UDC: 004:004.75:004.67(045)
DOI: 10.18372/1990-5548.88.20969

**[1]Vitalii Zubok,**
**[2]Mykola Kondratenko**

# FORMULATING REQUIREMENTS FOR HYBRID DISTRIBUTED COMPUTING SYSTEMS: AN INFRASTRUCTURE PERSPECTIVE

G. E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine
E-mails: [1]vitalii.zubok@pimee.ua ORCID 0000-0002-6315-5259,
[2]mykola.kondratenko@pimee.ua ORCID 0009-0009-0979-2626

***Abstract*—***The article examines the role of modern computing architectures in enabling the digital transformation of the energy sector, particularly in the context of the development of decentralised electricity markets. The advantages and limitations of on-premises, cloud, and hybrid infrastructure solutions for building distributed, scalable computing systems are analysed. Based on this analysis, requirements for the communication and information system of interaction among participants in a decentralised electricity market are formulated. The key design principles of such a system are identified, including scalability, architectural unification, high availability, and fault tolerance. Particular attention is given to processing large data volumes, ensuring data sovereignty, integrating blockchain technologies and smart contracts, and using consensus mechanisms suitable for industrial systems. Requirements for network infrastructure, geographical distribution of computing nodes, and cyber-resilience are also considered, particularly in the context of cascading risk effects. The study demonstrates that a hybrid computing architecture provides the most balanced approach by combining control over critical infrastructure components with the flexibility and scalability of cloud technologies, thereby creating a technological foundation for a resilient communication and information system supporting a decentralised electricity market.*

**Keywords**—Communication and information system, cyber resilience, data sovereignty, decentralised electricity market, distributed computing, hybrid computing architecture, smart contracts, digital transformation of the energy sector.

## I. INTRODUCTION

New computing architectures play a crucial role in digital transformation processes, providing scalability, flexibility, and enhanced data processing efficiency. In particular, distributed computing leverages the combined resources of a large number of interconnected nodes to perform complex computing tasks that previously required centralised, expensive systems. This approach facilitates the processing of large volumes of data, supports the operation of intelligent services, and ensures the resilience of digital infrastructure against failures of individual components. In addition, distributed architectures underlie cloud and edge computing, enabling organisations to flexibly scale IT resources according to needs. As a result, new computing paradigms create a technological basis for the development of digital platforms, the Internet of Things and big data analytics, which, in turn, accelerate the transformation of economic and management processes. One of such processes is the transformation of the energy sector of Ukraine [1], [2].

The issues of this subject area include research into the development of decentralised markets and P2P contracts [3], problems of conflict-free data processing in distributed systems [4], and the possibilities and safety of using blockchain technologies [5].

The aim of the analysis presented in this article is to determine the advantages and disadvantages of modern infrastructure solutions for distributed scalable computing systems, as well as to formulate, on this basis, the requirements for an information and communication system to support interaction between participants in the decentralised electricity market.

## II. MODERN INFRASTRUCTURE SOLUTIONS FOR DISTRIBUTED, SCALABLE COMPUTING SYSTEMS

### *A. On-premise, cloud, and hybrid architecture*

For computing systems, there are two traditional architectural solutions. The first architecture is to deploy the system on the enterprise's own hardware and software. This can take place in the enterprise's own territory (on-premise) or in a specialised premises of the data centre service provider (datacentres). Such placement is called co-location. These options differ in risk, but the most important comparison will be with the second architectural solution: cloud computing.

Cloud computing is a way to access dynamically scalable external computing resources as a service provided via the Internet. The concept of cloud technologies is closely related to the concept of virtualisation of IT infrastructure (computing resources, data storage, telecommunications components), while the user does not need any special knowledge about this infrastructure or skills in managing virtualisation technologies [6]. A cloud system, or cloud computing technology system, is a model for providing "on-demand access" to a common pool of configurable computing resources that can be quickly provisioned and released with minimal operating costs. A cloud system refers to the computing components (hardware and software, infrastructure) that enable the delivery of cloud computing services, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

To determine the advantages and disadvantages of on-premises and cloud architectures in the face of existing threats, the following analysis of strengths and weaknesses is proposed.

### *B. Strong sides of on-premise computational infrastructure*

For many ICS owners, *control over sensitive Data* is a top priority. Data is stored, transmitted, and processed within an infrastructure fully controlled by the enterprise, and it is the enterprise's responsibility to develop and implement data protection policies.

On-premise infrastructure allows *for maximum customisation.* These systems often allow extensive customisation to suit an organisation's specific needs, offering flexibility to adapt to unique business processes.

When deploying a local system, it can be tightly integrated *with existing leg*acy systems and applications, ensuring seamless data flow and interaction within the organisation. Since the early 1990s and to this day, these problems and challenges have been inherent in various industries in developed states – from the banking sector to manufacturing [7].

Equally important is the regulatory impact. Companies operating in regulated industries may find it easier to maintain *compliance with industry norms and standards*. For example, certification of information protection systems that are processed in a third-party cloud will be more complex.

### *C. Weaknesses of on-premise infrastructure*

On-premises computing infrastructures always require significant *upfront costs to build*. Implementing an on-premises system typically requires significant upfront investment in hardware, software licenses, and infrastructure setup [8].

Businesses are responsible for ongoing maintenance, upgrades, and troubleshooting, which can be resource-intensive and require specialised IT professionals. As a result, they incur additional costs *for hardware maintenance*, *software* support and upgrades across their entire computing infrastructure.

Scaling a local system is a challenge. In the case of business growth, scaling may be inevitable, but requires the purchase of additional equipment and the expansion of infrastructure and prepared territory, an increase in the number of personnel. Therefore, scaling "physically" is difficult and expensive.

*The difficulty of remote access* is not the least factor. For security reasons, local systems have restrictions on remote access, especially from public networks. Providing secure remote access significantly expands the threat landscape. Conversely, not providing remote access limits the flexibility of participants and administrators, most critically affecting business continuity during crises.

### *D. Advantages of cloud infrastructure*

Cloud platforms and infrastructure are often considered *cost-effective*. The reason is they are paid for under a subscription model that depends on the set of available tools and the number of resources, including dynamic provisioning and resource accounting (e.g., Amazon Web Services). This approach reduces upfront costs and allows businesses to pay only for the resources they use. This makes cloud systems more cost-effective for small and medium-sized enterprises (SMEs).

Cloud systems *scale on demand*, without physically rebuilding infrastructure or requiring significant capital investments. Cloud systems and data centre service providers usually address communications and hardware issues effectively, so, in conjunction with scalability, clouds provide *high availability.*

Automatic updates of system software for infrastructure elements (e.g., host operating systems), as well as the costs of maintaining their operation, are, in principle, the responsibility of the cloud service provider.

### *E. Threats to cloud infrastructure*

Cloud infrastructure, to varying degrees, *poses a security threat to confidential business data* entrusted to third-party cloud providers. To a lesser extent, if the cloud service provider provides a “private cloud” service. In any case, this can cause problems with the adequacy of the data centre

service provider's level of protection and the risk of unauthorised access or data leakage [9].

For infrastructure users, there is *a reliance on an Internet connection* because there are no other access methods (such as dedicated rooms with workstations for external personnel) in the cloud.

There is an additional *supply chain risk*: cloud provider lock-in. Migration from one cloud provider to another is complex and time-consuming due to data portability issues and reliance on proprietary technologies, leading to vendor lock-in and reduced flexibility.

There is also a limitation associated with the lack of flexibility in configuring cloud computing resources. While cloud systems offer some flexibility in configuration and resource allocation, they may not support extensive customisation options compared to on-premise solutions, potentially limiting their suitability for computing systems with highly specialised requirements [10].

### *F. Threats to cascading effects*

Despite the development of cloud solutions, many companies still use on-premises solutions, particularly for enterprise resource planning (ERP) systems in business and for operational technologies in production. According to system owners, this is the best way to maintain control over sensitive data: storing, transmitting, and processing it within the enterprise's fully controlled infrastructure. But business continuity requirements require a review of priorities. However, the deployment of on-premise poses additional tasks to ensure the safe functioning of the system, which include, in particular, the tasks of increasing cyber resilience:

- providing autonomous power supply using modern high-capacity batteries or generators;
- geographical distribution of production and backup servers to avoid the impact of one area on another in the event of serious power outages;
- modification of disaster recovery procedures taking into account the recovery points in time and recovery points in data that are realistically achievable during long outages;
- deployment of monitoring and management systems that allow remote monitoring of the system and infrastructure status, even during power outages, to quickly respond to any problems and ensure optimal recovery times.

## III. Case Study: Formation of Requirements for a Decentralised Electricity Market Communication and Information System

### *A. Basic principles decentralized energy systems*

The basic principles that are embedded in the concept of new decentralised energy systems include distributed generation and digitalisation (digital transformation) [11].

Decentralisation is the process of redistributing part of centralised management (technological, organisational, and market) and developing distributed generation using renewable energy sources to provide electricity to consumers, primarily enterprises and critical infrastructure facilities, on whose operations the lives of communities depend. It enables the creation of new opportunities for decentralised electricity trade between producers and consumers (P2P) and increases the flexibility of the regional (local) energy system, including under military threats.

Digital transformation is the implementation of digital technologies (Smart Grid, Micro Grid, artificial intelligence, blockchain and smart contracts [12], cyber resilience [13], etc.) to optimise processes in the field of production, distribution, consumption and management of energy resources at the regional level. It enables increased efficiency, reduced losses in distribution networks, and greater stability of the regional (local) energy system

### *B. Description of participants, main processes, and nodes*

The flowchart in Fig. 1 demonstrates the structure of interaction between participants in the decentralised electricity market. The following participants are involved in it:

*1) Energy producers:* Solar panels, wind turbines, small power plants, energy storage.

*2) Energy consumers:* Enterprises, infrastructure facilities.

*3) Distribution System Operator (DSO):* Ensures physical balance.

*4) Blockchain platform:* Used to record transactions.

The following main processes occur in the decentralised electricity market system.

*1) Smart contract initialisation:* The manufacturer registers on the platform. Contract parameters (price, energy volume, delivery time) are defined.

*2) Data collection:* Producers and consumers send data about energy generation/consumption to the blockchain network. The data is recorded in smart contracts.

*3) Contract Execution:* The consumer confirms receipt of energy. The blockchain triggers automatic calculations and fund transfers.

*4) Transaction completion:* All data is recorded in blocks, forming a transparent transaction history.

These processes occur in the following nodes.

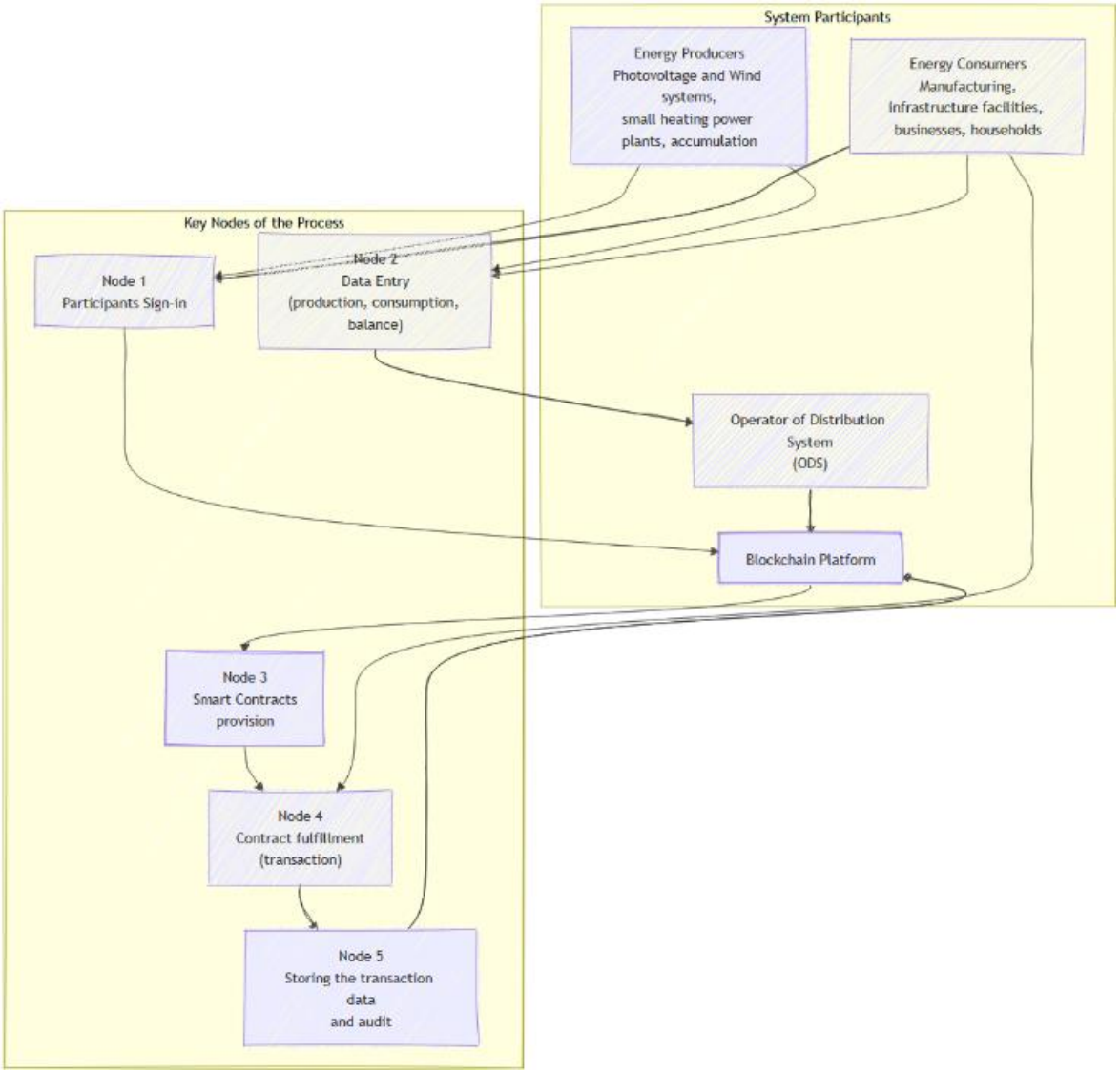


Fig. 1. Structure of interaction between participants in the decentralised electricity market

*Node 1: Participant Registration*. Participants connect to the blockchain.

*Node 2: Data input (generation, consumption, balance)*. Producers send data via Smart Grid to OSR.

*Node 3: Formation of smart contracts*. The terms of the contract are stored on the blockchain.

*Node 4: Contract execution (transaction)*. Transfer of energy and funds.

*Node 5: Information storage.* All actions are recorded for audit.

### *C. Functional and non-functional requirements*

Communication and information system for interaction between participants of the decentralized electricity market (hereinafter – ISDEM CIS) should provide unified means of describing objects, executing computational algorithms, system-wide software, installing and maintaining application and system software. The following requirements should be put forward for the software and technological support of ISDEM CIS:

- basing ISDEM CIS on modern solutions that will ensure long-term operation;
- unification of architectural elements ISDEM CIS;
- the ability of ISDEM CIS to scale by changing the number of architectural elements or their quantitative characteristics;
- functional distribution of application software taking into account the requirements of integrity, availability and confidentiality of information.

ISDEM CIS should handle tasks such as displaying and visualising information, logging, archiving, providing access to information, and transferring information to the next level. Given the number of parameters it will operate with, modern approaches are needed to ensure the performance of such tasks, which have been proven effective in

handling large volumes of data (or simply “big data”). The accumulation and storage of big data require modern, specialised infrastructure solutions. These solutions must meet the following basic requirements:

a) the system's performance and the maximum amount of information it stores should be scaled by increasing the number of typical nodes, storage devices, and using additional connections between them (the principle of horizontal scalability);

b) fault tolerance (or "high availability" – high availability) should allow the performance of functions without any significant consequences for solving the main production task in the event of a partial failure (failure of any typical element of the system or a certain group in accordance with the principle of high availability);

c) the system should be designed to optimize transmission distances and data volumes to be transmitted when scaling horizontally (data locality principle).

*D. Data sovereignty-related requirements*

ISDEM CIS will be designed as a national system, the sustainable functioning of which will affect the digital resilience of the nation, which consists in the continuity of critical services, the trust of individuals and legal entities (in particular, energy market participants) to digital tools, the ability of the economy to function in crisis conditions due to the reliability of electronic communications and digital services. At the same time, the landscape of geopolitical challenges requires the state and society to maintain control and autonomy in the digital sphere, ensuring independence from external forces in matters of technology, data, infrastructure and the rules of their use.

The practical implementation of digital sovereignty requires the government to have the ability to determine where and how the data of its citizens and organisations is stored, processed, and used, in other words, sovereignty of data. Sovereign data must be stored and processed in accordance with the laws of the state to which it belongs, even if physically located in cloud services or foreign data centres.

The ISDEM CIS architecture should be developed taking into account guarantees of compliance with national legislation, minimising the impact of external political or economic factors (including unfair economic competition), which may limit access to critical information or, conversely, disclose information as a result of loss of control over infrastructure or data.

*E. Requirements for the ISDEM CIS system-wide software*

The ISDEM CIS system-wide software should be designed and developed so as not to limit the range of parameters, analytical processes, information flows, the number of input sources, or the number of system users.

Maximum attention should be paid to scalability and the unification of system modules, since scaling is the key to addressing the problems inherent in any developing system.

Problems addressed by scaling:

- the need for shared and simultaneous use of resources and data;
- heterogeneity of resources and methods of their consolidation, which is due to the variety of equipment, deployed software, differences in use cases depending on the actions of personnel, region, etc.;
- resource dynamism in accordance with the volume of tasks and data;
- priority management for processes and users, the absence of which negatively affects processes that require "real-time" processing.

When designing a scalable system, attention should be paid to typical problems:

- the complexity of technical support for a single software system, which grows proportionally to the number of data sources or software components;
- difficulties arising when importing from software components and data sources from other places, which will increase as an increasing number of monitoring objects are included in the project;
- resource limitations on local components: with increasing computing demands, the limited capabilities of a local computing system can become a significant obstacle to progress in research;
- the growth in the number, complexity, and performance of local components, as well as requests for them, requires the reorganisation of components and improvement of connections between them again and again;
- the complexity of support that arises as the number of community members grows: the complexity of the model and the costs of its development and maintenance increase.

The ISDEM CIS must meet the requirements for increasing the amount of processed data and the speed of updates through horizontal scaling.

*F. Requirements for computing architecture for implementing smart contracts for a decentralised electricity market*

A computing system for processing smart contracts in a decentralised energy network must provide high performance, low latency, secure execution, and scalability, as well as integration with the energy infrastructure and redundancy

mechanisms. This is especially important in systems that must function continuously even during communication failures or external attacks.

Implementing blockchain technologies alongside smart contract execution mechanisms requires building a high-performance, scalable, and fault-tolerant computing infrastructure. In cloud environments, these requirements are realised through a combination of distributed computing nodes, flexible storage resources, and orchestration tools.

The combination of blockchain and cloud technologies in the implementation of smart contracts is based on a comprehensive architecture, where the interaction among computing nodes, the flexible use of fast and slow storage, geographical distribution, orchestration tools, and dynamic scaling ensure the stability, scalability, and high availability of the system.

*G. Computing nodes*

One key requirement is a distributed network of computing nodes that can act as full or light nodes. Full nodes (full nodes) must store a full copy of the blockchain and participate in transaction verification and smart contract execution. They are recommended for deployment at the fog or cloud infrastructure level. Lightweight nodes (lightweight nodes) can operate at the edge (the so-called edge level) – without storing the full chain, relying on trusted nodes to verify data. This allows blockchain to be integrated with Smart devices Grid without overload. Each computing node in the blockchain network must have sufficient computing power to execute consensus algorithms, verify transactions, and run smart contracts in a virtual machine (e.g., EVM in Ethereum). In the cloud, computing nodes can be located in different regions to reduce access delays and increase fault tolerance.

The information system should include a smart contract execution environment (e.g. Ethereum Virtual Machine or Hyperledger Chaincode). Node computing resources must ensure contract execution within acceptable latency (1–5 seconds), which is critical for managing real-time energy trading. In addition, support for safe execution mechanisms (sandbox), access control, and transaction logging for later auditing is required.

*H. Data storage subsystem*

For efficient operation, two categories of storage must be used. The first category is “fast storage” (NVMe SSD, in-memory storage) – for storing the so-called “data in motion”, i.e. active data, transaction logs, and temporary structures that are often used when processing smart contracts.

The second category is “slow storage” (on HDD or special archive storages at cloud providers) for the so-called “data in rest”, i.e. storage of historical blocks, backups and archives.

Full nodes should be equipped with high-speed solid-state drives (SSDs) to store the blockchain, which will grow in size over time. It is also necessary to implement storage optimization mechanisms, including pruning, archiving old data, and, if necessary, the use of distributed storage systems such as IPFS. This allows you to minimize local load while maintaining the immutability and availability of transactions.

*I. Influence of consensus mechanism on computational complexity*

Depending on the chosen blockchain model (public or private), the system must provide the necessary computational support for the corresponding consensus mechanism. In private or consortium networks, it is advisable to use energy-efficient algorithms – Proof-of-Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), Raft, etc. They enable fast transaction finalisation with minimal computational load, which is important given limited resources at the periphery [5].

*J. Network infrastructure and regional distribution*

The presence of computing nodes across different geographical regions allows for minimising transaction execution delays and ensuring continuous operation in the event of local failures. This requires low-latency communication channels between regions and load-balancing mechanisms. Since blockchain relies on distributed consensus, reliable, low-latency communication between nodes is critical. Support for peer-to-peer connections, secure tunnels (VPN), quality of service protocols and traffic encryption are mandatory. In fog architecture, it is necessary to provide for node autonomy in the event of a loss of connectivity to the cloud.

*K. Orchestration and automation*

The use of orchestration tools (e.g., Kubernetes, HashiCorp Nomad) enables centralised management of computing nodes' lifecycles, automatic deployment of new instances to execute smart contracts, and optimisation of resource allocation.

*L. Dynamic scaling*

Since the load on the blockchain network and smart contract processing can be uneven, the

computing infrastructure must support automatic scaling – both vertically (increasing node resources) and horizontally (adding new nodes to the pool). This allows you to optimize costs and maintain performance during peak periods. In addition, the system assumes a constant increase in the number of participants – active consumers, so its computing architecture must provide horizontal scaling. It is recommended to use sharding mechanisms, sidechains or segmentation of the network into clusters on a territorial or functional basis.

APIs and integration with power energy infrastructure. The information architecture should include API gateways for integration with SCADA systems, monitoring platforms and IoT devices. Support for OPC-UA, MQTT, REST protocols allow for the interaction of the blockchain system with external energy components, providing automation of data exchange and launching smart contracts based on actual consumption or generation indicators.

Security and compliance requirements. The system should include hardware security mechanisms, such as trusted modules (TPM) or hardware key protection modules (HSM), which provide cryptographic key storage and transaction signing. Support for modern cryptographic standards (SHA256, ECDSA, BLS) is a prerequisite for protecting information and preventing data compromise.

Processing smart contracts in a cloud environment requires implementing multi-layered security, including isolating execution environments, controlling access to fast and slow storage, and encrypting data in transit and at rest.

## IV. Conclusions And Further Discussion

The development of decentralised energy systems in modern conditions forms a new type of energy ecosystem, where digital technologies, management models and electricity market principles are integrated into a single information and communication infrastructure. Unlike traditional centralised energy solutions, a decentralised system requires completely different approaches to building a computing architecture, security, data processing and integration between participants. Within the framework of this study, the requirements for the information and communication system of a decentralised electricity market are formulated, and the technological solutions necessary for its implementation are substantiated.

The formulated requirements for the information and communication system of the decentralised electricity market are based on the principles of scalability, unification and fault tolerance. They determine the need to create a single software and technological environment capable of integrating heterogeneous data sources, processing large amounts of information in a near-real-time mode, and ensuring the high availability of services for all participants. Significant emphasis is placed on horizontal scaling, which allows increasing productivity and the volume of stored data by adding new nodes without a significant restructuring of the infrastructure. At the same time, the requirements for high availability allow continued operation in the event of failure of individual components, a critically important factor for the infrastructure that supports daily life in communities.

A special place is occupied by the issue of data sovereignty, which becomes strategically important amid geopolitical instability. For the national energy system, it is critically important that data be stored and processed in accordance with national legislation, and that control over the information infrastructure remain within the state's jurisdiction. Data sovereignty determines not only technical requirements, but also forms the requirements for choosing a deployment model - local, cloud or hybrid. The use of foreign cloud services, despite their high technological level, is associated with risks to accessibility and confidentiality, as well as potential geopolitical risks, while local infrastructure provides control but requires significant resources for scaling and support.

An essential element of the proposed architecture is the consideration of the features of blockchain technologies and smart contracts. The proposed division of storage into fast and slow allows optimising the operation of the system depending on the nature of the data – active or archival. The consensus mechanisms PoA, PBFT, and Raft significantly reduce computational costs compared to public blockchains, making them suitable for industrial use.

No less important is the analysis of the network infrastructure. The geographical distribution of nodes increases fault tolerance and resistance to regional failures, but at the same time imposes on the system the task of protecting communication channels, encrypting traffic, and maintaining the autonomous operation of fog and edge components in the event of a loss of connection to the cloud infrastructure.

An important component of the study is the comparison of on-premises, cloud, and hybrid architectures. Hybrid architectures are found to be the most balanced, combining control over critical components with the flexibility and scalability of cloud technologies.

A separate section is devoted to the analysis of risks of cascading effects arising from failures in local computing systems or network infrastructure. Providing autonomous power supply, geographical distribution of backup servers, updated disaster recovery procedures and implementation of comprehensive monitoring systems significantly increase overall resilience.

Summarising the conducted research, it can be stated that the formation of an information and communication system for a decentralised electricity market requires integrating modern technologies, adopting a thoughtful architectural design, and considering both technical and political factors. Despite the described difficulties in designing an optimal infrastructure, there are systems worldwide that operate with zero tolerance for downtime (so-called zero-downtime, ZDT). In addition to a reliable computing architecture that eliminates downtime longer than is acceptable to maintain business continuity, this requires careful consideration of the software development, implementation, operation, and update processes.

## V. ACKNOWLEDGMENTS

The research was conducted as part of the project "Development of Distributed Energy in the Context of the Ukrainian Electricity Market Using Digitalisation Technologies and Systems," implemented under the state budget program 'Support for Priority Scientific Research and Scientific-Technical (Experimental) Developments of National Importance' (CPCEL 6541230) at the National Academy of Sciences of Ukraine.

## REFERENCES

[1] S. Denysiuk, H. Bielokha "Decentralized Electricity Systems as Component Implementations of the 'Smart Grids' Concept," *System Research in Energy*, no. 4 (80), 2024 pp. 26–40, https://doi.org/10.15407/srenergy2024.04.026

[2] O. Sukhodolya "Principles of developing a new energy system of Ukraine", *Articles for National Institute of Strategic Studies. Mediacenter.* https://niss.gov.ua/sites/default/files/2026-01/principi-rozbudovi-energetiki-sayt.pdf

[3] V. Evdokimov, A. Polukhin, D. Tsvilii, Y. Lukashevych & O. Havva "Decentralized Energy Markets and P2P Contracts: New Opportunities for Automating Energy Exchange", *Grassroots Journal of Natural Resources*, 8(2), 2025, pp. 856–884. https://doi.org/10.33002/nr2581.6853.080240

[4] A. Prymushko, I. Puchko, M. Yaroshynskyi, D. Sinko, H. Kravtsov, & V. Artemchuk, "Efficient State Synchronization in Distributed Electrical Grid Systems Using Conflict-Free Replicated Data Types,". *IoT,* 6(1), 6, 2025. https://doi.org/10.3390/iot6010006

[5] A. Vykhlo, & L. Kovalchuk "Estimation of the Probability of Success of a Suppression Attack," *Theoretical and Applied Cybersecurity*, 7(1), pp. 65–70, 2025. https://doi.org/10.20535/tacs.2664-29132025.1.332340

[6] T. Erl, R. Puttini, & Z. Mahmood "Cloud computing: concepts, technology, & architecture," *Prentice Hall*. 2025. https://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/0133387526.pdf

[7] "Modernizing legacy systems in banking. How banks can succeed at core and app modernization". *Deloitte.* https://www.deloitte.com/us/en/Industries/financial-services/articles/modernizing-legacy-systems-in-banking.html

[8] "Banking IT Modernisation: The True Cost of Legacy Systems. A comprehensive analysis of total cost of ownership, modernisation strategies, and competitive advantages," *Digital Bank Expert*, https://digitalbankexpert.com/2025/08/the-true-cost-of-legacy-systems-a-deeper-dive-into-banking-it-modernisation

[9] D. Oluremi, R. Vallabhaneni, H. Lallie, M. Guglielmo, Caporale "Cloud Computing and Cybersecurity: Emerging Threats and Defense Mechanisms," *Researchgate. Cybersecurity, (2025),* https://tinyurl.com/CloudThreats2025

[10] E. Maniah, F. Abdurachman, Lumban Gaol, B. Soewito, "Survey on Threats and Risks in the Cloud Computing Environment," *Procedia Computer Science,* vol. 161, pp. 1325–1332, 2019. https://doi.org/10.1016/j.procs.2019.11.248

[11] H. Pudyncheva "Decarbonization, decentralization and digitalization – The key factors of modern energy sector," *Economics and business management*, vol. 71, 2021, https://doi.org/10.32843/bses.71-18

[12] V. Evdokimov, A. Kudin, V. Chikhladze, & V. Artemchuk, "A Blockchain Architecture for Hourly Electricity Rights and Yield Derivatives," *Preprints (2025)* https://doi.org/10.20944/preprints202512.0229.v1

[13] R. Drahuntsov, A. Symonov, O. Potenko, O. Dybach, and V. Zubok, "Cybersecurity Monitoring During Power Outages: Use Cases for Enhanced Infrastructure Observability and Potential Implications for NPP Combined Events," *Nuclear and Radiation Safety,* vol. 3(107), pp.17–29, 2025. https://doi.org/10.32918/nrs.2025.3(107).02

Received: February 28, 2026
Accepted: March 21, 2026
Published: April 18, 2026

**Zubok Vitalii.** ORCID 0000-0002-6315-5259. Doctor of Engineering. Senior Researcher.
G. E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine.
Education: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine, (1994).
Research interests: cybersecurity, complex networks, computer networks, resilience, topology.
Publications: over 120 papers.
E-mail: vitalii.zubok@pimee.ua

**Kondratenko Mykola.** ORCID 0009-0009-0979-2626. Postgraduate Student.
G. E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine
Education: Nizhyn Mykola Gogol State University, Nizhyn, Ukraine, (2018).
Research interests: blockchain technology, smart contracts, system analysis.
Publications: more than 10 papers.
E-mail: mykola.kondratenko@pimee.ua

**В. Ю. Зубок, М. С. Кондратенко. Формування вимог до гібридних розподілених обчислювальних систем: інфраструктурний підхід**

У статті досліджено роль сучасних обчислювальних архітектур у забезпеченні цифрової трансформації енергетичного сектору, зокрема в умовах формування децентралізованих ринків електроенергії. Проаналізовано переваги та обмеження локальних, хмарних і гібридних інфраструктурних рішень для побудови розподілених масштабованих обчислювальних систем. На основі проведеного аналізу сформульовано вимоги до інформаційно-комунікаційної системи взаємодії учасників децентралізованого ринку електроенергії. Визначено ключові принципи її побудови, зокрема масштабованість, уніфікацію архітектурних компонентів, високу доступність та стійкість до збоїв. Особливу увагу приділено питанням обробки великих обсягів даних, забезпечення суверенності даних, інтеграції блокчейн-технологій і смартконтрактів, а також використанню механізмів консенсусу, придатних для промислових систем. Розглянуто вимоги до мережевої інфраструктури, географічної розподіленості вузлів і забезпечення кіберстійкості системи, зокрема в контексті ризиків каскадних ефектів. Показано, що використання гібридної обчислювальної архітектури дозволяє поєднати контроль над критичними компонентами інфраструктури з гнучкістю та масштабованістю хмарних технологій, створюючи основу для побудови стійкої інформаційно-комунікаційної системи децентралізованого ринку електроенергії.

**Ключові слова:** комунікаційно-інформаційні системи, кіберстійкість, суверенність даних, децентралізований ринок електроенергії, розподілені обчислення, гібридна обчислювальна архітектура, смартконтракти, цифрова трансформація енергетики.

**Зубок Віталій Юрійович.** ORCID 0000-0002-6315-5259. Доктор технічних наук. Старший дослідник.
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, Київ, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, (1994).
Наукові інтереси: кібербезпека, складні мережі, комп'ютерні мережі, резильєнтність, топологія.
Публікації: понад 120 публікацій.
E-mail: vitalii.zubok@pimee.ua

**Кондратенко Микола Сергійович.** ORCID 0009-0009-0979-2626. Аспірант.
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, Київ, Україна.
Освіта: Ніжинський державний університет ім. М. В. Гоголя, Ніжин, Україна, (2018).
Наукові інтереси: технологія блокчейн, смарт-контракти, системний аналіз.
Публікації: понад 10 статей.
E-mail: mykola.kondratenko@pimee.ua