UDC 004.67
DOI https://doi.org/10.32782/tnv-tech.2024.5.12

APPLICATION OF HYBRID FEDERATED LEARNING MODELS INTEGRATING BLOCKCHAIN AND MACHINE LEARNING

Tsudzenko Yu. Ye. *– Postgraduate Student at the Department of System Design of the Ivan Franko National University of Lviv*
ORCID ID: 0009-0005-9316-7292

Mysiuk I. V. *– Postgraduate Student at the Department of System Design of the Ivan Franko National University of Lviv*
ORCID ID: 0000-0002-3641-4518
Scopus-Author ID: 58178909800

Mysiuk R. V. *– PhD, Lecturer at the Department of System Design of the Ivan Franko National University of Lviv*
ORCID ID: 0000-0002-7843-7646
Scopus-Author ID: 57939883600
Web of Science ID: GSE-0471-2022

The article explores a promising combination of blockchain technologies and Federated Learning-based machine learning to create hybrid models capable of transforming data mining in social networks through increased security, autonomy, and efficiency of data management. Blockchain provides a decentralized and secure environment for storing and transmitting information, which is especially important in the face of increasing requirements for the privacy and reliability of data in social networks. In turn, machine learning, which requires large amounts of reliable data to accurately predict and analyze, can take advantage of secure blockchain-based platforms to generate highly efficient models. The key aspects of the implementation of hybrid models are described, such as ensuring the confidentiality of user data, the scalability of the blockchain, and the complexity of integrating both technologies. Successful implementation of such systems can improve the efficiency and security of social media data analysis processes, creating new opportunities for innovation, improving content personalization, and providing better protection against manipulation. Thus, the study emphasizes that these approaches can significantly improve traditional methods of data analysis, making social networks safer and more adapted to the needs of modern users. The developed system allows you to evaluate the interaction between the user and the global machine learning model and the blockchain model. In addition, the collected metrics, namely: load reduction factor, estimation of network bandwidth utilization, blockchain processing time coefficient, allow you to evaluate the application of a hybrid model using blockchain technology using machine learning. A comparison of the load of the centralized and decentralized systems in accordance with the resource capacity of a personal computer is analyzed.

Key words: *blockchain, data analysis, decentralization, social networks.*

Цудзенко Ю. Є., Мисюк І. В., Мисюк Р. В. Застосування гібридних моделей федеративного навчання з інтеграцією блокчейну та методів машинного навчання

У статті досліджується перспективне поєднання технологій блокчейну та машинного навчання на основі Federated Learning для створення гібридних моделей, здатних трансформувати інтелектуальний аналіз даних у соціальних мережах завдяки підвищеній безпеці, автономності та ефективності управління даними. Блокчейн забезпечує децентралізоване та захищене середовище для зберігання та передачі інформації, що особливо важливо в умовах зростаючих вимог до конфіденційності й надійності даних у соціальних мережах. У свою чергу, машинне навчання, яке потребує великих обсягів достовірних даних для точного прогнозування та аналізу, може скористатися безпечними платформами на основі блокчейну для створення високоефективних моделей. Описано ключові аспекти впровадження гібридних моделей, таких як забезпечення конфіденційності даних користувачів, масштабованість блокчейну та складність інтеграції обох технологій. Успішна *реалізація таких систем може підвищити ефективність і безпеку процесів аналізу даних у соціальних мережах, створюючи нові можливості для інновацій, поліпшення персоналізації контенту та забезпечення кращого захисту від маніпуляцій. Таким чином, проведене дослідження підкреслює, що ці підходи можуть значно вдосконалити традиційні методи аналізу даних, зробивши соціальні мережі безпечнішими й адаптованими до потреб сучасних користувачів. Розроблена система дозволяє оцінити взаємодію між користувачем і глобальною моделлю машинного навчання та моделлю блокчейну. Крім того, зібрані метрики, а саме: коефіцієнт зменшення навантаження, оцінка використання пропускної здатності мережі, час обробки блокчейну коефіцієнт, дозволяють оцінити застосування гібридної моделі із застосування технології блокчейну використовуючи машинне навчання. Проаналізовано порівняння навантаженості централізованої та децентралізованої системи відповідно ресурсоспроможності персонального комп’ютера.*

Ключові слова: *блокчейн, аналіз даних, децентралізація, соціальні мережі.*

Introduction. Modern social media platforms have become an integral part of the global information environment, where users actively interact, exchange information, and shape public opinion. However, the growing influence of social media on society is accompanied by a number of challenges, including issues related to security, privacy, and content verification. The spread of fake news, fake accounts, and automated bots poses serious threats to users and trust in these platforms. Moreover, privacy violations, particularly through the collection and use of personal data without adequate control, remain one of the key problems faced by modern internet platforms.

In this context, traditional approaches to ensuring security and content verification based on centralized systems prove to be insufficiently effective. Blockchain technology, with its properties of decentralization, transparency, and immutability of data, offers new opportunities for creating more secure and reliable platforms. The use of blockchain in combination with machine learning methods, particularly algorithms for detecting anomalous activity and automatic content analysis, can significantly enhance the effectiveness of addressing the issues arising in social media.

The use of blockchain technology in combination with a Federated Learning model allows for the avoidance of third-party interference in the process of data processing and analysis. Federated Learning enables training machine learning models without the need to transfer raw data to centralized servers, keeping the data stored locally on users' devices. This ensures privacy, as personal data does not leave the boundaries of local devices.

In the context of systems combining blockchain with Federated Learning for data analysis in social media, blockchain serves as a decentralized platform to ensure the security, transparency, and immutability of machine learning model parameters. In environments where user privacy and data protection are paramount, blockchain ensures that all changes and updates to the model are authentic and verifiable, increasing trust in the learning outcomes.

One of the key roles of blockchain is ensuring data immutability. All contributions from individual devices are recorded as blocks in the chain, preserving the history of model changes. This means that all model updates are viewable and cannot be altered without a trace. This approach allows for tracking the sources and chronology of model parameters, creating a consistent and secure chain of updates.

The transparency and trust provided by blockchain are significant advantages for social media platforms aiming to handle user behavioral data correctly. Thanks to blockchain, all participants in the system can verify contributions to the model, which enhances trust in the learning and data processing results. In social media, this ensures transparency in data processing and protects against manipulation.

Furthermore, the decentralized structure of blockchain prevents unauthorized changes during the model training process. Any modifications or updates to the parameters require approval from the majority of nodes in the network, ensuring the system's resilience to external interference and maintaining the integrity of the model.

Blockchain also contributes to privacy protection by allowing only the updated model parameters to be stored, without the need to transmit raw user data. This reduces the risks associated with personal data breaches and complies with modern privacy requirements.

The aim of the study. This article presents the results of a study on the use of blockchain technology in combination with the Federated Learning model. The described combination allows for avoiding third-party interference in the process of data processing and analysis. Federated Learning enables training machine learning models without the need to transfer raw data to centralized servers, keeping the data stored locally on users' devices. This ensures privacy, as personal data does not leave the boundaries of local devices.

Related work. Hybrid models of federated learning based on blockchain and machine learning differ from the research presented so far in that they aim to integrate machine learning algorithms directly into the federated learning process. While traditional studies primarily focus on using blockchain for ensuring transparency, security, and decentralization, hybrid models offer a deeper interaction between these technologies.

In particular, previous research emphasizes the technical integration of blockchain with federated learning, focusing on addressing issues of scalability, privacy, and data exchange efficiency. Hybrid models, on the other hand, leverage machine learning capabilities to optimize the performance of the entire system, such as dynamically distributing tasks between nodes, predicting workloads, or automatically detecting anomalies.

Furthermore, hybrid models place a strong emphasis on practical applications, offering solutions for complex real-world scenarios such as medical diagnostics, smart cities, or financial technologies. They enable high performance through the flexible integration of modern machine learning algorithms with the advantages of blockchain, significantly expanding their capabilities compared to traditional approaches.

Blockchain technologies have become an important tool for ensuring transparency, security, and decentralization across many fields, from finance to data management. Many studies [1, 2] highlight the potential of blockchain to ensure the immutability of records, making it ideal for storing and verifying data, particularly in distributed systems. However, for blockchain to be used in real-world applications involving large volumes of data, scalability and transaction processing speed issues must be addressed [3]. One approach to solving these problems is the integration of blockchain with other technologies, such as machine learning.

Federated learning, introduced by Google in 2016 [4], is a promising technique for training machine learning models on distributed data without moving the data to a central repository. This allows for maintaining data privacy and minimizing the risk of leaks. Federated learning is used to create models that are trained on local devices (such as smartphones, sensors, etc.) and then aggregated to improve the global model. However, as studies [5] show, such a system faces challenges, including the efficient aggregation of models and ensuring accuracy based on limited local data.

Recent research focuses on combining blockchain technologies and Federated Learning to improve security, privacy, and scalability. Blockchain can be used to verify and store model updates, ensuring transparency and traceability of changes during the training process. In studies [6, 7], the use of blockchain for storing model parameters, such as weights, has been proposed, allowing for the distribution and updating of models without centralized control, while also enhancing resilience to attacks. Additionally, the combination of blockchain with Federated Learning minimizes the risks of data and model manipulation, as each transaction involving model updates is immutable and transparent.

Intelligent data analysis, which includes methods of machine learning, deep learning, and statistical analysis, is also actively applied in the context of blockchain systems. Particularly promising are approaches that combine data distribution with intelligent analysis for automatic anomaly detection and trend forecasting in large datasets [8]. This analysis can be performed both on local devices and in a distributed network, which helps reduce latency and improve prediction accuracy.

A comprehensive study on the integration of blockchain technologies and federated learning [9] systematically analyzes existing approaches and examines the main technical challenges, including ensuring privacy, computational efficiency, and scalability. This research helps to better understand the key use cases of these technologies across different industries.

The paper [10] provides a detailed analysis of solutions combining blockchain technologies and federated learning, focusing on architectures, algorithms, and security methods, as well as energy consumption and data storage efficiency.

The integration of these technologies in the context of edge computing is described in [11], highlighting the advantages for distributed systems and proposing solutions to address issues related to computational resources and data transmission delays.

Similarly, in articles [12], the use of blockchain technologies in federated learning for Internet of Things (IoT) security is discussed, particularly focusing on ensuring privacy and protection against attacks, as well as secure data exchange between IoT network nodes.

The research [13] also reviews the literature on blockchain integration in federated learning, emphasizing security and challenges related to attack resilience.

The article [14], which focuses on the integration of blockchain and federated learning in IoT networks for transportation systems, highlights data protection, reduction of latency, and improvement in system efficiency. Traditional aspects of blockchain usage are described in [15].

Presentation of the main research material. Regarding the methodological approach for integrating blockchain technology with Federated Learning and intelligent data analysis, the main stages, system components, and algorithms used to ensure security, privacy, and efficiency in data processing are explained.

The system consists of three main components: local devices, the global model, and the blockchain network. Each component plays a crucial role in ensuring decentralized data processing, model training, and the storage of updates. The system model is shown in Fig. 1.

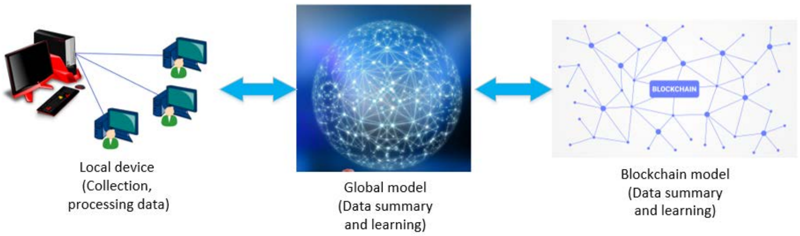

Fig. 1. Hybrid system architecture with blockchain technology and Federated learning

Local devices refer to the fact that each user has a mobile device or sensor that collects data locally, allowing for processing without the need to transmit data to centralized servers. These data may include user behavior metrics, environmental parameters, biometric data, or other types of input data, depending directly on the application context.

The machine learning model (local) operates on each device, processing the collected data without the need to send it to a centralized database. Models can be updated locally, where only the parameters (model weights, gradients) are transmitted, reducing the network load and ensuring a high level of privacy.

The global model is the result of combining the parameters of models sent from the local devices. This allows for an improved model based on collective learning, which aggregates knowledge from various sources. The global model is updated and sends new parameters back to the local devices for further training.

To ensure transparency, verification, and immutability of model parameters, blockchain is used. The model parameters sent from local devices are stored on the blockchain, where each record is immutable and open for verification, preventing manipulation and ensuring no third-party interference.

The system operates using a multi-step approach, ensuring secure collection, processing, and exchange of data between local devices and the global model with the use of blockchain. A local device, such as a smartphone or sensor, collects data about user behavior or environmental information and processes it directly on the device. At this stage, a local machine learning model analyzes the data and improves without the need to transmit raw data to a centralized database.

To improve the global model, the local device only sends updated parameters, such as model weights or gradients. These parameters are sent to the blockchain, where they are verified and stored in a secure environment. These data are then used to aggregate updates from various devices, allowing the global model to be enhanced. The updated parameters of the global model are returned to the local devices, ensuring the system adapts to new conditions and improves efficiency. This approach ensures confidentiality, transparency, and data security while maintaining high system performance.

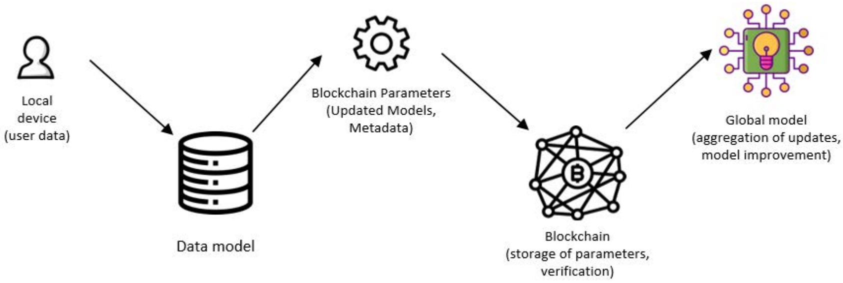

Fig. 2. Data Processing and Model Update Flow in Federated Learning with Blockchain Integration

In the first stage, as shown in Fig. 2, the local device collects user data and sends it for processing, while the data is processed locally, without the need for centralized access. This helps maintain confidentiality, as the data never leaves the device. The local model on the device processes this data and generates updates, which may include changes in model parameters, such as weights or gradients, but not the actual user data.

These updated parameters are then sent to the blockchain, where they are stored and verified.

In this case, blockchain ensures that the transmitted parameters are correct and belong to specific devices, which enhances transparency and security in the system. The updated parameters are then incorporated into the global machine learning model, which integrates them to improve accuracy and adaptability. After this, local devices receive the newly updated parameters from the global model, allowing them to continue training or use the model for further operations.

Thus, this approach ensures data confidentiality, as only model parameters are transmitted at all stages, not the users' actual data. This helps maintain security and confidentiality while simultaneously improving the model's effectiveness through aggregation from various local devices.

Hybrid models that combine these two technologies provide a powerful platform for addressing issues arising from large volumes of data and the complexity of verifying users and content in real-time. Blockchain can be used for data recording and verification, while machine learning helps detect anomalies. This approach ensures a higher level of protection for users' personal information, increases trust in content, and reduces risks related to fake accounts, bots, and fake news.

However, the implementation of hybrid models based on blockchain and machine learning requires a deep understanding of both technological and ethical aspects. Specifically, issues related to the effective integration of different systems need to be addressed, ensuring data confidentiality, protection against abuse, and maintaining transparency in decision-making processes. Therefore, the relevance of researching the effectiveness of such hybrid approaches is extremely high, as they have the potential to transform the paradigm of security and trust in social media ecosystems.

Enhancing privacy and data security: The use of Federated Learning (FL) combined with blockchain significantly improves privacy levels and protects user data from leakage and tampering. This can be measured by the number of potential attack vectors detected.

Blockchain combined with FL allows the system to scale without compromising its security. This can be evaluated by measuring latency time as the number of participants increases. The system is resilient to manipulation and attacks by malicious actors due to the protective mechanisms embedded in the blockchain and machine learning algorithms. This can be tested by evaluating the system under various types of attacks.

Thanks to decentralization, the system avoids overloading central servers, as computations are performed at the end-user level. This can be measured by monitoring central server usage. All tests were conducted using a dataset taken from the YouTube social network. The hardware used for the experiment had the following parameters: Intel Core i5 processor, 32 GB RAM, Nvidia 1050ti graphics card. In the figure, a comparison is shown between the performance of the centralized system and the hybrid system. The results indicate the system's CPU load, memory usage, and network usage. With the hybrid system, resource usage is significantly reduced. The formula for calculating the reduction coefficient of the load is:

$$Load\ reduction\ coefficient = \frac{load_{old-}\ Load_{new}}{Load_{new}}$$

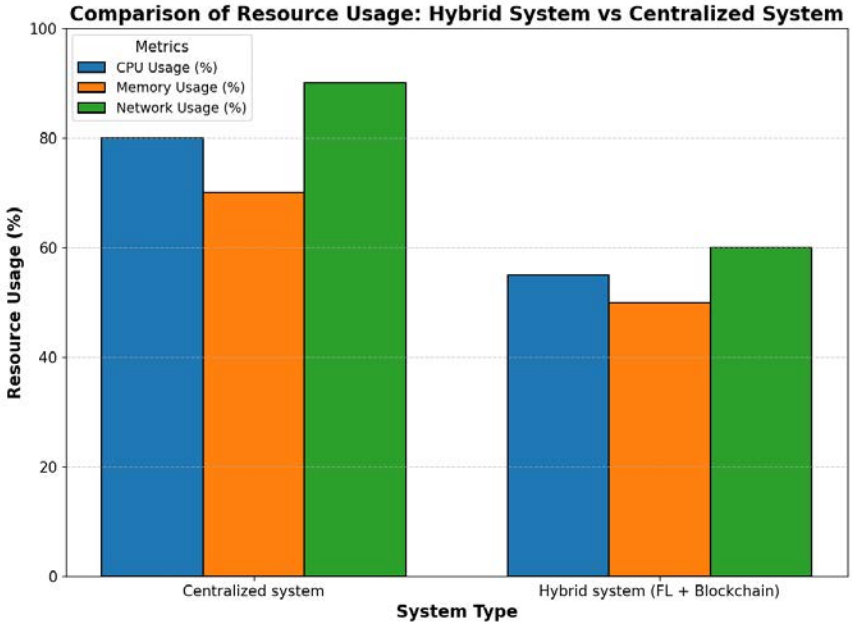

Fig. 3. Comparison of Resource Usage in Hybrid System vs. Centralized System
Load Reduction Coefficient = (80−55)/80 = 0.3125

To calculate network bandwidth usage in systems combining Federated Learning and blockchain, the following formula can be used:

$$\text{Network Bandwidth Usage} = \frac{\sum_{i=1}^{N} Data\ Size_i}{Time\ Period}$$

$\sum_{i=1}^{N} \boldsymbol{Data\ Size_i}$ – amount of data (in bytes) transmitted between nodes over a specific period of time. In Federated Learning systems, this refers to the volume of parameters or updates transmitted from each device iii to a central node or blockchain. Time Period – the time duration (in seconds or minutes) over which the traffic volume is measured. It is important to consider that when multiple nodes simultaneously transmit data, the traffic volumes from all nodes need to be summed, as each node may contribute its part to the total amount of data transmitted. This provides an accurate estimate of the overall traffic, which helps in network optimization and resource management. Moreover, if data transmission occurs in multiple stages, such as first from local devices to the blockchain, followed by processing and returning results, each stage should be considered separately. Each stage may have its own traffic and resource requirements, so they should be evaluated individually to ensure optimal performance and minimize delays.

Blockchain Processing Time:

$$Blockchain\ processing\ time = \frac{\sum_{i=1}^{N} T_{block_i}}{N}$$

where $\boldsymbol{Tblock_i}$ – The processing time (in seconds) for each block iii, which includes both the time for block creation and block confirmation within the network, and N – the total number of blocks created and confirmed during a certain training period.

Conclusions. The integration of blockchain technologies, Federated Learning (FL), and intelligent data analysis opens up significant prospects, but the implementation of such hybrid models comes with certain challenges that must be addressed. One of the primary limitations is the high complexity and resource intensity involved in developing such systems, especially when dealing with large volumes of data and high processing speed requirements.

For the effective use of blockchain data combined with machine learning algorithms, particularly Federated Learning, it is necessary to optimize these algorithms, which requires substantial computational resources. Federated Learning allows model training without centralized data storage, reducing the risk of confidential information leaks. However, it still increases the demands on computational efficiency and coordination between different nodes. Blockchain, in turn, can become a bottleneck when processing large data volumes, as storing each record in blocks may lead to delays and scalability issues.

Another important aspect is ensuring data confidentiality and regulation, especially in the context of processing personal data. Hybrid models that combine blockchain, Federated Learning, and intelligent data analysis can significantly enhance security and privacy in decentralized systems, as they allow users to maintain control over their data and offer resilience against attacks. Intelligent data analysis, particularly through machine learning and deep learning methods, can be used for automatic anomaly detection, trend forecasting, and process optimization based on distributed data, which significantly increases the effectiveness and accuracy of decisions.

However, the implementation of such systems in real-world conditions requires further research, particularly to assess latency, performance, resilience to external threats, and resource utilization efficiency. Experimental research results confirm that combining blockchain, Federated Learning, and intelligent data analysis can significantly improve process efficiency, reduce risks, and ensure a high level of confidentiality and privacy for users, unlocking new opportunities for innovation in various fields.

BIBLIOGRAPHY:

1. Blockchain for secure and efficient data sharing in vehicular edge computing and networks / Kang, J. et al. *IEEE Internet of Things Journal,* 2020, *7*(3), 2347-2363. https://doi.org/10.1109/JIOT.2020.2968332

2. Federated learning: Strategies for improving communication efficiency / Konecny, J. et al. *arXiv preprint arXiv:1610.05492*. 2016 https://arxiv.org/abs/1610.05492

3. Communication-efficient learning of deep networks from decentralized data / McMahan et al. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS),* 2016, pp. 1273-1282.

4. *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press. / Narayanan, A. et al. 2016

5. Tapscott, D., & Tapscott, A. *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world* (Updated ed.). Portfolio. 2017

6. Xu, X., Weber, I., Staples, M. Blockchain in Software Architecture. In: Architecture for Blockchain Applications. Springer, Cham. 2019. https://doi.org/10.1007/978-3-030-03035-3_5.

7. Smart contract-based access control for the internet of things. / Zhang, Y. et al. *IEEE Internet of Things Journal,* 2021 6(2), pp. 1594-1605. https://doi.org/10.1109/JIOT.2021.3055118

8. Blockchain and federated learning for collaborative intrusion detection in vehicular networks. / Zhou, Z. et al *IEEE Transactions on Intelligent Transportation Systems,* 2020, 22(5), pp. 2925-2937. https://doi.org/10.1109/TITS.2020.2995608

9. Blockchain-enabled federated learning: A survey. / Qu, Y. et al. *ACM Computing Surveys*, 2022, *55*(4), pp. 1-35. https://doi.org/10.1145/3524104

10. Wang, Z., & Hu, Q. Blockchain-based federated learning: A comprehensive survey. *arXiv preprint arXiv:2110.02182*. 2021. https://doi.org/10.48550/arXiv.2110.02182

11. Federated learning meets blockchain in edge computing: Opportunities and challenges / Nguyen, D. C. et al. *IEEE Internet of Things Journal*, 2021, *8*(16), 12806-12825. https://doi.org/10.1109/JIOT.2021.3072611

12. Blockchain-based federated learning for securing internet of things: A comprehensive survey / Issa, W. et al, *ACM Computing Surveys*, 2023, *55*(9), 1-43. https://doi.org/10.1145/3560816

13. Securing federated learning with blockchain: a systematic literature review. / Qammar, A. el al. *Artificial Intelligence Review*, 2023, *56*(5), 3951-3985.

14. Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. / Javed, A. R. et al. *Sensors*, 2022, *22*(12), 4394. https://doi.org/10.3390/s22124394

15. Tsudzenko, Y. (2023). Підходи в моделюванні смарт-контрактів на основі Ethereum. *Electronics and Information Technologies, 22*, 69–78. https://doi.org/10.30970/eli.22.7.

REFERENCES:

1. Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2020). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal, 7*(3), 2347-2363. https://doi.org/10.1109/JIOT.2020.2968332

2. Konecny, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*. https://arxiv.org/abs/1610.05492

3. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2016). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)* (pp. 1273-1282).

4. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

5. Tapscott, D., & Tapscott, A. (2017). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world* (Updated ed.). Portfolio.

6. Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer.

7. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2021). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal, 6*(2), 1594-1605. https://doi.org/10.1109/JIOT.2021.3055118

8. Zhou, Z., Li, W., Zhang, J., & Tang, X. (2020). Blockchain and federated learning for collaborative intrusion detection in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems, 22*(5), 2925-2937. https://doi.org/10.1109/TITS.2020.2995608

9. Qu, Y., Uddin, M. P., Gan, C., Xiang, Y., Gao, L., & Yearwood, J. (2022). Blockchain-enabled federated learning: A survey. *ACM Computing Surveys*, *55*(4), 1-35. https://doi.org/10.1145/3524104

10. Wang, Z., & Hu, Q. (2021). Blockchain-based federated learning: A comprehensive survey. *arXiv preprint arXiv:2110.02182*. https://doi.org/10.48550/arXiv.2110.02182

11. Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ... & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, *8*(16), 12806-12825. https://doi.org/10.1109/JIOT.2021.3072611

12. Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys*, *55*(9), 1-43. https://doi.org/10.1145/3560816

13. Qammar, A., Karim, A., Ning, H., & Ding, J. (2023). Securing federated learning with blockchain: a systematic literature review. *Artificial Intelligence Review*, *56*(5), 3951-3985.

14. Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. *Sensors*, *22*(12), 4394. https://doi.org/10.3390/s22124394

15. Tsudzenko, Y. (2023). Підходи в моделюванні смарт-контрактів на основі Ethereum. *Electronics and Information Technologies, 22*, 69–78. https://doi.org/10.30970/eli.22.7.