ISSN 3083-7715 (online) *Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)*
ISSN 3083-7650 (0135-1710)(print) *Management Information System and Devices. 2026. No. 1 (188)*

UDC 004.9 DOI: https://doi.org/10.30837/0135-1710.2026.188.108

Yehor Korniienko, Oleksii Liashenko

A STUDY OF THE METHODOLOGICAL FOUNDATIONS FOR IMPLEMENTING BLOCKCHAIN AND SMART CONTRACTS IN ELECTRIC POWER MICROGRIDS

The subject of research *covers the theoretical, methodological, and applied aspects of implementing blockchain technology and smart contracts into microgrid management systems, as well as the automation processes of energy resource exchange between participants of a distributed energy system.* ***The purpose of this work*** *is to investigate the methodological foundations for the application of blockchain and smart contracts in microgrids through the analysis of contemporary scientific research, systematization of approaches to consensus algorithm implementation, classification of smart contracts by application areas, and experimental verification of the proposed solutions. To achieve this goal, the following* ***tasks*** *were addressed: analyzing existing microgrid architectures and management methods; conducting a comparative analysis of consensus algorithms (PoW, PoS, PoA, PBFT, RAFT, etc.) regarding their applicability in private and public energy grids; developing a classification of smart contracts based on their application areas; and investigating software tools for implementing decentralized applications.* ***Research Methods.*** *The study employs system analysis methods to investigate microgrid architecture, comparative analysis to evaluate the efficiency of consensus algorithms, and classification methods for grouping smart contracts. For the practical part, computer modeling and experimental verification methods were used: smart contract development in Solidity, testing in the Remix IDE environment, and simulation of a local blockchain network using the Hardhat toolkit.* ***Research results****. The research systematized the methodological foundations for integrating blockchain into microgrids. It was determined that hybrid or private consensus models are most effective for energy trading within local communities. A classification of smart contracts was developed and justified, covering four levels: energy trading, monitoring, distributed management, and cybersecurity. The practical result is the implementation of the EnergyTrading smart contract, which successfully automates the process of listing offers and purchasing electricity, as confirmed by experiments in a local environment. The implementation of smart contracts allows for the creation of a reliable P2P platform for electricity trading without intermediaries, increasing economic efficiency for households. The functionality of the automated settlement mechanism was experimentally confirmed. At the same time, key challenges were identified: the limited scalability of existing blockchain solutions and the need to improve cyber defense against vulnerabilities in contract code. Further development requires adaptation of the legislative framework and modernization of the hardware components of energy grids.*

Keywords: *microgrid; blockchain; smart contract; P2P energy trading; consensus algorithm; Solidity; renewable energy sources; decentralization.*

1. Introduction

In today's world, blockchain technologies play a significant role in various areas, ensuring greater transparency, security, and decentralization of processes. Blockchain, as a technology that implements the concept of a distributed database storing an ordered chain of records, is widely used in many modern areas of human activity, such as the financial sector [1], healthcare [2], supply chain logistics [3], and others.

The relevance of microgrids in the modern energy system stems from the need to improve energy efficiency in existing transmission lines [4], reducing carbon emissions [5], the effective use and integration of renewable energy sources such as solar, wind, hydro, and wave energy, and other factors related to the storage, generation, and transmission of electricity [6–8]. Microgrids in Ukraine represent a highly promising and necessary direction in the context of energy sector development, given the instability of the system in recent years. In October 2022, the Government approved the Concept for the Implementation of "Smart Grids" in Ukraine and adopted a detailed Action Plan for its implementation by 2035 [9].

Blockchain can be implemented in several key aspects of microgrids, including decentralized energy management, where it ensures transparency and security in data exchange among participants. As a result of the expansion and digitalization of electricity distribution infrastructures, peer-to-peer energy trading has become a new paradigm for electricity trading within the microgrid system [10]. Blockchain-based energy system management can offer several advantages: data is protected against loss, tampering, and single points of failure, while security and privacy are enhanced through business rules in smart contracts [11]. Blockchain

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

technology enables secure transactions between parties that do not have prior trust in one another, eliminating the need for intermediaries [12].

2. Analysis of Recent Scientific Publications

Research on blockchain technologies in energy systems has been actively developing in recent years. A significant number of scientific papers are devoted to analyzing the possibilities of integrating distributed ledgers into various sectors of the economy and industry. In particular, Karadag et al. [1] systematized the application of blockchain in the financial sector, while Kasyapa and Vanmathi [2] conducted a comprehensive study of the implementation of this technology in healthcare, including the management of the pharmaceutical supply chain and the regulation of health insurance. Prakash [3] explored the potential of blockchain to enhance the transparency and efficiency of logistics systems.

In the energy sector, researchers are particularly interested in the efficiency of power grids and the integration of renewable energy sources. Ayaz and co-authors [4] analyzed methods for improving energy efficiency in smart grids, while Wang et al. [5] investigated the potential for reducing carbon emissions from microgrids through optimized management. The issue of integrating various types of renewable energy sources is addressed in the works of Dixit [6], Wang [7], and Pani [8], which cover solar, wind, and wave energy, respectively.

Regarding the application of blockchain directly in microgrids, Umar et al. [10] investigated decentralized energy trading using battery systems in community microgrids. Han et al. [11, 12] proposed a smart contract architecture for decentralized energy management and trading based on blockchain. Aghmadi et al. [13] conducted a systematic review of architecture, communications, and cybersecurity in networked microgrids.

The issue of organizing multi-microgrids has been investigated in the works of Inamdar [14] on nested microgrids, Alam [15] on networked microgrids, Ayrir [16] on interconnected microgrids, and Lasseter [17] on coupled microgrids. Bullich-Massagué et al. [18] systematized micro-network clustering architectures.

Azbeg and co-authors [20] made a significant contribution to the study of consensus algorithms by conducting a comparative analysis of various consensus mechanisms in blockchain networks. Bach et al. [21] compared the efficiency of consensus algorithms for different types of applications. Individual studies are devoted to specific algorithms: Islam [22] – Proof of Authority, Zheng and Feng [23] – PBFT, Bowman [24] – Proof of Elapsed Time, Xu [25] – RAFT, Moniz [26] – IBFT.

In the field of smart contracts for energy systems, Junaidi et al. [31] conducted a systematic review of blockchain solutions for demand management in power grids. Wang et al. [32] investigated the application of smart contracts for energy demand management. Practical implementations are represented by platforms such as Power Ledger [33], SunContract [34], and GridPlus [35].

An analysis of scientific publications indicates growing interest in integrating blockchain into microgrids. However, despite a significant amount of research, the issue of systematizing the methodological foundations for the application of smart contracts in microgrids remains underdeveloped. Most studies focus on individual aspects – consensus algorithms, network architecture, or practical implementations – while a comprehensive approach to the classification and methodology of smart contract implementation requires further research.

3. Research Objectives and Tasks

The objective of this work is to investigate the methodological foundations for the application of blockchain and smart contracts in microgrids by analyzing current scientific research, systematizing approaches to the use of consensus algorithms, classifying smart contracts by application areas, and experimentally verifying the proposed solutions.

To achieve this objective, the following tasks must be addressed:

– analyze existing approaches to the use of smart contracts in energy microgrids;

– evaluate the advantages and limitations of various consensus algorithms for private and public blockchain systems;

– identify key aspects of security and data management efficiency;

– investigate practical scenarios for the application of smart contracts to automate energy trading, monitor resources, and enhance cybersecurity;

– conduct experimental verification of the developed solutions using a local blockchain model as an example.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

4. Microgrids and Their Architecture: Definitions, Advantages, and Management Methods

The term "microgrid" refers to the concept of single power supply subsystems connected to a small number of distributed energy resources (DERs), which can be either renewable or conventional sources, including photovoltaic panels, wind power, hydropower, internal combustion engines, gas turbines, and microturbines, which may belong to either the microgrid itself or to individual households. The use of distributed energy resources can lead to issues such as voltage fluctuations, short-term self-sufficiency challenges, high capital costs, and others. In a microgrid, distributed energy resources must be equipped with appropriate electronic interfaces and control systems to ensure operational flexibility while maintaining power quality and energy production.

Microgrids demonstrate compelling advantages over traditional power grids. These include increased reliability, reduced energy costs through integration with renewable energy sources, improved energy security due to self-sufficiency, environmental benefits from reduced carbon emissions, and enhanced flexibility. From a grid perspective, the main advantage of microgrids is that a microgrid is treated as a controllable system within the existing power grid, capable of functioning as a single consumer. From a household perspective, microgrids meet consumers' electricity needs at the local level, ensuring an uninterrupted power supply while reducing transmission losses and providing voltage support. Microgrids are particularly useful in remote areas or in conflict zones where the main power grid may be absent or unreliable. Additionally, microgrids can provide energy independence and resilience, which is especially important in areas prone to natural disasters such as hurricanes or earthquakes.

Blockchain is a type of distributed ledger technology, which is a special form of database maintained by a network of peer-to-peer nodes. The ledger consists of a linear chain of cryptographically linked "blocks", each containing a set of transactions, making these records immutable [19]. Copies of this ledger are stored by all network participants, ensuring its integrity through a "consensus" process, during which nodes collectively verify transactions and add them to the ledger. Therefore, one of the key aspects of blockchain systems is the choice of a consensus algorithm, which determines how nodes reach agreement on each data block. Consensus algorithms in blockchain networks differ in their operating principles, security level, energy consumption, and productivity [20]. One of the best-known is Proof of Work (PoW), which provides high security but requires significant computational resources. An alternative to it is Proof of Stake (PoS), which reduces energy consumption by allowing nodes to validate transactions based on the number of tokens they hold. Further development led to the emergence of Delegated Proof of Stake (DPoS), where validators are elected by voting, which increases transaction speed. Meanwhile, Proof of Authority (PoA) uses a limited number of trusted participants to validate blocks, making it effective for private blockchains. To optimize storage resources, Proof of Capacity (PoC) / Proof of Space was proposed, where participants use disk space for mining.

Another approach is implemented by Proof of Burn (PoB), which involves burning coins to obtain the right to create new blocks. Distributed systems often use Practical Byzantine Fault Tolerance (PBFT), which effectively coordinates the network state among nodes, while Proof of Elapsed Time (PoET) is used in enterprise solutions due to its cost-effectiveness and low energy consumption. Also, among modern algorithms, it is worth noting Istanbul Byzantine Fault Tolerance (IBFT), which ensures fast block finalization, and Proof of Weight, which uses various participant weight parameters to achieve consensus.

Thus, the choice of algorithm depends on the type of blockchain and its purpose. Public networks most often use PoW, PoS, DPoS, PoC, PoB, and PoWeight, while private networks predominantly use Raft, PoA, IBFT, PoET, PBFT, and HotStuff. Depending on the requirements for security, energy efficiency, and transaction processing speed, the appropriate mechanism is implemented. For example, for a permissionless network with an emphasis on security and significant computational resources, Proof of Work is a suitable option.

Conversely, PoS or DPoS can be used when block validation speed is a priority. Additionally, PoS and DPoS provide speed, efficiency, and a sufficient level of security with lower energy consumption, which is critical for microgrids, especially in the case of autonomous (island) networks. The main differences between PoS and DPoS are that the latter provides higher speed and scalability due to a smaller number of delegates participating in consensus, but this may reduce the level of decentralization. PoS offers a more even distribution of power among network participants [21]. However, despite the fact that a permissionless (public) blockchain

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

is truly decentralized and open (with nearly zero risk of information being altered, edited, or deleted) unlike a non-public blockchain system, in reality, the participants in the microgrid – household owners – are known in advance, and trading occurs based on the identification of parties by territorial, physical, and other characteristics of households. Therefore, it is necessary to identify and highlight the advantages and disadvantages of consensus algorithms specific to private blockchains, namely Proof of Authority [22], Practical Byzantine Fault Tolerance [23], Proof of Elapsed Time [24], RAFT [25], and Istanbul Byzantine Fault Tolerance [26] (one of the BFT algorithm family: Dynamic BFT [27], Democratic BFT [28], R-PBFT [29]). A comparative analysis of leading consensus algorithms is presented in Table 1.

Table 1. *Comparative analysis of leading consensus algorithms*

Consensus algorithm	Advantages	Restrictions
RAFT	simplicity and clarity; coordination based on "leaders"; fault tolerance; no risk of attack; high throughput under stable conditions.	single point of failure (dependence on the leader); scalability issues; delay during leader election; the node is limited.
PBFT	high fault tolerance; high scalability; access control; deterministic finality.	complexity; susceptibility to network delays.
PoET	energy efficiency; scalability; fast consensus.	relies on trusted execution environments (TEEs); security issues; limited adoption.
HotStuff	energy efficiency; scalability; simplicity and modularity; security and reliability.	delay;complex implementation; high resource consumption; centralization issues.
PoA	fast decision-making; low power consumption; ease of configuration;accountability and transparency.	dependence on trust; vulnerability to trust-based attacks.
IBFT	guaranteed finality; defined finality; unambiguous finality.	risks of centralization; complex implementation; susceptibility to network delays.

For the operation of microgrids that use blockchain to manage energy transactions, ensuring data security and integrity is critical. The primary tool for achieving this level of security is cryptography, specifically digital signatures and hash functions. When a household in a microgrid performs a transaction, a digital signature mathematically links it to that transaction. If the digital signature verifies the authenticity and integrity of the transaction data, this guarantees that the transaction has not been altered. Cryptographic hash functions play a key role in this process. They operate as mathematical algorithms that convert variable-length data into a fixed size, enabling efficient searching and minimizing the risk of collisions – situations where different data produce the same hash result. Thanks to this, blockchain is capable of maintaining a high level of security and stability even in decentralized networks, such as microgrids. Thus, cryptographic mechanisms form the foundation for ensuring trust and security in energy transactions within blockchain-based microgrids. Among the large number of existing hash functions, the leaders are SHA-2, SHABAL, SHAVITE, Keccak, and Blake. The distinctive features of each algorithm include security characteristics, requirements for resistance, and computational resources [30]. Productivity metrics for hash functions show that there is a natural balance between computational speed and the level of security they provide. For example, although SHA-256 demonstrates better productivity in most scenarios, the choice of SHA-512 may be motivated by increased security requirements.

5. Analysis, Development, and Integration of Smart Contracts in Microgrids: Relevance and Applications

Smart contracts are programmable distributed systems that operate in a decentralized environment. They combine several key aspects of computer engineering, including software development, security, cryptography, distributed computing, and efficient

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

resource management. In addition to recording transactions or any other sequential information, a blockchain can also store smart contracts (SCs) that execute when certain conditions are met. A smart contract is added to the blockchain similarly to a transaction record. The compiled code and associated data are sent to the blockchain, where they are included in a block and added to the ledger via a consensus mechanism. Like transactions, smart contracts are secured by cryptographic hashing, making it impossible to alter or forge them.

Once deployed on the blockchain, a smart contract acts as a software process that executes when certain conditions arise, such as energy consumption, energy production, or any other processes on which the activation of the smart contract depends. The execution of the smart contract code takes place in a virtual environment distributed across all nodes of the blockchain.

From a methodological standpoint, the integration of smart contracts into microgrids requires a systematic approach involving several key stages. First, a domain analysis is conducted to identify business processes that can be automated. Next, a smart contract model is developed, taking into account security, execution efficiency, and compatibility with the selected blockchain protocol. The next step is testing and verifying the smart contract in a microgrid simulation environment, which allows for evaluating its behavior under real-world load conditions. The final stage of the methodology involves integrating the smart contract into the operational microgrid and continuously monitoring its execution, with the ability to make adjustments based on the data obtained. This approach ensures not only technical implementation but also a scientifically grounded methodology for applying blockchain technologies in microgrids, enhancing transparency, security, and the efficiency of energy resource management.

Smart contracts can be written in general-purpose programming languages such as Golang, Node.js, and Java, or in specialized languages such as Solidity, which is the first and most popular language for creating smart contracts to build decentralized applications (DApps). Smart contract features such as self-execution and automation, tamper-resistance, reliability, transparency and accessibility, security, speed and reliability, self-verification, computational productivity and costs, and dependence on a specific programming language make smart contracts a powerful tool for automating processes and ensuring security in various blockchain applications, including the energy sector.

Smart contracts automate various aspects of the execution and management of relationships between consumers, electricity producers, and other participants in the microgrid. For example, in the context of energy systems, smart contracts are used to ensure secure and transparent transactions between energy producers and consumers, as well as to control the reading, writing, and processing of data in the blockchain ledger. Blockchain-based smart contracts automate energy trading and Demand Response (DR) processes, enabling more efficient real-time balancing of supply and demand [31].

The application of smart contracts in microgrids is widespread; for example, one of the most common uses of smart contracts when building a blockchain-based microgrid is a situation where a homeowner (household) has a surplus of generated energy after installing solar panels or other renewable energy sources. In this case, a smart contract can establish the terms of the agreement between the owner and the energy consumer. The details of the smart contract may include the price and amount of energy, the duration of the agreement, as well as the conditions for terminating such a contract. Once the terms of the smart contract agreement have been agreed upon, it is deployed on the blockchain ledger. And in the future, when the solar panel generates excess energy and the smart contract conditions are met, the contract automatically initiates a transaction with the entity that needs this resource, such as the nearest household. Afterward, payment will be made in accordance with the terms of the contract. Since the transaction is recorded in the blockchain ledger, it is secure and transparent for both the seller and the buyer, and is available for further inspection and monitoring if necessary.

In addition, smart contracts can dynamically change the network configuration and the blockchain consensus algorithm. For example, a smart contract can be created that adjusts the block size, consensus mechanism, or transaction fees depending on current network dynamics. In particular, another application of smart contracts for decentralized energy systems is the development of a contract that can verify and prepare energy supply data for a database, and then analyze the stored data [32].

For example, the use of smart contracts in microgrids allows for the automation of the energy exchange process between producers and consumers, eliminating the need for centralized intermediaries. One of the key components of this approach is a mechanism for registering offers to sell electricity, which is implemented via a smart contract on a blockchain network. For example, let’s consider

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

the listEnergy() method (Listing 1), which can be used in microgrids to register offers to sell electricity. This mechanism allows producers (sellers) to set the price and available volume of energy, ensuring an automated process for concluding transactions in a smart contract implemented in the Solidity language.

Listing 1

```
// Adding an energy offer for sale
 function listEnergy(uint256 _pricePerKWh, uint256 _availableKWh) external {
    require(availableKWh > 0, "Кількість енергії має бути більшою за 0");
    require(pricePerKWh > 0, "Ціна має бути більшою за 0");
    offerCount++;
    offers[offerCount] = EnergyOffer(msg.sender, _pricePerKWh, _availableKWh);
    emit EnergyListed(offerCount, msg.sender, _pricePerKWh, _availableKWh);
}
```

The method's operation involves several key steps. First, the input parameters are checked: the function takes two arguments – _pricePerKWh, which specifies the price per 1 kWh, and _availableKWh, which indicates the amount of energy available for sale. The contract verifies that both values are greater than zero, which prevents invalid operations. After that, the offer is registered: a new entry is added to the general list (offers), containing information about the seller, the specified price, and the available amount of energy. Additionally, the offer counter (offerCount) is incremented, ensuring a unique identifier for each transaction. The final step is the generation of an event (emit EnergyListed), which records the creation of a new offer on the blockchain. This allows all participants in the microgrid to track the current list of available energy, ensuring transparency and efficiency in trading operations.

It should be noted that there are various implementations of smart contracts in distributed energy systems around the world. One such example is Power Ledger [33], an Australian startup that has developed a blockchain platform for peer-to-peer energy trading using smart contracts to ensure secure and transparent transactions between energy producers and consumers. SunContract [34] allows users to set energy prices and choose suppliers, giving them greater control and flexibility in managing their energy needs. The platform is based on a peer-to-peer (P2P) energy trading model, which allows users to trade energy generated from renewable sources, such as solar and wind power. By utilizing smart contracts on the blockchain, SunContract ensures transparency and automation of transactions, making the energy trading process more efficient and accessible to all participants. GridPlus [35] is also actively working on solutions for integrating blockchain into the energy sector, including smart contracts to automate processes and ensure transaction transparency. The platform aims to promote the use of renewable energy sources and improve the efficiency of energy systems.

6. Classification of Smart Contracts in Microgrids

The use of smart contracts is broad in scope, addressing the tasks and operational scenarios faced by microgrid engineers and designers.

After analyzing the variety of smart contract implementation options, the following layers were identified that characterize the application of smart contracts: energy trading and energy resource redistribution, as well as inspection, monitoring, and cybersecurity to ensure the stable operation of the electricity market and distribution processes within the microgrid. Figure 1 illustrates the relationship between contract types based on logical affiliation and application characteristics. Within the methodological approach, the classification of smart contracts ensures their orderly implementation in microgrids. The methodology includes identifying the functional zones of the microgrid, defining scenarios for the application of smart contracts, selecting the contract type according to the set tasks and execution conditions, as well as evaluating the effectiveness and security of the chosen solution. This approach not only formalizes the process of developing and integrating smart contracts but also creates a foundation for the scalable and scientifically sound implementation of blockchain technologies in energy systems.

Energy trading is one of the most common applications of blockchain in energy systems. A large number of studies analyze blockchain approaches based

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

on smart contracts for energy markets, which eliminate the need for third parties to create, regulate, or manage these markets. Such approaches can improve the efficiency of power systems, reduce peak loads, facilitate the participation of small sellers in the market, lower energy costs for residential users, and stimulate investment in renewable energy sources.

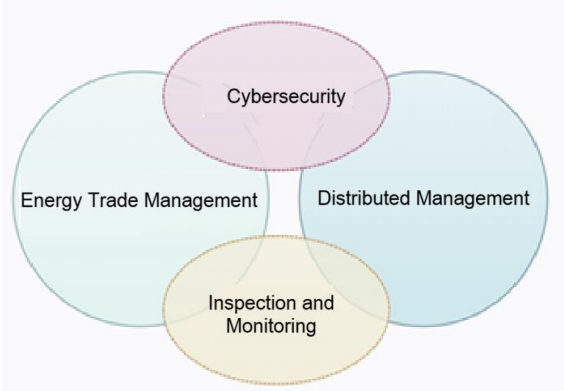

Fig. 1. Venn diagram illustrating the logical relationship between types of smart contract applications

Managing resource allocation in microgrids is a key challenge that can be significantly improved through smart contracts. Smart contracts can implement optimization algorithms. This allows for balancing load distribution among households and energy producers, ensuring a fair distribution of revenues. Smart contracts also help reduce peak load by automatically redistributing energy, leveraging the flexibility of distributed energy assets such as batteries or electric vehicles. In the case of decentralized battery management, smart contracts at this level can analyze information about battery charge status and capacity using "Inspection and Monitoring" level smart contracts, as well as send practical recommendations to synchronize charging and discharging processes. Additionally, such contracts can be used to automatically coordinate decisions among various network assets, thereby enhancing the efficiency and reliability of the energy system.

Inspection and monitoring are essential tools for the operation of any system, including the electricity trading market and distribution management. Current metrics or metrics over a specified period play a key role in forecasting, management, and the stability of the microgrid. Monitoring electricity traffic, financial transactions, conflicts or malfunctions, and other indicators of the microgrid's operation will help other smart contracts make decisions and "activate" when certain levels or values are reached.

Smart contracts also play a vital role in ensuring cybersecurity within energy systems, including microgrids. They enable the automation and protection of processes related to data exchange and information access.

Smart contracts in the "cybersecurity" layer aim to ensure reliable user authentication and authorization, preventing unauthorized access to critical data. Additionally, they ensure transparency and the immutability of records in the distributed ledger, reducing the risk of data tampering or cyberattacks. An important aspect is the ability to create smart contracts that automatically monitor anomalies or disruptions in system operation and can activate threat response protocols. This ensures an increase in the overall level of cybersecurity in decentralized energy networks.

7. Ethereum-Based Energy Exchange

The goal of the experimental phase was to confirm the possibility of a secure, transparent, and automated exchange of energy resources between participants using smart contracts on the Ethereum platform. To achieve this goal, two experimental environments were implemented: the Remix IDE environment for initial testing and the local Hardhat simulated network for advanced analysis.

In the first phase, the EnergyTrading smart contract, written in Solidity, was implemented. This contract models the exchange's basic functionality: the registration of energy sale offers and the process of the buyer acquiring the corresponding volumes. The contract includes basic protections against overpayment, processing of available resource quantity checks, and logging events (Listing 2).

Listing 2

```
pragma solidity ^0.8.0;
contract EnergyTrading {
    event EnergyListed(uint id, address seller, uint pricePerKWh, uint availableKWh);
    event EnergyBought(uint id, address buyer, uint kWh);
    struct Offer {
        address seller;
```

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

```
        uint pricePerKWh;
        uint availableKWh;
    }

    mapping(uint => Offer) public offers;
    uint public nextOfferId;
    function listEnergy(uint pricePerKWh, uint availableKWh) public {
        offers[nextOfferId] = Offer(msg.sender, pricePerKWh, availableKWh);
        emit EnergyListed(nextOfferId, msg.sender, pricePerKWh, availableKWh);
        nextOfferId++;
    }
    function buyEnergy(uint offerId, uint kWh) public payable {
        Offer storage offer = offers[offerId];
        require(kWh <= offer.availableKWh, "Not enough energy available");
        require(msg.value >= kWh * offer.pricePerKWh, "Not enough ETH sent");
        offer.availableKWh -= kWh;
        payable(offer.seller).transfer(msg.value);
        emit EnergyBought(offerId, msg.sender, kWh);
    }
}
```

Further testing was conducted in two modes. The first involved using the Remix IDE, where the contract was successfully compiled, deployed, and manually tested under typical scenarios. The second involved the local Hardhat environment, which emulates a full-fledged blockchain network. Within Hardhat, a local chain was deployed using the built-in Proof-of-Work (PoW) consensus mechanism; a corresponding interact.js script was created; automated simulation of user interactions (seller/buyer) was implemented; and execution logs, transaction volumes, and changes in participants' balances were collected.

To perform an initial verification of the EnergyTrading smart contract's functionality, the Remix IDE environment – a tool for online development and testing of Solidity contracts – was used. This allowed for a quick verification of the basic logic without the need to set up a local blockchain.

The following steps were performed as part of the experiment:

1) the contract was compiled – the contract's bytecode was successfully generated using the Solidity 0.8.0 compiler. Next, the contract was deployed on the virtual machine (VM) built into Remix, which emulates the behavior of the Ethereum network with support for multiple accounts and balances;

2) an energy sale offer was created – the listEnergy(pricePerKWh, availableKWh) function was called with the initial parameters. As a result, a new offer was saved in the contract's storage, and the corresponding EnergyListed event was logged in the console; a purchase was made – the buyEnergy (offerId, kWh) function was called, specifying the amount of energy and the corresponding amount in wei. This resulted in the transfer of funds to the seller, an update to the balance, and the triggering of the EnergyBought event (Fig. 2).

The results showed that the contract's business logic functions as expected. Function calls were accompanied by corresponding transactions and events. Additionally, Remix provided a visual interface for debugging and tracking changes in the contract repository, which helped identify logical errors at an early stage. This phase served as validation of the smart contract prior to its deployment in a more complex environment simulating real blockchain execution.

After the initial validation of the contract in Remix, interaction was simulated in a local test network created using the Hardhat toolkit. This provided a flexible and controlled environment supporting multiple accounts, automated scripts, and the ability to emulate the consensus process.

ISSN 3083-7715 (online) Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)
ISSN 3083-7650 (0135-1710)(print) Management Information System and Devices. 2026. No. 1 (188)

Fig. 2. Purchasing electricity via the EnergyTrading smart contract

The EnergyTrading smart contract was compiled and deployed to the built-in Hardhat network, which by default simulates the Proof-of-Work (PoW) mechanism. Following this, interaction was implemented via a script that executed the typical behavior of energy market participants – the seller and the buyer. The scenario consisted of the following steps:

1) initiation of an energy sale offer. The seller's account called the listEnergy method, which registers the offer in the contract with the specified price and amount of energy;

2) simulation of an energy purchase. Another account (the buyer) called the buyEnergy method, transferring the corresponding amount of energy and ETH within the contract logic;

3) reading the state. After the transactions, the remaining available energy was retrieved by the offer ID, and the seller's balances before and after the transaction were calculated to verify the correctness of the transfer.

As a result, the functionality of the contract's core logic was confirmed. The system responded correctly to typical use cases, including edge cases (e.g., exceeding the available energy volume). The use of Hardhat ensured the determinism of the experiment, and the PoW consensus allowed us to simulate conditions similar to those of public Ethereum networks prior to the transition to Proof-of-Stake. This lays the groundwork for further research on the application of alternative consensus algorithms, such as PoA or PoS, in private microgrids.

8. Problems and Challenges

There are a number of significant challenges to implementing blockchain technology in microgrids, one of which is scalability. Currently, blockchain solutions cannot efficiently execute the complex logic of a large number of smart contracts in a short time, requiring more and more resources as the blockchain system grows. A particular problem arises in the context of the overall power grid, where a large number of transactions per second is expected due to the diversity of end consumers, power generation points, and market regulation rules for resources. As of mid-2025, the integration of blockchain systems into Ukraine's overall power grid is impossible due to outdated equipment, limited support and management resources, and the absence of relevant legal regulations not only in Ukraine but globally.

The second issue is security and cybersecurity in the deployment of blockchain within the energy system, specifically in microgrids. Potential external interference with the energy system poses a threat at the national level and could cause serious problems for users, industry, and other consumers. Blockchain-based transactions must be secured at all levels of execution. Controlled management of consumer finances must be a priority when implementing blockchain in any power system. Therefore, improving software and hardware for user identification, encryption, and other means of protecting digital data offers a solution to cybersecurity challenges.

In turn, the deployment of smart contracts on the blockchain poses significant challenges in the areas of cybersecurity and privacy protection, due to the risk of losing access keys or their exposure for any reason. Smart contracts responsible for market control or resource allocation, despite being fully protected against forgery and having their defined methods and management remain unchanged after deployment, can

Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188) *ISSN 3083-7715 (online)*
Management Information System and Devices. 2026. No. 1 (188) *ISSN 3083-7650 (0135-1710)(print)*

have negative consequences in the event of code vulnerabilities resulting from intentional or accidental errors on the part of the developer. This can lead to catastrophic consequences for the operation of the microgrid and the improper management of energy resources and finances of end consumers, electricity producers, and other microgrid participants.

Conclusions and Prospects

This article examined the methodological foundations for applying blockchain technologies in microgrids through a comprehensive analysis of the current state of energy systems, an assessment of the relevance of microgrids, and the potential of decentralized solutions. The architectural principles of microgrids and the possibilities for blockchain integration were examined based on scientific sources, practical implementations, and modern technical solutions. A comparison of consensus algorithms and a classification of blockchain access models allowed for the formulation of general principles for selecting technologies for energy applications.

An important component of the study was a review of smart contracts and their capabilities in the context of microgrids. Based on an analysis of the literature, existing solutions, and development trends, four key areas of their application were identified: inspection and monitoring, energy trading management, distributed management, and cybersecurity.

The proposed classification can serve as a methodological basis for further standardization of approaches to the implementation of smart contracts, taking into account regional requirements, regulatory constraints, and the specifics of power systems in different countries.

The study also identifies the main challenges that complicate the implementation of blockchain solutions in microgrids. Technical limitations include scalability issues and high demands on computing resources, which become critical in large systems with high transaction frequencies. Security challenges include the risks of losing or compromising access keys, the possibility of errors in the immutable code of smart contracts, and vulnerabilities that could affect the operation of energy systems. The decentralized architecture provides protection against forgery, but at the same time exacerbates risks associated with developer errors or hidden software defects.

Given these limitations, a promising direction for further research is the development of methods for automated verification and testing of smart contracts prior to their deployment on the blockchain. Particular attention should be paid to identifying logical errors, malicious activation conditions, and potential vulnerabilities. The use of machine learning and artificial intelligence methods can ensure effective risk detection, increase the reliability of blockchain solutions, and accelerate the development of a standardized methodology for their application in microgrids.

Thus, the results obtained can serve as a basis for further applied developments, technology standardization, and the improvement of blockchain-based energy management systems.

Conflict of interest

The authors declare that they have no conflicts of interest regarding this study, including financial, personal, authorship, or other conflicts that could influence the study and its results presented in this article.

Funding

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technology in the creation of this work.

References

1. Karadag, B., Zaim, A. H., Akbulut, A. (2024), "Blockchain in Finance: A Systematic Literature Review", *Journal of Business, Economics and Finance (JBEF)*, Vol. 13, No. 2, P. 113–130. DOI: https://doi.org/10.17261/Pressacademia.2024.1945

2. Kasyapa, M. S. B., Vanmathi, C. (2024), "Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies", *Frontiers in Digital Health*, Vol. 6, P. 1359858. DOI: https://doi.org/10.3389/fdgth.2024.1359858

3. Prakash, A. (2024), "Blockchain Technology for Supply Chain Management: Enhancing Transparency and Efficiency", *International Journal for Global Academic & Scientific Research (IJGASR)*, Vol. 3, No. 2, P. 01–11. DOI: https://doi.org/10.55938/ijgasr.v3i2.73

4. Ayaz, K., Sulemani, M. S., Ahmed, N. (2017), "Efficient Energy Performance within Smart Grid", Smart Grid and Renewable Energy, Vol. 8, No. 3, P. 75–86. DOI: https://doi.org/10.4236/sgre.2017.83005

5. Gao, S., Wang, Z., Yang, Y., Li, C., Fan, J., Kou, J. (2024), "Economic Cost and Carbon Emission Reduction of Microgrid via Bi-Objective Optimization", *Proceedings of the 2024 43rd Chinese Control Conference (CCC), Kunming, China*, 28–31 July 2024, IEEE, P. 1–6. DOI: https://doi.org/10.23919/CCC63176.2024.10662760

6. Dixit, S., Singh, P., Ogale, J., Bansal, P., Sawle, Y. (2023), "Energy Management in Microgrids with Renewable Energy Sources and Demand Response", *Computers and Electrical Engineering*, Vol. 110, Article 108848. DOI: https://doi.org/10.1016/j.compeleceng.2023.108848

7. Wang, Y., Wang, Z., Sheng, H. (2024), "Optimizing wind turbine integration in microgrids through enhanced multi-control of energy storage and micro-resources for enhanced stability", *Journal of Cleaner Production*, Vol. 444, Article 140965. DOI: https://doi.org/10.1016/j.jclepro.2024.140965

8. Kodanda Pani, N. K., Ravi, A., Bai, L., Qiu, F., Zhao, S., Zhang, Y. (2023), "Enhancing Microgrid Resilience through Wave Energy Integration", *Proceedings of the 2023 North American Power Symposium (NAPS), Asheville, NC, USA*, 15–17 October 2023, IEEE. DOI: https://doi.org/10.1109/NAPS58826.2023.10318531

9. Верховна Рада України (2024), Проект Закону про внесення змін до деяких законів України щодо врегулювання окремих питань використання термінології у сфері впровадження "розумних мереж", URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43837

10. Umar, A., Kumar, D., Ghose, T. (2022), "Blockchain-based decentralized energy intra-trading with battery storage flexibility in a community microgrid system", *Applied Energy*, Vol. 322, Article 119544. DOI: https://doi.org/10.1016/j.apenergy.2022.119544

11. Han, D., Zhang, C., Ping, J., Yan, Z. (2020), "Smart contract architecture for decentralized energy trading and management based on blockchains", *Energy*, Vol. 199, Article 117417. DOI: https://doi.org/10.1016/j.energy.2020.117417

12. Hahn, A., Singh, R., Liu, C.-C., Chen, S. (2017), "Smart contract-based campus demonstration of decentralized transactive energy auctions", *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA. DOI: https://doi.org/10.1109/ISGT.2017.8086092

13. Aghmadi, A., Hussein, H., Polara, K. H., Mohammed, O. (2023), "A Comprehensive Review of Architecture, Communication, and Cybersecurity in Networked Microgrid Systems", *Inventions*, Vol. 8, No. 4, Article 84. DOI: https://doi.org/10.3390/inventions8040084

14. Inamdar, S., Mohanty, R., Chen, P., Majumder, R., Bongiorno, M. (2019), "On Benefits and Challenges of Nested Microgrids", *2019 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, Macao, China, 01–04 December 2019. DOI: https://doi.org/10.1109/APPEEC45492.2019.8994363

15. Alam, M. N., Chakrabarti, S., Ghosh, A. (2019), "Networked Microgrids: State-of-the-Art and Future Perspectives", *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 3, P. 1238–1250. DOI: https://doi.org/10.1109/TII.2018.2881540

16. Ayrir, W., Helmi, A. M., Ramadan, H. S. (2024), "Interconnected microgrids optimization via reconfiguration-based modular approach", *Applied Energy*, Vol. 375, Article 124050. DOI: https://doi.org/10.1016/j.apenergy.2024.124050

17. Lasseter, R. H. (2011), "Smart Distribution: Coupled Microgrids", *Proceedings of the IEEE*, Vol. 99, No. 6, P. 1074–1082. DOI: https://doi.org/10.1109/JPROC.2011.2114630

18. Bullich-Massagué, E., Díaz-González, F., Aragüés-Peñalba, M., Girbau-Llistuella, F., Olivella-Rosell, P., Sumper, A. (2018), "Microgrid clustering architectures", *Applied Energy*, Vol. 212, P. 340–361. DOI: https://doi.org/10.1016/j.apenergy.2017.12.048

19. Liu, B. (2021), "Overview of the Basic Principles of Blockchain", 2021 *International Conference on Intelligent Computing, Automation and Applications (ICAA), Nanjing, China*, 25–27 June 2021. DOI: https://doi.org/10.1109/ICAA53760.2021.00108

20. Azbeg, K., Ouchetto, O., Jai Andaloussi, S., Fetjah, L. (2021), "An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions", *Advances on Smart and Soft Computing. Advances in Intelligent Systems and Computing*, Vol. 1188, Springer, Singapore. DOI: https://doi.org/10.1007/978-981-15-6048-4_31

21. Bach, L. M., Mihaljević, B., Zagar, M. (2018), "Comparative Analysis of Blockchain Consensus Algorithms", *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 21–25 May 2018, P. 1545–1550. DOI: https://doi.org/10.23919/MIPRO.2018.8400278

22. Islam, Md. M., Merlec, M. M., In, H. P. (2022), "A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique", *2022 IEEE International Conference on Services Computing (SCC)*, Barcelona, Spain, 10–16 July 2022, P. 327–332. DOI: https://doi.org/10.1109/SCC55611.2022.00054

23. Zheng, X., Feng, W. (2021), "Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain", *Journal of Physics: Conference Series*, Vol. 1802, No. 3, Art. no. 032022. DOI: https://doi.org/10.1088/1742-6596/1802/3/032022

24. Bowman, M., Das, D., Mandal, A., Montgomery, H. (2021), "On Elapsed Time Consensus Protocols", *Progress in Cryptology – INDOCRYPT 2021. Lecture Notes in Computer Science*, Vol. 13143, Springer, Cham, 12–15 December 2021, Jaipur, India. DOI: https://doi.org/10.1007/978-3-030-92518-5_25

25. Xu, X., Hou, L., Li, Y., Geng, Y. (2021), "Weighted RAFT: An Improved Blockchain Consensus Mechanism for Internet of Things Application", *2021 7th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 10–13 December 2021. DOI: https://doi.org/10.1109/ICCC54389.2021.9674683

26. Moniz, H. (2020), "The Istanbul BFT Consensus Algorithm", *arXiv preprint*, arXiv:2002.03613. DOI: https://doi.org/10.48550/arXiv.2002.03613

27. Xu, H., Long, Y., Liu, Z., Liu, Z. H., Gu, D. (2018), "Dynamic Practical Byzantine Fault Tolerance", *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, China, 30 May – 1 June 2018, P. 1–8. DOI: https://doi.org/10.1109/CNS.2018.8433150

28. Crain, T., Gramoli, V., Larrea, M., Raynal, M. (2018), "DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains", *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, 1 November 2018, P. 1–8. DOI: https://doi.org/10.1109/NCA.2018.8548057

29. Liu, S., Wang, X., Hui, L., Wu, W. (2023), "Blockchain-Based Decentralized Federated Learning Method in Edge Computing Environment", *Applied Sciences*, Vol. 13, No. 3, Article 1677. DOI: https://doi.org/10.3390/app13031677

30. Kuznetsov, O., Peliukh, O., Poluyanenko, N., Bohucharskyi, S., Kolovanova, I. (2023), "Comparative Analysis of Cryptographic Hash Functions in Blockchain Systems", *CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems*, CEUR Workshop Proceedings, Vol. 3550, October 26, 2023, Kyiv, Ukraine, P. 81–94. URL: https://ceur-ws.org/Vol-3550/paper7.pdf

31. Junaidi, N., Abdullah, M. P., Alharbi, B., Shaaban, M. (2023), "Blockchain-based management of demand response in electric energy grids: A systematic review", *Energy Reports*, Vol. 9, P. 5075. DOI: https://doi.org/10.1016/j.egyr.2023.04.020

32. Wang, X., Yang, W., Noor, S., Chen, C., Guo, M., van Dam, K. H. (2019), "Blockchain-based smart contract for energy demand management", *Energy Procedia*, Vol. 158, P. 2719–2724. DOI: https://doi.org/10.1016/j.egypro.2019.02.028

33. Power Ledger. Офіційний сайт. URL: https://www.powerledger.io/ (дата звернення: 01.09.2025).

34. SunContract. Офіційний сайт. URL: https://suncontract.org/ (дата звернення: 01.09.2025).

35. GridPlus. Офіційний сайт. URL: https://gridplus.io/ (дата звернення: 01.09.2025).

Received (Надійшла) 08.11.2025
Accepted for publication (Прийнята до друку) 17.12.2025
Publication date (Дата публікації) 12.03.2026

Відомості про авторів / About the Authors

Корнієнко Єгор Дмитрович – Харківський національний університет радіоелектроніки, аспірант кафедри електронних обчислювальних машин; Харків, Україна;

Yehor Korniienko – Kharkiv National University of Radio Electronics, Postgraduate Student at the Department of Electronic Computers; Kharkiv, Ukraine;

e-mail: yehor.korniienko@nure.ua

ORCID ID: https://orcid.org/0009-0002-7274-2815

Ляшенко Олексій Сергійович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри електронних обчислювальних машин; Харків, Україна;

Oleksii Liashenko – Phd (Engineering Sciences), Associate Professor, Kharkiv National University of Radio Electronics, Associate Professor at the Department of Electronic Computers; Kharkiv, Ukraine;

e-mail: oleksii.liashenko@nure.ua

ORCID ID: https://orcid.org/0000-0002-0146-3934

ДОСЛІДЖЕННЯ МЕТОДОЛОГІЧНИХ ОСНОВ УПРОВАДЖЕННЯ БЛОКЧЕЙНУ Й СМАРТ-КОНТРАКТІВ В ЕЛЕКТРОЕНЕРГЕТИЧНИХ МІКРОМЕРЕЖАХ

Предметом дослідження *є теоретико-методологічні й прикладні аспекти впровадження технології блокчейн і смарт-контрактів у системи управління мікромережами (Microgrids), а також процеси автоматизації обміну енергетичними ресурсами між учасниками розподіленої енергосистеми.* ***Мета роботи*** *– дослідити методологічні основи застосування*

ISSN 3083-7715 (online) *Автоматизовані системи управління та прилади автоматики. 2026. № 1 (188)*
ISSN 3083-7650 (0135-1710)(print) *Management Information System and Devices. 2026. No. 1 (188)*

блокчейну й смарт-контрактів у мікромережах за допомогою аналізу сучасних наукових студій, систематизації підходів до використання алгоритмів консенсусу, класифікації смарт-контрактів за сферами застосування та експериментальної перевірки запропонованих рішень. Для досягнення окресленої мети необхідно було виконати такі ***завдання****: проаналізувати наявні архітектури мікромереж і методи їх управління; здійснити порівняльний аналіз алгоритмів консенсусу (PoW, PoS, PoA, PBFT, RAFT тощо) щодо їх застосовності в приватних і публічних енергетичних мережах; розробити класифікацію смарт-контрактів за сферами застосування; дослідити програмні засоби реалізації децентралізованих застосунків.* ***Методи дослідження.*** *Системний аналіз застосовано для вивчення архітектури мікромереж; порівняльний аналіз – для оцінювання ефективності алгоритмів консенсусу; класифікація – для групування смарт-контрактів. У практичній частині використано методи комп'ютерного моделювання та експериментальної перевірки: розроблення смарт-контракту мовою Solidity, тестування в середовищі Remix IDE й симуляція локальної блокчейн-мережі за допомогою інструментарію Hardhat.* ***Результати дослідження.*** *Систематизовано методологічні основи інтеграції блокчейну в мікромережі. Визначено, що для торгівлі енергією в межах локальних спільнот найбільш ефективними є гібридні або приватні моделі консенсусу. Розроблено та обґрунтовано класифікацію смарт-контрактів, що передбачає чотири рівні: торгівля енергією, моніторинг, розподілене управління й кібербезпека. Практичним результатом стала реалізація смарт-контракту EnergyTrading, який успішно автоматизує реєстрацію пропозицій та купівлю електроенергії, що підтверджено експериментом у локальному середовищі. Упровадження смарт-контрактів дає змогу створити надійну P2P-платформу для торгівлі електроенергією без посередників і водночас підвищити економічну ефективність для домогосподарств. Експериментально підтверджено працездатність механізму автоматизованих розрахунків. Крім цього, виявлено ключові виклики: обмежена масштабованість наявних блокчейн-рішень і необхідність удосконалення кіберзахисту від вразливостей у коді контрактів. Подальший розвиток потребує адаптації законодавчої бази й модернізації апаратної частини енергомереж.*

Ключові слова: *мікромережа; блокчейн; смарт-контракт; P2P-торгівля енергією; алгоритм консенсусу; Solidity; відновлювані джерела енергії; децентралізація.*

Бібліографічні описи / Bibliographic descriptions

Корнієнко Є. Д., Ляшенко О. С. Дослідження методологічних основ упровадження блокчейну й смарт-контрактів в електроенергетичних мікромережах. *Автоматизовані системи управління та прилади автоматики*. 2026. № 1 (188). С. 108–120. DOI: https://doi.org/10.30837/0135-1710.2026.188.108

Korniienko, Y., Liashenko, O. (2026), "A study of the methodological foundations for implementing blockchain and smart contracts in electric power microgrids", *Management Information System and Devices*, No. 1 (188), P. 108–120. DOI: https://doi.org/10.30837/0135-1710.2026.188.108