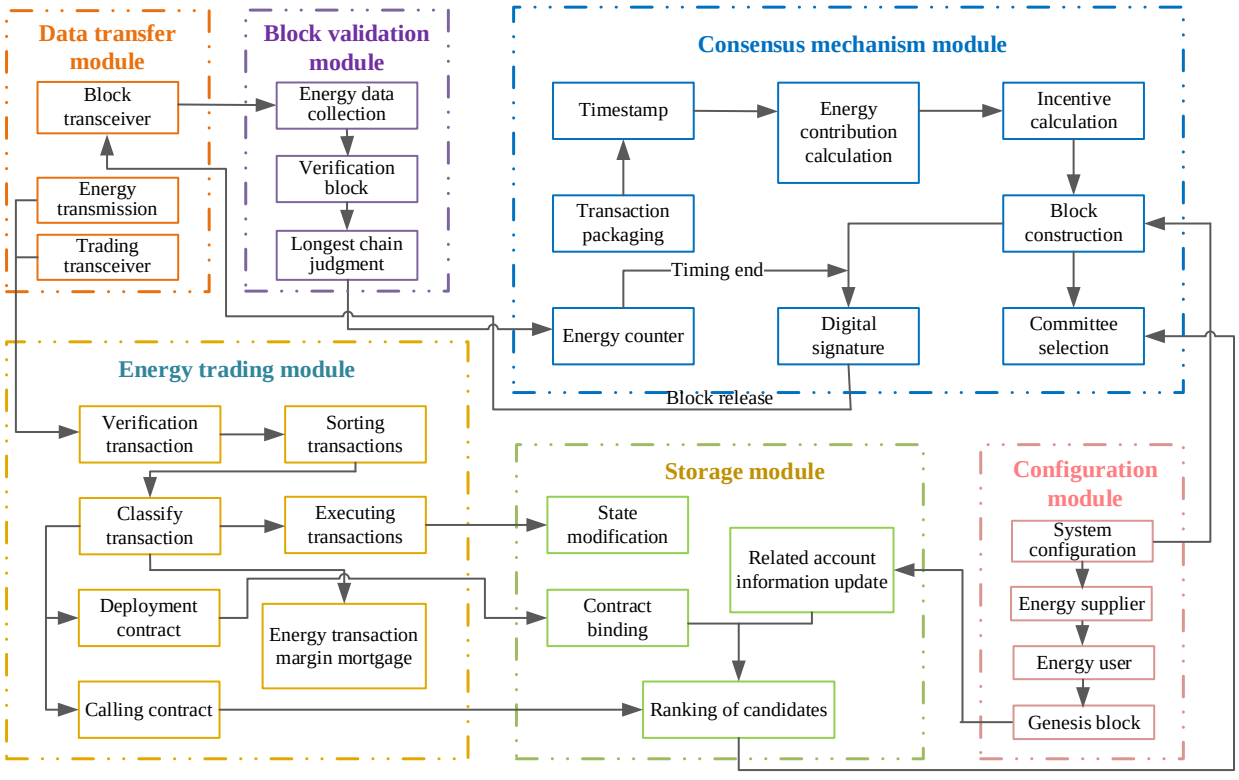

Fig. 3. Functional module structure in the blockchain-based DES.

executing transaction in the energy trading module. If this validation passes, the longest chain judgment verifies block height and weight, and determines whether termination information is required to be sent to the counter in the consensus mechanism module.

4. Proof of energy contribution consensus mechanism

In this section, we elaborate on the basic principles of the PoEC consensus mechanism, including committee nodes election, threshold digital signature, energy contribution calculation and the corresponding token incentive.

4.1. Committee nodes threshold-signature

The nodes in the energy management system include five categories, namely, ordinary nodes, candidate nodes, committee nodes, alternate committee nodes and regulatory nodes. Each prosumer is regarded as an ordinary node, and the prosumer expected to be a committee node is defined as the candidate node. The birth of the committee node is to deal with the malicious node of the BFT consensus algorithm. They mainly implement the consensus process and have the right to rotate out blocks. The committee nodes in PoEC consensus mechanism are responsible for data validation and transmission in the DES operation. The selection process of committee nodes is shown in Fig. 4. Each prosumer is regarded as an ordinary node, and the prosumer expected to be a committee node is defined as the candidate node. Moreover, some regulatory nodes for real-time supervision of the energy blockchain system are also set, such as the energy department, the tax department and the distribution network enterprises. The system dynamically calculates and sorts the energy contribution value of the candidate nodes. If the energy contribution value is greater than the preset threshold, it is elected as a committee node, and vice versa as an alternative committee node. The committee nodes are responsible for data confirmation, data interaction, transaction execution and other business common confirmation. When a committee node has the single point failure problem and cannot be responsible for consensus services, the alternative committee node with the highest energy contribution value is selected to replace it.

During the generation of new blocks, assume that committee node 1 first receives information that the current transaction needs to record or execute, including data in the current block, timestamps, hash values for the previous block, etc. Committee node 1 is responsible for completing the current block generation and transmission tasks. If the block cannot be generated within the unit time sequence, the current business will be completed by other committee nodes, and the operation completed by committee node 1 is regarded as invalid. If committee node 1 succeeds in generating a block for the current business, the voting phase for other committee nodes to digitally sign the block begins. After the digital signature is completed, ordinary nodes will track and record blockchain information. At the same time, regulatory nodes supervise to confirm the legitimacy and effectiveness of the transaction. Finally, this new block will broadcast over the whole network and arrange to the end in chronological order, namely updating the entire energy blockchain system. The timing diagram of the consensus phase is shown as Fig. 5.

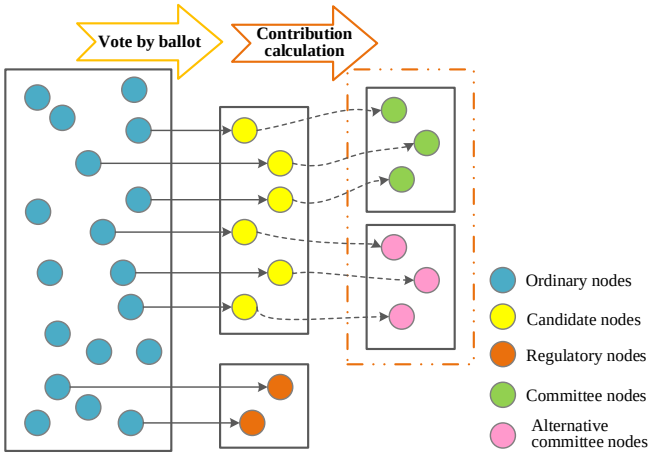

Fig. 4. Election procedures of the consensus committee nodes.

The elected committee node subgroup (CNS) verifies the information by digital signature. The set of committee nodes lists of m consensus validation nodes $C_1, C_2, \cdots, C_m$ that are independent individuals, mutually disjoint and influence. The public–private key pair $\left(K_C^{public}, K_C^{private}\right)$ of CNS is created to validate consensus data in the energy system. The signature would satisfy the following Eqs. (1) to (4), and the stage of this consensus round is completed as shown in the Eq. (5).

$$\{CNS\} = \{C_1 \| C_2 \| \cdots \| C_m, C_i \cap C_j = \varnothing\}, (1 \le i, j \le m) \tag{1}$$

$$|C_i| = n_i, (n_i > 0) \tag{2}$$

$$\sum_{i=1}^{m} n_i = n, m \ge 1 \tag{3}$$

$$K_{C_i}^{public}(ED, t_i, n_i) = \begin{cases} True, if \;\; n_i \ge t_i^{'} \ge t_i \\ False, otherwise \end{cases} \tag{4}$$

$$K_C^{public}(ED, t_1, n_1; \cdots; t_m, n_m; t, n) = \begin{cases} True, if \;\; n_i \ge t_i^{'} \ge t_i \;\; and \;\; \sum_{i=1}^{m} t_i \ge t \\ False, otherwise \end{cases} \tag{5}$$

Nodes involved in a consensus data validation in CNS digitally sign the information. The digital signature of $t^{'}$ can be mathematically represented by Eqs. (6) and (7). If the following conditions are satisfied simultaneously, these energy data form a new block. Otherwise, it ignores the energy data.

$$t_{current} \le t_{contract}^{deadline} - \Delta t \tag{6}$$

$$Traceability(ED, Key, sig) == 1 \tag{7}$$

4.2. Energy contribution calculation

The energy contribution value comprehensively considers the operation contribution of each prosumer in blockchain data communication and energy interaction behavior. In blockchain data communication, the contribution value is calculated according to three aspects including data preservation, data authorization and node online. On the other hand, energy trading in the DES is as important as data communication in the blockchain. The energy interaction contribution of prosumers considers the credible transactions, emission reduction and energy demand response. The calculation process of energy contribution value is shown in Fig. 6.

The data preservation is the basis for the energy blockchain operation. The more nodes are stored, the more comprehensive information is. It can better reflect the value of blockchain distributed database and improve the robustness of energy management system. Therefore, the PoEC takes data preservation as a contribution, which can better promote the data preservation and maintain the robustness. Data preservation contribution (DPC) can be calculated from Eqs. (8) to (10).

The reasons for considering data preservation as a contribution are as follows: First, data preservation is the basis for the operation of the entire energy system, and plays an obvious role in energy dispatching, trading and settlement. Secondly, in the actual operation stage, the preservation of other users' data can earn a certain commission, which can be used as a cash incentive to maintain the blockchain system. Finally, the more nodes preserve data, the less likely the data will be lost

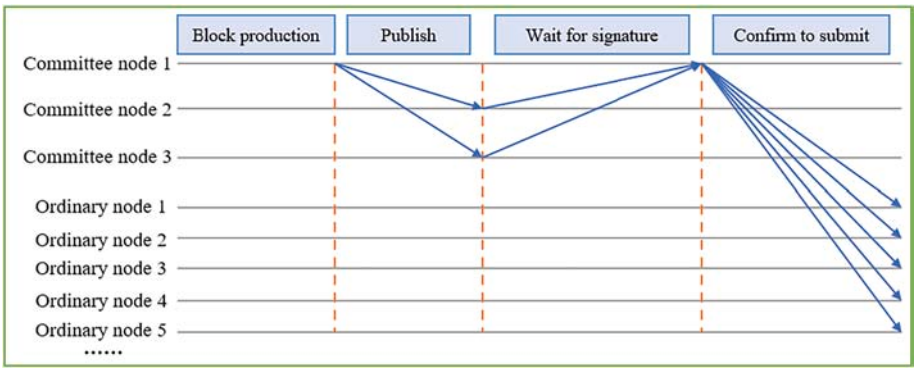

Fig. 5. Timing diagram of the consensus phase.

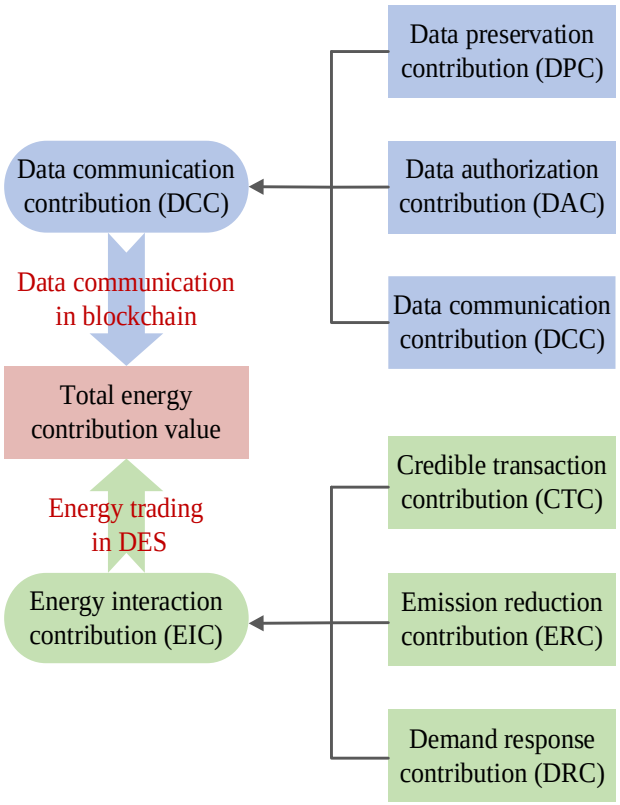

Fig. 6. Calculation process of energy contribution value.

or tampered with. Like other energy contribution values, *DPC* is calculated by the elected committee nodes and maintained by all nodes in the system.

$$DPC = \sum_{1}^{n} \alpha_2 \bullet \Delta T^2/\alpha_1 \tag{8}$$

$$\begin{cases} \Delta T = \sqrt{\alpha_1}, \Delta T > \sqrt{\alpha_1} \\ \Delta T = \Delta T, \Delta T \le \sqrt{\alpha_1} \end{cases} \tag{9}$$

$$\Delta T = T_{now} - T_{last} \tag{10}$$

The data authorization regulates the behavior of both sides of data communication by generating new transaction information. To a certain extent, the more the number of node data authorization is, the higher the contribution value is. Moreover, the data authorization can promote the data flow between energy prosumers and ensure the normal operation of the DES. Therefore, this consensus mechanism counts the data authorization contribution (*DAC*) as a contribution. The system rewards *DAC* according to the influence of data, and it can be calculated from Eqs (11) and (12).

$$DAC = \sum_{1}^{n} \alpha_2 \bullet \Delta T^2/\alpha_1 + (kr)^3 \tag{11}$$

$$kr = QA/QDP \tag{12}$$

The node online is the guarantee of the stable operation of the energy blockchain network, and the system can work normally when not less than a certain number of nodes are online. The more nodes remain online, the higher the security and stability of the energy blockchain network, and the lower the probability of malicious tampering with data. In addition, the node online can promote energy interaction of prosumers, and increase energy trading volume and transaction value. The contribution value of node online can be calculated according to Eq. (13).

$$OC = \alpha_3 \bullet (T_{lastblock} - T_{addtime} - T_{offline}) \tag{13}$$

Based on the above equations, the data communication contribution (*DCC*) can be summed up by *DPC*, *DAC* and *OC*, and the corresponding reward/punishment factor α_4 can be introduced for calculation. α_4 starts with a value of 1 and is fine-tuned according to the actual operation of the DES. For example, when the system needs to be more heavily regulated, α_4 is slightly increased for over-fully authenticated users. The *DCC* can be obtained from (14):

$$DCC = e^{\alpha_4} \bullet (DPC + DAC + OC) \tag{14}$$

Hence,

$$DCC = \alpha_4 \left[2 \bullet \sum_{1}^{n} \alpha_2 \bullet \Delta T^2/\alpha_1 + (kr)^3 + \alpha_3 \bullet (T_{lastblock} - T_{addtime} - T_{offline}) \right] \tag{15}$$

Energy transaction is the basic attribute of DESs and the basic condition of energy production and transmission. When two parties in an energy transaction sign a smart contract, one party fails to perform the transaction in accordance with the contract, resulting in economic losses for the other party. When the actual electricity provided by the supplier is lower than the contract within a certain period of time, the energy user will purchase the shortage of power from the grid. Power grid prices are generally higher than contract prices, causing economic losses to these users. On the other hand, if the actual energy consumption of the buyer is lower than that of the contract, the power provided by the seller cannot be fully utilized during this period, which causes economic losses to the seller. Therefore, the credible transaction contribution (*CTC*) ensures energy and financial interaction in the DES. The *CTC* of energy suppliers and users can be calculated from Eqs. (16) and (17).

$$CTC_{i,t}^{supplier} = \begin{cases} CTC_{i,t-1}^{supplier} + \alpha_5 \bullet Q_{i,j,t}^{actual}, Q_{i,j,t}^{actual} \geq Q_{i,j,t}^{contract} \\ CTC_{i,t-1}^{supplier}, Q_{i,j,t}^{actual} < Q_{i,j,t}^{contract} \end{cases} \tag{16}$$

$$CTC_{j,t}^{user} = \begin{cases} CTC_{j,t-1}^{user} + \alpha_5 \bullet Q_{i,j,t}^{actual}, Q_{i,j,t}^{actual} \geq Q_{i,j,t}^{contract} \\ CTC_{j,t-1}^{user}, Q_{i,j,t}^{actual} < Q_{i,j,t}^{contract} \end{cases} \tag{17}$$

Compared with traditional fossil fuels, renewable energy sources such as PV and WPP do not emit pollutants in energy supply. Emission reduction contribution (*ERC*) is a reward for these renewable energy prosumers to reduce the impact of DES on the environment. In order to flexibly calculate the *ERC* of different energy systems, this study introduces corresponding environmental governance punishment to different fossil energy suppliers. The punishment is based on the pollutant emissions of fossil energy and the environmental treatment cost of the pollutant, and there is no punishment to the renewable energy suppliers. The *ERC* of energy supplier *i* can be calculated from Eq. (18).

$$ERC_{i,t}^{supplier} = \alpha_6 \bullet Q_{i,t}^{actual} - \sum_{n=1}^{N}(e_1 \bullet p_1 + e_2 \bullet p_2 + \cdots + e_n \bullet p_n) \tag{18}$$

Energy demand-side response can suppress unstable power load to a certain extent and improve the utilization efficiency of renewable energy. Therefore, the PoEC consensus mechanism introduces the demand response contribution (*DRC*), and the calculation is as follows:

$$DRC_{j,t}^{user} = \alpha_7 \bullet Q_{j,t}^{rse} \tag{19}$$

Based on the above equations, the energy interaction contribution (*EIC*) can be obtained by *CTC*, *ERC* and *DRC*. The *ESC* is calculated by Eq. (20).

$$EIC = e^{\alpha_8} \bullet (CTC + ERC + DRC) \tag{20}$$

Hence, the integrated energy contribution (*IEC*) of each prosumer in the DES can be obtained from Eq. (21).

$$CTC_{j,t}^{user} = \begin{cases} CTC_{j,t-1}^{user} + \alpha_5 \bullet Q_{i,j,t}^{actual}, Q_{i,j,t}^{actual} \geq Q_{i,j,t}^{contract} \\ CTC_{j,t-1}^{user}, Q_{i,j,t}^{actual} < Q_{i,j,t}^{contract} \end{cases} \tag{21}$$

4.3. Token incentive

The blockchain token incentive is used to reward the committee nodes to improve the enthusiasm of prosumer to participate in consensus. Token is a negotiable proof of encrypted digital rights in blockchain networks and it means to maintain the benign operation of the system. Bitcoin digital currency firstly adopts the token mechanism, which uses the orderly increase method to avoid the digital currency inflation and promote the stable operation of blockchain network. Energy blockchain needs to provide stable value proof for the energy contribution of the committee nodes to ensure the credible interaction between prosumers. Therefore, this section designs the anchor mechanism between the entity assets and the token, and uses the token to incentivize the committee nodes.

Blockchain token incentive can be divided into three steps. First, all prosumers are regularly paid corresponding funds to maintain the basic cost of the energy interaction in the DES. These funds are like the "grid-through fees" in the distributed power market, and the larger the energy supply and demand, the more the funds paid. Secondly, the total token of the energy blockchain network is linked with the funds to make it dynamically change in a certain proportion. Then, every other period of time, such as one day, each committee node can automatically obtain the tokens based on the energy contribution value and obtain the corresponding funds according to the amount of token acquisition. Finally, each prosumer pays the corresponding funds according to the energy supply and demand to maintain the DES operation overhead in the next timing. The blockchain token incentive process is as follows:

$$\sum_{t=1}^{N} F_{i,t}^{supplier} = \sum_{t=1}^{N}(k^{supplier} \bullet Q_{i,t}^{actual}) \tag{22}$$

$$\sum_{t=1}^{N} F_{j,t}^{user} = \sum_{t=1}^{N}(k^{user} \bullet Q_{j,t}^{actual}) \tag{23}$$

$$\sum_{t=1}^{N} F_{t}^{total} = \sum_{t=1}^{N} F_{i,t}^{supplier} + \sum_{t=1}^{N} F_{j,t}^{user} \tag{24}$$

$$\sum_{t=1}^{N} Tok_{t}^{total} = k^{token} \bullet \sum_{t=1}^{N} F_{t}^{total} \tag{25}$$

$$Tok_{i,t}^{re,com} = \left(IEC_{i,t}^{com} \div \sum_{N}^{i=1} IEC_{i,t}^{com} \right) \cdot Tok_{t}^{total} \tag{26}$$

5. Optimized SM2 encryption algorithm

Encryption algorithm is the key to ensure the effective transmission of data. In order to improve the operational efficiency of energy blockchain, this section proposes an optimization algorithm based on SM2. Firstly, the concept and basic principle of SM2 encryption algorithm are described. Then, the optimizing strategy and execution method are expounded for simplifying the data communication process.

5.1. SM2 signature algorithm

SM2 encryption algorithm is the most widely used asymmetric encryption algorithm in China. It is an elliptic random curve cryptography including encryption, decryption and digital signature. Due to the addition of elliptic random curve parameters, basis points and public key information, the security of SM2 in data communication is greatly increased [56]. Blockchain uses SM2 encryption algorithm to manage public and private keys and data interaction mainly includes three aspects: key generation, SM2 signature and signature verification [57].

Key generation needs to input SM2 elliptic curve parameters, including elliptic curve equation E_p, large prime p, base point G and order n of the base point. A randomly generated private key is saved and a public key is generated by public-private key relationship. This process can be obtained from Eq. (27). Where p is the public key of SM2 signature algorithm, and it is an important basis of the encryption and signatures.

$$p = [d]^{*}G \tag{27}$$

The SM2 signature needs to calculate the hash value Z_A that is based on the input numbers of elliptic curve parameters, private key and the energy message M. After obtaining the hash value Z_A, hash summary e is calculated and the energy message M to be signed. Finally, calculate the signature parameters r and s, and output the signature (r, s). These processes can be obtained from Eqs. (28) to (32).

$$Z_A = H_{256}(ENTL_A||ID_A||a||b||x_G||y_G||x_A||y_A) \tag{28}$$

$$e = H_{256}(Z_A||M) \tag{29}$$

$$X_1 = (x_1, y_1) = [k]G \tag{30}$$

$$r = (e + x_1) mod n \tag{31}$$

$$s = \left[(1+d)^{-1} \bullet (k - rd)\right] mod n \tag{32}$$

Signature verification should input elliptic curve parameters, public key of verifiers, energy messages and signature messages sent by the signing party (r', s'). Next, calculate the message to be validated M, the hash summary e and t. If t is equal to 0, the message signature fails and

the information validation fails. If t is not equal to 0, then continue to calculate the elliptic curve point $X_1^{'}$, and verify the signature is successful when formula (35) is true.

$$t = (r' + s')modn \tag{33}$$

$$X_1^{'} = (x_1, y_1) = [s^{'}]G + [t^{'}]P_A \tag{34}$$

$$r^{'} = (e^{'} + X_1^{'})modn \tag{35}$$

5.2. Optimizing strategy

Because the calculation of complex elliptic curve points is involved, the traditional SM2 national encryption algorithm has a high complexity in the encryption process, which makes the entire encryption process take a long time. Moreover, when the SM2 algorithm is applied to the DES requiring second level response, solving random number is the most important factor restricting energy trading efficiency. Therefore, it is necessary to optimize the encryption/decryption process of the SM2 algorithm and shorten the processing time of energy transaction information.

In the DES with high permeability renewable, voltage, power, electric charge and other energy data fluctuate randomly. The model inversion process of energy blockchain system based on SM2 would lead to network delay and cannot quickly manipulate a large number of changing energy data. Therefore, this section verifies transactions and data through the committee node group (CNS) dynamically selected by the PoEC consensus mechanism, eliminating the model inversion process to improve data communication efficiency. The optimized data communication strategy is shown in Fig. 7.

The nodes in the DES divide the public and private key pair of the interactive data into two parts, one part is stored locally in these nodes, the other part is transmitted to the CNS through the key exchange protocol. Each energy data communication needs to be verified by the CNS and the hash value after verification is calculated. The committee nodes cooperate to complete the digital signature. Since each committee node is dynamically selected according to the energy contribution value, the key management process does not affect the decentralization degree of the energy blockchain network. Moreover, the higher energy contribution value guarantees the credibility and reliability of key management. In summary, the model inversion process of SM2 encryption algorithm is replaced by the verification function of the CNS, which simplifies the encryption algorithm and key management of energy blockchain.

5.3. Optimized algorithm execution

According to the optimization strategy of SM2 encryption algorithm, the basic process of energy data communication is expounded from three aspects: key production, digital signature and signature verification. The elliptic curve parameters of the optimized SM2 encryption algorithm are Parms, and CNS is the core mechanism for consensus verification and key management.

Fig. 8 shows the basic process of key production for the optimization algorithm. When a node initiates the energy interaction demand, this node is regarded as the signature initiator Signer. CNS establishes a temporary energy storage file for the node, and generates two random numbers d_1 and d_2 as the private key parameters of the signature initiator and the CNS, respectively. Where $d_1 + d_2 \in [1, n-1]$, and public key $P_s = [d_1 + d_2]G$. Record the current timestamp for hash encryption, and pass the identity password P_w and Signer private key component d_1 to Signer by key exchange protocol.

The digital signature process of the optimized SM2 is shown in Fig. 9. Signer submits the hash password P_w to CNS for identity authentication. If the authentication fails, the signature will not be assisted and this message can be recorded. The node of the Signer would be treated as a failure or untrusted node. If the identity authentication is passed, the private key component of Signer is used to digitally sign the message, and hash summary e is calculated. In addition, a set of $\alpha, \beta \in [1, n-1]$ is randomly generated, and the random number k is constructed with the private key and e. Then, the elliptic curve point X_1 and the output digital signature (r, s, β) are calculated by the following equations.

$$k = (\alpha d_1 + \beta e)modn \tag{36}$$

$$r = (e + x_1)modn \tag{37}$$

$$s = d_1(\alpha + er)modn \tag{38}$$

In the signature verification stage, the node that has been verified (the Verifier) submits hash code P_w to CNS for consensus verification. If the verification fails, the digital signature is not assisted and this information is ignored. At the same time, the node is recorded as a fault node or an untrusted node. If the verification is successful, the digital signature $(r^{'}, s^{'}, \beta^{'})$ of M can be obtained and the private key component d_2 can be saved by CNS. At the same time, the public key in the system is used to verify the information signed by Signer. The basic process is shown in Fig. 10. The verifier needs to determine whether the incoming signature parameters meet the system requirements, namely $(r^{'}, s^{'}, \beta^{'}) \in [1, n-1]$. If the requirements are not met, the data communication cannot be validated. If system requirements are met, hash summary e and two intermediate parameters $t^{'}$ and $u^{'}$ are calculated. According to these intermediate parameters, the elliptic random curve point X_1 can be obtained. Finally, whether R is equal to the value passed by Signer is calculated. Digital signature verification is successful if equal, otherwise not passed. The mathematical description can be obtained by the following equations.

$$t' = (s^{'} + \beta^{'} e^{'} + e' d_2 r')modn \tag{39}$$

$$u^{'} = e^{'} r^{'} modn \tag{40}$$

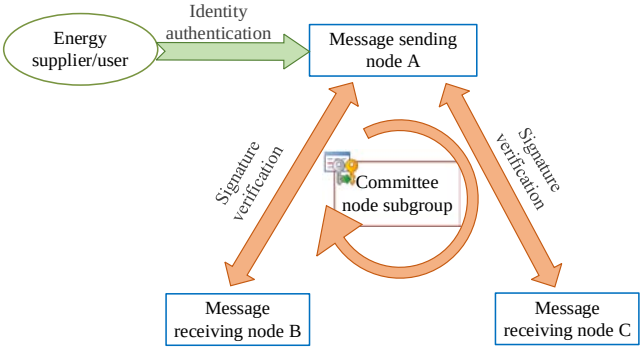

Fig. 7. Optimized data communication strategy.

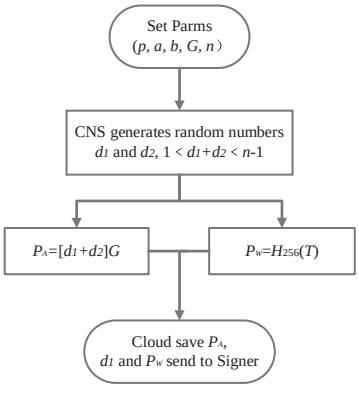

Fig. 8. Key production process of the optimized SM2 encryption algorithm.

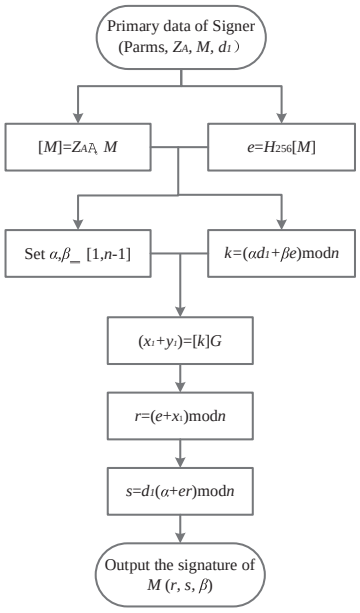

Fig. 9. Digital signature process of the optimized SM2 encryption algorithm.

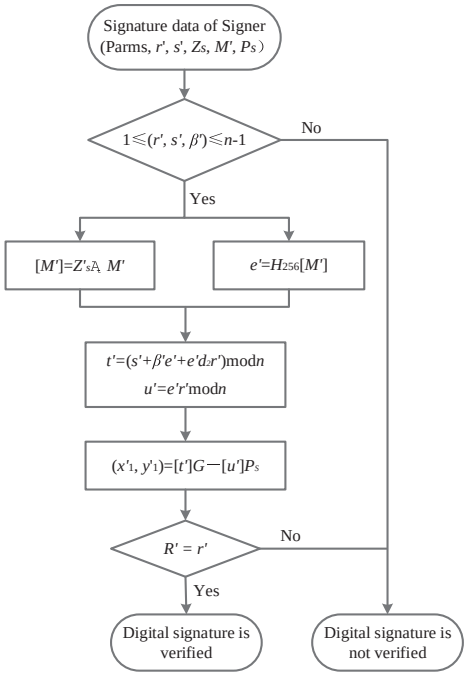

Fig. 10. Signature verification process of the optimized SM2 encryption algorithm.

$$(x_1, y_1) = [t']G - [u']P_s \tag{41}$$

$$R = (e' + x_1')modn \begin{cases} R = r', passed \\ R \neq r', notpassed \end{cases} \tag{42}$$

The optimized SM2 encryption algorithm includes two parts. For one thing, the original random number k value is replaced by the known random number sequence determined by the CNS, where all k values in the known random number sequence meet the initial conditions ($k \in [1, n\text{-}1]$). The difference between the two random number k values before and after the setting remains constant. For another, the k value of the random number encrypted twice has a certain mathematical correlation. This correlation is also jointly formulated by the CNS.

The optimized SM2 algorithm has three characteristics. First, each time the energy data is encrypted, the CNS takes the random number k value from the random number sequence. The random number sequence is composed of a plurality of k-valued short sequences, and the first element of each random number short sequence is randomly generated. Secondly, each short sequence of random numbers has the same length. Finally, in each short sequence of random numbers, the difference between each two adjacent elements is the same.

To sum up, when calculating two elliptic curve points, the point addition operation replaces the point multiplication operation in the original algorithm, which significantly reduces the computational complexity of the algorithm as a whole. Therefore, the optimized SM2 encryption algorithm shortens the encryption/decryption time, thus improving the operation efficiency of the DES.

6. Theoretical analysis

This section verifies the proposed energy management mode through theoretical analysis, including the validity, anti-falsification and security. PoEC consensus algorithm needs to assume that the number of malicious nodes in a certain slot is less than one third of the total nodes. Moreover, each client's transaction request can only be authenticated successfully after 5 stages of management. First, execute the client's request after the server reaches an agreement through two interactions. Then, after receiving multiple transaction requests from ordinary nodes, the committee nodes sort the requests and send the results to the system. At least two thirds of the committee nodes can send the sorting results to all nodes and execute the transaction request only after they have successfully authenticated the sorting results.

6.1. Validity analysis

The energy management mode proposed in this study improves the consensus mechanism of the blockchain network, and fully considers the energy contribution to select a more credible node group for consensus verification. Since the elected committee nodes are dynamically elected according to their actions, the participants responsible for verifying information can be considered trustworthy. On the other hand, the information transmission is based on SM2 encryption algorithm, which can use an elliptic curve discrete logarithm problem to realize signature. Therefore, the success of digital signature needs to meet the validity of the signature scheme first, that is, the signature information of the Signer can be verified by the Verifier.

According to the digital signature process, (r', s', β') is the signature information transmitted by the Signer, and the elliptic curve point X_1' can be calculated from Eq. (43). Through the improved signature strategy relationship, the values of r' and s' can be substituted into Eq. (44).

$$(x_1', y_1') = [t']G - [u']P_s = (s' + \beta' e' + e'^{d_2} r')G - (e'r')P_s \tag{43}$$

$$(x_1', y_1') = (\alpha d_1 + \beta' e')G \tag{44}$$

As long as the signature information (r', s', β') is consistent with (r, s, β) generated by the signature process of the Signer, and the message hash summary is the same. Therefore, Eqs. (45) and (46) are workable, that is, the signature verification process in the system is valid.

$$(x_1', y_1') = [k]G = (x_1, y_1) \tag{45}$$

$$R = (e' + x_1')modn = (e + x_1)modn = r \tag{46}$$

6.2. Anti-falsification analysis

The energy management system based on blockchain has an identity authentication function, especially for energy prosumers, entity

authentication is needed to join the DES. The malicious attackers must obtain signature information through the CNS to join the system. Assuming the attacker is a malicious attack node in the DES, it gets the message (r, s, β) sent by Signer and falsifies the message $M^{''}$ to replace M for digital signature. The three parameters s, e and r in the digital signature process are known. The Attacker uses the forged replaced message $M^{''}$ to calculate $e^{''} = H_{256}(\overline{M^{''}})$. Next, the signature calculation $s^{''} = d_1(\alpha + e^{''}\gamma) mod n$ is forged, and $(r, s^{''}, \beta)$ is taken as the signature data of $M^{''}$. After the Verifier receives the signature information $(r, s^{''}, \beta)$, it verifies the signature and calculates the elliptic curve point $X_1^{''}$. The falsify process can be obtained from (47).

$$\left(x_1^{''}, y_1^{''}\right) = [t^{''}]G - [u^{''}]P_s = (\alpha d_1 + \beta e'')G \neq [k]G \tag{47}$$

It can be seen that the integrity of data can be achieved by hashing the message. Once the data are tampered with, the hash number will change and invalidate the digital signature. Since the probability of hash conflict can be ignored, the proposed information interaction algorithm is an anti-falsification mode.

6.3. Security analysis

The security of energy management mode can be analyzed from three aspects, that is key confidentiality, forward/backward confidentiality and node hazard resistance.

Key confidentiality means that in an open environment, an attacker cannot learn any key information. In the above method, the generation of secret sharing is non-interactive, which means there is no secret key information leakage during transmission. In addition, the optimized strategy is the discrete logarithm problem based on elliptic key construction and the SM2 large number decomposition problem. Both problems have been proved to be difficult, that is, no algorithm can find the private key in polynomial time, so this method is secure in the key confidentiality.

For forward/backward confidentiality, they focus on preventing adversaries from obtaining new keys through old keys. In the proposed method, the communication keys of energy nodes are independent of each other. In addition, the new node independently constructs its communication key. Even if an attacker knows a key or subset key, an attacker cannot obtain another key. Therefore, this method provides confidentiality of backward/forward.

Node hazard resistance is the ability to resist or tolerate attacks in the blockchain-based energy system. If a node wants to obtain the key of information transmission, it must obtain multiple sub-keys from the committee nodes. Only by breaking 51% and above member nodes at the same time can the management consensus mechanism and key communication. With the increasing number of energy nodes joining the DES, the selected committee nodes would also increase. It is extremely expensive to obtain authentication to join the blockchain network and be able to attack more than half of the nodes at the same time. Therefore, the method has strong node resistance and high security.

7. Case study

This section analyzes the operational efficiency of the energy management mode based on PoEC consensus mechanic and optimized SM2 algorithm. Taking the Brooklyn energy blockchain project with high renewable energy penetration as the experimental scenario, the network delay of the constructed block under different conditions is simulated.

7.1. Smart contract deployment

In 2017, the LO3 energy company established the world's first energy blockchain project in Brooklyn, New York. Initially, based on the decentralized architecture of blockchain, this project sold wealthy electricity from five house rooftop PVs directly to their neighbors. The peer-to-peer energy trading platform eliminates the participation of third-party intermediaries in the DES. So far, a range of energy transactions including multi-party trading across 300 business and residential participants have used the blockchain technology. These energy nodes dynamically trade power and autonomous execution based on real-time information from the system.

The proposed blockchain-based energy management mode is deployed on the Ethereum platform. Ethereum is an open-source public blockchain platform with smart contract function, and provides a decentralized virtual machine to deal with peer-to-peer contracts through its dedicated encryption currency. Since Ethereum provides a turing-complete scripting language for users to build any precisely defined smart contract or transaction type, we can implement the PoEC consensus mechanic and the optimized SM2 encryption algorithm. We built a simulation test environment in a computer, which has the configuration is as follows: CPU, Intel Core i7; memory size, 32 GB; operating system, Windows 10. Moreover, the computer must be connected to the network and has a better broadband communication condition.

The network nodes of energy management system include two categories: committee nodes and light nodes. Committee nodes adopt a fully connected network topology, and light nodes and committee nodes adopt a radial network topology centered on committee nodes. According to the current mainstream civil broadband configuration, the network bandwidth of committee nodes and light nodes is set to 100 Mb downlink / 20 Mb uplink. In terms of the computing power, the signature time is set to 0.1 ms, the check time is set to 0.2 ms, and the hash calculation rate is set to 200 MB/s. The resource management of the test platform can be shared remotely, so that participants can log in to the test platform through the network in different locations. Nodes participating in the test can come from different regions and have no distance requirements. With Internet technology, remote resource sharing and testing can be achieved as long as the participant 's authentication is successful.

We encode the underlying architecture that runs DES, including energy contribution calculation, token incentive, information communication, data encryption and decryption. Next, smart contracts for power transactions are installed and deployed on this architecture. Finally, three parameters such as the total number of energy nodes N_{tot}, the number of committee nodes N_{com} and the transaction amount of each block γ are adjusted to test the developed system. The experimental operation interface of the blockchain network is shown in Fig. 11.

7.2. Simulation and analysis

The influencing factors of system operating efficiency are analyzed by the network delay under building blocks in different conditions. We fix the total number of energy nodes in DES, adjust the number of committee nodes and the number of transactions in each block, simulate and count the network delay under different states. These parameters are set as $N_{tot} = 300$, $\gamma = 10, 20, 30$, N_{com} takes different values in the interval [20, 100] with a step size of 10. The network delay varies with the γ and N_{com} can be shown in Fig. 12. The simulation data show that the number of committee nodes has a great influence on the network delay, and the increase proportion of network delay decreases to a certain extent with the increase of N_{com}. On the other hand, the number of transactions in a block also has an impact on the operating efficiency of the DES. But doubling the number of transactions will only delay the blockchain network's growth by a small margin.

To analyze the impact of the total number of energy nodes on the operating efficiency, we fixed the number of transactions $\gamma = 20$. We simulate the network delay of the designed energy management system to build a block under a different condition: $N_{tot} = 250, 300, 350$, N_{com} takes different values in the interval [20, 100] with a step size of 10. The network delay varies with the N_{tot} and N_{com} can be shown in Fig. 13. The simulation data show that the number of participating units in the DES

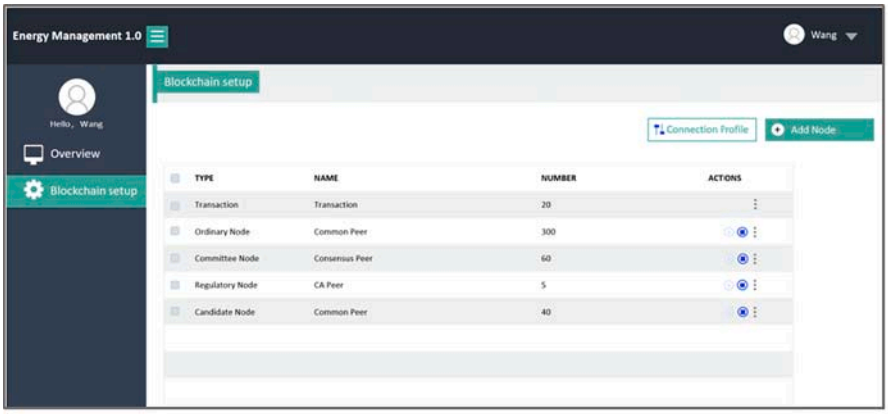

Fig. 11. User interface of the energy management experiment.

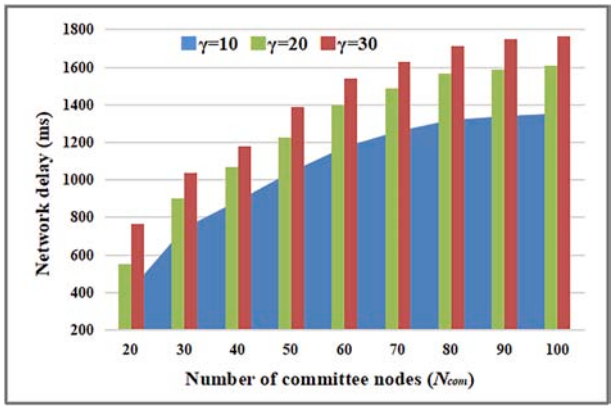

Fig. 12. Network delay in different γ and N_{com}.

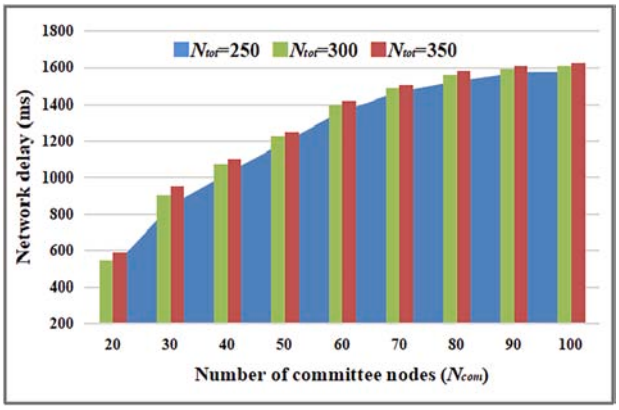

Fig. 13. Network delay in different N_{tot} and N_{com}.

has little effect on the operating efficiency of the blockchain system. Under different energy scale, the number of committee nodes always directly affect the operating efficiency. The main reason is that ordinary nodes receive data synchronously in the blockchain network, and the distributed information communication mode is little affected by the total number of nodes. Committee nodes are responsible for the verification and proof of all data in the blockchain network. The increase of the number of committee nodes directly affects the operating efficiency.

In order to verify the superiority of the proposed energy management mode in improving the operation efficiency of the DES, we compared the network delay of a new block generated by the optimized SM2 algorithm and the encryption algorithm of Ethereum. According to the above analysis, the total number of nodes in the energy blockchain system has little effect on the operation efficiency. Therefore, only the network delay under different consensus nodes and the number of transactions in each block is analyzed. Fig. 14 shows the system operation network delay of optimized SM2 and Ethereum SM2 under different conditions. The simulation shows that when there are fewer nodes involved in consensus verification, that is, when the number of committee nodes is less than 30, the optimized SM2 encryption algorithm makes the system operation network delay lower, but the effect is not obvious. With the increase of nodes involved in consensus verification, that is, after the number of committee nodes is more than 30, the optimized SM2 encryption algorithm has more obvious effect on reducing the network delay of system operation.

In order to further verify the advantages of the optimized SM2 algorithm, we tested the performance of the proposed algorithm and the traditional algorithm on the Hyperledger Caliper platform. Hyperledger Caliper is a convenient and easy-to-use blockchain performance testing tool developed by Huawei and contributed to the Linux Foundation. It supports users to use predefined cases to test the performance of various blockchain applications and obtain a set of detailed performance test results. The Brooklyn energy blockchain project is also taken as the background, and the number of total energy nodes and committee nodes is set to the maximum, that is $N_{tot} = 300$ and $N_{com} = 300$. Five rounds of tests were conducted for the energy P2P transaction function. Fig. 15 shows the transmission efficiency and throughput under different encryption algorithms. The test results show that the transaction transmission efficiency of the optimized SM2 algorithm is 7.84% higher than that of the basic SM2 algorithm. The transaction throughput increased by 38.2%. This is because the encryption/decryption process has no obvious impact on transaction transmission, but it can simplify the key solving process to improve the throughput of energy data.

It is necessary to further explain the simulation. As the quotation,

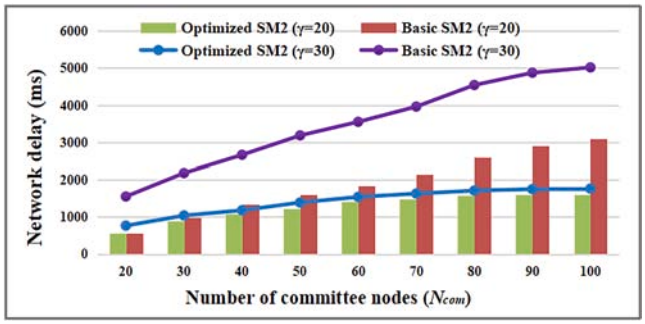

Fig. 14. Network delay in optimized/basic SM2 encryption algorithm.

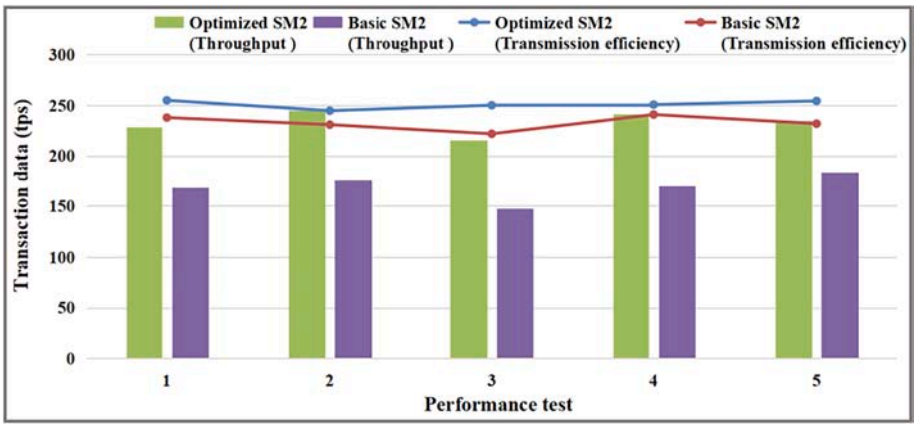

Fig. 15. Transmission efficiency and throughput under different encryption algorithms.

settlement and whether to send transaction requests of each node are independently determined by itself, that is, they are submitted to the system after distributed decision. Therefore, the distributed behavior of each node will not affect the performance test. Theoretically, the system performance of simulation analysis is consistent with that of distributed energy management.

8. Conclusion

A dynamic energy management mode based on blockchain has been presented. It aims at providing a simple but practical mode for the DES with high penetration of renewable energy, in order to improve the applicability of blockchain technology in the energy field. The proposed mode and its novelties can be summarized as following:

(1) This paper tailors a blockchain consensus mechanism for the DES with high penetration of renewable energy. The consensus mechanism introduces the energy contribution value to quantify six operating characteristics, including data communication and energy interaction.
(2) An optimized SM2 encryption algorithm is introduced into the energy management mode, which simplifies the model inversion process and improve the computation ability. Through theoretical analysis, the validity, anti-falsification and security of the proposed mode are proved.
(3) The case study shows that the optimized algorithm can reduce the network delay to less than 2000 ms, which is more than twice as efficient as the traditional SM2. Moreover, the larger the number of committee nodes, the more obvious the improvement of operation efficiency. Lower network delay improves energy management efficiency and helps deal with the uncertainties of high permeability renewables.
(4) The influencing factors of energy blockchain operation efficiency are analyzed. The number of committee nodes has a great influence on the network delay, and with the increase of committee nodes, the proportion of network delay increases decreases. The number of transactions in the new block also affects the network delay, but doubling the number of transactions will only slightly increase the network delay. In addition, the total number of nodes in the system is not strongly correlated with network delay.

The large-scale use of blockchain technology in the energy field also requires attention to non-technical factors, of which the regulatory issue is one of the most noteworthy issues. Government departments or trusted institutions need to monitor all prosumers in real-time through technical means. It is also necessary to formulate corresponding regulations to ensure the orderly operation of the distributed energy market. Meanwhile, it is also necessary to formulate engagement inventiveness measures to enable all stakeholders to actively participate in the energy blockchain system. The expansion of market scale can further promote technological progress.

Future works should be focused on the practical application of this energy management mode and verify its advantages in improving energy system efficiency, economy and emission reduction. Moreover, we would expand the novel consensus mechanism in the field of integrated energy systems and multi-energy markets.

CRediT authorship contribution statement

Longze Wang: Conceptualization, Investigation, Methodology, Software, Writing – original draft, Writing – review & editing, Data curation, Project administration. **Siyu Jiang:** Writing – original draft, Writing – review & editing, Formal analysis, Data curation, Investigation. **Yuyao Shi:** Writing – review & editing, Formal analysis, Investigation. **Xinxin Du:** Writing – review & editing, Formal analysis, Investigation. **Yuxin Xiao:** Writing – review & editing. **Yiyi Ma:** Writing – review & editing. **Xinxing Yi:** Writing – review & editing. **Yan Zhang:** Funding acquisition, Project administration, Resources, Supervision, Validation. **Meicheng Li:** Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgement

This work is supported partially by National Natural Science Foundation of China (Grant Nos. 71974055, and 51772096), Beijing Science and Technology Project (Z211100004621010), Par-Eu Scholars Program, 2022 Strategic Research Key Project of Science and Technology Commission of the Ministry of Education, the Fundamental Research Funds for the Central Universities (2020FR002, 2020MS023, 2020MS028), China Postdoctoral Science Foundation (2022M721130) and the NCEPU "Double First-Class" Program.

References

[1] Wang L, Ma Y, Zhu L, et al. Design of integrated energy market cloud service platform based on blockchain smart contract. Int J Electr Power Energy Syst 2022; 135.
[2] Zhang Y, Deng S, Ni J, et al. A literature research on feasible application of mixed working fluid in flexible distributed energy system. Energy 2017;137:377–90.
[3] Li G, Li Q, Song W, et al. Incentivizing distributed energy trading among prosumers: A general Nash bargaining approach. Int J Electr Power Energy Syst 2021;131(5).
[4] Goudarzi H, Rayati M, Sheikhi A, et al. A clearing mechanism for joint energy and ancillary services in non-convex markets considering high penetration of renewable energy sources. Int J Electr Power Energy Syst 2021;129(3):106817.
[5] Cui S, Xiao J-W. Game-based peer-to-peer energy sharing management for a community of energy buildings. Int J Electr Power Energy Syst 2020;123:106204.
[6] Peng P, Li Y, Li D, et al. Optimized economic operation strategy for distributed energy storage with multi-profit mode. IEEE Access 2020;9:8299–311.
[7] Ramos J S, MORENO M P, RODRíGUEZ L R, et al. Potential for exploiting the synergies between buildings through DSM approaches. Case study: La Graciosa Island. Energy Conversion and Management 2019; 194: 199-216.
[8] Wang L, Jiao S, Xie Y, et al. A permissioned blockchain-based energy management system for renewable energy microgrids. Sustainability 2021;13(3):1317.
[9] Ahl A, Yarime M, Tanaka K, et al. Review of blockchain-based distributed energy: Implications for institutional development. Renew Sustain Energy Rev 2019;107: 200–11.
[10] Hasankhani A, Hakimi SM, Bisheh-Niasar M, et al. Blockchain technology in the future smart grids: A comprehensive review and frameworks. Int J Electr Power Energy Syst 2021;129:106811.
[11] Karaszewski R. The Use of Blockchain Technology in Public Sector Entities Management: An Example of Security and Energy Efficiency in Cloud Computing Data Processing[J]. Energies 2021:14.
[12] Li R, Song T, Mei B, et al. Blockchain for Large-Scale Internet of Things Data Storage and Protection[J]. IEEE Trans Serv Comput 2019;12(5):762–71.
[13] Oprea SV, Adela B. Devising a trading mechanism with a joint price adjustment for local electricity markets using blockchain. Insights for policy makers[J]. Energy Policy 2021;152:112237.
[14] Liu E, Pentland AS, Adamson G, et al. Guest editorial: Blockchain technologies and applications[J]. China Commun 2019;16(6):iii–v.
[15] Chen CL, Deng YY, Tsaur WJ, et al. A Traceable Online Insurance Claims System Based on Blockchain and Smart Contract Technology[J]. Sustainability 2021;13 (16):9386.
[16] Mengelkamp E, Gärttner J, Rock K, et al. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Appl Energy 2018;210:870–80.
[17] Samuel O, Javaid N, Alghamdi TA, et al. Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence. Sustain Cities Soc 2022;76:103371.
[18] Xu S, Liao B, Yang C, et al. Deep reinforcement learning assisted edge-terminal collaborative offloading algorithm of blockchain computing tasks for energy Internet. Int J Electr Power Energy Syst 2021;131:107022.
[19] Foti M, Vavalis M. Blockchain based uniform price double auctions for energy markets. Appl Energy 2019;254:113604.
[20] Wang L, Liu J, Yuan R, et al. Adaptive bidding strategy for real-time energy management in multi-energy market enhanced by blockchain. Appl Energy 2020; 279:115866.
[21] Zhang H, Wang J, Ding Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. Energy 2019;180:955–67.
[22] Han D, Zhang C, Ping J, et al. Smart contract architecture for decentralized energy trading and management based on blockchains. Energy 2020;199:117417.
[23] Wang L, Wu J, Yuan R, et al. Dynamic adaptive cross-chain trading mode for multi-microgrid joint operation. Sensors 2020;20(21):6096.
[24] Zhang P, Zhou M. Security and trust in blockchains: Architecture, key technologies, and open issues. IEEE Trans Comput Social Syst 2020;7(3):790–801.
[25] Ren W, Hu J, Zhu T, et al. A flexible method to defend against computationally resourceful miners in blockchain proof of work. Inf Sci 2020;507:161–71.
[26] Cho H. ASIC-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols. IEEE Access 2018;6:66210–22.
[27] Wang Y, Cai S, Lin C, et al. Study of blockchains's consensus mechanism based on credit. IEEE Access 2019;7:10224–31.
[28] Yang Z, Yang K, Lei L, et al. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet Things J 2018;6(2):1495–505.
[29] Li Y, Yang W, He P, et al. Design and management of a distributed hybrid energy system through smart contract and blockchain. Appl Energy 2019;248:390–405.
[30] Xu G, Liu Y, Khan PW. Improvement of the DPoS consensus mechanism in Blockchain based on vague sets. IEEE Trans Ind Inf 2019;16(6):4252–9.
[31] Liu Y, Xu G. Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value. Comput Netw 2021;199:108432.
[32] Tang S, Wang Z, Jiang J, et al. Improved PBFT Algorithm For High-Frequency Trading Scenarios of Alliance Blockchain. Sci Rep 2022.
[33] Mišić J, Mišić VB, Chang X, et al. Adapting PBFT for use with blockchain-enabled IoT systems. IEEE Trans Veh Technol 2020;70(1):33–48.
[34] Coelho IM, Coelho VN, Araujo RP, et al. Challenges of pbft-inspired consensus for blockchain and enhancements over neo dbft. Future Internet 2020;12(8):129.
[35] Lasla N, Al-Sahan L, Abdallah M, et al. Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm[J]. Comput Netw 2022;214:109118.
[36] Wang D, Wang Z, Lian X. Research on Distributed Energy Consensus Mechanism Based on Blockchain in Virtual Power Plant[J]. Sensors 2022;22(5):1783.
[37] Liu C, Chai KK, Zhang X, et al. Peer-to-peer electricity trading system: smart contracts based proof-of-benefit consensus protocol[J]. Wirel Netw 2021;27(6): 4217–28.
[38] Yu B, Liu J, Nepal S, et al. Proof-of-QoS: QoS based blockchain consensus protocol [J]. Comput Secur 2019;87:101580.
[39] Teng F, Zhang Q, Wang G, et al. A comprehensive review of energy blockchain: Application scenarios and development trends. Int J Energy Res 2021;45(12): 17515–31.
[40] Nguyen CT, Hoang DT, Nguyen DN, et al. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access 2019;7:85727–45.
[41] Varan M, Akgul A, Kurugollu F, et al. A Novel Security Methodology for Smart Grids: A Case Study of Microcomputer-Based Encryption for PMU Devices. Complexity 2021;2021.
[42] Noh S, Kim D, Cai Z, et al. A Novel User Collusion-Resistant Decentralized Multi-Authority Attribute-Based Encryption Scheme Using the Deposit on a Blockchain. Wirel Commun Mob Comput 2021;2021.
[43] Zhou H, Gross WJ, Zhang Z, et al. Low-Complexity Construction of Polar Codes Based on Genetic Algorithm. IEEE Commun Lett 2021;25(10):3175–9.
[44] Jing N, Liu Q, Sugumaran V. A blockchain-based code copyright management system. Inf Process Manag 2021;58(3):102518.
[45] Chen S, Zhang L, Yan Z, et al. A distributed and robust security-constrained economic dispatch algorithm based on blockchain. IEEE Trans Power Syst 2021;37 (1):691–700.
[46] Ren Y, Zhu F, Sharma PK, et al. Data query mechanism based on hash computing power of blockchain in internet of things. Sensors 2019;20(1):207.
[47] Wang B, Liu H, Zhang S. A privacy protection scheme for electricity transactions in the microgrid day-ahead market based on consortium blockchain. Int J Electr Power Energy Syst 2022;141:108144.
[48] Xue Z, Wang M, Zhang Q, et al. A Regulatable Blockchain Transaction Model with Privacy Protection. Int J Computational Intelligence Syst 2021;14(1):1642–52.
[49] Mehrabi MA, Doche C, Jolfaei A. Elliptic curve cryptography point multiplication core for hardware security module. IEEE Trans Comput 2020;69(11):1707–18.
[50] Shani B. The security of all private-key bits in isogeny-based schemes. Discret Appl Math 2020;282:184–95.
[51] Dong X, Hua M, Zhao C, et al. Research on Energy Blockchain Platform Based on Private Key Storage Algorithm of Image Information Hiding[J]. IOP Conference Ser: Earth Environ Sci 2019;237(3).
[52] Alornyo S, Zhao Y, Zhu G, et al. Identity Based Key-Insulated Encryption with Outsourced Equality Test[J]. Int J Network Security 2020;22(2):257–64.
[53] Wu K, Cheng R, Cui W, et al. A lightweight SM2-based security authentication scheme for smart grids. Alex Eng J 2021;60(1):435–46.
[54] Lin C, He D, Zhang H, et al. Privacy-enhancing decentralized anonymous credential in smart grids. Computer Standards and Interfaces 2021;75:103505.
[55] Van Leeuwen G, Alskaif T, Gibescu M, et al. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. Appl Energy 2020;263:114613.
[56] Li W, Li R, Wu K, et al. Design and implementation of an SM2-based security authentication scheme with the key agreement for smart grid communications. IEEE Access 2018;6:71194–207.
[57] Yu G, Zha X, Wang X, et al. Enabling attribute revocation for fine-grained access control in blockchain-IoT systems. IEEE Trans Eng Manag 2020;67(4):1213–30.