UNIVERSITY OF NOVI SAD **FORM – 4**
FACULTY OF TECHNICAL SCIENCES

REPORT ON THE ASSESSMENT OF THE SUITABILITY OF THE THESIS TOPIC,CANDIDATES AND SUPERVISORS FOR THE PREPARATION OF THE DOCTORAL DISSERTATION

I INFORMATION ABOUT THE COMITTEE

The authority that appointed the committiee: Dean of the Faculty of Technical Sciences based on the decision of the Scientific-Teaching Council

Date of appointment of the commission: 05.5.2025

Committee members information in accordance with *Regulations for doctoral studies at University of Novi Sad*:

1.	dr Ognjanović Zoran	Research Professor	Mathematical sciences
	Surname and name	Title	Scientific area
	Mathematical institute SANU, Belgrade		Chair
	Institution of employment		Committee member role
2.	dr Gilezan Silvia	Full Professor	Theoretical and Applied Mathematics
	Surname and name	Title	Scientific area
	Faculty of Technical Sciences, Novi Sad		Member
	Institution of employment		Committee member role
3.	dr Vujošević Janičić Milena	Associate Professor	Computer Science and Informatics
	Surname and name	Title	Scientific area
	Faculty of Mathematics, Belgrade		Member
	Institution of employment		Committee member role
4.	dr Davidović Tatjana	Research Professor	Mathematics and Computer Science
	Surname and name	Title	Scientific area
	Mathematical institute SANU, Belgrade		Member
	Institution of employment		Committee member role
5.	dr Dragan Dinu	Associate Professor	Applied Computer Science and Informatics
	Surname and name	Title	Scientific area
	Faculty of Technical Sciences, Novi Sad		Member
	Institution of employment		Committee member role
6.	dr Dedeić Jovana	Assistant Professor	Theoretical and Applied Mathematics
	Surname and name	Title	Scientific area
	Faculty of Technical Sciences, Novi Sad		Member
	Institution of employment		Committee member role

II INFORMATION ABOUT THE CANDIDATE

1. First name, first name of one parent, last name: Milan, Dragan, Todorović
2. Date of birth: 20.7.1987 Place and country of birth: Zaječar, Serbia

II.1 Bachelor Studies

Year of enrolment: 2006 Year of graduation: 2009 Average grade: 9.77

University: University of Belgrade

Faculty: Faculty of Mathematics

Study programme: Computer Science

Degree obtained: Bachelor of Science in Computer Science

II.2 Master Studies

Year of enrolment: 2009 Year of graduation: 2011 Average grade: 9.85

University: University of Belgrade

Faculty: Faculty of Mathematics

Study programme: Computer Science

Degree obtained: Master of Science in Computer Science

Scientific area: Computer Science

Title of master thesis: Application of non-CNF SAT solvers

II.3 Doctoral Studies

Year of enrolment: 2020

University: University of Novi Sad

Faculty: Faculty of Technical Sciences

Study programme: Mathematics in Engineering

Number of ECTS points acquired: 120 Average grade: 10.00

II.4 Scientific and professional work of the candidate

No.	authors, title of the paper, journal, **volume** (year), pages, DOI or ISBN/ISSN	category
1.	**Todorović, M.,** Matijević, L., Ramljak, D., Davidović, T., Urošević, D., Jakšić Krüger, T., & Jovanović, Đ. Proof-of-Useful-Work: BlockChain Mining by Solving Real-Life Optimization Problems. *Symmetry*, **14**(9), 2022, 1831, doi: 10.3390/sym14091831	M22
The paper is within the scope of the proposed doctoral dissertation: **YES** NO PARTIALLY		

No.	authors, title of the paper, journal, **volume** (year), pages, DOI or ISBN/ISSN	category
2.	Mihaljević, M. J., Wang, L., Xu, S., & **Todorović, M**. An Approach for Blockchain Pool Mining Employing the Consensus Protocol Robust against Block Withholding and Selfish Mining Attacks. *Symmetry*, **14**(8), 2022, 1711, doi: 10.3390/sym14081711	M22
The paper is within the scope of the proposed doctoral dissertation: **YES** NO PARTIALLY		

No.	authors, title of the paper, journal, **volume** (year), pages, DOI or ISBN/ISSN	category
3.	Mihaljević, Miodrag J., **Todorović, M**, and Knežević, M. An Evaluation of Power Consumption Gain and Security of Flexible Green Pool Mining in Public Blockchain Systems. *Symmetry* **15**(4), 2023, 924, doi: 10.3390/sym15040924	M22
The paper is within the scope of the proposed doctoral dissertation: **YES** NO PARTIALLY		

No.	authors, title of the paper, journal, **volume** (year), pages, DOI or ISBN/ISSN	category
4.	Davidović, T., **Todorović, M.,** Sharma, B., & Ramljak, D. Exploring Arbitrary Real-Life Problems in Proof-of-Useful-Work: Myth Busting?. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA),* 2023, 1-6, doi: 10.1109/BCCA58897.2023.10338884	M33
The paper is within the scope of the proposed doctoral dissertation: **YES** NO PARTIALLY		

No.	authors, title of the paper, journal, **volume** (year), pages, DOI or ISBN/ISSN	category
5.	Davidović, T., **Todorović, M.**, Ramljak, D., Krüger, T. J., Matijević, L., Jovanović, D., & Urošević, D. COCP: Blockchain Proof-of-Useful-Work Leveraging Real-Life Applications. In *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA),* 2022, 107-110, doi: 10.1109/BCCA55292.2022.9922117	M33
The paper is within the scope of the proposed doctoral dissertation: **YES** NO PARTIALLY		

No.	authors, title of the paper, journal, **volume** (year), pages, DOI or ISBN/ISSN	category
6.	**Todorović, M.,** Knežević, M., Ševerdija, D., Jelić, S., & Mihaljević, M. J. Implementation Framework of a Blockchain Based Infrastructure for Electricity Trading within a Microgrid, EAI CollaborateCom 2023 - 19th EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing, October 4-6, 2023, Corfu Island, Greece, Proceedings, Collaborative Computing: Networking, Applications and Worksharing, 2024, 38 – 53, doi: 10.1007/978-3-031-54521-4_3	M33
The paper is within the scope of the proposed doctoral dissertation: **YES** NO PARTIALLY		

III ASSESSMENT OF THE SUITABILITY OF THE THESIS TOPIC

Evaluation of:

III.1 thesis title

New Additions to Blockchain Technology Techniques and Applications in Electricity Trading
(srp. Нови прилози техникама блокчејн технологија и применама у трговини електричном енергијом)
The Committee finds the proposed thesis title suitable.

Is the proposed thesis title suitable? YES

III.2 subject (problem) of research

Blockchain systems are modern distributed systems, known for their decentralization, immutability, and transparency. Depending on access control, blockchain systems can be classified as public or private — public systems are open and allow anyone to participate in consensus and data validation, while private systems apply access control over who can participate. The first and most well-known application of public blockchain systems is in cryptocurrencies, but since then they have found use in various domains, where they ensure data immutability and eliminate the need for centralized entities that must be trusted. Blockchain systems achieve this through consensus protocols executed by network participants to reach agreement in a decentralized manner. However, these advantages are often accompanied by high costs, such as significant resource consumption, particularly electricity, which not only poses a challenge for practical adoption but also drives the development of more efficient protocols.

One of the applications of blockchain systems is found in the energy sector, which is undergoing major transformations due to climate-related challenges that have led to increased use of renewable energy sources, such as wind and sun. These changes have given rise to *prosumers*, users who both produce and consume energy, as well as to the emergence of multiple microgrids, which are small, decentralized networks with their own energy sources, most often owned by prosumers. Blockchain systems naturally suggest themselves as a platform for energy trading within these networks, but they face challenges related to efficiency, privacy, and the use of public blockchain systems, making this area highly attractive for further research.

The drawbacks of the most commonly used consensus protocol in public blockchain systems, Proof-of-Work (PoW), such as high electricity consumption and a tendency toward centralization due to the formation of mining pools that process transactions and engage in consensus, have stimulated the development of new protocols. These new protocols are mostly focused on addressing energy consumption issues, but they have also introduced new challenges and, in general, do not offer the same level of security as PoW. Moreover, the growing application of blockchain systems across different domains has shown that not all consensus protocols are suitable for all use cases, which creates a need for the development of protocols with more specific purposes.

The application of blockchain technology in the energy system is a relatively new research area and encompasses numerous possibilities. Part of the research is focused on its use in electricity trading, primarily within microgrids and typically relying on private blockchain systems. On the other hand, many countries lack legal frameworks that regulate decentralized energy trading. Further research is needed that involves public blockchain systems, in order to reduce dependence on centralized entities and to go beyond the boundaries of individual microgrids. The development of such systems could contribute to a better understanding of trading models and support the creation of future regulatory frameworks.

The Committee finds the subject of the research to be suitable, as the proposed topic is timely and relevant, enabling the advancement of scientific results and opening new avenues for future research.

Is the subject of the research suitable? YES

III.3 understanding of the problem based on the selected literature, with a list of literature

A blockchain system is a decentralized system composed of blocks containing user transactions, which are assembled and proposed for recording by system participants. To establish trust, particularly in open blockchain systems where anyone can participate, the participants maintaining the system execute a consensus protocol for each block to validate its correctness, which requires significant computational resources [1]. After this, users verify the new block, which is recorded on the blockchain if approved by the majority. This protocol enables the recording of valid data without the need for a centralized trusted entity. In open systems, participants receive a cryptocurrency reward for each of their blocks that were successfully recorded. Although many consensus protocols exist, the new ones are still developed in order to address the shortcomings of existing solutions and to create protocols suitable for specific blockchain system applications [2][3].

Proof-of-Work (PoW) [1][2][4] is the most well-known consensus protocol for blockchain systems. It was first introduced in [5] as a method for combating spam e-mails, and later in [6] as a core component of Bitcoin. Participants who maintain the system (known as miners in the context of PoW) attempt to solve a complex cryptographic problem that requires a large number of hash function computations. The goal is to find a value which, when hashed together with the new block, produces a result lower than a predefined threshold. The main drawbacks of PoW include high electricity consumption and the need for large amounts of cooling water for the devices, as well as a tendency toward centralization due to formation of mining pools [7][8][9].

Proof-of-Stake (PoS) [2][10][11][12] emerged as a solution to the main drawback of PoW — energy consumption. Instead of using energy, participants stake the blockchain system's cryptocurrency in order to gain the right to assemble a bloc, for which they receive a reward. PoS reduces energy consumption, but introduces new issues such as the "nothing at stake" problem and incentives for users to hoard cryptocurrency rather than spend it. Additionally, the value of stakes depends only on the system's cryptocurrency, which creates disparities among participants — the same stake has different significance for wealthier versus less wealthy users. Ethereum is the most well-known system that has adopted PoS [13].

Proof-of-Space/Capacity (PoS/C) [1][4][14][15] is an alternative to PoW in which participants use memory, or disk space, instead of energy. The probability that a participant will publish a new block is proportional to the amount of allocated memory used to hold potential solutions. The participant who finds the closest solution creates the new block. During verification, it is also checked whether the participant's reserved space matches the declared amount. PoS/C reduces energy consumption, but increases the time required to create new blocks.

Proof-of-Useful-Work (PoUW) [16] replaces the computationally intensive task of PoW with solving real-world problems submitted by blockchain users. PoUW does not reduce energy consumption, but instead uses it more rationally by applying it to solving practical problems. Various PoUW protocols address different problems, such as the traveling salesman problem [17][18][19], training machine learning and deep learning models [20][21][22][23][24][25], clustering transport requests [26], and other optimization problems [27][28]. PoUW protocols introduce new security challenges, such as preventing users from submitting easy problem instances or solving problem instances they submitted themselves, since they may already know the solution in advance.

Due to their distributed and decentralized nature, blockchain systems have found applications in various domains, including the power sector. Some of these applications are meter reading, billing, grid management, electricity trading, issuance of renewable energy certificates, and electric vehicle charging. Electricity trading is particularly relevant with the inclusion of prosumers, as blockchain enables distributed trading without a central authority, most often within microgrids. In studies such as [29–33][36–40][45], the authors implement electricity trading by selecting a blockchain system to which microgrid users are connected and on which smart contracts are deployed to carry out the trading process. Due to the relatively small number of users within a microgrid, blockchain systems are typically private, which leads to the presence of a central entity that controls access, thereby reducing decentralization. Trading is most commonly realized via smart contracts using various auction methods, such as double auctions [30][31][42][44] and blind auctions [40][45]. In addition to auctions, there are contracts that match user offers and demands in specific ways, as in [34], where matching is performed periodically to pair compatible offers and demands. In some cases [44], a hybrid approach is applied, in which trading is conducted in cycles, combining double auctions with predefined matching for unmatched users.

In addition to blockchain-based platforms for electricity trading, some authors also implement

additional functionalities, such as adaptive controllers for frequency regulation [31], energy management using the Internet of Things (IoT) and cloud computing [34], forecasting of energy production and consumption [44], solar panel positioning based on weather conditions [40], procurement of spinning reserves in cases of energy shortages [42], as well as new consensus protocols [35][39] and reputation systems that reward honest and penalize dishonest users [38][43].

Although these systems are decentralized, many authors introduce elements that reduce decentralization. For example, some systems include centralized entities that must be trusted: system [29] features control nodes, [36] employs a regulator for issuing renewable energy production certificates, and [43] includes a centralized node that controls energy rights.

Some authors have implemented their proposed systems in real-world environments. For example, the system from [30] was tested in a Canadian microgrid, while the system from [37] was deployed in a remote community in Pakistan. Additionally, some authors provide a detailed performance analysis of the system [46]. On the other hand, there are systems that have not been fully implemented, such as the one in [42], where the simulation was conducted solely within the Remix IDE development environment, without deployment to a blockchain platform.

In addition to studies that focus on trading within individual microgrids, in [41] the authors develop a blockchain-based platform for trading between interconnected microgrids. The system takes into account optimal greedy behavior of the networks, giving priority to microgrids with lower energy prices. Two pricing ranking algorithms are proposed: distributed lowest-price discovery and grouping of microgrids by price for simultaneous trading.

The research in this dissertation will also focus on the topics and findings presented in [47–67].

[1] Merrad, Y., Habaebi, M. H., Elsheikh, E. A., Suliman, F. E. M., Islam, M. R., Gunawan, T. S., & Mesri, M. (2022). Blockchain: Consensus algorithm key performance indicators, trade-offs, current trends, common drawbacks, and novel solution proposals. *Mathematics*, *10*(15), 2754.

[2] Yadav, A. K., Singh, K., Amin, A. H., Almutairi, L., Alsenani, T. R., & Ahmadian, A. (2023). A comparative study on consensus mechanism with security threats and future scopes: Blockchain. *Computer Communications*, *201*, 102-115.

[3] Xu, Y., Tao, X., Das, M., Kwok, H. H., Liu, H., Wang, G., & Cheng, J. C. (2023). Suitability analysis of consensus protocols for blockchain-based applications in the construction industry. *Automation in Construction*, *145*, 104638.

[4] Islam, S., Islam, M. J., Hossain, M., Noor, S., Kwak, K. S., & Islam, S. R. (2023). A survey on consensus algorithms in blockchain-based applications: Architecture, taxonomy, and operational issues. IEEE Access.

[5] C. Dwork, M. Naor, Pricing via processing or combatting junk mail, in: Annual International Cryptology Conference, Springer, 1992, pp. 139–147.

[6] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review, 21260. 2008. Доступно на адреси: https://bitcoin.org/bitcoin.pdf (присутпљено 16.9.2024).

[7] O'Dwyer, K.J.; Malone, D. Bitcoin mining and its energy footprint. In Proceedings of the 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Limerick, Ireland, 26–27 June 2014; pp. 280–285

[8] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 3-16).

[9] de Vries, A. (2 024). Bitcoin's growing water footprint. Cell Reports Sustainability, 1(1).

[10] King S., Nadal S., Ppcoin: Peer-to-peer crypto-currency with proof-of-stake, Self-Published Paper, August 19 (2012) 1

[11] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review, 21260. 2008. Доступно на адреси: https://bitcoin.org/bitcoin.pdf (присутпљено 16.9.2024).

[12] Oliveira, M., Chauhan, S., Pereira, F., Felgueiras, C., & Carvalho, D. (2023). Blockchain protocols and edge computing targeting industry 5.0 needs. Sensors, 23(22), 9174.

[13] "Proof of Stake (PoS)." Ethereum, Ethereum, 19. Март 2024, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. Приступљено 16. 9. 2024.

[14] Dziembowski, S., Faust, S., Kolmogorov, V., & Pietrzak, K. (2015, August). Proofs of space. In *Annual Cryptology Conference* (pp. 585-605). Berlin, Heidelberg: Springer Berlin Heidelberg.

[15] Ateniese, G., Bonacina, I., Faonio, A., & Galesi, N. (2014). Proofs of space: When space is of the essence. In *Security and Cryptography for Networks: 9th International Conference, SCN 2014, Amalfi, Italy, September 3-5, 2014. Proceedings 9* (pp. 538-557). Springer International Publishing.

[16] Ball, M.; Rosen, A.; Sabin, M.; Vasudevan, P.N. Proofs of Useful Work. IACR Cryptology ePrint Archive. 2017. Доступан на: https://eprint.iacr.org/2017/203.pdf (Приступио 16.9.2024)

[17] Loe, A.F.; Quaglia, E.A. Conquering generals: An NP-hard proof of useful work. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 54–59.

[18] Syafruddin, W.A.; Dadkhah, S.; Köppen, M. Blockchain Scheme Based on Evolutionary Proof of Work. In Proceedings of the 2019 IEEE Congress on Evolutionary Computation (CEC), Wellington, New Zealand, 10–13 June 2019; pp. 771–776.

[19] Li, W. Adapting Blockchain Technology for Scientific Computing. arXiv 2018, arXiv:1804.08230.

[20] Lihu, A.; Du, J.; Barjaktarevic, I.; Gerzanics, P.; Harvilla, M. A Proof of Useful Work for Artificial Intelligence on the Blockchain. arXiv 2020, arXiv:2001.09244.

[21] Chenli, C.; Li, B.; Shi, Y.; Jung, T. Energy-recycling blockchain with proof-of-deep-learning. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 19–23.

[22] Li, B.; Chenli, C.; Xu, X.; Shi, Y.; Jung, T. DLBC: A Deep Learning-Based Consensus in Blockchains for Deep Learning Services. arXiv 2020, arXiv:1904.07349v2.

[23] Li, B.; Chenli, C.; Xu, X.; Jung, T.; Shi, Y. Exploiting computation power of blockchain for biomedical image segmentation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Long Beach, CA, USA, 16–20 June 2019; pp. 2802–2811.

[24] Qiu, C.; Wang, X.; Yao, H.; Du, J.; Yu, F.R.; Guo, S. Networking Integrated Cloud-Edge-End in IoT: A Blockchain-Assisted Collective Q-Learning Approach. IEEE Internet Things J. 2020, 8, 12694–12704.

[25] Baldominos, A.; Saez, Y. Coin. AI: A proof-of-useful-work scheme for blockchain-based distributed deep learning. Entropy 2019, 21, 723

[26] Haouari, M.; Mhiri, M.; El-Masri, M.; Al-Yafi, K. A novel proof of useful work for a blockchain storing transportation transactions. Inf. Process. Manag. 2022, 59, 102749.

[27] Fitzi, M.; Kiayias, A.; Panagiotakos, G.; Russell, A. Ofelimos: Combinatorial Optimization via Proof-of-Useful-Work\A ProvablySecure Blockchain Protocol. IACR Cryptology ePrint Archive. 2021. Доступно на: https://eprint.iacr.org/2021/1379.pdf

[28] Shibata, N. Proof-of-search: Combining blockchain consensus formation with solving optimization problems. IEEE Access 2019, 7, 172994–173006

[29] Lu, X., Shi, L., Chen, Z., Fan, X., Guan, Z., Du, X., & Guizani, M. (2019). Blockchain-based distributed energy trading in energy Internet: An SDN approach. IEEE access, 7, 173817-

173826.

[30] Saxena, S., Farag, H. E., Brookson, A., Turesson, H., & Kim, H. (2020). A permissioned blockchain system to reduce peak demand in residential communities via energy trading: A real-world case study. IEEE Access, 9, 5517-5530.

[31] Veerasamy, V., Hu, Z., Qiu, H., Murshid, S., Gooi, H. B., & Nguyen, H. D. (2024). Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids. Applied Energy, 353, 122107.

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

[33] Wang, X., Liu, Y., Ma, R., Su, Y., & Ma, T. (2023). Blockchain enabled smart community for bilateral energy transaction. International Journal of Electrical Power & Energy Systems, 148, 108997.

[34] Condon, F., Franco, P., Martínez, J. M., Eltamaly, A. M., Kim, Y. C., & Ahmed, M. A. (2023). EnergyAuction: IoT-Blockchain Architecture for Local Peer-to-Peer Energy Trading in a Microgrid. Sustainability, 15(17), 13203.

[35] Mu, C., Ding, T., Shahidehpour, M., Liu, S., Chen, B., Jia, W., ... & Huang, Y. (2023). A Light Blockchain for Behind-the-Meter Peer-to-Peer Energy Transactions in Cyber-Physical Power Systems. IEEE Transactions on Smart Grid.

[36] Tkachuk, R. V., Ilie, D., Robert, R., Kebande, V., & Tutschku, K. (2023). Towards efficient privacy and trust in decentralized blockchain-based peer-to-peer renewable energy marketplace. Sustainable Energy, Grids and Networks, 35, 101146.

[37] Baig, M. J. A., Iqbal, M. T., Jamil, M., & Khan, J. (2022). A low-cost, open-source peer-to-peer energy trading system for a remote community using the internet-of-things, blockchain, and hypertext transfer protocol. Energies, 15(13), 4862.

[38] Guo, M., Zhang, K., Wang, S., Xia, J., Wang, X., Lan, L., & Wang, L. (2023). Peer-to-peer energy trading and smart contracting platform of community-based virtual power plant. Frontiers in Energy Research, 10, 1007694.

[39] Cui, D., He, J., Zhang, G., & Hou, Z. (2022). Blockchain-based Distributed Power Market Trading Mechanism. Computers, Materials & Continua, 72(2).

[40] Kwak, S., Lee, J., Kim, J., & Oh, H. (2022). EggBlock: Design and Implementation of Solar Energy Generation and Trading Platform in Edge-Based IoT Systems with Blockchain. Sensors, 22(6), 2410.

[41] Hamouda, M. R., Nassar, M. E., & Salama, M. M. A. (2023). Blockchain-based sequential market-clearing platform for enabling energy trading in Interconnected Microgrids. International Journal of Electrical Power & Energy Systems, 144, 108550.

[42] Damisa, U., Nwulu, N. I., & Siano, P. (2022). Towards blockchain-based energy trading: A smart contract implementation of energy double auction and spinning reserve trading. Energies, 15(11), 4084.

[43] Xiong, X., Qing, G., & Li, H. (2022). Blockchain-based P2P power trading mechanism for PV prosumer. Energy reports, 8, 300-310.

[44] Rahman, M., Chowdhury, S., Shorfuzzaman, M., Hossain, M. K., & Hammoudeh, M. (2023). Peer-to-peer power energy trading in blockchain using efficient machine learning model. Sustainability, 15(18), 13640.

[45] Gajić, D.B.; Petrović, V.B.; Horvat, N.; Dragan, D.; Stanisavljević, A.; Katić, V.; Popović, J. A Distributed Ledger-Based Automated Marketplace for the Decentralized Trading of Renewable Energy in Smart Grids. *Energies* **2022**, *15*, 2121. https://doi.org/10.3390/en15062121

[46] Horvat, N., Gajić, D. B., Trifunović, P., Petrović, V. B., Dragan, D., & Katić, V. (2024). Performance Evaluation of a Distributed Ledger-based Platform for Renewable Energy Trading. *IEEE Access*.

[47] M.J. Mihaljevic, "A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off", IEEE Access, vol. 8, pp. 141258-141268, Avg 2020

[48] M.J. Mihaljevic, L. Wang, S. Xu and M. Todorovic, "An Approach for Blockchain Pool Mining Employing the Consensus Protocol Robust against Block Withholding and Selfish Mining Attacks", Symmetry 2022, 14 (8), 1711. (28 pages)

[49] Chaudhry, N., & Yousaf, M. M. (2018, December). Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. In *2018 12th international conference on open source systems and technologies (ICOSST)* (pp. 54-63). IEEE.

[50] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432-1465.

[51] Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of financial studies*, *34*(3), 1156-1190.

[52] Hoffmann, F. (2022, November). Challenges of proof-of-useful-work (PoUW). In *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)* (pp. 1-5). IEEE.

[53] Merlina, A., Garrett, T., & Vitenberg, R. (2024). On Replacing Cryptopuzzles with Useful Computation in Blockchain Proof-of-Work Protocols. *arXiv preprint arXiv:2404.15735*.

[54] Salhab, M., & Mershad, K. (2023). Proof of Deep Learning: approaches, challenges, and future directions. *arXiv preprint arXiv:2308.16730*.

[55] Oyinloye, D. P., Teh, J. S., Jamil, N., & Alawida, M. (2021). Blockchain consensus: An overview of alternative protocols. *Symmetry*, *13*(8), 1363.

[56] M. Nour, J. P. Chaves- ´Avila and ´A. S´anchez-Miralles, “Review of Blockchain Potential Applications in the Electricity Sector and Challenges for Large Scale Adoption,” IEEE Access, vol. 10, pp. 47384–47418, 2022, doi: 10.1109/AC-CESS.2022.3171227.

[57] Uddin, S. S., Joysoyal, R., Sarker, S. K., Muyeen, S. M., Ali, M. F., Hasan, M. M., ... & Tasneem, Z. (2023). Next-generation blockchain enabled smart grid: Conceptual framework, key technologies and industry practices review. Energy and AI, 100228.

[58] Mengelkamp, E., G¨arttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. Applied energy, 210, 870-880.

[59] Yolda¸s, Y., ¨Onen, A., Muyeen, S. M., Vasilakos, A. V., and Alan, I. (2017). Enhancing smart grid with microgrids: Challenges and opportunities. Renewable and Sustainable Energy Reviews, 72, 205-214. https://doi.org/10.1016/j.rser.2017.01.064

[60] Y. Guoa, Z. Wanb and X. Cheng, ”When blockchain meets smart grids: A comprehensive survey”, High-Confidence Computing, vol. 2, no. 2, 100059, June 2022.

[61] Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger Shanghai Version. 2024-09-02, https://ethereum.github.io/yellowpaper/paper.pdf. 2024

[62] Todorović, M., Knežević, M., Ševerdija, D., Jelić, S., & Mihaljević, M. J. (2023, October). Implementation Framework of a Blockchain Based Infrastructure for Electricity Trading Within a Microgrid. In International Conference on Collaborative Computing: Networking, Applications and Worksharing (pp. 38-53). Cham: Springer Nature Switzerland.

[63] Davidović, T., Todorović, M., Sharma, B., & Ramljak, D. (2023, October). Exploring Arbitrary Real-Life Problems in Proof-of-Useful-Work: Myth Busting?. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)* (pp. 1-6). IEEE.

[64] Mihaljević, M. J., Todorović, M., & Knežević, M. (2023). An Evaluation of Power Consumption Gain and Security of Flexible Green Pool Mining in Public Blockchain Systems. *Symmetry*, *15*(4), 924.

[65] Davidović, T., Todorović, M., Ramljak, D., Krüger, T. J., Matijević, L., Jovanović, D., & Urošević, D. (2022, September). COCP: blockchain proof-of-useful-work leveraging real-life applications. In *2022 Fourth International Conference on Blockchain Computing and*

Applications (BCCA) (pp. 107-110). IEEE.

[66] Mihaljević, M. J., Wang, L., Xu, S., & Todorović, M. (2022). An approach for blockchain pool mining employing the consensus protocol robust against block withholding and selfish mining attacks. *Symmetry*, *14*(8), 1711.

[67] Todorović, M., Matijević, L., Ramljak, D., Davidović, T., Urošević, D., Jakšić Krüger, T., & Jovanović, Đ. (2022). Proof-of-useful-work: Blockchain mining by solving real-life optimization problems. *Symmetry*, *14*(9), 1831.

The Committee finds that the selection of literature is appropriate and that the listed references are relevant to the research area. The cited bibliographic sources clearly indicate the timeliness of the research within the field.

Is the selection of literature appropriate? YES

III.4 research objectives

Research objectives:

1) Development of a new consensus protocol based on the PoUW family, which requires from participants to solve real world, user-submitted optimization problems. This protocol is expected to enable rational energy usage while maintaining a high level of blockchain system security, providing a valid alternative to existing protocols.
2) Implementation of a new PoW-based consensus protocol that incorporates the use of both memory and processing power for problem-solving. Miners will be able to flexibly choose the ratio of these resources, which allows them to more efficiently manage their energy consumption. The protocol will be implemented within the Ethereum blockchain system.
3) Development of an electricity trading system on the network that includes the role of energy provider and uses the public Ethereum blockchain with the new consensus protocol. A proof-of-concept implementation is planned, which will include a user interface and simulated communication with smart meters.

The Committee finds that the objectives of the proposed research are appropriately defined, well-conceived, and suitable for the preparation of a doctoral dissertation.

Are the research objectives appropriate? YES

III.5 expected results (hypothesis)

The research will result in the development of two new consensus protocols: one based on the *Proof-of-Useful-Work* (PoUW) concept, which enables the integration of real-world optimization problems into the process of block creation and verification, and another that combines the use of memory and processing power, providing participants with greater energy flexibility. Both protocols are expected to ensure a high level of security and offer a sustainable alternative to existing PoW solutions.
In addition, a proof-of-concept platform for distributed electricity trading is planned, which will use the public Ethereum blockchain with the new consensus protocol, and will include simulated communication with smart meters and a corresponding user interface.

The Committee finds the stated results to be suitable, as they represent a significant research contribution and provide a foundation for further research and practical application.

Do the expected results represent a significant scientific contribution? YES

III.6 work plan (based on the research phases and the indicative content of the dissertation from Form 1)

The research plan consists of the following:

1) Definition and description of the problem
2) Review of relevant literature and presentation of the current state of the art
3) Development of a consensus protocol based on the Proof-of-Useful-Work family of protocols
4) Development and implementation of a consensus protocol based on Proof-of-Work, which allows flexible selection of resources used
5) Design and implementation of a proof-of-concept electricity trading system based on the

Ethereum platform, using the newly developed PoW-based consensus algorithm
6) Analysis of results and formulation of conclusions

Preliminary Structure of the Dissertation:
1) *Introduction*
2) *Blockchain Technology and Consensus Protocols* – This chapter will provide a detailed introduction to blockchain technologies and consensus protocols. It will also present an in-depth overview of the most significant consensus protocols.
3) *Proof-of-Useful-Work: Combinatorial Optimization Consensus Protocol* – This chapter will present in detail the novel Combinatorial Optimization Consensus Protocol, based on the Proof-of-Useful-Work family of protocols. The protocol is based on solving instances of combinatorial optimization problems submitted by blockchain users.
4) *Proof-of-Inversion Capacity Consensus Protocol* – This chapter will describe the Proof-of-Inversion Capacity consensus protocol. It will also cover its implementation within the Ethereum blockchain system, specifically within the official Go-Ethereum client. The chapter will include experimental results comparing the performance of this algorithm with that of the standard Proof-of-Work algorithm.
5) *Blockchain Systems and Power Networks* – This chapter will explore the application of blockchain technology in the context of power systems, with a focus on electricity trading.
6) *Blockchain-Based Electricity Trading System* – This chapter will present the implementation of a proof-of-concept electricity trading system based on blockchain technology. It will include a detailed description of the system architecture as well as the technical implementation details.
7) *Conclusion and Future Work*
8) *References*
9)

The Committee finds that the work plan is suitable and appropriately structured.

Is the work plan appropriate? YES

III.7 methods and research samples

The proposed algorithms will be theoretically explained, while the implementation of the Proof-of-Inversion Capacity algorithm will be experimentally tested in order to compare it with the Proof-of-Work algorithm. The implemented electricity trading system will be deployed in a test environment utilizing Docker and Docker-compose software, as well as Raspberry Pi device.

The data used in the experiments consist of blocks generated during mining. The experiment compares Ethereum which uses the Proof-of-Inversion Capacity protocol with Ethereum which uses Proof-of-Work, where blocks are generated through actual mining. The blocks from different blockchain systems are not identical, as they depend on the time of creation and the address of the participant who generated them, but this does not affect the results of the experiment. The sample size varies depending on the mining difficulty being analyzed.

Are the research method and sample appropriate? YES

III.8 facilities, laboratories, and equipment for research activities

Computational resources of the Mathematical Institute of the Serbian Academy of Sciences and Arts.

Are the research conditions appropriate? YES

III.9 Methods for statistical analysis and processing of data, as well as other relevant information

No statistical processing of the data is planned.

Are the proposed methods appropriate? YES

IV ASSESSMENT OF THE CANDIDATE'S ELIGIBILITY

Requirements defined by the study programme for the candidate:

In accordance with the Law on Higher Education, as well as the Rules of Doctoral Studies of the University of Novi Sad, adopted at the session of the Senate of the University of Novi Sad held on February 25, 2021, which entered into force on March 5, 2021 and have been applicable since April 1, 2021 (with amendments adopted on October 27, 2022; March 30, 2023; and March 28, 2024), and in accordance with the Regulations on Enrolment, Study in Doctoral Academic Studies, and the Attainment of the Title of Doctor of Science or Doctor of Arts of the Faculty of Technical Sciences (no. 01-195/11-1) dated October 7, 2021, the right to submit a doctoral dissertation topic is granted to a doctoral student who has passed all exams required by the study program and who has successfully defended the Theoretical Foundations of the Doctoral Dissertation.

Justification:

The candidate, Milan Todorović, has fulfilled all coursework requirements prescribed by the doctoral study program Mathematics in Engineering and has earned a total of 120 ECTS credits. The remaining 60 ECTS credits are to be acquired through the conduct of research, as well as the writing and defense of the doctoral dissertation. The candidate has also published three papers in M22-category journals and three papers in M33-category conference proceedings and journals, demonstrating appropriate and sufficient engagement as a researcher. The Committee concludes that the candidate meets the formal requirements and possesses the scientific and professional competence necessary for the preparation of a doctoral dissertation.

Does the candidate meet the defined requirements? YES

V ASSESSMENT OF THE SUPERVISOR'S ELIGIBILITY

V.1 Supervisor's Biography (up to 500 words):

Prof. Miodrag J. Mihaljević, PhD, is a corresponding member of the Serbian Academy of Sciences and Arts (since 2021), a research professor and deputy director of the Mathematical Institute of the Serbian Academy of Sciences and Arts, as well as the head of the National Center for Cybersecurity and Privacy. He received his bachelor's degree in 1979 from the Faculty of Electrical Engineering, University of Belgrade, where he also completed his master's degree in 1981. He defended his doctoral dissertation in 1990 at the Military Technical Academy of the Yugoslav People's Army (JNA) in Zagreb. He began his professional career in 1979 at the Institute for Applied Mathematics and Electronics, where he worked until 1998. From 1992 to 1998, he was an external associate of the Mathematical Institute, and since 1998 he has been employed there full-time. In 1999, he was appointed research professor, and since 2015 he has served as deputy director.

He is the author of over 75 papers published in leading international scientific journals, *including IEEE Transactions on Information Theory, IEEE Transactions on Communications, IEEE Communications Letters*, and others. He has participated in more than 50 international conferences, published over 50 papers in national publications, and authored more than 50 patents, software solutions, and technical reports. His work has been cited more than 3,000 times.

Prof. Mihaljević has led numerous national and international projects in the fields of cryptology, image processing, and computational topology. He has held visiting positions in Japan, including at the University of Tokyo, SONY Computer Science Laboratories, and AIST. For his scientific contributions, he has received numerous accolades, including the SASA Award for a Decade of Achievements (2003–2012), and in 2014 he was elected a member of the Academia Europaea. He has been included on Stanford University's list of the "Top 2% of the World's Scientists" for the years 2020–2024.

In addition to his scientific work, Prof. Mihaljević is active as an associate editor and editorial board member of several international journals, and has repeatedly served as a member of the Scientific Council of the relevant ministry in Serbia.

V.2 Supervisor's References in the Scientific Field Related to the Doctoral Dissertation Topic:

No.	authors, title of the paper, journal, **volume** (year), pages, DOI or ISBN/ISSN	category
1.	S. Xu, L. Zhang, L. Wang, **M.J. Mihaljevic,** S. Zhang, W. Shao, Q. Wang, Relay network-based cross-chain data interaction protocol with integrity audit, *Computers and Electrical Engineering*, **117**, 2024, https://doi.org/10.1016/j.compeleceng.2024.109262	M21
2.	S. Xu, F. Wang, L. Wang, **M.J. Mihaljevic**, S. Zhang, W. Shao, and Q. Huang, A Sharding Scheme Based on Graph Partitioning Algorithm for Public Blockchain, *Computer Modeling in Engineering & Sciences, (CMES),* **139**(3), 2024, 3311-3327, doi: 10.32604/cmes.2023.046164	M22
3.	**M.J. Mihaljevic**, M. Todorovic, and M. Kneževic, An Evaluation of Power Consumption Gain and Security of Flexible Green Pool Mining in Public Blockchain Systems, *Symmetry*, **15**(924), 2023, doi: doi.org/10.3390/sym15040924	M22
4.	S. Xu, S. Dong, L. Wang, **M.J. Mihaljević**, S. Zhang, W. Shao, Q. Wang, Blockchain-based secure data sharing with overlapping clustering and searchable encryption, *Computer Standards & Interfaces*, **93**, 2025, doi: https://doi.org/10.1016/j.csi.2025.103979	M21
5.	**M.J. Mihaljević**, M. Knežević, D. Urošević, L. Wang, and S. Xu, An Approach for Blockchain and Symmetric Keys Broadcast Encryption Based Access Control in IoT, *Symmetry*, **15**(299), 2023 doi: 10.3390/sym15020299	M22
6.	**M.J. Mihaljevic**, L. Wang, S. Xu and M. Todorovic, An Approach for Blockchain Pool Mining Employing the Consensus Protocol Robust against Block Withholding and Selfish Mining Attacks, *Symmetry* , **14**(8), 2022, 1711, doi: 10.3390/sym14081711	M22
7.	**M.J. Mihaljevic**, A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off, *IEEE Access*, **8**, 2020, 141258-141268, doi: 10.1109/ACCESS.2020.3013199	M21
8.	S. Zhang, C. Hu, L. Wang, **M.J. Mihaljevic**, S. Xu, and T. Lan, A Malware Detection Approach Based on Deep Learning and Memory Forensics, *Symmetry*, **15**(3), 2023, 758. doi: 10.3390/sym15030758	M22
9.	**M.J. Mihaljevic**, L. Wang and S. Xu, An Approach for Security Enhancement of Certain Encryption Schemes Employing Error Correction Coding and Simulated Synchronization Errors, *Entropy* , **24**(3), 2022, 406; doi: 10.3390/e24030406	M22
10.	**M.J. Mihaljevic**, A. Radonjic, L. Wang and S. Xu, "Security Enhanced Symmetric Key Encryption Employing an Integer Code for the Erasure Channel", *Symmetry*, **14** (8), 2022, 1709, doi: 10.3390/sym14081709	M22
11.	S. Tomovic, M. Knezevic, and **M.J. Mihaljevic**, nalysis and Correction of the Attack against the LPN-Problem Based Authentication Protocols, *Mathematics*, **9** (5), 2021, doi:10.3390/math9050573.	M21a
12.	M. Kneževic, S. Tomovic and **M.J. Mihaljevic**, Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation, *Electronics*, **9** (8), 2020, 1296, doi: 10.3390/electronics9081296	M22
13.	**M.J. Mihaljevic,** Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security, *Entropy*, 21 (7), 2019, doi: https://doi.org/10.3390/e21070701	M21
14.	**M.J. Mihaljevic** and F. Oggier, Security Evaluation and Design Elements for a Class of Randomized Encryptions, *IET Information Security*, **13**(1), 2019, 36–47, doi:10.1049/iet-ifs.2017.0271	M23
15.	**M.J. Mihaljevic**, A. Kavcic and K. Matsuura, An Encryption Technique for Provably Secure Transmission from a High Performance Computing Entity to a Tiny One, *Mathematical Problems in Engineering*, **2016**, 2016, doi: http://dx.doi.org/10.1155/2016/7920495 .	M23

16.	S. Tomovic, **M.J. Mihaljevic**, A. Perovic and Z. Ognjanovic, A Protocol for Provably Secure Authentication of a Tiny Entity to a High Performance Computing One, *Mathematical Problems in Engineering*, **2016**, 2016, doi: 10.1155/2016/9289050	M23
17.	S. Xu, H. He, **M.J. Mihaljević** , S. Zhang, W. Shao, Q. Wang, DBC-MulBiLSTM: A DistilBERT-CNN Feature Fusion Framework enhanced by multi-head self-attention and BiLSTM for smart contract vulnerability detection, *Computers and Electrical Engineering*, **123**, 2025, doi: https://doi.org/10.1016/j.compeleceng.2025.110096	M21
18.	Q. Wang, L. Wang, S. Xu, S. Zhang, W. Shao, **M.J. Mihaljević** , Single-Layer Trainable Neural Network for Secure Inference, *IEEE Internet of Things Journal*, **12**(3), 2025, pp. 2968-2978, doi: 10.1109/JIOT.2024.3480195	M21a

V.3 Requirements for the supervisor, as defined by the *Rules of Doctoral Studies of the University of Novi Sad,* for the scientific field to which the doctoral dissertation belongs:

In accordance with the Law on Higher Education, as well as the Rules of Doctoral Studies of the University of Novi Sad, adopted at the session of the Senate of the University of Novi Sad held on February 25, 2021, which entered into force on March 5, 2021 and have been applicable since April 1, 2021 (amendments adopted on October 27, 2022; March 30, 2023; and March 28, 2024), and in accordance to the Regulations on Enrolment, Study in Doctoral Academic Studies, and the Attainment of the Title of Doctor of Science or Doctor of Arts of the Faculty of Technical Sciences (no. 01-195/11-1) dated October 7, 2021, the supervisor is, as a rule, a faculty member of the given study program who, in addition to meeting the conditions defined by accreditation standards, has authored at least five papers published in journals with an impact factor listed in the SCI or SCIe databases in the past ten years.

Justification:

The Committee concludes that **Prof. Miodrag J. Mihaljević, PhD**, meets the requirements defined for a supervisor in accordance with the Rules of Doctoral Studies of the University of Novi Sad and is deemed **ELIGIBLE** to serve as the supervisor for the candidate's doctoral dissertation.

Does the supervisor meet the requirements? YES

VI CONCLUSION

Thesis Topic is Suitable	**YES**
Candidate is Eligible	**YES**
Supervisor is Eligible	**YES**

Justification of the Suitability of the Thesis Topic, Candidate, and Supervisor (up to 500 words):

To reach the conclusions presented in this report, the Committee reviewed the candidate's submitted application, evaluated the relevance of the listed references related to the research topic, as well as the references of the proposed supervisor and the candidate, and assessed their previous achievements in the stated research area. Based on the facts outlined in this report, the Committee concludes the following:

- the proposed topic is suitable for a doctoral dissertation,
- the proposed research, hypotheses, objectives, methodology, and expected results are well-conceived and appropriate for the preparation of a doctoral dissertation,
- the candidate, Milan Todorović, MSc in Computer Science, is eligible to undertake the proposed doctoral dissertation and
- Prof. Miodrag J. Mihaljević, PhD, Scientific Advisor at the Mathematical Institute of the Serbian Academy of Sciences and Arts and Corresponding Member of SASA (since 2021), is eligible to serve as the supervisor for the proposed doctoral dissertation.

Based on the above conclusions, the Committee proposes to the Teaching-Scientific Council of

the Faculty of Technical Sciences in Novi Sad and to the relevant bodies of the University of Novi Sad to approve the doctoral dissertation topic entitled: "New Additions to Blockchain Technology Techniques and Applications in Electricity Trading" (Serbian: „Нови прилози техникама блокчејн технологија и применама у трговини електричном енергијом“)
submitted by the candidate Milan Todorović, and to appoint Prof. Miodrag J. Mihaljević, PhD, Scientific Advisor at the Mathematical Institute of the Serbian Academy of Sciences and Artsand Corresponding Member of SASA, as the dissertation supervisor.

Place and date: Novi Sad, May 28. 2025.

1. dr Zoran Ognjanović, Research Professor
_____, chair

2. dr Silvia Gilezan, Full Professor
_____, member

3. dr Milena Vujošević Janičić, Associate Professor
_____, member

4. dr Tatjana Davidović, Research Professor
_____, member

5. dr Dinu Dragan, Associate Professor
_____, member

6. dr Jovana Dedeić, Assistant Professor
_____, member

NOTE: *A member of the Committee who does not wish to sign the report due to disagreement with the opinion of the majority is required to provide a written explanation within the report, stating the reasons for refusing to sign it, and must sign that explanation.*