Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.046698

ARTICLE

An Energy Trading Method Based on Alliance Blockchain and Multi-Signature

Hongliang Tian and Jiaming Wang*

College of Electrical Engineering, Northeast Electric Power University, Jilin, 132012, China

*Corresponding Author: Jiaming Wang. Email: 2202100359@neepu.edu.cn

Received: 11 October 2023 Accepted: 03 December 2023 Published: 27 February 2024

ABSTRACT

Blockchain, known for its secure encrypted ledger, has garnered attention in financial and data transfer realms, including the field of energy trading. However, the decentralized nature and identity anonymity of user nodes raise uncertainties in energy transactions. The broadcast consensus authentication slows transaction speeds, and frequent single-point transactions in multi-node settings pose key exposure risks without protective measures during user signing. To address these, an alliance blockchain scheme is proposed, reducing the resource-intensive identity verification among nodes. It integrates multi-signature functionality to fortify user resources and transaction security. A novel multi-signature process within this framework involves neutral nodes established through central nodes. These neutral nodes participate in multi-signature's signing and verification, ensuring user identity and transaction content privacy. Reducing interactions among user nodes enhances transaction efficiency by minimizing communication overhead during verification and consensus stages. Rigorous assessments on reliability and operational speed highlight superior security performance, resilient against conventional attack vectors. Simulation shows that compared to traditional solutions, this scheme has advantages in terms of running speed. In conclusion, the alliance blockchain framework introduces a novel approach to tackle blockchain's limitations in energy transactions. The integrated multi-signature process, involving neutral nodes, significantly enhances security and privacy. The scheme's efficiency, validated through analytical assessments and simulations, indicates robustness against security threats and improved transactional speeds. This research underscores the potential for improved security and efficiency in blockchain-enabled energy trading systems.

KEYWORDS

Alliance blockchain; multi-signature; energy trading; security performance; transaction efficiency

1 Introduction

With the advancements in modern encryption technologies and the increasing demand for information encryption, blockchain has played a pivotal role in various domains [1–3]. For instance, it has been applied in Internet of Things (IoT) systems to enhance data security [4–6]. It has also found use in data-sharing solutions for healthcare IoT [7], providing efficient and secure data storage services. Moreover, its primary application lies in the financial sector, involving areas such as asset protection and transaction traceability [8]. This paper will delve into the application of blockchain in

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

energy trading, addressing the existing issues in current energy trading schemes and proposing a novel solution.

During the transition from a centralized generation model to a distributed one, the number of energy trading entities has increased, and the application scenarios have become increasingly complex. This presents significant challenges for the operation and management of traditional energy trading systems. Some proposed solutions aim to enhance the original traditional grid. For example, stochastic gaming strategies have been employed to manage user interactions in energy trading, while simultaneously increasing the benefits of user transactions [9]. Other approaches increase the reliability of energy transactions by detecting illegal activities in complex energy networks [10] and utilizing deep learning to learn and manage the transaction process. However, recent research has pointed out that traditional electricity consumers may also participate in energy trading as distributed electricity producers in the current and future distributed energy trading market [11]. This shift sets the stage for the Peer-to-Peer (P2P) energy trading market and has led to the emergence of distributed energy trading systems.

Blockchain-based distributed energy trading is an emerging solution for distributed power generation and consumption [12–15]. The distributed energy trading system possesses several characteristics, such as low loss, low pollution, efficient energy utilization, and convenient deployment, which allows for trading close to users based on their needs. Additionally, it is highly flexible and can reduce the loss of electricity transmission over long distances. In contrast to the traditional energy trading system, where ordinary users can only purchase electricity from the national power sector, the distributed energy trading system enables users to function both as electricity consumers and suppliers. This allows for excess electricity to be traded with other power-shortage users nearby, resulting in mutual benefits. However, the distributed energy trading system's complex transaction mechanism and management, along with the involvement of multiple participants, make it challenging to implement. Nevertheless, the decentralization and tamper-evident characteristics of blockchain technology can effectively overcome these difficulties and meet the distributed energy trading system's requirements.

In traditional signature schemes, the Elliptic Curve Digital Signature Algorithm (ECDSA) is sufficient for its intended purpose. However, it cannot perform signature aggregation and key aggregation, which requires verifying signatures one by one. This process is cumbersome and requires a significant amount of space and resources. To enhance the privacy and robustness of the transaction process between two parties, the conventional blockchain distributed energy transaction scheme incorporates the multi-signature method. The Rivest-Shamir-Adleman (RSA) signature algorithm based on large number decomposition is the most complete and mature public key cryptosystem in theory and application [16]. It is the first algorithm that can be applied to both encryption and signature. The multi-signature is a signature method that Harn first proposed based on RSA [17]. Subsequently, multi-signatures based on Schnorr's algorithm [18] and the efficient aggregated multi-signature Boneh-Lynn-Shacham (BLS) scheme [19] based on the computational cooperative Diffie-Hellman puzzle constructed have emerged. With its simplicity and effectiveness, the BLS algorithm has become a new direction and goal for the study of multi-signature. These evolving and improved schemes enhance the security and efficiency of multi-signature and are well-suited for practical applications when combined with blockchain technology.

The Schnorr signature algorithm represents a significant improvement over ECDSA, as it can merge all signatures and keys in a transaction without revealing the merging process. Additionally, it can perform a single verification of the merged signatures, thereby speeding up the signature verification process. Nonetheless, the Schnorr signature algorithm necessitates multiple communications

and relies on a random number generator during the signature process. Moreover, its m-n mechanism necessitates constructing a public key Merkle tree structure, which consumes considerable space when the m and n values required for a signature are too large. The BLS signature algorithm resolves these issues. It does not require a random number generator and avoids redundant communication before the signer. Furthermore, it can aggregate the signatures in a block into one, and the signature length of this method is shorter, only half that of the Schnorr or ECDSA method. Regarding the BLS signature algorithm, the explanation for its ability to perform multi-signature and its greater conciseness compared to the ECDSA and Schnorr algorithms hinges on two key operations: curve hashing and curve pairing.

Curve Hashing: In the ECDSA and Schnorr signature algorithms, a hash calculation is performed on the message, resulting in a numerical hash value. BLS signature algorithm differs in this regard; it slightly modifies the hashing process, mapping the result to a point on an elliptic curve. This means that in the BLS algorithm, the hash function remains unchanged, but the resulting hash value is used as the x-coordinate to find the corresponding point on the elliptic curve. The signing operation simply involves multiplying the hash result by the private key, producing a point on the curve, which is stored in compressed serialized format, occupying only 33 bytes.

Curve Pairing: After completing the curve hashing, a special function is required that can map two points P and Q from either the same or different curves to a single number, $e(P, Q) \to n$. This function also needs to have a crucial property: for a variable x and two points P and Q, the result remains the same regardless of which point is multiplied by x, $e(x * P, Q) = e(P, x * Q)$. In addition to preserving equality with the exchange of multipliers, it is essential that all other exchanges also maintain equality.

$$e(a * P, b * Q) = e(P, ab * Q) = e(ab * P, Q) = e(P, Q) * e(ab) \tag{1}$$

If there is a public key P, a private key S, $P = S * G$, a signature Sig, $Sig = S * G$, encrypted information M, a hash function H, and a hashed point value G, the following formula holds:

$$e(P, H(M)) = e(S * G, H(M)) = e(G, S * H(M)) = e(G, Sig) \tag{2}$$

From the above formulas, the key aggregation involves merely summing the corresponding hash points, resulting in a point that still resides on the curve and maintains the curve's mapping relationship. Therefore, for multiple keys ($S_1 + S_2$) and their corresponding signatures ($Sig_1 + Sig_2$), the following formula also holds. It demonstrates the aggregability of BLS signatures.

$$e(G, Sig) = e(G, Sig_1 + Sig_2) = e(G, (S_1 + S_2) * H(M)) = e((S_1 + S_2) * G, H(M)) = e(P, H(M)) \tag{3}$$

However, the characteristics of the blockchain itself can lead to a less efficient transaction process, while the anonymity of blockchain nodes and the uncertainty of online status can result in increased uncertainty and possible risks in the step of applying for intermediate node participation in the multi-signature process. Therefore, based on the inclusion of multi-signature, the concept of the alliance blockchain is introduced to transform the required anonymous and uncertain free intermediate nodes into alternate neutral nodes generated and distributed in advance by the central node of the alliance blockchain. This approach can ensure the security of the intermediate nodes involved in the signature. Furthermore, the central node generates a batch of neutral nodes in advance for both sides of the transaction to apply and call, which can effectively reduce the waiting time for intermediate nodes before each transaction. For security considerations, the central node can reset the identity and key

of the intermediate nodes at regular intervals to prevent malicious nodes from stealing transaction information or engaging in other illegal operations by collecting and obtaining the keys of most intermediate nodes.

The main work of this paper has the following three aspects:

1) This paper introduces the alliance chain as the basis of energy trading and considers the central node of the alliance chain as the supervisory center, tasked with providing identity and authentication to the nodes. This paper also generates official and trusted intermediate nodes in advance for subsequent multi-signature to ensure the security and reliability of the transaction process. Additionally, this paper utilizes the characteristic that all nodes can package and store transaction information on the chain without requiring joint authentication of transaction information from all nodes. This approach reduces the verification and uploading time compared to the public chain.

2) This paper proposes an improved multi-signature process structure that utilizes intermediate nodes prepared in advance by the central node of the alliance blockchain. By generating intermediate nodes to collaborate with the two parties involved in the transaction, multi-signature and verification operations can be carried out. This approach eliminates the need for user nodes to frequently and extensively acquire other users' key information, reducing the communication overhead and time consumption inherent in traditional solutions. It simplifies the traditional multi-signature process, effectively enhancing the efficiency of multi-signature.

3) This paper employed security testing tools to detect and analyze the proposed workflow. It also conducted performance comparisons with related articles, demonstrating the advantages of this solution in terms of security, stability, and communication overhead. Additionally, the runtime of this solution was tested and compared to traditional approaches, highlighting its efficiency benefits.

The remainder of the paper is structured as follows. Section 2 covers a discussion of recently proposed new-style energy trading schemes. In Section 3, this paper provides a detailed description of the system framework and operational mechanism of our proposed scheme. Section 4 provides a security analysis of our proposed scheme and compares its performance to that of traditional schemes. Finally, Section 5 concludes this paper.

2 Related Works

In practical applications, Li et al. [20] presented descriptions related to blockchain security and collaborative defense, addressing issues concerning the security of blockchain systems. Cai et al. [21] proposed a blockchain-based information security system that enhances reliability. Additionally, Park et al. [22] introduced a bilateral authorized blockchain data trading system that enhances security and fairness. This illustrates that the current focus in blockchain endeavors predominantly emphasizes security. However, when addressing distributed energy trading schemes, we must also consider efficiency as a simultaneous concern.

In recent years, various schemes for new distributed energy trading models have been proposed. For instance, Dafda et al. [23] proposed a blockchain-based energy trading model to address the problem of energy sharing and make energy trading a more secure and transparent process by eliminating single points of failure and maintaining load balancing and price governance. Additionally, Wang et al. [24] proposed a blockchain-based distributed community energy trading mechanism, which utilizes smart contracts to ensure the confidentiality and integrity of shared information and enhance community economic benefits. However, these two schemes do not optimize for the

disadvantage of slow verification of blockchain transactions when using the nature of blockchain security.

Che et al. [25] and Feng et al. [26] utilized a form of alliance blockchain as a means of improving the transaction rate of traditional blockchain systems. The scheme proposed by Huang et al. [27] adds an incentive mechanism to the alliance blockchain, which improves transaction efficiency. Furthermore, Makhsoos et al. [28] employed a novel Byzantine fault-tolerant consensus algorithm and a Nash equilibrium strategy based on an alliance chain to enhance the performance of the transaction model and the profitability of both sides of the transaction. These solutions generally improve the system efficiency but do not optimize the security of the transaction process.

To address the interactions between producers and consumers in energy trading, Jiang et al. [29] proposed a game theory and Byzantine fault-tolerant alliance blockchain pricing model. Similarly, Dong et al. [30] and Chen et al. [31] incorporated a game theory approach into their schemes, which enables all participants to maximize benefits while reducing the operational costs of energy transactions. However, these schemes do not address the issue of data security in energy transactions.

To address the issue of data privacy protection in energy trading, Gai et al. [32] utilized account mapping techniques to prevent attackers from directly accessing data. They also create different types of accounts based on the user's situation to achieve the goal of privacy protection and transaction storage. Li et al. [33] made a tradeoff between the regulation of energy trading data by regulators and the privacy protection of data. They use Pedersen commitment and Bulletproof range proof to conceal the transaction amount and ensure the authenticity and reliable regulation of trading data. Zhang et al. [34] employed a quality-aware incentive scheme, offering an efficient privacy protection solution.

Some schemes aim to enhance data privacy security by improving the signature and authentication processes while simultaneously protecting user identity, such as the ring signature scheme proposed by Jiang et al. [35]. This scheme achieves anonymity of identity information by using a ring signature instead of a traditional signature and has advantages in privacy, linkability, and attack resistance. However, the communication overhead of the ring signature is relatively large and increases linearly as the ring signature size increases.

Pan et al. [36] proposed a multi-signature scheme based on ECDSA. They designed a new temporary group public key for the signer and introduced an interactive signature protocol to output a single ECDSA signature, which can be verified by the temporary group public key. They also designed a well-constructed secret exchange mechanism, which can hide the content and help to reduce unnecessary resource consumption. However, the nature of multi-signature itself requires the joint participation of multiple nodes, making the system less efficient.

As pointed out in the scheme proposed by Cao et al. [37], the unconditional anonymity of user identity hinders the realization of good transaction order and also leads to the misuse of signatures, which makes it impossible to trace malicious users. And the current smart meter hardware has limited computing power and storage space, which is not suitable for complex public key computation operations at nodes.

Taking into account the advantages and disadvantages of the aforementioned schemes, this paper proposes a new distributed energy trading scheme based on the alliance chain and multi-signature. Our proposed scheme uses the central node of the alliance chain to prepare trusted intermediate nodes in advance, save them, and provide them to both sides of the transaction for invocation. This relieves the computational burden of the user nodes involved in the transaction while ensuring the security

of using multi-signature. The central node of the alliance blockchain can update the key information of the intermediate node according to a certain period, which increases the reliability and security of the system. Additionally, the alliance blockchain does not require all nodes to verify the transaction information to be stored on the chain, avoiding the disadvantage of slow verification in traditional blockchain systems.

3 Proposed Frameworks

The workflow of blockchain-based distributed energy trading entails multiple communication and interaction sessions between the parties, and each transaction involves several necessary steps. The transaction process begins with one party initiating the transaction request, which the other party accepts. Both parties then engage in communication and negotiation before trading energy quotas and amounts. Subsequently, both parties verify the transaction results and submit them to the blockchain for preservation. The energy and amount trading parts are particularly critical as they involve the attribution of energy and money to both parties. It is necessary to ensure that both parties comply with the normal transaction process while preventing attacks from possible malicious node users. Furthermore, confidentiality, integrity, and resistance to attack are essential throughout the entire operation process of distributed energy trading. Since the other parts do not involve the exchange of property and resources, their likelihood of being attacked is low. Therefore, the privacy and security of the entire system can be simplified to the privacy and security of this critical part.

In this section, this paper provides a detailed description of the proposed scheme. The scheme is primarily utilized for authentication and subsequent secure communication between components of smart grids in energy transactions, particularly for secure and trusted signature verification schemes without the participation of other user nodes in multi-signature.

3.1 Components of System

A comparison of this solution with the traditional energy trading model is shown in Fig. 1.

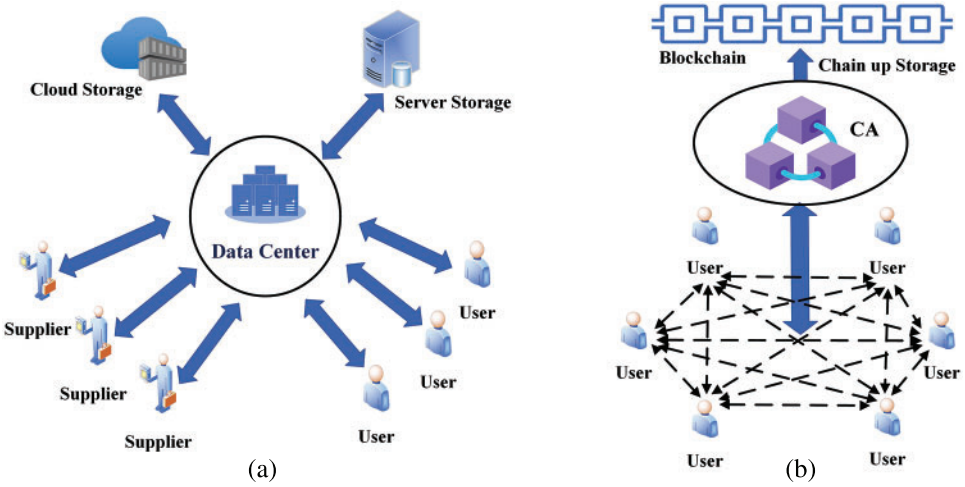

Figure 1: Different network architectures (a) traditional trading system architecture (b) alliance blockchain-based trading architecture

In Fig. 1a, the traditional transaction system architecture is shown. In this architecture, both suppliers and users need to have frequent data interactions with the data center of the trading platform. The communication connection between suppliers and users is carried out through the trading platform, and all transaction processes are computed in the data center and finally sent to the database or stored in the cloud. On the other hand, as shown in Fig. 1b, the multi-signature structure based on the alliance blockchain mainly consists of each node user, the Certificate Authority (CA), the blockchain system, and the communication network between the components. The CA only authenticates the nodes when they enter the network and generates some necessary key materials and intermediate nodes. The transaction process will only be carried out between the user nodes and intermediate nodes, and after the transaction is finished, the CA only needs to authenticate the transaction information and publish and write it to the blockchain system.

Compared to the traditional transaction system architecture, the proposed scheme based on the alliance blockchain significantly reduces the number of data interactions between users and the data center of the trading platform. Additionally, all transaction details are stored on the blockchain, making it easier to track and verify transactions. The use of intermediate nodes also reduces the computational burden on user nodes, making the transaction process more efficient. Overall, the proposed scheme offers a more efficient, secure, and transparent approach to energy trading.

The symbols used in the subsequent description of the system operation and their meanings are shown in Table 1.

Table 1: Symbols and their meanings

Symbols	Meaning
G_1, G_2	Two elliptic curve groups
ID_{Seller}, ID_{Buyer}, ID_{User}	The unique identifiers corresponding to *Seller*, *Buyer* and *User*
S_i, S_{Seller}, S_{Buyer}, S_{User}	Keystore and private keys corresponding to various user nodes
P_i, P_{Seller}, P_{Buyer}, P_{User}	Keystore and public keys corresponding to various user nodes
Add_{Seller}, Add_{Buyer}, Add_{User}	Addresses corresponding to various user nodes

3.2 Network Situation

Here are some known situations and presets of energy trading networks.

1) During the key material generation phase, the communication channel between the alliance blockchain center CA and the user node is private and secure.

2) The communication link between user components for information exchange is public and risky during the key signing and verification phase.

3) Each device has a unique number that can be used to identify it, e.g., ID_{Seller}.

4) Only legal device components can have the parameters published by the system.

3.3 Multi-Signature Scheme

In this section, this paper leverages the BLS signature algorithm to minimize the time required for the signing and verification process. Additionally, this paper employs an alliance blockchain approach to prepare intermediate nodes required in multi-signature in advance and store them in a key vault for

backup. Intermediate nodes are updated with random keys according to a predetermined time interval, thereby enhancing privacy and confidentiality. The number of intermediate nodes can be allocated according to the user's transactional demands, thereby further reducing the time and communication overhead required for traditional node-to-node interactions. To balance confidentiality and the number of communications, the Keystore can communicate with nodes in batches using different ports. This approach reduces the corresponding number of communications as long as the number of batches is less than the required number of neutral nodes. Using different ports and sending in batches also increases confidentiality.

Therefore, this paper proposes an energy transaction scheme that combines an alliance blockchain with BLS multi-signature.

3.3.1 System Initialization

Before allowing nodes to transact, the central node of the alliance blockchain will generate a batch of random intermediary nodes in advance to prepare for the subsequent multi-signature process:

1. A curve function that satisfies the BLS signature scheme, such as the BLS12-381 curve, is selected, and the system curve parameters $\{G_1, G_2\}$ are constructed. G_1 and G_2 are functions of different orders of the BLS12-381 curve and both satisfy the properties of summable and dot product points on the BLS curve.
2. Generate random numbers K_i corresponding to the preset number of neutral nodes, and $K_i \in Z_q^*$.
3. The node's private keys S_i is generated from K_i, and then the G_1 function is used to generate the corresponding public keys P_i, $(S_i, G_1) \rightarrow P_i$.
4. Transfer the generated public-private key pairs $\{S_i, P_i\}$ to the keystore $ARRAY$ for storage.
5. Select the hash function H: $sha256$ to convert the information to a hash value.

3.3.2 User Node Admission Application and Identity Authentication, as well as the Generation of User Key Materials

Regardless of the type of user node identity, all users must apply for admission and undergo identity verification through the CA before engaging in transactions. After successful verification, the CA generates a unique public-private key pair and user address for the user, which is securely stored in the user's digital wallet. The user can access their private key through secure means to initiate a transaction:

1. The CA generates a random number $K_{Seller}/K_{Buyer} \in Z_q^*$ for the user node and creates a unique user identity ID_{Seller}/ID_{Buyer} based on the user's submitted information.
2. The user generates a unique private key S_{Seller}/S_{Buyer} by using the random number and user identity, and calculates the public keys $(S_{Seller}, G_1) \rightarrow P_{Seller}$ and $\left(S_{Buyer}, G_1\right) \rightarrow P_{Buyer}$ by using the G_1 function.
3. The user node uses the public key and a hash function to generate its address, which is then published on the network. Other users can use this address to contact the user and initiate transactions, $(P_{Seller}, H) \rightarrow Add_{Seller}$, $\left(P_{Buyer}, H\right) \rightarrow Add_{Buyer}$.

Eventually, the Keystore $ARRAY$ will hold a collection of public-private key pairs $\{S_i, P_i\}$, and each user node will have its own set of parameters $\{ID_{User}, S_{User}, P_{User}, Add_{User}\}$.

The generation of key materials can be completed during system initialization and user onboarding, as this process is relatively independent of the subsequent multi-signature verification process.

This reduces network overhead when the device is running online, and enables user nodes to perform transactions without the involvement of the central node. The process of key material generation is shown in detail in Fig. 2.

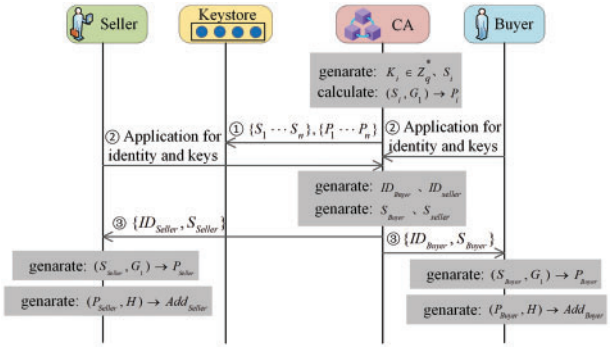

Figure 2: The generation process of key materials

3.3.3 The Process of Multi-Signature and Verification by Both Parties to the Transaction

1. User *Buyer* sends a transaction request to user *Seller* via the network address of *Seller*, $Buyer \rightarrow Add_{Seller}$.
2. The user *Seller* agrees to the transaction request with the user *Buyer*, $Seller \rightarrow Add_{Buyer}$.
3. The user *Buyer* requests n private keys for random nodes from the Keystore *ARRAY*, $ARRAY: \{S_1, S_2 \cdots S_n\} \rightarrow Buyer$, the keystore *ARRAY* needs to send the private keys in batches and the number of batches sent needs to be smaller than n. At the same time, the Keystore *ARRAY* will also send the corresponding public keys to *Seller* in batches, $ARRAY: \{P_1, P_2 \cdots P_n\} \rightarrow Seller$.
4. The user *Buyer* hashes the contents of the transaction message, $MSG = H(message)$.
5. The user *Buyer* uses his private key S_{Buyer} and $\{S_1, S_2 \cdots S_n\}$ to multi-sign and aggregate the signatures of *MSG* according to Algorithm 1 in Algorithm 1, and then sends the aggregated signature and P_{Buyer} to *Seller*, $\{Aggregate\_Signature, P_{Buyer}\} \rightarrow Seller$.
6. The user *Seller* aggregates the public key P_{Buyer} with $\{P_1, P_2 \cdots P_n\}$ and then verifies the multi-signature, this process is also shown in Algorithm 1.

If the verification is successful, both users can confirm the transaction object and the transaction content and proceed with the normal transaction process. If the verification fails, several confirmation verification actions will be performed. If it is determined that the key used or the transaction information has been altered, the user can stop the transaction process, indicating that the transaction has failed.

The algorithms for both multi-signature and verification are shown in Algorithm 1. After executing this algorithm, a prompt will be returned indicating whether the validation was successful.

Algorithm 1: Multi-signature and verification during the transaction process

1. Sign the message with its private key and with a neutral private key, respectively:
2. For S_i in $\{S_{Buyer}, S_1, S_2, \cdots, S_n\}$:
3. $Sign(S_i, MSG) \rightarrow Signatures_i$
4. Aggregate all signatures:

(Continued)

Algorithm 1 (continued)

For *Signature* in $Signatures_i$:
  Mapping signatures to points on the $G2$ curve:
  $signature\_to\_G2\,(Signature) \rightarrow Signature\_point$
  Summing point values using the properties of the $G2$ curve:
  $add\,(Signature\_point) \rightarrow aggregate\_Sig$
Reduction of the summed point value to the signature:
  $G2\_to\_signature\,(aggregate\_Sig) \rightarrow Agg\_Signatures$
Perform public keys aggregation:
For P in $\{P_{Buyer}, P_1, P_2, \cdots, P_n\}$:
  Map the public keys to $G1$ points on the curve:
  $publickey\_to\_G1(P) \rightarrow Publickey\_point$
  Using the $G1$ properties of the curve to sum the point values:
  $add(Public\_point) \rightarrow aggregate\_P$
Reduction of the summed point values to the aggregated public key:
  $G1\_to\_publickey\,(aggregate\_P) \rightarrow Agg\_Publickeys$
Verification of signatures using aggregated public keys:
If $Valid = AggregateVerify\,(Agg\_Publickeys, MSG, Agg\_Signatures)$
  $Valid = True$ Verification success
Else
  $Valid = False$ Verification Failure
End if

The exact process of multi-signature and verification by the user is shown in Fig. 3.

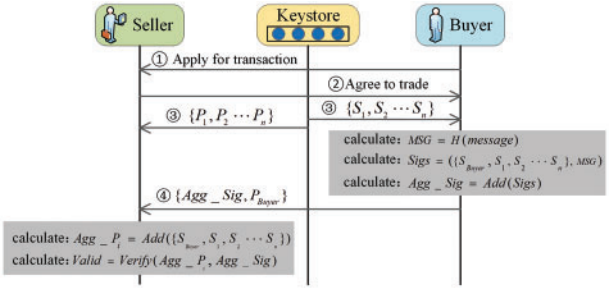

Figure 3: The process of multi-signature and verification

3.3.4 The CA Verifies the Transaction Information and Writes It into the Blockchain for Storage

At this stage, the CA obtains the key information from both parties involved in the transaction, as well as the key information from *ARRAY*, and the contents of the transaction processed using a hash function.

The CA then re-verifies all transaction information to ensure its accuracy and consistency. All transactions that have been confirmed by the CA are permanently recorded in the form of a block in the tamper-evident ledger, which provides a secure and transparent record of all energy transactions conducted within the system.

1) After the transaction is completed, the user sends the total transaction information *Trans* to the CA, which includes their public keys, the hash value of the transaction content, and the aggregated signature, $Trans = \{P_{Buyer}, P_{Seller}, MSG, Aggregate\_Signature\} \rightarrow CA$.

2) At the same time, the CA obtains the information of the public-private key pairs participating in this multi-signature from $ARRAY$.

3) The CA uses the total transaction information *Trans* and the public-private key pairs of neutral nodes to re-validate the transaction information. Since the key information of the neutral nodes is obtained directly from $ARRAY$, the accuracy of this part of the key information can be guaranteed. By verifying the correctness of the keys and transaction content provided by both parties, the CA can confirm the validity of the transaction and ensure that no malicious nodes are involved.

4) After the verification, due to the characteristics of the alliance blockchain, the CA can directly package this transaction information into a block without requiring verification from other user nodes. This block can be written directly into the blockchain for storage after being publicly announced. This process can precisely avoid the problem of slow traditional blockchain validation.

5) The structure of the packaged blockchain is shown in Fig. 4.

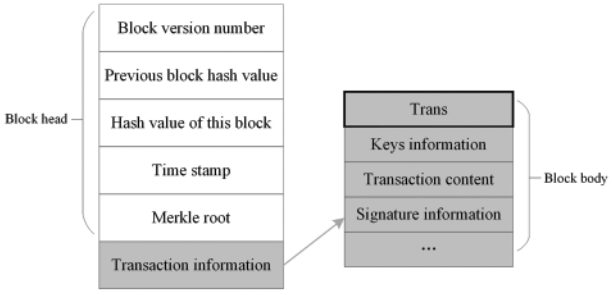

Figure 4: The structure of the packaged blockchain

4 Performance Analysis and Comparison

In this chapter, this paper will conduct an overall performance analysis of the proposed energy transaction scheme and compare it with other existing schemes, as shown in Table 2. Furthermore, this paper will perform a detailed operational efficiency analysis in Subsection 4.2.

Table 2: Overall performance comparison

	SG-SGEM [9]	CE-SDT [21]	PBT [29]	Raptor-LET [32]	Ours
Defend against imitation attacks	-	√	√	√	√
Defend against man-in-the-middle attacks	-	-	√	√	√
Defend against desynchronization attacks	√	-	-	-	√

(Continued)

Table 2 (continued)

	SG-SGEM [9]	CE-SDT [21]	PBT [29]	Raptor-LET [32]	Ours
Avoid single point of failure problem	-	√	√	√	√
Defending against complicit attacks	√	√	√	-	√

4.1 Overall Performance Analysis

By utilizing the security analysis tool Mythril from the Ethereum community, it is possible to detect security vulnerabilities in Solidity smart contracts and perform in-depth analysis. The main vulnerabilities that can be identified include integer overflow, timestamp dependency, and reentrancy attacks.

Therefore, in this experiment conducted in a Linux environment, the Mythril tool was deployed to analyze a Solidity-format multi-signature file. The result obtained was {"error": null, "issues": [], "success": True} and "The analysis was completed successfully. No issues were detected". Indicates that the contract does not have significant security vulnerabilities or logical errors.

In this section, this paper will conduct a performance analysis of the proposed solution on common issues and compare it with other existing solutions.

4.1.1 Defend against Imitation Attacks

Imitation attacks are typically carried out by stealing and disguising valid identity credentials to achieve unauthorized communication.

In the proposed energy transaction scheme, the communicating parties generate public-private key pairs through the CA, as well as the key information of the intermediate node. Moreover, the central node key invoked during the transaction is obtained randomly. During the transaction, the key information of the intermediate nodes in the keystore is also periodically updated. These measures make it difficult for malicious nodes to successfully imitate another entity during the transaction because its key information, which is aggregated with multiple randomly generated key information, will not match the valid key information of the actual entity.

4.1.2 Defend against Man-in-the-Middle Attacks

A Man-in-the-Middle (MitM) attack is an indirect intrusion attack in which the attacker can intercept, read, and modify the transmitted information without the knowledge of the communicating parties. MitM attacks are similar to replay attacks in that they use fraudulent methods, but in a MitM attack, the attacker defrauds both communicating parties.

In the proposed energy transaction scheme, both sides of the transaction verify the correctness of the received message by verifying the aggregated key information of the multi-signature and the hash value of the transmitted message. This process helps prevent Man-in-the-Middle attacks and ensures that the transaction is secure and tamper-proof.

4.1.3 Defend against Desynchronization Attacks

A de-synchronization attack is a type of attack in which an attacker blocks the transmission of messages between the two sides of a transaction, causing them to lose key synchronization and rendering them unable to communicate properly.

In the proposed energy transaction scheme, the session key used during a transaction is not dependent on the previous session key. Additionally, a different batch of intermediate nodes can be invoked to sign and verify each time a new transaction is created. These measures make it difficult to achieve a de-synchronization attack. Even if the transmitted message is blocked, a new session key can be constructed at the cost of re-running the transaction process. So, the proposed scheme is resilient to such attacks and ensures that communication between the parties is not disrupted.

4.1.4 Avoid Single Point of Failure Problem

The single point of failure problem occurs when a trusted third party that a system relies on is occupied or suffers a mechanical failure, causing the entire system to fail. Traditional authentication and key negotiation methods typically rely on trusted third parties, which can lead to a single point of failure.

To address this issue, the proposed energy transaction scheme uses an alliance blockchain, where the CA is composed of several large nodes or institutions. The CA is not directly involved in the specific transaction process, which ensures the freedom of node transactions while avoiding a single point of failure. This approach provides a high level of security and availability, as the system can continue to function even if one or more nodes fail or are compromised. Moreover, the decentralized nature of the alliance blockchain ensures that no single entity can control the system, further enhancing its resilience to attacks and failures.

4.1.5 Defending against Complicit Attacks

A conspiracy attack is an attempt by multiple participants to steal and tamper with transaction information through private conspiracy. It is commonly observed in systems that require multiple nodes to participate in the transaction process, such as ring signatures and multi-signature.

In the proposed energy transaction scheme, the intermediate nodes involved in multi-signature are generated in advance and their key information is updated periodically. This measure directly prevents the possibility of malicious nodes participating in the transaction and ensures the security and integrity of the transaction information. The use of pre-generated intermediate nodes also provides an additional layer of security, as the nodes can be verified and trusted by all parties involved in the transaction. This mitigates the risk of conspiracy attacks and ensures the trustworthy execution of the transaction process.

The specific comparison with the performance analysis of other existing schemes is shown in Table 2.

4.2 Operational Efficiency Analysis

In this section, this paper analyzes the performance of the proposed energy transaction scheme in terms of key computation time and operational efficiency.

To test the performance of the scheme, this paper uses a 64-bit operating system configured with an AMD Ryzen 7 CPU at 3.20 GHz and 16 GB RAM. Due to the limitations of actual user node hardware equipment in energy trading, as well as the involvement of a large number of nodes in this

scheme, this paper builds a simulation program using Python 3.8.0 to simulate the key information generation process and the specific process of multi-signature in transactions.

This paper simulates the scenario where different numbers of nodes participate in the multi-signature of the scheme and analyzes its operational efficiency to verify the feasibility and operation efficiency of the scheme.

In the key generation stage of the proposed energy transaction scheme, the BLS signature algorithm is used to generate public-private key pairs. Compared to other algorithms such as RSA and Schnorr, which are based on large number decomposition and discrete logarithm problems respectively, BLS using the BLS12-381 curve can generate key pairs more efficiently and with smaller key sizes.

In Fig. 5, the time spent by RSA, Schnorr, and BLS in generating different numbers of public-private key pairs is shown.

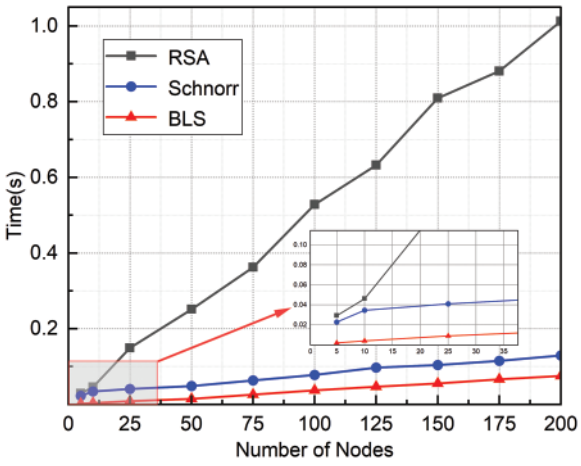

Figure 5: The time spent by RSA, Schnorr, and BLS

As shown in Fig. 5, the RSA algorithm requires a large number of operations, which makes it much slower in key generation compared to the Schnorr and BLS schemes. Both the Schnorr and BLS algorithms generate key information based on elliptic curves, but when comparing them, it is clear that the BLS algorithm takes less time than the Schnorr algorithm to generate the same number of keys. Overall, BLS is the most efficient algorithm in terms of key generation time, especially when a large number of key pairs need to be generated.

Fig. 6 illustrates the time taken for signature algorithms in blockchain applications concerning multi-signature and authentication. Due to the efficiency constraints of the RSA algorithm, the testing was simulated with the Schnorr and BLS algorithms for signature verification processes.

From Fig. 6, it is evident that these two algorithms, both utilizing elliptic curves, have a relatively small time difference. However, considering that the number of nodes involved in real-world scenarios is not very large, and the fact that the BLS algorithm generates smaller aggregate signatures for the same number of nodes. So, in this experiment, the BLS algorithm outperforms the Schnorr algorithm.

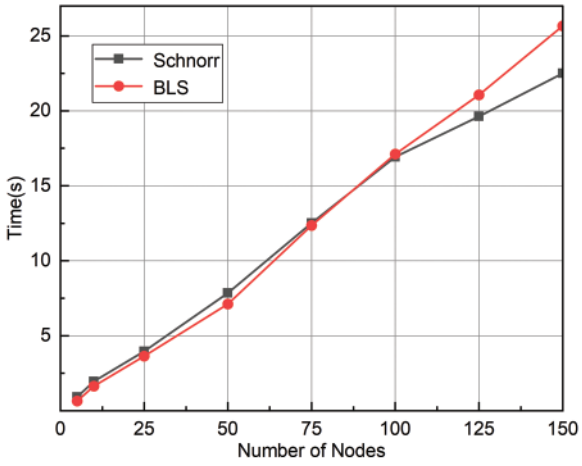

Figure 6: Comparison of signature verification time between Schnorr and BLS

The computational processes in Table 3 are required during user transactions, and the time spent on simulating individual key pairs for interaction is examined. Since the private key is a random number generated directly from the curve, no specific computation is involved, so the time T_{GS}, spent on generating the private key is almost negligible. The running time involving the data aggregation operation is the average of the number of nodes in the corresponding actual process. The specific data of the main computation processes are shown in Table 3.

Table 3: Time spent on each part of the calculation

Symbols	Operation of the representative	Calculation time
T_{GP}	Generate public key	0.0020 s
T_{Sig}	Signing of messages	0.10917 s
T_{AGGSIG}	Aggregate signatures	0.00735 s
T_{AGGP}	Aggregate public keys	0.00025 s
T_{VERIFY}	Verification of aggregated signatures	0.39271 s

The proposed energy transaction scheme places the key generation stage at the CA for operation and places the generated key information of the intermediate nodes in the keystore waiting to be invoked. This approach eliminates the call for key generation during the subsequent actual n-node multi-signature process, which can reduce the time of $nT_{GS} + nT_{GP}$ required for each transaction. As a result, only the time of $nT_{SIG} + nT_{AGGSIG} + nT_{AGGP} + T_{VERIFY}$ is needed in the subsequent actual n-node multi-signature process.

At the same time, another part of the time saved in the operation efficiency is the response time of the user node in the traditional multi-signature process. In this scheme, the user calls the corresponding number of key information from the keystore instead of interacting with other user nodes to obtain their key information, which is also the reason why the multi-signature will reduce the operation speed. In the simulation, the response time of the conventional user node to the key application is about 0.01–0.1 s, so the running time of this scheme is compared with that of the traditional multi-signature

scheme. When different numbers of nodes participate in multi-signature, the corresponding running time of the two schemes is shown in Fig. 7.

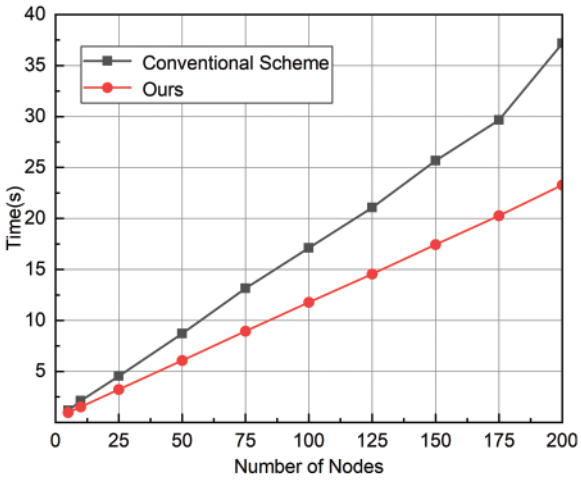

Figure 7: The corresponding running time of the two schemes

It can be seen from the comparison that this scheme is superior to the traditional multi-signature scheme in operation efficiency, especially when the number of user nodes participating in multi-signature transactions is increasing, this advantage in operation speed will be more obvious. Meanwhile, the simulation results demonstrate that the proposed scheme is efficient and feasible. The key computation time is within an acceptable range, and the operational efficiency of the scheme is high, even when a large number of nodes are involved in the transaction process.

5 Conclusion

To fortify data security and operational efficiency within the domain of distributed energy trading systems, this proposal introduces a multi-signature approach based on an alliance blockchain. This scheme devises a novel structure for multi-signature processes, enhancing reliability and operational speed during transactions.

1) In this scheme, trusted intermediate nodes generated by the CA, substitute the role of independent user nodes for multi-signature interactions. This method significantly reduces the communication overhead of user nodes involved in transactions. Simultaneously, the randomness of intermediate node generation and periodic updates by CA ensure the privacy of node keys.

2) Meanwhile, once a transaction is completed, it only needs to be verified by the master node in CA. If the transaction is confirmed to be correct, it can be uploaded to the blockchain for public disclosure and preservation. The advantages of the alliance blockchain over the completely decentralized traditional blockchain system are fully realized.

3) This proposed scheme undergoes meticulous simulation and in-depth analysis, thereby elucidating its intrinsic feasibility and compelling advantages. The reliability of the solution was evidenced through a security analysis of the smart contracts. Additionally, the efficiency of the solution was demonstrated through an analysis of the runtime during simulation experiments.

Evident through these evaluations is its superior competitive edge in addressing the intricacies of energy trading and multi-node challenges when juxtaposed against contemporary schemes.

Acknowledgement: The authors would like to express their gratitude to the members of the research group for their support.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Hongliang Tian; simulation, analysis, interpretation of results and draft manuscript preparation: Jiaming Wang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data not available due to the nature of this research, participants of this study did not agree for their data to be shared publicly, so supporting data is not available.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Afraz, F. Wilhelmi, H. Ahmadi and M. Ruffini, "Blockchain and smart contracts for telecommunications: Requirements *vs*. cost analysis," *IEEE Access*, vol. 11, pp. 95653–95666, 2023.

[2] S. Yao, M. Wang, Q. Qu, Z. Y. Zhang, Y. F. Zhang *et al.,* "Blockchain-empowered collaborative task offloading for cloud-edge-device computing," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3485–3500, 2022.

[3] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2964–2973, 2021.

[4] J. Zhou, G. Feng and Y. Wang, "Optimal deployment mechanism of blockchain in resource-constrained IoT systems," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8168–8177, 2022.

[5] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang *et al.,* "A lightweight and attack-proof bidirectional blockchain paradigm for Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371–4384, 2022.

[6] W. Wang, J. Chen, Y. Jiao, J. Kang, W. Dai *et al.,* "Connectivity-aware contract for incentivizing IoT devices in complex wireless blockchain," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10413–10425, 2023.

[7] L. H. Zhu, Y. M. Xie, Y. A. Zhou, Q. F, C. Zhang *et al.,* "Enabling efficient and secure health data sharing for Healthcare IoT systems," *Future Generation Computer Systems*, vol. 149, pp. 304–316, 2023.

[8] Y. Song, C. Sun, Y. Peng, Y. Zeng and B. Sun, "Research on multidimensional trust evaluation mechanism of fintech based on blockchain," *IEEE Access*, vol. 10, pp. 57025–57036, 2022.

[9] S. R. Etesami, W. Saad, N. B. Mandayam and H. V. Poor, "Stochastic games for the smart grid energy management with prospect prosumers," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2327–2342, 2018.

[10] H. Sun, S. Kitamura, D. Nikovski, K. Mori and H. Hashimoto, "Illegitimate trade detection for electricity energy markets Proceedings," in *2020 Int. Conf. on Smart Grids and Energy Systems*, Perth, Australia, pp. 338–343, 2020.

[11] U. G. K. Mulleriyawage and W. X. Shen, "Impact of demand side management on Peer-to-Peer energy trading in a DC microgrid," in *Proc. of 2021 31st Australasian Universities Power Engineering Conf.*, Perth, Australia, pp. 1–6, 2021.

[12] X. Y. Shen, B. H. Luo, S. J. Chen, Z. Yan, J. Ping *et al.,* "An evaluation method and empirical analysis of energy blockchain consensus algorithms: A case study of distributed energy trading," *Zhongguo Dianji Gongcheng Xuebao*, vol. 42, no. 14, pp. 5113–5125, 2022 (In Chinese).

[13] C. Liu, X. W. Xia, Y. Yan, J. W. Ma and F. Qi, "Research on distributed energy trading mode and mechanism based on blockchain," in *Signal and Information Processing, Networking and Computers*, pp. 345–350, 2022.
[14] Z. Y. Shen, S. J. Chen, Z. Yan, J. Ping, B. H. Luo *et al.,* "Distributed energy trading technology based on blockchain," *Zhongguo Dianji Gongcheng Xuebao/Proc. of the Chinese Society of Electrical Engineering*, vol. 41, no. 11, pp. 3841–3850, 2021 (In Chinese).
[15] S. Y. Yu, J. Peng, A. L. Chen, S. C. Yang and Y. P. Li, "Based on blockchain to construct distributed energy trading," in *2021 Int. Conf. on Power System Technology: Carbon Neutrality and New Type of Power System*, Haikou, China, pp. 2112–2117, 2021.
[16] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[17] L. Harn and T. Kiesler, "New scheme for digital multi-signatures," *Electronics Letters*, vol. 25, no. 15, pp. 1002–1003, 1989.
[18] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.
[19] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing," in *Int. Conf. on the Theory and Application of Cryptology and Information Security*, Berlin, Heidelberg, Springer, pp. 514–532, 2001.
[20] X. Li, J. Cheng, Z. Shi, J. Liu, B. Zhang *et al.,* "Blockchain security threats and collaborative defense: A literature review," *Computers, Materials & Continua*, vol. 76, no. 3, pp. 2597–2629, 2023.
[21] W. Cai and J. Qu, "Systematic research on information security based on blockchain technology," in *2022 Int. Conf. on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, pp. 900–903, 2022.
[22] Y. Park, M. H. Jeon and S. U. Shin, "Blockchain-based secure and fair IoT data trading system with bilateral authorization," *Computers, Materials & Continua*, vol. 76, no. 2, pp. 1871–1890, 2023.
[23] J. Dafda, S. Patil and K. Parmar, "Decentralized energy trading model with smart grids and blockchain," in *INDICON, 2022–2022 IEEE 19th India Council Int. Conf.*, Kochi, India, 2022.
[24] B. Z. Wang, J. F. Xu, C. L. P. Chen, J. Y. Wang, N. X. Wang *et al.,* "CE-SDT: A new blockchain-based distributed community energy trading mechanism," *Frontiers in Energy Research*, vol. 10, pp. 1091350–1091359, 2023.
[25] Z. Che, Y. Wang, J. J. Zhao, Y. Qiang, Y. Ma *et al.,* "A distributed energy trading authentication mechanism based on a consortium blockchain," *Energies*, vol. 12, no. 15, pp. 2878–2898, 2019.
[26] Y. C. Feng, J. Fan, J. L. Wang and Y. C. Li, "Peer-to-peer energy trading platform using consortium blockchain," in *Asia-Pacific Power and Energy Engineering Conf., APPEEC*, Nanjing, China, 2020.
[27] D. Huang, C. Y. Zhang, Q. Li, H. C. Han, D. W. Huang *et al.,* "Consortium blockchain-based decentralized energy trading mechanism for virtual power plant," in *2020 IEEE 4th Conf. on Energy Internet and Energy System Integration: Connecting the Grids Towards a Low-Carbon High-Efficiency Energy System(EI2)*, Wuhan, China, pp. 3084–3089, 2020.
[28] P. T. Makhsoos, B. Bahrak and F. Taghiyareh, "Designing a high performance and high-profit P2P energy trading system using a consortium blockchain network," in *2022 12th Int. Conf. on Computer and Knowledge Engineering*, Mashhad, Iran, pp. 458–464, 2022.
[29] Y. N. Jiang, K. L. Zhou, X. H. Lu and S. L. Yang, "Electricity trading pricing among prosumers with game theory-based model in energy blockchain environment," *Applied Energy*, vol. 271, pp. 115239–115254, 2020.
[30] J. Y. Dong, C. H. Song, S. Liu, H. H. Yin, H. Zheng *et al.,* "Decentralized peer-to-peer energy trading strategy in energy blockchain environment: A game-theoretic approach," *Applied Energy*, vol. 325, pp. 119852–119868, 2022.
[31] Y. L. Chen, Y. F. Li, Q. Chen, X. M. Wang, T. Li *et al.,* "Energy trading scheme based on consortium blockchain and game theory," *Computer Standards and Interfaces*, vol. 84, pp. 103699–103710, 2023.
[32] K. K. Gai, Y. L. Wu, L. H. Zhu, M. K. Qiu and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.

[33] Y. F. Li, Y. L. Chen, T. Li and X. J. Ren, "A regulatable data privacy protection scheme for energy transactions based on consortium blockchain," *Security and Communication Networks*, vol. 2021, pp. 1–11, 2021.

[34] C. Zhang, M. Y. Zhao, L. H. Zhu, W. T. Zhang, T. Wu *et al.,* "FRUIT: A blockchain-based efficient and privacy-preserving quality-aware incentive scheme," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3343–3357, 2022.

[35] Z. L. Jiang, Y. J. Pan, M. S. Fan, L. Yao, Y. Liu *et al.,* "Local energy trading platform based on privacy-preserving blockchain with linkable ring signature," in *2022 4th Int. Conf. on Data Intelligence and Security*, Shenzhen, China, pp. 134–141, 2022.

[36] S. M. Pan, K. Y. Chan, H. D. Cui and T. H. Yuen, "Multi-signatures for ECDSA and its applications in blockchain," in *Information Security and Privacy*, Springer, Cham, pp. 265–285, 2022.

[37] Y. N. Cao, Y. J. Wang, Y. Ding, Z. W. Guo, Q. H. Wu *et al.,* "Blockchain-empowered security and privacy protection technologies for smart grid," *Computer Standards and Interfaces*, vol. 85, pp. 103708–103726, 2023.