Teknik Koordinatör / Technical Coordinator

Sekreterlik / Secretarial

mahmud.mutlu@hbv.edu.tr, hanefi.calp@hbv.edu.tr

Ankara Hacı Bayram Veli Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, Emniyet Mahallesi, Muammer Bostancı Caddesi, No:4, 06500 Beşevler/Ankara, Türkiye

İÇİNDEKİLER (Cilt: 6 / Sayı: 1 - Haziran 2024)

Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Araştırma Makalesi / Research Article

Yönetimde Metaverse Araştırmaları: Bibliyometrik Bir Analiz

İbrahim DURMUŞ*,a

[a,*] *Bayburt Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu, Ulaştırma Hizmetleri Bölümü, Posta Hizmetleri Programı, Bayburt, Türkiye*

MAKALE BİLGİSİ

Alınma: 23.11.2023
Kabul: 13.03.2024

Anahtar Kelimeler:
Bibliyometrik Analiz,
Organizasyonlar,
Metaverse,
Yönetim

Sorumlu Yazar
e-posta:
ibrahimdurmus@bayburt
.edu.tr

ÖZET

Organizasyonlar geleceğe yönelik amaçlarını gerçekleştirebilmek için teknolojik yenilikleri iş faaliyetlerine adapte etmişlerdir. Bu durum metaverse teknolojisinin organizasyon politikalarında yer almasını sağlamıştır. Organizasyon politikalarına yön veren yönetim mekanizması, metaverse uygulamalarını iş faaliyetlerine eklemiştir. Yönetimde metaverse araştırmalarında, literatürde yer alan araştırmalar incelenmiştir. Analizler Web of Science (WoS) veri tabanı yardımı ile bibliyometrik analizler kullanılarak gerçekleştirilmiştir. Araştırma konusuna ilişkin toplam 289 araştırmada, vurgulanan kelimelere, yazarlara, kullanılan kaynaklara ve ilişkilere yer verilmiştir. Araştırma sonucunda yönetimde metaverse araştırmalarının teknolojik değişim ve gelişime bağlı olarak pazarlama, turizm, eğitim, sağlık ve endüstri gibi birçok alanla ilişkili olduğu görülmüştür. Araştırma sonuçları metaversenin artık birçok organizasyonun politikasına yön verebildiğini göstermiştir.

DOI: 10.59940/jismar.1394934

Metaverse Studies in Management: A Bibliometric Analysis

ARTICLE INFO

Received: 23.11.2023
Accepted: 13.03.2024

Keywords:
Bibliometric analysis,
Organizations,
Metaverse, Management

Corresponding Authors
e-mail:
ibrahimdurmus@bayburt
.edu.tr

ABSTRACT

Organizations have adapted technological innovations to their business activities to realize their future goals. This has enabled metaverse technology to take place in organizational policies. The management mechanism that directs organizational policies has added metaverse applications to business activities. In management metaverse research, studies in the literature were examined. Analyzes were performed using bibliometric analyses with the help of the Web of Science (WoS) database. A total of 289 studies on the research subject included the highlighted words, authors, sources, and relationships. As a result of the research, it has been seen that metaverse studies in management are related to many areas such as marketing, tourism, education, health, and industry, depending on technological change and development. Research results have shown that the metaverse can now shape the policy of many organizations.

DOI: 10.59940/jismar.1394934

1. INTRODUCTION *(GİRİŞ)*

The interest in technology in people has led to many innovations to direct the activities in business life day by day. Technological changes have also changed the interests of individuals. In this respect, technological innovations such as the metaverse (or virtual universe) are among the strategic plans of many managers in today's organizations. Managers who can adapt Metaverse technology to their business activities will have the ability to compete with their competitors. The practical information that Metaverse applications will provide in business activities provides serious advantages to organizations. The research is aimed to clarify metaverse research in management from the perspective of organizations.

From an organizational perspective, the metaverse can be viewed as a business opportunity, not a technological problem. Metaverse provides efficiency, profitability, interaction, and communication in many business areas [1]. This allows the metaverse to be examined at the organizational level. Employees' work activities may be affected by the use of the metaverse. This situation makes it necessary for the management of the organization to consider the metaverse applications in their business activities.

The world of the metaverse can be both beneficial and harmful. Just as social media has its good and bad sides, so does the metaverse [2]. This shows that metaverse applications in management can have positive or negative results. In particular, the usage area of metaverse applications affects employees and other stakeholders (consumers, partners, society, and others). To achieve beneficial results, metaverse applications and the organizational system must carry out activities together. In this respect, the metaverse in management is a very effective system for the future of organizations.

The metaverse is a complex global system that is active outside of traditional or local areas. This situation shapes the meta-universe of governance and regulation, governments, and organizations suitable for virtual worlds [3]. The adaptability of this system to business activities by organizations may pose a serious problem for some organizations. Metaverse transformation can be difficult in organizations that do not have sufficient facilities or infrastructure. In organizations that carry out technology-oriented business activities, the use of metaverse can become more functional. In this case, organizational possibilities become effective. Both employee and consumer-based access opportunities affect the usage area of metaverse applications.

How the metaverse is adapted to an organization's overall strategy and business model is important. Organizations can develop their metaverse repository or invest in an established metaverse repository [4]. In this respect, metaverse applications and organizational activities should work in coordination. Effectively, metaverse applications contribute to the practicality and access possibilities of the work.

In organizations, management has a say in many decisions such as directing organizational policies, shaping future activities, and determining the application areas of employees. Metaverse applications are affected by the management mechanism in the organization. In this context, the research focuses on the metaverse perspective in management.

2. THEORETICAL FRAMEWORK *(TEORİK ÇERÇEVE)*

2.1. Metaverse *(Metaverse)*

The metaverse, which is the next stage of internet development, is expressed as the universe created by the mental perceptions of individuals using virtual reality tools without physical effort. Many people or organizations in the world are rapidly entering the metaverse process [6]. For example, Çelik et al. emphasized that today individuals and organizations can use the metaverse in their business activities [31]. Additionally, Mehta et al. stated that the metaverse facilitates people's communication with each other in many sectors of the business world [1]. Metaverse is a 3D virtual world where many activities can be done with augmented and virtual reality technology. The world of the metaverse is like the real world with the technology it uses (such as tablets, smartphones, smart glasses, headphones, and gloves) [7]. The use of metaverse in organizations brings innovations to the work activities of employees. In addition, the tools used in the workplace (such as machinery, and equipment) are also affected by this innovation. Technological changes bring new perspectives to the field of activity and the future goals of many organizations.

The features of the metaverse deliver an accessible, affordable, usable, beautiful experience and value: it ensures that it is used by users who are ready for technology and are competent in technology [8]. In terms of organizations, this can happen under the control of management. The organizational policies implemented by the management mechanisms affect the application area of the employees. In this respect, the use of metaverse in the organization is the result of management policies.

2.2. Organizational Management *(Organizasyonel Yönetimler)*

Managers in organizations must have the knowledge and skills to apply new technologies effectively. Organizations' adoption of technological developments is effective for competition in the digital age. Managers should be able to respond to the needs of the staff and the organization as well as improve themselves [5]. There is a great need for human and machine collaboration in organizations, especially in environments that carry out technology-oriented activities. This shows the effectiveness of metaverse applications in organizations. The ability of

management to transfer their technological experience to employees contributes to the implementation of organizational policies.

Some organizations today are making strong investments in the metaverse. Metaverse is very important for the future of organizations. Metaverse provides opportunities to build a business in organizations. In addition, in the metaverse, there is virtual reality that is not limited by natural resources [9]. Organizations that can provide continuity in the future are those that can adapt to technological changes and harmonize the changes with their goals. Organizations that can adapt quickly and securely to metaverse change can achieve many goals sooner than their competitors.

3. METHODOLOGY *(METODOLOJİ)*

The research method was carried out within the framework of metaverse research in management. In the literature, metaverse research in management in the WoS database has been taken into account. No year or research-type limitations were made in the analysis. In the research application, bibliometric analyses were used. In the bibliometric analysis method, the social and structural relationships of different research components (such as subjects, institutions, authors, and countries) can be revealed [29]. In the research, the keyword searched in the WoS database was "Metaverse in Management". There was no category limitation in the research. Other information on the research methodology is as follows.

3.1. Bibliometric Analysis and R Program *(Bibliyometrik Analiz ve R Programı)*

In bibliometric applications, one or more bibliometric analysis or statistical software can be used for data analysis [26]. The bibliometric analysis package is an application written in R. R is software with an ecosystem running in an integrated environment of accessible books, algorithms, and graphics software [27]. In addition, biblioshiny, which is used with this software and has a powerful library feature, is divided into 7 categories. The biblioshiny categories are: 1) overview, 2) sources, 3) authors, 4) documents, 5) conceptual structure, 6) intellectual structure, and 7) social structure [28]. Metaverse bibliometric analyses in management were carried out using biblioshiny categories with the help of the R program.

Programs used in bibliometric analysis and mapping, such as SPSS and Pajek, and graphical interpretations of maps such as Vosviewer can be used [32]. It is emphasized in the literature that the application of bibliometric analyses in the R program is quite flexible, can be quickly upgraded, and can be integrated with other R packages. Researchers state that R is useful in constantly changing fields such as bibliometrics [26]. In this respect, bibliometric analyses were applied in the research with the help of the R program.

3.2. Basic Questions Related to the Research Problem *(Araştırma Problemine İlişkin Temel Sorular)*

In the analysis, solutions were sought for the following basic questions, taking into account the WoS database in metaverse research in management.

What is the general information (year, source, growth rate, number of authors, etc.) about metaverse research in management in the literature?

What are the title, author and highlighted keywords in metaverse research in management?

What are the trending topics in metaverse research in management, corresponding author countries and years?

What is the level of relationship between the concepts emphasized in metaverse studies in management?

What is the centralization and intensity of the concepts emphasized in metaverse studies in management?

How have the words emphasized in metaverse research in management changed over the years?

4. ANALYSIS RESULTS *(ANALIZ SONUÇLARI)*

Bibliometric analyzes of metaverse research in management were carried out on 26.07.2023. The studies in the WoS database were examined. The general results of the analysis are given below.

Table 1. Result of metaverse research in management *(Yönetimde metaverse araştırmaları sonucu)*

Main Information			
Timespan	*Sources*	*Documents*	*Annual growth rate*
2009-2023	*189*	*289*	*31.79%*
Authors	*Authors of single-aothored*	*International co-authorship*	*Co-authorsh per doc*
914	*33*	*42.91%*	*4.02*
Author's keywords	*References*	*Document average age*	*Average citations per doc*
1207	*15524*	*1.23*	*5.093*

As a result of the analysis, it was seen that metaverse research in management started in the WoS database in 2009. This shows that the research topic is quite up-to-date. It was understood that 289 studies from 189 different sources were included in the analysis. Annual growth rates of metaverse research in management represented a significant figure of 31.79%. This result reveals that there has been intense demand for metaverse research in management in recent years. As a result of the analysis, it was seen that 914 authors researched the subject, and studies with a single author consisted of 33 people. The rate of international co-authors in the study was 42.91%, and the rate of co-authors per study was 4.02. It is seen that the authors used 1207 keywords related to the metaverse in management and benefited from a total of 15524 sources. The average year of metaverse research in management is 1.23, with an average of 5,093 citations per research.

4.1. Metaverse Research in Management Annual Scientific Production Amount *(Yönetimde Metaverse Araştırmaları Yıllık Bilimsel Üretim Miktarı)*

The annual scientific production amounts of metaverse research in management are given in the figure below.

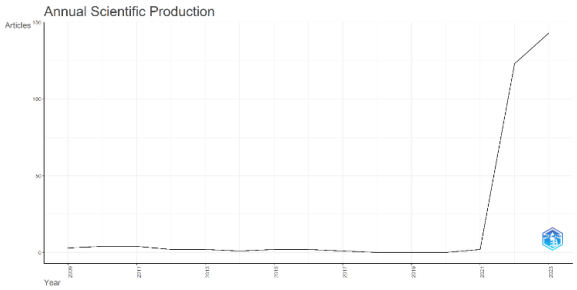


Figure 1. Metaverse in management, annual amount of scientific production
(Yönetimde metaverse yıllık bilimsel üretim miktarı)

As a result of the analysis, it is observed that metaverse research in management followed a horizontal course between 2009 and 2021. The results of the analysis show that metaverse research in management has increased significantly, especially after 2021. This situation reveals that metaverse research in management may have a more intense research network in the future.

4.2. Metaverse in Management Title, Author and Keyword Matching *(Yönetimde Metaverse Başlık, Yazar ve Anahtar Kelime Eşleşmesi)*

The concepts emphasized by the authors in the metaverse research in management, the authors conducting research on the subject and the keywords used in general are stated below.

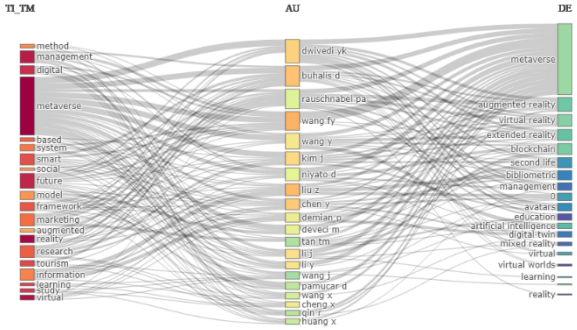


Figure 2. Metaverse research in management title, author and keyword matching
(Yönetimde metaverse araştırmaları başlık, yazar ve anahtar kelime eşleşmesi)

As a result of the analysis, in the title part of the authors' research: it has been observed that they mainly use the words method, management, digital, metaverse, based, system, smart, social, future, model, framework, marketing, augmented, reality, research, tourism, information, learning, study and virtual. Authors who carry out metaverse research in management: Dwivedi YK., Buhalis D., Rauschnabel PA., Wang FY., Wang Y., Kim J., Niyato D., Liu Z., Chen Y., Demian P., Deveci M., Tan TM, Li J. , Li Y., Wang J., Pamucar D., Wang X., Cheng X., Qin R., and Huang X. keywords used by the authors in metaverse research in management are: metaverse, augmented reality, extended reality, blockchain, second life, bibliometric, management, 0, avatars, education, artificial intelligence, digital twin, mixed reality, virtual, virtual worlds, learning and reality.

4.3. Metaverse in Management, Corresponding Author Countries *(Yönetimde Metaverse Sorumlu Yazar Ülkeleri)*

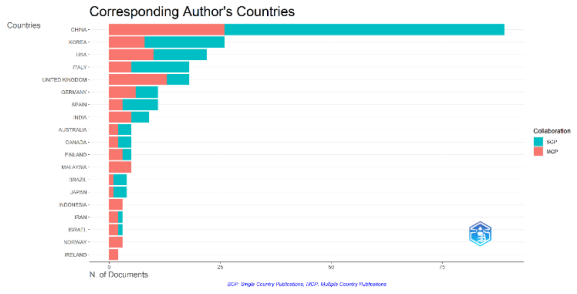


Figure 3. Metaverse studies in management, responsible author countries
(Yönetimde metaverse araştırmaları sorumlu yazar ülkeleri)

As a result of the analysis, the authors who carry out intensive research on the metaverse in management: are listed as China, Korea, USA, Italy, United Kingdom, Germany, Spain, India, Australia, Canada, Finland, Malaysia, Brazil, Japan, Indonesia, Iran, Israel, Norway, and Ireland. These results showed

that, in general, in developed and developing countries, a great deal of importance is given to metaverse research in management. Studies addressing Turkey on the subject were not included in the list. This situation shows that there is a great need for metaverse research in management for Turkey.

4.4. The Most Emphasized Words by the Authors in Metaverse Studies in Management *(Yönetimde Metaverse Araştırmalarında Yazarların En Fazla Vurguladığı Kelimeler)*

In the research, the most emphasized keywords by the authors in metaverse research in management are included. The relevant results are as follows.

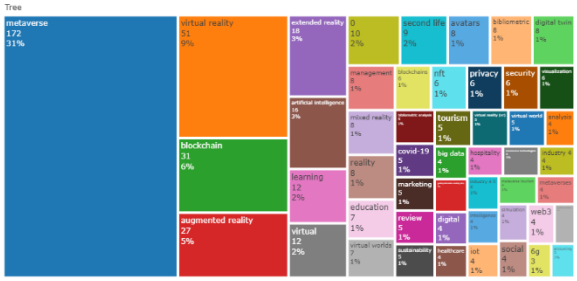


Figure 4. Keywords highlighted by authors in metaverse studies in management
(Yönetimde metaverse araştırmaları yazarların vurguladığı anahtar kelimeler)

The most emphasized words by the authors in metaverse research in management: metaverse, virtual reality, blockchain, augmented reality, extended reality, artificial intelligence, learning, virtual, 0, second life, management, avatars, bibliometric, mixed reality, reality, education, virtual worlds, blockchains, nft, privacy, security, visualization , bibliometric analysis, tourism, virtual reality, virtual world, covid-19, marketing, review, sustainability, analysis, big data, hospitality, digital, healthcare, industry, metaverse tourism, industry 4 0, metaverses, intelligence, simulation, web3, They are listed as iot, social, 6g and accounting. In addition to the metaverse being related to management, the results reached have relations with many different fields such as virtual realities, artificial intelligence, education, tourism, marketing, sustainability, health, industry, and social environments.

4.5. Trend Topics and Years in Metaverse Studies in Management *(Yönetimde Metaverse Araştırmalarında Trend Konular ve Yılları)*

Trending concepts in metaverse in management and the years they were trending are given below.

Figure 5. Trend topics and years of metaverse research in management
(Yönetimde metaverse araştırmaları trend konular ve yılları)

As a result of the analysis, it was observed that the years in which the metaverse concepts in management were trending generally belonged to the years 2022 and 2023. Trending concepts in metaverse research in management in 2022-2023: metaverse, blockchain, augmented reality, virtual reality, artificial intelligence. In the analysis, it has been observed that the concept of learning is a trend in 2022.

4.6. Keyword Relationships Emphasized in Metaverse Studies in Management *(Yönetimde Metaverse Araştırmalarında Vurgulanan Anahtar Kelime İlişkileri)*

The co-associations (relationships) of the words emphasized in metaverse research in management are given below. The colors and thicknesses of the lines in the figure reveal the ratio and strength of the relationships.

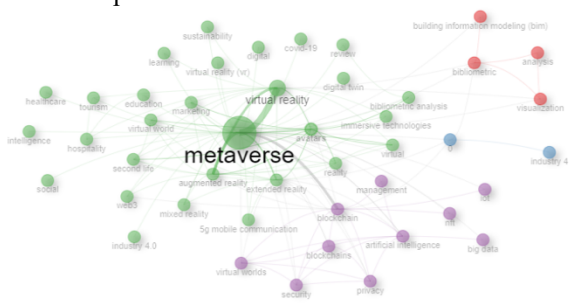


Figure 6. Keyword relationships highlighted in metaverse research in management
(Yönetimde metaverse araştırmaları vurgulanan anahtar kelime İlişkileri)

As a result of the analysis, it is understood that the metaverse has the strongest relationships with the words virtual reality, augmented reality, and blockchain. Considering the relationships between the lines representing the same color in the research:

virtual reality with metaverse, augmented reality, avatars, extended reality, reality, marketing, mixed reality, 5g mobile communication, digital twin, bibliometric analysis, immersive technologies, virtual, industry 4 0, web3, second life, virtual world, virtual reality, It has been observed that digital, covid-19, review, sustainability, learning, education, tourism, hospitality, social, healthcare and intelligence show strong relationships. As a result of the analysis, it has been understood that the words blockchains, management, nft, iot, 0, artificial intelligence, big data, privacy, security, and virtual worlds are related. In the analysis, it was seen that the words building information modeling, bibliometric, analysis, and visualization have associations together. In the obtained results, it has been observed that the metaverse is used quite extensively in research, and many concepts such as the virtual world, virtual reality, technology, industry, digitality, education, tourism, and artificial intelligence reveal strong relationships in metaverse research in management.

4.7. Centralization and Density of Keywords Emphasized in Metaverse Studies in Management

(Yönetimde Metaverse Araştırmalarında Vurgulanan Anahtar Kelimelerin Merkezileşme ve Yoğunluk Düzeyi)

In the figure, the centralization and density levels of the keywords emphasized by the authors in metaverse research in management are given. It has been stated in the studies that there are different visualization techniques in the thematic map. It is emphasized that these strategic diagrams are classified according to centrality and density measures. It has been stated that the variables in the charts are enriched with bibliometric measurements [20]. In the figure below, the words in each group in terms of centralization and density had strong relationships with each other. The words in the motor themes section have a high level of both density and centralization. The words in the motor themes section for metaverse research in management both reveal strong relationships and are extensively researched in the literature. It is understood that the centralization level of the words in the niche themes is low and the density is high. The level of density and centralization is low in the disappearing or newly emerging theme. In the simple themes section, there are words with high centralization and low density.

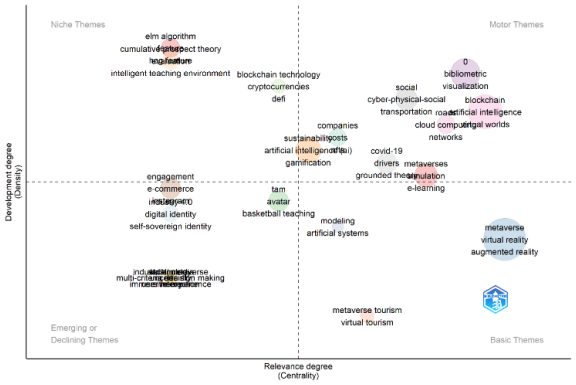


Figure 7. The level of centralization and density of keywords highlighted in metaverse research in management

(Yönetimde metaverse araştırmaları vurgulanan anahtar kelimelerin merkezileşme ve yoğunluk düzeyi)

As a result of the analysis of metaverse studies in management, it was observed that many words emphasized by the authors were included in the motor themes section. Motor themes are in the first group of words: blockchain, artificial intelligence, virtual worlds, blockchains, nft, privacy, security, iot, web3, and 5g mobile communication. Both the level of centralization and the intensity of these concepts are high. It is seen that concepts such as blockchain, artificial intelligence, virtual world, and mobile communication are effective in the metaverse relationship in management. The second set of motor themes: is 0, bibliometric, visualization, analysis, building information modeling, industry, design, internet of things (iot), non-fungible token (nft), and smart city. In the third group: the words social, cyber-physical-social, transportation, foundation model, organizations, organizations (daos), parallel management, and transformers were included. Fourth group: metaverse consists of the words simulation, e-learning, immersion, behavior, emerging Technologies, environment, learning management system, and virtual learning. In the fifth group word list: roads, cloud computing, networks, scene understanding, and software. The sixth group: is formed from the words covid-19, drivers, grounded theory, meta, pandemic, and tourism marketing. In the seventh group: The words companies, costs, nfts, trust, and value creation are included. The eighth group: consists of the words sustainability, artificial intelligence (ai), gamification, knowledge, game, data, data mining, experience, extended reality (xr), and games.

In the research, the first group of the niche themes section where the density is high and the level of centralization is low: is cumulative prospect theory, evaluation, intelligent teaching environment, Pythagorean fuzzy set theory, and teaching

importance. In the second group: the words elm algorithm, feature, hog feature, lbp, torsional neural network, and traffic sign recognition are included. The third group: blockchain technology consists of the words cryptocurrencies and defi.

The first group of disappearing or emerging themes: consists of the words engagement, e-commerce, Instagram, machine, satisfaction, shopping, and telepresence. In the second group: the words industry 4.0, digital identity, and self-sovereign identity were included. Third group: tam, avatar, basketball teaching, customization, enjoyment, usage intention, and virtual space. The fourth group: consists of the words industrial metaverse and user interaction. In the fifth group: the word multi-criteria decision making is included.

The first group of the simple themes section, where the level of centralization is high and the density is low: metaverse consists of the words virtual reality, augmented reality, extended reality, virtual, learning, second life, digital twin, mixed reality, and avatars. In the second group: the words metaverse tourism and virtual tourism were included. Third group: consists of the words modeling and artificial systems.

4.8. Change of Keywords Emphasized in Metaverse Studies in Management by Years

(Yönetimde Metaverse Araştırmalarında Vurgulanan Anahtar Kelimelerin Yıllara Göre Değişimi)

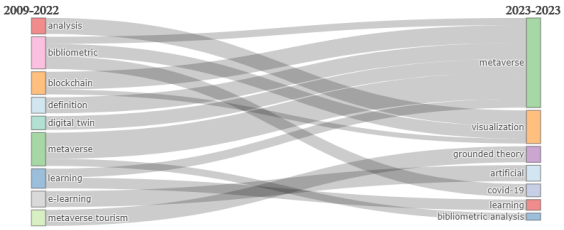


Figure 8. Change of keywords highlighted in metaverse research in management by years

(Yönetimde metaverse araştırmaları vurgulanan anahtar kelimelerin yıllara göre değişimi)

As a result of the analysis of metaverse research in management, in the years 2009-2022: it is understood that the words analysis, bibliometric, blockchain, definition, digital twin, metaverse, learning, e-learning, and metaverse tourism are emphasized. In 2023, it has been observed that the word metaverse is used extensively, and the words visualization, grounded theory, artificial, covid-19, learning, and bibliometric analysis are frequently emphasized. The obtained results show that the help of bibliometric analyzes on metaverse is frequently used in management. In addition, it is understood that the concept of metaverse is very popular, especially in 2023. It is observed that the metaverse in management is used or studied by individuals in many different fields.

4.9. Metaverse Research in Management, Global Citation Rates *(Yönetimde Metaverse Araştırmaları, Küreselde Alıntılanma Oranları)*

Below are the most cited sources globally in metaverse research in management. In the analysis, the responsible authors of the most cited sources in management metaverse studies, the year of publication of the work, and the information of the journal in which it was published were included.

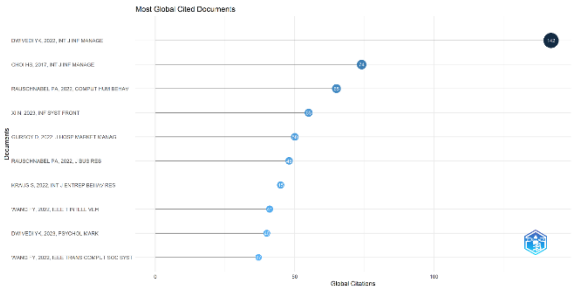


Figure 9. Metaverse research in management, global citation counts

(Yönetimde metaverse araştırmaları, küreselde alıntı sayıları)

As a result of the analysis, it was understood that the most cited source in metaverse research in management is 'Dwivedi YK., 2022, International Journal of Information Management'. The most cited sources are 'Choi HS., 2017, International Journal of Information Management', 'Rauschnabel PA., 2022, Computers in Human Behavior', 'Xi N., 2023, Information Systems Frontiers', 'Gursoy D., 2022, Journal of Hospitality Marketing & Management', 'Rauschnabel PA., 2022, Journal of Business Research', 'Kraus S., 2022, International Journal of Entrepreneurial Behavior & Research', 'Wang FY., 2022, IEEE Transactions on Intelligent Vehicles,' 'Dwivedi YK., 2023, Psychology & Marketing', 'Wang FY., 2022, IEEE Transactions on Computational Social Systems'. The results showed that the most cited sources were generally research published in recent years.

5. DISCUSSION *(TARTIŞMA)*

Metaverse application areas are developing day by day and can provide many conveniences to organizations. In addition to facilitating organizational activities, it can also contribute to advertising, information, transportation, and research and development opportunities. In the literature, Çelik et al. [31] stated that the metaverse creates advantages

for businesses, consumers, institutions, and many areas of life. Researchers have emphasized that organizations can communicate without limitation with their employees, business partnerships, other businesses, and stakeholders.

In metaverse research in management, it has been observed that Covid-19 is among the keywords emphasized by the authors, motor themes, and topics researched in 2009-2022. Covid-19 has caused changes in many applications both at the individual and organizational levels. Organizations have tried to integrate technology more into their business activities in terms of remote working opportunities. In the literature, Wisnu Buana [7] emphasized that in covid-19, where restrictions are experienced, individuals are more oriented to the digital world and this situation develops the metaverse.

As a result of the analysis, it has been shown that metaverse studies in management are studied in the field of tourism. It was seen that tourism was very popular in the keywords emphasized by the authors, in the metaverse relationship network in management, in the motor themes of tourism marketing, and in the simple themes section of metaverse tourism in the years 2009-2022. This situation has shown that metaverse applications are effective in management in the field of tourism. Adaptation to technological innovations in tourism activities has contributed to the functionality of metaverse applications. In the literature, Buhalis et al. [8] the building blocks of metaverse tourism: are network infrastructure, enabling devices, empowering platforms, and technology-ready users. They stated that although the metaverse is still in its infancy, it affects the competitiveness of tourism and organizations.

In the research, it has been observed that the concept of digital is included in the words emphasized in metaverse research in management and the relationship matrix. In the thematic map, the concepts of digital twin and digital identity took place. The construction of knowledge and knowledge modeling has also been involved in metaverse research in management. In the literature, Mancuso et al. [10] have metaverse opportunities for digital business model innovations in organizations: they emphasize that they provide physical transformation, internal processes, virtual transformation, and positive activities for customers. In addition, the information supported in virtual scenarios in terms of metaverse: stated that it encourages virtual communities, and increases intuitive design, user satisfaction, and loyalty. Gadalla et al. [25] stated that most of the products concerning the metaverse are digital. They stated that social experience, flexibility, production, and creative opportunities are provided with metaverses.

In metaverse studies in management, it has been seen that the word social is included in the highlighted keywords and in the motor themes section. In addition, the word cyber-physical-social was also included in the motor themes. In the literature, Serpil and Karaca [11] emphasized that the meta-order can change positively if individuals with digital addiction use social networks with a high level of awareness.

In the analysis, the importance of metaverse research in management is emphasized for organizations. It is stated that organizational policies should act with integrity with metaverse practices. In this respect, the metaverse can have many advantages in organizational activities. In the literature, Gauttier et al. [4] emphasized that an organization that wants to take advantage of the metaverse strategically should consider whether it has advantages and the ability to act flexibly. In this respect, Park et al. [12], on the other hand, emphasized that the physical constraints of any workplace cause a disadvantage in the organization. However, they stated that the metaverse environment does not have any physical or spatial barriers, thus creating an advantage.

Metaverse has shaped the lives and activities of individuals in many areas. The intense use of technology and digital media in many places and areas has expanded the application area of the metaverse. In the literature, Narin [13] emphasized that in the digital universe created by the metaverse, individuals can perform many activities such as working, shopping, traveling, having fun, and getting an education.

In the metaverse application in management, it has been observed that sustainability is included in the highlighted keywords, relations section, and motor themes. A sustainable metaverse occurs when organizational policies support activities. In the literature, Truong et al. [14] emphasized that the metaverse should have a financially complete and stable economic system in terms of sustainability. They stated that the virtual contents in the metadata store should retain their value.

The research revealed that the term "avatars" appeared within the highlighted keyword list, and thematic mapping in the analysis of the metaverse within the field of management. Metaverse research in management has also involved visualization. Visualization: It has been seen that it is used quite intensively in the highlighted keywords, relationships, motor themes, and in 2023 research. In the literature, Lyons [15] employee avatars: emphasized that it was

effective in developing remote equipment service and operational metrics by utilizing data visualization, remote sensing systems, and technology. Šímová et al. [33] emphasized that with the metaverse application in the organization, employees can carry out their business activities, communication, and creativity opportunities in a virtual environment by using their avatar identities.

In management metaverse research, a great deal of emphasis has been placed on the concepts of blockchain and artificial intelligence. These algorithms are very effective in the formation of the metaverse. In the literature, Nagy et al. [16] emphasized that a blockchain-based metaverse with digital asset management was created using artificial intelligence information processing, data visualization, and emotion recognition technologies. Zvarikova et al. [17] stated that with cloud and edge computing technologies, remote monitoring capability and virtual connections can be optimized by using artificial intelligence-supported virtual agents in metaverse operation management.

It has been observed that metaverse research is used seriously in tourism, health, education and industrial areas, and management. The analysis also revealed that metaverse applications in management are associated with many other fields and organizations. This has shown that the metaverse plays an active role in many sectors. In the literature, Koohang et al. [18] revealed that the metaverse is related to many fields such as tourism, production, education, health, operations, and human resources management.

Metaverse is a very influential factor for organizational activities. Organizations should demonstrate their technological activities to achieve their future goals. This situation brings the concept of metaverse, which has been used frequently in recent years and emphasized in many areas, to the agenda. In the literature, Setiawan et al. [19] emphasized that the metaverse has become important for the business world and affects businesses. They stated that the metaverse reduces the risks in business activities.

In the research, it has been seen that words such as virtual, virtual reality, virtual identity, virtual worlds, virtual learning, and virtual tourism are frequently used in metaverse research in management. In addition, the word avatars is often used. This situation is closely related to the virtual reality created by the metaverse. In today's digital technology era, the virtual environment has influenced many fields of activity. People have started to live their lives with virtual habits. In the literature, Wang et al. [21] emphasized that people represented by avatars in the metaverse can communicate with virtual environments, virtual identities, digital objects, and items created by computers, and they develop the phenomenon of cooperation and socialization. Ning et al. [22] stated that new worlds can be discovered with the metaverse, and time and resource savings can be achieved through activities and meetings in the virtual space.

It has been seen that sociability and security are included in the words used by the authors in metaverse research in management. In terms of organizations, sociability in the working environment contributes to the management of business activities. The adaptability of the metaverse to the social field of activity also contributes to the continuity of the organization. With the help of the metaverse, organizational activities must be risk-free and reliable. In the literature, Lee et al. [23] stated that the metaverse should be similar to society in the physical world, compatible with content creation, virtual economy, social norms, and regulations. They stated that individuals should not face privacy risks and security threats in their activities. Choi et al. [24] revealed that social metaverse experience increases psychological well-being in terms of managing mood in individuals.

In the metaverse analysis in management, it has been observed that the concepts of virtual reality, augmented reality, extended reality, reality, and mixed reality have strong relationships. This situation has shown that metaverse applications in reality province administration have intense scrutiny. In this respect, it is necessary to ensure harmony in the organization in terms of virtual and reality. In the literature, Guan et al. [30] stated that if the metaverse and physical domains fail to communicate consistently to work together, there may be incompatibility, resulting in overloading for both physical and virtual domains.

6. CONCLUSION *(SONUÇ)*

As a result of the analysis, the metaverse in management is generally: virtual environments (such as virtual world, virtual reality, virtual identity, and virtual learning), technology, education, health, tourism, marketing, artificial intelligence, blockchain, sustainability, digitality, industry, and social environments. This situation shows the effect of metaverse applications in management in many different fields and organizations. In particular, the intense research network in recent years reveals that organizations should consider metaverse applications depending on technological changes.

As a result, management creating some digital activities for employees with the help of Metaverse can contribute to employee productivity. Metaverse applications can be used to increase employees' workplace motivation. Virtual applications can be created by taking into account technological changes in the relationship between managers and employees. Metaverse can be used to help employees introduce innovations regarding their business activities. Metaverse can be used to help employees gain experience in new jobs. Metaverse applications can be used in administrators' application-oriented policies.

Metaverse contributes to the training and development of employees in organizations with its applications. Information about organization activities is organized quickly and securely with the metaverse. By integrating technological innovations into business activities, the production of goods or services can be carried out more effectively. In this respect, metaverse applications contribute to reducing the workload of employees and using time effectively. It provides convenience in terms of workflow control with metaverse applications in manager-employee interaction. In promoting and advertising organizational outcomes, metaverse applications are a valuable tool.

The research application is limited to July 2023 and WoS database research. In future research, serious contributions can be made to the literature by using different databases on the subject. In addition to metaverse research in management, the effects of metaverse use, especially on the habits of young individuals, can be examined. In addition, social relations, and human and machine power in the organization, can be evaluated within the framework of the metaverse.

REFERENCES *(KAYNAKLAR)*

[1] M. Mehta, G. Pancholi and A. Saxena, "Metaverse changing realm of the business world: A bibliometric snapshot", *Journal of Management Development*, Vol. 42, No. 5, pp.373-387, 2023. Doi: 10.1108/JMD-01-2023-0006

[2] M. Damar, "Metaverse Shape of Your Life for Future: A bibliometric snapshot", *Journal of Metaverse,* Vol. 1, No.1, pp.1-8, 2021.

[3] M. Kalyvaki, "Navigating the metaverse business and legal challenges: Intellectual property, privacy, and jurisdiction", *Journal of Metaverse,* Vol. 3, No.1, pp.87-92, 2023. Doi: 10.57019/jmv.1238344

[4] S. Gauttier, W. Simouri and A. Milliat, "When to enter the metaverse: Business leaders offer perspectives", *Journal of Business Strategy*, pp. 1-8, 2022. Advance online publication. Doi: 10.1108/JBS-08-2022-0149

[5] M. E. Khatib, A. A. Khayat, S. A. Mansoori, A. Alzaabi and A. Ankit, "Metaverse skills for executives and senior managers: The pros and cons", *International Conference on Business Analytics for Technology and Security (ICBATS),* pp. 1-7, May 2023. Doi: 10.1109/ICBATS57792.2023.10111483

[6] A. D. Yemenici, "Entrepreneurship in the world of metaverse: Virtual or real?", *Journal of Metaverse,* Vol. 2, No.2, pp.71-82. 2022.

[7] I. M. Wisnu Buana, "Metaverse: Threat or opportunity for our social world? in understanding metaverse on sociological context", *Journal of Metaverse,* Vol. 3, No.1, pp.28-33. 2023. Doi: 10.57019/jmv.1144470

[8] D. Buhalis, D. Leung and M. Lin, "Metaverse as a disruptive technology revolutionising tourism management and marketing", Tourism Management, Vol. 97, pp. 1-11, 2023. Doi: 10.1016/j.tourman.2023.104724

[9] A. E. Williams, "Human-centric functional modeling and the metaverse", *Journal of Metaverse,* Vol. 2, No.1, pp.23-28, 2022.

[10] I. Mancuso, A. M. Petruzzelli and U. Panniello, "Digital business model innovation in metaverse: How to approach virtual economy opportunities", *Information Processing and Management*, Vol. 60, pp.1-28, 2023. Doi: 10.1016/j.ipm.2023.103457

[11] H. Serpil and D. Karaca, "The metaverse or meta-awareness?", *Journal of Metaverse*, Vol. 3, No. 1, pp. 1-8, Doi: 10.57019/jmv.1093347

[12] H. Park, D. Ahn and J. Lee, "Towards a metaverseworkspace: Opportunities, challenges, and design implications", *CHI,* pp. 1-20, 2023. Doi: 10.1145/3544548.3581306

[13] N. G. Narin, "A content analysis of the metaverse articles", *Journal of Metaverse*, Vol. 1, No. 1, pp.17-24, 2021.

[14] V. T. Truong, L. B. Le and D. Niyato, "Blockchain meets metaverse and digital asset management: a comprehensive survey", *IEEE Access,* Vol. 11, pp. 26258-26288, 2023. Doi: 10.1109/ACCESS.2023.3257029

[15] N. Lyons, "Talent acquisition and management, immersive work environments, and machine vision algorithms in the virtual economy of the metaverse", *Psychosociological Issues in Human Resource Management,* Vol. 10, No. 1, pp. 121–134, 2022. Doi: 10.22381/pihrm10120229

[16] M. Nagy, P. Kubala, E. R. Tucmeanu and A. Mişa, "Metaverse-based industrial services, ambient intelligence and simulation modeling tools, and brain-inspired cognitive and empathetic computing systems across 3d digital twin factories", *Journal of Self-Governance and Management Economics,* Vol. 10, No. 4, pp. 9–23, 2022. Doi: 10.22381/jsme10420221

[17] K. Zvarikova, J. Cug and S. Hamilton, "Virtual human resource management in the metaverse: Immersive work environments, data visualization tools and algorithms, and behavioral analytics", *Psychosociological Issues in Human Resource Management,* Vol. 10, No. 1, pp. 7–20, 2022. Doi: 10.22381/pihrm10120221

[18] A. Koohang, J. H. Nord, K-B. Ooi, G. W-H. Tan, M. Al-Emran et al., "Shaping the Metaverse into Reality: A Holistic Multidisciplinary Understanding of Opportunities, Challenges, and Avenues for Future Investigation", *Journal Of Computer Information Systems,* Vol. 63, No. 3, pp. 735–765, 2023. Doi: 10.1080/08874417.2023.2165197

[19] K. D. Setiawan, A. Anthony, Meyliana and Surjandy, "The essential factor of metaverse for business based on 7 layers of metaverse – systematic literature review", *ICIMTech,* pp. 687-692. August 2022.

[20] M. J. Cobo, A. G. Lopez-Herrera, E. Herrera-Viedma and F. Herrera, "SciMAT: A new science mapping analysis software tool", *Journal of the American Society for Information Science and Technology,* Vol. 63, No. 8, pp. 1609–1630, 2012. https://doi.org/10.1002/asi.22688

[21] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T.H. Luan and X. Shen (2023). "A survey on metaverse: fundamentals, security, and privacy", *IEEE Communications Surveys & Tutorials*, Vol. 25, No. 1, pp. 319-352, Doi: 10.1109/COMST.2022.3202047

[22] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding and M. Daneshmand, "A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges", *IEEE Internet of Things Journal*, pp. 1-18, Doi: 10.1109/JIOT.2023.3278329

[23] L-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo and P. Hui, "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda", *Journal of Latex Class Files*, Vol. 14, No. 8, pp. 1-66, September 2021.

[24] D. Choi, H. K. Lee and D. Y. Kim, "Mood management through metaverse enhancing life satisfaction", *International Journal of Consumer Studies,* Vol. 47, pp. 1533-1543, 2023. Doi: 10.1111/ijcs.12934

[25] E. Gadalla, K. Keeling and I. Abosag, "Metaverse-retail service quality: A future framework for retail service quality in the 3D internet", *Journal of Marketing Management,* Vol. 2, No. 13-14, pp. 1493-1517, 2013. Doi: 10.1080/0267257X.2013.835742

[26] M. Aria and C. Cuccurullo, "Bibliometrix: An R-tool for comprehensive science mapping analysis", *Journal of Informetrics*, Vol. 11, pp. 959–975. 2017. Doi: 10.1016/j.joi.2017.08.007

[27] H. Derviş, "Bibliometric analysis using bibliometrix an R package", *Journal of Scientometric Research,* Vol. 8, No. 3, pp. 156-160, 2019. Doi: 10.5530/jscires.8.3.32

[28] J. A. Moral-Muñoz, E. Herrera-Viedma, A. Santisteban-Espejo and M. J. Cobo, "Software tools for conducting bibliometric analysis in science: An up-to-date review". *El Profesional de la Información*, Vol. 29, No. 1, pp. 1-20, 2020. Doi: 10.3145/epi.2020.ene.03

[29] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines", *Journal of Business Research,* Vol. 133, pp. 285-296, 2021. Doi: 10.1016/j.jbusres.2021.04.070

[30] J. Guan, J. Irizawa and A. Morris, "Extended reality and internet of things for hyper-connected metaverse environments", *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Christchurch*, New Zealand, pp. 163-168, 2022. Doi: 10.1109/VRW55335.2022.00043

[31] Z. Çelik, B. Dülek, İ. Aydın and R Saydan, "Metaverse: Bibliometric Analysis, A Conceptual Model Proposal, and a Marketing-Oriented Approach", *Bingöl University Journal of Social Sciences Institute*, Vol. 24, pp. 383-394, 2022. Doi: 10.29029/busbed.

[32] N.J. Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping", *Scientometrics,* Vol. 84, pp. 523–538, 2010. Doi: 10.1007/s11192-009-0146-3

[33] T. Šímová, K. Zychová and M. Fejfarová, "Metaverse in the virtual workplace: Who and what is driving the remote working research? A bibliometric study", *The Journal of Business Perspective*, Vol. 28, N0. 1, pp. 1-16, 2023. Doi: 10.1177/09722629231168690

Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Araştırma Makalesi / Research Article

Cyber Security Based Visitor Control System Design

Mehmet NACAROĞLU[*,a], Çiğdem TARHAN[b], Murat KOMESLİ[c], Vahap TECİM[d]

[a]*Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, İZMİR, 35400, TÜRKİYE*
[b]*Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü - Bölgesel Kalkınma ve İşletme Bilimleri Araştırma ve Uygulama Merkezi (DEÜ-BİMER), İZMİR, 35400, TÜRKİYE*
[c]*Yaşar Üniversitesi, Uygulamalı Bilimler Yüksekokulu, Yönetim Bilişim Sistemleri Bölümü, İZMİR, 35030, TÜRKİYE*
[d]*Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, İZMİR, 35400, TÜRKİYE*

ARTICLE INFO

Received: 09.12.2023
Accepted: 29.04.2024

Keywords: *:*

Raspberry PI,
QR code,
visitor control systems,
cyber security

Corresponding Authors

e-posta:
wnacaroglu@ gmail.com

ABSTRACT

In this study, a cyber security-based visitor control system has been designed to maximize participant security in institutions, to prevent unauthorized access, and to easily control participants. The Visitor Control System has been developed using Raspberry Pi 3 and the information of the visitors who will participate is uploaded to the system along with their pictures. Within the scope of cyber security measures, the Visitor Entry Card, which is created with a QR code to prevent fake ID or entrance cards, is sent to the participants days before the dates of programs such as meetings, seminars, interviews, symposiums, workshops, briefings, fairs, and they are requested to enter with these cards. At the entrance points of the institutions, the visitors' Visitor Entry Card is questioned by the security guards and the QR code on the card is scanned with the help of the camera to confirm whether the visitor is authorized or not. After it is confirmed by the security personnel that it is the same as the person's photo, it is allowed to enter.

DOI: 10.59940/jismar.1402494

Siber Güvenlik Tabanlı Ziyaretçi Kontrol Sistemi Tasarımı

MAKALE BİLGİSİ

Alınma: 09.12.2023
Kabul: 29.04.2024

Anahtar Kelimeler
Raspberry PI
QR kod,
ziyaretçi kontrol
sistemleri,
siber güvenlik

Sorumlu Yazar
e-mail:
wnacaroglu@gmail.com

ÖZET

Bu çalışmada kurumlarda katılımcı güvenliğini en üst düzeye çıkarmak, yetkisiz erişimleri önlemek ve katılımcıların kolayca kontrol edilmesini sağlamak amacıyla siber güvenlik tabanlı bir ziyaretçi kontrol sistemi tasarlanmıştır. Ziyaretçi Kontrol Sistemi, Raspberry Pi 3 kullanılarak geliştirilmiş olup, katılım sağlayacak ziyaretçilerin bilgileri resimleriyle birlikte sisteme yüklenmektedir. Siber güvenlik tedbirleri kapsamında, sahte kimlik veya giriş kartlarının önlenmesi amacıyla QR kod ile oluşturulan Ziyaretçi Giriş Kartı, toplantı, seminer, söyleşi, sempozyum, çalıştay gibi programların tarihlerinden günler önce katılımcılara gönderilir ve brifinglere, fuarlara bu kartlarla girmeleri rica olunur. Kurumların giriş noktalarında ziyaretçilerin Ziyaretçi Giriş Kartı güvenlik görevlileri tarafından sorgulanmakta ve kart üzerinde yer alan QR kod kamera yardımıyla taranarak ziyaretçinin yetkili olup olmadığı teyit edilmektedir. Kişinin fotoğrafıyla aynı olduğu güvenlik personeli tarafından onaylandıktan sonra içeriye girişine izin verilmektedir.

DOI: 10.59940/jismar.1402494

1. INTRODUCTION *(GİRİŞ)*

With the rapid development of science and technology, computer technologies have become indispensable in many areas of life. By greatly affecting human life, the traditional habits of coming together physically have almost disappeared. Many gathering activities such as seminars, talks, symposiums, workshops, briefings, and fairs are held in different parts of the world [25]. In institutions where physical participation is needed due to reasons such as time becoming more valuable with the developing technology and epidemic diseases, these activities are alternatively carried out online. The reliability of participant/visitor access control systems has recently become a much more important criterion in cases where online participation is insufficient and physical participation is mandatory. As a result, the organizers apply many different security measures to prevent unauthorized participants to increase the security of the participants in organizations such as meetings, fairs, and seminars. Some of those; security guards, identity checks, fingerprint checks, entrance cards, tickets are measures to prevent unauthorized participation. However, the mentioned security measures always contain a security vulnerability in their content; for example, such as fake ticket, fake ID, fake fingerprint [26].

Institutions take cyber security measures to protect their systems against cyber-attacks. However, despite this, many institutions experience inadequacies in visitor control processes. Visitor control is the first step that creates the security barrier of the institution, and it is important to manage this process effectively. Traditional visitor registration systems can introduce security vulnerabilities and increase the risk of visitor data falling into malicious hands. Therefore, institutions need cyber security-based visitor control systems. On the other hand, personalized entrance cards created with quick-response (QR) code, where the security personnel do not know what the participants clearly write on, provide extra participant security. The QR code was developed by a Japanese company in 1994 and has survived until today. Besides being easy to use, QR codes have high data processing capability [1, 2]. It was originally developed in Japan for use in the automotive industry. When QR codes consisting of black dots and lines are read by the camera of a mobile device, direct access to the digital information source on the internet or stored on a server can be provided [3].

Within the scope of this study, a cyber security-based visitor control system was designed to maximize participant security in institutions, to prevent unauthorized access, and to easily control participants. The designed visitor control system was developed using the Raspberry Pi 3 hardware and Python as the programming language. The information of the visitors who will participate in the institutions are uploaded to the system with their pictures, and only a visitor entry card with a specially prepared QR code is given to the visitors. Security officers can determine whether the person is an authorized participant or not when the entrance card given to them at the entrance to the institutions is read into the system by the visitors/participants. The security guard allows the participant to pass by checking everything from the person's photo to other identifying personal information on the screen. When trying to enter with fake entrance cards prepared with QR code technology, the security personnel will not be allowed to enter the participant, since no photo is displayed with an unauthorized entry warning on the screen. Within the scope of cyber security measures, a possible cyber-attack, infiltration of the system, changing fake identity or visitor information, or generating fake QR code, etc. provides an advantage in preventing situations.

It has been stated that, due to the rapid development of information technologies in the world, the use of computers and the internet has become an indispensable element of life. However, they [13] stated that while the rapid spread of the Internet around the world provides great convenience and freedom to users, it also causes the systems to be misused due to the security vulnerabilities that arise. These vulnerabilities can target individuals or large systems. The devices communicating with each other, that is, the Internet of Things (IoT) and the unpredictable increase in the number of devices connected to the Internet, will bring about cyber security problems [13].

The concept of cyber is used to describe concepts or entities that include computers and networks. The word cyber space is also used to describe the abstract or concrete area where interconnected hardware, software, systems and people communicate and/or interact. The concept of Cyber Attack is defined as "planned and coordinated attacks on the information systems and critical infrastructures of targeted individuals, companies, institutions and states."

2. LITERATURE REVIEW *(LİTERATÜR TARAMASI)*

With the developing technology, embedded computers, in other words embedded systems, are used in many areas of life today. Embedded computers; in mobile devices, vehicles, bank ATMs, televisions, white goods, toys, printers, smart home systems, factories, workplaces, security points, etc. It

is configured and used in many places to serve every need.

Türk and Lüy [14] have stated that embedded systems are microprocessor-based computer hardware systems that perform a specific task independently or as part of a larger system and also have their own software. Embedded computers; GPU (Graphics Processing Unit) technology, digital signal processors, microcontrollers or application-specific integrated circuits, etc. used on systems.

The program strings used in embedded computers constitute the software architecture of the system. Since a simple industrial microcontroller is designed to perform specific tasks, tuning power consumption, size, reliability, and performance is extremely important. These basic devices are programmed through the machine code of the CPU (Central Process Unit). Their software is implemented with C, C++, Java or similar programming languages. Embedded computers often use interfaces or language platforms suitable for embedded use, along with real-time operating environments. Examples of these are Linux, Windows IoT and Embedded Java. However, to give an example of embedded computers, or in other words, simple programmable computers; Arduino or Raspberry Pi can be given as examples.

Arduino is a type of development board that appeals to many users, from the lowest level to the engineering level, with its simple and easily integrated coding language. Arduino is also a microcontroller platform with open source software and hardware. For example, using Arduino, you can read data from sensors and control electronic systems, turn on and off lights or start the engine according to this data.

Raspberry Pi, on the other hand, is a small, low-cost credit card-sized computer that can be attached to a monitor, television or special display, and uses a standard keyboard and mouse. Although it is similar to the Arduino system, it is a platform that appeals to users of all levels and allows them to learn programming in languages such as Scratch and Python. The microprocessor, RAM (Random Access Memory), GPIO (General purpose Input Output) pins and all the features required for a computer are built on a single circuit board PCB (Printed Circuit Board) on the Raspberry Pi. These types of computers are also called Single Board Computers (SBC). Unlike the computers we use in daily life, SBCs consume less power and have a smaller size. While Raspberry Pi performs most tasks that a normal computer can do, it also has the ability to program and control many different electronic systems via the GPIO pins on it.

Access control systems with different technologies are used wherever access security is needed. Among these technologies, password use, radio frequency identification (RFID) card use, magnetic card usage and biometric measures (fingerprint, iris scanner, retina scanner, voice recognition, face detection, etc.) are used very frequently today. Along with these, it is used in the QR code system, which has become very common in recent years. However, the QR code system is used not only for identity verification purposes, but also to respond to needs such as internet address, stock inquiry, sharing bank account information, use instead of business cards, address directions, electronic menu display in restaurants, etc. The reliability of these mentioned technologies against cyber-attacks, which is increasing day by day in the world, is becoming a more important issue. In this context, a literature review has been carried out for access control systems with different technologies currently used in the world.

Karaca [4] used RFID system to develop instant Personnel Tracking System. With the RFID system used, considering the entry-exit times and current location information of the personnel, considering the importance of security in secret gatherings with limited participants, increasing the security level by monitoring and intervening unauthorized participations, increasing the security level of the institutions / organizations by processing the current personnel attendance list. It is aimed to make it easy to follow up.

Mamak et al. [5] designed a face recognition-based personnel control and tracking system to track the time entry and exit processes of the personnel in the workplaces quickly, effectively, and accurately. In the developed system, the images of the personnel were taken by installing a camera system at the entrance and exit of the workplace. By identifying the facial regions of the personnel and matching the personnel, the images taken are identified by the fisherface, eigenface and local binary pattern histogram methods. The entry-exit data of the found personnel are displayed on the screen, and they are archived by being processed into the personnel personal database.

Genli [6] developed an application that will report the use of this card to the system as an alarm when the card holder wants to enter any room or section in the building and prevent entry to the room or passing through the turnstile. If there is no access authorization, the system is provided to generate an alarm directly.

Musayevave and Yahyayev [7], with regard to fingerprint recognition technology, defined that each

human hand has a different skin structure, there are indented protruding bumps on the skin of the fingertips, and the fingerprints left on the surfaces as a result of the contact of these raised structures. They stated that fingerprints in humans have unique and unchanging biometric measurements.

Özkaya and Sağıroğlu [8] have stated that the use of fingerprint technology in identity verification is very old. The Automatic Fingerprint Recognition System (OPTS) history is based on fingerprint ink. Although OPTS is known as a secure system, malicious people stated that they managed to imitate using finger patterns. On the other hand, they stated that it is possible to eliminate this problem with systems that check whether an imitated fingerprint pattern is a live real finger or not.

Noma-Osaghae et al. [9] stated that biometric authentication systems use unique physiological and behavioral features to limit access.

Wahyudi and Syazilawati [10] stated that secure buildings are protected against unauthorized access by various devices. They explained that although there are many types of devices such as PIN codes, both traditional and electronic keys, ID cards, cryptographic and binary control procedures, human voice can also be used to guarantee system security. They argued that the ability to authenticate a speaker by analyzing speech or speaker verification is an attractive and relatively inconspicuous way of providing security for entry to an important or safe place, that a person's voice cannot be stolen, lost, forgotten, unpredictable, or fully imitated.

4. CURRENT ACCESS CONTROL SYSTEMS IN INSTITUTIONS *(KURUMLARDAKİ MEVCUT GEÇİŞ KONTROL SİSTEMLERİ)*

There are different access control systems in use, such as fingerprint technology, card access systems, password access systems and barcode systems.

4.1. Fingerprint Technology Passage System *(Parmak İzi Teknolojisi Geçiş Sistemi)*

Nowadays, considering the cost, applications for different entry systems can be found in different areas. Businesses and individual measures provide faster and more effective entry-exit control compared to traditional systems by using many technological entry methods. Many security control systems are used successfully. One of the most commonly used ones is the fingerprint-based security control system. Fingerprint technology is basically used as a key in entry-exit systems for security purposes because fingerprints have specific properties. With to this feature, maximum security can be ensured. The process of using the fingerprint as a control tool in input-output systems with the Minutiae (Detail) Matching Algorithm [15], [16], [17].

Fingerprint recognition systems require special software to work. Fingerprint recognition algorithms form the basis of this software [27]. Algorithms form the basis of all software-based devices we use. Hardware and software work together in personnel fingerprint reader systems. The fingerprint reading device detects the fingerprint by scanning the finger. Then the algorithm, the software side, comes into play to match the fingerprint. When the fingerprint matches, the entry is confirmed and the lock is unlocked. To put it another way, the fingerprint is scanned. This scanning process is actually the process of taking photos. The camera and optics take a photo of the finger placed on the device. The process is completed electronically. Fingerprint algorithms transform this photograph into a special digital model. The indentations and protrusions in the trace are used to create the digital model. The resulting numerical model is compared with the database on the computer. If there is a match in the database, fingerprint verification is completed. This process can be applied in different areas such as personnel tracking system and door unlocking system [28].

As shown in Figure 1, the access systems with fingerprint technology, unauthorized access is prevented by using the password or card sharing method. On the other hand, fake fingerprints of authorized persons can be made using various techniques. In this way, unauthorized people can also pass through.

Figure 1. Fingerprint Reader Access System *(Parmak İzi Okuyucu Geçiş Sistemi)*

4.2. Card Access System *(Kartlı Geçiş Sistemi)*

Card access systems; These are systems that record the entry and exit times of individuals, employees, visitors or vehicles entering the parking lot by scanning the cards given to individuals and enabling the opening and closing of turnstiles, doors or barriers

[29]. Card access control systems are among the frequently preferred control systems for personnel tracking. These systems are also called access control system, access control system and access control system [30].

Baykara and Sherzad [18] defined RFID Card Entry Systems as a technique used to manage information and access for people or visitors who want to enter a place from the main door. Accordingly, the system they developed was designed as a web application connected to a database to maintain information on the movements of residents or visitors within a secure area to control entry before gaining access to any home. It provides a measure of security for building occupants and can help minimize the risk of unauthorized access, increase security, reduce theft and accidents, and secure sensitive information.

Card access control systems are considered the ancestors of personnel tracking systems. The card access systems, shown in Figure 2, used to keep personnel under control in institutions or businesses, to record entry and exit times, to ensure that only authorized people can access certain areas in businesses and to prevent anyone other than them from entering.

Card access control systems are very practical, convenient and low-cost. Additionally, certain people are allowed to pass through permitted areas safely through the authorization feature of card access systems [31].

Figure 2. Card Access System
(Kartlı Geçiş Sistemi)

However, the biggest disadvantage of card pass systems is that unauthorized entries occur as a result of voluntary or unintentional use of the cards of people authorized to pass to a certain region or area by other people, creating a security vulnerability [19].

4.3. Password Access System *(Şifre Geçiş Sistemi)*

Password access systems are systems that allow turnstiles and doors to be opened with the help of a password [32]. Coded access systems, which have hundreds of different models on the market as shown in Figure 3, are generally used at building entrances, office rooms, hospitals, especially at the entrances of surgery and intensive care units, elevators, warehouses, etc. It is used in places. The working principle of password-protected passage systems is that the user who wants to pass must know the correct password. When the user enters the correct password, the system completes the circuit in the lock system on its own electronic circuit, voltage is instantly sent to the lock system inside the door and the door is unlocked [20].

Kolekar et al. [21] designed password-based door entry systems using 8051 microcontroller. They stated that the system works on the principle that the numbers entered from a key panel match the password previously saved in the 2 Kilobyte memory. As a result of entering the correct password, the motor interface connected to the microcontroller was activated and the door was unlocked or closed by rotating the motor forward or backward.

With the developing technology in password access systems, password entry is now used as touch buttons or panels instead of buttons. It is also possible to pass with a magnetic card in touch coded pass systems [33].

However, the biggest disadvantage of this system is that if the password is disclosed, that is, if the password is given to an unauthorized person or if an authorized person learns the password by watching from behind while typing it, it will create a security vulnerability [34].

However, a thief or someone with malicious intent who has good electronic technical knowledge can easily remove the password panel if it is not mounted securely. Even if he does not know the password, he can easily open the door by connecting the cable from the power supply to the door lock in a way that short-circuits it.

Figure 3. Password Access System
(Şifre Geçiş Sistemi)

4.4. Barcode Access System *(Barkod Geçiş Sistemi)*

In our world where technology is developing very rapidly, the security lock and access systems we use in daily life have also been subject to many changes. Card access systems are used in every aspect of our daily lives. Currently, public institutions, buses, universities, hospitals, dining halls, entertainment centers, hotels, etc. Card access system technology is used in many places.

San Hlaing and San Lwin [22] stated that card access systems are systems that allow entry when some voltage electricity is applied to the RFID door lock mechanisms without the need for a lock and key.

This technology is known both in the past and today as an affordable and reliable solution for users. However, the pandemic epidemic that affected the whole world in the past years has forced us to use alternative systems to the conventional cards. For these reasons, lately, solutions that are both safe and do not require contact have been preferred, especially at access control points, in order to minimize physical contact in public areas.

With the development of technology, access systems that can read RFID cards and also scan QR codes or barcodes have begun to take their place in the market. Some security technology companies work with public institutions, buildings, businesses, etc. that have existing access control systems. In places, they are transforming into passage systems with QR or barcode technology shown in Figure 4, without damaging the existing infrastructure systems.

However, these systems, like card pass systems and cards with QR or barcode technology, are used voluntarily or unintentionally by other than their real owners, resulting in unauthorized passage, which creates a security vulnerability for the institutions and businesses in question [23].

Figure 4. Barcode Access System
(Barkodlu Geçiş Sistemi)

5. VISITOR CONTROL SYSTEM DESIGN AND IMPLEMENTATION *(ZİYARETÇİ KONTROL SİSTEMİ TASARIM VE UYGULAMASI)*

During the Visitor Control System design development process, the System Development Life Cycle steps shown in Fig.5 were followed [11].

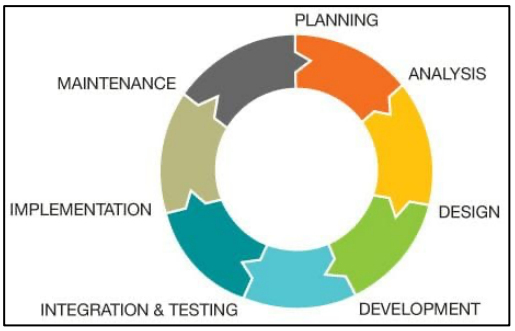


Figure 5. System development life cycle
(System development life cycle)

System Development Life Cycle consists of seven processes;

1. Defining Problems, Opportunities and Goals,
2. Determination of Information Requirements,
3. System Requirements Analysis,
4. Design of the Recommended System,
5. Software Development and Document Creation,
6. Testing and Maintaining the System,
7. Implementation and Evaluation of the System.

5.1. Defining Problems, Opportunities and Goals
(Problemlerin, Fırsatların ve Amaçların Tanımlanması)

It is known that cyber attacks targeting all information systems in the world can also damage exhibitor/visitor access control systems. If the cyber attacks in question affect the entrance control systems of the institutions, participant / visitor information can be changed and unregistered persons are also allowed to enter. Meeting, fair, seminar, interview, symposium, workshop, fair, etc. Since the security guards at the entrances of the buildings where the organizations are held have never seen or known the participants from different parts of the world, there is a possibility that they may make mistakes about whether they are real authorized participants or not.

It is aimed to upload the information of the visitors who will participate with the Visitor Control System, along with their pictures, to the system days in advance. In addition, participants/visitors can be provided with meetings, seminars, interviews, symposiums, workshops, briefings, fairs, etc. Within the scope of cyber security measures, within the scope of cyber security measures, Visitor Entry Cards with

their names on them, created with a QR code, were delivered to them and they were intended to enter with these cards.

In this way, the Visitor Entry Card of the participants is questioned by the security guards at the entrance points of the institutions through the Visitor Control System and it is aimed to confirm whether the visitor is an authorized/registered user by scanning the QR code on the card with the help of a camera. It is intended that the security personnel will be allowed to enter after the system confirms that the person's photo is exactly the same as the person's photo, that is, after double checking.

5.2. Determination of Information Requirements
(Bilgi Gereksinimlerinin Belirlenmesi)

While designing the Visitor Control System, access control systems currently used in institutions were examined. The operating principles, designs and security vulnerabilities of these systems have been identified in detail. The first of these systems to be examined is the encrypted access systems. Password pass systems are systems that allow passage by dialing a certain number of numbers in a correct order. However, it is not a very suitable system in terms of security. Because it is very easy for anyone who knows or obtains the password to gain access. Although it is low-cost, it is generally used in apartments, buildings, in-house doors, schools, hospitals, etc. It is used at the entrances of places.

When card access systems are examined, it is a system based on the principle that the door or turnstile opens when card holders bring the RFID-enabled card closer to the system. However, the biggest weakness of this system is that it allows an unauthorized person to access the system by scanning the card in case the card is given to someone else or if it is lost or stolen. Card pass system, just like the coded pass system, can be used in apartments, buildings, in-house doors, schools, hospitals, etc. It is used at the entrances of places.

Fingerprint reader access systems are one step ahead in terms of reliability compared to the mentioned password and card access systems. It is based on the principle that people physically identify their fingers to the system beforehand and then have their fingerprints read into the system if they want to pass through, and then the door or turnstile opens. Although it is better in terms of reliability than password or card access systems, fake fingerprints of people with access authorization can be imitated using various techniques. However, unauthorized persons may pass through.

Barcoded passage systems allow passage by scanning the ticket or card given to the participant/visitor into the system. However, when used alone, this system creates a security vulnerability by allowing unauthorized persons to pass in case the ticket is given to someone else or lost, as is the case with card pass systems.

While designing the Visitor Control System, the security vulnerabilities of the access control systems mentioned were examined and a system that could eliminate these vulnerabilities was developed. Within the scope of the system's information requirements, people's photographs and identity information are needed to upload real photographs of participants or visitors to the system days in advance. Within the framework of the photographs and information provided by the people, a Visitor Entry Card is prepared for the participant or visitor, which contains nothing but the QR code and the visitor's name. When the Visitor Entry Card is scanned into the system, the photo of the incoming participant/visitor is checked by the security guard, and if the photo displayed in the system matches the participant/visitor, passage is allowed, otherwise they are rejected. In this way, possible security vulnerabilities are prevented.

5.3. System Requirements Analysis
(Sistem İhtiyaçlarının Analizi)

When designing the Visitor Control System, the hardware and software required by the system differ from traditional access control systems. Traditional access control systems, which are widely available on the market, generally contain hard cards and embedded software. However, in the Visitor Control System design, it is planned to use Raspberry Pi, which has the same function as a computer but is very small in volume and size, Raspberry Pi LCD Touch Screen, Raspberry Pi Camera, power supply and Python programming language as software. The purpose of planning to use Raspberry Pi can be considered as its cost being much smaller in size and less than other computer-controlled or embedded systems.

The equipment used in the Visitor Control System are Raspberry Pi 3 (Fig.6), Raspberry Pi Camera (Fig.7), 16GB Micro SD Card, Raspberry Pi 7 inch LCD Touch Screen (Fig.7) and 2 x Power Adapters.

Figure 6. Raspery Pi 3 ands its camera
(Raspery Pi 3 ve kamerası)

Figure 7. Raspery Pi 7 inch LCD Touch Screen
(Raspery Pi 7 inç LCD dokunmatik ekran)

5.4. Design of the Recommended System
(Önerilen Sistemin Tasarımı)

During the Design process of the Recommended System, which is the fourth process of the System Development Life Cycle, the screens, cameras, etc. that make up the Visitor Control System. The operating system to be used was determined by assembling the hardware parts. The Visitor Control System Application is planned to be developed on the Raspberry Pi operating system using the Python programming language and the necessary libraries for the application.

There is a "QUERY" button on the Visitor Control System shown in Fig. 9. When the button is clicked, the QR Code on the Visitor Entry Card, shown as an example in Fig. 10, is scanned by the camera at the back of the system, and it is determined whether the visitor is authorized to participate by the system.

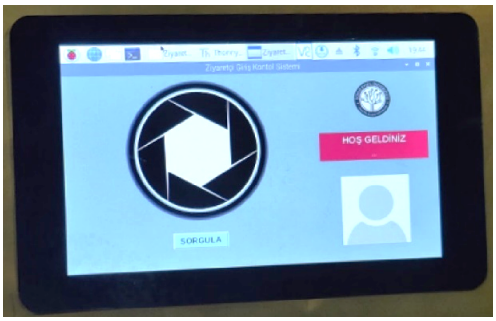


Figure 9. Visitor control system
(Ziyaretçi kontrol sistemi)

Figure 10. Visitor Entry Card Example
(Ziyaretçi kontrol kart örneği)

When the visitor shows the visitor entrance card with the QR code given to him before to the camera, it is shown in Fig. 11 together with the visitor's photo whether he is authorized or not. When the QR code is read with the Raspberry Pi camera in the application, if it is a registered participant, the message "ENTRY CONFIRMED" is displayed on the screen with the participant's name and surname on the Green Background as in Fig.11. Additionally, the photo of the participant previously uploaded to the system is shown, helping the visitor who wants to enter by the security guard to check over the photo.

On the other hand, when the Raspberry Pi camera reads the QR code, if it is not a registered participant, the message "INPUT NOT CONFIRMED" is displayed on the Red Background as in Fig. 12.

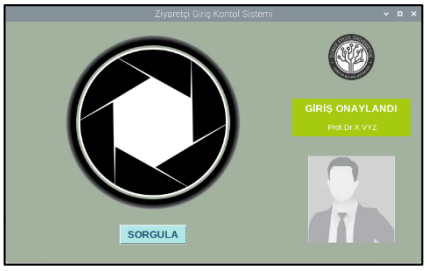


Figure 11. Screenshot of Visitor's Login Confirmation
(Ziyaretçi kontrol giriş onay ekran görüntüsü)

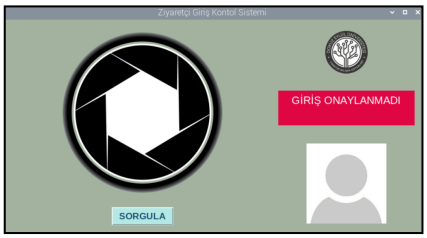


Figure 12. Screenshot of Visitor's Login Denial
(Ziyaretçi kontrol giriş ret ekran görüntüsü)

5.5. Software Development and Document Creation
(Yazılımın Geliştirilmesi ve Belge Oluşturulması)

Python programming language was used while developing the Visitor Control System application. In order for the codes and functions to be used in the design to work smoothly, the necessary libraries must be installed.

Raspbian Desktop Operating System (OS): Raspberry Pi does not come with an operating system inside. Therefore, to use Raspberry Pi, it needs to be installed an operating system. In this study, Raspian Desktop operating system was used for Raspberry Pi.

SD CardFormatter: Before printing the operating system on the SD card, it must be formatted. SD Card Formatter software is used for this.

Win32DiskImager: Win32DiskImager program is used to install Raspian Desktop operating system on the formatted SD card.

VNC Viewer: VNC Viewer program is used to remotely connect and control Raspberry Pi.

While developing the Visitor Control System application, Python programming language was used and the codes were tested online via the website https://snyk.io/code-checker/python/. Screenshots of the test and its results are shown in Figure 8.

As a result of the online test, it was determined that there was no security problem in the codes of the Visitor Control System Application. However, since the Visitor Control System Application is a system that works offline, it is a safe application against cyber attacks that can be made over the internet.

5.6. Testing and Maintaining the System
(Sistemin Test Edilmesi ve Sürdürülmesi)

After the software development process of the Visitor Control System application was completed, the system was tested. While testing the system, a few visitor photos and identification information were uploaded to the system as examples. Afterwards, the Visitor Entry Card with the QR code and participant/visitor information was scanned into the system. The information was checked by the QR code read by the system. As a result of the questioning, if the participant/visitor is registered or authorized, his/her photo is displayed to the security officer and his/her passage is approved. If the QR code is not registered or authorized as a result of the query, its entry is not approved and its passage is blocked.

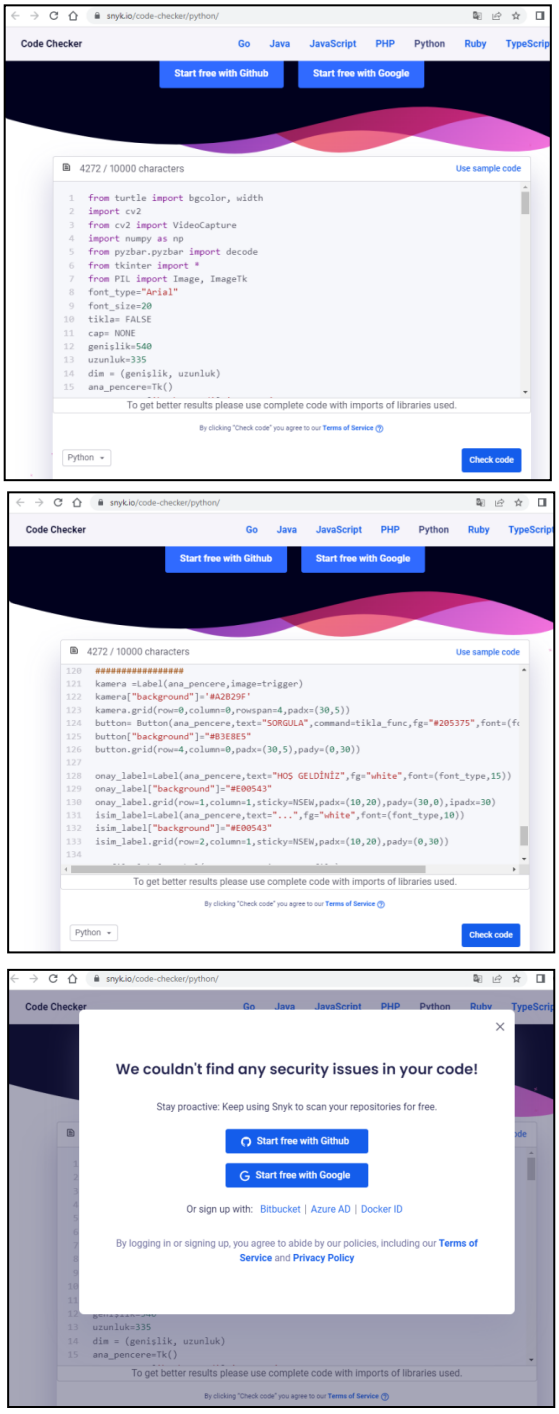


Figure 8. Test Result Screenshots of Application Codes *(Uygulama Kodlarının Test Sonucu Ekran Alıntıları)*

5.7. Implementation and Evaluation of the System
(Sistemin Test Edilmesi ve Sürdürülmesi)

The workflow for the visitor control system is presented in the Figure 13.

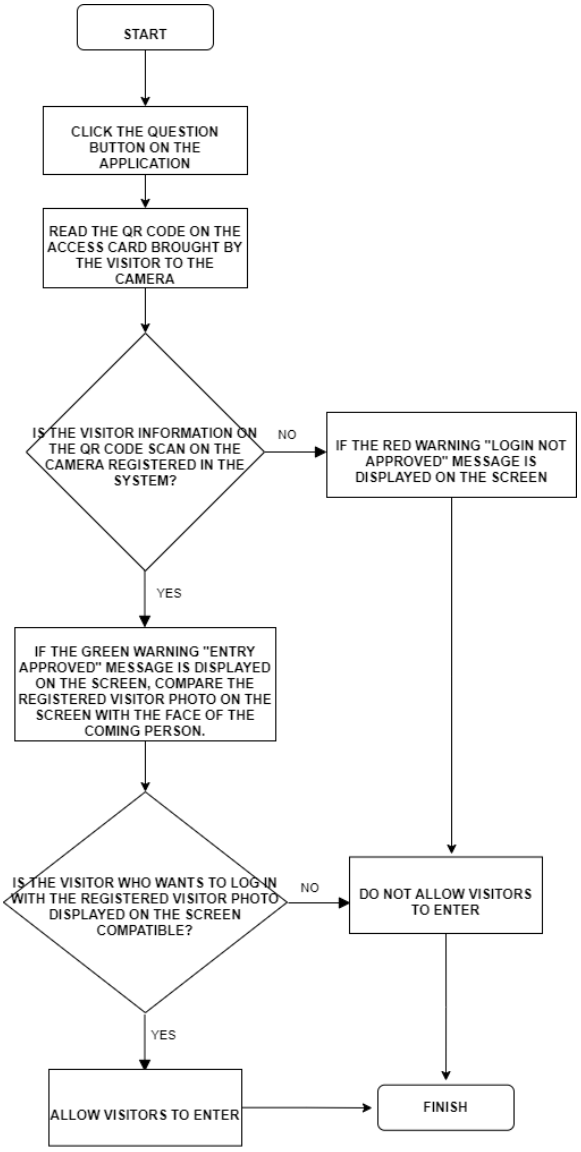


Figure 13. Workflow of Visitor Control System
(Ziyaretçi Kontrol Sistemi İş Akışı)

Visitor Control System can operate without being connected to any network or the internet. Thanks to its LCD Touch screen, it does not require any keyboard etc. It has been found that it can be used like a tablet without the need for hardware. Mobile power supplies, power banks, etc. are included in the system. It has been determined that when supported by devices, it has the ability to function in any environment without being exposed to power outages and cyber attacks.

5.8. Limitations *(Kısıtlar)*

In this study, the Visitor Control System Application was designed on the Raspberry Pi 3 board. It is not known whether the application will work on hardware or operating systems of other brands and perform the same functions. To give the simplest example of this from the Visitor Control System Application system, the developed application interface was developed in accordance with the Raspberry Pi 7 inch LCD Touch screen size (800 x 480 pixels). There is a possibility that the application interface may not work the same on different computers and screens and that there may be difficulties in using the system due to screen sizes.

Visitor Control System works with a Visitor Entry Card containing a QR code. The system works independently of the internet or any network. For this reason, it does not allow remote cyber attacks or remote modification of participant/visitor information. However, the reliability of the personnel who will upload photographs and identity information to the system is very critical. Because, as a result of the malevolent behavior of the personnel assigned to do these jobs, unwanted people will be able to pass, which may create a security vulnerability.

When the transition to the designed Visitor Control System is approved, the control of turnstile systems can also be integrated. This provides us with many opportunities to develop applications with the Raspberry Pi system. With the development of the system, statistics of participants/visitors who log in and records of people who are denied entry can be kept. In addition, the NFC feature of the new ID cards issued for use in Turkey can be integrated into the system and the participant/visitor security level can be increased to higher levels.

6. CONCLUSION AND DISCUSSION *(SONUÇ VE TARTIŞMA)*

The reliability of exhibitor / visitor access control systems in institutions has become a very important problem with the rapidly developing technology. When traditional visitor control systems are applied; In some cases, those who act in bad faith can use a fake ID, fake ticket, magnetic card belonging to someone else, shared password, etc. It is known that registered or unauthorized participants and visitors can log in with many different methods. This situation causes security gap in institutions. Today, it is known that cyber-attacks targeting all information systems in the world can also damage exhibitor / visitor access control systems. If the said cyber-attacks affect the access control systems in the institutions, the

participant/visitor information can be changed, and unregistered people are allowed to enter. Meeting, fair, seminar, conversation, symposium, workshop, fair etc. There is a possibility that the security guards at the entrances of the buildings where the organizations are held may make mistakes as to whether they are the real authorized participants since they have never seen and recognized the participants from different parts of the world.

In the study carried out within the scope of the study, it is aimed to develop a Visitor Control System to prevent these problems. While the Visitor Control System was being designed, the security vulnerabilities of the mentioned access control systems were examined, and a system was developed to eliminate these vulnerabilities. Within the scope of the information requirements of the system, the photos and identity information of the participants are required to upload the real photos of the participants or visitors to the system days before. Within the framework of the photos and information provided by the people, a Visitor Entry Card is prepared for the participant or visitor, which does not contain anything other than a QR code and the visitor's name. When the Visitor Entry card is scanned into the system, the participant/visitor's photo is checked by the security guard, and if the photo displayed in the system matches the participant/visitor, his/her pass is allowed, otherwise it is rejected. In this way, possible security vulnerabilities are prevented.

While testing the system, a few visitor photos and identity information were uploaded to the system as an example. Afterwards, the Visitor Entry Card containing the QR code and participant/visitor information was read into the system. The information was checked by the QR code read by the system. As a result of the inquiry, if the participant/visitor is registered or authorized, it was displayed to the security guard with his/her photograph and his/her pass was approved. If the QR code is not registered or authorized because of the question, its entry is not approved, and its passage is blocked. Visitor Control System can operate independently from any network or internet The LCD Touch screen can be used like a tablet without the need for hardware such as a keyboard. When mobile power supplies are supported by devices such as powerbanks, it can function in any desired environment without being exposed to power cuts and cyber-attacks.

The difference of the developed application compared to other security and transition systems is that it works offline and is not likely to be exposed to any cyber-attacks. Since the security guards do not know and see the participants at the entrance controls of the visitors before, they can make unauthorized entrances by malicious people with fake identities, apart from the real participants, and can engage in actions such as information spying, terrorist attacks, etc., according to their purposes. In this system, the information of the visitors is uploaded to the system by recording them together with their photos. Visitors are only given an entrance card with a QR code. In this way, it is almost impossible for an unauthorized user to log in, as the real photo and information of the person will be displayed when the QR code is scanned into the system, even if the ID is issued with fake photos.

There are access control systems produced by a wide variety of different companies in the market. However, these systems are not easy to maintain, requiring very high-cost annual maintenance contracts by companies. In addition, when a malfunction occurs in these systems in the following years, in cases where the company or the manufacturer cannot be reached, the system remains idle, and users must supply a new system. This situation has become a process that businesses and institutions do not want to encounter. Since the operating system used in Raspberry Pi, Raspberry Pi OS (formerly known as Raspbian), is a Linux-based operating system, Raspberry Pi was preferred when developing the Visitor Control System design and application because it is more stable than Windows and safer against cyber attacks.

Figure 14. Management Information Systems Pyramid *(Yönetim Bilişim Sistemleri Piramidi)*

Within the scope of this study, which is of interest to Management Information Systems, when the Management Information Systems Pyramid shown in Fig. 14 [24] is examined, the Cyber Security Based Visitor Control System in Institutions will play an active role in solving the problems that can be encountered from the lowest step of the pyramid to the top. Because when it comes to participant/visitor entrance security in institutions, it is a need that concerns everyone from the lowest employees to the highest-level managers.

However, if it is necessary to position this work exactly on the pyramid, the Cyber Security Based Visitor Control System in Institutions is within the scope of "Office Automation / Data Processing Systems", which is at the bottom of the Management Information Systems Pyramid. It is included in the scope of “Structural” within the scope of Problem Type, “Operational Decisions” in the scope of Decision Types and Operational Managers at the Managers level. However, when the Management Information Systems Pyramid is considered as a whole and an interrelated structure, it can easily see that all steps are needed.

REFERENCES *(KAYNAKLAR)*

[1] D. Hampton, A. Peach, and B. Rawlins, “Reaching Mobile Userswith QR Code,” *Kentucky Libraries*, vol. 75 (2), pp.6-10, 2011.

[2] X. Dou, and H. Li, “Creative Use of QR Codes in Consumer Communication,” *International Journal of Mobile Marketing*, Vol. 3, Issue 2, p. 61-67, 2008.

[3] N.-S. Chen, D. C.-E. Teng, and C. -H. Lee, “Augmenting Paper-Based Reading Activitieswith Mobile Technology to Enhance Reading Comprehension,”. in *The 6th IEEE Intenational Conference on Wireless*, DOI: 10.1109/WMUTE.2010.39, 2010.

[4] S. Karaca, “RFID teknolojisi ile anlık personel takip sistemi,” (Unpublished Master Thesis). İstanbul: Maltepe Üniversitesi, Fen Bilimleri Enstitüsü, 2010.

[5] U. Mamak, M. Z. Konyar, S. Solak, and M. H. Uçar, “Gerçek zamanlı yüz tanıma tabanlı personel kontrol ve takip sistemi tasarımı,”. *Avrupa Bilim ve Teknoloji Dergisi*, vol. (19), pp.497-504, 2020.

[6] M. M. Genli, “Bina Otomasyon Sistemleri,” (Unpublished Master Thesis), İstanbul: Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2005.

[7] G. Musayeva, and M. Yahyayev, “Biyometrik Güvenlik Sistemleri,”, 2014.

[8] N. Özkaya, and Ş. Sağıroğlu, “Açık Anahtar altyapısı ve Biyometrik sistemler,” in *I. Ulusal Elektronik İmza Sempozyumu*, pp.283-290, Ankara, Türkiye, 2006.

[9] E. Noma-Osaghae, O. Robert, C. Okereke, O. J. Okesola, and K. Okokpujie, “Design and implementation of an iris biometric door Access control system,” in *2017 International conference on computational science and computational intelligence (CSCI)*, pp. 590-593. IEEE, December 2017.

[10] W. A. Wahyudi, and M. Syazilawati, “Intelligent voice-based door Access control system using adaptive-network-based fuzzy inference systems (ANFIS) for building security,” *Journal of ComputerScience*, 3(5), 274-280, 2007.

[11] M. Dönerçark, and V. Tecim, “Kurumsal Karar Destek Sistemlerinde Yapay Zekâ Kullanımı: Tasarım ve Uygulama,” *Yönetim Bilişim Sistemleri Dergisi*, 6(2), 77-103, 2020.

[12] R. Rainer, “Introduction to information systems,” Hoboken, NJ: John Wiley and Sons, Inc. 2014.

[13] F. Aslay, “Siber saldırı yöntemleri ve Türkiye’nin siber güvenlik mevcut durum analizi,” *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28, 2017.

[14] F. Türk & M. Lüy, “Gömülü Sistemler ve Mühendislikte Uygulama Alanları,” *International Journal of Engineering Research & Development (IJERAD)*, 13(3), 2021.

[15] M. Merkepçi & M.S. Özyazıcı, “Parmak izine dayalı kapı kilit ve personel devam control sistemi,” in *Elektrik, Elektronik,Bilgisayar ve Biyomedikal Mühendislikleri Eğitim 4. Ulusal Sempozyumu*, 22-24 Ekim 2009, Eskişehir.

[16] M.K. Pehlivanoğlu & D.U.R.U. Nevcihan, “Üniversite Öğrencilerinin Devamlılığının Parmak İzi Okuyucu Cihaz Kullanılarak İzlenmesi,” *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 8(2), 9-16, 2016.

[17] A.B. Boydak, “İşyerlerinde Uygulanan Parmak İzli Giriş Kontrol Sistemine Hukuki Bakış,” *Türkiye Adalet Akademisi Dergisi*, (30), 321-336, 2017.

[18] M. Baykara & A. Sherzad, “Designing a securable smart home access control system using RFID cards,” *Journal of Network Communications and Emerging Technologies (JNCET)*, 10(12), 1-12, 2020.

[19] Komsek Elektronik Güvenlik Sistemleri Mühendislik İnşaat ve Reklam Tanıtım Hizmetleri Sanayi ve Ticaret Limited Şirketi. *Komsek Güvenlik Sistemleri, Kartlı Geçiş Sistemi Nedir ?* Available: https://www.komsek.com.tr/kartli-gecis-sistemi-nedir/. [Accessed: 14.05.2023].

[20] Perkotek Teknoloji Dış Tic. A.Ş. Şifreli Kapı ve Şifreli Kapı Kilidi. Available: https://www.perkotek.com/sifreli-kapi#:~:text=%C5%9Eifreli%20kap%C4%B1%20sistemleri%2C%20kap%C4%B1lar%C4%B1n%20kartlar,odalar%C4%B1nda%20da%20s%C4%B1k%C3%A7a%20tercih%20edilmektedir. [Accessed: 15.05.2023].

[21] S. D. Kolekar, V. B. Walekar, P. S. Patil, A. O. Mulani & A. D. Harale, "Password Based Door Lock System," *Int. J. of Aquatic Science*, 13(1), 494-501, 2022.

[22] N. N. San Hlaing & S. San Lwin, "Electronic door lock using RFID and password based on arduino," *International Journal of Trend in Scientific Research and Development*, 3(2), 799-802, 2019.

[23] BARFAŞ Otomasyon Teknolojileri Sanayi ve Ticaret Limited Şirketi. Kartlı Geçiş Sistemleri Tarihe Karışıyor, QR Geçiş Sistemleri Kolaylık ve Hız Sağlıyor. Available: https://www.barfas.com/blog-detay/kartli-gecis-sistemleri-tarihe-karisiyor-qr-gecis-sistemleri-kolaylik-ve-hiz-sagliyor. [Accessed: 26.05.2023].

[24] Tecim,V. (2023). Yönetim Bilişim Sistemleri (YBS). Available: https://vahaptecim.com.tr/yonetim-bilisim-sistemleri/, [Accessed: 12.06.2023].

[25] M. Oktaviandri & K. K. Foong. "Design and Development of Visitor Management System", *MEKATRONIKA*, vol. 1, no. 1, pp. 73–79, Jan. 2019.

[26] J. -J. Lin & S. -C. Huang. "The implementation of the visitor access control system for the senior citizen based on the LBP face recognition," *2017 International Conference on Fuzzy Theory and Its Applications (iFUZZY)*, Pingtung, Taiwan, 2017, pp. 1-6, doi: 10.1109/iFUZZY.2017.8311817.

[27] Alonso-Fernandez, F., Bigun, J., Fierrez, J., Fronthaler, H., Kollreider, K., Ortega-Garcia, J. "Fingerprint Recognition". In: Petrovska-Delacrétaz, D., Dorizzi, B., Chollet, G. (eds) *Guide to Biometric Reference Systems and Performance Evaluation*. Springer, London. https://doi.org/ 10.1007/978-1-84800-292-0_4. 2009.

[28] Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., Jain, A.K. "Performance evaluation of fingerprint verification systems," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 28(1), 3–18, 2006.

[29] R. Sanchez-Reillo & C. Sanchez-Avila. "Fingerprint verification using smart cards for access control systems," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 17, no. 9, pp. 12-15, Sept. 2002, doi: 10.1109/MAES.2002.1039788.

[30] L. A Mohammed, Abdul Rahman Ramli, V. Prakash, and Mohamed B. Daud. "Smart Card Technology: Past, Present, and Future," *International Journal of The Computer, the Internet and Management* Vol. 12#1 (January – April, 2004) pp 12 – 22.

[31] Meng Zheng and Shi-Bao. "A common smart-card-based conditional access system for digital set-top boxes," in *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 601-605, May 2004, doi: 10.1109/TCE.2004.1309434.

[32] A. Conklin, G. Dietrich and D. Walz. "Password-based authentication: a system perspective," *37th Annual Hawaii International Conference on System Sciences*, 2004. Proceedings of the, Big Island, HI, USA, 2004, pp. 10 pp.-, doi: 10.1109/HICSS.2004.1265412.

[33] Ting-Yi Chang, Cheng-Jung Tsai, Jyun-Hao Lin. "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices", *Journal of Systems and Software*, Volume 85, Issue 5, 2012, Pages 1157-1165, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2011.12.044.

[34] Brumen, Boštjan. "*System-Assigned Passwords: The Disadvantages of the Strict Password Management Policies*". 1 Jan. 2020 : 459 – 479.

Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Araştırma Makalesi / Research Article

Birleşik Krallık'ın Siber Güvenlik Politikasını Güç ve Caydırıcılık Üzerinden Anlamlandırmak

İbrahim Çağrı ERKUL*,a

[a,*] *Osmaniye Korkut Ata Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Osmaniye, Türkiye*

MAKALE BİLGİSİ

Alınma: 02.05.2024
Kabul: 04.06.2024

Anahtar Kelimeler:
Birleşik Krallık, Siber Güvenlik, Siber Caydırıcılık, Siber Uzay.
Sorumlu Yazar
e-posta:
ibrahimcagrierkul@osmaniye.edu.tr

ÖZET

Bilgisayar korsanlarının eylemlerinin ve yetkinliklerinin anlaşılmasına paralel olarak, 1980'li yıllarda siber uzayın Birleşik Krallık tarafından güvenlikleştirilmeye başlandığı görülmüştür. Web sitelerinin oluşturulmasının ardından tehdidin çeşitlenmesi ise siyasetin hem ulusal hem de uluslararası alanda konuya odaklanmasını mümkün kılmıştır. 1990'lı yılların hemen başında siber güvenliğin sağlanması noktasında kurumsallaşmaya yönelik adımlar atılmış olsa da siber saldırıların etkileri, hükümet ve çeşitli sektörler üzerinde hissedilmeye devam etmiştir. 2000'li yıllarda ise Birleşik Krallık siber uzayda gerçek bir anarşinin hüküm sürdüğü gerçeğiyle yüzleşerek, siber saldırılar karşısındaki savunmasızlığını giderecek siber güvenlik stratejileri belirlemek durumunda kalmıştır. Bu yönüyle makale, siber uzayın Birleşik Krallık için önemli hale gelme sürecini de dikkate alarak, 2009 ve sonrasında açıklanan siber güvenlik stratejileri üzerinden Birleşik Krallık'ın siber güvenlik politikasını ve siber yetkinliklerini analiz etmeyi amaçlamaktadır. Makale, realist bir perspektif üzerinden Birleşik Krallık'ın siber güvenliğini yalnızca savunmada kalarak elde etmesinin mümkün olmadığını ortaya koyarak, siber caydırıcılık ve saldırı kapasitesini realist temelde artırmasının gerekli olduğu iddiasındadır. Makalede realist anlayışa bağlı olarak arttırılması gereken siber güç ve saldırı kapasitesine rağmen siber uzayda dost ve müttefik aktörlerle iş birliğinin gerekliliği üzerinde de durulmuştur.

DOI: 10.59940/jismar.1477284

Interpreting the UK's Cyber Security Policy in Terms of Power and Deterrence

ARTICLE INFO

Received: 02.05.2024
Accepted: 04.06.2024

Keywords:
United Kingdom, Cyber Security, Cyber Deterrence, Cyberspace.
Corresponding Authors
e-mail:
ibrahimcagrierkul@osmaniye.edu.tr

ABSTRACT

In the 1980s, in parallel with understanding hackers' actions and capabilities, the United Kingdom (UK) began securitizing cyberspace. The diversification of the threat following the use of websites has made it possible for politicians to focus on cyberspace both nationally and internationally. Although institutionalization steps were taken to ensure cyber security in the early 1990s, the effects of cyber attacks impacted the government and various sectors. In the 2000s, the United Kingdom had to face the fact that there was absolute anarchy in cyberspace and determine cyber security strategies that would eliminate its vulnerability to cyber-attacks. In this respect, the article aims to analyze the UK's cyber security policy and cyber competencies through the cyber security strategies announced in 2009 and later, considering how cyberspace has become important for the UK. From a realistic perspective, the article claims that the UK can't achieve cyber security only through cyber defense and that it is necessary to increase her cyber deterrence and attack capacity on a realistic basis. The article also focuses on the necessity of cooperation with friendly and allied actors in cyberspace, even though the UK needs to increase its cyber power and attack capacity based on a realistic approach.

DOI: 10.59940/jismar.1477284

1. GİRİŞ *(INTRODUCTION)*

Birleşik Krallık Kabine Ofisi'nin 2009'da parlamentoya sunulması için hazırladığı bir strateji belgesinin sonuç bölümünde yer alan "*Nasıl ki 19. yüzyılda ulusal güvenliğimiz ve refahımız için denizleri, 20. yüzyılda havayı güvence altına almamız gerekiyorsa, 21. yüzyılda da siber uzaydaki konumumuzu güvence altına almamız gerekiyor*." [1] ifadesi, siber uzayın Birleşik Krallık için ne kadar önemsendiğini ortaya koymak açısından önemli bir kalkış noktası oluşturmaktadır. Buradan hareketle, Birleşik Krallık için siber uzayın güvenli hale getirilmesi sahip olunan büyük güç statüsünün devamı için de hayati bir yere sahiptir.

Birleşik Krallık'ın siber uzaya verdiği önem ve bu alanda güvenliğini sağlayabilmek için ortaya koyduğu çaba, 1980'li yıllara kadar geri gitmektedir. Zaman içerisinde siber tehdidin çeşitlenmesi ve bu alanda yetkinliklerini arttıran aktörlerin yapabilecekleri tahribatın anlaşılması, Birleşik Krallık'ın mevcut kurum ve yatırımlarla siber uzayda güvende kalamayacağını açıkça ortaya koymuştur. Devlet ve devlet destekli siber saldırılar başta olmak üzere tüm siber saldırılara karşı hazır olma ve bunlara cevap verebilecek bir siber kapasiteye sahip olma isteği, Birleşik Krallık'ın siber uzaya yaptığı kurumsallaşma çabalarının yanında, yatırımlarını da belirli stratejiler çerçevesinde gerçekleştirmesini gerekli kılmıştır.

Siber saldırıya uğrayan devletin, saldırının failini cezalandırılma ihtimalinin uluslararası hukuk nezdinde düşük olduğu dikkate alındığında, siber uzay anarşinin hüküm sürdüğü bir alan olarak değerlendirilebilir. Bu anarşi ortamında dost ve müttefik aktörler arasında ikili ve kurumsal temelde iş birliği imkânlarının önemsenmesi gerekmekle birlikte, Birleşik Krallık'ın başlıca tehdit aldığı Rusya, Çin, Kuzey Kore ve İran'a karşı realist bir temelde (saldırı ve caydırıcılığı da içerecek şekilde) oluşturulacak siber strateji izlemesi elzemdir.

Birleşik Krallık hem siber uzaydaki savunmasızlığını azaltmak ve caydırıcı olmak hem de bu alanda lider aktörlerden biri olabilmek amacıyla açıkladığı siber güvenlik stratejilerinin bir bütün olarak anlaşılmasını sağlamanın yanında, Birleşik Krallık'ın niçin realist temelde bir siber güvenlik stratejisi izlemesi gerektiğini gerekçelendirmeye çalışan bu makale, giriş ve sonuç bölümleri dışında üç bölümden oluşmaktadır. İlk bölümde siber uzayın Birleşik Krallık için önemli hale gelme süreci güvenlikleştirme kavramı ve yaşanan siber saldırılar üzerinden değerlendirmeye tabi tutulmuştur. İkinci bölümde ilki 2009'da açıklanan siber güvenlik strateji belgeleri üzerinden, Birleşik Krallık'ın siber güvenlik politikaları siber saldırılar, siber kapasite ve bu alandaki kurumsallaşmayı da içerecek şekilde detaylıca incelenmiştir. Son bölümde ise Birleşik Krallık'ın siber alanda izlediği/izlemesi gereken küresel iş birliğinin mümkün ve gerekli olduğu kabul edilerek, Birleşik Krallık için siber caydırıcılığı merkeze alan realist bir yaklaşımın gerekliliği ortaya koyulmuştur.

2. SİBER UZAYIN BIRLEŞİK KRALLIK İÇİN ÖNEMLİ HALE GELME SÜRECİ *(THE PROCESS OF CYBERSPACE BECOMING IMPORTANT FOR THE UNITED KINGDOM.)*

Siber casusluğun ilk örneklerinden biri olarak, 1986'da Lawrence Berkeley Ulusal Laboratuvarı'nın muhasebe sistemindeki küçük bir tutarsızlığın izini süren Clifford Stoll ve iş arkadaşları, tutarsızlığın sebebine yönelik olarak yaptıkları araştırmalarında, ABD'den bilgi çalarak KGB aracılığıyla Sovyetler Birliği'ne satan ve Batı Almanya'da ikamet eden bir bilgisayar korsanına ulaşmışlardır [2]. Yaşanan bu casusluk olayı, aktörlerin dikkatlerini dijital casusluğa çevirmelerini beraberinde getirmiştir.

Aynı dönemde Birleşik Krallık'ta siber güvenlik, bankacılık sektörü üzerinden ön plana çıkmaya başlamıştır. Bankaların bu noktada güvenliklerine yatırım yapmalarına rağmen bilgisayar dolandırıcılığı sebebiyle güvende olmadıkları ve büyük meblağlarda kayıp yaşadıkları iddia edilmiştir. Ortaya çıkan bu yeni tehdide karşı Birleşik Krallık'ta faaliyet gösteren çok sayıda banka, bilgisayar dolandırıcılığına karşı araştırma yapma ve bilgi paylaşımını içeren bir koordinasyon mekanizmasına dahil olmuştur. Yaşanan gelişmelere ve sektörde yaşanabilecek sorunların ortaya koyulmasına paralel olarak, bilgisayar güvenliğini sağlamak ve yönetmek, 1980'lerin ikinci yarısında Birleşik Krallık'ta giderek daha karmaşık bir hale gelmiştir [3].

1980'lerin sonlarında ise bilgisayar güvenliğine ilişkin konular, Birleşik Krallık'ta en üst düzeyde siyasetin gündemine gelmiştir. Bunda bilgisayarların artık yalnızca bilgi saklayan araçlar olmaktan çıkarak, operasyonel olarak çok sayıda sektörde kilit rol oynamaya başlaması önemli olmuştur. Finans sektörünün operasyonlarını baltalamaya yönelik kötü niyetli girişimlere bağlı olarak ortaya çıkan tehditler de Birleşik Krallık'ta farkındalığı arttırmıştır. Bankalar bilgisayar virüslerine karşı güvende olmak için büyük yatırımlar yapmayı gerekli görmüşlerdir [3]. Bu dönemde yaşananlarla Birleşik Krallık'ta siber uzay güvenlikleştirilmeye başlamıştır.

Barry Buzan'ın ifadesiyle güvenlikleştirme "*Güvenlikleştirme, bir şeyin, değerli olduğu kabul*

edilen bir öznenin varlığına yönelik bir tehdit olarak kurgulanması ve bu kurgulamanın buna mukabil alınan istisnai tedbirleri desteklemek için kullanılmasıdır." Diğer bir ifadeyle güvenlikleştirme, daha önce tehdit olarak görülmeyen bir konunun artık tehdit olarak kabul edilmesi ve bu tehdidin, zihni yönden inşa edilmesi olarak belirtilebilir [4]. Bu açıdan bakıldığında Birleşik Krallık, kendi varlığına yönelik olarak siber uzayda ortaya çıkan tehdidi güvenlikleştirmeye başlayarak, bu konuda atacağı adımları da halk nezdinde gerekçelendirme çabası içinde olmuştur.

Ayrıca şu da belirtilmelidir ki 1980'li yıllarda bilgisayar etiği konusu, ABD ve Birleşik Krallık'ta çok sayıda bilim insanının ilgisini çekmiştir. Bu konuya akademik anlamda odaklanılması, konuyu toplumun gündemine de taşımıştır [5]. Diğer taraftan en başından itibaren Birleşik Krallık'ın siber saldırıların yalnızca mağduru olmadığı, aynı zamanda bu saldırıları gerçekleştirdiği de unutulmamalıdır. CERN'deki bilim insanlarının ilk web sitesini oluşturmalarının hemen ardından birçok aktör, ağlar üzerinden gerçekleştirilebilecek casusluk faaliyetlerine yönelik bilgi sahibi değildi. İşte bu noktada Birleşik Krallık ortaya çıkan bu fırsatı değerlendirmiş ve ilk hedeflerinden biri olarak, Pakistan'ın nükleer programını seçmiştir. Bu programda çalışan bilim insanları, Birleşik Krallık Hükümet İletişim Merkezi[1] karşısında savunmasız kalmıştır [6].

Birleşik Krallık'ta gerçekleşen ilk siber suçlara bağlı olarak bu konuda yasal düzenleme yapılması kaçınılmaz hale gelmiştir. Bu bağlamda 29 Haziran 1990'da Bilgisayar Kötüye Kullanma Yasası kabul edilmiştir. Yasa metni incelendiğinde bilgisayar ve verilere yetkisiz erişimin ön planda olduğu belirtilmelidir. Ayrıca bu yasada cezai yaptırımların da detaylı bir şekilde düzenlendiği dikkate alınırsa, yasanın suç işleme niyetinde olanlar için caydırıcı bir yönü de bulunmaktaydı [7].

1990'lı yıllar web siteleri üzerinden siber güvenliği farklı bir noktaya taşımıştır. Bu noktada hacktivism Birleşik Krallık'ın siber suçlara yönelik farkındalığını arttıran bir diğer eylem olarak değerlendirilebilir. Birleşik Krallık'ta yaşanan ilk hacktivist olay, 1994 yılında "Zippies" ismindeki Kaliforniyalı grubun dönemin başbakanı John Major'un açık havada yapılacak gösteri ve festivallerine yönelik yasaklama kararı sonrasında, Birleşik Krallık'taki web sitelerini çökerten bir siber saldırı gerçekleştirmesiyle meydana gelmiştir [8]. Bireysel veya grup halinde hareket eden internet korsanlarının siyasi tepkilerini ortaya koymak için gerçekleştirdikleri eylemler, devlet düzeyinde sahip olunan imkân ve tecrübeden yararlanılması durumunda, casusluk da dahil olmak üzere karşılaşılabilecek zararlar üzerinde düşünülmesini gerekli kılmıştır.

Geleneksel yöntemlerle gerçekleştirilen casusluk, halen Birleşik Krallık için bir tehdit olmakla birlikte, iletişim alanındaki küresel gelişmeler siber uzayın bir casusluk aracı olarak kullanılmasını da beraberinde getirmiştir. Siber uzayın casusluk eylemleri için önemi, siber casusluğun güvenli bir mesafeden operasyon yapılmasını mümkün kılması ve saldırıları yapanlara suçlama atfedilmesini zorlaştırmasıyla ilişkilidir. Böylece aktörlerin casuslukla bağlantılı siyasi sorumluluk/suçlama riski de minimize edildiği için [9] siber casusluk yaygın olarak kullanılmaya başlanmıştır. Birleşik Krallık siber casusluğu hem uygulayan hem de bu konudan mustarip olan bir aktör olarak nitelendirilebilir.

Siber alanda yaşanabilecek güvenlik sorunlarına karşı, Birleşik Krallık'ın görece erken bir dönemde önlemlerini almaya başlaması önemlidir. Bu bağlamda Birleşik Krallık hükümeti ilk bilgisayar güvenliği ekibini 1992 yılında UNIRAS (Birleşik Olay Müdahale ve Uyarı Hizmeti) ismiyle kurmuştur. Ancak ekibin kurulduğu ilk dönemde nasıl bir görev yaptığı anlaşılamadığı için büyük ölçüde işlevsiz kalmıştır. Diğer taraftan Birleşik Krallık, gelebilecek saldırılara yönelik temkinli olması nedeniyle, parlamento yetkililerinin ofislerinden internete erişmelerine müsaade edilmemiştir. Tony Blair'in 1997'de başbakan olmasından sonra ise bu uygulama kaldırılmıştır. Şu husus ayrıca ifade edilmelidir ki Birleşik Krallık Hükümeti'nin internete Amerikalılardan daha geç ulaşması[2], siber güvenlik konusunda daha fazla düşünebilmesi için de bazı fırsatlar sunmuştur. ABD'nin 1990'lı yıllarda bilgisayar korsanları için Birleşik Krallık'a nazaran daha ilgi çekici bir hedef olması, Birleşik Krallık için güvenli internetin sağlanması noktasında önemliydi. Çünkü bu dönemde hükümet siber uzayı araştırırken, karşılaşılabilecek tehlikelerin de farkına varmaya başlamıştır. Bu farkındalığa rağmen kısa süre sonra Çin kaynaklı olduğu düşünülen siber saldırılar, hükümeti ve havacılık sektörünü etkilemeye başlamıştır [6].

2000'li yılların ortalarına gelindiğinde, Birleşik Krallık Ulusal Altyapı Güvenliği Koordinasyon

[1] Government Communications Headquarters (GCHQ).

[2] Hükümet yetkililerinin ofislerinde internet kullanmaları açısından.

Merkezi[3] bir süredir devam eden siber saldırıların, son dönemde karmaşıklığının arttığı uyarısında bulunmuştur. Bu dönemde aralarında savunma, iletişim ve hükümet sistemlerinin yer aldığı yüzlerce devlete bağlı kurum ve kritik kabul edilebilecek işletmenin hedef alındığı dikkate alınmalıdır [6]. Bu saldırıların Çin merkezli olduğu ve aralarında ABD'nin de olduğu çok sayıda devleti etkilediği not edilmelidir.

Her ne kadar MI5[4] Çin'in siber saldırılarına yönelik görüşünü 2007'de belirtmiş olsa da Birleşik Krallık'ın Çin'den aldığı siber tehdit, MI5'ın 2008'de hazırladığı bir raporla görünür hale gelmiştir. 2009'da Ortak İstihbarat Komitesi[5] de Çin'in Birleşik Krallık'a yönelik siber saldırılarıyla ilgili bir uyarıda bulunmuştur. Devam eden süreç içerisinde Çin'den alınan siber tehdit, Birleşik Krallık tarafından resmi olarak tekrar tekrar vurgulanmıştır [10]. Bu dönemde Birleşik Krallık karşılaştığı siber saldırılarla, siber uzayda gerçek bir anarşinin hüküm sürdüğünü tecrübe etmek durumunda kalmıştır. Kısaca anarşinin hüküm sürdüğü bir alanda pasifist[6] olmak, gerçeklikten kopmak anlamına geleceği için Birleşik Krallık siber uzaya realist temelde bakmak mecburiyetini hissetmiştir.

Realist teorinin önemli isimlerinden Thomas Hobbes, anarşi kavramını açıklarken kullandığı Leviathan'ı her ne kadar yerel toplumlara yönelik kullansa da ortaya koyduğu fikirlerinin uluslararası politikayı da kapsadığı ileri sürülebilir. Uluslararası politikada düzeni sağlayacak bir Leviathan'ın (egemen gücün) yokluğunda ortaya çıkacak anarşinin, beraberinde getireceği savaş/çatışma ise kaçınılmaz olacaktır. Devletlerin böyle bir ortamda güvenliklerini sağlayabilmeleri için ihtiyaç duydukları şey güçtür. Haliyle devletlerin güçlerini artırarak güvenliklerini sağlama yoluna gitmeleri ise bir zorunluluk olarak görülür [12].

Şu husus vurgulanmalıdır ki realist bakış açısıyla savaş, küresel siyasal kültürün bir parçası olarak kabul edilmiştir. Bahsi geçen siyasal kültüre göre savaştan kaçmak değil onunla baş etmek ve savaştan sağ çıkmak esastır [13]. Bu bağlamda gelinen noktada Birleşik Krallık için en iyi tercih siber uzayda yaşanabilecek "savaşlardan" kaçınmak değil, bu savaşlardan sağ çıkmak olacaktır. Siber savaşlardan sağ çıkabilmek için ise ortaya koyulacak gerçek bir iradenin yanında siber stratejilere de ihtiyaç duyulmuştur.

3. SİBER GÜVENLİK STRATEJİ BELGELERİ BAĞLAMINDA BİRLEŞİK KRALLIK'IN SİBER GÜVENLİK POLİTİKASI *(CYBER SECURITY POLICY OF THE UNITED KINGDOM IN THE CONTEXT OF CYBER SECURITY STRATEGY DOCUMENTS)*

Birleşik Krallık'ın ilk siber güvenlik strateji belgesini 2009'da ortaya koyduğu dikkate alındığında, ilk ulusal siber güvenlik stratejisini 2003 yılında yayınlayan ABD'nin zamansal olarak gerisinde kaldığı ileri sürülebilir. 11 Eylül 2001'de gerçekleşen terör saldırıları, bu noktada ABD için motive edici olmuşken, Birleşik Krallık için ise 2007'de Estonya'ya karşı gerçekleştirilen siber saldırılar, siber uzayda karşılaşılabilecek zorlukları görünür kılmış ve siber güvenlik stratejisinin ilan edilmesinde dikkate alınmıştır [14].

Estonya'nın 2007'de II. Dünya Savaşı'nda ölen Sovyet askerleri anısına inşa edilen bir anıtı, şehir merkezinden kaldırarak kenar mahallelere taşıma kararı almasının hemen ardından, Estonya'da Rusça konuşan topluluk eş zamanlı olarak fiziksel bir isyan başlatmıştır. Estonyalı yetkililere göre arkasında Rusya'nın olduğu bu siber saldırı, Estonya'yı hedef almıştır. Başlatılan siber saldırıyla 85 bin bilgisayar hacklenmiş ve önemli kabul edilebilecek 58 web sitesi de ele geçirilmiştir [15]. Siber alandaki en karmaşık tehditlerin farklı teknikleri bir arada kullanan ve siber kapasiteleri yüksek olan devletler tarafından yapıldığının [1], Estonya'da yaşananlarla bir kez daha görülmesi, Birleşik Krallık'ın da devleti merkeze alan bir siber güvenlik stratejisi ile sürece adım atmasına gerekçe olmuştur.

Ayrıca 2009'da hükümetin, Birleşik Krallık çıkarlarının siber operasyonlara karşı savunmasızlığını ve siber operasyonların Birleşik Krallık çıkarları üzerindeki etkisini azaltma hedefinde olunduğunun belirtilmesi önemlidir [1]. Bu noktada siber uzay kavramının ağ bağlantılı her türlü dijital etkinliğin yanında, dijital ağlar üzerinden gerçekleşen eylemleri de kapsadığı dikkate alındığında [1], güvenlik ihtiyacının ne kadar geniş bir alanda sağlanması gerektiği ve Birleşik Krallık'ın bunu başarabilmek için gerçek bir iradeye ihtiyaç duyduğu açıktı.

Bu dönemde konunun ne kadar ciddiye alındığının görülmesi bakımından, Birleşik Krallık'ın en yüksek önceliğe sahip ulusal güvenlik konusu olarak kabul

---

[3] The National Infrastructure Security Co-ordination Centre (NISCC).
[4] Military Intelligence, Section 5 (MI5).
[5] Joint Intelligence Committee (JIC).

[6] Keane'nin belirttiği üzere pasifizm "*şiddetle karşı karşıyayken bile, şiddete başvurmayı açıkça ve ilkeli bir tarzda reddetmek*" şeklinde tanımlanırsa [11] pasifist bir yaklaşımın caydırıcılığı tamamen sonlandıracağı açıktır.

ettiği siber güvenliğin ekonomiyi[7] de kapsaması [9], Birleşik Krallık için iş dünyasını siber anlamda güvenli kılınmasının önemini ortaya koymuştur. 2011'de açıklanan "Birleşik Krallık Siber Güvenlik Stratejisi: Birleşik Krallık'ı Dijital Dünyada Korumak ve Desteklemek" başlığını taşıyan siber güvenlik strateji belgesinde, 2015'e kadar ulaşılması istenen bazı hedefler belirlenmiştir. Buna göre Birleşik Krallık'ın siber suçlarla mücadele ve siber uzayda iş yapmak için dünyanın en güvenli yerlerinden biri olması, siber saldırılara karşı dayanıklı ve siber uzaydaki çıkarlarını daha iyi koruyabilecek bir konuma gelmesi, Birleşik Krallık halkının güvenle kullanabileceği ve açık toplumları da destekleyen açık, istikrarlı ve canlı bir siber alana sahip olmasına destek olunması ve Birleşik Krallık'ın siber güvenlik hedefleri için ihtiyaç duyduğu ortak bilgi, beceri ve yeteneğe ulaşması hedeflenmiştir [17]. Burada siber güvenliğin ancak bütüncül bir yaklaşımla sağlanabileceğinin altının çizilmesi önemlidir.

2011'de dönemin başbakanı David Cameron'un hükümetin yayınladığı yeni siber güvenlik stratejisine yönelik olarak ifade ettikleri önemlidir:

> *"İnternet şüphesiz sosyal ve politik faydaya yönelik bir güç ve ekonomimizin büyümesi açısından da hayati önem taşıyor olsa da güvenliğimize yönelik tehditlere karşı korunmamız gerekiyor. Bu strateji yalnızca teröristlerin ulusal güvenliğimize yönelik tehdidini değil, aynı zamanda refahımızı tehdit eden ve siber suçlar yoluyla birçok sıradan insanın hayatını mahveden suçluları da ele alıyor. Siber güvenlik hükümet için en önemli önceliklerden biridir ve Birleşik Krallık'ın iş yapmak için dünyadaki en güvenli yerlerden biri olarak kalmasını sağlamak için polis, güvenlik hizmetleri, uluslararası ortaklar ve özel sektörle yakın iş birliği içinde çalışmaya devam edeceğiz*" [18].

Açıklanan siber güvenlik stratejisine bağlı olarak, Birleşik Krallık'ın siber güvenlik için ayırdığı bütçede de bir artış yapılmıştır. Buna göre 2011-2012 döneminde 105 milyon Pound olan bütçe, 2012-2013 döneminde 155 milyon Pound'a yükseltilmiştir. 2011-2015 yılları arasında ayrılan kaynağın toplam 650 milyon Pound olduğu da dikkate alınırsa, bu dönemde hükümet siber güvenlik için artan oranlarda kaynak ayırmaya devam ettiği görülecektir [18].

Birleşik Krallık, Soğuk Savaş döneminde diğer birçok aktör gibi büyük ölçüde öngörülebilir bir biçimde askeri veya nükleer tehditlerle karşılaşmıştır. Soğuk Savaş döneminde hissedilen bu varoluşsal tehdit, öngörülebilirliği üzerinden değerlendirildiğinde, bugün tehditlerin öngörülmesi zorlaşmıştır. Bugünün uluslararası ilişkilerinde aktörler geleneksel savaştan daha ucuz,[8] daha kolay erişilebilir ve daha az suçlama yapılabilecek/atfedilebilebilecek tehdit ve saldırı araçları arayışındadırlar. Buna bağlı olarak düşman tanımlaması farklılaştığı gibi, karşılaşılan tehditler de çeşitlenmektedir. Bu tehditlerin arasında siber saldırı ve kritik hizmetlerin kesintiye uğratılması da yer almaktadır [9]. Tüm dünyada siber güvenlik çekincelerini artmasına sebep olan Stuxnet saldırıları, Birleşik Krallık'a kritik alt yapı güvenliğinin önemini bir kez daha hatırlatmıştır.

Stuxnet kötü amaçlı yazılımı üzerinden İran'ın nükleer tesislerine yönelik gerçekleştirilen saldırıların sorumluluğunu hiçbir grup veya ülke üstlenmemesine rağmen uzmanlar gelişmiş ve karmaşık yapısı üzerinden Stuxnet'in bir devlet tarafından geliştirilmiş olması gerektiğine inanmışlardır. Bu bağlamda ABD, İsrail, Birleşik Krallık, Rusya, Çin ve Fransa Stuxnet'i geliştirebilecek maddi ve teknik becerilere sahip ülkeler arasında değerlendirilmiştir. İran'ın Stuxnet sebebiyle NATO'nun yanında özellikle ABD ve İsrail'i suçladığı da not edilmelidir [20].

Stuxnet saldırıları iki ayrı sebeple önemli kabul edilebilir: Stuxnet enerji ve diğer birçok endüstriyel kontrol merkezindeki sistemlerin ne kadar savunmasız olduğunu ortaya çıkarmıştır. Kritik alt yapı unsurları da benzer sistemlere sahip olduğu için siber saldırılara karşı güçlendirilmesi gerekli hale gelmiştir. İkinci olarak Stuxnet gibi kötü amaçlı yazılımlar, diğer aktörler tarafından kopyalanmasının ardından geliştirilerek yeni bir siber silah olarak farklı amaç ve hedefler üzerinde kullanılabileceği unutulmamalıdır [21].

Birleşik Krallık'ta 1980'ler ve 1990'larda gerçekleştirilen özelleştirilmelerden önce devletin ulusal kritik alt yapı unsurları üzerinde doğrudan kontrolü az olmakla birlikte, devam eden süreçte ulusal kritik altyapı unsurlarının büyük ölçüde özel sektöre geçmesi ve özel sektör tarafından işletildiği [22] dikkate alındığında, tehlike ve Birleşik Krallık'ın sorumluluğu daha net görülecektir. Osborne'un belirttiği üzere yalnızca elektrik alt yapısının işlevsiz kalması durumunda bile bankalar ve hastanelerin çalışmayı durdurması veya hükümetin kendisinin

---

[7] Birleşik Krallık'ın ekonomik sebeplerle siber güvenliği önemsemesi fazlasıyla anlaşılabilir. Örneğin kötü amaçlı bir yazılım olan "NotPetya", bir Birleşik Krallık şirketi olan Reckitt Benckiser'i 120 milyon Pound zarara uğratmıştır [16].

[8] Son dönemde bazı bilim insanları ve politikacılar arasında konvansiyonel savaş hazırlıklarının fazlasıyla maliyetli olduğu ve bu maliyete rağmen hazırlıkların ulusal güvenliğe olumsuz etkide bulunduğu yönündeki düşünce yaygınlaşmaktadır [19]. Bu noktada siber uzayda yaşanabilecek savaşlara karşı yapılacak hazırlıklar önemli bir alternatif olarak ön plana çıkmaktadır.

artık faaliyet gösteremeyecek bir hale gelmesinin oluşturduğu etki, Birleşik Krallık toplumunu felakete sürükleyebilir. Bu sebeple Birleşik Krallık'ın kritik sektörlerin korunmasına yönelik sorumluluğu olmakla birlikte, bahsi geçen sektörlerdeki şirketlerin de kendi siber dayanıklılıklarını sağlama sorumluluğu bulunmaktaydı [23].

Birleşik Krallık'ın 2011 siber güvenlik stratejisine göre, siber uzayda Birleşik Krallık'a yönelik en karmaşık olarak değerlendirilebilecek tehditlerin bir kısmı, casusluk temelinde diğer devletlerden gelmekteydi. Bu devletler aynı zamanda Birleşik Krallık'ın askeri, endüstriyel ve ekonomik varlıklarını hedef almalarının yanı sıra Birleşik Krallık'ta ikamet eden ve kendi rejimlerine muhalif olan kişileri de takip etmekteydiler. Diğer taraftan olası bir çatışma durumunda düşman olarak nitelendirilebilecek bir aktör, siber uzaydaki güvenlik açıklarından yararlanarak Birleşik Krallık ordusunun teknolojik anlamda sahip olduğu avantajı azaltabilir ve bunu Birleşik Krallık'ın kritik altyapı unsurlarına saldırmak için kullanılabilirdi [17]. Tüm bunları dikkate alan Birleşik Krallık, devam eden süreç içerisinde siber uzaydaki yetkinliklerini artırmaya çalışmakla beraber bir ikilemle karşılaşmıştır.

2013'te Edward Snowden'ın aralarında Birleşik Krallık'ın da bulunduğu Batılı devletlerin istihbarat teşkilatlarının iletişim verilerine müdahale ettiğine yönelik yaptığı ifşaatları, devletlerin izleme yetkilerinin genişletilmesine karşı olan lobinin güçlenmesine sebep olmuştur [24]. Esasında Birleşik Krallık İç İşleri Bakanlığı'nın "siber suç stratejisi" başlığını taşıyan 2010 yılına ait belgede de belirtildiği üzere vatandaşların güvenliğini ve yaşam hakkını korumak için gerekli önlemleri alırken, bu önlemlerin Birleşik Krallık için hayati öneme sahip olan temel haklar üzerindeki etkisini dengelemeye çalışılması [25], zorlayıcı olmuştur. Konuya yönelik artan farkındalık gizlilik ve insan hakları yasaları, istihbarat teşkilatlarının faaliyetlerine giderek daha fazla kısıtlama getirmeye devam etmektedir. Bu nedenle aralarında Birleşik Krallık'ın da yer aldığı çok sayıda Batılı ülkenin istihbarat teşkilatları, veri koruma ve diğer yasaları izlemek için avukatlar ve halkla ilişkiler uzmanları çalıştırmak durumunda kalmaktadırlar [26]. Snowden'ın ifşası bu noktada Birleşik Krallık için demokratik bir aktör olarak, demokratik olmayanlara göre siber güvenliği sağlamasının daha zor olacağı bir dönemi başlatması sebebiyle önemliydi.

Özetle Lucas'ın da belirttiği üzere, casuslukta kapalı toplumlar açık olanlara göre üstün bir konuma gelmiştir. Diğer taraftan Batılı ülkelerin Çin, İran, Rusya gibi aktörler üzerinde gözetleme yapması zorlaşırken, bu ülkelerin istihbarat servislerinin dünyanın geri kalanını gözetlemesi kolaylaşmıştır [26]. Ayrıca şu husus da belirtilmelidir ki Birleşik Krallık ve ABD, baskıcı rejimlere sahip olan ülkelerde faaliyet gösteren muhalif gruplara siber temelde verdiği destekle, internet kullanıcılarının gözetim ve sansüründen kaçmasına yardımcı olmaktadır. Baskıcı rejimler ise bunu bir çeşit siber saldırı olarak değerlendirmektedir [27]. Bu yönüyle Batılı liberal demokrasiler ve otoriter devletlerin siber uzaydan aldıkları tehdit farklılaşmaktadır. Otoriter devletler için bu noktada temel endişe kaynağı rejimin benimsediği dünya görüşü ve kontrol altında tuttuğu bilgi akışının sorgulanmasına ve eleştirilmesine yol açacak siber destekli eylemler ve devrimlerin ortaya çıkmasıdır. Buradan hareketle siber suçlar otoriter devletler için de bir sorun olmakla birlikte, siber uzay rejimlerinin devamı için bir tehdit olarak görülmüştür [28].

2016 yılının sonlarıyla birlikte başlatılmış olan yeni siber güvenlik stratejisi ise ortaya koyulan stratejinin bir parçası olarak Birleşik Krallık veri, sistem ve ağlarını savunmanın yanında, düşmanlar için caydırıcı olmayı, siber güvenlik sektörünü büyütmeyi ve siber alanda kritik yeteneklerini geliştirme amacındaydı. Bunu gerçekleştirmek için, 1,9 milyar Pound yatırım yapılmasının planlanmış olması dikkate değerdir [29].

Bu dönemde Birleşik Krallık siber güvenlik temelinde sahip olduğu pozisyona güvenmekle birlikte, dünya çapında az sayıda devletin kendi güvenliğine ve refahına ciddi bir tehdit oluşturacağı yönünde bir düşünceye sahipti. Bu devletler, yıkıcı olanlar da dahil olmak üzere, Birleşik Krallık'ın altyapısı ve endüstrisi için tehdit oluşturma potansiyeline sahip olarak değerlendirilmekteydi. Diğer taraftan çok sayıda devletin de geliştirmeye devam ettikleri siber programlar aracılığıyla Birleşik Krallık için gelecekte tehdit oluşturmaları mümkün olarak kabul edilmiştir. Burada dikkat edilmesi gereken husus, bazı devletlerin cezalandırılmayacaklarını düşünerek gerçekleştirdikleri siber saldırılarla diğer aktörleri benzer eylemler için motive edebileceklerinin belirtilmiş olmasıdır [30]. Siber güvenlik stratejisinde üzerinde durulan devlet veya devlet destekli eylemlerin yanıtsız bırakılmaması düşüncesi, yalnızca savunmayı değil saldırı imkanlarının arttırılmasını da gerekli kılmıştır.

Siber güvenlik kavramı sıklıkla tehdit, saldırı ve savunma gibi kelimelerle bir arada kullanıldığı için askeri bir sorun gibi algılanabilse de yalnızca askeri bir sorun değildir. Çünkü siber güvenlik, bir bütün olarak ve tüm toplum için bir sorun olarak ortaya çıkmıştır. Bu bağlamda geniş, işbirlikçi ve çok sayıda kurumun dahil olduğu bir müdahaleyi de gerektirmektedir [31]. Birleşik Krallık geniş bir

temelde siber güvenliğe önem vermek durumundadır. Bahsi geçen gereklilik Birleşik Krallık tarafından kabul edilmiştir. Buradan hareketle siber güvenlik yalnızca hükümete yönelik bir tehdit olarak değerlendirilmemiş, özel sektör ile vatandaşlar da bu kapsamda önemsenmiştir [9].

2016'ya dair değinilmesi gereken bir diğer gelişme, Birleşik Krallık'ta Hükümet İletişim Merkezi siber güvenliğe ilişkin konularda ana organ olmaya devam etse de kurulan Ulusal Siber Güvenlik Merkezi[9]aracılığıyla, ulusal düzeyde siber güvenliği sağlayacak merkezi bir yapılanma[10] oluşturulmasıdır. Ulusal Siber Güvenlik Merkezi'nin ulusal düzeydeki siber olayları yönetme, siber güvenlik konusunda uzmanlık ve tavsiye sunmanın yanında, siber güvenlik endüstrisini destekleme çabasında olması amaçlanmıştır [30]. Bu bağlamda ulusal düzeydeki siber güvenlik konularında Birleşik Krallık'a işlevsel katkı sunmaya başlayan Ulusal Siber Güvenlik Merkezi aktif bir siber savunma üzerinden Birleşik Krallık'ın siber saldırılara karşı daha güçlü olmasını mümkün kılmıştır [33]. Aktif siber savunma stratejisinin uygulanmasına paralel olarak Birleşik Krallık'ta siber suç tehdidinin azaldığı dikkate alınırsa [34], aktif siber savunmanın işlevsel olarak Birleşik Krallık'ın siber güvenlik stratejisine katkı sunduğu belirtilmelidir.

Siber güvenlik stratejilerinde hedeflendiği şekilde yetkinliklerini arttıran Birleşik Krallık, siber uzayda önemli bir aktör olmakla birlikte, geniş bir alanda çevrimiçi sistemlere sahip olması ve ekonomisini dijital bir temele oturtması sebebiyle, aynı zamanda siber saldırılara karşı korunmasız kalma riskini de sürdürdüğüne inanmaktadır [35]. Ulusal Siber Güvenlik Merkezi'nin verilerine göre Birleşik Krallık'ta Eylül 2020 ile Ağustos 2021 arasında Ulusal Siber Güvenlik Merkezi'nin tarafından yönetilen 777 siber güvenlik olayının yaklaşık %40'ının kamu sektörünü etkilediği göz önünde bulundurulursa, kamu siber saldırılar için cazip bir hedef olmayı sürdürmektedir [36].

İşte bu sebeple Birleşik Krallık 2022-2030 yıllarını kapsayan siber güvenlik strateji belgesinde bulunan siber dayanıklılık hedefi, izlenmek istenen siber stratejinin merkezinde yer almaktadır. Siber dayanıklılığın siber saldırılara rağmen bir kuruluşun temel işlevlerini ve hizmetlerini sürdürme ve verilerinin korunmasını sağlama yeteneği olduğu dikkate alındığında, Birleşik Krallık'ta hükümetin ekonomi ve toplumsal temeldeki hizmetleri sunma sorumluluğunda olması, siber dayanıklılığı vazgeçilmez kılmaktadır. Bu bağlamda Birleşik Krallık'ın 2022-2030 vizyonu, dijitalleşen temel/kritik hükümet işlevlerinin 2025 yılına kadar siber saldırılara karşı önemli ölçüde sağlamlaştırılması ve kamu sektörü genelinde faaliyet gösteren tüm hükümet kuruluşlarının en geç 2030 yılına kadar bilinen güvenlik açıklarına ve saldırı yöntemlerine karşı dayanıklı hale getirilmesi amaçlanmaktadır [36].

Birleşik Krallık'ın 2022-2030 vizyonunda kurulması öngörülen Hükümet Siber Koordinasyon Merkezi[11] ile hükümete bağlı kuruluşların operasyonel siber güvenlik çabalarını daha iyi koordine etmek ve hükümetin kurumlarıyla birlikte "tek vücut" olarak savunma yeteneğini geliştirmesi hedeflenmektedir [36]. Siber uzayın bütüncül bir biçimde korunması gerekliliği dikkate alındığında, bu merkezin kurulması fazlasıyla rasyoneldir.

Birleşik Krallık'ın güncel siber güvenlik stratejisinde üzerinde durulan bir diğer husus, toplumda siber kültür oluşturulmasının gerekliliğidir. Bu noktada kamu çalışanlarına odaklanılmış ve oluşturulacak olan siber güvenlik kültürüyle, kamu görevlilerinin siber güvenlik farkındalığını ve bilgilerini arttırarak kendilerini ve çalıştıkları devlet kuruluşlarını daha iyi koruyabilmelerinin sağlanması amaçlanmıştır [36].

4. BİRLEŞİK KRALLIK'IN SİBER GÜCÜNÜN GELECEĞİ *(THE FUTURE OF THE UNITED KINGDOM'S CYBER POWER)*

Siber saldırıların uluslararası niteliği saldırının faillerinin gizlenmesini kolaylaştırmakla birlikte, saldırıyı gerçekleştirenler amaçlarına ulaşmaları durumunda açığa çıkmaktan da görece endişe etmezler. Diğer taraftan, devlet onaylı veya devlet destekli olarak gerçekleştirilen siber saldırıların cezalandırılma ihtimali, mevcut uluslararası yasal çerçeve dikkate alındığında düşüktür. Nihai olarak ise siber eylemi sebebiyle hiçbir yaptırımla karşılaşmayan bir aktörün faaliyetlerine devam etme olasılığı da yüksektir. Bu aktöre karşı etkili bir ceza/karşılık verilmediği takdirde diğer aktörlerin de benzer siber saldırılara teşvik edilmesi de ihtimal dahilindedir [37]. Bu sebeple siber saldırılara karşı aktörlerin savunmada kalmak yerine saldırı yeteneklerini geliştirmelerinin mümkün olduğunu [38] kabul etmeleri ve buna uygun bir strateji

[9] The National Cyber Security Centre (NCSC).
[10] Birleşik Krallık'ın siber güvenlik alanında özel sektör ile kamu sektörü arasındaki boşluğu doldurması ve Ulusal Siber Güvenlik Merkezi'nin sağlamakta olduğu siber hizmetlere erişilebilirliği artırılması, ulusal siber güvenliğin sağlanmasına yardımcı olacaktır [32].
[11] Government Cyber Coordination Centre (GC3).

izlemeleri ulusal siber güvenliğin sağlanması için elzemdir.

Savunmada kalmanın ulusal güvenliği sağlayacağı düşüncesinin sorunlu olduğu, Maginot Hattı üzerinden verilecek bir örnekle belirtilebilir. Bilindiği üzere 19. Yüzyılda gerçekleşen Alman-Fransız rekabeti, Almanya'nın lehine sonuçlanmıştır. I. Dünya Savaşı'nda da Almanya, Fransa için büyük bir tehdit olmuştur. Bu sebeple I. Dünya Savaşı sonrasında Fransa, Almanya'ya karşı kendisini koruyacağına inandığı bir savunma hattı inşa etmeye başlamıştır. Dönemin Fransa Savunma bakanının adıyla anılan Maginot Hattı'nın hem Almanya'ya karşı caydırıcı olacağına hem de yeni bir Alman saldırısına karşı aşılmaz bir set çekeceğine inanılmıştır. Ancak 1940'ta Maginot Hattı, Alman saldırılarına karşı başarısız olarak sabit istihkama dayalı bir savunma düşüncesinin işe yaramayacağını kanıtlamıştır [39]. Bu örnek siber uzay üzerinden yeniden yorumlanırsa, Birleşik Krallık'ın ulusal siber güvenlik duvarlarını tahkim ederek güvende kalması mümkün değildir. Nasıl Alman zırhlıları farklı stratejiler ve hattın zayıf noktalarını değerlendirerek Maginot'u aştılarsa, ulusal savunmayı sağlayacak siber stratejinin de yalnızca savunmada kalarak bunu mümkün kılması olası değildir. Tarihsel tecrübe dikkate alındığında, güvenliğin savunma ve saldırı unsurlarının bir arada kullanılmasıyla sağlanabileceği ileri sürülebilir.

Ayrıca şu husus belirtilmelidir ki uluslararası hukuk öğretileri dikkate alındığında, belirli koşulların karşılanması koşuluyla, ulusların bir siber saldırının failine karşı savunma ve saldırı temelinde gerçekleştirebilecekleri eylemler bulunmaktadır [40]. BM Hükümet Uzmanları Grubu'nun 2013'te mevcut uluslararası hukukun aynı zamanda devletlerin siber faaliyetlerine yönelik olarak uygulanmasını onaylamasına ek olarak, 2015'te BM Uzman Grubu, BM Şartı'nın bütünüyle siber uzaya uygulandığını kabul etmiştir. Buna bağlı olarak silahlı saldırı eşiğini aşan bir siber operasyona yanıt olarak saldırıya uğrayan devletin meşru müdafaa yönünde hareket etme hakkının geçerliliği de kabul edilmiştir [41]. İşte bu noktada Birleşik Krallık'ın 2019'da kurduğu 6. Tümen, istihbarat, siber ve elektronik savaşta uzmanlaşmış tugayları da bünyesinde bulundurmaktadır. Konvansiyonel olmayan yöntemlerin de içeren yöntemlerle savaşabilecek şekilde oluşturulan bu tümen, Birleşik Krallık'ın gelecek dönemde çıkabilecek savaşlara ilişkin öngörüsünün de bir sonucu olarak değerlendirilebilir [42].

Siber güvenliğe yönelik alınan tehditlerde, silahlı kuvvetlere de ayrı bir yer açılması elzemdir. Silahlı kuvvetlerin bilgi ve iletişim teknolojisine artan ihtiyacı, silahlı kuvvetlerce kullanılan sistemlerin bir siber saldırıya maruz kalmasını mümkün kılmaktadır. Böyle bir saldırı sonucunda silahların çalışma yeteneklerinin büyük bir şekilde tehlikeye girebileceği dikkate alınmalıdır. Bu bağlamda siber tehdidin hızla değişen doğası, Birleşik Krallık Savunma Bakanlığı'nın siber güvenlik temelinde araştırma ve geliştirmeye önem vermesini zorunlu hale getirmektedir [43] ki siber savaş, aynı zamanda askeri teçhizat üreten büyük savunma şirketleri için de cazip bir alan haline gelmiştir [27].

İşe yarar olup olmayacağı kesin olmamakla birlikte, Birleşik Krallık'ın olası bir savaş durumunda kullanılmak üzere siber silahlar geliştirdiği bilinmektedir [6]. Devletler nasıl silahlarını test etmek için tatbikat yapıyorsa, siber uzayda da durum görece benzerdir. Devlet güdümlü[12] bir zararlı yazılım olduğuna inanılan "NotPenya" ile ağırlıklı olarak Ukrayna üzerinde bir siber silahın etkilerinin test edildiği ileri sürülebilir [16].

Siber operasyonlar, devletlerin güç projeksiyonunu ortaya koyabilmeleri[13] açısından giderek daha önemli hale gelmektedir. Birleşik Krallık, düşman devlet aktörlerine, teröristlere ve ciddi örgütlü suçlulara karşı saldırı operasyonları yürütme hedeflerine yardımcı olmak için 2020'de Ulusal Siber Güç'ü[14] oluşturmuştur. Ulusal Siber Güç, aynı zamanda Birleşik Krallık'ın düşmanlarını tespit etmesine, onlara zarar vermesine ve en nihayetinde siber uzayda caydırıcı olmasına destek olma potansiyeline sahiptir [45]. Ulusal Siber Güç, Birleşik Krallık ve müttefiklerinin güvenliklerini siber uzayda sağlamakla yükümlüdür. Bu kurumu farklı kılan savunma ve istihbarat alanında faaliyet gösteren personellerin uzmanlık ve kaynaklarını tek bir yapı altında birleştirmesinin yanında, Birleşik Krallık dış politikasına bağlı olarak siber uzayda operasyon düzenleme yetki ve kabiliyetine sahip olmasıdır. Diğer bir ifadeyle Ulusal Siber Güç siber savunmanın yanında devlet, terör ve suç örgütlerine yönelik olarak siber saldırı düzenlemekle yetkilendirilmiştir [33]. Ayrıca şu husus belirtilmelidir ki Ulusal Siber Güç'ün

[12] Rusya.

[13] Bilindiği üzere görece az sayıda devletin sahip olduğu uçak gemileri, bir güç projeksiyonu aracı olarak ön plana çıkmaktadır. Hemen hemen dünyadaki tüm devletlere saldırabilme imkanını sağlaması, uçak gemilerini güç projeksiyonu olarak ön plana çıkaran hususların başında gelmektedir [44]. Benzer bir bakış açısı siber yetkinlikler üzerinden kurgulanırsa, siber uzay dünyanın tamamına yönelik saldırı düzenleyebilmeyi mümkün kıldığı için güç projeksiyonu için önemli bir araç olarak değerlendirilebilir.

[14] National Cyber Force (NCF).

oluşturulmasında Rusya'dan alınan tehdit en önemli güdüleyici sebeplerden biri olarak öne plana çıkmıştır [45].

Birleşik Krallık Hükümet İletişimleri Başkanlığı, Rusya'yı siber uzayda etkili olabilecek operasyonları yürütme konusunda kapasitesi olan ve oldukça yetenekli bir siber aktör olarak değerlendirmektedir. Rusya'nın demokratik seçim sonuçlarını etkileme çabasının yanında, aralarında Birleşik Krallık'ın da olduğu devletlerin kritik altyapı unsurlarına saldırı düzenlemesi, kamu kurumlarına siber saldırıda bulunması ve organize suç örgütleriyle iş birliği kurarak siber alanda diğer aktörlere zarar verme girişimleri, Birleşik Krallık'ın Rusya'yı ulusal güvenliği için tehdit olarak görmesine neden olmuştur [46].

Rusya'nın yanında teknik anlamda kat ettiği gelişme ve sahip olduğu siber güvenlik gücüne bağlı olarak, Çin'in Birleşik Krallık için en büyük tehdit unsuru olması öngörülmektedir. Görece daha basit yöntemlerle siber saldırılarda bulunmakla birlikte, İran'ın da çeşitli casusluk ve yıkıcı siber yetenekleriyle, Birleşik Krallık tarafından saldırgan bir siber aktör olarak değerlendirildiği not edilmelidir. Diğer taraftan Birleşik Krallık'ın Kuzey Kore'yi, Rusya, Çin ve İran kadar gelişmiş siber imkanlara sahip olmasa da siber uzayda yetenekli bir aktör olarak görmeye devam ettiği belirtilmelidir [47]. Birleşik Krallık siber uzayda belirli yeteneklere sahip olan bu aktörlere karşı caydırıcı olmalıdır. Aynı zamanda devlet destekli saldırılara karşı da caydırıcı olmalı ve bu alanda caydırıcılığını görünür kılmalıdır.[15]

Libicki, siber saldırıyı gerçekleştiren bir aktörün kendisine yapılacak misillemelerin büyüklüğü noktasında öngörü sahibi olmaması durumunda, misillemenin etkilerini abartma ya da küçümseme yoluna gidilebileceğini ileri sürmektedir. Diğer bir ifadeyle, büyüklüğü bilinmeyen veya öngörülemeyen bir tehditle karşı karşıya kalmaları durumunda aktörler, kötümser olup durumu olduğundan kötü bir yere konumlandırabilir veya iyimser bir yaklaşımla tehdidi küçümseyebilirler. Libicki'ye göre istisnaları olsa da büyüklüğü ve etkisi daha öngörülebilir olan bir misilleme, öngörülemeyen bir misillemeden daha fazla caydırıcı olacaktır [49]. Goodman da benzer bir şekilde aktörlerin siber caydırıcılık mesajlarını görünür kılmamalarının siber saldırıların yaygınlaşmasına etki ettiğine değinmiştir [50]. Bu noktada Birleşik Krallık'ın siber güç unsurlarını siber caydırıcılığı sağlayabilmek için görünür kılması ayrıca önemli hale gelmektedir.

Suz Tzu'nun "Savaş Sanatı" isimli eserinde ifade ettiği "güçlüyken onlardan sakın" ifadesi [51], realist temelde caydırıcı olmanın önemini ortaya koyar. Birleşik Krallık siber alanda caydırıcı olmasına rağmen, bir saldırıyla karşılaşması durumunda ise yapılan saldırıya misliyle karşılık vererek caydırıcılığını korumalıdır. Yine realist bir temelde bakılırsa, Machiavelli'nin devletin başındaki liderlerin hem kendilerinin hem de devletlerinin bekasını sağlamak için başvuracakları bütün araçları doğru ve övgüye değer olarak değerlendirdiği [52] dikkate alındığında, Birleşik Krallık'ın da kendisine karşı gerçekleştirilen siber saldırılara karşılık verebileceği araçlar arasında ahlakiliği devre dışı bırakma eğiliminde olması, bir gereklilik olarak düşünülebilir.

Caydırıcılık, düşmana yapmayı planladığı saldırı sonucunda ortaya çıkacak yüksek maliyetin gösterilmesi ve düşmanın henüz başlatmadığı saldırıdan vazgeçirilmesini ifade etmektedir. Caydırıcılıkta dikkat edilmesi gereken temel husus, düşmana yapacağı saldırının sonucunda elde edeceği faydanın, zarardan daha az olacağının açıkça hissettirilmesidir. Bu noktada düşman, muhtemel saldırısı öncesinde uyarılmalıdır. Düşman buna rağmen saldırı yapması durumunda bedel ödeyeceğini bilmeli ve bu yetkinliğe sahip olduğunuza inanmalıdır. Düşman yapacağı fayda/zarar hesabına rağmen bir saldırı düzenlemesi durumunda ise cezalandırılmalıdır [39]. Birleşik Krallık'ın siber yetkinlikleri üzerinden oluşturduğu caydırıcılığa rağmen bir saldırıya uğraması durumunda cezalandırma mekanizmasının işletilebilmesi,[16] siber saldırı yeteneklerinin önemini ortaya çıkarmaktadır.

McKenzie'nin ABD'nin siber caydırıcılığına yönelik ifade ettiği hususların Birleşik Krallık için de geçerli olduğu ileri sürülebilir. McKenzie'ye göre ABD'nin siber caydırıcılığının inandırıcı olması için ortaya koyulan ceza tehdidinin muhatap aktörde karşılık bulması gerekmektedir. Düşman aktörün ceza tedbirlerinden korkarak saldırı düzenlemekten vazgeçtiği bir durum yaratılması için cezalandırma

[15] Diğer aktörlerin davranışlarını etkilemeye dönük olarak kullanılmayan unsurların güç olarak nitelendirilemeyeceğine yönelik düşünce [48] dikkate alınırsa caydırıcılığın görünür kılınması gücün kullanılması olarak da düşünülebilir.

[16] Siber uzayda cezalandırma mekanizması işletilirken şu husus unutulmamalıdır ki siber silahlar, nükleer silahlar veya diğer konvansiyonel silahlar kadar şiddetli bir tahribat yaratamayabilir. Yapılacak bir siber saldırıda kritik altyapı unsurları hedef alınması durumunda bile nükleer silahların kullanımındaki gibi yıkıcı bir etki öngörülemez. Bu anlamda siber saldırıların/misillemenin büyüklüğü ve kapasitesinin görece sınırlı olacağı [53] dikkate alınmalıdır.

mekanizmasının işetilmesinde istekli olunması önem arz etmektedir. Uygulanabilir bir caydırıcılık stratejisi üzerinden kurgulanan caydırıcılık, saldırgan bir yöne sahip olarak bir tür misillemeyi içerir. Bu misilleme siber uzayda olabileceği gibi orantılılık esasına dayanarak saldırıyı düzenleyen aktöre karşı siyasi ve ekonomik eylemlerde bulunulmasıyla [54] da desteklenebilir. Bu noktada siber caydırıcılığın bir tür misilleme üzerinden yalnızca siber uzayda verilmesi zorunlu değildir. Sahip olunan diğer güç unsurları üzerinden ve yapılan saldırıyla orantılı olarak caydırıcılığın sağlanması da ihtimal dahilindedir.

Nye'a göre siber uzayda cezalandırma hem devletlere hem de suça dahil olan aktörlere yönelik olarak mümkün olmakla birlikte, siber uzayda caydırıcılığın gerçek anlamda işe yarayıp yaramayacağı sorusunun cevabı bazı değişkenlere bağlı olarak farklılaşabilir. Diğer taraftan tüm siber saldırılar eşit öneme sahip olmadıkları için ulusal güvenlik üzerinde bir tehdit olarak değerlendirilmez. Bu sebeple bu tür düşük düzeyli saldırılara karşı caydırıcılık kullanılamayacağı için politikacıların önemli saldırılara odaklanması gerekir [55].

Devletlerin dışında, devlet destekli olmayan siber terörizm de Birleşik Krallık için önemli bulunmuş ve ciddiye alınarak güvenlikleştirilmiştir. Teröristler fiziki zarar verebilecekleri terör eylemlerine öncelik vermekle birlikte, Birleşik Krallık'a karşı zarar verici siber faaliyetler yürütmeyi de hedeflemektedirler.[17] Bu saldırılar, devlet olarak Birleşik Krallık için büyük bir tehdit potansiyeline sahip olmasa da düşük kapasiteli siber saldırıların etkisi orantısız derecede yüksek olmaktadır. Örneğin hacklenen kişisel bilgilerin çevrimiçi olarak yayınlanması, medyanın ilgisini çektiği için halkın korkutulmasını da beraberinde getirmektedir. Bahsi geçen orantısız etki dikkate alındığında, terör örgütlerinin siber kapasitelerindeki görece küçük bir artış bile Birleşik Krallık ve onun çıkarları için ciddi bir tehdit oluşturabilir [30].

ABD'nin Ulusal Güvenlik Ajansı[18] siber casusluk konusunda ilk sırada yer alsa [57] da Birleşik Krallık'ın son dönemde Hükümet İletişim Merkezi ile Ulusal Güvenlik Ajansı'na yakın bir kapasiteye ulaştığı düşünülmektedir. Özellikle 2009 sonrasında Birleşik Krallık'ın siber güvenlik alanında yaptığı yatırımlar ve konuya verdiği önemin bunda etkili olduğu söylenebilir.

Ortaya koyulan çabaya bağlı olarak Birleşik Krallık, siber güvenlik yatırımlarının sonuçlarını almaya başlamıştır. Birleşmiş Milletler Uluslararası Telekomünikasyon Birliği'nin (ITU), 2018'de yayınladığı Küresel Siber Güvenlik Endeksi'ne göre Birleşik Krallık, siber güvenlik temelinde yapılan bir sıralamada ilk sırada [58] (ITU, 2019: 62), ITU'nun 2020 yılı Küresel Siber Güvenlik Endeksi'ne göre ise ABD'nin hemen ardından ikinci sırada yer almaktadır [59] (ITU, 2021: 25). Bu noktada Birleşik Krallık'ın yapması gereken siber güvenlikteki sahip olduğu öncü rolü, dünyadaki konumunun temel bir parçası haline getirmektir [60] (Prince & Sullivan, 2019: 17). Siber uzayda kazandığı yeteneklere rağmen Birleşik Krallık'ın küresel bir tehditle yalnız başa çıkması mümkün değildir. Bu noktada tercih edilecek en rasyonel yol, ulusal siber gücün arttırılmasının yanında dost ve müttefik aktörlerle iş birliği yapmaktır.

Romalı tarihçi Tacitus'un devletler kendilerini ilgilendiren bir tehlikeye karşı birleşmek yerine bu tehlikeyle teker teker mücadele eder ve mağlup olurlar yönündeki düşüncesi [61], siber uzayda karşılaşılan tehdide karşılık devletlerin realist temelde kendi kapasitelerini geliştirme çabaları ve bunun sonucunda yaşanabilecek başarısızlık üzerinden uyum içerisindedir. Diğer bir ifadeyle realizmin ön gördüğü self help (kendi kendine yardım) kavramı, siber uzayda aktörler açısından geçerliğini korumakla birlikte, başarılı olmak için iş birliğinin sağlanması gerekmektedir.

Bu yönüyle düşünüldüğünde siber güvenliğin sağlanabilmesi için yalnızca yurt içinde siber güvenliğe ilişkin savunma imkanlarının geliştirilmesi yeterli olmayacaktır. Çünkü yapısı gereği internetin ulusötesi olması, devletlerin karşılaşacağı tehditlerin kaynağını da sınır ötesine taşımaktadır. Bu noktada Birleşik Krallık'ın siber alanda ihtiyaç duyduğu güvenliği tek başına sağlayamayacağı dikkate alınarak, diğer ülkelerle ortaklıkların yapılması elzemdir [17] (Cabinet Office, 2011: 22). Siber uzayda uluslararası iş birliğini mümkün kılmak önemli ve gereklidir. 2016 ve 2019 yılları arasında Birleşik Krallık'ta başbakanlık görevinde bulunan Theresa May de organize suçlara karşı güçlü ortaklıklar kurulmasını gerekli görmektedir. May'e göre terörle mücadele nasıl yalnızca ülke sınırları içerisinde ortaya koyulan çabayla sona erdirilemez ve hükümetler arası bir stratejiye ihtiyaç duyarsa, burada da benzer bir durum bulunmaktadır [62]. Bu

[17] Siber terörizm her ne kadar bombalı bir terör eyleminin ve bu eylemdeki can kaybının medyaya yansıyan görsel etkisine sahip olmasa da bir ülkenin önemli ağlarına yapılacak saldırılarla kaosa sebebiyet verebilirler. Teröristlerin temel amaçları arasında yer alan hükümetin halkını koruyamadığı algısının [56] siber saldırılar üzerinden verilebileceği dikkate alındığında terörizm temelinde siber güvenliğin önemi daha iyi anlaşılacaktır.

[18] National Security Agency (NSA).

farkındalığa sahip olan Birleşik Krallık, siber suçlar başta olmak üzere siber alanda operasyonlar, politika, araştırma, bilgi paylaşımı ve askeri iş birliğini de kapsayan çok sayıda siber paylaşım anlaşması imzalamıştır [63]. Tüm bunlar dikkate alındığında, Birleşik Krallık siber konularda ikili ilişkilere ve çok taraflılığa değer veren bir ülke olarak değerlendirilebilir.

Birleşik Krallık istihbarat ve siber güvenlik alanında, ABD'nin önemli bir müttefiki olarak ön plana çıkmaktadır [64]. Birleşik Krallık ve ABD'nin 4 Ekim 2019'da imzaladıkları antlaşma, tarafların iletişim hizmeti sağlayıcılarından ciddi suçların önlenmesi, tespiti, soruşturulması veya kovuşturulmasına ilişkin elektronik verileri yapılan anlaşmaya uygun bir şekilde elde edebilmesini mümkün kılması [65], siber alanda yakın ilişkilerin önemli göstergelerinden birisidir.

Siber güvenlik ve çok taraflılık üzerinden ifade edilmesi gereken bir diğer konu, Birleşik Krallık, ABD, Kanada, Avustralya ve Yeni Zelanda'nın dahil olduğu önemli ve gelişmiş bir istihbarat sistemi olan Echelon'dur. Echelon'un küresel internet ve iletişimi denetleme, ilgili istihbarat servislerini uyarma ve elde ettiği bilgileri/verileri arşivleme yeteneklerine sahip olduğu [66-67] dikkate alındığında, siber uzayda kolektif bir yaklaşım sergilemenin önemi yeniden hatırlanacaktır.

Birleşik Krallık'ın daha güçlü kolektif eylem için NATO ittifakının siber güvenlik yeteneklerinin geliştirilmesini desteklemeye devam edeceğini beyan etmesi [33] de önemsenmelidir. Siber uzayı operasyonel bir alan haline getirme yönünde bir irade ortaya koyan Birleşik Krallık'ın kendi geliştirdiği modellerin nasıl çalıştığını ve askeri operasyonlarının bir parçası olarak siber etkileri nasıl kullanmayı planladığını NATO ile paylaşması önemlidir. Birleşik Krallık'ın bu noktada istekli ve gönüllü bir tavır ortaya koyması da ayrıca kıymetlidir [16] Son olarak Birleşik Krallık aynı zamanda Küresel Dijital Erişim Programı kapsamında 10 milyon Pound'luk bir yardım ile şimdiye kadarki en büyük denizaşırı siber kapasite geliştirme projesini gerçekleştirmiştir. Bu kapsamda Brezilya, Nijerya, Güney Afrika, Kenya ve Endonezya'da çok sayıda projeye destek verilmiştir [68].

5. TARTIŞMA ve SONUÇ *(DISCUSSION and CONCLUSION)*

1980'li yıllarda siber uzayı güvenlikleştirmesi gerektiğini kavrayan Birleşik Krallık, sonrasındaki süreçte siber uzaydaki konumunu güven altına almayı, ulusal güvenliği sağlamanın ön koşulu olarak değerlendirmiş ve bu konuyu fazlasıyla önemsemiştir. Siber uzayda karşı karşıya kalınan tehditlerin çeşitlenmesine bağlı olarak siber güvenlik yatırımlarını arttıran Birleşik Krallık lider aktörlerden biri haline gelmiştir. Siber güvenlik stratejileri özelinde analiz edildiğinde, Birleşik Krallık bu stratejileri ortaya koyma noktasında görece geç kalmış olsa da siber uzaya gereken önemi vermiştir.

Siber güvenlik stratejilerinin açıklanmasına paralel olarak siber güvenlikte kurumsallaşma da hızlanmıştır. Hükümet İletişim Merkezi halen Birleşik Krallık'ın siber güvenliğini sağlayan ana çatı olmakla birlikte, farklı birimler arasındaki iletişim ve uyumu mümkün kılan mekanizmaların oluşturulması, siber güvenlik ve caydırıcılığın sağlanması için rasyonel bir politika olarak değerlendirilebilir. Birleşik Krallık'ta silahlı kuvvetlerin de siber uzayda yaşanan gelişmeleri dikkate alarak savunma ve saldırı yetenekleri üzerinden kendisini yeniden yapılandırdığı not edilirse, siber uzayda Birleşik Krallık'ın daha etkili bir siber güç olmasının da önü açılmıştır.

Makalede üzerinde durulduğu üzere, aktif siber savunmanın işlevsel olarak siber güvenlik stratejisine katkı sunduğu görülse de Birleşik Krallık'ın yalnızca ulusal siber güvenlik duvarlarını tahkim ederek güvende kalması mümkün değildir. Bunun farkında olan Birleşik Krallık, elektronik savaş yöntemleri ve siber uzayda operasyon düzenleme kabiliyetine sahip olmayı önemsemektedir. Devlet, devlet destekli, terör ve suç örgütlerine yönelik siber uzayda caydırıcı olunabilmesi için siber savaş ve siber saldırı yetkinliklerinin geliştirilmeye devam edilmesi hayati öneme sahiptir. Birleşik Krallık'ın siber yetkinlikleri üzerinden oluşturduğu caydırıcılığa rağmen bir saldırıya uğraması durumunda, saldırıyı düzenleyen aktör Çin ve Rusya gibi siber kabiliyetleri yüksek olan aktörler bile olsa, cezalandırma mekanizmasının işletilebilmesi yeni saldırılara karşı güvende olabilmek için elzemdir. Diğer bir ifadeyle siber operasyonlar, devletlerin güç projeksiyonunu ortaya koyabilecekleri bir alan olarak değerlendirildiğinde, Birleşik Krallık'ın geliştirmiş olduğu yetkinliklerini gerçekleştireceği siber operasyonlarla görünür kılması gerekmektedir. Kısaca Birleşik Krallık'ın siber güvenliğini yalnızca savunmada kalarak elde etmesi mümkün olmadığı için siber caydırıcılık ve saldırı kapasitesini realist temelde arttırması mühimdir. Burada bir hususun ayrıca açıklanması gerekir ki caydırıcı ve saldırı potansiyeli yüksek olan bir siber güç oluşturabilmek için iş birliği imkanları önemsenmeli ve aşağıda açıklanacak saldırgan realizm ile karıştırılmamalıdır.

Saldırgan realizmin hegemonya hedefine ulaşabilmesi için peşinden gittiği daha fazla güce sahip olma dürtüsü, diğer aktörler tarafından istenmeyeceği için hegemon olma yolundaki aktörün gücünün dengelenmesini beraberinde getirebilir. Diğer taraftan savunmacı realistler, hegemonyaya sahip olma çabasını stratejik bir hata olarak nitelemekte ve gücü maksimize etmek yerine yeterince güce sahip olmayı gerekli görmektedirler [69]. Bu noktada gücü bir araç olmaktansa amaç olarak düşünmek,[19] iş birliği imkanını dost ve müttefik aktörler için bile sınırlandırmanın ötesinde sorunlu hale getirmektedir. Ayrıca siber uzayın anarşik yapısı da self help düşüncesi üzerinden işbirliği imkanlarını sıklıkla gereksiz kılmaktadır. İşte bu noktada makalede Tacitus'a atıfla ifade edilen ortak tehdide karşı teker teker mücadele edilip birlikte mağlup olunmasına yönelik düşünce dikkate alındığında, Birleşik Krallık'ın gücü bir amaç olmaktansa araç haline getirerek müttefikleriyle iş birliği imkanlarını dışarıda bırakmaması önem arz etmektedir.

KAYNAKLAR *(REFERENCES)*

[1] Cabinet Office. (2009). *Cyber security strategy of the United Kingdom. safety, security and resilience in cyber space*. London: The Stationery Office.

[2] Applegate, S. (2015). Cyber conflict: disruption and exploitation in the digital age. Frederic Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations Policy, Strategy, and Practice*. Palgrave Macmillan, 19-36.

[3] Sweetman, A. (2022). *Cyber and the city securing London's banks in the computer age*. Springer.

[4] Buzan, B. (2008). Askeri güvenliğin değişen gündemi. *Uluslararası İlişkiler*, *5*(18), 107-123.

[5] Ning, H. (2022). *A brief history of cyberspace*. CRC Press.

[6] Corera, G. (2015). *Intercept: the secret history of computers and spies*. London: Weidenfeld & Nicolson.

[7] Computer Misuse Act 1990. (1990). https://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf

[8] Healey, J. (2013). A brief history of US cyber conflict. Jason Healey (Ed.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 14-87.

[9] HM Government. (2010). *A strong Britain in an age of uncertainty: the national security strategy.* London: The Stationery Office.

[10] Hjortdal, M. (2011). China's use of cyber warfare: espionage meets strategic deterrence. *Journal of Strategic Security*, *4*(2), 1–24.

[11] Keane, J. (1998). *Şiddetin uzun yüzyılı*, Bülent Peker (Çev.), Ankara: Dost Kitabevi.

[12] Viotti, P. R., Kauppi, M. V., (2016). *Uluslararası ilişkiler teorisi*, (Metin Aksoy, Çev. Ed.), Ankara: Nobel.

[13] Vasquez, J. A. (2015). *Savaş bulmacası,* Haluk Özdemir (Çev.), Uluslararası İlişkiler Kütüphanesi.

[14] Tumkevič, A. (2018). Uncertain security community: building Western cyber-security order. *Journal of Information Warfare, 17*(1), 74–86.

[15] Rid, T. (2013). Cyberwar and peace: hacking can reduce real-world violence. *Foreign Affairs, 92*(6), 77–87.

[16] Shea, J. (2017). How is NATO meeting the challenge of cyberspace? *PRISM*, *7*(2), 18–29.

[17] Cabinet Office. (2011). The UK cyber security strategy: protecting and promoting the UK in a digital world. https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf

[18] National Audit Office. (2013). *The UK cyber security strategy: Landscape review*. London: The Stationery Office.

[19] Tinker, J. A. (2015). Güvenlik revizyonu. Ken Booth & Steve Smith (Ed.), *Uluslararası İlişkiler Kuramları*, Muhammed Aydın (Çev.), Uluslararası İlişkiler Kütüphanesi. 175-197.

[20] Keshavarz, A. (2017). Stuxnet. Paul J. Springer (Ed.), *Encyclopedia of Cyber Warfare*. ABC-CLIO, 279-282.

[21] Umbach, F. (2012). Critical energy infrastructure and risk of cyber attack. Konrad Adenauer stiftung-international reports, 35-66.

[19] Güç "*bir şeylerin olmasını sağlamak için diğerlerinin davranışlarını etkileme becerisine sahip olma*" [70] anlamında değerlendirilirse burada önemli olan en güçlü olmak değil muhatap aktörün davranışını etkileyebilme yeteneğidir.

[22] Stoddart, K. (2016). Live free or die hard: U.S.-UK cybersecurity policies. *Political Science Quarterly*, *131*(4), 803–842.

[23] Osborne, G. (2015). Chancellor's speech to GCHQ on cyber security. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

[24] Richards, J. (2014). *Cyber-war: the anatomy of the global security threat*. Palgrave Macmillan.

[25] Home Office. (2010). *Cyber crime strategy*. London: The Stationery Office.

[26] Lucas, E. (2019). The spycraft revolution. *Foreign Policy*, *232*, 20–27.

[27] Singer, P. W. & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. Oxford: Oxford University Press.

[28] Steed, D. (2019). *The politics and technology of cyberspace*. Routledge.

[29] Cabinet Office. (2016). The UK cyber security strategy 2011-2016 annual report. https://assets.publishing.service.gov.uk/media/5a81bae5e5274a2e8ab558ca/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

[30] HM Government. (2016). National cyber security strategy 2016-2021. https://data.parliament.uk/DepositedPapers/Files/DEP2016-0790/National_Cyber_Security_Strategy_v20.pdf

[31] Cornish, P., Hughes, R., Livingstone, D. (2009). *Cyberspace and the national security of the United Kingdom: threats and responses*. Chatham House.

[32] Montasari, R. (2023). *Countering cyberterrorism the confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity.* Springer.

[33] HM Government. (2021). National cyber strategy 2022 pioneering a cyber future with the whole of the UK. https://assets.publishing.service.gov.uk/media/620131fdd3bf7f78e469ce00/national-cyber-strategy-amend.pdf

[34] Stevens, T., O'Brien, K., Overill, R., Wilkinson, B., Pildegovičs, T., Hill, S. (2019). *UK active cyber defence a public good for the private sector*. King's College London.

[35] House of Commons Committee of Public Accounts. (2019). Cyber security in the UK ninety-ninth report of session 2017–19. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf

[36] HM Government. (2022a). Government cyber security strategy building a cyber resilient public sector 2022-2030. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

[37] Oxford Economics. (2014). Cyber-attacks: effects on UK companies July 2014.

[38] Harrop, W & Matteson, A. (2015). Cyber resilience: a review of critical national ınfrastructure and cyber-security protection measures applied in the UK and USA. Frederic Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations Policy, Strategy, and Practice*. Palgrave Macmillan, 149-166.

[39] Roskin, M. G., Berry, N. O. (2014). *Uluslararası ilişkiler: ui'nin yeni dünyası*. Özlem Şimşek (Çev.), Ankara: Adres Yayınları.

[40] Kramer, F. D., & Butler, R. J. (2019). *Cybersecurity: changing the model,* Atlantic Council.

[41] Wright, J. (2018). Cyber and international law in the 21st century. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[42] Elefteriu, G. (2020). United Kingdom: thinly global. G. J. Schmitt (Ed.), *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners.* Strategic Studies Institute, US Army War College, 359–390.

[43] House of Commons Defence Committee. (2013). *Defence and cyber-security sixth report of session 2012–13*. London: The Stationery Office Limited.

[44] Goldstein, J. S., Pevehouse, J. C. (2017). *Uluslararası ilişkiler*, Haluk Özdemir (Çev.), Ankara: BB101 Yayınları.

[45] Devanny, J., Dwyer, A., Ertan, A., & Stevens, T. (2021). *The national cyber force that Britain needs?*. King's College London.

[46] Intelligence and Security Committee of Parliament. (2020). Russia. https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf

[47] The National Cyber Security Centre. (2022). Annual review 2022 making the UK the safest place to live and work online.

https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf

[48] Özdemir, H. (2008). Uluslararası ilişkilerde güç: çok boyutlu bir değerlendirme. *Ankara Üniversitesi SBF Dergisi, 63*(03), 113-144.

[49] Libicki, M. C. (2018). Expectations of cyber deterrence. *Strategic Studies Quarterly*, *12*(4), 44–57.

[50] Goodman, W. (2010). Cyber deterrence: tougher in theory than in practice?. *Strategic Studies Quarterly*, *4*(3), 102–135.

[51] Tzu, S. (2014). *Savaş sanatı*. Hasan İlhan (Çev.), Ankara: Alter Yayıncılık.

[52] Machiavelli, N. (1999). *Hükümdar*. Selahattin Bağdatlı (Çev.), İstanbul: Der Yayınları.

[53] Chen, J. (2017). Cyber Deterrence by Engagement and Surprise. *PRISM*, *7*(2), 100–107.

[54] McKenzie, T. M. (2017). *Is cyber deterrence possible*? Air University Press.

[55] Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71.

[56] Viotti, P. R., Kauppi, M. V., (2014). *Uluslararası ilişkiler ve dünya siyaseti*. Ayşe Özbay Erozan, (Çev.), Ankara: Nobel.

[57] Aid, M. M. (2013). Espionage moves into the cyber age: the National Security Agency's shift to cyber espionage. R. Huisken, O. Cable, D. Ball, A. Milner, R. Sukma, & Y. Wanandi (Ed.), *CSCAP Regional Security Outlook 2014*, 24–27.

[58] ITU. (2019). Global cybersecurity index (GCI) 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[59] ITU. (2021). Global cybersecurity index 2020. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[60] Prince, C., & Sullivan, J. (2019). *The UK cyber strategy: challenges for the next phase*. Royal United Services Institute.

[61] Erkul, İ. Ç. (2021). *Commonwealth'i anlamak: beşikten mezara Britanya İmparatorluğu*. Konya: Çizgi Kitabevi.

[62] HM Government. (2013). *Serious and organised crime strategy.* London: The Stationery Office.

[63] Hitchens, T., & Goren, N. (2017). International cybersecurity information sharing agreements. Center for International & Security Studies, U. Maryland.

[64] Billon-Galland, A. (2019). *UK defence policy and Brexit: time to rethink London's European strategy*. European Defence Policy Brief, European Leadership Network.

[65] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on access to electronic data for the purpose of countering serious crime. (2019). https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019

[66] Bayraktar, G. (2015). *Siber savaş ve ulusal güvenlik stratejisi*. Yeni Yüzyıl Yayınları.

[67] Akkuş, B. (2017). *Özgürlük ve güven(siz)lik ikileminde siber uzay : yeni dünya için bir toplum sözleşmesi denemesi*. Milenyum Yayınları.

[68] HM Government. (2022b). UK government's global digital access programme (DAP) -Pillar 2 Trust & Resilience project summaries. https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2022/12/fcdo-dap.pdf

[69] Mearsheimer, J. J. (2016). Yapısal realiizm. Tim Dunne, Milja Kurki, Steve Smith (ed), *Uluslararası ilişkiler teorileri disiplin ve çeşitlilik*, Özge Kelekçi (Çev.), Sakarya: Sakarya Üniversitesi Kültür Yayınları, 86-106.

[70] Nye, J. S. (2005). *Dünya siyasetinde başarının yolu yumuşak güç*. Rayhan İnan Aydın (Çev.), Ankara: Elips Kitap.

Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Araştırma Makalesi / Research Article

Blok Zincir Teknolojisine Akademik Yönden Ne Kadar Hazırız: Türkiye Adresli Blok Zincir Konusundaki Uluslararası Yayınların Analizi ve Alanın Gelişimine Yönelik Öneriler

Serkan ALICI[*,a], Muhammet DAMAR[*,a], Yılmaz GÖKŞEN[*,a]

[a*] *Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, İZMİR, TÜRKİYE*
[b] *Dokuz Eylül Üniversitesi, Rektörlük, İZMİR, TÜRKİYE*
[c] *Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, İZMİR, TÜRKİYE*

MAKALE BİLGİSİ

Alınma: 15.05.2024
Kabul: 24.06.2024

Anahtar Kelimeler:
Blok Zincir, Türkiye, Makine Öğrenmesi, Metin Madenciliği, Tedarik Zinciri, Bibliyometrik

Sorumlu Yazar
e-posta:
serkan.alici@deu.edu.tr

ÖZET

Blok zincir kavramı, ilk olarak 2008 yılında Satoshi Nakamoto tarafından Bitcoin'in temel teknolojisi olarak tanıtılmıştır. Blok zinciri teknolojisi günümüzde pek çok alanda kullanılmaya başlamıştır. Araştırmamızda, Web of Science (WoS) üzerindeki yayınların bibiyometrik analizi ortaya konulmaktadır. Türkiye 330 doküman ile dünyada 18.sırada yer almıştır. Yayınların h-indeks değeri 39, ortalama atıf değeri 15,25, alınan toplam atıf değeri 5.034 ve yıllık makale artış oranı %37.64 olduğu görülmüştür. İlk sıradaki Çin, ABDnin iki katından fazla alanda yayın üretmiştir. Hindistan'ın ilgili alanda bilimsel üretkenlik açısından ABD'ye çok yakın olması, Suudi Arabistan ve Pakistan gibi ülkelerin ilgili konuda dünyada ilk onda yer almıştır. Blok zincir konusunda, 5G, teknoloji yönetim olgusu, bilgi güvenliği, sistem performansı, nesnelerin interneti, endüstri 4.0, büyük veri ve bulut teknolojisi gibi entegre sistemler, bilişim sistemi mimarisi, mahremiyet, akıllı kontratlar, islami finans, sürdürülebilirlik, akıllı araçlar, öne çıkan başlıklardır. İlgili teknoloji dijitalleşme veya dijital dönüşüm altında farklı sektörlerdeki firmalar için mahremiyet konusunda çözüm olarak sunulmaktadır. Genelde sağlık sektörü veri mahremiyetinin önem kazandığı benzer sektörlerde blok zincir Türkiye'de yoğun ilgi görmüştür.
DOI: 10.59940/jismar.1483935

How Academically Ready are We for Blockchain Technology: Analysis of International Publications on Blockchain in Türkiye and Recommendations for the Development of the Field

ARTICLE INFO

Received: 15.05.2024
Accepted: 24.06.2024

Keywords:
Blockchain, Türkiye, Machine Learning, Text Mining, Supply Chain, Bibliometrics

Corresponding Authors
e-mail:
serkan.alici@deu.edu.tr

ABSTRACT

The concept of blockchain was initially introduced by Satoshi Nakamoto in 2008 as the fundamental technology behind Bitcoin. Blockchain technology has begun to be used in many fields today. Our research presents a bibliometric analysis of publications indexed in the Web of Science (WoS). Turkey ranks 18th globally with 330 documents. The publications have an h-index of 39, an average citation rate of 15.25, total citations received amounting to 5,034, and an annual article growth rate of 37.64%. China, leading in the first place, has produced more publications than twice the number of the United States in the field. India's scientific productivity in this area is comparable to that of the United States, while countries such as Saudi Arabia and Pakistan are also among the top ten worldwide. In the field of blockchain, integrated systems such as 5G, technology management phenomena, information security, system performance, Internet of Things, Industry 4.0, big data, and cloud technology are prominent topics. Blockchain technology is presented as a solution for privacy concerns under digitalization or digital transformation for various sectors. Particularly in sectors where data privacy is crucial, such as healthcare, blockchain has garnered significant interest in Turkey.
DOI: 10.59940/jismar.1483935

1. GİRİŞ *(INTRODUCTION)*

Nakamoto tarafından yazılan Bitcoin makalesinde, blok zinciri terimi ilk kez kullanılmış ve bu teknoloji, Bitcoin'in işlem kayıtlarını güvenli bir şekilde depolamak ve doğrulamak için kullanılan bir dağıtık defter olarak tanımlanmıştır [1]. Blok zinciri teknolojisi, merkezi olmayan ve güvenli yapısıyla tanınan kripto paraların temelindeki teknoloji olarak hizmet etmektedir [2]. Bitcoin ve Ethereum gibi kripto paralar katılımcılar arasında güveni garanti ederek, uçtan uca işlemleri kolaylaştırmak için blok zinciri teknolojisini kullanır [3]. Blok zinciri tabanlı dijital paralarda kriptografik tekniklerin kullanılması işlemlerin güvenliğini ve bütünlüğünü sağlar [4]. Kripto paraların ortaya çıkması tüketicilerin bu dijital varlıkları anlama ve kabul etme eğilimlerini anlamak için ilgi uyandırmaktadır [5]. Blok zinciri şeffaflığı gibi faktörler kullanıcılar arasında güven oluşturmada kilit bir rol oynamakta ve kripto paraların benimsenmesini etkilemektedir [6]. Ayrıca, blok zinciri teknolojisinin merkezi olmayan yönetim ve geliştirilmiş güvenlik gibi potansiyel avantajları, kripto paraların olumlu algısına katkıda bulunmaktadır [7].

Blok zinciri teknolojisinin tanımı konusunda literatürde farklı yorumlar bulunmakla birlikte Butijn ve diğerleri [8], genellikle bir ağda uçtan uca dağıtılmış kullanıcılara güven veren merkezi olmayan bir ekonomiyi güçlendiren bir teknoloji olarak tanımlanmaktadır [9]. Teknoloji gelişmeye devam ettikçe yapı, zorluklar ve çeşitlilikleri anlamak, yeteneklerini kapsamlı bir şekilde kavramak için hayati öneme sahiptir [10].

Blok zinciri, dağıtık bir defter teknolojisi olarak hizmet vermekte olup merkezi olmayan bir şekilde veri bütünlüğünü sağlayan açık bir genel defterdir [11]. Bu teknoloji değişmezliği, şeffaflığı ve anonimliği ile diğer dağıtık defter teknolojilerinden ayrılmaktadır [12]. Blok zincir, ardışık kriptografik blokların bir zincirini oluşturan ve bu blokların tüm blok zinciri sistemi üzerine yayılması şeklinde tasarlanmıştır [13]. Blok zincir, işlemleri merkezi olmayan bir uçtan uca (peer-to-peer) ağda, yani düğümler olarak bilinen bir dizi bilgisayarda paylaşılan bir defter olarak saklanmakta ve işlenmektedir [14].

Blok zincirinin pek çok alanda potansiyeli ve etkisi ortadadır ve bunlar arasında tedarik zinciri yönetimini devrim niteliğinde değiştirmesi, sağlık sektöründe güvenliği artırması ve denetim süreçlerini iyileştirmesi yer almaktadır [15-17]. Teknolojinin veri bütünlüğünü sağlama, yolsuzluğu önleme ve işlemleri kolaylaştırma yeteneği, farklı endüstrilerde değerli bir varlık haline getirmektedir [18]. Ayrıca blok zincirinin merkezi olmayan doğası ve değiştirilemezliği sağlık kayıtları ve finansal işlemler gibi hassas bilgilerin depolanması ve paylaşılması için güvenli bir platform sağlamaktadır [19].

Blok zincir teknolojisi çeşitli endüstrileri devrim niteliğinde dönüştürebilecek potansiyele sahip bir yenilik olarak ortaya çıkmıştır. Blok zincirinin merkezi olmayan, değiştirilemez ve şeffaf yapısı, imkanlarını geniş kapsamda keşfetmeyi ve yaygın olarak benimsemeyi sağlamıştır. Üretim, eğitim, tarım, finans, sağlık hizmetleri gibi sektörlerde kullanımı ve araştırılması giderek artmaktadır [20-25]. Blok zincirinin merkezi olmayan doğası, üçüncü taraflara olan bağımlılığı azaltırken şeffaflığı ve güvenliği artırmaktadır [26]. Elektronik oy sistemleri bağlamında blok zinciri doğruluğu ve güvenliği sağlayarak kullanıcılar arasında güven oluşturmak için büyük öneme sahiptir [27]. Sağlık alanında blok zinciri veri kökenini, şeffaflığı ve değiştirilemezliği sağlayarak klinik deneyleri ve sağlık kayıtlarını yönetmede kuruluşlara destek sağlar [28-30]. Gıda ve içecek endüstrisi blok zincirinin şeffaflığından faydalanarak çevresel ve sosyal sorumluluk hedeflerine ulaşmada yardımcı olmaktadır [31]. Tüm bu ihtiyaçlar sektörde insan kaynağından beklenen gereksinimlerin çeşitlenmesine de sebep olmaktadır [32].

Blok zincir teknolojisi, muhasebe, denetim ve tedarik zinciri yönetimi gibi çeşitli alanları, işlem maliyetlerini değiştirerek, firma sınırlarını etkileyerek ve akıllı sözleşmelerin yürütülmesini sağlayarak dönüştürme potansiyeline sahiptir [33-35]. Merkezi olmama ve şeffaflık özelliklerinin etkisiyle muhasebe alanı üzerinde önemli etkileri olması beklenmektedir [34-35]. Ayrıca blok zincir sigorta dahil olmak üzere farklı sektörlere önemli faydalar getirebilecek çığır açan bir teknoloji olarak kabul edilmektedir [36].

Blok zincir teknolojisi Türkiye'deki çeşitli sektörlerde artan ilgi ve araştırma dikkatine sahip olmuştur. Erol ve diğerleri [37] tarafından yapılan çalışmada lojistik, tedarik zinciri, sağlık, enerji, finans, otomotiv, ilaç ve tarım gibi Türk endüstrilerinde blok zinciri teknolojisinin uygulanabilirliğini bir karar destek yöntemi kullanarak değerlendirmiştir. Araştırmada Türkiye'de blok zinciri teknolojisinin benimsenmesi için en uygun sektörün finans sektörü olduğu belirtilmiştir. Ayrıca Gulen ve Karaagac [38] Türkiye'deki tarımsal gıda tedarik zincirinde blok zinciri teknolojisinin uygulanmasına yönelik bir proje

önermiş ve başarılı bir uygulama için kamu ve özel sektörler arasındaki iş birliğinin önemini vurgulamıştır. Kahraman [39] çalışmasında finans sektöründe blok zinciri teknolojisinin Türkiye'deki finansal görünümü etkileme potansiyelinin yüksek olduğunu belirtmiştir. Türkiye'nin dijital çağı benimsemesiyle kripto paraların ve yeniliklerinin küresel ekonomiyi ve Türkiye'deki finans sektörünü nasıl etkileyebileceğinin önemli potansiyelini vurgulamıştır. Ozturan ve diğerleri [40] tarafından yapılan çalışmada Türk bankacılık sektöründe blok zinciri teknolojisinin benimsenme hazırlığını değerlendirmiş ve Türkiye'deki bankaların çoğunluğunun blok zinciri teknolojisini benimseme sürecinin başlangıç aşamasında olduğu sonucuna varmıştır. Ayrıca Bowden ve Baral [41] çalışmalarında Türkiye de dahil olmak üzere gelişmekte olan pazarlarda faaliyet gösteren tedarik zincirlerinde blok zinciri uygulamalarını araştırmıştır. Teknoloji-organizasyon-çevre çerçevesini kullanarak çalışma İngiltere ve Türkiye'den uzmanların görüşlerini incelemiş ve Türkiye'deki tedarik zinciri operasyonlarında blok zinciri teknolojisine artan ilgiyi belirtmiştir. Özetle tüm bu çalışmalar Türkiye'de blok zinciri benimseme için hazırlık ve potansiyel sektörler konusunda değerli görüşler sağlamakta ve endüstriye özgü zorluklar, teknolojik yetenekler ve kurumsal hazırlık gibi çeşitli faktörleri dikkate almanın önemini vurgulamaktadır.

Bu çalışmada blok zincir kapsamında Web of Science (WoS) üzerindeki Türkiye adresli yayınlarının makine öğrenmesi tekniği olan Latent Dirichlet Allocation (LDA) Gizli Dirichlet Ayrımı ve bibliyometrik analizi ortaya konulmuştur. WoS, çeşitli disiplinlerdeki bilimsel makaleler, konferans bildirileri ve diğer akademik materyallerden oluşan geniş bir koleksiyona erişim sağlayan, yaygın olarak kullanılan bir araştırma veri tabanı ve atıf indeksidir. Clarivate Analytics (eskiden Thomson Reuters'in bir parçasıydı) tarafından sürdürülmekte olup akademik araştırmalar için en kapsamlı ve prestijli kaynaklardan biri olarak kabul edilmektedir. WoS, araştırmacılar, bilim insanları, kütüphaneciler ve akademik kurumlar tarafından literatür taraması, bibliyometrik analiz ve kendi alanlarındaki en son gelişmelerden haberdar olmak için yaygın olarak kullanılmaktadır. Atıf analizi için gelişmiş arama yetenekleri ve araçları sağlar. Bu da onu bilimsel iletişim ve araştırma değerlendirmesi için değerli bir kaynak haline getirir.

Literatürde blok zincir konusunda Türkiye'nin üretkenliğini WoS kaynaklarında ölçmek amacıyla bu çalışma gerçekleştirilmiştir. Çalışmanın bu yönüyle gelişmekte olan Blok zincir teknolojisine yönelik Türkiye'nin durumunun ortaya konmasında, çok güncel bir teknoloji olan blok zincir konusunda sektörde ve akademide daha iyisi için yapılabilecekleri ortaya koyacağı ve bu sayede özellikle Türkçe literatüre katkı sağlayacağı düşünülmektedir.

2. YÖNTEM *(METHOD)*

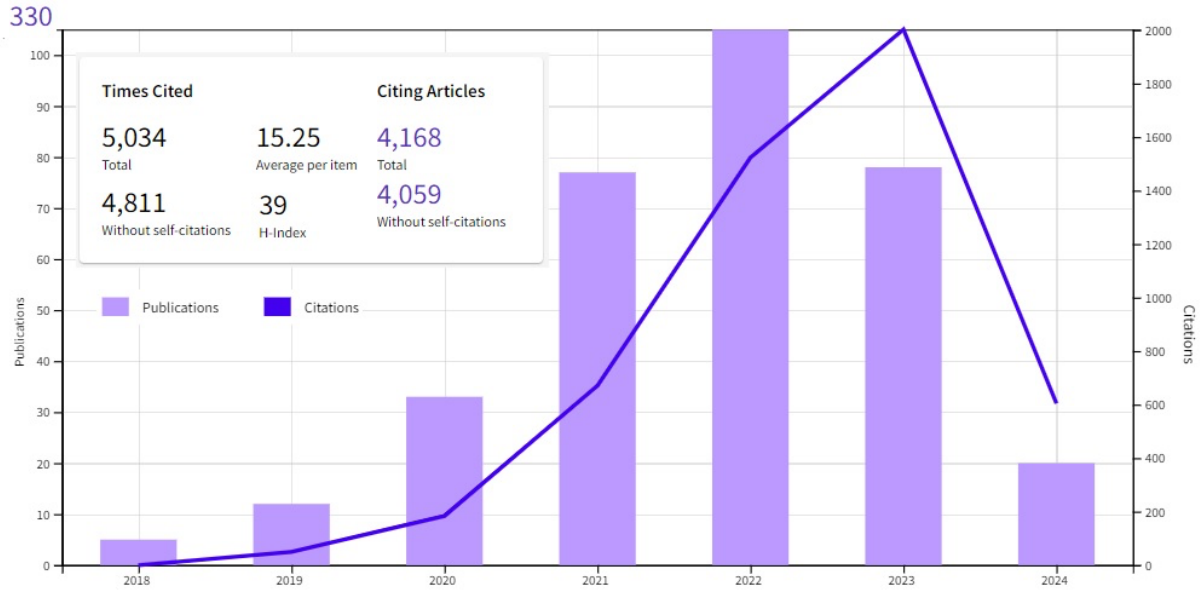
WoS üzerinde blok zincir, İngilizce "blockchain*" veya "block-chain*" veya "block chain*" sözcükleri ile arama gerçekleştirilerek 29.972 dokümana erişilmiştir. İlgili arama araştırmacı anahtar kelimeleri ve araştırma başlıkları üzerinden gerçekleştirilmiştir. Türkiye fitresi ile elde edilen son veri setinde 330 araştırma makalesi ve derleme makalesi bibliyometrik yöntemler ile analiz edilmiştir. Veriler 04/04/2024 tarihinde elde edilmiştir. İlgili veri WoS Core Collection üzerinden elde edilmiştir. Elde edilen veri formatımız plainText ve Excel formatı olmak üzere iki formda olmuştur.

Analizler için kullanılan araçlarımız sırasıyla WoS Raporlama Sayfası, InCites Rapor Sayfası, R Bibliometrix Paketi Biblioshiny kütüphanesi, LDA Analizi için Pyton Scikit-learn kütüphanesi, VosViewer paket programı, Microsoft Excel programı, Oracle Database ve SQL Sorgu dili şeklindedir. Analiz sürecinde kullanılan teknikler ise ortak yazarlık analizi, ortak anahtar kelime kullanımı analizi, atıf ve ortak atıf analizi, tematik harita analizi, doküman analizi ve LDA konu modelleme analizi, şeklindedir.

Literatürde belirli bir araştırma alanında sistematik bir değerlendirme ortaya koymak ve geleneksel literatür analizi için kapsamlı ve ilgili bilgileri elde edebilmek için var olan araştırmaların miktarı zorluk teşkil etmektedir. Bibliyometrik yöntemler aracılığı ile belirli bir alandaki araştırma çıktıları hakkında pek çok bilgiye sahip olunabilmekte, LDA yöntemi ile de konu modellemesi gerçekleştirilebilmekte, yüksek içerikli metin belgeleri organize edilebilmekte ve özetlenebilmektedir.

3. BULGULAR *(FINDINGS)*

Literatürdeki ilk makale 2018 yılında yayınlanmış ve ilgili yılda toplamda beş makalenin yayınlanmış olduğu görülmüştür. Ardından 2019 yılında 12, 2020 yılında 33, 2021 yılında 77, 2022 yılında 105, 2023 yılında 78 ve içinde bulunduğumuz yılda ise şimdiye kadar 20 makalenin yayınlanmış olduğu görülmüştür (Şekil 1).



Şekil 1. Türkiye Adresli Blok Zincir Makalelerin Yıllara Göre Üretkenliği

(*Productivity of Türkiye Addressed Blockchain Articles by Years)*

İlgili konuda Türkiye adresli araştırmaların en yoğun olduğu yıl 105 makale ile 2022 yılı olmuştur. Yayınların indekslerine göre dağılımı değerlendirildiğinde, Science Citation Index Expanded (SCI-Expanded) (f:13.638, 45.50%), Emerging Sources Citation Index (ESCI) (f:4.020,13.41%), Social Sciences Citation Index (SSCI) (f:3.186, 10.63%), ve Arts & Humanities Citation Index (A&HCI) (f:79, 0.26%), şeklinde olduğu görülmüştür.

Türkiye adresli ilgili yayınların h-indeks değeri ise 39'dur. Ortalama atıf değeri 15,25 ve alınan toplam atıf değeri ise 5.034'dür. İlgili konuda üretilen dokümanların yıllık büyüme oranının %37.64 olduğu görülmüştür. 330 araştırmanın %51.22'sinin açık erişim olduğu fakat ilgili yayınların sadece %19.1'inin desteklendiği görülmüştür. İlgili konuda en fazla destek olan kurumların sırasıyla, Türkiye Bilimsel Ve Teknolojik Araştırma Kurumu (TÜBİTAK) (f:16, 4.84%), Avrupa Birliği (AB) (f:3, %0.90), Çin 3 Ulusal Doğal Bilimler Vakfı (NSFC) (f:3, %0.90), Şangay Doğa Bilimleri Vakfı (f:2, 0.60%), Galatasaray Üniversitesi Bilimsel Araştırma Projeleri Komisyonu (f:2, 0.60%), olduğu görülmüştür.

İlgili araştırmalardın en yoğun ilişkilendirildiği sürdürülebilirlik hedeflerinin (Bahsedilen WoS tarafından yayınların ilişkilendirildiği sürdürülebilirlik hedefleridir.) ise yoğunluk sırasına göre şu şekilde olduğu görülmüştür: Sürdürülebilir şehirler ve topluluklar (f:21, %6.36), endüstri inovasyonu ve altyapı (f:14, %4.24), uygun fiyatlı ve temiz enerji (f:8, %2.42), sağlık ve refah (f:6, %1.81), kaliteli eğitim (f:6, %1.81), sorumlu tüketim ve üretim (f:5, %1.51), insana yakışır iş ve ekonomik büyüme (f:3, %0.90), sıfır açlık (f:1, %0.30), eşitsizliğin azaltılması (f:1, %0.30), barış ve adalet güçlü kurumlar (f:1, %0.30).

3.1. Araştırmacı, Kurum ve Ülke Analizleri

(Researcher, Institution and Country Analyzes)

Bu bölümde incelemeye konu olan araştırma makalesi sayısı (f:17.386, 58.00%) ve derleme türündeki makale sayısı (f:1.347, 4.49%), olmak üzere toplamda 18,733 dokümandır. İlgili konuda ülkelere göre bir sıralama yaptığımızda ilk on sırada Çin (f:6.626, 35.37%), Amerika Birleşik Devletleri (ABD) (f:2.611, 13.93%), Hindistan (f:2.596, 13.85%), İngiltere (f:1.403, 7.48%), Avustralya (f:1.144, 6.10%), Sudi Arabistan (f:1.122, 5.98%), Güney Kore (f:1.041, 5.55%), Kanada (f:857, 4.57%), İtalya (f:747, 3.98%), ve Pakistan (f:617, 3.29%), bulunmaktadır. Türkiye ise blok zincir konusunda 330 makale ile 18. sırada yer alıştır. 330 makale toplamda 856 farklı araştırmacı tarafından üretilmiştir ve aşağıda blok zincir konusundaki en üretken araştırmacılar Tablo 1 üzerinde listelenmektedir.

Tablo 1. Türkiye Adresli Blok Zincir Araştırmalarını En azla Üreten Yazarlar (Minimum 4)
(Authors Who Produced the Most Blockchain Research from Türkiye (Min 4))

Sıra	Araştırmacı	N	%	Sıra	Araştırmacı	N	%
1	Al-Turjman, Fadi	14	4.24	15	Onen, Ahmet	4	1.21
2	Erol, Ismail	9	2.72	16	Zengin, Ahmet	4	1.21
3	Peker, iskender	7	2.12	17	Uludag, Suleyman	4	1.21
4	Akhter, A. F. M. Suaib	7	2.12	18	Anwar, Adnan	4	1.21
5	Heidari, Arash	7	2.12	19	Pathan, Al-Sakib Khan	4	1.21
6	Jafari Navimipour, Nima	7	2.12	20	Ahmed, Mohiuddin	4	1.21
7	Ar, Ilker Murat	7	2.12	21	Shah, A. F. M. Shahen	4	1.21
8	Mostarda, leonardo	6	1.81	22	Cali, Umit	4	1.21
9	Sonmez, Rifat	5	1.51	23	Kazancoglu, Yigit	4	1.21
10	Karakus, Murat	5	1.51	24	Medeni, ihsan tolga	4	1.21
11	Ahmadisheykhsarmast, Salar	5	1.51	25	Rajasekaran, Arun Sekar	4	1.21
12	Ozkasap, Oznur	5	1.51	26	Guler, Evrim	4	1.21
13	Searcy, Cory	5	1.51	27	Ünal, Mehmet	4	1.21
14	Kayikci, Yasanur	5	1.51	28	Souri, Alireza	4	1.21

Yayınlar 527 farklı kurum ve 61 farklı ülke işbirliği ile gerçekleştirilmiştir. İlgili alanda en üretken ilk beş kurum sırasıyla; Yakın Doğu Üniversitesi (f:25, 7.57%), Ankara Yıldırım Beyazıt Üniversitesi (f:15 4.54%), Ankara Üniversitesi (f:14, 4.24%), Yıldız Teknik Üniversitesi (f:13, 3.93%), Orta Doğu Teknik Üniversitesi (f:12, 3.63%), şeklindedir. Tablo 2 üzerinde Türkiye adresli en üretken kurumların listesi verilmiştir.

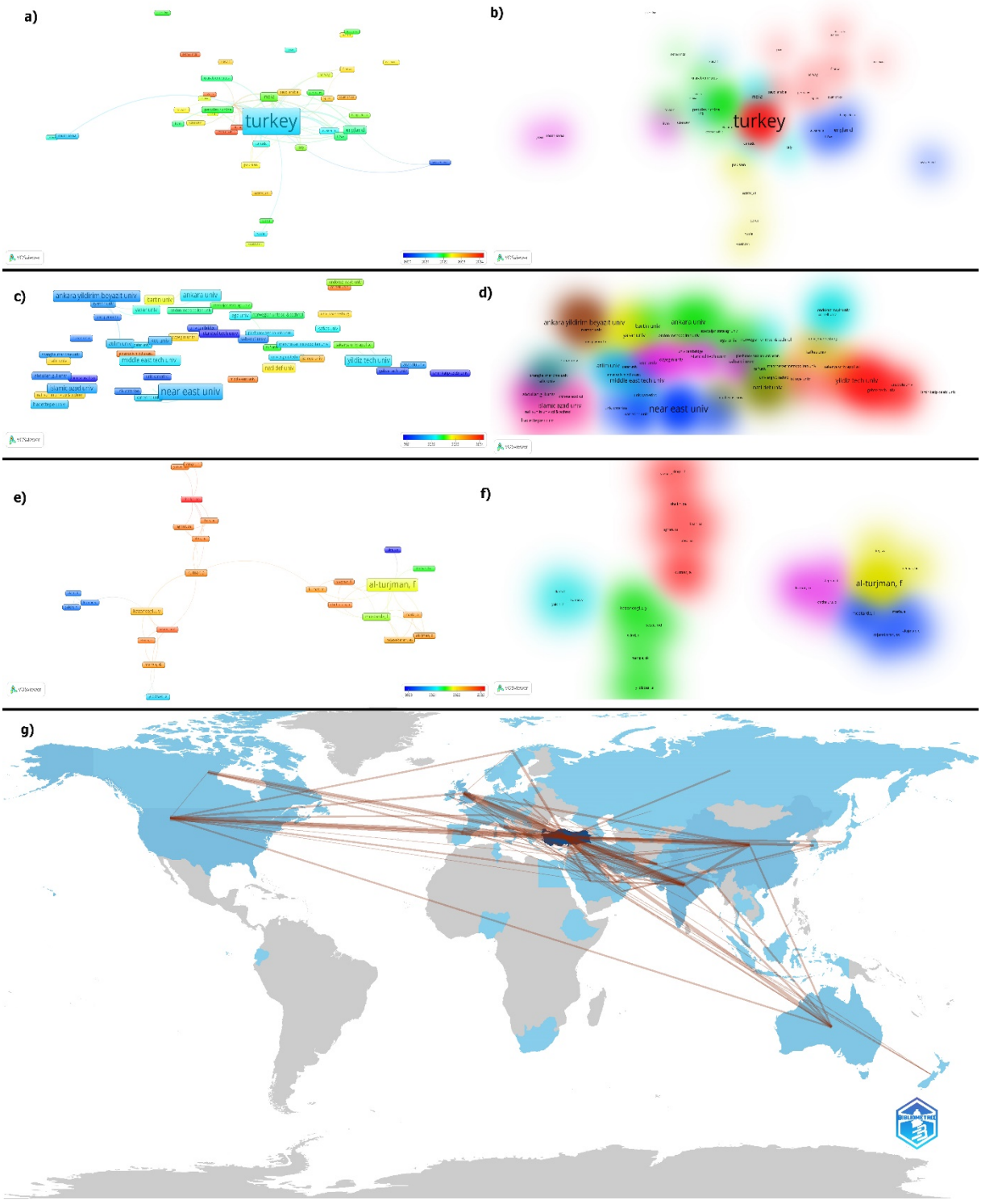
Tablo 2. Blok Zincir Konusunda Alanda En Üretken Kurumlar (Minimum 5)
(Most Productive Institutions in the Field on Blockchain (Min 5))

Sıra	Üniversite	N	%	Sıra	Üniversite	N	%
1	Yakın Doğu Üniversitesi	25	7.57	22	Abdullah Gül Üniversitesi	6	1.81
2	Ankara Yıldırım Beyazıt Üniversitesi	15	4.54	23	Altınbaş Üniversitesi	6	1.81
3	Ankara Üniversitesi	14	4.24	24	Uluslararası Kıbrıs Üniversitesi	6	1.81
4	Yıldız Teknik Üniversitesi	13	3.93	25	Haliç Üniversitesi	6	1.81
5	Orta Doğu Teknik Üniversitesi	12	3.63	26	Nişantaşı Üniversitesi	6	1.81
6	Boğaziçi Üniversitesi	11	3.33	27	Özyeğin Üniversitesi	6	1.81
7	İslami Azad Üniversitesi	11	3.33	28	Camerino Üniversitesi	6	1.81
8	Bartın Üniversitesi	9	2.72	29	Celal Bayar Üniversitesi	5	1.51
9	Kadir Has Üniversitesi	9	2.72	30	Deakin Üniversitesi	5	1.51
10	Ulusal Savunma Üniversitesi	9	2.72	31	Dokuz Eylül Üniversitesi	5	1.51
11	Sakarya Üniversitesi	9	2.72	32	Edith Cowan Üniversitesi	5	1.51
12	Atılım Üniversitesi	8	2.42	33	Gebze Teknik Üniversitesi	5	1.51
13	Bahçeşehir Üniversitesi	8	2.42	34	İstinye Üniversitesi	5	1.51
14	Gazi Üniversitesi	8	2.42	35	Kafkas Üniversitesi	5	1.51
15	Hacettepe Üniversitesi	8	2.42	36	Lübnan Amerikan Üniversitesi	5	1.51
16	Koç Üniversitesi	8	2.42	37	Norveç Bilim Teknoloji Üniversitesi (NTNU)	5	1.51
17	Yaşar Üniversitesi	8	2.42	38	Sakarya Uygulamalı Bilimler Üniversitesi	5	1.51
18	Ege Üniversitesi	7	2.12	39	Toronto Metropolitan Üniversitesi	5	1.51
19	Gümüşhane Üniversitesi	7	2.12	40	Türk Alman Üniversitesi	5	1.51
20	İstanbul Teknik Üniversitesi	7	2.12	41	Univ Kyrenya	5	1.51
21	Sabancı Üniversitesi	7	2.12	42	Waterloo Üniversitesi	5	1.51

İlgili dokümanlarda tek yazarlı doküman sayısı 36 ve uluslararası ortak yazarlık işbirliği değeri %45.15 olduğu görülmüştür. Aşağıda Şekil 2 üzerinde ortak yazarlık gösterimi sunulmuştur.

Türkiye sırasıyla Tayvan, İspanya, Almanya, Birleşik Arap Emirlikleri, Fransa, Malezya ve Japonya'nın artından 330 makale ile 18. sırada yer almıştır. Ardından Singapur ve Rusya gelmiştir. En yoğun

işbirliği yapılan ülkeler ise yoğunluk sırasına göre; Hindistan (f:37), İngiltere (f:35), ABD (f:29), Çin (f:17), Kanada (f:14), İran (f:14), Avustralya (f:14), Pakistan (f:13), Birleşik Arap Emirlikleri (f:12), İtalya (f:11), Suudi Arabistan (f:11), Tayvan (f:11), Fransa (f:8), Güney Kore (f:8), Bangladeş (f:6), Irak (f:6), Norveç (f:6), Almanya (f:5), Lübnan (f:5), İspanya (f:5), şeklindedir.



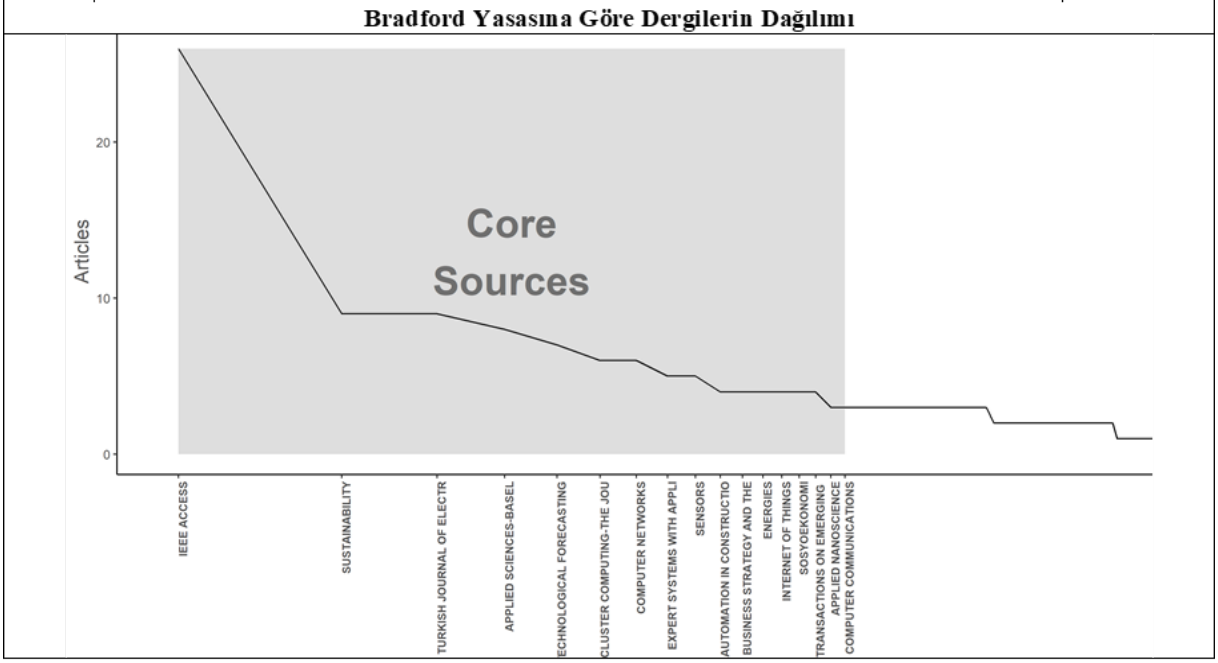
Şekil 2. Araştırmacıların Yazarlar, Kurumlar ve Ülkelere Göre Ortak Yazarlık Analizi

(*Researchers' Co-Authorship Analysis by Authors, Institutions and Countries)*

3.2. Yayın Yapılan Dergi, Referans ve Atıf Analizleri *(Published Journal, Reference and Citation Analyzes)*

330 araştırma makalesi ve derleme makalesinin 186 farklı dergide basıldığı ve 330 eserde toplamda 16.499 esere atıf verildiği, ilgili yayınların toplamda 5.034 atıf aldığı ve makale başına düşen ortalama atıf değerinin 15.25 olduğu görülmüştür. Aşağıda sırasıyla yayın yapılan dergilerin Bradford yasasına göre dağılımı (Şekil 3), blok zincir konusunda Türkiye adresli en fazla atıf alan makaleler (Tablo 3) ve en yoğun yayınlandığı yirmi dergi (Tablo 4) sırasıyla verilmektedir.

Sıra	Dergi İsmi	Zone
1	IEEE Access	Zone 1
2	Sustainability	Zone 1
3	Turkish Journal of Electrical Engineering and Computer Sciences	Zone 1
4	Applied Sciences-Basel	Zone 1
5	Technological Forecasting and Social Change	Zone 1
6	Cluster Computing-The Journal of Networks Software Tools and Applications	Zone 1
7	Computer Networks	Zone 1
8	Expert Systems with Applications	Zone 1
9	Sensors	Zone 1
10	Automation in Construction	Zone 1
11	Business Strategy and The Environment	Zone 1
12	Energies	Zone 1
13	Internet of Things	Zone 1
14	Sosyoekonomi	Zone 1
15	Transactions on Emerging Telecommunications Technologies	Zone 1
16	Applied Nanoscience	Zone 1
17	Computer Communications	Zone 1



Şekil 3. Türkiye Adresli Blok Zincir Makalelerin Bradford Yasasına Göre Kümelenmesi
(*Clustering Türkiye-Addressed Blockchain Articles According to Bradford's Law)*

Blok zincir konusunda uluslararası yayın yapan Türkiye adresli araştırmacıların ilgili yayınları yaparken en yoğun faydalandıkları ilk on dergi yoğunluk sırasına göre şu şekildedir: IEEE ACCESS (f:603), Lecture Notes in Computer Science (f:291), Journal of Cleaner Production (f:269), International Journal of Production Research (f:260), Sustainability (f:250), IEEE Internet Things (f:214), International Journal of Information Management (f:196), Future Generation Computer Systems (f:172), Sensors (Basel, Switzerland) (f:158), Computers & Industrial Engineering (f:151). Aşağıda Şekil 4 üzerinde makalelerin referanslarında kullanılan kaynaklar arasında dergi ve birinci yazarlık durumuna göre ön çıkan dergi ve kişiler ve kümelenmeleri gösterilmektedir.

Tablo 3. Blok Zincir Konusunda Türkiye Adresli Makaleler Arasında En Yoğun Atıf Alan Makaleler

(The Most Cited Articles Among Türkiye Addressed Articles on Blockchain)

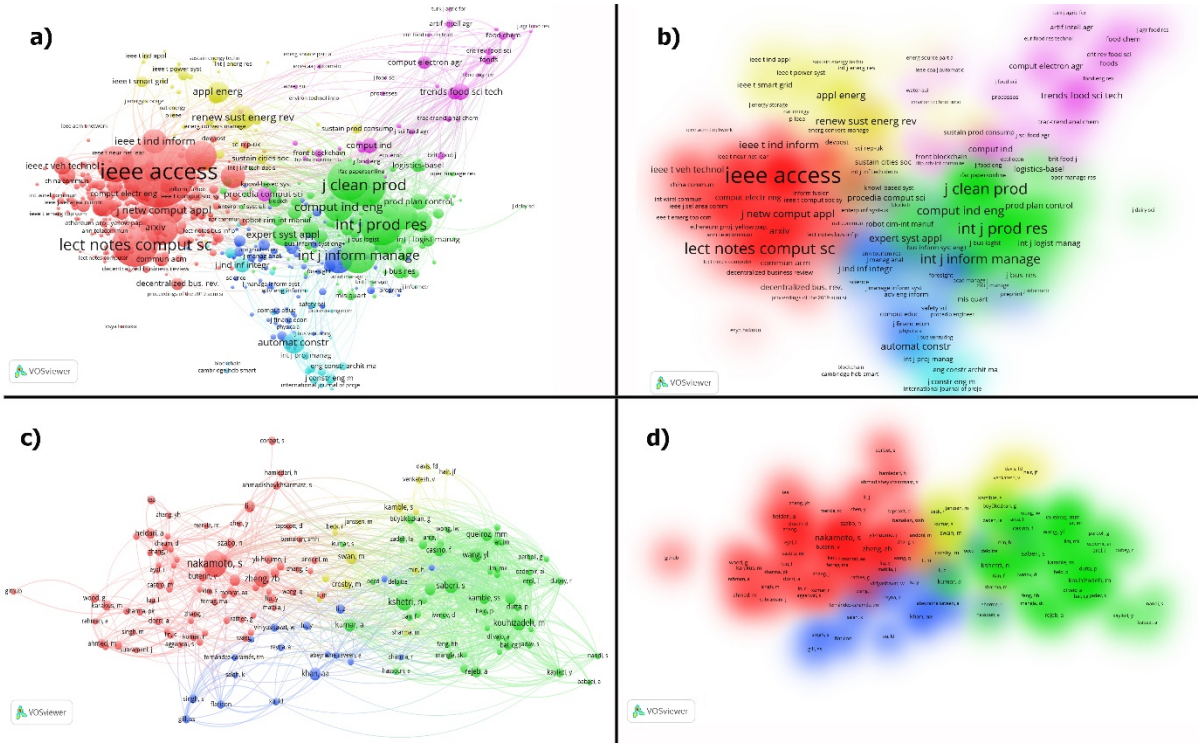
Sıra	Makale Başlığı	Dergi	ESCI/ SCIE	5YDED	Araştırmacı(lar)	Yıl	A
1	Blockchain technology and the circular economy: Implications for sustainability and social responsibility	Journal Of Cleaner Production	SCIE	11.00	Upadhyay, A; Mukhuty, S; (...); Kazancoglu, Y	2021	236
2	Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges	Internet Of Things	SCIE	6.40	Gill, SS; Tuli, S; (...); Garraghan, P	2019	170
3	Food supply chain in the era of Industry 4.0: blockchain technology implementation opportunities and impediments from the perspective of people, process, performance, and technology	Production Planning & Control	SCIE	7.90	Kayikci, Y; Subramanian, N; (...); Bhatia, MS	2022	166
4	Blockchain-Based Securing of Data Exchange in a Power Transmission System Considering Congestion Management and Social Welfare	Sustainability	SCIE	4.00	Dehghani, M; Ghiasi, M; (...); Taghizadeh-Hesary, F	2021	160
5	A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems	IEEE Communications Surveys And Tutorials	SCIE	35.80	Khalilov, MCK and Levi, A	2018	141
6	Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges	IEEE Access	SCIE	4.10	Gupta, R; Tanwar, S; (...); Kim, SW	2020	99
7	A smart contract system for security of payment of construction contracts	Automation In Construction	SCIE	11.40	Ahmadisheykhsarmast, S and Sonmez, R	2020	89
8	Expert oriented approach for analyzing the blockchain adoption barriers in humanitarian supply chain	Technology In Society	SCIE	8.50	Sahebi, IG; Masoomi, B and Ghorbani, S	2020	81
9	A Blockchain-Based Auditable Access Control System for Private Data in Service-Centric IoT Environments	IEEE Transactions On Industrial Informatics	SCIE	11.90	Han, DZ; Zhu, YJ; (...); Li, KC	2022	77
10	Evaluating the feasibility of blockchain in logistics operations: A decision framework	Expert Systems With Applications	SCIE	8.30	Ar, IM; Erol, I; (...); Medeni, IT	2020	77
11	Designing a Blockchain-Based IoT With Ethereum, Swarm, and LoRa The software solution to create high availability with minimal security risks	IEEE Consumer Electronics Magazine	SCIE	4.00	Özyilmaz, KR and Yurdakul, A	2019	77
12	The fourth industrial revolution in the food industry-Part I: Industry 4.0 technologies	Critical Reviews In Food Science And Nutrition	SCIE	11.80	Hassoun, A; Aït-Kaddour, A; (...); Regenstein, J	2023	74
13	Realizing the potential of blockchain technologies in genomics	Genome Research	SCIE	11.80	Ozercan, HI; Ileri, AM; (...); Alkan, C	2018	74
14	Blockchain and renewable energy: Integration challenges in circular economy era	Renewable Energy	SCIE	8.40	Yildizbasi, A	2021	3
15	A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities	Neural Computing & Applications	SCIE	5.6	Ullah, F and Al-Turjman, F	2023	66
16	Forecasting technological positioning through technology knowledge redundancy: Patent citation analysis of IoT, cybersecurity, and Blockchain	Technological Forecasting And Social Change	SCIE	12.00	Daim, T; Lai, KK; (...); Kumar, V	2020	64
17	Peer-to-Peer Energy Trading in Virtual Power Plant Based on Blockchain Smart Contracts	IEEE Access	SCIE	4.10	Seven, S; Yao, G; (...); Muyeen, SM	2020	62
18	CertLedger: A new PKI model with Certificate Transparency based on blockchain	Computers & Security	SCIE	5.7	Kubilay, MY; Kiraz, MS and Mantar, HA	2019	61
19	Using system dynamics to analyze the societal impacts of blockchain technology in milk supply chainsrefer	Transportation Research Part E-Logistics And Transportation Review	SCIE	10.00	Mangla, SK; Kazancoglu, Y; (...); Sezer, MD	2021	60
20	The impact of blockchain related name changes on corporate performance	Journal Of Corporate Finance	SCIE	6.90	Akyildirim, E; Corbet, S; (...); Yarovaya, L	2020	59

5YDED: Beş Yıllık Dergi Etki Değeri, A: Atıf

Tablo 4. Blok Zincir Konusunda Türkiye Adresli Makalelerin En Yoğun Yayınlandığı Yirmi Dergi
(The Twenty Journals Where Articles Addressed to Türkiye on Blockchain are Most Published)

Sıra	**Dergi İsmi**	**5YDED**	**Derginin İlişkilendirildiği Araştırma Alan(lar)ı**	**SCIE/ ESCI**	**OMBDAS**	**HI**	**N**	**%**
1	IEEE Access	4.10	Computer Science, Information Systems; Engineering, Electrical & Electronic; Telecommunications	SCIE	14.58	9	26	7.87
2	Sustainability	4.00	Environmental Sciences; Environmental Studies; Green & Sustainable Science & Technology; Green & Sustainable Science & Technology	SCIE	24.56	5	9	2.72
3	Turkish Journal Of Electrical Engineering And Computer Sciences	1.00	Computer Science, Artificial Intelligence; Engineering, Electrical & Electronic	SCIE	1.00	1	9	2.72
4	Applied Sciences Basel	2.90	Chemistry, Multidisciplinary; Engineering, Multidisciplinary; Materials Science, Multidisciplinary; Physics, Applied	SCIE	11.13	5	8	2.42
5	Technological Forecasting And Social Change	12.00	Business; Regional & Urban Planning	SCIE	19.00	5	7	2.12
6	Cluster Computing The Journal Of Networks Software Tools And Applications	2.60	Computer Science, Information Systems; Computer Science, Theory & Methods	SCIE	4.00	2	6	1.81
7	Computer Networks	4.90	Computer Science, Hardware & Architecture; Computer Science, Information Systems; Engineering, Electrical & Electronic; Telecommunications	SCIE	4.83	3	6	1.81
8	Expert Systems With Applications	8.30	Computer Science, Artificial Intelligence; Engineering, Electrical & Electronic; Operations Research & Management Science	SCIE	28.20	4	5	1.51
9	Sensors	4.10	Chemistry, Analytical; Engineering, Electrical & Electronic; Instruments & Instrumentation	SCIE	11.80	3	5	1.51
10	Automation In Construction	11.40	Construction & Building Technology; Engineering, Civil	SCIE	37.00	4	4	1.21
11	Business Strategy And The Environment	14.30	Business; Environmental Studies; Management	SCIE	22.75	3	4	1.21
12	Energies	3.30	Energy & Fuels	SCIE	3.00	2	4	1.21
13	Internet Of Things	6.40	Computer Science, Information Systems; Engineering, Electrical & Electronic; Telecommunications	SCIE	47.00	3	4	1.21
14	Sosyoekonomi	-	Economics	ESCI	2.50	1	4	1.21
15	Transactions On Emerging Telecommunications Technologies	2.70	Telecommunications	SCIE	19.50	3	4	1.21
16	Applied Nanoscience	4.288	Nanoscience & Nanotechnology	SCIE	20.67	2	3	0.90
17	Computer Communications	4.80	Computer Science, Information Systems; Engineering, Electrical & Electronic; Telecommunications	SCIE	7.67	3	3	0.90
18	Concurrency And Computation Practice Experience	1.70	Computer Science, Software Engineering; Computer Science, Theory & Methods	SCIE	0.33	1	3	0.90
19	Electronics	2.90	Computer Science, Information Systems; Engineering, Electrical & Electronic; Physics, Applied	SCIE	6.67	2	3	0.90
20	Energy Reports	5.6	Energy & Fuels	SCIE	15.33	3	3	0.90

N: Makale Sayısı; HI: H-indeks; 5YDED: Beş Yıllık Dergi Etki Değeri; OMBDAS: Ortalama Makale Başıa Düşen Atıf Sayısı



Şekil 4. Makalelerinin Referanslarında Kullanılan Kaynaklar Arasındaki Dergi ve Birinci Yazarlık Durumuna Göre İş Birliği Ağı

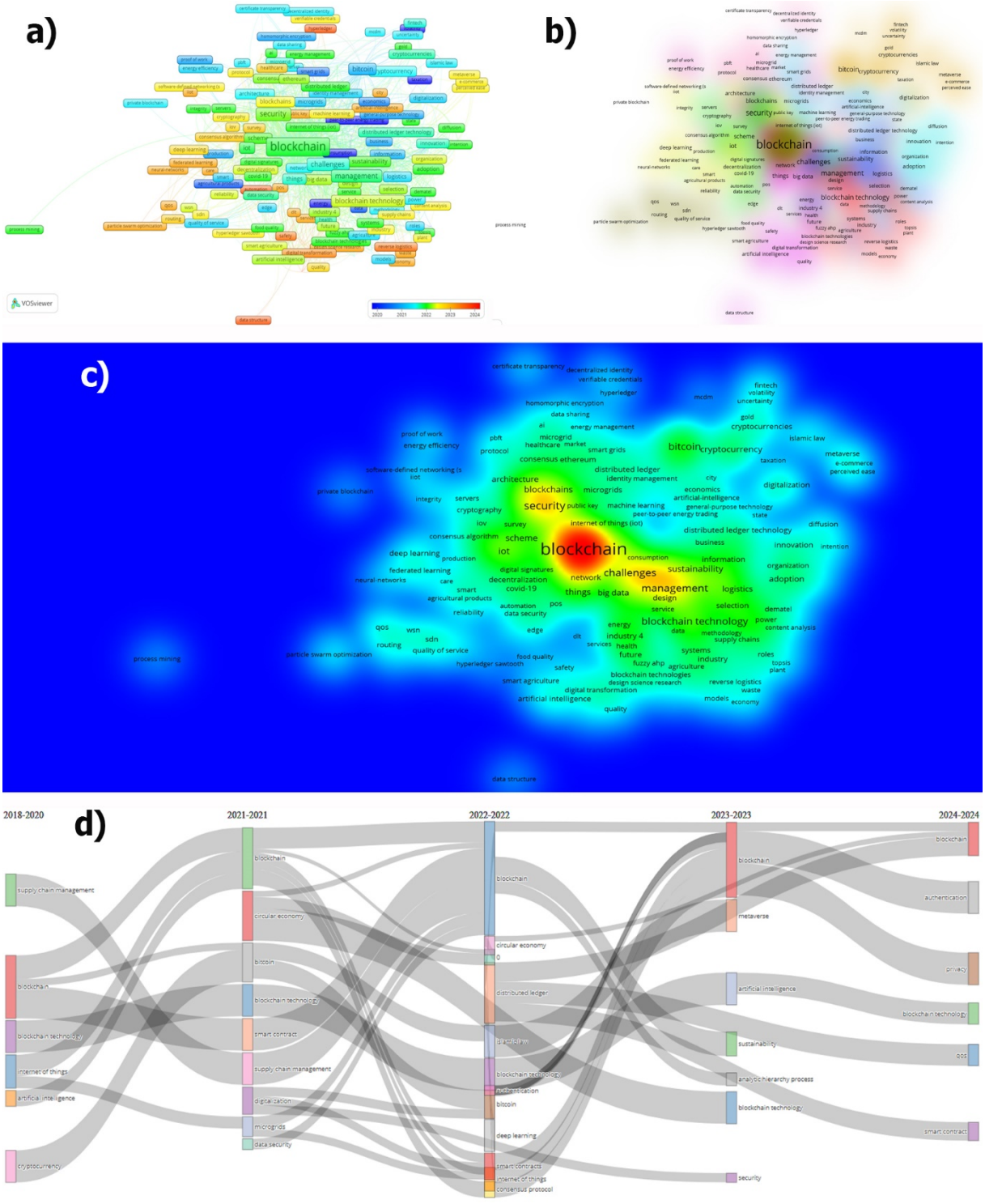
(*Collaboration Network According to Journal and First Authorship Status Among the Sources Used in References of Articles)*

3.3. Makale Araştırma Alanları ve Makalelerde Kullanılan Anahtar Kelimeler, Makale Başlıkları, Özetlerin Analizi *(Article Research Areas and Keywords Used in Articles, Article Titles, Analysis of Abstracts)*

Türkiye adresli blok zincir konusundaki makalelerin ilişkilendirildiği 47 araştırma alanı aşağıda Tablo 5 üzerinde gösterilmektedir. En yoğun ilişkilendirilen ilk beş araştırma alanının yoğunluk sırasında göre; bilgisayar bilimi (f:149, 45.15%), mühendislik (f:124, 37.57%), telekomünikasyon (f:63, 19.09%), işletme ve ekonomi (f:57, 17.27%), bilim, teknoloji, diğer konular (f:23, 6.97%), çevre bilimleri ve ekoloji (f:22, 6.66%), yöneylem araştırması ve yönetim bilimi (f:16, 4.84%), kimya (f:14, 4.24%), enerji yakıtları (f:14, 4.24%), fizik (f:13, 3.93%), şeklindedir. 330 araştırma makalesinde toplamda 1.047 araştırmacı anahtar kelimesi ve dergi ve yayıncı kurumlar tarafından oluşturulan 428 anahtar kelime bulunmaktadır. Blok zincir teknolojisi ile araştırmacıların birlikte odaklandığı öne çıkan başlıklar; siber güvenlik ve bilgi güvenliği (f:58), nesnelerin interneti (f:55), akıllı kontratlar (f:54), güvenlik, mahremiyet (f:31), kripto paralar (f:24), bitcoin (f:23), tedarik zinciri ve tedarik zinciri yönetimi (f:18), dağıtık defter (f:16), sürdürebilirlik (f:13), kimlik doğrulama (f:12), dijitalleşme ve dijital dönüşüm (f:11), büyük veri (f:9), ethereum (f:9), endüstri 4.0 (f:9), eşler arası (peer to peer) bilgi işleme (f:9), yapay zeka (f:9), bulut bilişim (f:9), fikir birliği ve fikir birliği algoritmaları (f:8), COVID-19 (f:7), mikro şebekeler (f:7), döngüsel ekonomi (f:6), akılı şebekeler (f:6), ademi merkeziyet (f:6), derin öğrenme (f:6), yönlendirme (f:5), izlenebilirlik (f:5), dematel (f:4), birleşik öğrenme (f:4), sağlık hizmetleri (f:4), islam hukuku (f:4), lojistik (f:4), makine öğrenme (f:4), metaverse (f:4), çok kriterli karar verme (f:4) ve ölçeklenebilirlik (f:4) öne çıkan başlıklar olmuştur.

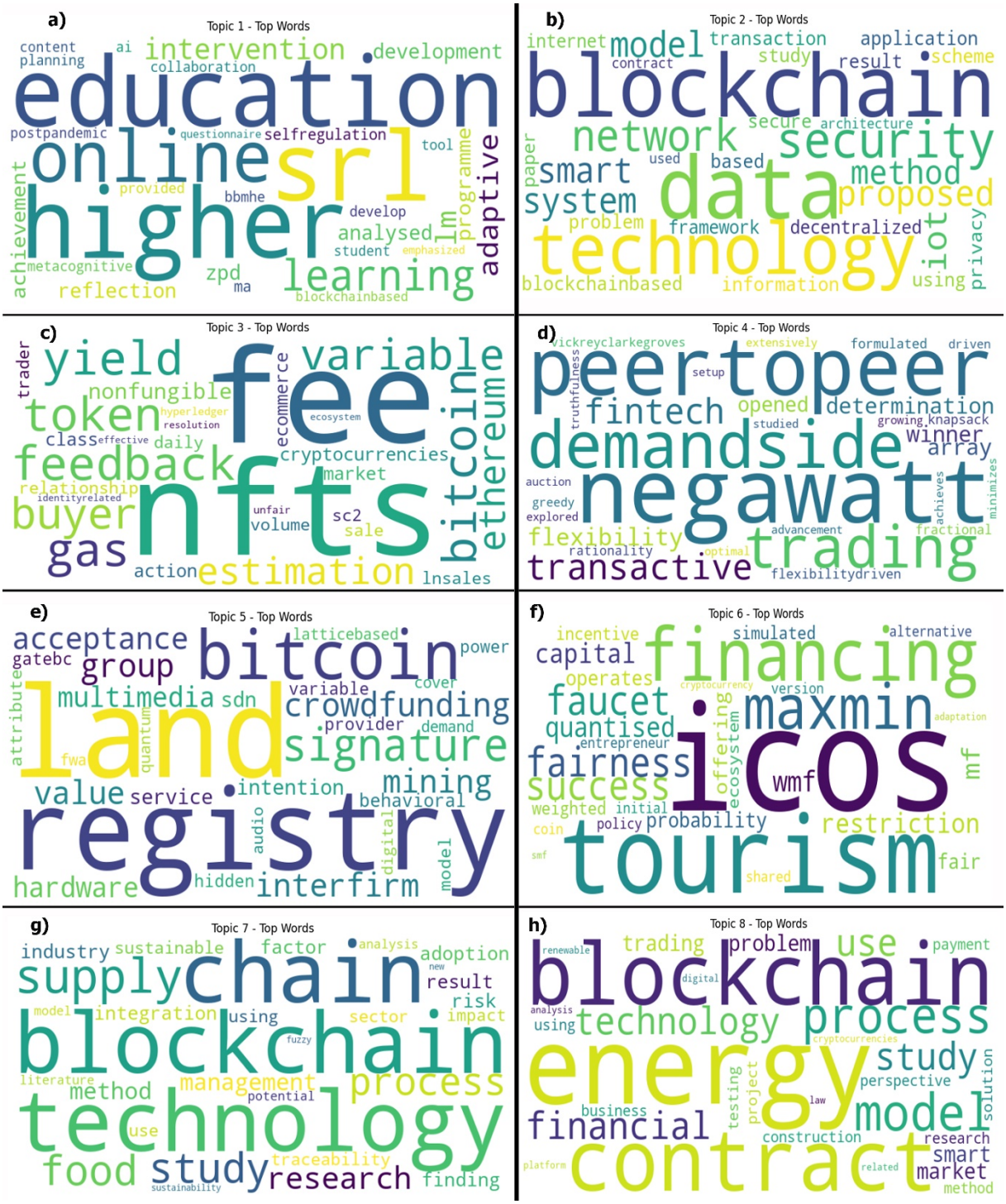
Aşağıda Türkiye adresli makalelerin anahtar kelimelerinin analizi Şekil 5 üzerinde dört farklı analiz ile gösterilmektedir. Bunlara ek olarak gıda tedarik zinciri, fintek, ekonomi, bilgisayar mimarisi, inşaat sözleşmeleri, kimlik yönetimi, enerji verimliliği, uç bilişim, genetik algoritma, entegrasyon, mikro şebeke, konum, yenilenebilir enerji kaynakları, sunucular, akılı şehirler ve 5G teknolojisi öne çıkan diğer başlıklardır.

Aşağıda Şekil 6 üzerinde Latent Dirichlet Allocation konu modellemesi makine öğrenmesi analizi ile Türkiye adresli 330 makalenin özetleri ve başlıkları üzerinden analiz edilmiş, elde edilen sekiz başlık kelime bulutu ile gösterilmektedir. Şaşkınlık metrik değeri 3808.17 ve tutarlılık skoru: 0.48'dir.



Şekil 5. Türkiye Adresli Blok Zincir Makalelerinde Kullanılan Anahtar Kelimelerinin Analizi

(*Analysis of Keywords Used in Blockchain Articles Addressed from Türkiye)*



Şekil 6. Makalelerin Başlıkları ve Özetleri Üzerinden LDA Analiz Sonuçları

(*LDA Analysis Results Based on Titles and Abstracts of Articles)*

Tablo 5. Blok Zincir Konusundaki Makalelerin En Yoğun İlişkilendirildiği Araştırma Alanları
(Research Areas to which Articles on Blockchain are Most Intensively Associated)

Sıra	Araştırma Alanı	N	%	Sıra	Araştırma Alanı	N	%
1	Bilgisayar Bilimi	149	45.15	25	Jeoloji	2	0.60
2	Mühendislik	124	37.57	26	Optik	2	0.60
3	Telekomünikasyon	63	19.09	27	Uzaktan Algılama	2	0.60
4	İşletme ve Ekonomi	57	17.27	28	Robotik	2	0.60
5	Bilim Teknoloji ve Diğer Konular	23	6.97	29	Toplu taşıma	2	0.60
6	Çevre Bilimleri Ekoloji	22	6.66	30	Tarım	1	0.30
7	Yöneylem Araştırması ve Yönetim Bilimi	16	4.84	31	Mimari	1	0.30
8	Kimya	14	4.24	32	Biyokimya ve Moleküler Biyoloji	1	0.30
9	Enerji Yakıtları	14	4.24	33	Biyoteknoloji ve Uygulamalı Mikrobiyoloji	1	0.30
10	Fizik	13	3.93	34	İletişim	1	0.30
11	Bilgi Bilimi ve Kütüphane Bilimi	11	3.33	35	Geliştirme Çalışmaları	1	0.30
12	Malzeme Bilimi	9	2.72	36	Genetik Kalıtım	1	0.30
13	Kamu Yönetimi	9	2.72	37	Sağlık Bilimleri Hizmetleri	1	0.30
14	Sosyal Bilimler ve Diğer Konular	7	2.12	38	Görüntüleme Bilimi ve Fotoğraf Teknolojisi	1	0.30
15	Otomasyon Kontrol Sistemleri	6	1.81	39	Yaşam Bilimleri, Biyotıp ve Diğer Konular	1	0.30
16	İnşaat Yapı Teknolojisi	6	1.81	40	Sosyal Bilimlerde Matematiksel Yöntemler	1	0.30
17	Devlet Hukuku	6	1.81	41	Tıp Bilişimi	1	0.30
18	Aletler ve Enstrümantasyon	5	1.51	42	Sinir Bilimleri ve Nöroloji	1	0.30
19	Matematik	5	1.51	43	Fiziki Coğrafya	1	0.30
20	Gıda Bilimi ve Teknolojisi	3	0.90	44	Bitki Bilimleri	1	0.30
21	Matematiksel Hesaplamalı Biyoloji	3	0.90	45	Psikoloji	1	0.30
22	Beslenme Diyetetik	3	0.90	46	Sosyal Sorunlar	1	0.30
23	Din	3	0.90	47	Kentsel çalışmalar	1	0.30
24	Eğitim ve Eğitim Araştırmaları	2	0.60				

4. TARTIŞMA *(DISCUSSION)*

Blok zinciri, verilerin güvenli, manipüle edilmeye karşı korumalı ve geri döndürülemez bir şekilde saklanmasını ve güncellenmesini sağlamak üzere tasarlanmıştır. Henüz başlangıç aşamasında olmasına rağmen, blok zinciri araştırmaları farklı alanlarda hızla gelişmektedir [42]. Türkiye'den araştırmacılar da 2018 yılından sonra alanın önemli dergilerinde ilgili konuda yayın çıkarmaya başlamıştır. Türkiye 330 doküman ile dünyada bu alanda araştırma yapan ve yayınlayan bilim insanlarının ülkeleri arasında on sekizinci sırada yer almıştır. İlgili konuda ülkelere göre bir sıralama yaptığımızda ilk sıradaki Çin'in ABD'den iki kattan daha fazla ilgili alanda yayın üretiyor olması, Hindistan'ın ilgili alanda bilimsel üretkenlik açısından ABD'ye çok yakın olması, Sudi Arabistan ve Pakistan gibi ülkelerin ilgili konuda dünyada ilk oda yer alması araştırmanın ilginç bulgularından birisi olmuştur.

Türkiye adresli araştırmalardan ilk elde edilen sonuç blok zincir konusunda, internetin, teknoloji yönetim olgusunun, bilgi güvenliğinin, sistem performansının, adaptasyonun, nesnelerin interneti (IoT), endüstri 4.0, büyük veri ve bulut teknolojisi gibi entegre sistemlerin, bilişim sistemi mimarisinin, mahremiyetin, oldukça önemli konu başlıkları olarak alanda öne çıktığıdır. İlgili teknoloji inovasyon, dijitalleşme veya dijital dönüşüm altında farklı sektörlerdeki firmalar için mahremiyet konusunda çözüm olarak sunulmaktadır. Genelde sağlık sektörü veri mahremiyetinin önem kazandığı benzer sektörlerde blok zincir Türkiye'de yoğun ilgi görmüştür. Analizlerimiz sonucunda akıllı kontratlar, kripto para, tedarik zinciri, tedarik zinciri yönetimi, enerji, turizm, eğitim, güvenlik, ağ, IoT, akıllı sistemler, sürdürülebilirlik blok zincir konusunda en fazla göze çarpan konular olmuştur.

Türkiye adresli araştırmalarda blok zincir konusunun döngüsel ekonomi başlığı ile de yoğun ilişkilendiği görülmüştür. Döngüsel ekonomi, ekonomik büyümenin yanı sıra sürdürülebilirliği ve sosyal sorumluluğu artırmaya da odaklanmaktadır [42]. Kaynakların kullanılabilirliğine önem veren sürdürülebilirlik sisteminde geri dönüşüm, yenileme ve yeniden üretim stratejileri döngüsel ekonomi adı altında ele alınabilir [43]. Blok zinciri, özellikle teknolojik, organizasyonel ve ekolojik olmak üzere bu

engellerden bazılarını ele alma potansiyeline sahip yıkıcı bir teknolojidir. Blok zinciri, döngüsel ekonominin benimsenmesinin önündeki tedarik zinciri odaklı engellerin ele alınmasına yardımcı olmak için özellikle uygundur [44]. Blok zinciri teknolojisinin döngüsel ekonomiye mevcut ve potansiyel katkısı, sürdürülebilirlik ve sosyal sorumluluk açısından pek çok çalışmada değerlendirilmiştir [42-46]. Analizlerimiz sonucunda da Türkiye merkezli çalışmalarda döngüsel ekonomi konusunda gerçekleştirilen çalışmaların çok fazla atıf aldığı ve önem verildiği görülmektedir.

Hastaların hassas ve kişisel verileri, bilgisayar korsanlarından korunurken çeşitli zorluklara yol açmaktadır. Bu nedenle, hasta tıbbi bilgilerinin bulut üzerinde depolanması, erişilmesi ve paylaşılması, verilerin E-sağlık sistemlerinin yetkili kullanıcı bileşenleri tarafından tehlikeye atılmaması için güvenlik dikkatine ihtiyaç duyar [47]. Blok zincirin sağladığı bilgi güvenliği konusundaki imkanlar bu güncel teknolojiyi sağlık sektörü için oldukça cazip hale getirmektedir. Türkiye adresli araştırmalarda da oldukça yoğun çalışılan konulardan birisi olmuştur [47-49]. Baysal ve diğerleri [49] yapmış olduğu analizde blok zincirinin bu zorlukların çözümüne önemli katkılar sağladığını göstermektedir. Bununla birlikte, blok zincir teknolojisinin sağlık alanında benimsenmesiyle birlikte yeni tuzakların çıktığını belirtmişlerdir: hassas verilerin bir zincire eklendikten sonra silinememesi, büyük ölçekli verilerin blok zincirinde tutulma kabiliyetinin sınırlı olması ve performans sorunları. Ancak büyük veri ekosisteminde nesnelerin interneti özellikli sağlık verileri analitiği için doğrulanabilir veri erişim mekanizması sağlayan ölçeklenebilir bir bilgi işlem sistemi sunmaya imkân verebilir [48].

Günümüzde giderek yaygınlaşan nesnelerin interneti tabanlı sağlık hizmetleri, sürekli olarak büyük veri olarak adlandırılan çok büyük miktarlarda veri üretmektedir. Büyük veri sistemleri, IoT sistemlerinin amacına daha iyi hizmet etmek ve kritik karar alma süreçlerini desteklemek için önemli bir altyapı hizmeti üstlenmektedir. Öte yandan, gizliliğin korunması, veri bütünlüğü ve kimlik doğrulama, sağlık hizmetleri büyük veri hizmeti yönetiminde temel gereksinimlerdir. Bu noktada blok zincir teknolojisi kritik ve değerli bir teknoloji olarak karşımıza çıkmaktadır [48].

Yeni sensör teknolojilerinin gelişmesiyle birlikte, Nesnelerin İnterneti tabanlı sağlık uygulamaları son yıllarda ivme kazanmıştır. Ancak Nesnelerin İnterneti cihazlarının sınırlı kaynaklara sahip olması, onları büyük hesaplama işlemlerini gerçekleştirme konusunda yetersiz kılmaktadır. Bu sorunu çözmek için, dinamik ölçeklenebilirlik ve altyapı yönetimi gibi avantajlarıyla sunucusuz paradigma, Nesnelerin İnterneti tabanlı uygulamaların gereksinimlerini desteklemek için kullanılabilir. Bu noktada da blok zincir teknolojisi öne çıkmaktadır [50].

Sağlık hizmetlerinde Nesnelerin İnterneti akıllı sistem tabanlı blok zincirinin güvenlik ve gizlilik gereksinimleri açısından modellenmesi, çok kriterli karar verme sorunu olarak kabul edilmektedir. Literatür incelemeleri Nesnelerin İnterneti akıllı sistem tabanlı blok zincirini değerlendirmiş olsa da bilgi belirsizliği, belirsizlik ve belirsizlik hala açık konular olmaya devam etmektedir [51].

Blok zincir ve akıllı sözleşmeler, bilgi teknolojisi sahnesindeki gelecek vaat eden konu başlıkları olarak karşımıza çıkmıştır ki Türkiye adresli araştırmalarda yoğun olarak bu başlık işlenmiştir. Günümüzde akıllı sözleşmelerin dijital mimarisi, sözleşme yükümlülüklerinin yerine getirilmesini otomatik hale getirmekte ve bu yükümlülüklerin yerine getirilmesini sağlayan dijital özelliklere sahiptir. Güncel teknolojik yeniliklere ve blok zincir teknolojisine dayanan akıllı sözleşmelerin en önemli farkı, akıllı sözleşmelerin sözleşme tarafları veya başka bir kişi tarafından yüklendiği blok zincir sistemine dışarıdan müdahale edilmesinin teknik ve fiili olarak mümkün olmamasıdır [52]. Blok zincir ağındaki işlemlere çerçeve sağlayan akıllı sözleşmeler, sistem katılımcılarının sadece kripto para işlemlerinin ötesine geçerek aralarında birçok farklı işlem yapmasına olanak sağlamaktadır. Ancak işlem geçmişinin değiştirilemeyeceği ilkesine dayanan blok zincir teknolojisi ve bu teknolojiye bağlı akıllı sözleşmeler, veri koruma hukuku ve borçlar hukuku açısından da birçok sorunu beraberinde getirmektedir [53].

Akıllı sözleşmeler pek çok alanda kullanılabilmektedir [54-58]. Elektronik ortamda tutulan verilerin katlanarak artması, geleneksel merkezi uygulamaların yeni zorluklarla karşı karşıya kalmasına neden olmaktadır. Bunlardan en önemlileri hesap verebilirlik, şeffaflık, güvenlik, maliyet ve zaman verimliliğidir. Çalık ve diğerleri [58] tarafından akıllı sözleşmeler, çok paydaşlı paylaşılan tıbbi verilerin şeffaflığını, hesap verebilirliğini ve güvenliğini artırmak için bir çözüm olarak sunmuştur**.** Akıllı sözleşmelerle paylaşılan tıbbi verilerin güvenliğinin sağlanmasına yönelik yeni bir yöntem olarak değerlendirilmiştir [58]. Sağlık sektörü yanında, akıllı sözleşmeler, inşaat projelerinin etkili bir şekilde yönetilmesinde önemli bir rol oynamaktadır. Araştırmacılar blok zincir teknolojisinin inşaat sektöründe uygulanmasını önünde dört ana engele ulaşıldığını ifade etmiştir:

Teknik, finansal, güvenlik/teknolojik ve zaman. Ayrıca, finansal ve teknik hususların akıllı sözleşmelerin benimsenmesini engelleyen en önemli kategorileri oluşturduğunu, pahalı ve hantal taslak hazırlama ve kayıt süreci ile beceri geliştirme maliyetinin ise en önemli engeller olduğunu göstermektedir [59].

Blok zincir konusunda öne çıkan bir diğer teknoloji de büyük veri olmuştur. Yapay zeka, büyük veri, Nesnelerin İnterneti cihazları ve blok zincir içeren bilgi teknolojileri dünya çapında birçok mühendislik alanında geliştirilmiş ve uygulanmıştır. Tamamı iletişim, bilgi ve veri analizine dayanan bu teknolojiler doğal olarak veri tutarlılığı ile entegre edilebilir. Yapay zeka modelleri, enerji kullanımını ve yük profillerini tahmin etmenin yanı sıra, enerji kaynaklarının güvenilir performans ve etkin kullanımını sağlamak için kaynakları zamanlar. Yapay zeka modellerinin eğitimi muazzam miktarda veri gerektirir. Büyük veri sistemlerinden ve veri madenciliğinden faydalanmak, yapay zekanın performansını belirleyen yeni fonksiyonların ve ilişkilerin keşfedilmesine olanak sağlar. Veri madenciliği aynı zamanda bilgiyi de geliştirir; Böylece yapay zeka daha doğru verilerle yinelemeli olarak eğitilir. Tüm bunlara ek olarak uç (edge), sis ve bulut katmanlarını içeren Nesnelerin İnterneti platformu, yapay zekanın diğer donanım ve yazılım cihaz ve sistemlerine bağlanmasına yardımcı olur. Ayrıca, Nesnelerin İnterneti platformu, verileri verimli bir şekilde iletip saklayarak veri madenciliği için paydaşların erişimini ve kullanılabilirliğini artırır [60].

Tarım ve gıda endüstrisinde, tarımsal gıda üretimi ve ticaretinde bir sonraki aşamayı mümkün kılan, Tarımsal Gıda 4.0 olarak adlandırılan devrim niteliğindeki konseptler, süreçler ve teknolojilerle yeni bir dönem yaklaşıyor. Ayrıca tüketiciler, tarım-gıda ürünlerinin menşei, izlenebilirliği, sağlıklı ve yüksek kalitesi konusunda giderek daha bilinçli hale geliyor [61]. Endüstri 4.0 çağındaki dijital teknolojiler, gıdanın izlenme şeklini iyileştirme, gıda israfını azaltma ve sahtekarlığa karşı savunmasızlığı azaltma konusunda önemli bir potansiyele sahip olup, daha akıllı gıda izlenebilirliğine ulaşmak için yeni fırsatlar açmaktadır [62]. Gıda izlenebilirliği 4.0, gıdanın orijinalliğini, güvenliğini ve yüksek gıda kalitesini sağlamak için dördüncü sanayi devrimi (veya Endüstri 4.0) teknolojilerinin uygulanmasını ifade eder. İzlenebilirlik 4.0'ın birçok meyve ve sebzenin kalitesini ve güvenliğini artırma, şeffaflığı artırma, gıda geri çağırma maliyetlerini azaltma ve atık ve kayıpları azaltma konusunda önemli bir potansiyele sahiptir [63].

Liu ve diğerleri [64], blok zincir teknolojisini kullanan ülkelerin rüzgar ve güneş yatırımlarına özellikle önem vermesi gerektiğini belirtmiştir. Bu konuda rüzgar ve güneş enerjisini kullanan şirketlerin blok zincir teknolojisini kullanan kişi veya kurumlarla iş birliği içinde olması gerekli görülmektedir. Yenilenebilir enerji alternatifleri sayesinde blok zincir teknolojisinin kullanımından kaynaklanan fazla enerji tüketimi, çevre dostu enerji kaynaklarıyla sağlanabilmektedir. Yani bu teknolojinin kullanılmasıyla ortaya çıkan karbon emisyonu problemini en aza indirmek mümkün olacaktır [64]. Yapay zeka, büyük veri ve ileri dijital teknolojilerin etkin ve kusursuz entegrasyonunun sağlanması, enerji sektörünün daha düşük karbonlu sisteme geçişinde önemli bir faktör olacaktır [60]. Dolayısı ile blok zincir teknolojisinin sürdürülebilir enerji kavramı için de oldukça önem arz ettiği ifade edilebilir.

Nesnelerin İnterneti, İnternet bağlantısını e-Sağlık, akıllı şehirler, siber-fiziksel sistemler vb. gibi çeşitli uygulama ortamlarına genişletmek için her yerde bulunan bilgi işlemi entegre etmektedir. Bunu da 5G ağ dağıtımında yüksek hız aktarım ile gerçek zamanlı nesneleri birbirine bağlayarak gerçekleştirir [55]. Bu durum blok zincir teknolojisi için de gerçekli ve kritik değerdedir. 5G teknolojisi ve blok zincir teknolojisi birbirlerini tamamlayan özelliklere sahiptir ve bu iki teknoloji arasındaki sinerji, bir dizi önemli avantaj sağlar. 5G'nin blok zincir için neden önemli olduğuna dair anahtar noktalar şu şekilde sıralanabilir: Daha hızlı ve daha güvenilir veri aktarımı, düşük gecikme süresi, geniş bant genişliği, gelişmiş güvenlik ve gizlilik, yeni uygulama alanları ve iş modelleri, dağıtık ağların etkin yönetimi ve enerji verimliliğidir. Hız, güvenilirlik, düşük gecikme süresi ve geniş bant genişliği gibi özellikler, blok zincir ağlarının daha verimli ve etkili çalışmasını sağlar. Bu iki teknolojinin birleşimi, dijital dönüşümü hızlandıracak ve çeşitli sektörlerde yenilikçi çözümlerin önünü açacaktır.

Literatürde ağırlıklı olarak akıllı sözleşmelerin IoT cihazları ile entegrasyonuna yönelik incelemelere dayanan sınırlı sayıda çalışma bulunmasına rağmen, bu yöntemlerin turizm sektöründe nasıl uygulanacağına ilişkin sorular ile yeterli çalışma bulunmamaktadır [56]. Turizm endüstrisi dünya ekonomisi için son derece önemlidir; ancak sektör ekonomik, sosyal ve çevresel konularda yetersiz kalıyor. Bir bilgi teknolojisi olarak blok zincir, bu sorunların çözülmesine ve küresel olarak sürdürülebilir turizmin kurulmasına yardımcı olmak için kullanılabilir [65]. Akılı kontratlar turizm sektörü için blok zincirin uygulanması noktasında önemli bir hizmet kalemi olarak karşımıza çıkmaktadır. Demirel ve diğerleri [56] bu noktada otel hizmetlerine entegre bir rezervasyon sistemi ile sözleşme oluşturarak

mevcut literatüre katkı sağlamaktadır. Önerilen yöntem, müşteriler ve oteller arasında benzersiz bir akıllı sözleşmeye sahip bir rezervasyon sistemi oluşturmaktadır. Bu sözleşmeler ile, müşterinin konaklama süresince ihtiyaç duyabileceği her türlü hizmeti içerecek ve blok zincir yapısı ile güvence altına alınacağını idea etmişlerdir [56].

Başer ve diğerleri [66], dağıtılmış bir dijital defter olarak blok zincir teknolojisi, kullanıcıların üçüncü şahıslar tarafından ihlal edilmeden kimlik bilgilerini kontrol etmelerini sağlayacağını ve turizm açısından konuya bakıldığında, turistlerin beklemeden ve üçüncü taraf işlemlerine gerek kalmadan kontrol noktalarından ve/veya rezervasyonlardan geçmelerine olanak tanıdığını ifade etmiştir.

Bunun yanında turizm sektöründe blok zincir teknolojisinin bir diğer tartışma alanı ilk madeni para tekliflerinin turizm finansmanı için kullanılabilirliğidir. Kitlesel fonlamanın yeni bir biçimi olan ilk madeni paralar (initial coin offerings), girişimcilere sermaye toplamak için kullanılabilecek halka arzlar olup finansman sıkıntısı çeken turizm girişimleri için yeni bir finansman yöntemi olma potansiyeli olarak görülmektedir. Görüldüğü üzere turizmin desteklenmesinden, müşteri verilerinin saklanmasına kadar pek çok noktadaki problemler için blok zincir teknolojisi çözüm olarak değerlendirilmiştir.

Covid-19 virüsü dünya çapında 200'den fazla ülkeye hızla yayılmış ve 690.000'den fazla insanın ölümüne neden olmuştur. Bu hastalığın hızla yayılmasını önlemek için Covid-19 hastalığı bulgularına ilişkin bilgi paylaşımının ülkeler arasında hızlı ve güvenli olması gerekmektedir. Semptomlar ve özel hasta kayıtları gibi Covid-19 ile ilgili sağlık verileri gizli olduğundan bu tür bilgiler mahremiyetin korunmasını gerektirmektedir. Blok zincir ve akıllı sözleşmeler, Covid-19 ile ilgili bilgilerin yayılmasında hız, gizlilik ve güvenlik ihtiyaçları için çok uygun çözümlerdir [67].

Küresel bir sorun olan COVID-19, dünya genelindeki tüm tedarik zincirlerini etkilemektedir. COVID-19'dan en çok etkilenen tedarik zincirlerinden biri gıda tedarik zincirleridir. Sürdürülebilir gıda tedarik zinciri süreçleri, ürün çeşitliliği açısından karmaşık ve hassas olduğundan, COVID-19'un operasyonel etkilerinden olumsuz etkilenmiştir. Tedarik zinciri süreçlerinde yaşanan sorunlar ve hammadde kısıtları üretimin durmasına neden olurken, yeni iş modellerinin ve üretim yaklaşımlarının önemi öne çıkmıştır [68].

Türkiye adresli araştırmacıların blok zincir konusunda yoğunlaştığı bir diğer başlık ise islami finans açısından blok zincir teknolojisini değerlendirdikleri araştırmalar olmuştur [69-71]**.** Kripto paralar gibi benzeriz dijital varlıkların ve Metaverse projelerinin ve mallarının ticareti İslam Hukuku perspektifinden analiz edilmektedir [69]. Kripto paraların İslam hukukuna göre meşruiyeti konusunda doğru bir sonuca ulaşabilmemiz için çağımızın gerçekleriyle yüzleşmemiz kaçınılmaz olacaktır. Günümüzde finansal işlemler kripto para borsalarında, risklere rağmen çok geniş bir ağ içerisinde gerçekleştirilmekte ve çok yüksek hacimlere ulaşmaktadır [71]. Kripto para piyasa büyüklüğü 2018 yılı başında 800 milyar doları aşmıştır. Kripto para kullanıcılarının çoğu, kripto paraların değer artışlarından pay almak istiyor. Ancak bu davranışlar kripto paraların felsefesine uygun değildir. Kripto para birimleri aynı zamanda Müslüman kullanıcılar açısından İslam Fıkhı açısından meşruiyet sorunu da yaratmaktadır. Pek çok dini kurum ve İslam alimi kripto para birimlerinin haram olduğunu söylese de birçok İslam alimi bunların helal olduğunu düşünmektedir [70].

Dünya literatüründe blok zincir tartışmalarında olduğu gibi Özdağoğlu ve diğerleri [72] Türkiye'de de akıllı araçlar, blok zincir teknolojisinin güvenliği, bulut teknolojisi ve burada veri transferleri ve veri barındırılması, lojistik yönetimi ve yukarıda da bazı noktalarda değindiğimiz tedarik zinciri yönetimi gibi pek çok başlık Türkiye adresli araştırmacılar için de ortak konular olmuştur.

5. SONUÇ *(CONCLUSION)*

Bu çalışmada WoS gibi dünyada önde gelen yayınevlerini tarayan bir veri tabanından gerçekleştirilen tarama ile Türkiye adresli blok zincir konusunda 330 araştırma ve derleme türünde makale elde edilmiştir. Elde edilen makale kayıtları için bibliyometrik analiz ve makine öğrenmesi tabanlı LDA konu modellemesi yöntemi kullanılarak analiz edilmiştir. Çalışmada, Türkiye adresli blok zincir konusundaki araştırmacıların yıllara göre yayın çıktıları, yayınların yapıldığı dergiler, yayınları destekleyen kurumlar, açık erişim durumu, yayınlarda kullanılan kaynaklar ve bu kaynaklarda geçen dergi ve birinci yazarlık durumu detaylı olarak analiz edilmiştir. Ortak yazarlık, orta atıf analizi ve ortak kelime analizleri kümelenme, tematik haritalandırma, ortak ağda bulunma durumları gibi pek çok farklı duruma göre değerlendirilmiştir. Türkçe literatürde bu yönde gerçekleştirilen ilk araştırma olması yanında, alan okuyucularına alanın gelişmesi ve analizlerden elde ettiği sonuçlar ile bu yönde alanda gerçekleştirilen en kapsamlı ve detaylı araştırmadır. Alanda Türkiye tüm dünya genelinde bilimsel üretkenlik açısından 18. sırada yer almaktadır. Türkiye gibi dünyada ilk on ekonomide yer alma

hedefi olan bir ülkenin bu noktada daha üst sıralarda yer alabilmesi için farklı stratejiler oluşturması gerekli görülmektedir.

6. ÖNERİLER *(SUGGESTIONS)*

Blok zincir teknolojisi farklı sektörlerde veri bütünlüğünü ve güvenliğini sağlamada önemli bir rol oynayabilir. Örneğin, enerji sektöründe blok zinciri büyük ölçekli enerji sistemleri ve varlık yönetimi için kullanılabilir ve bu da verimliliğin artmasına katkı sağlayabilir [73]. Ayrıca, sağlık endüstrisinde, blok zincir çözümleri hasta kimlik güvenliğini artırabilir, tedarik zincirlerini yönetebilir ve tıbbi hileleri tespit edebilir [74]. Bu uygulamalar Türkiye'nin sağlık sisteminin veri yönetimini ve hasta bakımını iyileştirmesi açısından önemli faydalar sağlayabilir. Ayrıca, Türkiye'de blok zinciri teknolojisinin benimsenmesi, denetim uygulamalarında da ilerlemelere yol açabilir. Blok zinciri entegrasyonu, ekonomik denetim fonksiyonlarını, veri güvenliğini artırabilir ve denetim süreçlerini otomatikleştirebilir [75]. Bu, kuruluşlar içinde daha iyi finansal şeffaflık ve sorumluluk sağlayabilir.

Türkiye'de blok zincir teknolojisinin benimsenmesi, küçük ve orta ölçekli işletmelerin (KOBİ) tedarik zinciri operasyonlarını geliştirmede de fayda sağlayabilir. Araştırmalar, blok zinciri teknolojisinin maliyetleri optimize edebileceğini, kayıt tutmayı iyileştirebileceğini ve tedarik zincirlerinde şeffaflık sağlayabileceğini göstermektedir. Bu da KOBİ'lerin pazarda etkili bir şekilde rekabet etmelerini sağlayacaktır [76]. Türkiye'de KOBİ'lerin tedarik zinciri yönetim sistemlerine blok zinciri entegre etmesi işlemleri hızlandırabilir, işletme verimsizliklerini azaltabilir ve ortaklar ve müşterilerle güven inşa edebilir. Tedarik zinciri yönetiminin yanı sıra blok zinciri teknolojisi Türkiye'de finansal işlemleri ve işletme finansmanını geliştirmede de önemli bir rol oynayabilir. Blok zincirinin güvenli ve şeffaf doğası, tarımsal işletme finansmanını kolaylaştırabilir, kayıt tutmayı iyileştirebilir ve paydaşlar arasında güven oluşturabilir [77]. Böylece Türkiye'deki tarım endüstrisi için özellikle faydalı olabilir. Finansmana erişim ve şeffaf işlemler, sürdürülebilir büyüme ve kalkınma için büyük öneme sahiptir. Çalışma kapsamında gerçekleştirilen analizler sonucunda da tedarik zinciri, gıda tedarik zinciri, akıllı tarım, gıda güvenliği gibi konuların ön plana çıkması da bu konuların önemini ortaya çıkarmaktadır.

Türkiye'de blok zinciri teknolojisinin benimsenmesinin, kamu sektörüne de faydası olabilir. Blok zinciri, kamu hizmetlerinde şeffaflığı artırmak, dolandırıcılığı önlemek ve e-devlet hizmetlerine güven oluşturmak için kullanılabilir [78]. Kamu sektörü operasyonları için blok zincirinden yararlanarak Türkiye, veri güvenliğini artırabilir, idari süreçleri düzenleyebilir ve vatandaşların devlet hizmetlerine olan güvenini artırabilir. Bu da kamu yönetiminde daha büyük verimlilik, sorumluluk ve duyarlılık sağlayabilir. Çalışma kapsamında analizlerde de görüldüğü gibi dijital dönüşüm, dijitalleşme, akıllı sözleşmeler gibi kavramların sıklıkla kullanılması blok zincir teknolojisinin kamu yönetiminde de önemli bir rol alacağını göstermektedir.

Türkiye'deki mühendislik-inşaat endüstrisinde, blok zinciri teknolojisi geleneksel uygulamaları dönüştürebilir ve projelerde iş birliği ve entegrasyon yönetimini iyileştirebilir [79]. Blok zinciri çözümlerinden yararlanarak mühendislik-inşaat sektöründeki paydaşlar proje görünürlüğünü artırabilir, iletişimi kolaylaştırabilir ve projenin yaşam döngüsü boyunca veri bütünlüğünü sağlayabilir. Türkiye'deki inşaat endüstrisinde maliyet tasarrufu, anlaşmazlıkların azalması ve iyileştirilmiş proje sonuçlarını sağlayabilir.

Türkiye'de enerji verimliliğini ve sürdürülebilirlik girişimlerini artırmada blok zinciri teknolojisi önemli bir rol oynayabilir. Enerji ticaret sistemlerinde, uçtan-uca enerji ticareti ve varlık yönetiminde blok zinciri uygulamalarının keşfedilmesiyle Türkiye enerji kullanımını optimize edebilir. Karbon emisyonlarını azaltabilir ve yenilenebilir enerji kaynaklarını teşvik edebilir [73]. Dolayısıyla Türkiye'nin sürdürülebilir kalkınma ve çevre koruma hedefleriyle uyumlu olabilir. Böylece daha yeşil ve daha dirençli bir enerji sektörüne katkıda bulunulabilir. Çalışma kapsamındaki analizler sonucunda enerji sektörüyle ilgili konuların akademik çalışmalarda sıklıkla kullanılması enerji sektörüne yönelik blok zincir teknolojisinin önemini ortaya koymaktadır.

Türkiye'deki bankacılık ve finans teknolojisi (fintek) sektörleri arasındaki iş birliği, büyük veri, yapay zeka ve blok zinciri gibi teknolojileri kullanarak sürdürülebilir finansı önemli ölçüde ilerletebilir. İstanbul Finans Merkezi'nde olduğu gibi, korumalı/sanal ortam gibi girişimler blok zincirini içeren fintek çözümlerinin ortaya çıkmasını kolaylaştırabilir ve risk değerlendirmesini geliştirmek için ulusal bir karbon ticaret mekanizması kurabilir [80]. Bu tür iş birliklerinin ve düzenleyici desteğin teşvik edilmesiyle Türkiye, finans sektöründe blok zinciri inovasyonu için uygun bir ortam yaratabilir. Araştırmalar, Dijital Türk Lirası (DTL) gibi dijital para birimlerinin geliştirilmesini ve Borsa İstanbul'daki blok zinciri teknolojisinden yararlanan girişimleri vurgulamıştır [81]. Diğer ülkelerden

başarılı modelleri inceleyerek ve özelleştirilmiş çözümler uygulayarak, Türkiye finansal kapsayıcılığı artırabilir ve ekonomide blok zinciri uygulamaları için yeni olanakları keşfedebilir.

Yeşil tedarik zinciri yönetiminde blok zinciri benimsemenin engelleriyle başa çıkmak, sürdürülebilir uygulamalar için hayati öneme sahiptir. Engelleri kaldırarak ve yeşil tedarik zinciri yönetiminde blok zinciri uygulamalarını genişleterek Türkiye çevresel sürdürülebilirliği teşvik edebilir ve operasyonel verimliliği artırabilir [82]. Bu tür yaklaşımlar, sürdürülebilir uygulamalara yönelik küresel trendlerle uyumlu olup Türkiye'yi yeşil teknoloji benimsemede bir öncü olarak konumlandırabilir [83-84].

Blok zinciri benimseme ve uygulamanın temel başarı faktörlerini anlamak esastır. Sistem güvenilirliği, veri bütünlüğü ve genel maliyet gibi farklı kategorilerdeki anahtar performans göstergelerini değerlendirmek, Türkiye'nin blok zinciri teknolojisini etkili bir şekilde benimsemesine rehberlik edebilir [85]. Bu başarı faktörlerine odaklanarak ve olası zorlukları ele alarak, Türkiye blok zincirini çeşitli sektörlerde entegre etmeyi kolaylaştırabilir. Ayrıca, terör finansmanıyla mücadelede blok zinciri kullanımının araştırılması Türkiye için kritik bir odak alanı olabilir. Kripto paraların yasadışı faaliyetlere karışan organizasyonlar tarafından nasıl kullanıldığının anlaşılması ve riskleri azaltıcı önlemlerin uygulanması ulusal güvenliği güçlendirebilir [86]. Farklı ülkelerdeki teknolojik gelişmelerin de incelenmesi oldukça faydalı görülmektedir. İrlanda, Hindistan ve son zamanlarda yükselen Çin bu konuda oldukça ileri noktalardadır ve bu ülkelerden çıkarılacak dersler Türkiye'nin güncel teknolojiler konusunda daha rekabetçi olmasını sağlayabilir [87-89]. Detaylı araştırmalar yaparak ve hedefe yönelik stratejiler geliştirerek, Türkiye blok zinciri teknolojisi ile ilişkili olası tehditleri ele almak için düzenleyici çerçevesini güçlendirebilir.

Blok zinciri teknolojisinin yükseköğretim kurumlarında benimsenmesi, öğrenci akreditasyonunu doğrulamak için *blok zincir akıllı müfredat sistemi* gibi yenilikçi sistemlerin geliştirilmesini sağlamıştır [90]. Bu sistemler, eğitim sürecinde biriken akademik kayıtların ve başarıların güvenli bir şekilde saklanması ve paylaşılmasına odaklanmaktadır [91]. Ayrıca, blokzinciri teknolojisi sahte akademik sertifikaları tespit etmek ve önlemek için uygulanmış olup doğrulama sürecinin etkinliğini artırmaktadır [92]. Eğitim diplomalarının blokzinciri çözümleri aracılığıyla düzenlenmesi ve doğrulanması, idari görevlerin kolaylaştırılması ve maliyetlerin azaltılması gibi faydalar sunmaktadır [93]. Türkiye'de de yükseköğretim kurumlarında blok zincir teknolojisinin kullanılması yukarıda verilen örnekler gibi birçok açıdan katkı sağlayacağı düşünülmektedir. Ayrıca araştırmanın Ozdagoglu ve diğerlerinin [72] Scopus ve Web of Science veri tabanı üzerinden gerçekleştirdiği İngilizce makalenin Türkçe versiyonu ve güncel tarihli incelemesi yönüyle özellikle Türkçe literatür için önemli bir katkı sunduğu düşünülmektedir.

Sonuç olarak, Türkiye'de blok zinciri teknolojisinin benimsenmesi, çeşitli sektörlerde büyük potansiyele sahiptir. Türkiye, blok zincirini tedarik zinciri yönetimi, finans, tarım, enerji verimliliği, sağlık ve denetim alanlarında kullanarak farklı endüstrilerde işletme verimliliğini, şeffaflığı ve güvenliği artırabilir ve nihayetinde ekonomik büyümeyi ve inovasyonu teşvik edebilir. Blok zincirinin merkezi olmayan, şeffaf ve güvenlik gibi benzersiz özelliklerinden yararlanarak Türkiye kendisini dijital dönüşümde bir lider olarak konumlandırabilir. Teknolojik olarak gelişmiş bir ekonominin faydalarını elde ederek uluslararası alanda daha rekabetçi konuma gelebilir. Türkiye'de diğer ülkelerde de olduğu gibi blok zinciri teknolojisinin benimsenmesi kurumsal, teknolojik ve çevresel faktörlerden etkilenen çok yönlü bir süreçtir. Türkiye, blok zinciri teknolojisinin potansiyelini değerlendirerek, zorlukları ele alarak ve sektörler arası iş birliği yaparak çeşitli endüstrilerde gelişme sağlayabilir ve ülkedeki gelişime katkıda bulunulabilir. Blok zinciri benimsemeyi etkileyen faktörleri değerlendiren çerçevelerin benimsenmesi, sektörler arası iş birliklerinin teşvik edilmesi, tarım ve finans alanlarında uygulamaların keşfedilmesi, yeşil tedarik zinciri yönetimindeki engellerin ele alınması ve proje yönetimi uygulamalarının iyileştirilmesi gibi adımlarla Türkiye blok zinciri teknolojisinin gelişiminde öncü bir rol üstlenebilir.

KAYNAKLAR *(REFERENCES)*

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system [White paper]", Bitcoin.org.

[2] C. Yu, W. Yang, F. Xie, ve J. He, "Technology and Security Analysis of Cryptocurrency Based on Blockchain", *Complexity*, c. 2022, 2022, doi: 10.1155/2022/5835457.

[3] G. Gunarso ve Stephanie, "Cryptocurrency and Its State of Research", *International Dialogues on Education Journal*, c. 9, sy 1, ss. 151-175, Ağu. 2022, doi: 10.53308/IDE.V9I1.280.

[4] M. Arias-Oliva, J. Pelegrín-Borondo, ve G. Matías-Clavero, "Variables influencing cryptocurrency use: A technology acceptance model in Spain", *Front Psychol*, c. 10, sy MAR, s. 438810, Mar. 2019, doi: 10.3389/fpsyg.2019.00475.

[5] C. Li, N. Khaliq, L. Chinove, U. Khaliq, J. Popp, ve J. Oláh, "Cryptocurrency Acceptance Model to Analyze Consumers' Usage Intention: Evidence From Pakistan", *Sage Open*, c. 13, sy 1, Oca. 2023, doi: 10.1177/21582440231156360.

[6] A. Sousa, E. Calçada, P. Rodrigues, ve A. Pinto Borges, "Cryptocurrency adoption: a systematic literature review and bibliometric analysis", *EuroMed Journal of Business*, c. 17, sy 3, ss. 374-390, Ağu. 2022, doi: 10.1108/EMJB-01-2022-0003.

[7] Y.-C. Yeong, "What drives cryptocurrency acceptance in Malaysia?", *Science Proceedings Series*, c. 1, sy 2, ss. 47-50, Nis. 2019, doi: 10.31580/SPS.V1I2.625.

[8] B. J. Butijn, D. A. Tamburri, ve W. J. Van Den Heuvel, "Blockchains: a Systematic Multivocal Literature Review", *ACM Comput Surv*, c. 53, sy 3, Kas. 2019, doi: 10.1145/3369052.

[9] L. Zhang, X. Ma, ve Y. Liu, "SoK: Blockchain Decentralization", May. 2022, Erişim: 12 Mayıs 2024. [Çevrimiçi]. Erişim adresi: https://arxiv.org/abs/2205.04256v6

[10] I. A. Reshi ve S. Sholla, "The blockchain conundrum: An in-depth examination of challenges, contributing technologies, and alternatives", *Concurr Comput*, c. 36, sy 8, s. e7987, Nis. 2024, doi: 10.1002/CPE.7987.

[11] J. Partala, "Provably Secure Covert Communication on Blockchain", *Cryptography 2018, Vol. 2, Page 18*, c. 2, sy 3, s. 18, Ağu. 2018, doi: 10.3390/cryptography2030018.

[12] L. Ghiro *vd.*, "A blockchain definition to clarify its role for the internet of things", *2021 19th Mediterranean Communication and Computer Networking Conference, MedComNet 2021*, 2021, doi: 10.1109/MedComNet52149.2021.9501280.

[13] S. Secinaro, F. Dal Mas, V. Brescia, ve D. Calandra, "Blockchain in the accounting, auditing and accountability fields: a bibliometric and coding analysis", *Accounting, Auditing and Accountability Journal*, c. 35, sy 9, ss. 168-203, 2021, doi: 10.1108/AAAJ-10-2020-4987.

[14] N. Ajienka, P. Vangorp, ve A. Capiluppi, "An empirical analysis of source code metrics and smart contract resource consumption", *Journal of Software: Evolution and Process*, c. 32, sy 10, s. e2267, Eki. 2020, doi: 10.1002/SMR.2267.

[15] E. Tijan, S. Aksentijević, K. Ivanić, ve M. Jardas, "Blockchain Technology Implementation in Logistics", *Sustainability 2019, Vol. 11, Page 1185*, c. 11, sy 4, s. 1185, Şub. 2019, doi: 10.3390/SU11041185.

[16] M. Cheng, G. Liu, Y. Xu, ve M. Chi, "When Blockchain Meets the AEC Industry: Present Status, Benefits, Challenges, and Future Research Opportunities", *Buildings 2021, Vol. 11, Page 340*, c. 11, sy 8, s. 340, Ağu. 2021, doi: 10.3390/buildings11080340.

[17] M. Gupta, R. B. Patel, S. Jain, H. Garg, ve B. Sharma, "Lightweight branched blockchain security framework for Internet of Vehicles", *Transactions on Emerging Telecommunications Technologies*, c. 34, sy 11, s. e4520, Kas. 2023, doi: 10.1002/ETT.4520.

[18] O. Ali, A. Jaradat, A. Kulakli, ve A. Abuhalimeh, "A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities", *IEEE Access*, c. 9, ss. 12730-12749, 2021, doi: 10.1109/ACCESS.2021.3050241.

[19] A. Pal, C. K. Tiwari, ve A. Behl, "Blockchain technology in financial services: a comprehensive review of the literature", *Journal of Global Operations and Strategic Sourcing*, c. 14, sy 1, ss. 61-80, Mar. 2021, doi: 10.1108/JGOSS-07-2020-0039.

[20] T. Ko, J. Lee, ve D. Ryu, "Blockchain Technology and Manufacturing Industry: Real-Time Transparency and Cost Savings", *Sustainability 2018, Vol. 10, Page 4274*, c. 10, sy 11, s. 4274, Kas. 2018, doi: 10.3390/SU10114274.

[21] G. Chen, B. Xu, M. Lu, ve N.-S. Chen, "Exploring blockchain technology and its potential applications for education", *Smart Learning Environments 2018 5:1*, c. 5, sy 1,

ss. 1-10, Oca. 2018, doi: 10.1186/S40561-017-0050-X.

[22] A. Younas ve M. Al Wahaibi, "Exploration of Blockchain Technology in the Education Sector in the Sultanate of Oman", *International Journal of Academic Research in Business and Social Sciences*, c. 13, sy 4, Nis. 2023, doi: 10.6007/IJARBSS/V13-I4/15889.

[23] L. Wang, C. Qi, P. Jiang, ve S. Xiang, "The Impact of Blockchain Application on the Qualification Rate and Circulation Efficiency of Agricultural Products: A Simulation Analysis with Agent-Based Modelling", *International Journal of Environmental Research and Public Health 2022, Vol. 19, Page 7686*, c. 19, sy 13, s. 7686, Haz. 2022, doi: 10.3390/IJERPH19137686.

[24] S. Ahluwalia, R. V. Mahto, ve M. Guerrero, "Blockchain technology and startup financing: A transaction cost economics perspective", *Technol Forecast Soc Change*, c. 151, s. 119854, Şub. 2020, doi: 10.1016/J.TECHFORE.2019.119854.

[25] C. Peng, Z. Liu, F. Wen, J. Y. Lee, ve F. Cui, "Research on Blockchain Technology and Media Industry Applications in the Context of Big Data", *Wirel Commun Mob Comput*, c. 2022, 2022, doi: 10.1155/2022/3038436.

[26] Y. Wang, M. Singgih, J. Wang, ve M. Rit, "Making sense of blockchain technology: How will it transform supply chains?", *Int J Prod Econ*, c. 211, ss. 221-236, May. 2019, doi: 10.1016/J.IJPE.2019.02.002.

[27] U. Jafar, M. Juzaiddin, A. Aziz, Z. Shukur, J. Wu, ve H. Wang, "Blockchain for Electronic Voting System—Review and Open Research Challenges", *Sensors 2021, Vol. 21, Page 5874*, c. 21, sy 17, s. 5874, Ağu. 2021, doi: 10.3390/S21175874.

[28] A. Moatari-Kazerouni, D. R. Pai, A. E. Chicas, ve A. Keramati, "How blockchain technology supports the business processes of clinical trials: a systematic review", *Business Process Management Journal*, c. 30, sy 2, ss. 388-410, Nis. 2024, doi: 10.1108/BPMJ-04-2023-0301.

[29] T. T. Kuo, H. E. Kim, ve L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications", *Journal of the American Medical Informatics Association*, c. 24, sy 6, ss. 1211-1220, Kas. 2017, doi: 10.1093/JAMIA/OCX068.

[30] A. Panigrahi, A. K. Nayak, ve R. Paul, "HealthCare EHR: A Blockchain-Based Decentralized Application", *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJISSCM.290017*, c. 15, sy 3, ss. 1-15, Oca. 1M.S., doi: 10.4018/IJISSCM.290017.

[31] H. W. Jang, H. S. Jung, ve M. Cho, "Blockchain adoption in the food and beverage industry from a behavioral reasoning perspective: moderating roles of supply chain partnerships", *Journal of Hospitality and Tourism Technology*, c. 15, sy 1, ss. 138-155, Oca. 2024, doi: 10.1108/JHTT-01-2023-0020.

[32] M. Damar, "Dijital Çağda Bilişim Sektörünün İhtiyacı Olan Yetkinlikler Üzerine Bir Değerlendirme", *Journal of Information Systems and Management Research*, c. 4, sy 1, ss. 25-40, 2022, [Çevrimiçi]. Erişim adresi: https://dergipark.org.tr/en/pub/jismar/issue/70966/1112479

[33] S. Kummer, D. M. Herold, M. Dobrovnik, J. Mikl, ve N. Schäfer, "A Systematic Review of Blockchain Literature in Logistics and Supply Chain Management: Identifying Research Questions and Future Directions", *Future Internet 2020, Vol. 12, Page 60*, c. 12, sy 3, s. 60, Mar. 2020, doi: 10.3390/FI12030060.

[34] J. Schmitz ve G. Leoni, "Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda", *Australian Accounting Review*, c. 29, sy 2, ss. 331-342, Haz. 2019, doi: 10.1111/AUAR.12286.

[35] E. Bonsón ve M. Bednárová, "Blockchain and its implications for accounting and auditing", *Meditari Accountancy Research*, c. 27, sy 5, ss. 725-740, Eki. 2019, doi: 10.1108/MEDAR-11-2018-0406.

[36] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, ve V. Santamaría, "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?", *Future Internet 2018, Vol. 10, Page 20*, c. 10, sy 2, s. 20, Şub. 2018, doi: 10.3390/FI10020020.

[37] I. Erol *vd.*, "Assessing the feasibility of blockchain technology in industries: evidence from Turkey", *Journal of Enterprise Information Management*, c. 34, sy 3, ss. 746-

769, Nis. 2021, doi: 10.1108/JEIM-09-2019-0309/FULL/PDF.

[38] K. G. Gülen ve A. Karaağaç, "Agricultural Food Supply Chain with Blockchain Technology: A Review On Turkey", *Journal of Global Strategic Management*, 2024, doi: 10.20460/jgsm.2023.314.

[39] Y. E. Kahraman, "Finance of the Digital Age: Cryptocurrencies", *Evoluation of Financial Markets 2*, Haz. 2023, doi: 10.58830/OZGUR.PUB105.C644.

[40] M. Ozturan, I. Atasu, ve H. Soydan, "Assessment of Blockchain Technology Readiness Level of Banking Industry: Case of Turkey", 2019.

[41] V. Chittipaka, S. Kumar, U. Sivarajah, J. L. H. Bowden, ve M. M. Baral, "Blockchain Technology for Supply Chains operating in emerging markets: an empirical examination of technology-organization-environment (TOE) framework", *Annals of Operations Research 2022 327:1*, c. 327, sy 1, ss. 465-492, Tem. 2022, doi: 10.1007/S10479-022-04801-5.

[42] A. Upadhyay, S. Mukhuty, V. Kumar, ve Y. Kazancoglu, "Blockchain technology and the circular economy: Implications for sustainability and social responsibility", *J Clean Prod*, c. 293, 2021, doi: 10.1016/j.jclepro.2021.126130.

[43] E. Yontar, "Critical success factor analysis of blockchain technology in agri-food supply chain management: A circular economy perspective", *J Environ Manage*, c. 330, 2023, doi: 10.1016/j.jenvman.2022.117173.

[44] I. Erol, I. Murat Ar, I. Peker, ve C. Searcy, "Alleviating the Impact of the Barriers to Circular Economy Adoption Through Blockchain: An Investigation Using an Integrated MCDM-based QFD With Hesitant Fuzzy Linguistic Term Sets", *Comput Ind Eng*, c. 165, 2022, doi: 10.1016/j.cie.2022.107962.

[45] A. Yildizbasi, "Blockchain and renewable energy: Integration challenges in circular economy era", *Renew Energy*, c. 176, 2021, doi: 10.1016/j.renene.2021.05.053.

[46] I. Erol, I. Peker, I. M. Ar, İ. Turan, ve C. Searcy, "Towards a circular economy: Investigating the critical success factors for a blockchain-based solar photovoltaic energy ecosystem in Turkey", *Energy for Sustainable Development*, c. 65, 2021, doi: 10.1016/j.esd.2021.10.004.

[47] H. B. Mahajan, "Emergence of Healthcare 4.0 and Blockchain into Secure Cloud-based Electronic Health Records Systems: Solutions, Challenges, and Future Roadmap", *Wireless Personal Communications*, c. 126, sy 3. 2022. doi: 10.1007/s11277-022-09535-y.

[48] U. Demirbaga ve G. S. Aujla, "MapChain: A Blockchain-Based Verifiable Healthcare Service Management in IoT-Based Big Data Ecosystem", *IEEE Transactions on Network and Service Management*, c. 19, sy 4, 2022, doi: 10.1109/TNSM.2022.3204851.

[49] M. V. Baysal, Ö. Özcan-Top, ve A. Betin-Can, "Blockchain technology applications in the health domain: a multivocal literature review", *Journal of Supercomputing*, c. 79, sy 3, 2023, doi: 10.1007/s11227-022-04772-1.

[50] M. Golec *vd.*, "BlockFaaS: Blockchain-enabled Serverless Computing Framework for AI-driven IoT Healthcare Applications", *J Grid Comput*, c. 21, sy 4, 2023, doi: 10.1007/s10723-023-09691-w.

[51] A. A. Zaidan, H. A. Alsattar, S. Qahtan, M. Deveci, D. Pamucar, ve B. B. Gupta, "Secure Decision Approach for Internet of Healthcare Things Smart-System-Based Blockchain", *IEEE Internet Things J*, c. 10, sy 24, 2023, doi: 10.1109/JIOT.2023.3308953.

[52] M. O. Başar, "Smart Contracts and the Problems Likely to Appear in the Field of Private Law Regarding Its Possible Implementation", *Istanbul Law Review*, c. 80, sy 4, ss. 1067-1103, Ara. 2022, doi: 10.26650/MECMUA.2022.80.4.0001.

[53] M. S. Cekin, "Blockchain Technology and Smart Contracts in terms of Law of Obligations and Data Protection Law", *ISTANBUL HUKUK MECMUASI*, c. 77, sy 1, 2019.

[54] S. Seven, G. Yao, A. Soran, A. Onen, ve S. M. Muyeen, "Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts", *IEEE Access*, c. 8, 2020, doi: 10.1109/ACCESS.2020.3026180.

[55] B. D. Deebak ve F. AL-Turjman, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements", *Journal of Information Security and Applications*, c. 58, 2021, doi: 10.1016/j.jisa.2021.102749.

[56] E. Demirel, S. Karagöz Zeren, ve K. Hakan, "Smart contracts in tourism industry: a model with blockchain integration for post pandemic economy", *Current Issues in Tourism*, c. 25, sy 12, 2022, doi: 10.1080/13683500.2021.1960280.

[57] S. Ahmadisheykhsarmast, S. G. Senji, ve R. Sonmez, "Decentralized tendering of construction projects using blockchain-based smart contracts and storage systems", *Autom Constr*, c. 151, 2023, doi: 10.1016/j.autcon.2023.104900.

[58] E. Çalık, H. Kaya, ve F. V. Çelebi, "A novel method to ensure the security of the shared medical data using smart contracts: Organ transplantation sample", içinde *Concurrency and Computation: Practice and Experience*, 2022. doi: 10.1002/cpe.6752.

[59] H. Kunkcu, K. Koc, A. P. Gurgun, ve H. H. Dagou, "Operational Barriers against the Use of Smart Contracts in Construction Projects", *Turkish Journal of Civil Engineering*, c. 34, sy 5, 2023, doi: 10.18400/tjce.1322972.

[60] J. Li, M. S. Herdem, J. Nathwani, ve J. Z. Wen, "Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management", *Energy and AI*, c. 11. 2023. doi: 10.1016/j.egyai.2022.100208.

[61] R. Ben Ayed, M. Hanana, S. Ercisli, R. Karunakaran, A. Rebai, ve F. Moreau, "Integration of Innovative Technologies in the Agri-Food Sector: The Fundamentals and Practical Case of DNA-Based Traceability of Olives from Fruit to Oil", *Plants*, c. 11, sy 9. 2022. doi: 10.3390/plants11091230.

[62] A. Hassoun *vd.*, "Food traceability 4.0 as part of the fourth industrial revolution: key enabling technologies", *Critical Reviews in Food Science and Nutrition*, c. 64, sy 3. 2024. doi: 10.1080/10408398.2022.2110033.

[63] A. Hassoun *vd.*, "Implementation of relevant fourth industrial revolution innovations across the supply chain of fruits and vegetables: A short update on Traceability 4.0", *Food Chem*, c. 409, 2023, doi: 10.1016/j.foodchem.2022.135303.

[64] J. Liu, J. Lv, H. Dinçer, S. Yüksel, ve H. Karakuş, "Selection of Renewable Energy Alternatives for Green Blockchain Investments: A Hybrid IT2-based Fuzzy Modelling", *Archives of Computational Methods in Engineering*, c. 28, sy 5, 2021, doi: 10.1007/s11831-020-09521-2.

[65] I. Erol, I. O. Neuhofer, T. Dogru (Dr. True), A. Oztel, C. Searcy, ve A. C. Yorulmaz, "Improving sustainability in the tourism industry through blockchain technology: Challenges and opportunities", *Tour Manag*, c. 93, 2022, doi: 10.1016/j.tourman.2022.104628.

[66] M. Y. Başer, T. Büyükbeşe, ve M. Kizildag, "What if we could travel without passport? First sight to blockchain-based identity management in tourism", *Asia Pacific Journal of Tourism Research*, c. 28, sy 4, 2023, doi: 10.1080/10941665.2023.2229922.

[67] B. Aslan ve K. Ataşen, "COVID-19 Information Sharing with Blockchain", *Information Technology and Control*, c. 50, sy 4, 2021, doi: 10.5755/j01.itc.50.4.29064.

[68] Y. Kazancoglu, M. Ozbiltekin-Pala, M. D. Sezer, S. Luthra, ve A. Kumar, "Resilient reverse logistics with blockchain technology in sustainable food supply chain management during COVID-19", *Bus Strategy Environ*, c. 32, sy 4, 2023, doi: 10.1002/bse.3251.

[69] C. Liv, "İslâm Hukuku Açısından NFT Ve Metaverse Ürünlerin Satım Sözleşmesine Konu Olması", *Dinbilimleri Akademik Araştırma Dergisi*, c. 22, sy 2, 2022, doi: 10.33415/daad.1117984.

[70] M. Selcuk ve S. Kaya, "A Critical Analysis of Cryptocurrencies from an Islamic Jurisprudence Perspective", *Turkish Journal of Islamic Economics*, c. 8, sy 1, 2021, doi: 10.26414/a130.

[71] N. Kahveci ve Y. Bilginer, "Çağdaş İslâm Hukukçularının Kripto Paraların Meşruiyetine Dair Görüşlerinin Analizi", *Şırnak Üniversitesi İlahiyat Fakültesi Dergisi*, sy 26, 2021, doi: 10.35415/sirnakifd.894874.

[72] G. Ozdagoglu, M. Damar, ve A. Ozdagoglu, "The State of the Art in Blockchain Research (2013–2018): Scientometrics of the Related

Papers in Web of Science and Scopus", içinde *Contributions to Management Science*, 2020. doi: 10.1007/978-3-030-29739-8_27.

[73] A. Khatoon, P. Verma, J. Southernwood, B. Massey, ve P. Corcoran, "Blockchain in Energy Efficiency: Potential Applications and Benefits", *Energies 2019, Vol. 12, Page 3317*, c. 12, sy 17, s. 3317, Ağu. 2019, doi: 10.3390/EN12173317.

[74] M. N. Kamel Boulos, J. T. Wilson, ve K. A. Clauson, "Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare", *Int J Health Geogr*, c. 17, sy 1, ss. 1-10, Tem. 2018, doi: 10.1186/s12942-018-0144-x.

[75] Y. Xiao, Z. Liu, B. Gong, ve W. Yan, "Research on the Development Trend of Block-Chain Audit Theory——Based on CiteSpace V Analysis", Şub. 2023, doi: 10.4108/EAI.18-11-2022.2326765.

[76] A. Kumar Bhardwaj, A. Garg, ve Y. Gajpal, "Determinants of Blockchain Technology Adoption in Supply Chains by Small and Medium Enterprises (SMEs) in India", *Math Probl Eng*, c. 2021, 2021, doi: 10.1155/2021/5537395.

[77] A. Rijanto, "Business financing and blockchain technology adoption in agroindustry", *Journal of Science and Technology Policy Management*, c. 12, sy 2, ss. 215-235, 2020, doi: 10.1108/JSTPM-03-2020-0065.

[78] F. R. Batubara, J. Ubacht, ve M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review", *ACM International Conference Proceeding Series*, May. 2018, doi: 10.1145/3209281.3209317.

[79] M. Cheng ve H. Y. Chong, "Understanding the Determinants of Blockchain Adoption in the Engineering-Construction Industry: Multi-Stakeholders' Analyses", *IEEE Access*, c. 10, ss. 108307-108319, 2022, doi: 10.1109/ACCESS.2022.3213714.

[80] O. Bayram, I. Talay, ve M. Feridun, "Can Fintech Promote Sustainable Finance? Policy Lessons from the Case of Turkey", *Sustainability 2022, Vol. 14, Page 12414*, c. 14, sy 19, s. 12414, Eyl. 2022, doi: 10.3390/SU141912414.

[81] Y. Toraman, "Interest-Free Finance Model by Using Blockchain-Based Company Tokens: Research on Digital Turkish Lira (DTL) and Borsa Istanbul with Technology Acceptance Model (TAM)", *EMAJ: Emerging Markets Journal*, c. 12, sy 2, ss. 56-66, Ara. 2022, doi: 10.5195/emaj.2022.275.

[82] S. Bag, D. A. Viktorovich, A. K. Sahu, ve A. K. Sahu, "Barriers to adoption of blockchain technology in green supply chain management", *Journal of Global Operations and Strategic Sourcing*, c. 14, sy 1, ss. 104-133, Mar. 2021, doi: 10.1108/JGOSS-06-2020-0027.

[83] Y. Gökşen ve M. Damar, "Yeşil Bilişim Yaklaşımıyla Kullanıcı Ve Kurum Odaklı Enerji Yönetim Sistemi", *Deu Muhendislik Fakultesi Fen ve Muhendislik*, c. 20, sy 58, 2018, doi: 10.21205/deufmd.2018205821.

[84] M. Damar, O. Doğan, ve Y. Gökşen, "Yeşil Bilişim: Bir Kamu Kurumu Örneği Ve Politika Önerileri", *Ege Akademik Bakis (Ege Academic Review)*, c. 16, sy 4, 2016, doi: 10.21121/eab.2016.478.

[85] M. O. Grida, S. Abd Elrahman, ve K. A. Eldrandaly, "Critical Success Factors Evaluation for Blockchain's Adoption and Implementing", *Systems 2023, Vol. 11, Page 2*, c. 11, sy 1, s. 2, Ara. 2022, doi: 10.3390/systems11010002.

[86] B. Baytemir Kontacı, "'Terörizmin Finansmanının Bir Aracı Olarak Kripto Paralar'", içinde *Karşılaştırmalı Hukukta ve Türk Hukukunda Terörizm, Terör Suçları ve İnfaz Hukuku Cilt 1*, 2023. doi: 10.53478/tuba.978-625-8352-88-7.ch17.

[87] M. Damar, G. Özdağoğlu, ve A. Özdağoğlu, "Küresel Ölçekte Yazılım Kalitesi ve Standartları: Sektörel ve Bilimsel Perspektiften Literatürdeki Eğilimler", *Alphanumeric Journal*, c. 6, sy 2, 2018, doi: 10.17093/alphanumeric.404102.

[88] M. Damar ve G. Ozdagoglu, "Yazılım Sektörü ve Uluslararasılaşma, Politika Önerileri (Software Industry and Internationalization, Policy Recommendations)". [Çevrimiçi]. Erişim adresi: https://www.researchgate.net/publication/354511095

[89] M. Damar, "Dijital Dünyanın Dünü, Bugünü ve Yarını: Bilişim Sektörünün Gelişimi Üzerine Değerlendirme", *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi*, c. 12, sy Dijitalleşme, 2022, doi: 10.30783/nevsosbilen.1121818.

[90] D. Cahyadi, A. Faturahman, H. Haryani, E. Dolan, ve S. millah, "RETRACTED (ditarik) : BCS : Blockchain Smart Curriculum System for Verification Student Accreditation", *International Journal of Cyber and IT Service Management*, c. 1, sy 1, ss. 65-83, Nis. 2021, doi: 10.34306/IJCITSM.V1I1.20.

[91] M. Kataev ve L. Bulysheva, "Blockchain system in the higher education: Storing academical students' records and achievements accumulated in the educational process", *Syst Res Behav Sci*, c. 39, sy 3, ss. 589-596, May. 2022, doi: 10.1002/SRES.2872.

[92] C. Reis-Marques *vd.*, "Applications of Blockchain Technology to Higher Education Arena: A Bibliometric Analysis", *European Journal of Investigation in Health, Psychology and Education 2021, Vol. 11, Pages 1406-1421*, c. 11, sy 4, ss. 1406-1421, Kas. 2021, doi: 10.3390/EJIHPE11040101.

[93] R. Q. Castro ve M. Au-Yong-oliveira, "Blockchain and Higher Education Diplomas", *European Journal of Investigation in Health, Psychology and Education 2021, Vol. 11, Pages 154-167*, c. 11, sy 1, ss. 154-167, Şub. 2021, doi: 10.3390/EJIHPE11010013.