IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Blockchain-based REC System for Improving the Aspects of Procedural Complexity and Cyber Security

Yeonouk Chu[1], Sungjoong Kim[1], Youngkook Song[1], Yongtae Yoon[1], and Younggyu Jin[2,*]

[1]Electric Power Network and Economics Laboratory, Department of Electrical and Computer Engineering, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul 08826, Korea

[2]Department of Electrical Engineering, Jeju National University, 102 Jejudaehak-ro, Jeju-si 63243, Korea

Corresponding author: Younggyu Jin (e-mail: ygjin93@jejunu.ac.kr).

ABSTRACT In response to global efforts to deal with climate change, various renewable energy policies are being implemented. Among these, renewable portfolio standards (RPS) and renewable energy 100 (RE100) regulate the obligated supply of renewable energy to ensure compliance with set quotas by nations and institutions. In this context, the renewable energy certificate (REC) system is employed to assist obligated entities in meeting their renewable energy generation quotas. Obligated entities can purchase REC from renewable energy generators to obtain recognition for their renewable energy allocation. However, the current REC system is insufficient in addressing issues related to procedural complexity and cyber security. This study aims to overcome its limitations by applying the blockchain technology. Blockchain, a distributed financial network, serves as a digital ledger, enabling peer-to-peer transactions in a simple, transparent, and secure way. The proposed new REC system based on blockchain moves away from the complex structure of the traditional REC system, simplifying the system into four processes: participation, issuance, transaction, and authentication. Moreover, by applying blockchain algorithms, it addresses the cyber security issues of the traditional system. The case study using Hyperledger Besu, or one of blockchain platforms, demonstrates that the aspects of procedural complexity and cyber security are improved in the proposed system.

INDEX TERMS Renewable Energy Generation, REC, RPS, RE100, Blockchain, Smart Contract

I. INTRODUCTION

The proportion of renewable energy generation is increasing worldwide in response to the issues of climate change. With the adoption of the Paris Agreement in 2015, a universal framework was established to enable participation in climate action, considering the economic situation of each country [1, 2]. As a result, governments and private organizations in various countries have been implementing renewable energy policies. Representative renewable energy policies implemented by the government include renewable portfolio standards (RPS) and feed-in tariffs (FiT), while renewable energy campaigns conducted by a private organization include RE100.

RPS and RE100 are policies that obligate power generation companies and normal companies to achieve a certain proportion of renewable energy generation [3]. The mandatory share of renewable energy supply in both policies has increased every year. However, the construction of renewable energy resources typically takes more than a year, limiting companies' ability to catch up with the policy target. Also, the financial burden coming from the integration to complement the intermittent nature of renewable energy sources discourages companies from meeting the obligation [4]. Therefore, various institutions employ renewable energy certificate (REC) systems to fulfill the obligated amounts of renewable energy generation. RECs are tradable documents that prove the production of electricity through renewable energy sources. Companies required to meet the obligated supply in the RPS or RE100 can assert their renewable energy generation by purchasing RECs from renewable energy generation companies.

However, the current REC system has limitations in terms of procedural complexity and cyber security. At first, the procedure is complex because various entities such as issuers, brokers, aggregators, system operators (SOs), market operators (MOs), and power exchanges (PX) are involved in the issuance and trading of the RECs. As the number of intermediary entities increases, the transaction system becomes more complex, resulting in a considerable amount of time being required for the issuance and trade of RECs.

In addition, the current REC system lacks considerations from the perspective of cyber security. For example, various countries use weight schemes in the REC system, if an offender manipulates the weight of the REC, unfair additional benefits can be taken to the manipulator. In the existing studies on REC systems, there has not been much research on cyber security, such as the manipulation of REC contents. Therefore, measures to reinforce the security of the REC system should be prepared.

Meanwhile, blockchain refers to a mechanism for data integrity and tamper-proofing based on distributed computing technology Blockchain is essential for implementing decentralized financial systems [5]. In an ideal blockchain system, nodes with equal authority form a network, and transactions are conducted in a peer-to-peer (P2P) manner. Transactions, which are details of completed dealing, should all be recorded in blocks that serve as books for safe trading. Completed transactions construct blocks, and it is referred to as the blockchain if blocks are connected in a chain-like structure. Once recorded in the blockchain, the content cannot be modified by any participant in the network. The expected benefits of applying blockchain technology to a conventional REC system include strong security achieved through consensus algorithms and hash functions without the need for a central node. Also, the ability for anyone to access data by storing transaction data in a distributed storage environment is another advantage.

Blockchain technology can be categorized into two types based on the level of content visibility; public blockchain and private blockchain [6]. Public blockchain allows anyone to participate and form transactions on the network. All nodes participating in the network can verify the content recorded in transactions. On the other hand, in the private blockchain system, only nodes authorized by an authority can participate in the network.

Several studies have been conducted to overcome the limitations of the REC system, taking advantage of blockchain technology, which offers various benefits from different perspectives. Zuo utilized the blockchain simulation program MultiChain to simulate a series of processes, including REC issuance, transactions, and renewable energy generation confirmation [7]. Wang et al. applied the PBFT consensus algorithm of blockchain to the REC trading system, conducting simulations for REC purchases and sales [8]. Castellanos et al. implemented a certificate trading market with MO on the Ethereum network using smart contracts [9]. However, these studies have some limitations. In Zuo's research, the simulation included only one node for REC buyers and sellers in the scenario, making it impossible to handle the issuance and transactions of various types of REC. Wang et al.'s simulation assumed that all REC products are of the same type, neglecting the consideration of REC characteristics with different weights based on the type of renewable energy. Castellanos et al.'s proposed blockchain REC market primarily focuses on REC transactions and lacks adequate consideration of issuance and renewable energy certification aspects.

Therefore, in this study, we aim to address the previously mentioned issues of procedural complexity and cybersecurity within the REC system by applying blockchain technology. Additionally, we seek to incorporate the aspects that previous research overlooked. The contributions of this study, based on improvements to the existing REC system and prior research, are as follows:

- The limitations of existing REC systems are defined in two aspects: procedural complexity and cyber security.
- A new system is proposed, which simplifies the complex nature of the existing REC system by applying blockchain technology, thereby reducing the involvement of multiple intermediary entities.
- It is shown that the cyber security of the REC system can be relieved through the use of blockchain techniques.
- The simulation in the REC ecosystem with blockchain technology is conducted, considering many REC sellers and buyers, enabling transactions of diverse types of REC.
- The REC system incorporates blockchain technology to simulate the entire process, from issuance to transactions and renewable energy generation certification, utilizing the Hyperledger Besu program.
- We simulate the weighting system based on the power source in the recognition process of renewable energy generation for the new REC system incorporating blockchain technology.

The paper is structured as follows. In Section 2, we review previous studies that have applied blockchain to renewable energy certificate systems and electricity trading. Section 3 explains the limitations of the existing REC system. Section 4 provides an explanation of the new REC system we propose, while Section 5 presents a detailed case study. Section 6 discusses the significance and provides a discussion of the paper. The results are presented in Section 7.

II. LITERATURE REVIEW

The application of blockchain technology to the power system has been a widely discussed topic in previous research. Cheng et al. identified the high costs and difficulties in data processing associated with the construction, management, and maintenance of traditional centralized solutions in the distribution market [10]. To address these issues, they proposed a new transaction framework using blockchain technology. Wörner et al. discussed the advantages of distributed energy resources (DERs) in terms of their environmental impact and resiliency, considering the growing trend of DER integration. They further highlighted the limitations of the centralized operation of DERs and emphasized the application of distributed systems like blockchain [11].

various models applying blockchain technology to the electricity market have been analyzed and proposed in [12-14]. Various mechanisms utilizing blockchain technology have also been developed in studies related to microgrid operation [15-19]. In these studies, blockchain technology is employed to enhance the security of microgrids and to modernize existing systems by leveraging the unique features of blockchain, such as transparency, security, and rapidity. Furthermore, concerning the active discussions on flexibility market operations in many countries, research is underway to explore ways to activate P2P transactions among market participants by applying blockchain technology [20-23].

The aforementioned studies have explored the application of blockchain technology to the power system but did not specifically address the REC system associated with it. Although there have been some studies on applying blockchain technology to the REC system, they are limited in number meaning that this topic is at the early stage.

Zuo conducted research on REC issued as non-fungible tokens (NFTs) based on Ethereum private blockchain [7]. The blockchain-based REC ecosystem was established by granting authorities to central nodes such as the Authority and Registry. The ecosystem was modeled in a Multichain environment, and simulations of issuance and transactions between nodes were conducted. However, the model and simulation only included one node for renewable energy generators and one node for REC buyers, which limited the consideration of diverse transactions. Furthermore, the concentration of authority in the central nodes, such as Authority and Registry raises concerns about the true utilization of a distributed ledger system.

Cali et al. present a structural framework for a system that applies blockchain technology to the REC system [24]. The system is structured in a multi-layered approach, with each layer serving a specific role as follows:

- Layer 1: Autonomous DER Generation and Storage
- Layer 2: DER Energy Management
- Layer 3: DER Information and Communication Technology
- Layer 4: DER Operation Analysis
- Layer 5: Transmission Operations

Cali et al. examine the security advantages of applying blockchain technology to the REC system using the multi-layered system structure [24]. However, a limitation of this study is the lack of consideration for transactions between nodes using the proposed model.

Wang et al. and Castellanos et al. discussed REC systems applying blockchain technology from a market perspective. Wang et al. presented a model that mathematically represents decision-making by nodes and demonstrated through transaction simulations that certificates are determined at appropriate market prices [8]. Unlike previous research, multiple buyers and sellers were included in the simulations. However, this study focuses solely on the market and transaction aspects, and lacks an examination of the overall ecosystem of REC, from issuance to retirement. Castellanos et al. researched implementing the role of a market operator using smart contracts in the existing supply certificate market [9]. The model included various market participants in addition to multiple sellers and buyers, and simulations were performed considering various consensus algorithms. However, a limitation was the lack of consideration for proof of authority, which could simplify transactions.

Ashley and Johnson [25], as well as Zhang et al. [26], proposed renewable energy certificate systems incorporating blockchain and conducted studies describing the advantages of these systems. Ashley and Johnson highlighted the inefficiencies of the current system and emphasized the economic and security benefits, in terms of time, cost, and enhanced security, resulting from the application of blockchain technology [25]. Zhang et al. divided the system's structure into five layers: data layer, network layer, consensus layer, incentive layer, and contract layer [26]. They described the advantages of blockchain systems in terms of security aspects such as immutability, traceability, and transparency. Furthermore, they provided a conceptual framework for the system's implementation. However, both studies lacked simulation processes.

This study meets the needs of the limitations mentioned in previous studies. First, the REC system with blockchain should be designed following sufficient discussions on decentralization and simplicity of the system. Second, simulations should be conducted for the system model with an adequate number of nodes. Lastly, the overall ecosystem of the REC system should be comprehensively described, including its components and interactions.

III. LIMITATIONS OF THE EXISTING REC SYSTEM

A. PROCEDURAL COMPLEXITY

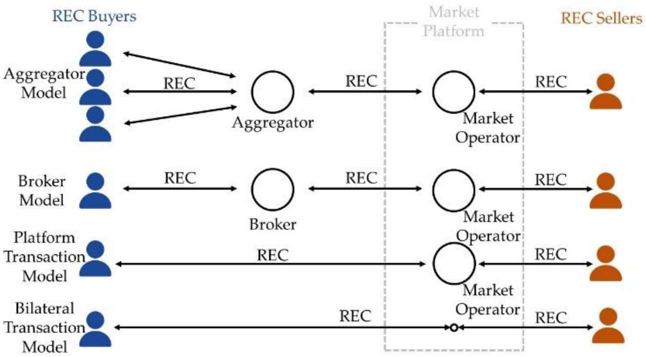

FIGURE 1. Various transaction models utilized in the current REC system.

The existing REC system exhibits procedural complexity in three aspects: transaction formats, the number of participants, and the lengthy transaction processes. Firstly, REC buyers and sellers can engage in various transaction formats depending on the trading model and duration. Various models are illustrated in Figure 1.

Secondly, besides buyers and sellers, diverse mediators participate in REC transactions. Aggregators and brokers assist buyers in REC purchases, while entities like the distribution system operator (DSO) manage grid congestion, the balance responsible party (BRP) intervenes in grid balance, and members of the market platform, such as the MO, PX, and settlement parties, act as intermediaries in the transactions. The involvement of multiple stakeholders in transactions may result in higher fees that the trading parties have to bear, leading to unnecessary costs.

Lastly, REC transactions entail long transaction processes involving various stakeholders, leading to intricate settlement procedures and extended transaction times. Globally, a multitude of REC systems exists. Most of all, a simplified representation of the typical process for REC issuance and trading within the conventional REC system is illustrated in Figure 2. In Figure 2, the content on the left side of the dotted line represents the process of issuing RECs to the renewable energy generation company (RE GenCo). On the right side, the content describes the process of REC trading between the seller and the buyer. RE GenCo can obtain REC by establishing a new renewable energy facility, subject to approval from the central institution issuing the REC. Upon receiving REC, RE GenCo becomes the REC seller and sells REC to REC Buyers with the assistance of MO. When RE GenCo and REC Buyer agree to a transaction, RE GenCo transfers ownership of REC, and REC Buyer makes the corresponding payment. Participants in the transaction settle by paying fees to MO.

Despite the outlined streamlining of procedures, the issuance of REC certificates necessitates multiple verification steps and interactions among participants. Moreover, since each step is carried out individually, a considerable amount of time is consumed. To manage these problems, institutions seeking participation in the REC system should have a high degree of expertise and human resources. Therefore, given the protracted duration of issuance, there arises a need for time-efficient REC procurement strategies.

The combination of these three factors contributing to procedural complexity can raise entry barriers for potential participants in REC transactions. Therefore, there is a need for a new REC system with a simplified procedure.

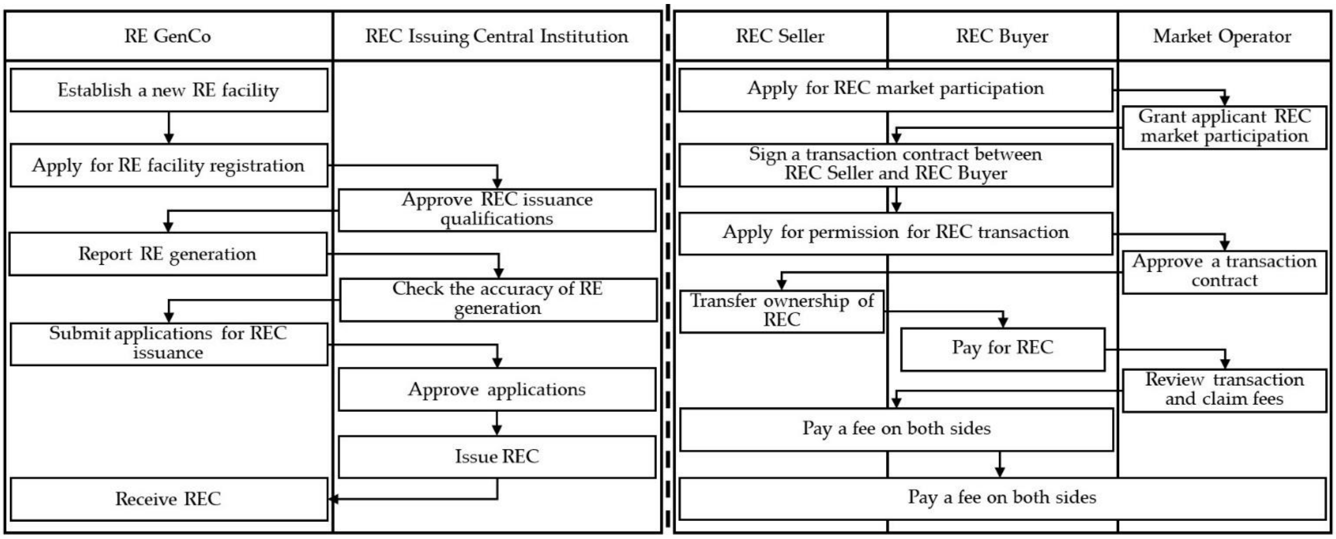
RE GenCo
REC Issuing Central Institution
REC Seller
REC Buyer
Market Operator
Establish a new RE facility
Apply for RE facility registration
Approve REC issuance qualifications
Report RE generation
Check the accuracy of RE generation
Submit applications for REC issuance
Approve applications
Issue REC
Receive REC
Apply for REC market participation
Grant applicant REC market participation
Sign a transaction contract between REC Seller and REC Buyer
Apply for permission for REC transaction
Approve a transaction contract
Transfer ownership of REC
Pay for REC
Review transaction and claim fees
Pay a fee on both sides
Pay a fee on both sides

FIGURE 2. The typical issuance and transaction process of the existing REC system.

B. CYBER SECURITY

Security issues in the existing system can be addressed in terms of information omission by intermediaries and potential counterfeiting by transaction participants. Firstly, since various entities participate in REC transactions, there is a risk of missing information during the data transmission process. When information is missing, it becomes difficult to identify the exact point of manipulation or omission in the complex intermediary processes. Moreover, the allocation of responsibility for the issue becomes unclear, leading to complicated procedures for punishment and compensation.

On the other side, there are security vulnerabilities where transaction participants may engage in intentional misconduct for personal gain. REC traders could create forged RECs to gain unfair profits, and on a more sophisticated level, they might manipulate the content of RECs. For instance, they could modify the recorded type of renewable energy source in the REC to receive greater weights than those deserved from actual renewable energy generation. To establish a highly reliable REC system, security vulnerabilities in recording electronic documents need to be addressed.

IV. STRUCTURE OF THE NEW REC SYSTEM USING PRIVATE BLOCKCHAIN

A. BASIC STRUCTURE OF THE NEW REC SYSTEM

The proposed new REC system using private blockchain adopts a significantly simplified structure for the current REC system, utilizing blockchain technology and smart contracts. A smart contract entails the programming of agreed-upon conditions and content between contract parties, recorded as electronic documents. Upon the fulfillment of conditions specified within the smart contract, the agreed-upon actions are executed automatically. Smart contracts enable the blockchain system to possess diverse functionalities. Once deployed within the blockchain system, a smart contract cannot be altered by anyone. The process of REC issuance and transaction is illustrated in Figure 3.

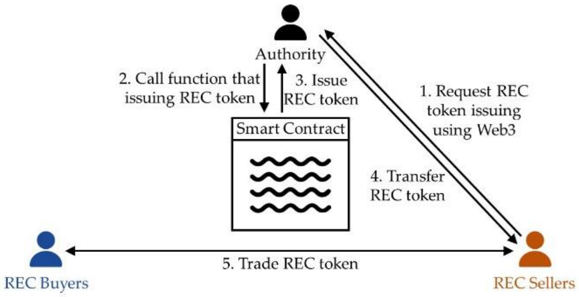

FIGURE 3. The approximate structure of REC issuance and transactions in the proposed system, where blockchain and smart contract technologies are applied to the existing REC system.

REC sellers represent renewable energy generators, while REC buyers typically correspond to obligated entities. In the first step, REC sellers generate renewable energy and communicate this information to the DSO. Subsequently, the DSO verifies the generation details, and if they are authentic, invokes the REC issuance function recorded in the smart contract. Based on the information, REC is issued to the REC seller, and transactions with REC buyers can be conducted.

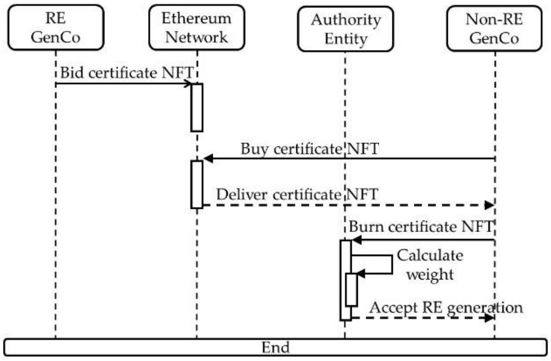

FIGURE 4. The detailed process of REC transactions occurring in the proposed system.

The transaction process is illustrated in Figure 4. Initially, both REC buyers and sellers submit bids on the Ethereum network, offering the quantity and price of REC they desire. If the settlement price is reasonable for both parties, the transaction proceeds. After settlement, the seller’s REC is automatically transferred to the buyer, concluding the transaction process.

After the transaction, a process of burning the purchased REC is required for the buyer to receive recognition for their renewable energy obligation. The buyer submits the REC to the DSO for burning, and the DSO calculates the weightage based on the REC’s content. The DSO multiplies the weightage by the number of submitted RECs to determine the amount of energy generated, recognized as MWh for the corresponding obligation.

B. THE OPERATING METHOD OF THE NEW REC SYSTEM

The New REC system is a system that applies a private blockchain to the existing REC framework. In the context of a private blockchain, there exists an Authority node within the system, and obtaining permission from the authority node is important for participation in the network. In the New REC system, the role of the Authority node is fulfilled by the DSO. The DSO not only grants permission for other participants to join the network but also provides and manages the functionalities accessible to nodes participating in the network. General participants, upon receiving permission from the DSO, can participate in the network as regular nodes. Regular nodes can be further categorized as REC seller nodes and REC buyer nodes. REC seller nodes represent users who possess renewable energy generation resources. By generating renewable energy, they can receive REC issuance and subsequently sell them for profit. REC buyer nodes correspond to entities such as energy companies or businesses. They purchase RECs from REC seller nodes to fulfill their renewable energy obligation quotas.

The interaction among DSO, REC seller nodes, and REC buyer nodes can be divided into four aspects: participation, issuance, transaction, and authentication. Detailed explanations for each aspect can be found in the sub-subsection below.

1) PARTICIPATION

To establish the network's configuration, a process of entities participating in the Ethereum network is necessary. The process of participation is illustrated in Figure 5. Initially, those seeking participation authority must transmit their node information to the DSO. Then the DSO, upon verifying the information of the node, needs to assess the suitability of the aspiring participant. If the applicant intends to join as a REC seller node, the DSO must examine whether it includes eligible renewable energy sources for REC issuance. Likewise, if the applicant wants to join as a REC buyer node, the DSO should confirm the purpose of the REC purchase and assess if the participant is not engaging in any malicious activities. If the entity applying for participation meets the DSO's criteria for network entry, the DSO grants authorization for the node to participate in the network. Users whose participation has been confirmed are assigned public and private keys, enabling them to join the network as either seller or buyer nodes. The public key functions as the node's account number and is visible to all network users. The private key acts as the account's password and is known only to the owner, not disclosed to all nodes, including the DSO.

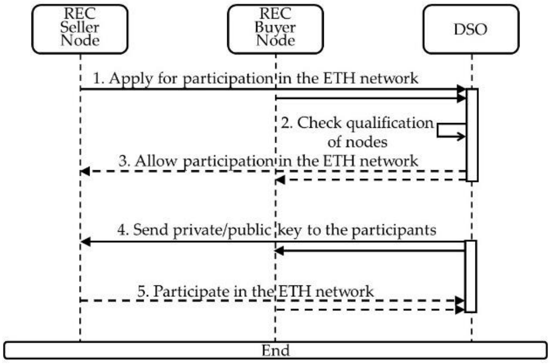
REC Seller Node
REC Buyer Node
DSO
1. Apply for participation in the ETH network
2. Check qualification of nodes
3. Allow participation in the ETH network
4. Send private/public key to the participants
5. Participate in the ETH network
End

FIGURE 5.The process by which regular nodes obtain permission from the DSO to participate in the Ethereum network and receive their public and private keys.

2) ISSUANCE

Once an appropriate number of nodes participate in the REC network, a system of interactions between nodes utilizing the system's functionalities needs to be established. Within the Ethereum network, the system's functionalities can be devised through smart contracts.

In the New REC system, the DSO generates and deploys smart contracts onto the blockchain network. The smart contract in this system includes three functionalities: Minting, REC Token ID assignment, and REC Token information recording. The Minting functionality utilizes ERC721, used for issuing NFTs, to issue REC tokens. REC Token ID assignment serves the purpose of distinguishing REC tokens by allocating an incremental ID to each token in sequential order of issuance. Thus, the ID of the most recently issued REC token corresponds to the total number of REC tokens issued up to that point. The functionality that records information on the REC token facilitates the recording of necessary information onto the REC token.

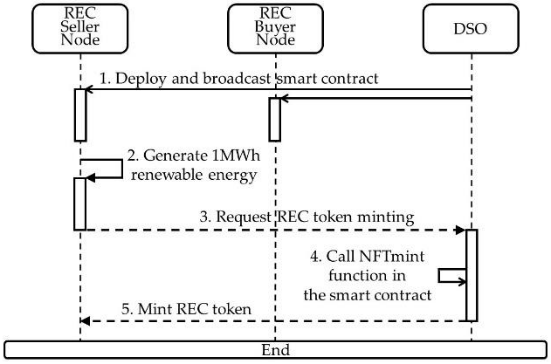
REC Seller Node
REC Buyer Node
DSO
1. Deploy and broadcast smart contract
2. Generate 1MWh renewable energy
3. Request REC token minting
4. Call NFTmint function in the smart contract
5. Mint REC token
End

FIGURE 6. The process where the DSO deploys a smart contract onto the network, and REC Seller nodes receive REC tokens.

The process of issuing REC to users can be understood from the Figure 6. Initially, the DSO drafts and deploys a smart contract onto the network. This smart contract is distributed throughout the network, and its contents can be verified by all system users. Regular nodes seeking to utilize functionalities recorded within the smart contract can invoke functional actions through the DSO. Upon generating 1MWh of renewable energy, the REC seller node can request the issuance of one REC from the DSO. The DSO assesses the validity of the request received from the REC seller node and can request the mint function within the smart contract to issue REC. The issued REC is then conveyed to the REC seller node, concluding the process of REC issuance.

3) TRANSACTION

The issued RECs can be transferred to the respective REC buyer nodes through transactions. The process of transaction is illustrated in Figure 7. Both buyer and seller nodes have the option to set a price and place bids for buying or selling REC. If the proposed REC price is reasonable for both parties, the settlement process is undertaken to determine the price. The settlement price, inclusive of fees, is conveyed to both nodes and if both nodes agree on this price, the transaction price is established. Both the buyer and seller nodes pay fees to the Ethereum network, and upon the buyer node transferring the agreed-upon amount to the seller node, the ownership of the REC is transferred to the buyer node. By utilizing the purchased RECs, the REC buyer node becomes eligible for recognizing renewable energy generation.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3370687

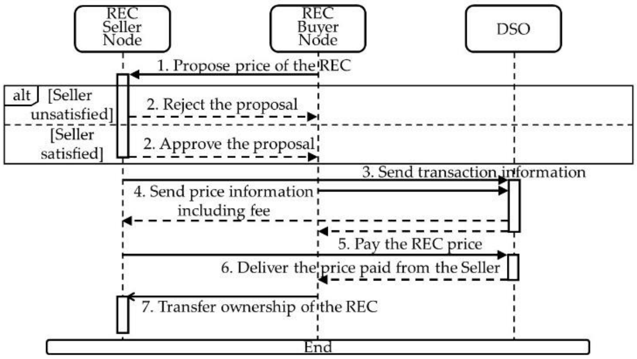
REC Seller Node
REC Buyer Node
DSO
1. Propose price of the REC
alt
[Seller unsatisfied]
2. Reject the proposal
[Seller satisfied]
2. Approve the proposal
3. Send transaction information
4. Send price information including fee
5. Pay the REC price
6. Deliver the price paid from the Seller
7. Transfer ownership of the REC
End

FIGURE 7. **The process of REC transactions between REC seller nodes and REC buyer nodes.**

4) AUTHENTICATION

Lastly, a process is required for the REC buyer node to validate renewable energy generation using the purchased RECs. This process is illustrated in Figure 8. In the context of the blockchain system, "burning" refers to sending tokens to a single node with an unknown private key. Since no node knows the private key of the burning node, tokens sent to that node cannot be utilized by anyone.

In the process of recognizing renewable energy, a calculation of weights is also necessary. Presently, many countries employ a weighted system for different types of renewable energy sources. These sources vary in terms of efficiency, environmental impact, and equipment costs. By utilizing the weight system of RECs, it's possible to encourage the utilization of specific renewable energy sources, thereby promoting effective facilities for combating climate change.

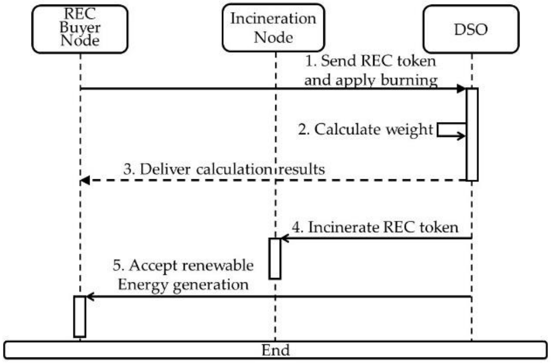
REC Buyer Node
Incineration Node
DSO
1. Send REC token and apply burning
2. Calculate weight
3. Deliver calculation results
4. Incinerate REC token
5. Accept renewable Energy generation
End

FIGURE 8. **The process by which REC buyer nodes, who have purchased RECs, undergo weight calculation and obtain recognition for renewable energy generation, including weight calculation.**

Within this system, the authority for burning and weight calculation lies solely with the DSO. The first step of the authentication process begins when a REC buyer node desiring to burn their REC sends the REC to the DSO and requests burning. The DSO verifies the renewable energy source of the received REC and calculates the weight. The calculation result is then communicated back to the REC buyer node, and the REC is burned. Upon verification of the burnt REC, the DSO recognizes the weight as the corresponding amount of renewable energy generation achieved by the REC buyer node.

V. CASE STUDY

In this section, following the qualitative analysis of overcoming the limitations of the existing system in subsection 4.C, a quantitative analysis using simulations is conducted. The simulation environment was set up on Linux version 22.04, and the blockchain simulator employed was Hyperledger Besu. Hyperledger Besu supports both public and private blockchains. For this simulation, a private blockchain was utilized, employing the proof-of-authority (PoA) consensus algorithm commonly used in private blockchain systems.

Firstly, by simulating the streamlined processes of participation, issuance, and transaction explained in subsection 4.B, the improvement in the procedural complexity is demonstrated by showing that the existing procedure can be replaced by simplified steps. Next, the implementation of scenarios involving fraudulent REC issuance and manipulation of REC contents demonstrates enhanced security compared to the conventional system.

A. SYSTEM SIMULATION FOR RESOLUTION OF PROCEDURAL COMPLEXITY

Through simulating the configuration of the network, node participation, issuance of REC tokens, and the process of REC sale, it is possible to verify how much the procedures have been streamlined in the existing system. The network configuration starts with the creation of DSO nodes. Based on the DSO node, regular nodes can be generated. In this simulation, a total of 7 general nodes were created, including 3 REC seller nodes, 3 REC buyer nodes, and 1 incineration node. Once the generation of nodes constituting the Ethereum network is completed, each node receives private and public keys. Participating nodes can engage in financial activities on the network using these keys.

Next, the process of issuing REC tokens was simulated. The compiled smart contract is deployed to the Ethereum network by the DSO node after which addresses are generated for each deployed smart contract. These addresses are utilized to invoke functions within the smart contract for usage. The addresses of the deployed smart contracts can be found in Table 1.

TABLE 1. **The smart contract addresses responsible for issuing REC tokens for each Seller node.**

	Contract Address
Seller1	0xef963F8C31a801E0776b631Ce972A017cF3EAe31
Seller2	0x54CE388bBb81883af06bf4E4F05a641abF8dFf64
Seller3	0x8872955A58E9820f59872185aA182FEC6Baaa6E3

Information about what to input in the REC tokens using the tokenURI function is available in JSON language. The contents to be entered into the REC tokens issued by REC sellers 1, 2, and 3 can be seen in Table 2. After the issuance of REC tokens by the DSO node is completed, they are transferred to the respective REC sellers, concluding the process of REC token issuance.

TABLE 2. The information recorded in each REC token issued by REC seller nodes.

RE Owner	Seller 1	Seller 2	Seller 3
Location	Seoul	Daegu	Gwangju
Installation Year	2018	2018	2016
RE type	PV	WT	Hydroelectric
Installation Type	Existing Facility	General Site	Existing Facility
Facility Capacity	2000kW	3000kW	7000kW
ESS Connection	No	Yes	No
Minter Address	DSO	DSO	DSO

In this simulation, it is assumed that all seller nodes have generated 3MWh of electricity each. Upon receiving requests from sellers, the DSO node calls smart contracts for each seller, resulting in the issuance of three REC tokens per seller node. Once issued by the DSO, the information of tokens is verified for accuracy and then forwarded to the suitable seller nodes. Each token can be distinguished based on the renewable energy generator and its token ID.

Once a buyer interested in purchasing REC emerges, the process of negotiation and transaction follows. Figure 9 illustrates the inter-node transactions within an Ethereum network configured using the Hyperledger Besu program. Seller 1 trades REC tokens 1 and 3 with Buyer 1 and 2 respectively, Seller 2 exchanges REC token 2 with Buyer 2, and Seller 3 transacts REC tokens 2 and 3 with Buyer 1 and 3 individually. All transaction processes are documented within the blockchain.

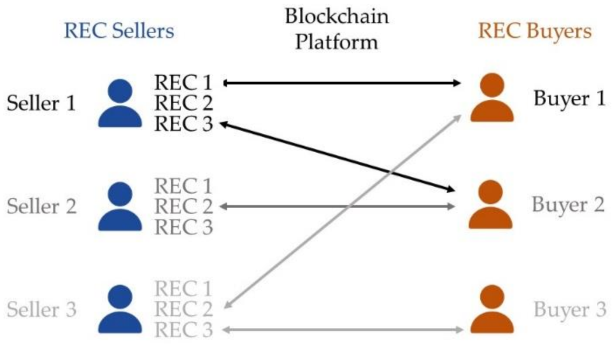

FIGURE 9. **The form in which REC tokens issued by each REC seller are transferred to REC buyers in the simulation.**

After the completion of transactions between buyers and sellers, buyers can obtain renewable energy generation certification by using the REC tokens they hold. To obtain renewable energy generation certification, buyers send their REC tokens to the DSO, which then calculates the weightage based on the type of renewable energy generation and transfers the tokens to the incineration node. All nodes in the network, including the DSO, are unaware of the incineration node's private key. Therefore, once a REC token is transferred to the incineration node in the simulation, it cannot be circulated within the network again. The process of transferring REC tokens from the DSO to the incineration node is referred to as the 'incineration of token.' Simultaneously with token incineration, the buyer node that submitted the token is notified of the amount of recognized renewable energy generation, and the entire process is then concluded. The weightage criteria used in this simulation are provided in Table 3.

TABLE 3. REC Weight Table.

	RE Type		Weight
PV	Installed on General Site	Cap<100kW	1.2
		3000kW>Cap>100kW	1.0
		Cap>3000kW	0.7
	Installed on Existing Facility	Cap<3000kW	1.5
		Cap>3000kW	1.0
	Connected with ESS		5.0
WT	Not Connected with ESS		1.0
	Connected with ESS		5.0
Hydro electric	-		1.0

DSO calculates the renewable energy weightage according to the criteria in Table 3 when all tokens within the system have been incinerated. In this simulation, we verified the incineration process for tokens as follows: token 1 purchased by Buyer 1 from Seller 1, token 2 purchased by Buyer 2 from Seller 2, and token 3 purchased by Buyer 3 from Seller 3. Each buyer node sends its REC token to the DSO, which calculates the weightage for the received tokens. REC token issued to Seller 1 is based on building solar power generation, not integrated with ESS, and has a capacity of 2000 kW, thus receiving a weightage 1.5 times the generation amount. REC token issued to Seller 2 is based on onshore wind power generation, integrated with ESS, thus receiving a weightage 5 times the generation amount. REC token issued to Seller 3 is based on hydroelectric power generation, receiving recognition of renewable energy generation at the same amount without additional weightage. Once the weightage calculation is completed, the DSO sends the REC tokens to the incineration node and recognizes renewable energy generation for the submitting node.

In this subsection, we have outlined the simulation procedure from REC token issuance to obtaining renewable energy generation certification in the new REC system using the Hyperledger Besu program. It is evident that in the new REC system, participant types have been simplified, procedures streamlined, and time reduced due to blockchain automation, thereby mitigating procedural complexity compared to the existing system.

B. REINFORCEMENT OF CYBER SECURITY

Applying blockchain to the REC system offers significant advantages in terms of cyber security. In this subsection, we aim to illustrate through simulations how two potential issues within the REC system can be addressed. Firstly, we plan to address cases where the information recorded in REC is manipulated by system users, and secondly, where system users maliciously issue counterfeit RECs.

1) MANIPULATION OF REC CONTENT BY SYSTEM USER

In terms of cyber security, the first scenario that can pose problems is when a user attempts to modify the content of REC to gain additional profits. There are various methods by which users can manipulate REC content to obtain unjustified additional benefits, such as modifying the renewable energy resource listed in the REC to a resource with a higher weight or changing the ESS ownership status from 'No' to 'Yes.' By altering REC information to deviate from the actual renewable energy generation environment, users can exploit the weighting system to potentially gain up to a fivefold increase in additional revenue.

In the conventional REC system, if a user manipulates the contents of a certificate for unfair gain, it becomes challenging to identify the perpetrator due to the system's procedural complexity and the security vulnerabilities in the recorded information. With the application of blockchain technology, procedural complexity is simplified, and once recorded, the information cannot be altered. This characteristic of REC tokens in blockchain provides a rigid defense against content manipulation.

In the simulation conducted in Subsection 4.A, Buyer1, who purchased REC tokens from Seller1, modified the information recorded in the REC token to achieve greater weighting in line with Seller3's renewable energy generation conditions to gain additional profit. If the content of the REC token is altered, the fact that the REC token's content is recorded within the blockchain network allows the DSO to identify manipulated content and confirm fraudulent activities. Therefore, someone attempting to manipulate tokens must also modify the blocks containing the issuance history to align with the intended content.

Even if the content manipulated within a block is altered, blockchain's characteristics can be leveraged to prevent illicit activities. Each block contained within the blockchain possesses a unique hash value. This hash value represents the result obtained by inputting the entire content of the block into a hash function. Hash functions exhibit the property that even a slight change in input results in a significantly different output, ensuring that the hash value of a block, which is part of the content issued in REC tokens, changes substantially. Due to the nature of blockchain systems, where the hash value of one block is included in the next block, any change in one block leads to alterations in the hash values of all subsequent blocks generated afterward. Consequently, network users can identify when all hash values from the point of misconduct onwards have changed, allowing them to detect network malfeasance. The process is illustrated in Figure 10.

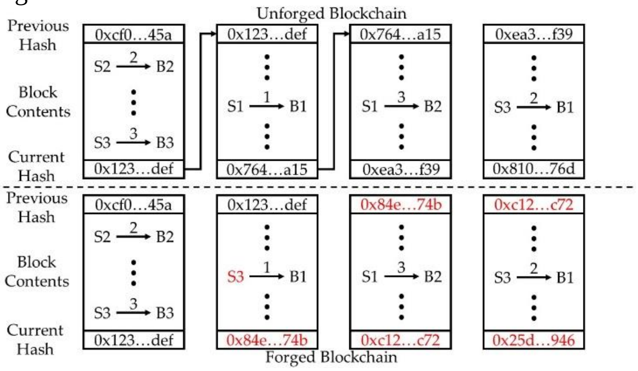

FIGURE 10. **The process of identifying manipulated content when information recorded in the blockchain is maliciously altered in the New REC system.**

2) ISSUANCE OF COUNTERFEITED REC BY SYSTEM USER

The second potential cybersecurity issue is the ability of users to arbitrarily generate counterfeit REC tokens without obtaining DSO approval. Official REC tokens are issued by REC seller nodes only after appropriately generating 1MWh of renewable energy and applying to DSO, which issues them after verification. If REC tokens are issued directly from a specific seller node without passing through DSO, they cannot be considered legitimate REC tokens. If counterfeit tokens circulate within the network without being detected, forgers can gain significant unfair advantages, potentially confusing the entire network.

The second issue can be addressed by recording the issuer's public key within the REC token. In the simulation conducted in this research, DSO's public key is 0x7d8b46c0ecd1afb673a5db70d08ee78066589b65, and this hexadecimal value is recorded in all valid REC tokens issued within the network. The public key of DSO can be used to construct a counterfeit REC token detection program. All nodes within the network can utilize the counterfeit detection program to identify instances of forgery.

To simulate the process of detecting counterfeit REC tokens, Seller 2 node called a smart contract to issue an NFT. The process of issuing counterfeit REC tokens is illustrated in Figure 11 below. By comparing this process with the issuance and transaction of legitimate REC tokens depicted in Figure 3, differences can be identified. Seller 2 node issues counterfeit REC tokens using the smart contract's mint function without reporting to DSO. Subsequently, Seller 2 node sells legitimate REC token 1 and counterfeit REC token 2 to Buyer 2 node through the normal process.

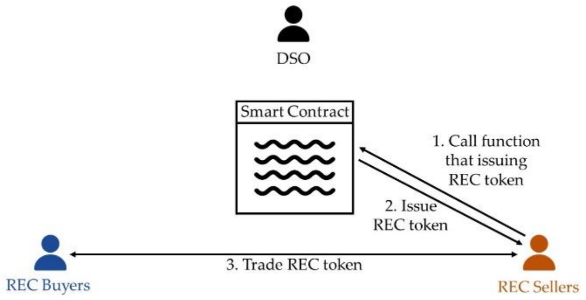

FIGURE 11. The process of generating counterfeit REC tokens.

Buyer 2 node executes a counterfeit detection program to verify if the two tokens it purchased are legitimate REC tokens. When running the program, if the token's issuer is identified as DSO, the REC token is recognized as legitimate. Conversely, if the program results in identifying a token as being issued by a node other than DSO, the REC token is deemed counterfeit.

Suppose the Seller 2 node attempts to alter the issuer information within the REC token to evade the counterfeit detection program by replacing it with DSO's public key. In that case, the process specified in subsubsection 4.B.1 reveals the malpractice. The effective prevention of the two potential malpractices demonstrates the superior security of this system.

VI. DISCUSSION

A. RESOLUTION OF LIMITATIONS THROUGH NEW REC SYSTEM STRUCTURE

In the existing REC system, issues have been raised concerning procedural complexity and cyber security. The application of blockchain technology can address both of these problems. In the traditional REC system, limitations were observed in terms of procedural complexity, transaction formats, the number of participants, and the length of transaction processes. Firstly, the use of blockchain technology allows for the reduction of various transaction formats into a single transaction mechanism. Standardizing the transaction mechanism reduces the complexity for participants, as they no longer need to choose among different options. Secondly, a private blockchain can simplify transaction participants into three entities: buyers, sellers, and the DSO. In the new REC system, the tasks previously handled by REC Issuing Central Institution, DSO, MO, and PX in the existing system are all carried out by the DSO. This eliminates intermediaries like Aggregators and Brokers, facilitating direct transactions between buyers and sellers, thus enhancing simplicity. Finally, the new REC system departs from the verbosity of the old system. The participation, issuance, transaction, and authentication processes in the new system are automated through blockchain technology and smart contracts. Additionally, the security and integrity provided by blockchain technology reduce the multiple authentication steps present in the existing REC system to a single step, simplifying the process.

On the other side, the utilization of blockchain technology can help alleviate the cyber security deficiencies in the system. Information recorded in a blockchain system is immutable, and transaction histories are transparent and accessible to all participants. The two simulations conducted in Subsection 5.B demonstrated the use of blockchain technology's security features to address the previously mentioned issues of tampering with REC content and REC forgery. Furthermore, the security and integrity offered by blockchain can proactively prevent problems such as double-spending and repudiation that could occur in the existing REC system [27]. Consequently, the adoption of the new REC system enables the establishment of a straightforward and secure REC framework.

B. ADDITIONAL ADVANTAGE OF THE NEW REC SYSTEM: INSTITUTIONAL CONSISTENCY

Another advantage that can be gained by applying blockchain technology to the REC system is institutional consistency. The primary utilization of the existing REC was driven by RPS policies and the RE100 campaign. The RPS system is established at the national and state levels, leading to variations in recognized renewable energy sources among different countries. As a result, renewable energy resources that receive high weights in one country may receive low weights or even be unrecognized in another country. The RE100 campaign, being a bottom-up approach developed by the private sector, lacks clear criteria. Consequently, renewable energy certificates used in RPS and RE100 are difficult to be universally applicable worldwide.

By using blockchain technology, the rules of the system can be recorded in electronic documents, and the recorded content is uniformly applied to all users within the system. Applying blockchain technology to the existing REC system can move away from the varying criteria that individual countries previously had and enable the establishment of internationally standardized renewable energy standards. The formulation of a transnational REC system not only encourages global efforts toward climate change using a uniform system but also facilitates REC trading and related negotiations between countries. From the perspective of renewable energy policies, the implementation of blockchain technology ensures that REC markets, such as those for RPS and RE100, operate within the same market rather than forming distinct markets. Standardizing the REC market across different jurisdictions offers advantages such as expanding the market size, and providing a rational and stable REC price in the market as REC quantities and market participants increase.

VII. CONCLUSION

This paper analyzes the limitations of the existing REC system, particularly in terms of procedural complexity and cyber security, and proposes a new REC system that can address these issues. The new REC system incorporates blockchain technology in the form of a private blockchain network consisting of DSO, REC sellers, and REC buyers. DSO plays a central role in permitting network participation, issuing REC, facilitating REC transactions, and aiding in renewable energy generation settlement. RE GenCo and REC holders can participate in the network as REC Sellers, while entities obligated to supply renewable energy can join as REC Buyers within the network.

The previously complex structure of REC issuance and trading systems is simplified in the new REC system, centered around DSO and comprising four stages: participation, issuance, transaction, and authentication. Additionally, the immutability of REC content and recorded information is ensured through the technological features of blockchain. The alleviation of procedural complexity and the enhancement of cybersecurity were demonstrated using the blockchain simulator program, Hyperledger Besu. The simulation involved one DSO node and various scenarios with three REC Seller nodes, each issuing different types of REC and three REC Buyer nodes.

Regarding future works related to the topic of this paper, improvements to the weighted settlement system can be considered. In the new REC system, REC tokens are issued as NFTs based on ERC721, which may have varying values based on their weights. To address this, a system can be developed using ERC20 smart contracts to exchange Fungible Tokens (FT) corresponding to the value of REC tokens. If various NFTs with different values are converted into a single product called FT, it can simplify the market structure and streamline the price formation process.

REFERENCES

[1] Agreement, P. (2015, December). Paris agreement. In report of the conference of the parties to the United Nations framework convention on climate change (21st session, 2015: Paris). Retrived December (Vol. 4, p. 2017). HeinOnline.

[2] Delbeke, J., Runge-Metzger, A., Slingenberg, Y., & Werksman, J. (2019). The paris agreement. In Towards a climate-neutral Europe (pp. 24-45). Routledge.

[3] Gao, A. M. Z., Fan, C. T., & Chen, J. S. (2020). A critical review of the World's first renewable portfolio standard (RPS) for large electricity users in Taiwan: The return of the RPS?. Energy Strategy Reviews, 32, 100585.

[4] Shrimali, G., & Tirumalachetty, S. (2013). Renewable energy certificate markets in India—A review. Renewable and Sustainable Energy Reviews, 26, 702-716.

[5] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59, 183-187.

[6] Guegan, D. (2017). Public blockchain versus private blockhain.

[7] Zuo, Y. (2022). Tokenizing Renewable Energy Certificates (RECs)—A Blockchain Approach for REC Issuance and Trading. IEEE Access, 10, 134477-134490.

[8] Wang, D., Xuan, J., Chen, Z., Li, D., & Shi, R. (2021). Renewable energy certificate trading via permissioned blockchain. Security and Communication Networks, 2021, 1-11.

[9] Castellanos, J. A. F., Coll-Mayor, D., & Notholt, J. A. (2017, August). Cryptocurrency as guarantees of origin: Simulating a green certificate market with the Ethereum Blockchain. In 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE) (pp. 367-372). IEEE.

[10] Cheng, S., Zeng, B., & Huang, Y. Z. (2017, November). Research on application model of blockchain technology in distributed electricity market. In IOP Conference Series: Earth and Environmental Science (Vol. 93, No. 1, p. 012065). IOP Publishing.

[11] Wörner, A., Meeuw, A., Ableitner, L., Wortmann, F., Schopfer, S., & Tiefenbeck, V. (2019). Trading solar energy within the neighborhood: field implementation of a blockchain-based electricity market. Energy Informatics, 2, 1-12.

[12] Dang, C., Zhang, J., Kwong, C. P., & Li, L. (2019). Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market. IEEE Transactions on Smart Grid, 10(6), 6426-6435.

[13] Oprea, S. V., & Bâra, A. (2021). Devising a trading mechanism with a joint price adjustment for local electricity markets using blockchain. Insights for policy makers. Energy Policy, 152, 112237.

[14] Esfahani, M. M. (2022). A hierarchical blockchain-based electricity market framework for energy transactions in a security-constrained cluster of microgrids. International Journal of Electrical Power & Energy Systems, 139, 108011.

[15] Xue, L., Teng, Y., Zhang, Z., Li, J., Wang, K., & Huang, Q. (2017, September). Blockchain technology for electricity market in microgrid. In 2017 2nd International Conference on Power and Renewable Energy (ICPRE) (pp. 704-708). IEEE.

[16] van Leeuwen, G., AlSkaif, T., Gibescu, M., & van Sark, W. (2020). An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. Applied Energy, 263, 114613.

[17] Noor, S., Yang, W., Guo, M., van Dam, K. H., & Wang, X. (2018). Energy demand side management within micro-grid networks enhanced by blockchain. Applied energy, 228, 1385-1398.

[18] Di Silvestre, M. L., Gallo, P., Ippolito, M. G., Sanseverino, E. R., & Zizzo, G. (2018). A technical approach to the energy blockchain in microgrids. IEEE Transactions on Industrial Informatics, 14(11), 4792-4803.

[19] Yang, J., Paudel, A., & Gooi, H. B. (2020). Compensation for power loss by a proof-of-stake consortium blockchain microgrid. IEEE Transactions on Industrial Informatics, 17(5), 3253-3262.

[20] Antal, C., Cioara, T., Antal, M., Mihailescu, V., Mitrea, D., Anghel, I., ... & Bellesini, F. (2021). Blockchain based decentralized local energy flexibility market. Energy Reports, 7, 5269-5288.

[21] Mladenov, V., Chobanov, V., Seritan, G. C., Porumb, R. F., Enache, B. A., Vita, V., ... & Bargiotas, D. (2022). A flexibility market platform for electricity system operators using blockchain technology. Energies, 15(2), 539.

[22] Wu, Y., Wu, Y., Cimen, H., Vasquez, J. C., & Guerrero, J. M. (2022). P2P energy trading: Blockchain-enabled P2P energy society with multi-scale flexibility services. Energy Reports, 8, 3614-3628.

[23] Boerger, M., Lämmel, P., Tcholtchev, N., & Hauswirth, M. (2022). Enabling short-term energy flexibility markets through blockchain. ACM Transactions on Internet Technology, 22(4), 1-25.

[24] Cali, U., Kuzlu, M., Sebastian-Cardenas, D. J., Elma, O., Pipattanasomporn, M., & Reddi, R. (2022). Cybersecure and scalable, token-based renewable energy certificate framework using blockchain-enabled trading platform. Electrical Engineering, 1-12.

[25] Ashley, M. J., & Johnson, M. S. (2018). Establishing a secure, transparent, and autonomous blockchain of custody for renewable energy credits and carbon credits. IEEE Engineering Management Review, 46(4), 100-102.

[26] Zhang, S., Xuan, J., Lyu, Z., & Fu, Y. (2020, October). Application prospect of blockchain in renewable energy certificates. In Proceedings of the 4th International Conference on Computer Science and Application Engineering (pp. 1-5).

[27] Chu, Y., Lee, J., Kim, S., Kim, H., Yoon, Y., & Chung, H. (2022). Review of offline payment function of CBDC considering security requirements. Applied sciences, 12(9), 4488.