Journal of Turkish

Operations Management

Blockchain technology and the applicability of digital clustering in the defense industry [1]

Aygül Aytaç[1*], Serhat Çakır[2]
[1] The Ministry of National Defense, Ankara, Türkiye
e-mail: aygul04020112@gmail.com, ORCID No: http://orcid.org/0000-0003-1716-213X
[2] Başkent University, Faculty of Economics and Administrative Sciences, Department of Technology and Knowledge Management, Ankara, Türkiye
e-mail: serhatc@baskent.edu.tr, ORCID No: http://orcid.org/0000-0002-1588-1360

Article Info

Article History:
Received :
Revised :
Accepted :

Keywords:

Blockchain,
Digital clustering,
Defense industry,
Data security,
Innovation

Abstract

This article provides an in-depth analysis of the potential uses and benefits of blockchain technology and digital clustering within the defense industry. Owing toits decentralized architecture and robust security features, blockchain has attractedconsiderable attention, especially in high-risk sectors such as defense. Its capacityto facilitate secure data exchange, ensure traceability, and improve operational efficiency makes it particularly valuable. Meanwhile, digital clustering emerges asa promising approach for fostering innovation and strengthening cooperation among defense stakeholders. Employing a literature review and case analysis methodology, this study explores the feasibility and implications of integrating these technologies into defense systems. The findings suggest that, when effectively implemented, blockchain and digital clustering can offer substantial gains in term of data security, traceability, and sector-wide innovation.

1. Introduction

The defense industry plays a critical role in ensuring national security and requires the highest levels of security, efficiency, and innovation (Aytaç, 2023; 2024a; 2024b). This sector demands rapid adoption and implementation of technological innovations. The integration of advanced technologies such as blockchain and digital clustering is seen as a strategic move to solve existing problems in the defense industry and make it more competitive.

Blockchain technology is known for its decentralized and secure structure. Since this technology ensures that data cannot be altered without consensus, it offers a significant advantage in data security. The security and integrity of sensitive data are crucial, especially in the defense industry (Aytaç and Çakır, 2023). Blockchain technology provides great value to the sector by ensuring the secure storage and traceability of this data (Aytaç, 2023, 2024a; Nakamoto, 2008). Moreover, the transparency and immutability features of blockchain offer critical benefits in the management and monitoring of supply chains, thus preventing counterfeit products from entering the supply chain and enhancing operational reliability (Kshetri, 2018).

Digital clustering, on the other hand, creates collaborative environments that enhance innovation and efficiency in the defense industry. Digital clustering encourages collaboration and facilitates information sharing among companies, research institutions, and other stakeholders operating in the defense industry. As a result, actors within the sector can benefit from each other's competencies and develop joint projects. This collaborative structure provided by digital clustering is particularly important in the process of developing and implementing new defense technologies (Cooke, 2002; Porter, 1998).

[1] An earlier version of this paper was presented at the 6th International Engineering and Technology Management Summit, held by Başkent University, 17-19 October 2024.

This article explores the convergence of blockchain and digital clustering technologies and evaluates their potential applications within the defense industry through an analysis of current literature and relevant case studies. The primary objective is to gain deeper insight into how these technologies can be synergistically implemented to support defense capabilities. Within this framework, the integration of blockchain and digital clustering holds considerable promise for enhancing data security, traceability, innovation, and operational efficiency in defense-related contexts.

2. Literature Review

2.1. Blockchain Technology in the Defense Industry

Blockchain technology has moved beyond cryptocurrencies to become a solid solution for secure data management in various industries. Its decentralized structure ensures that data cannot be altered without consensus, providing a high level of security (Aytaç, 2024; Aytaç and Çakır 2023; Nakamoto, 2008). In the defense industry, blockchain can be used to secure communication channels, manage supply chains, and ensure the integrity of sensitive data (Ketels, 2013). This is a significant advantage in ensuring cybersecurity in the defense sector. For example, the immutability of blockchain records protects critical defense information by preventing unauthorized access and changes (Aytaç, 2023; Yli-Huumo, Ko, Choi, Park and Smolander, 2016). This is particularly important in a sector where data breaches and cyberattacks can have serious consequences for national security (Zhang, Xue and Liu, 2019).

Blockchain technology also plays an important role in ensuring traceability in supply chains. Recording every step in the supply chain makes it possible to verify the accuracy and authenticity of components and products. Thus, the inclusion of counterfeit or low-quality components in the supply chain can be prevented, enhancing the reliability of defense equipment. This feature of blockchain is critically important for ensuring the quality and reliability of equipment used in military operations (Kshetri, 2018).

2.2. Digital Clustering for Innovation and Collaboration

Digital clustering involves creating collaborative networks among companies, research institutions, and other stakeholders to promote innovation and efficiency (Porter, 1998). Digital clustering facilitates information sharing and joint development projects within the defense industry, leading to significant progress (Cooke, 2002). As a result, costs can be reduced, and processes can be accelerated in the development of new technologies. Clusters can be geographic or virtual, using digital platforms to overcome physical barriers and increase collaboration (Ketels, 2013). This feature of digital clustering allows actors in the defense industry to collaborate globally and combine their expertise. For instance, digital clusters can facilitate the rapid prototyping and testing of new defense technologies by pooling resources and expertise from multiple organizations (Muro and Katz, 2010).

Digital clustering can also enhance the effectiveness of research and development (R&D) activities in the defense industry. R&D projects bring different stakeholders together to work towards common goals, accelerating the development of new technologies (Poter, 1998). Through digital clustering, innovative solutions in the defense industry can be brought to market more quickly, providing a competitive advantage in the sector.

2.3. Synergy Between Blockchain and Digital Clustering

The synergy between blockchain technology and digital clustering can address various challenges faced by the defense industry. Blockchain enhances the security and traceability of information shared within digital clusters, ensuring that all participants have access to accurate and immutable data (Aytaç, 2024; Swan, 2015). This can lead to more efficient collaboration and innovation since stakeholders can trust the integrity of shared data. Additionally, the transparency provided by blockchain increases accountability and governance within digital clusters, further enhancing their effectiveness.

This synergy between blockchain and digital clustering ensures that defense industry projects are carried out more efficiently and that the results are more reliable. For example, in cases where multiple stakeholders are involved in a defense project, blockchain technology can be used to transparently monitor each stakeholder's contributions and progress within the process. This allows potential delays or errors in projects to be quickly identified and resolved.

Using blockchain within digital clusters also enhances information security, making it possible to conduct collaborative work more reliably. The data integrity and security provided by blockchain are crucial in innovation processes conducted within clusters. Thus, different organizations working on joint projects in the defense industry can increase their trust in each other and develop more effective collaboration (Tapscott and Tapscott, 2016; Saberi, Kouhizadeh, Sarkis and Shen 2019; Casino, Dasaklis and Patsakis, 2019).

3. Methods

This study employed a qualitative research methodology, including an extensive literature review and practical case analyses, to evaluate the potential applications and advantages of blockchain technology and digital clustering in the defense industry. The literature review was conducted to explore existing research and theories on blockchain and digital clustering technologies, with a specific focus on their use in the defense sector. Various academic articles, reports, and case studies were analyzed to understand the theoretical foundations and practical implications of these technologies.

For the case analysis, specific examples from the defense industry were examined to illustrate the practical applications and challenges of integrating blockchain and digital clustering. These case studies provided insights into the operational benefits, potential risks, and best practices for implementing these technologies.

Data collected from the literature and case studies were systematically analyzed to identify key themes, patterns, and relationships. This approach enabled the study to provide a comprehensive understanding of how blockchain and digital clustering could synergize to enhance data security, traceability, and innovation in the defense industry. Since the study is a literature review, there is no need for ethical committee approval.

2.4. Case Studies

2.4.1. Blockchain in Defense Supply Chains

One of the important applications of blockchain in the defense sector is supply chain management. Kshetri's (2018) study emphasizes how blockchain can prevent counterfeit products from entering the supply chain. By providing a transparent and immutable record of the source and movements of a product, blockchain ensures that only verified components are used in defense production. This traceability increases the reliability and quality of defense equipment, ensuring operational security.

This traceability and transparency also enable different stakeholders involved in digital clustering processes to share data with each other in a reliable manner, creating synergy in collaborative innovation and supply chain management. For example, when each stage of the components used in the production of defense equipment is recorded with blockchain, information such as where these components were sourced, what tests they underwent, and when they were manufactured can be easily traced. This prevents counterfeit products from being included in the supply chain, increasing the success of defense projects.

2.4.2 Digital Clustering for Innovation

Digital clustering has been successfully applied to increase innovation in various defense projects. A case study by the European Defense Agency (EDA, 2020) shows how digital clusters facilitate joint R&D projects across different countries, leading to the development of advanced defense technologies. These clusters significantly reduce the time and cost associated with defense innovation by enabling real-time information sharing and collaborative problem-solving.

Digital clustering plays a critical role in accelerating innovation and reducing costs in the defense industry. The collaboration of defense companies and research institutions from different countries in joint projects accelerates the development process of new technologies. Such collaborations enable more efficient management of R&D processes, which require significant time and cost in the defense industry.

The cost and time advantages provided by digital clustering are an important factor supporting the use of blockchain technology in processes. Blockchain technology ensures that data shared within digital clusters is secure and traceable, speeding up collaboration and reducing process costs. The data sharing conducted through blockchain by different actors within digital clusters saves time in R&D processes and increases operational

efficiency. Thus, it becomes possible to reduce costs and implement innovative solutions more quickly in projects supported by digital clustering.

4. Findings

This study systematically reviewed the literature to identify the applicability and synergistic potential of blockchain technology and digital clustering within the defense industry. The findings are presented below, with references to key studies that support the conclusions.

1. Blockchain Technology and Data Security

Blockchain's decentralized and immutable structure enhances data security, a critical requirement for the defense industry. Studies such as Yli-Huumo et al. (2016) and Zhang et al. (2020) highlight that blockchain effectively prevents unauthorized alterations and ensures the integrity of sensitive information, reducing risks of cyberattacks and data breaches. Furthermore, Kshetri (2018) and Aytaç (2024) demonstrated blockchain's role in securing communication channels and ensuring traceability in defense supply chains. By providing a transparent ledger of all transactions, blockchain prevents counterfeit components from infiltrating supply chains, a persistent challenge in the defense sector.

2. Digital Clustering and Innovation

Digital clustering has been shown to foster innovation by creating networks among defense companies, research institutions, and other stakeholders (Porter, 1998; Cooke, 2002). These clusters promote real-time knowledge sharing and collaborative problem-solving, accelerating the development of advanced defense technologies (Ketels, 2013). According to the European Defense Agency (EDA, 2020), digital clusters significantly reduce costs and time for R&D projects. This finding is supported by Muro and Katz (2010), who emphasize the efficiency gains from pooling resources and expertise across geographic and institutional boundaries.

3. Synergy Between Blockchain and Digital Clustering

The integration of blockchain technology within digital clusters enhances security and trust among participants. Swan (2015) noted that blockchain’s transparency and immutability provide an additional layer of accountability, essential for collaborative innovation in sensitive industries like defense. Aytaç (2023) and Kshetri (2017) emphasized that blockchain can ensure secure data sharing within clusters, reducing coordination inefficiencies and enhancing operational reliability. For instance, blockchain-based systems track contributions and progress of each stakeholder in a cluster, ensuring project accountability and timely identification of bottlenecks.

4. Case Studies Supporting Practical Applications

A notable application of blockchain in defense supply chains was documented by Kshetri (2017, 2025), where the technology ensured authenticity and prevented the inclusion of counterfeit components. This enhanced trust in supply chain operations and improved overall equipment reliability. The European Defense Agency's case studies (EDA, 2020) illustrate successful implementation of digital clusters in cross-border R&D collaborations. These clusters facilitated the rapid prototyping and testing of new technologies, leading to competitive advancements in defense systems.

5. Challenges and Future Directions

Despite its benefits, blockchain's integration with digital clustering requires standardized protocols to ensure interoperability, as emphasized by Zheng et al. (2018) and Zyskind & Nathan (2015). Variations in blockchain platforms and regulatory inconsistencies across nations pose challenges for seamless collaboration. To overcome these barriers, Aytaç (2024) recommends the establishment of pilot projects to evaluate blockchain’s scalability and effectiveness within digital clusters, while Muro and Katz (2010) suggest developing common frameworks to guide cluster formation and governance.

In conclusion, the systematic review highlights that blockchain and digital clustering technologies, when integrated, hold transformative potential for the defense industry. However, addressing interoperability and governance challenges remains critical for maximizing their combined benefits.

As seen in Table 1, the integration of blockchain and digital clustering in the defense industry offers enhanced security, innovation, and collaboration while addressing interoperability challenges.

Table 1. Blockchain and digital clustering themes and categories

Theme	Category	Key References	Key Insights
Blockchain Technology and Data Security	Enhancing data security in the defense industry	Yli-Huumo et al. (2016); Zhang et al. (2020); Kshetri (2018); Aytaç and Çakır (2023)	Blockchain prevents unauthorized alterations and enhances data traceability in supply chains.
Digital Clustering and Innovation	Fostering innovation and collaboration	Porter (1998); Cooke (2002); Ketels (2013); EDA (2020); Muro and Katz (2010)	Clusters promote knowledge sharing, reducing costs and time for R&D projects.
Synergy Between Blockchain and Digital Clustering	Improving trust and operational efficiency	Swan (2015); Aytaç (2024); Kshetri (2017)	Integration of blockchain enhances security and accountability in digital clusters.
Case Studies Supporting Practical Applications	Practical applications in supply chains and R&D	Kshetri (2018); EDA (2020)	Blockchain ensures component authenticity; clusters accelerate technology prototyping.
Challenges and Future Directions	Addressing standardization and interoperability challenges	Zheng et al. (2018); Zyskind & Nathan (2015); Aytaç (2024); Muro and Katz (2010)	Standardized protocols and regulatory consistency are needed for interoperability.

As demonstrated in Table 1, the integration of blockchain technology and digital clustering presents significant transformative potential for the defense industry. It underscores advancements in data security, innovation-oriented collaboration, enhanced trust and accountability mechanisms, and practical applications in supply chain management and research and development processes. Additionally, the analysis highlights the critical necessity of establishing standardized protocols and governance frameworks to address interoperability challenges effectively.

6. Discussion

The integration of blockchain technology and digital clustering into the defense industry offers a transformative potential that can significantly enhance efficiency, trust, and security in defense-related processes. Blockchain technology, by its very design, ensures immutable record-keeping, decentralized control, and transparent data sharing. These features are particularly valuable in defense supply chains, procurement, logistics, and lifecycle management of critical equipment (Aytaç, 2024; Erol ve Eraslan, 2024; Xu et al., 2019; Kshetri, 2025). For instance, traceability enabled by blockchain can reduce fraudulent activities in the acquisition of sensitive components, while smart contracts may improve the automation and reliability of transnational agreements (Casino, et al., 2019; Hardjono and Smith 2019).

However, despite these potential benefits, the integration of blockchain into a complex and hierarchical ecosystem such as the defense sector is fraught with both technical and institutional challenges. One of the primary technical hurdles is interoperability. Different organizations including NATO member states, private defense contractors, and national defense ministries may utilize different blockchain platforms (e.g., Ethereum, Hyperledger, or private blockchains), which lack standardized communication protocols (Zheng et al., 2018). This fragmentation can inhibit seamless data exchange and collaborative workflows. Thus, establishing interoperable and standardized blockchain frameworks is critical (Hardjono and Smith, 2019).

Moreover, the implementation of blockchain demands substantial changes in the existing organizational architecture. Defense institutions are traditionally structured around hierarchical, risk-averse frameworks, which may resist the decentralization and transparency inherent to blockchain systems (Tapscott and Tapscott, 2016). To

overcome institutional inertia, a phased adoption model accompanied by pilot projects and policy sandboxes can be effective in demonstrating feasibility and building institutional confidence (Yaga et al., 2018).

Another equally crucial aspect is the governance and compliance structure required for transnational blockchain collaborations. As defense systems often involve multinational stakeholders, establishing mutual trust, legal alignment, and shared protocols becomes paramount. This calls for internationally recognized blockchain governance models that define roles, access rights, and auditing capabilities for all parties involved (Beck et al., 2017). In this regard, NATO and similar alliances can play a facilitating role in setting cross-border blockchain standards.

Parallel to blockchain, digital clustering the strategic co-location and network formation of defense-related industries, R&D institutions, and logistics hubs offers its own advantages. Digital clusters can accelerate innovation diffusion, reduce response times in crisis logistics, and foster public-private synergies (Ketels, 2013). However, these benefits are contingent upon trust and data sharing between stakeholders within the cluster. Establishing this collaborative infrastructure often requires national-level policy incentives, cybersecurity assurances, and cultural shifts toward cooperative competition (Özceylan and Tanyaş, 2023; Porter, 1998; European Commission, 2020).

In conclusion, while blockchain and digital clustering present immense strategic opportunities for transforming the defense industry, their success depends on overcoming interoperability issues, organizational resistance, and governance gaps. A multilateral, standards-driven, and trust-based approach is necessary to harness the full potential of these technologies.

7. Conclusion and Recommendations

The integration of blockchain technology and digital clustering represents a transformative development opportunity for the defense industry, particularly in an era marked by rapid technological advancement, global security challenges, and the need for adaptive innovation strategies. Blockchain's decentralized, transparent, and tamper-resistant nature offers significant advantages in terms of data integrity, supply chain security, contract enforcement, and logistics traceability. Simultaneously, digital clustering facilitates the creation of collaborative innovation ecosystems by bringing together key stakeholders defense contractors, SMEs, academic institutions, research centers, and governmental organizations under a shared strategic framework.

When effectively integrated, these two technologies can complement each other to significantly enhance the resilience, agility, and competitiveness of national and allied defense ecosystems. Blockchain ensures the secure, verifiable flow of information, while digital clustering enables dynamic, interdisciplinary collaboration and faster diffusion of technological advances. However, the full realization of these benefits hinges on addressing key implementation challenges, including technical interoperability, stakeholder coordination, policy alignment, and cybersecurity considerations. In this context, the following recommendations have been developed:

1. Development of International Standards and Frameworks
There is an urgent need to establish international standards for the deployment of blockchain and digital clustering technologies in defense. Standardization efforts should be coordinated through multinational bodies such as NATO, the European Defence Agency (EDA), and national standardization organizations. These standards will help reduce fragmentation, ensure cross-border interoperability, and create a common language among defense stakeholders operating in different jurisdictions.

2. Ensuring Interoperability through Shared Protocols and Platforms
The defense industry is a heterogeneous environment composed of various systems, platforms, and actors. To ensure seamless integration, interoperability protocols and modular architectures must be developed for both blockchain applications and digital cluster ecosystems. Open-source frameworks and common application programming interfaces (APIs) should be encouraged to enable flexible and secure data exchange among allies and partners.

3. Fostering a Strong Ecosystem of Collaboration and Trust
The success of digital clustering relies heavily on mutual trust, aligned objectives, and sustained collaboration. Governments should provide incentives for public-private partnerships (PPPs), cross-sectoral joint ventures, and collaborative R&D initiatives. Platforms for regular multilateral dialogue, such as defense innovation forums and working groups, should be institutionalized to reinforce trust and build shared strategic agendas.

4. Increasing Education, Capacity Building, and Stakeholder Awareness
Widespread adoption of emerging technologies requires a deep understanding of their technical, operational, and strategic implications. Defense stakeholders including military personnel, policymakers, engineers, and procurement officials should receive tailored training programs, certification modules, and technical workshops on blockchain and digital clustering. This will enhance digital literacy and facilitate smoother transition and uptake of new systems.

5. Strengthening Data Security, Privacy, and Compliance
While blockchain offers high levels of transparency and traceability, these characteristics may conflict with the confidentiality and compartmentalization requirements of defense data. Therefore, privacy-preserving techniques such as zero-knowledge proofs, homomorphic encryption, and permissioned blockchain networks should be developed and implemented. Additionally, clear regulatory frameworks should be established to ensure compliance with national and international security standards.

6. Launching Pilot Projects and Testbeds for Validation
Before large-scale implementation, pilot projects should be initiated to test the viability, scalability, and integration challenges of blockchain and clustering technologies in real-world defense scenarios. These testbeds should be designed to simulate multi-actor environments and assess performance under operational conditions. Lessons learned from these pilots can inform national strategies and guide broader rollouts.

7. Strategic Roadmaps and Policy Integration
Defense ministries and related agencies should develop strategic roadmaps outlining how blockchain and digital clustering will be integrated into their broader defense transformation plans. These roadmaps should include milestones, resource allocations, and impact assessment metrics, and should be aligned with national digitalization and innovation policies.

In the coming years, defense organizations must prioritize standardization, interoperability, and cross-sectoral collaboration to fully capitalize on the potential of blockchain and digital clustering. As security threats become more asymmetric and supply chains more globalized, the ability to innovate securely and cooperatively will define a nation's strategic advantage. By investing in these technologies today supported by thoughtful governance, inclusive stakeholder engagement, and robust technical infrastructure countries can lay the groundwork for a more agile, secure, and innovative defense industry of the future.

Contributions of Authors

Aygül Aytaç: Conceptualization, Supervision, Methodology, Validation, Writing – original draft, **Serhat Çakır:** Methodology, review and editing.

Conflicts of Interest

No potential conflicts of interest were reported by the authors.

References

Aytaç, A. (2023). Milli savunma sanayiinde blok zincir teknolojisinin uygulanması sürecinde karşılaşılan sorunlar ve çözüm önerileri. *II. Uluslararası Korkut Ata Bilimsel Araştırmalar Konferansı Bildiriler Kitabı*, 345-360.

Aytaç, A. (2024a). *Milli savunma sanayiinde blok zincir model önerisi* (Doktora tezi, Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü, Savunma Yönetimi Anabilim Dalı). https://avesis.metu.edu.tr/yonetilen-tez/e65da4c4-4b41-4e0d-a629-e5cc142d47fb/milli-savunma-sanayinde-blokzincir-model-onerisi

Aytaç, A. (2024b). Ahilik teşkilatı, organize sanayi bölgeleri ve blok zincir teknolojisi entegrasyonu. *VII. Uluslararası Ahilik ve Ahi Evran Sempozyumu Bildiriler*. https://ahiliksempozyumu2024.ahievran.edu.tr/ahilik2024_sempozyum_programi.pdf

Aytaç, A., & Çakır, S. (2023). An analysis of the feasibility of blockchain technology in the national defense industry. *Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi (KAÜİİBFD)*, 14(27), 525–541. https://doi.org/10.36543/kauiibfd.2023.021

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research. Business & Information Systems Engineering, 59(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Cooke, P. (2002). *Knowledge economies: Clusters, learning and cooperative advantage*. Routledge.

Erol, M., & Eraslan, E. (2024). Nesnelerin İnterneti, Uygulama Alanları ve İş Sağlığı ve Güvenliği İle Etkileşimi. Journal of Turkish Operations Management, 8(1), 73-89. https://doi.org/10.56554/jtom.1258262

European Commission. (2020). *Clusters and industrial transformation*. https://ec.europa.eu/growth/industry/policy/cluster_en

European Defense Agency (EDA). (2020). *Annual report*. https://eda.europa.eu/docs/default-source/eda-annual-reports/eda-annual-report-2020.pdf

Hardjono, T., & Smith, N. (2019). Decentralized Trusted Computing Base for Blockchain Infrastructure Security. Front. Blockchain 2:24. http://doi: 10.3389/fbloc.2019.00024

Ketels, C. (2013). Recent research on competitiveness and clusters: What are the implications for regional policy? *Cambridge Journal of Regions, Economy and Society*, 6(2), 269–284. http://doi.org/10.1093/cjres/rst008

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027–1038. http://doi.org/10.1016/j.telpol.2017.09.003

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. http://doi.org/10.1016/j.ijinfomgt.2017.12.005

Kshetri, N. (2025). Blockchain and supply chain management. *TNQ Technologies*, 2nd Edition, p.87

Muro, M., & Katz, B. (2010). The new "cluster moment": How regional innovation clusters can foster the next economy. *Brookings Institution*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Erişim adresi: https://bitcoin.org/bitcoin.pdf

Özceylan, A., & Tanyaş, M. (2023). Sürdürülebilir İnsani Yardım Lojistiği Alanındaki Yayınların İçerik ve Bibliometrik Açıdan Analizi. *Journal of Turkish Operations Management*, 7(2), 1644-1671. https://doi.org/10.56554/jtom.1214269

Porter, M. E. (1998). Clusters and the new economics of competition. *Harvard Business Review*, 76(6), 77–90.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world* [Kindle version]. Penguin Publishing Group. https://www.amazon.com/Blockchain-Revolution-Technology

Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer. https://doi.org/10.1007/978-3-319-99058-3

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (NIST Interagency/Internal Report (NISTIR) 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLOS ONE*, 11(10), e0163477. http://doi.org/10.1371/journal.pone.0163477

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3), 1–34. http://doi.org/10.1145/3316481

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (ss. 557–564). IEEE. http://doi.org/10.1109/BigDataCongress.2017.85

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (ss. 180–184). IEEE. http://doi.org/10.1109/SPW.2015.27