

# The Impact of Ethereum Node Service Centralization on the Security and Efficiency of Blockchain

Denis Sinkevich, Anton Anikin(✉), Alexey Chibrikov, and Dmitry Rak

Volgograd State Technical University, Volgograd, Russia
anton@anikin.name

**Abstract.** The purpose of this article is to analyze the impact of centralization of node services on the security and efficiency of smart contracts in the Ethereum network, taking into account the massive scale and importance of cloud services in modern blockchain architecture. A key aspect of this analysis is the use of relevant data and academic sources, including information from Ethernodes.org and publications published on sites such as MDPI, Ethereum.org, CoinDesk and CoinMarketCap. This research aims to identify the risks and benefits associated with centralization of node services in the context of cloud technologies and develop recommendations to minimize potential threats to the Ethereum blockchain system. In the course of achieving this goal, all necessary steps are performed, such as analyzing and studying the impact of cloud services on the availability, scalability, reliability and security of the Ethereum network, assessing issues related to governance and trust in decentralized networks. The analysis shows that the process of centralizing node services exposes the network to security and censorship risks. Despite the advantages of cloud platforms, such as affordable and fast scalability of the system and accessibility to the consumer, in order to preserve the basic idea of blockchain decentralization, it is necessary to increase the security of smart contracts and reduce the level of centralization, this article suggests techniques and solutions. The study analyzes the complexity of building a relationship between the basic principles of blockchain and the advantage of cloud technologies and offers recommendations to cloud service providers, network users and developers on how to find a balance between decentralization, efficiency and security.

**Keywords:** Blockchain · Ethereum · Smart contract · Cloud technologies

## 1 Introduction

Ethereum is an open and decentralized blockchain system (launched in 2015) offered a unique opportunity - the creation and execution of smart contracts. These contracts are some kind of programs that automatically fulfill the previously prescribed legal conditions avoiding the influence of interested third parties

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14815, pp. 214–225, 2024.
https://doi.org/10.1007/978-3-031-65154-0_13

after agreement. Due to this, the platform gained popularity and mass popularity among developers.

With the help of smart contracts, users can develop complex contract execution scenarios using code, without resorting to control from a third, possibly interested, party for their execution. This became possible due to the fact that the program code runs on the Ethereum network, where the results follow the basic principles in the blockchain. When such an architecture is implemented into the network, it guarantees the immutability of the terms of the contract, security and transparency [3,10].

The role of smart contracts in the Ethereum ecosystem is high. They have become the basis for the development and operation of many applications: decentralized financial services (DeFi), games, tokenized assets and others. Smart contracts automate the execution of transactions and agreements, providing a high degree of trust and reliability without the need to involve intermediaries [11–13].

The Ethereum blockchain platform is a powerful and high-performance platform for concluding smart contracts. It improves and modernizes business practices, data management, and application development in the digital world. This approach not only provides a secure and transparent environment for the execution of contracts, but also opens up new opportunities for creating complex decentralized systems that are less subject to control or management by third parties [2].

In recent times, blockchain platforms are being heavily influenced by cloud services, which are noticeably changing the behavior and development of these platforms, including Ethereum. The cloud computing model provides developers and enterprises with reliable computing resources, data storage capabilities, and a set of tools for development, testing, and deployment. This approach helps to reduce complexity and costs for many projects in the field of blockchain technology. Studying the aspects allows us to highlight several key points:

- Accessibility and scalability. Cloud services allow companies to develop their blockchain solutions or buy ready-made ones and adapt to changing needs without having to spend additional resources on long-term scaling of infrastructure or new equipment. This makes it easier to launch new projects and guarantees high availability and reliability of the network, since cloud platforms often provide distributed computing resources and data storage on a global scale.
- Simplify development and deployment. Cloud computing platforms offer a range of tools and services that facilitate the creation, testing and implementation of blockchain applications. Using the provided templates, developers can focus on creating targeted applications without worrying about the basic functionality.
- Increase efficiency and reduce costs. The development and implementation of blockchain applications using cloud services allows you to reduce the cost of purchasing and maintaining the necessary infrastructure. Moreover, there are many designers, thanks to which consumers can choose the best tariff plan for themselves.

– Potential Risks and Challenges: Despite the apparent advantages, the use of cloud services in blockchain infrastructure carries potential risks, especially related to centralization and security. Dependence on cloud providers can lead to vulnerabilities in the event of hacking of their systems or sudden shutdown of services. In addition, the centralization of nodes from a single cloud provider is more at risk of attacks, such as distributed denial-of-service (DDoS).

On the one hand, cloud services participate in the development and expansion of blockchain platforms - offering developers and companies a number of significant advantages. On the other hand, it is necessary to carefully analyze potential risks and develop strategies to minimize them in order to ensure the security and stability of blockchain systems.

The purpose of this article is to explore the disadvantages of using cloud services to service nodes on the Ethereum network. Special attention is paid to the security and effectiveness of smart contracts in the context of popularization of cloud technologies. It is necessary to identify potential risks and vulnerabilities that arise due to centralization and dependence on cloud providers.

## 2 Cloud Computing and Its Impact on Ethereum's Infrastructure: Analyzing Scalability, Security, and Centralization Challenges

Cloud computing is the concept of distributing various computing resources and services (such as servers, storage, databases, network components and software) over the Internet on a consumer basis. Thanks to this paradigm, enterprises do not need to invest in internal IT infrastructure to take advantage of reliable computing capabilities. Platform as a Service (PaaS), software as a Service (SaaS), and Infrastructure as a Service (IaaS) are just a few examples of several types of cloud services, each offering different levels of management, flexibility, and scalability.

The role of cloud computing in blockchain:

1. Flexibility and scalability: cloud services enable efficient scaling of blockchain systems, which allows them to be rapidly expanded by adding additional resources in response to growing demand. Because cloud solutions provide flexible resource management, enterprises can reduce costs while increasing productivity;
2. Cloud services simplify development and implementation by providing programmers with access to environments and tools for creating, testing and deploying blockchain applications. This reduces the technical barriers associated with the creation and implementation of new businesses, making blockchain technology available to a wider range of developers;
3. Reliability and availability - the use of cloud services can enhance the reliability and availability of blockchain systems. The distributed architecture of cloud platforms ensures a high level of fault tolerance and guarantees continuous operation of services even in the event of failures at individual nodes;

4. Security - despite concerns related to centralization and control by cloud service providers, many cloud platforms offer advanced security solutions. This includes data encryption, access and identity management, and regular security audits.

But even with all the advantages, the use of cloud computing in the blockchain also entails certain risks related to data security, dependence on specific service providers and potential vulnerability to centralized attacks [1]. It is very important to carefully assess these risks and develop strategies to mitigate them in order to fully exploit the potential of cloud technologies for the development and support blockchain infrastructure.

Centralization of node maintenance in the Ethereum network is a serious problem, as it contradicts the basic principles of security and decentralization of blockchain technology. Nodes are autonomous computers or servers that participate in the Ethereum blockchain, performing transactions and/or verifying blocks. When a significant portion of these nodes are supported by a small number of cloud service providers, centralization occurs. This raises concerns about network administration, security, and trust:

1. Distributed Denial of Service (DDoS) attacks. If most nodes are located in the infrastructure of several cloud providers, DDoS attacks on these providers can temporarily disable a significant part of the network;
2. Censorship of transactions. Because nodes are centralized, it is easier for cloud service providers working under external pressure to censor or block transactions;
3. A security breach. In centralized systems, the likelihood of data compromise and network manipulation increases due to the presence of individual points of failure.

The centralization of nodes also calls into question the principles of trust and management in the Ethereum network:

1. Dependency on cloud service providers. A strong reliance on a few cloud providers reduces the degree of decentralization and increases the risks associated with external management and control;
2. Reduced resistance to censorship. One of the primary objectives of blockchain is its resistance to censorship and external control. The centralization of nodes threatens this objective by simplifying the potential for blocking or restricting access to the network;
3. Loss of trust. An increase in centralization can undermine the network participants' trust, as one of the key advantages of blockchain over traditional financial systems is its decentralized nature.

The centralization of node maintenance in the Ethereum network poses a serious problem for the security, trust and sustainability of the ecosystem [4]. It is extremely important to look for strategies and solutions aimed at reducing the degree of centralization, for example, to encourage the deployment of nodes

within a diverse and distributed infrastructure. The development and application of such strategies will help preserve the fundamental principles of decentralization and security of the Ethereum blockchain, ensuring its long-term functioning and sustainability.

Analysis of the current state of Ethereum infrastructure.

Statistical analysis of the proportion of Ethereum nodes serviced through cloud platforms (2022–2024). The study used data from several sources, such as direct requests to Ethereum nodes and information received from large cloud service providers. The information was collected in order to find out how many nodes of the Ethereum network are currently in use in general, what proportion of nodes are hosted in cloud services such as Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) and others, and where these nodes are located.

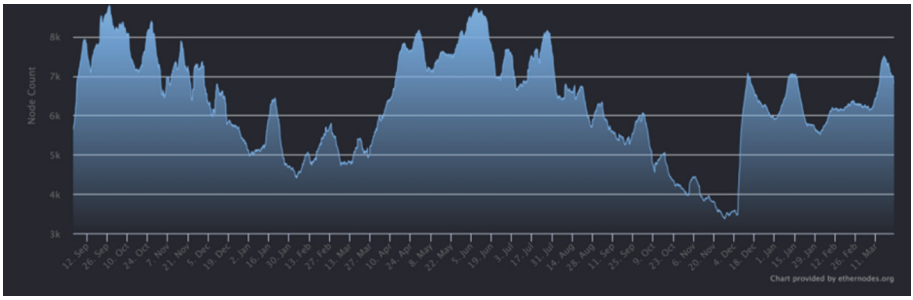


**Fig. 1.** Distribution of node count by time.

The analysis yielded the following conclusions:

1. The total number of active nodes in the Ethereum network fluctuated between 8700 and 3390 from 2022 to 2024, and as of March 2024, it returned to the figures of September 2022 - the moment of the network's transition to PoS (Fig. 1) [5].
2. The share of nodes on cloud platforms in 2022 accounted for approximately 60% of all Ethereum nodes, with AWS dominating at 40%, followed by GCP at 12% and Azure at 8%. By 2023, there was a slight increase to 65%, indicating a continuing trend towards centralization. In 2024, the proportion of cloud-hosted nodes decreased to 47% (Fig. 2), which may suggest the beginning of distribution and diversification of infrastructure among developers and network users [7].
   The diversity of cloud providers (Fig. 3) and the significant proportion of non-cloud nodes highlight the move towards diversification and distribution of the Ethereum infrastructure [7].
3. Geographic Distribution. Nodes situated on cloud platforms were predominantly concentrated in North America and Europe (Fig. 4), highlighting the

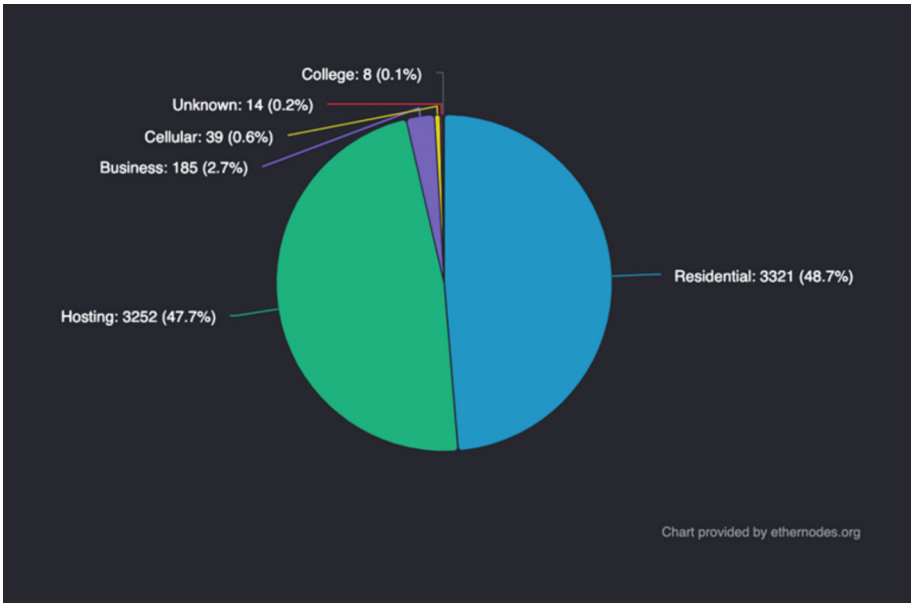


**Fig. 2.** Distribution of nodes by hosting type.

geopolitical and economic factors influencing the distribution of blockchain infrastructure [6].

Statistics show that a significant percentage of Etherium nodes are hosted in cloud services, which contributes to centralization. The situation may improve in 2024 if there is a slight trend towards decentralization, but there are still significant threats to network security and reliability when using large cloud providers. These results highlight the need for additional research and strategies to promote more dispersed and decentralized node hosting. This may include improving the availability and usability of nodes on personal computers and in small data centers, as well as developing tools and incentives for deploying local nodes.

As shown, a significant part of the Ethereum nodes are hosted on the internal servers of well-known cloud providers. The centralization of nodes affects the structure and functionality of the network, which raises security concerns and threatens the concept of decentralization underlying blockchain technology. One of the main security concerns is that any flaws or failures in cloud services can have far-reaching consequences for the Ethereum network as a whole. A careful strategy is required to reduce the degree of centralization and the associated security risks:

1. Expanding the range of cloud service providers. Encouraging the installation of nodes on other cloud platforms, such as standalone small cloud services;

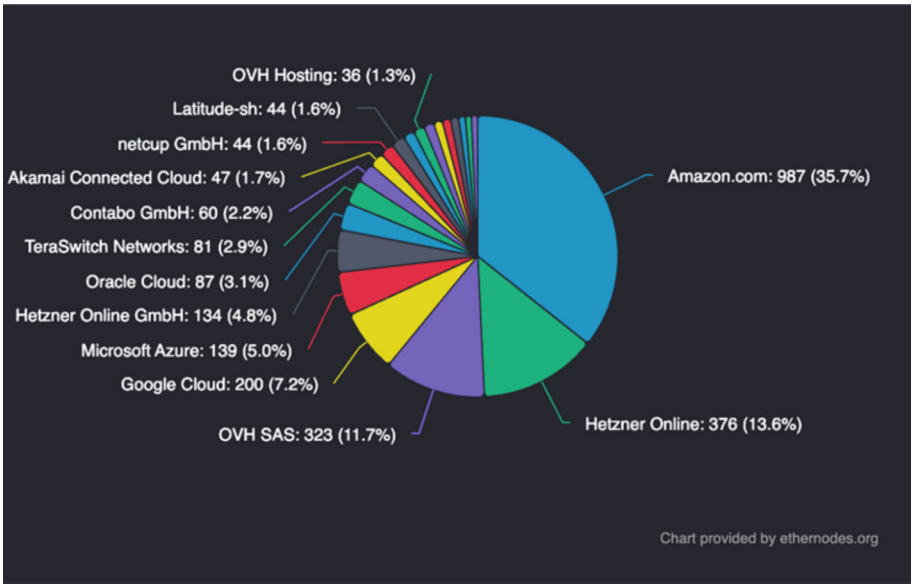


**Fig. 3.** Distribution of nodes across cloud services.

2. Deployment of local nodes. Encouraging local node deployment by network users and developers to reduce reliance on centralized cloud infrastructures;
3. Enhancing security measures. Implementing advanced security measures, including encryption, authentication, and regular audits, to reduce the vulnerabilities of nodes hosted on cloud platforms;
4. Regulatory support and standardization. Developing standards and regulatory frameworks to ensure the security and resilience of cloud services used for maintaining blockchain infrastructure.

Reducing the level of centralization in the Ethereum network and improving its security require joint efforts from the community, developers, and cloud providers. Maintaining decentralization not only contributes to the networks security and resilience but also ensures adherence to its fundamental principles.

## 3 The Block Censorship Problem in Ethereum and the Role of Flashbots

In Ethereum the ability of some parties, such as miners or validators, to choose which transactions to reject is known as blocking censorship. This possibility raises questions about the transparency and fairness of the Ethereum network, especially in light of the decentralized nature of blockchain technology; One of the key players in this scene is Flashbots, a research and development company whose goal is to prevent the centralization risks associated with MEV, mitigate

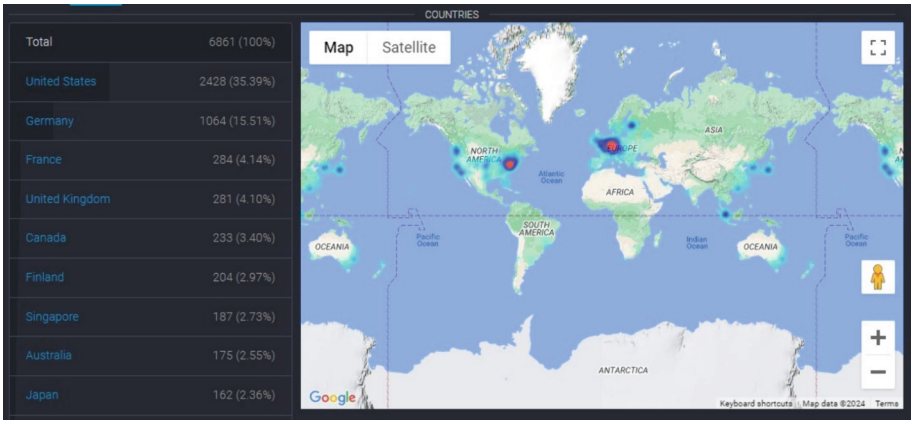


**Fig. 4.** Geography of node distribution.

the negative effects of existing mining (MEV) strategies (such as gas auction wars, which can lead to the strangulation of the network).

Flashbots introduced MEV-Boost [8], a protocol that allows validators to outsource the construction of blocks to specialized builders, which include Flashbots and others, in a sealed-bid auction format. While this system was designed to make the MEV extraction process more efficient and reduce network congestion, it inadvertently introduced a potential vector for censorship, especially concerning transactions associated with certain protocols or wallets.

A significant portion of Ethereum blocks processed with MEV-Boost is attributed to flashbots. The obtained data suggests that a significant portion of transactions in Ethereum can and has been censored. So the situation in 2022 was critical, the share of censored blocks amounted to 80% (Fig. 5). This high level of censorship raises critical questions about the integrity and censorship-resistant stability of the Ethereum network. It is important to realize that although Flash bots aim to improve network efficiency and reduce MEV issues, but the concentration of power in a few blockchain builders can lead to censorship vulnerabilities [9].

The central role of flashbots in block production and related censorship issues highlight the contradiction between improving the effectiveness of specialized MEV strategies and the fundamental principles of decentralization and anti-censorship in Ethereum. Depending on a limited number of block developers, even with the intention of optimizing MEV extraction, can lead to a scenario in which transactions are excluded based on criteria set by several organizations, thereby jeopardizing the open and non-permissive nature of the network. In addition, the current situation sheds light on the broader problem of reconciling the technical and economic optimization provided by solutions such as flashbots with the ethical and philosophical foundations of blockchain technology. As Ethereum continues to evolve, especially with its transition to Proof of Stake - (PoS) and

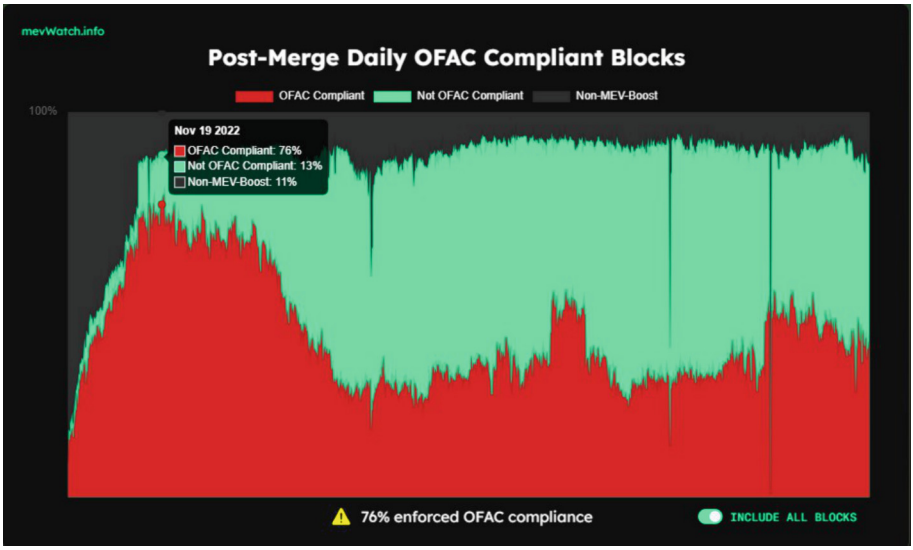


**Fig. 5.** Percentage of censored blocks 2022

increased focus on scalability and efficiency, the community faces an important challenge to address the issues of centralization and censorship.

To solve the block censorship problem by taking advantage of flash bots and similar MEV-related innovations, several strategies can be considered:

1. Diversification of block developers. Encouraging a wider range of participants to participate in the development of blocks can help reduce the risks of censorship and centralization. This includes encouraging small operators and ensuring transparency and fairness in the selection process for block developers.
2. Transparent censorship policy. Implementing clear guidelines and transparency measures regarding the reasons for excluding transactions can help maintain trust in the ecosystem. This transparency should extend to the criteria used by blockchain developers to censor transactions.
3. Supervision and management by the community. Creating mechanisms for public oversight and contributing to the practice of MEV extraction and block creation can enhance accountability. This may include management proposals and voting procedures that allow stakeholders to voice their concerns and influence the direction of MEV-related development.
4. Technical solutions to counter censorship. Research and development of technical solutions that make it difficult or economically impractical to censor certain transactions or types of transactions can provide better protection against censorship.

Thanks to the aforementioned methods, the share of censored blocks has begun to decrease. As of March 2024, the share of such blocks is around 50%

(Fig. 6), which is almost twice as low as in 2022 [9]. This indicates that society is striving to return to one of the fundamental principles of blockchain - decentralization.

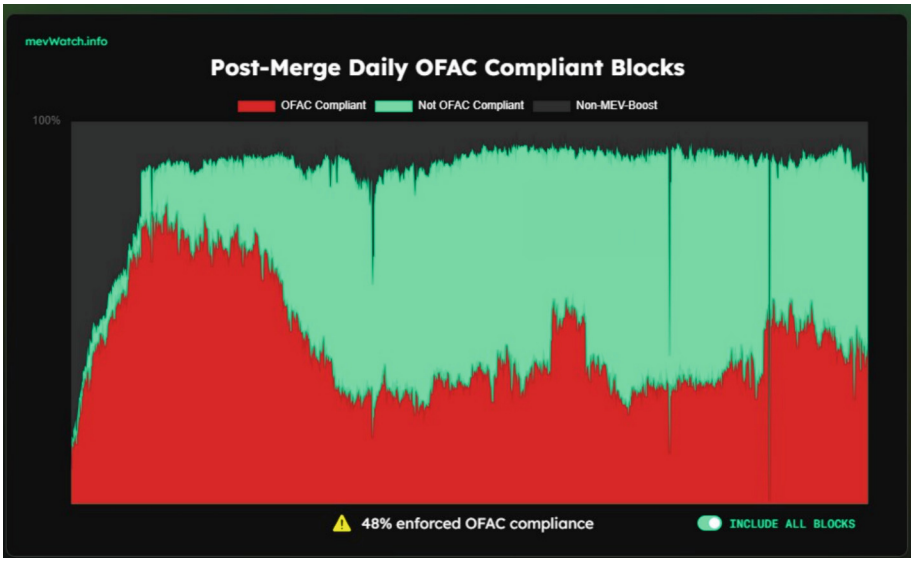


**Fig. 6.** Percentage of censored blocks 2024

## 4 Conclusion

This research shows that hosting blockchain nodes on cloud platforms significantly increases the security and transparency risks of smart contracts, making them more vulnerable to cyber-attacks, data leaks, and third-party interference. This paper analyzes the impact of the centralization process on the security, efficiency, and transparency of smart contracts hosted on the Ethereum network. As a result, the data obtained demonstrates the problem of violation of one of the fundamental principles of blockchain technology - decentralisation. The following conclusions can be drawn:

1. Impact on performance parameters. The analysis revealed that using centralised cloud services can have a negative impact on transaction execution time and cost on the Ethereum blockchain, which affects overall network performance.
2. Security. The study found that centralisation increases the security risk of smart contracts, exposing them more privately to cyberattacks, data breaches and third-party interference.

3. Decentralisation. The process of centralising the maintenance of blockchain platform nodes contradicts one of the main approaches of the technology, compromising its reliability and openness.

The results of this research work reflect the need to move away from the massive use of cloud servers, which is a centralised service model to a more decentralised one:

1. Development of new technological solutions. Introducing innovations that aim to simplify the process of building proprietary platforms, including improved deployment and management protocols that will entail decentralisation of nodes.
2. Encouraging decentralisation. There is a need to improve the implementation of economic mechanisms and technical solutions that will explicitly encourage platform members to use their own decentralised nodes.
3. Increase the inflation of blockchain platforms. Increase the quantity and quality of information about the benefits of decentralisation and the risks of centralisation, which will generate ideas to support the principle of decentralisation.

Decentralisation is not just a technical challenge, it is an important aspect on which blockchain systems are based. By adhering to this principle and moving to more decentralised service models, openness, transparency and trustworthiness can be strengthened in the system.

The realization of this transformation requires collective efforts from researchers, developers, and users to explore and implement innovative solutions that contribute to genuine decentralization.

## References

1. CoinMarketCap. A Deep Dive Into Infrastructure Centralization in Ethereum. https://coinmarketcap.com/academy/article/a-deep-dive-into-infrastructure-centralization-in-ethereum
2. Ethereum. Nodes and Clients. https://ethereum.org/en/developers/docs/nodes-and-clients/
3. Ethereum. Security Considerations for Smart Contracts. https://ethereum.org/en/developers/docs/smart-contracts/security/
4. CoinDesk. ETH May Already Be Showcasing Increased Signs of Centralization (2022). https://www.coindesk.com/tech/2022/09/15/eth-may-already-be-showcasing-increased-signs-of-centralization/
5. Ethernodes. Ethereum Node History (2024). https://ethernodes.org/history
6. Ethernodes. Ethereum Nodes Geographic Distribution (2024). https://ethernodes.org/countries
7. Ethernodes. Network Types (2024). https://ethernodes.org/network-types
8. MEV-Boost (2024). https://github.com/flashbots/mev-boost
9. MEV Watch. Post-Merge Daily OFAC Compliant Blocks (2024). https://www.mevwatch.info/

10. Dostov, V., Krivoruchko, S., Shust, P., Titov, V.: Are digital signatures in blockchain functionally equivalent to handwritten signatures? In: Gervasi, O., et al. (eds.) Computational Science and Its Applications - ICCSA 2023 Workshops - Athens, Greece, July 3–6, 2023, Proceedings, Part I. Lecture Notes in Computer Science, vol. 14104, pp. 527–537. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-37105-9_35
11. Sinkevich, D., Anikin, A., Smirnov, V.: Embracing Blockchain technology in logistics. In: Kabassi, K., Mylonas, P., Caro, J. (eds.) NiDS 2023. LNCS, vol. 784, pp. 127–133. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-44146-2_13
12. Sychev, O., Denisov, M., Anikin, A.: Verifying algorithm traces and fault reason determining using ontology reasoning. In: Taylor, K.L., Gonçalves, R., Lécué, F., Yan, J. (eds.) Proceedings of the ISWC 2020 Demos and Industry Tracks: From Novel Ideas to Industrial Practice co-located with 19th International Semantic Web Conference (ISWC 2020), Globally online, November 1-6, 2020 (UTC). CEUR Workshop Proceedings, vol. 2721, pp. 49–54. CEUR-WS.org (2020). http://ceur-ws.org/Vol-2721/paper495.pdf
13. Zhou, H., Milani Fard, A., Makanju, A.: The state of Ethereum smart contracts security: vulnerabilities, countermeasures, and tool support. J. Cybersecur. Priv. **2**(2), 358–378 (2022)