Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, 2. Uluslararası Güvenlik Kongresi Özel Sayısı (İstihbarat ve Güvenlik), 175-194, doi:10.28956/gbd.1016087

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, The Special Issue of the 2nd International Security Congress (Intelligence & Security), 175-194, doi:10.28956/gbd.1016087

Makale Türü ve Başlığı / Article Type and Title
Konferans Bildirisi / Conference Paper
Blok Zincirinin (Blockchaın) Literatür Büyümesi Işığında Yeni Siber Güvenlik Arayışları.
New Search for Cyber Securıty in the Light of Blockchaın's Literature Expansion

Yazar(lar) / Writer(s)
1- Dr. Öğr. Gör. Mürsel DOĞRUL, Necmettin Erbakan Üniversitesi, mdogrul@erbakan.edu.tr, ORCID: 0000-0002-0637-843X
2- Ahmet ERĞURUM, Bilkent Üniversitesi, Yüksek Lisans Öğrencisi, ahmet.ergurum@bilkent.edu.tr, ORCID: 0000-0003-2995-4927

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur
-Bu makalede araştırma ve yayın etiğine uyulmuştur.
-23-25 Eylül 2021 tarihlerinde Jandarma ve Sahil Güvenlik Akademisi'nde icra edilen 2. Uluslararası Güvenlik Kongresi'nde sunulan tebliğin genişletilmiş halidir.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 28.10.2021
Makale Kabul Tarihi / Accepted : 23.12.2021

Atıf Bilgisi / Citation:
Doğrul, M. ve Erğurum, A. (2021). Blok Zincirinin (Blockchaın) Literatür Büyümesi Işığında Yeni Siber Güvenlik Arayışları, Güvenlik Bilimleri Dergisi, 2. Uluslararası Güvenlik Kongresi Özel Sayısı (İstihbarat ve Güvenlik), ss175-194, doi:10.28956/gbd.1016087

BLOK ZİNCİRİNİN (BLOCKCHAIN) LİTERATÜR BÜYÜMESİ IŞIĞINDA YENİ SİBER GÜVENLİK ARAYIŞLARI

Öz

Bu çalışma, blok zinciri teknolojisi ve devletlerin güvenlik politikaları arasındaki ilişkiyi Web of Science verilerinin bibliyometrik analizi ışığında incelemektedir. Verilere göre Çin, Blok zinciri üzerine yapılan çalışmaların %30'unu üreterek başı çekmiştir. ABD, Çin'i %19 ile izlemektedir. Blok zinciri teknolojisine artan ilgi, devletlerin güvenlik politikalarına da yansımaktadır. Büyük güçler blok zinciri teknolojisini aralarındaki rekabette üstünlük sağlayacak unsur olarak kabul etmektedirler. Nitekim, bu çalışma, blok zincirinin kullanımına ilişkin Amerikan, Çin ve Rus politikalarına odaklanmaktadır. Çalışmada politik söylemlere, resmî belgelere, akademik raporlara ve makalelere dayanarak blok zincirinin yükselişiyle ortaya çıkan yeni güvenlik boyutları analiz edilmeye çalışılmaktadır. ABD'nin blok zinciri politikası, temel olarak terör gruplarının bağış toplama kampanyalarını takip etme, kendi askerî lojistik maliyetlerini düşürme ve uluslararası sistemdeki başat pozisyonunu güçlendirme üzerine şekillenmektedir. Çin'in politikaları, dijital merkez bankacılık sistemini kurmayı ve ordusunu yenilemeyi amaçlamaktadır. Rusya'nın blok zinciri üzerine araştırma ve politikalarını ise siber güvenlik konusundaki endişeleri şekillendirmektedir.

Anahtar Kelimeler*; Siber Güvenlik, Blok Zinciri Sistemi, Veri Madenciliği, İstihbarat Birimleri, Kripto Para.*

NEW SEARCH FOR CYBER SECURITY IN THE LIGHT OF BLOCKCHAIN'S LITERATURE EXPANSION

Abstract

This study examines the nexus between blockchain technology and states' security policies in light of the bibliometric analysis of Web of Science data. The data reveals that China pioneers publications on blockchain technology, which amounts to 30% of the works. The U.S.A. follows China with 19%. The rising attention to blockchain technology is reflected on the states' security policies. Great powers regarded Blockchain technology as a factor that can provide them with superiority in the power competition. Thus, this study focuses on the American, Chinese and Russian policies on the use of Blockchain. Based on the political discourses, official documents, academic reports, and articles, it is aimed to analyse the new security dimensions appearing with the rise of Blockchain. The U.S. policy on the Blockchain is mainly shaped by surveillance of the use of Blockchain by terror groups for fundraising, decreasing military logistics costs, and reinforcing its place in the international system. China's policies aim to improve its military's digital central banking system and military innovation. Russia's concerns over cyber security mold Russian formulates its researches and policies regarding Blockchain.

Keywords; *Cybersecurity, Blockchain System, Data Mining, Intelligence Units, Cryptocurrency.*

GİRİŞ

Soğuk Savaş'ın sona ermesiyle beraber güvenlik kavramının boyutları eleştirel güvenlik yaklaşımları ile çeşitlendiği söylense de Pınar Bilgin güvenlik kavramının kapsamının sorgulanmasını 1980'lerin öncesine götürmektedir (Bilgin, 2010). Çünkü güvenlik araştırmaları 1983'de ciddi bir literatüre dönüşmüş, Buzan'ın "İnsanlar, Devletler ve Korku" kitabı (Buzan, 1983) ve Richard H. Ullman'ın (1983) "Güvenliği Yeniden Tanımlama" makalesi ile güvenlik kavramı askerî alanın dışına çıkartılmıştır. Soğuk Savaş'ın sonlarına doğru güvenlik kavramına dair çalışmalarıyla öne çıkan Jessica Tuchman Mathews (1989) nüfus ve çevresel etkenler özelinde, Theodore Moran (1990) ekonomik konular özelinde ve Brad Roberts (1990) ise insan hakları özelinde güvenlik kavramını irdelemişlerdir. Böylece güvenlik meselelerine klasik/askerî yaklaşımın yerini enerji arz güvenliği, çevre güvenliği ve siber güvenlik gibi başlıklar almaya başlamıştır (European Commission, 2017).

Son 20 yıldır siber güvenliğin temel sorunsalları, devletlerin kendi bireylerinin bilgilerini güvenilir bir şekilde depolama yöntemleri üzerine odaklanmıştır (Ghanea-Hercock, 2012). Bu sırada hâlen en büyük güvenlik endişesi elbette savaşlar kabul edilirken Elon Musk, Stephen Hawking ve Bill Gates gibi büyük teknoloji firmalarının yöneticileri ve bilim insanları yıllardır kamuoyunun dikkatini konvansiyonel savaşlar ve füze krizleri yerine nanoteknoloji, siber virüsler ve yapay zekâ gibi başlıklara çekme çabalarını sürdürmüşlerdir (Culbertson, 2018).

1983 yılında her şey doğru olmayan bir radar okuması ile savaşa dönüşebilecekken Sovyet Yarbay Stanislav Petrov (1939-2017) ABD nükleer saldırısına ilişkin yanlış bilgisayar uyarılarını görmezden gelerek ABD ile SSCB arasında bir nükleer savaşı önlemişti. Günümüzdeki teknolojik donanım ve veri düzeninde benzer bir senaryo ile savaş sistemlerinin ele geçirilmesi ve doğru olmayan radar verilerinin gönderilme ihtimali pek muhtemel kabul edilmez. Ancak Londra merkezli *Royal Institute of International Affairs* (*Chatham House* olarak da bilinir), Ocak 2018 tarihli bir raporunda ABD ve İngiltere başta olmak üzere nükleer silaha sahip ülkelerin nükleer silah sistemlerinin siber saldırılara karşı giderek daha savunmasız hâle geldiğine yer vermiştir (Adams, 2019).

Cybersecurity Ventures verilerine göre ise küresel siber güvenlik harcamalarının 2017 ile 2021 arasında 1 trilyon doları aşacağı tahmin edilmektedir. Bu inanılmaz giderlere rağmen birçok teknoloji uzmanı, önlemlerin saldırıları önlemede büyük ölçüde başarısız olacağını tahmin ediyor (Culbertson, 2018). Siber güvenlik konusundaki kaygı ve güvensizliklerin gün geçtikçe çeşitlendiği günümüzde (The

Third Prague 5G Security Conference, 2021), yeniliğin kalbi Silikon Vadisi'nden İnternet'i baştan başlayıp yeniden icat etme konusunda iddialı konuşmalar yapılmaya devam ediliyor (Metry, 2017). Bu tür yaklaşımların geri planındaki itici etkenin blok zinciri teknolojisi olması ise siber güvenlik ile blok zinciri teknolojilerinin olası etkileşimine dair mülahazaları beraberinde getirmektedir.

Son 20 yılın önde gelen güvenlik başlığı olarak siber güvenliğin temel sorusu, devletlerin kendi bireylerinin bilgilerini güvenilir bir şekilde depolama yöntemleri üzerine odaklanmıştır. Böylece siber alanın güvensiz tanımlanması ile güvenliğin algılanışı detaylandırılmış, konvansiyonel tehdit algıları dijital alanı da kaplayacak şekilde genişletilmiştir. Teknolojik gelişmeler ve toplumsal ihtiyaçlara binaen kapsam alanı sürekli genişleyen bir kavram olarak güvenlik, artık devleti sadece vatandaşını korumakla değil aynı zamanda bireylerinin verisini korumakla görevli ve dijital güvensizliği önleyici bir alana taşımıştır. Şimdi ise verinin merkeziyetçiliğini savunan bu siber güvenlik anlayışından blok zincirinin kriptografisi ile bir çıkış söz konusudur.

Blok zincirinin kriptografisi ciddi anlamda ilk kez 2017'de hızlı değer artışları sonrası gündeme gelen ve hâlen gündemdeki yerini koruyan Bitcoin gibi kripto paralar ile kendini büyük oranda duyurmuştur (Doğrul & Korkut, 2020). Siber güvenliğin yeni bir boyutunu getiren bu kriptografi ile verilerin tek bir merkezde toplanması yerine İnternet vasıtasıyla birçok farklı ve şifreli sunuculara serpilmiş şekilde tutulması mümkün hâle gelmiştir (Gray, 2018, s. 7). İşlemlerde güvenliği sağlayan kriptografisi ile blok zinciri teknolojisi, kullanıcılara dağıtılmış bir ağ üzerinden *(distributed ledger technology-DLT)* katılımla veride ademimerkeziyetçiliğin (yerel sunucuların yetkilerinin artırılmasını) sağlar. Blok zincirinde tek bir hata noktası yoktur ve tek bir kullanıcı işlem kaydını değiştiremez (IBM, 2021).

Dağıtılmış hâli ile blok zincirinin, "*finansal ve siber güvenliğin geleceğini teşkil edeceği", "uygulamalarda devrim yaratma ve dijital ekonomiyi yeniden tanımlama"* potansiyeline sahip olacağı ifade edilmiştir (Singh & Singh, 2016; Underwood, 2016). Netice itibarıyla tek merkezde tüm verilerin saklanması yöntemine verileri farklı merkezlerde kodlayarak gizleyen ve böylece daha güvenlikli bir çalışma mantığı getiren blok zinciri sistemsel olarak yenilik ve kullanılabilirlik açısından ülkelerin odağına girmiştir. Bu sistem ile birçok ülkenin kamu hizmetlerini bu yeni teknoloji vasıtasıyla gerçekleştirmeye başlayacağına yönelik çalışmalar artmıştır.

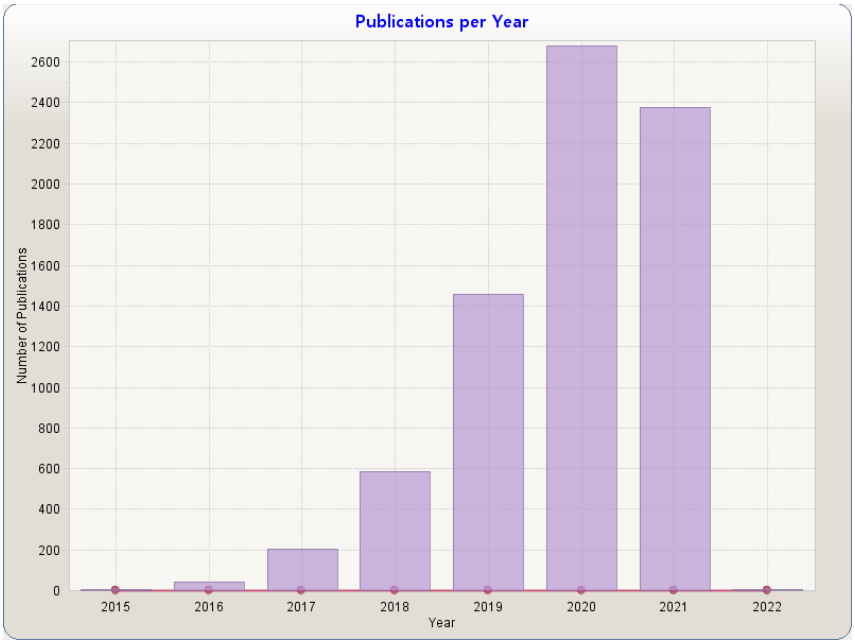
Bu çalışmada ilk olarak blok zinciri üzerine yapılan araştırmaların bibliyometrik analizi Web of Science veri tabanından elde edilen veriler ile yapılmaktadır. Ardından uluslararası sistemin üç büyük aktörü, ABD, Çin ve Rusya'nın blok zinciri teknolojisi üzerine ülke

stratejilerine yer verilmektedir. Bibliyometrik veriler, dünyanın önde gelen üç ülkesinin blok zinciri konusunda başatlığına işaret edecektir. Uygulamada da bu ülkelerin siber güvenlik düzlemindeki sorunlarının çözümü noktasında yükselen teknoloji olan blok zincirine yönelimlerinin geri planı sorgulanacaktır.

1. BLOK ZİNCİRİNİN LİTERATÜR BÜYÜMESİ

Yükselen bir teknoloji olarak tanımlanan blok zinciri üzerine Web of Science (WoS) bütün veri tabanlarında yapılan bibliyometrik veri taramasında[1] bilimsel yayınlarda 2015 yılından günümüze doğru doğrusal bir artış göze çarpmaktadır. Bu tarama, süper güçlerin blok zinciri konusuna eğilimini ve blok zinciri üzerine yapılan yayınlarda öne çıkan yönelim ve kümelenmeleri göstermesi açısından çalışmamızın çıkış noktasını teşkil etmektedir.

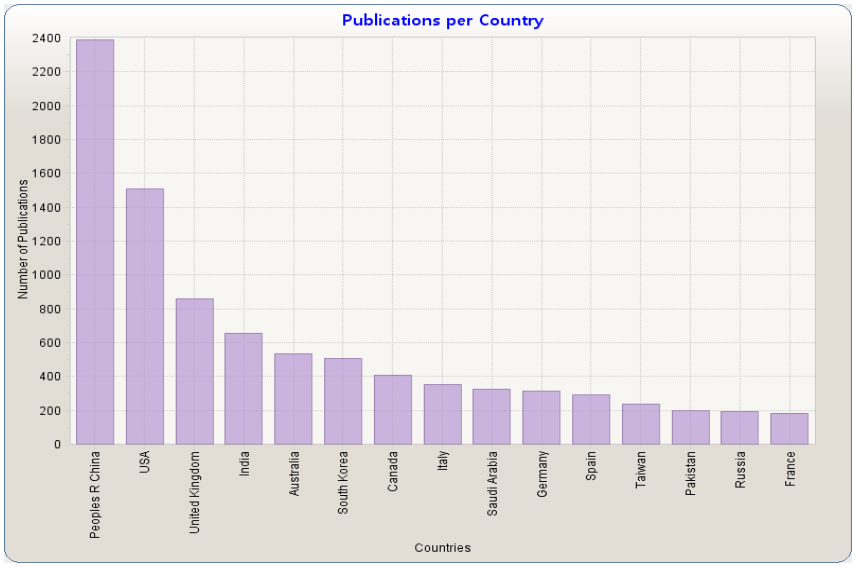
Grafik 1. Blok Zinciri Üzerine Yapılan Yayın Sayıları (Yıl bazında)



2015-2022 yılları için taranan veriye göre yıl bazlı literatür büyümesi sürekli artan bir eğilim göstermektedir.

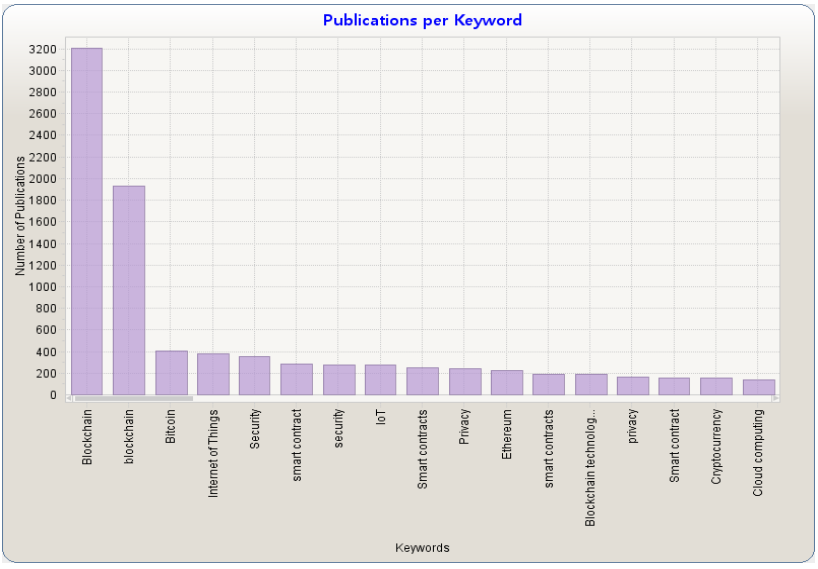
[1] Web of Science (WoS) bütün veri tabanlarında konu taraması gerçekleştirilmiştir. Sorgu ile ilgili detaylar şu şekildedir: TOPIC: (blockchain) Timespan: 2015-2022. Indexes: SCI-EXPANDED, SSCI, A&HCI, ESCI. Datalara erişim noktasında değerli katkılarından dolayı Doç. Dr. Haydar Yalçın'a teşekkürlerimizi sunarız.

Grafik 2. Blok Zinciri Üzerine Yapılan Yayın Sayıları (Ülke bazında)



Ülke bazlı literatür sayıları elde edilmiş ve 2400 yayın ile başı Çin çekerken onu 1500 yayın ile ABD ve 700 yayın ile Birleşik Krallık takip etmiştir.

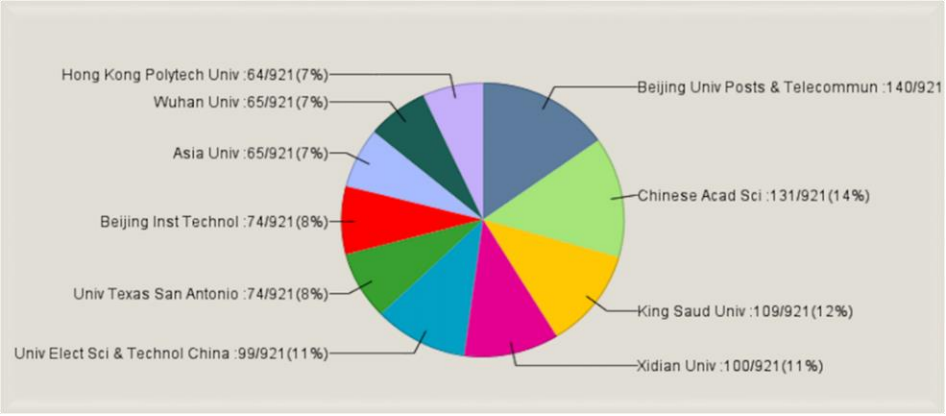
Grafik 3. Yayınların Anahtar Kelimelerine Göre Dağılımları



Grafik 3'e göre, blok zinciri üzerine yapılan yayınlarda anahtar kelimeler sıralanmıştır. Dördüncü sırada güvenlik (*security*) anahtar kelimesinin yer alması, bu konudaki yayınlarda

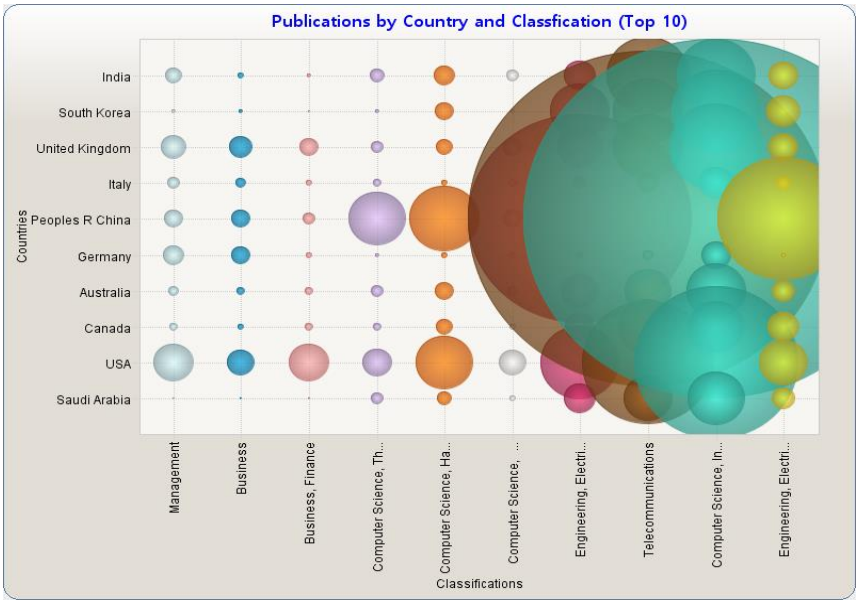
blok zinciri teknolojisinin güvenlik kelimesi ile ilişkilendirildiğini göstermesi açısından önemlidir.

Grafik 4. Yayınların Kurumsal Dağılımları



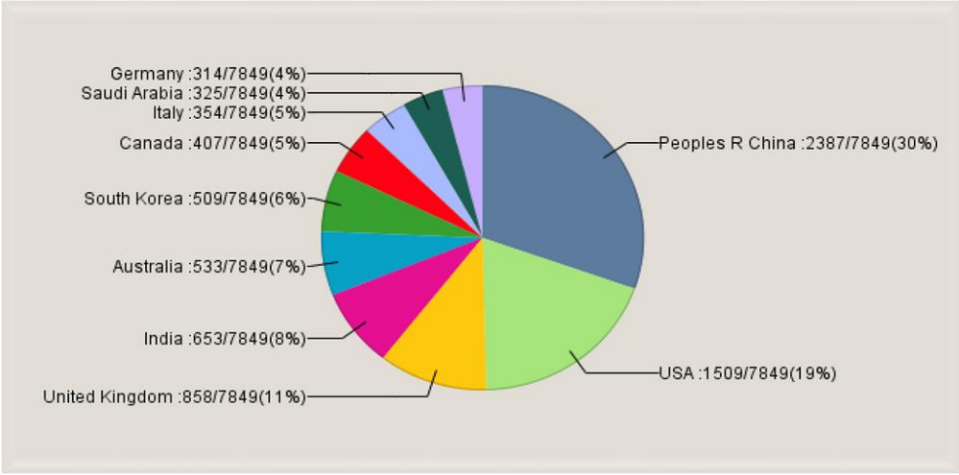
Yayınların yapıldığı kurumların yer aldığı Grafik 4'ter Çin'den *Beijing University of Posts and Telecommunications* %15 ile en fazla yayının yapıldığı yükseköğretim kurumu olmuştur. Bu kurumu takip eden diğer kurumlara bakıldığında Çin merkezli kurumların önemli bir yer tuttuğu görülmektedir.

Grafik 5. Ülkelere ve Kategorilerine Göre Yayınların Kümelenmesi



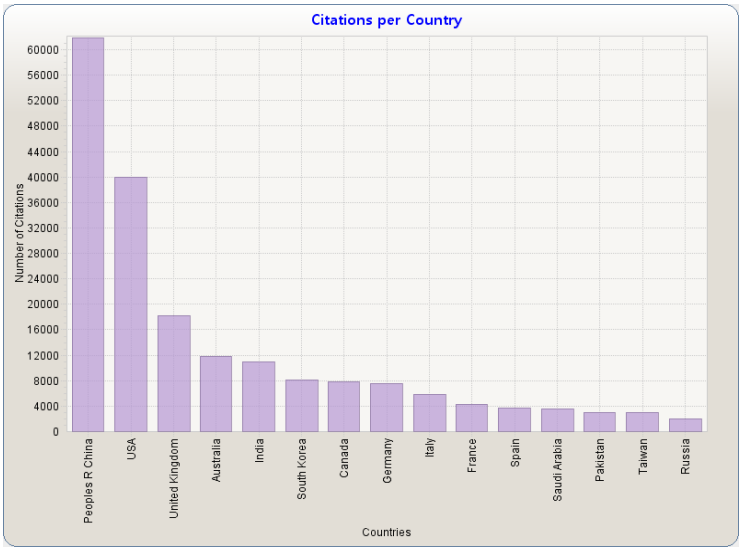
Grafik 5, blok zinciri üzerine yapılan yayınların iletişim, bilgisayar ve mühendislik konu başlıklarında yoğunlaştığını gösterirken Çin ve ABD'nin yanı sıra Almanya, Kanada ve Avustralya burada başı çekmiştir.

Grafik 6. Yayınların Ülkelere Göre Dağılımı



Grafik 6'ya göre blok zinciri üzerine yapılan yayınlarda ilk 10 ülke sıralanırken birincinin %30'luk bir oranla Çin olması ve ikinci sırada %19 ile ABD'nin yer alması dikkat çekicidir.

Grafik 7. Yayınlara Ülke Bazlı Yapılan Atıf Sayıları



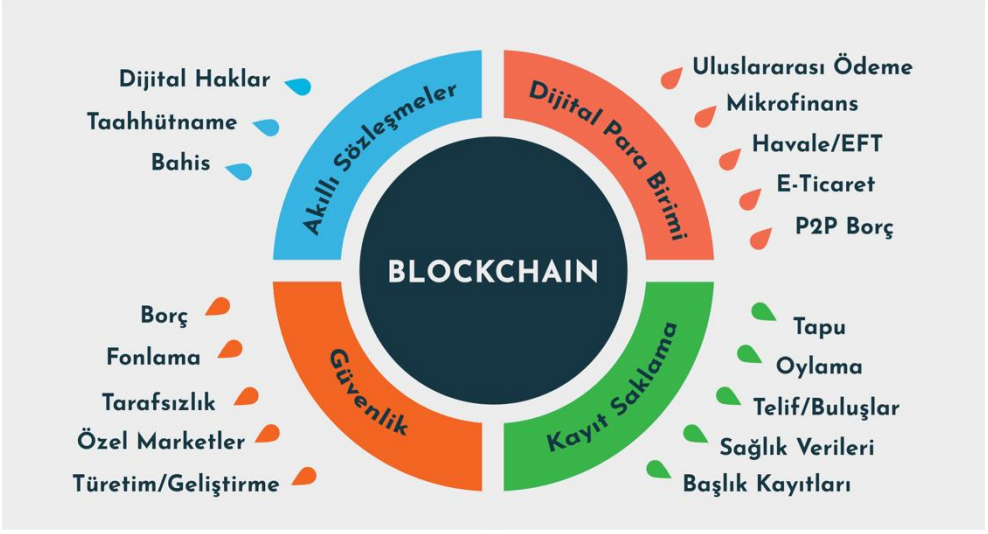
Grafik 7, blok zinciri konulu yayınlara yapılan atıflarda Çin 60.000 düzeyindeki atıf ile yayın sayısında olduğu gibi burada da başı çekmektedir. Onu 40.000 atıf ile ABD takip etmiştir.

Çinli araştırmacılar, "blok zinciri teknolojisi ve potansiyel askerî değeri" (Lin vd., 2016; Matisek, 2019) başlıklı makaleyi 2016 yılında yayımlamışlardır. 2015'den günümüze uzanan grafiklerde görülmüştür ki Çin, blok zinciri üzerine yapılan yayınlar ve atıflar konusunda diğer ülkelerin önünde yer alırken yine Çin'deki yükseköğretim kurumları ABD'dekiler ile beraber ana bilimsel içerik üreticileri olmuştur.

2. BLOK ZİNCİRİNİN KULLANIM ALANLARI VE GÜVENLİK

Her ne kadar kendisini kripto paralardaki jetonlaştırmanın geri planındaki sistem olarak duyursa da blok zinciri teknolojisi, lojistik, tedarik zinciri, sözleşmeler, veri alışverişi, komuta ve kontrol, terörist eylem ve olay veri takibi ve dijital varlıklara kadar birçok kullanım alanında şimdiden test edilmeye başlanmıştır. Ayrıca blok zinciri teknolojisi; bilgisayar bilimi, kriptografi ve finanstaki temelinin ötesinde uygulama geliştirmeyi, ekonomiyi, sağlığı, bankacılık sistemini, risk yönetimini, veri bilimini, eğitimi, hukuku, siyaset bilimini, psikolojiyi, etiği, sanatı ve sosyal bilimleri kapsayan çok çeşitli disiplinler bağlamında yeni kavramları beraberinde getirmektedir (Ducrée vd., 2021).

Şekil 1. Blok Zinciri Teknolojisinin Sektörel Düzeyde Kullanım Alanları (Ünal & Uluyol, 2020, s. 170)



Kullanımı somut olarak sağlık sistemi bağlamında örneklenecek olursa blok zinciri teknolojisinin sağladığı ağ üzerinden bir kişi dünyadaki herhangi bir tıbbi tesise gidebilir ve

herhangi bir ülkeden sağlık kayıtlarına erişme izni verebilir. Hasta kayıtlarının küçük bir kasabadaki bir doktorun muayenehanesinde ya da ülke çapında bir sistemde tutmak yerine, blok zinciri üzerinde tutarak yurt dışında tıbbi yardım almaya çalışırken ihtiyaç duyduğu anda verilerine erişilebilir (Wallace, 2016). Böylesi bir kullanım dünya çapındaki sağlık ekiplerine büyük bir destek sağlayacaktır.

Yenilikçi, dönüştürücü ve ilham verici olası kullanım alanlarına paralel blok zinciri teknolojisi büyük güçlerin odağına girmiştir (Green, 2021). ABD'nin küresel hegemonyasını koruması ve savunması için bu teknolojiye yatırım yapmasının gerekliliği Amerikan Ulusal Kongre'sinde birçok defa gündem olmuştur. Nitekim Kongre üyelerine, izinli ve özel blok zinciri ağlarının, dünya istihbarat teşkilatları veya askerî organizasyonları arasında veri paylaşım ve koordinasyon ortamları hâline gelebilmesinin an meselesi olduğu yönünde raporlar sunulmuştur (Brett, 2021). Bu ağlarda faaliyetlere girişen terör örgütlerinin, kara para aklayıcılarının ve uyuşturucu kartellerinin riskli faaliyetlerinin yine onların kullanmış olduğu blok zinciri teknolojileri ile takip edilebileceği söz konusu olmuştur.

Kripto paralar terör grupları tarafından yeni bir finansman kaynağı olarak suiistimal edilebilmektedir (Dion-Schwarz vd., 2019). 2013 yılında Devlet'ül Irak ve'ş Şam (DAEŞ)[2] terör örgütünün kripto paralar yoluyla bağış kampanyası yapması, terörle mücadeleye yeni bir boyut katmıştır (Lilly & Lilly, 2021). 2018'de Amerikan Kongre'sinde, terörizmin finansmanıyla mücadele bağlamında kripto paraları da içeren yeni finansal teknolojilerin kullanımının araştırılması gündeme gelmiştir (House Hearing, 2018). 2020 yılında ise Adalet Bakanlığı terörizmin siber kaynaklarının kesilmesi amacıyla 300'den fazla kripto para hesabının, çeşitli WEB sayfası ve Facebook hesaplarının tespit edildiğini belirtmiştir (U.S. Department of Justice, 2020).

ABD hegemon gücünü sürdürme ekseninde blok zinciri teknolojisinin önemini gündemine taşıyan ülkelerdendir. Zira kriptografik olarak korunmuş ve merkezî olmayan blok zinciri defterlerine erişim ayrıcalığı, ABD ve müttefiklerinin küresel hâkimiyetini güçlendirmesi muhtemeldir. Böylece siber uzaydaki tehlikeli sabotaj girişimlerinin etkisi azaltılmış ve açığa çıkartılmış olacaktır (U.S. Department of Defense, 2020). NASA tarafından yayımlanan raporda blok zinciri teknolojisinin siber güvenliğin artırılması, siber saldırıların önlenmesi ve havacılık bilgilerinin korunması gibi amaçlarla kullanılabileceği belirtilmiştir (Reisman, 2019).

Bibliyometrik analizlerde görüldüğü üzere blok zinciri konusunda en önemli aktör

[2] Bu terör örgütünü isimlendirirken DEAŞ, IŞİD, IŞTÖ ve ILTÖ gibi kısaltmalar da kullanılmaktadır ve bu çalışmada DAEŞ tercih edilmiştir.

olarak Çin, bu teknolojinin bilimsel kaynak üretiminin yanında donanımsal üretimi noktasında da son derece kararlı ve aktiftir. Çin Devlet Başkanı Xi Jinping 2019 yılının Ekim ayında, Komünist Parti yetkilileriyle yaptığı bir toplantıda blok zincirine daha fazla araştırma ve yatırım yapılması çağrısında bulunmuştur. Başkan Jinping ayrıca blok zincirinin (Qū kuài liàn-区块链) *"bir sonraki teknolojik yenilik ve endüstriyel dönüşüm turunda önemli bir rol oynayacağını"* ve Çin'in diğer büyük ülkelere göre "avantaj" kazanmak istediğini belirtmiştir (Sagolj, 2019).

Çin için blok zinciri teknolojisi üzerine yapılan araştırma ve geliştirme harcamalarının, geniş anlamda Çin'in küresel güç olma yarışındaki teknolojik vizyonun bir parçası olduğu söylenebilir (Green, 2021). Çin, bu alanda yatırım yapmakla aynı zamanda dışa bağımlılığını da azaltmayı hedeflemektedir. 2015 yılında yayımlanan *"Made in China 2025"* isimli on yıllık planda Çin, üretim ve teknoloji alanında lider olmayı amaçladığını ifade etmiştir. Çin'de üretim alanındaki liderlik hedefi teknolojik ilerlemeden bağımsız ele alınmamaktadır. İlki 2016 yılında Sanayi ve Bilgi Teknolojileri Bakanlığı' tarafından yayımlanan "Blok Zinciri Teknolojisi ve Uygulama Geliştirme Üzerine Beyaz Kitap" (*White Paper on Blockchain and Application Development*) isimli belgeyi çeşitli başka belgeler takip etmiştir (Ekman, 2021).

Çin hükümetinin bir başka projesi ise Blok Zinciri Hizmet Ağı'dır *(Blockchain Service Network-BSN)*. 2020'de faaliyete geçen proje ile Çin temelde, "*Blok zinciri teknolojisinin daha hızlı ve daha ucuz bir şekilde uygulanmasına yardımcı olmayı amaçlıyor.*" (Bloomberg, 2020). Çin'in BSN'i, 'Dijital İpek Yolu' ve e-ticaret alanında kullanmasının da muhtemel olduğu öne sürülmektedir (Ekman, 2021). Yine bu yapı ile dünyada merkez bankalarınca kurulan dijital para birimlerine hızlı bir ödeme ve entegrasyon ağı kurulması arzu edilmektedir (Ekman 2021). Nisan 2020'de Huawei ve Baidu gibi büyük şirketlerin yöneticilerini, araştırmacılarını ve devlet görevlilerini bir araya getiren "Ulusal Blok Zinciri ve Dağıtılmış Muhasebe Teknolojisi Standardizasyon Teknik Komitesi" *(National Blockchain and Distributed Accounting Technology Standardization Technical Committee)* kurulmuştur. Çin, bu komite ile blok zinciri teknolojisi alanında standartlaşmaya gitmeyi planlamıştır (Hsu & Green, 2021). Xi Jinping, standartlaşma üzerine yapılan araştırmaların "*Çin'in dünyadaki etkisini ve kural koyucu gücünü"* artıracağını vurgulamıştır (Xinhua, 2019). 2019'un ilk yarısında yaptığı açıklamasında Çin'in, blok zinciri teknolojileri alanında toplamda 3.547 adet patenti olduğunu ilan etmiştir (Ekman, 2021). Buna ek olarak, Çin dünyadaki toplam blok zinciri patent sayısının yarısından fazlasına sahiptir (Ekman, 2021). 2019 yılında Çin Hükümetinin blok zinciri ile ilgili çalışmalara 300 milyon dolar ve 2020'de ise ek olarak 1 milyar dolar harcadığı tahmin ediliyor (Pan, 2019).

Çin, blok zinciri teknolojisini askerî alanda kullanmanın yollarını da aramaktadır. Halkın Kurtuluş Ordusu, blok zinciri teknolojisini personel bilgisini depolamak ve yönetmek, eğitim ve görev performansını artırmak için kullanmak noktasında girişimlerde bulunmaktadır. Askerî personelin performansının hesaplanması ve performansına göre jeton (*token*) verilmesi yoluyla bir ödül mekanizmasının getirebileceği ifade edilmektedir (Xuanzun, 2019). Bu teknoloji yardımıyla daha objektif yükselme kriterlerinin geleceği ve bunun da askerlere motivasyon vereceği düşünülmektedir. Böylece askerî bilgilerin siber anlamda güvenliği blok zinciri teknolojisi ile sağlanmaya çalışılmaktadır.

Rus Savunma Bakanlığı ise siber güvenlik saldırılarını azaltma ve askerî operasyonları destekleme noktasında blok zinciri teknolojisinin kullanım alanlarını araştırmak üzere 2018 yılında araştırma laboratuvarı kurduğunu duyurmuştur. Özellikle önemli veri tabanlarına ve silah sistemlerine yönelik siber saldırıları önleme hedefiyle çalışmalar sürdürülmektedir (Shen, 2018). 2017'de Etherum'un kurucusu Vitalik Buterin ile St.Ptersburg da görüşen Vladimir Putin, Rusya'da blok zinciri teknolojisinin uygulamaya alınmasına ilişkin iş birliği yolları aramıştır (President of Russia, 2017). Rus Savunma Bakanlığı kurduğu bu Blok Zinciri Araştırma Laboratuvarlarında (ERA) bu teknolojinin ulusal güvenliği güçlendirmesine, askerî altyapıların ele geçirilmesinin engellenmesine ve ordunun siber güvenliğini geliştirmeye yönelik çalışmalar yapmaktadır (Cornella vd., 2020)

Rusya, 2017 yılında Tokyo'da yapılan ve blok zinciri teknolojisinin kullanımına yönelik standartlar geliştirmeyi hedefleyen toplantıya, Rus heyet başkanı olarak Rus İstihbarat Teşkilatı, Rusya Federal Güvenlik Servisini yöneten Grigory Marshalko'yu göndermiştir. Bu durumun Rusya'nın blok zinciri teknolojisine yaklaşımı konusunda da ipuçları verdiği ifade edilebilir. Ayrıca, blok zinciri teknolojisini finansal alanda da kullanmak isteyen Rusya, 2014'de ekonomik yaptırımlara karşı geliştirdiği Mali Haberleşme Transfer Sistemi *(The Financial Communications Transfer System-SPFS)* adıyla SWIFT sisteminin mukabili amaçlanan sistemde blok zinciri teknolojisinden yararlanmaya başlamıştır (Cornella vd., 2020).

Özetle, bu teknolojiyi temel olarak

- Çin, ABD'nin dolar üzerinden kurmuş olduğu ekonomik hegemonyasını kırma ve askerî sistemlerini kendine özgü kodlar ile modernleştirme,
- ABD, askerî lojistik harcamalarını azaltma, sistemlerini güçlendirme ve merkezi verinin kırılganlığını azalma, (Lilly & Lilly 2021)
- Rusya ise silah sistemlerinin yazılımsal güvenliğini biricikleştirme ve onları siber saldırılara karşı daha az kırılgan hâle gelmek için

teknolojiyi araştırmaya ve/veya kullanmaya başlamıştır.

Öte yandan Avustralya, Kanada ve Çin dahil olmak üzere birçok ülkede, merkez bankaları blok zinciri sisteminin fonksiyonlarını kullanan dijital para birimlerini *(Central Bank Digital Currencies - CBDC)* geliştirme çalışmalarına devam etmektedir (Bank of Canada, 2019; Reserve Bank of Australia, 2019; CNCEditor, 2020). Ancak dijital para edinme girişimleri şimdilik günümüz dijital bankacılık yöntemini aynen takip ederek verileri merkezî sunucularda toplama yoluyla çalışarak blok zinciri teknolojisinin asıl özelliklerinden güvenlik açıkları yönünden ödün vermektedir. Son olarak UNICEF, İnsan Hakları Vakfı, Uluslararası Kızılhaç Federasyonu ve Oxfam gibi organizasyonlar da insani yardımlar bağlamında özel blok zinciri tabanlı uygulamalar kullanmaya başlamıştır. Bu kurumlar aynı zamanda blok zinciri teknolojisinin diğer kullanım alanlarını araştırmaktadır (UNICEF, 2020).

3. BLOK ZİNCİRİ İLE SİBER GÜVENLİĞİN OLASI DÖNÜŞÜMÜ

Blok zinciri, temel askerî teknolojiler ve askerler için stratejik, operasyonel ve taktik savunma üstünlüğünün yanında bilgi alışverişini kaydeden, bozulmaz, merkezî olmayan ve sayısallaştırılmış işlem protokolleri sağlar. Blok zincirleri son teknoloji şifreleme teknikleri, veri işlemleri için dijital parmak izleri ve imzalar üretir. Ağın 'dağıtılmış' doğası, farklı coğrafyalar ve ortamlardaki tüm katılımcıların ortak bir amaç ile işlem yapabilmesini sağlar. Ayrıca blok zinciri fiziksel veya dijital nesneler (örneğin uçak parçaları ve deniz taşımacılığı) için izleme veya denetleme işlemini yüksek seviyede güvenilir kanallar ile sağlar. Böylece bu teknolojinin; dijital para birimlerini değerleme ve manipüle etme (Akba vd., 2020; Akba vd., 2021) başta olmak üzere terörle mücadele, siber saldırı, savunma, istihbarat ve küresel para politikası gibi alanlarda kullanılan hassas teknoloji unsuru olduğu görülmüştür.

Diğer yandan blok zinciri sistemi, veri madenciliği adında yeni bir sektörü de beraberinde getirmektedir. Veri madenciliği yapabilmek için de gelişmiş bir teknolojik donanıma ve İnternet'in işleyişi konusunda uzman bireylere ihtiyaç duyulmaktadır. Donanımı ve bilgiyi bir araya getiren veri madenciliği mühendisliği, günümüzde çok az bir kesim tarafından yapılabilmektedir. Bu kişiler madenciliklerini Bitcoin vb. kripto para cüzdanlarında biriktirdikleri meblağlar üzerinden gelire dönüştürmektedir.

Bu hâli ile oldukça yeni ve marjinal addedilen blok zinciri teknolojisi ulus-devletler için şeffaflık ve takip edilebilirlik bakımından bazı kaygıları da beraberinde getirmiştir (Vigna & Ostroff, 2020). Böylece teknoloji mahiyeti itibari ile siber güvenliğin alanına taşmıştır. Şimdilik denetimsiz kabul edilen kripto para piyasasında yapılan işlemlerin amacı dijital cüzdana para eklemektir. Ancak bu yapılırken kazanılan paranın amacı ve süreci devletlerin

vergilendirme yetkisinin dışında kalabilmektedir. Bu sistemde bir kişi belli bir talep ile başkasına bir miktar para aktardığında bu işlemin izinin sürülemeyeceği bu zamana kadar yaygın söylemdi. Yakın zamanda bu iddianın doğruluğu tartışmalara açılmış ve istihbarat servislerinin benzer veri madenciliği yöntemiyle bu işlemlerin izlerini sürebileceği anlaşılmıştır (Financial Services Agency, 2019). Netice itibarıyla gizli bir işlem başka bir gizlilik yöntemi (yazılımsal istihbarat düzeyi bir gizlilik) ile açıklığa kavuşurken ülkelerin istihbarat servisleri de veri madencileri hâline gelebilmektedir. Bu durumda bir başka ülkenin istihbarat servisinin iz sürerek elde edeceği veriler ise ülke ilişkilerinde yeni gelişmelerin/krizlerin sebebi olacaktır. Tüm bu süreçler beraberinde istihbarat özelinden devletlerin güvenliğine etki ederek uluslararası ilişkilerin güvenlik perspektiflerini şekillendirme ihtimalini beraberinde getirmektedir. Nitekim blok zinciri, kripto paralar özelinde sosyal inşacı bir güvenlik yaklaşımı ile daha önceki çalışmalara konu olmuştur. Güvenliğin buradaki anlamı; sosyo-teknik güvenlik çerçevesidir. Bu çerçeve toplumdaki ve iş yerlerindeki insanlar ve teknoloji arasındaki etkileşimler ile ilgilenmektedir (Nabben, 2021). Böylece benzer etkileşimin ürünü ve sosyo-teknik bir konu olarak blok zinciri teknolojisi, siber güvenliğin bugününü şekillendirmeye devam etmektedir.

Blok zincirleri, bir ağdaki kullanıcılar arasında işlemleri mümkün kılar. Özel ve konsorsiyum blok zinciri ağları merkezî 'izinli', 'yarı izinli' veya 'izinsiz' olarak düzenlenebilir ve yönetilebilirler. Blok zinciri sisteminin bu yapısı, onun güvenliğinin hem teknik hem de sosyal bir mesele olduğunu göstermektedir. Kamusal blok zincirleri (ki Bitcoin gibi kripto paralar bu sistemi kullanır), merkezî olmayan fikir birliği sağlama konusundaki benzersiz özellikleri nedeniyle toplumdaki makro-sosyal yapıların (eşitlik, adalet, kalkınma gibi hedefler eksenindeki örgütlenmeler) koordinasyonu için de kullanılabilir.

Kullanıcıları için bir blok zinciri ağının güvenliği her disipline göre farklı yorumlanabilir. Örneğin siber güvenlik alanından bakılırsa amaç, bu ağın kendisini tehditlerden korumaktır. Sosyo-teknik güvenlik alanından bakılırsa amaç, ağdaki katılımcıları sistemin kendisi dahil tehditlerden korumaktır.

Blok zincirinin merkezî olmayan özelliği onu güvensiz olarak niteleyen yaklaşımları da beraberinde getirmiştir. Ancak Nabben'in "güvensizlik güven gerektirir" *(trustlessness requires trust*) cümlesinde hareketle buradaki güvensizlik, insanların blok zinciri teknolojisiyle başarmayı umdukları normatif bir güvene işaret eder (Nabben, 2020). Güvensiz olarak tanımlanması otoritenin veya üçüncü kişilerin yetki ve iznine tabi olmamasından ileri gelmektedir. Ancak blok zincirler, toplumdaki insanların koordinasyonundan ve aralarındaki tahkimden sorumlu olan makro-sosyal etkileşimleri yönetmek için uygulandığında, birer kurum gibi işlev görürler. Amaç; insan güvenini

bilgisayarlar ile ikame etmek değil, teknik ve sosyal mekanizmalar aracılığıyla güven garantileri sunmak, böylece 'güvenilir' altyapılar oluşturmaktır.

Ulus devletlerin blok zinciri teknolojisinde uzmanlaşması, işlem kayıtlarının uygun maliyetlerle ve yasal yollarda sürdürülmesi ve sosyo-teknik anlamda kullanımının artmasıyla sonunda insanlar en güvenilir ve işlevsel olana yönelerek blok bilgi zincirlerini (*infochains*) tercih eder hâle gelmeleri olasıdır. Nitekim günümüz dijital bankacılık sistemlerinde ve sosyal platformlarında geçici süreli aksaklıklar yaşanırken insanlar tercihlerini en az sorun çıkaran bankadan ya da platformdan yana kullanmaktadır. Başta Çin ve ABD olmak üzere ülkeler bu dijital dönüşümlerin farkına varmış, bir şekilde blok zinciri teknolojisini güvenli kılmanın bilimsel Ar-Ge yollarını aramaya koyulmuşlardır.

SONUÇ

Zincir tabanlı sistemlerdeki kendilerine has yazılımsal yeniliklerin getireceği sosyal, siyasi ve askerî sonuçlar odağında güvenlik çerçevelerinin literatür büyümesi ışığında ele alındığı bu çalışmada yükselen bir teknoloji olan blok zinciri teknolojisinin güvenlik politikalarıyla etkileşime giren yönleri analiz edilmiştir. Blok zinciri belirli bir ulusal stratejiye entegre edildiğinde devletler, toplumlar ve vatandaşlar arasındaki ilişkilerin geleceğini temelden değiştirme potansiyeline sahiptir. Fütürist Roy Amara'nın; *"Bizler teknolojinin etkisini kısa vadede abartma ve uzun vadede ise hafife alma eğilimindeyiz."* (Ratcliffe, 2016) vurgusundan hareketle bir değerlendirme yapılırsa şimdiden blok zinciri konusunda uzun dönemli politikaların ülkeler ve kurumlarca uygulamaya alındığı söylenebilmektedir. Bitcoin kriptopara biriminin yasaklandığı ülke olarak Çin, Bitcoin'in kullandığı blok zinciri teknolojisi üzerine yapılan çalışmalarda dünyada başı çekmektedir. Çin'in Keskin Gücü'nde *(sharp power)* blok zinciri şimdiden önemli bir yere sahipken süper güçlerin önceliği, şimdilik blok zincirini silahlandırmaktır *(weaponizing blockchain*). Nihai kertede eldeki mevcut literatür büyümesi ve uygulamalar, siber güvenliğin yeni rekabet ve gelişim alanının blok zinciri teknoloji üzerine yoğunlaştığını göstermiştir.

KAYNAKÇA

Adams, Victoria (2019). Why Military Blockchain is Critical in the Age of Cyber Warfare, ConsenSys. Erişim tarihi: 20.09.2021, https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619.

Akba, F., I. T. Medeni, M. S. Guzel and I. Askerzade (2020). "Assessment of Iterative Semi-Supervised Feature Selection Learning for Sentiment Analyses: Digital Currency Markets". IEEE 14th International Conference on Semantic Computing (ICSC). pp. 459-463, doi: 10.1109/ICSC.2020.00088.

Akba, F., I. T. Medeni, M. S. Guzel and I. Askerzade (2021). "Manipulator Detection in Cryptocurrency Markets Based on Forecasting Anomalies. IEEE Access, vol. 9, doi: 10.1109/ACCESS.2021.3101528.

Bank of Canada (2019). The road to digital money. Ottawa, ON: Bank of Canada. Erişim tarihi, 08.11.2021, https://www.bankofcanada.ca/2019/04/the-road-to-digital-money/.

Bilgin, Pınar (2010). "Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları." Stratejik Araştırmalar, Cilt 8, No 14.

Brett, Jason (2021). Congress Has Introduced 18 Bills On Crypto And Blockchain In 2021. Forbes. Aug 22, 2021. Erişim tarihi: 2 Aralık, 2021. https://www.forbes.com/sites/jasonbrett/2021/08/22/congress-has-introduced-18-new-bills-on-crypto-and-blockchain-in-2021/

Buzan, Barry (1983). People, States, and Fear: National Security Problem in International Relations, Brighton: Harvester Wheatsheaf.

CNC Editor, (2020). "State media sheds light on China's central bank digital currency." China Banking News. Erişim tarihi, 01.11.2021, http://www.chinabankingnews.com/2020/04/24/state-media-highlights-regtech-functions-controlled-anonymity-of-chinas-central-bank-digital-currency/.

Cornella, Alessia et al. (2020). "Blockchain in defence: a breakthrough?". European Army Interoperability Center, Erişim tarihi, 20.11.2021, https://finabel.org/wp-content/uploads/2020/09/FFT-Blockchain.pdf.

Culbertson, Matt (2018). Blockchain, Nuclear War, and Artificial Intelligence: 2018's Most Extreme Cybersecurity Forecasts. Erişim tarihi, 15.09.2021, https://www.linkedin.com/pulse/blockchain-nuclear-war-artificial-intelligence-2018s-most-culbertson/.

Çin'de Blockchain Tabanlı Servis Ağı Faaliyete Geçiyor, Bloomberg HT, 2020. Erişim tarihi, 17.11.2021, https://www.bloomberght.com/cin-de-blockchain-tabanli-servis-agi-faaliyete-geciyor-2253229.

Dion-Schwarz, Cynthia et al, (2019). "Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats" 2019 RAND Corporation, Erişim tarihi, 15.11.2021, https://www.rand.org/content/dam/rand/pubs /research_reports/RR3000/RR3026/RAND_RR3026.pdf.

Doğrul, Mürsel & Korkut, Cem (2020). "*Bilişim Teknolojilerindeki Gelişmeler Işığında Kripto Paraların Finansal Sisteme Entegrasyonu*", Bilişim Teknolojileri ve İletişim: Birey ve Toplum Güvenliği, Ed. Muzaffer Şeker, Yasin Bulduklu, Cem Korkut, Mürsel Doğrul, Türkiye Bilimler Akademisi Yayınları, ISBN: 978-605-2249-48-2, Ankara, ss. 279-280.

Ekman, Alice (2021). "China's Blockchain and Cryptocurrency Ambitions; The first-mover advantage." European Union Institute for Security Studies, BRIEF 15, Erişim tarihi, 12.11.2021, https://www.iss.europa.eu/sites/default/files/ EUISSFiles/Brief_15_2021.pdf

European Commission (2017). "Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector", EECSP Report: Cyber Security in the Energy Sector. Erişim tarihi, 16.11.2021, https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_ report_final.pdf.

Financial Services Agency (2019). "Research on Privacy and Traceability of Emerging Blockchain-Based Financial Transactions", The Japanese Government. Erişim tarihi, 09.09.2021, https://www.fsa.go.jp/ policy/bgin/ResearchPaper_MRI_en.pdf.

General Office of Fujian Provincial People's Government (2021). "Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China". Erişim tarihi, 10.09.2021,
https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm.

Ghanea-Hercock, Robert (2012). "Why Cyber Security Is Hard." Georgetown Journal of International Affairs, pp. 81–89.

Global Times (2021). "China takes steps to boost blockchain industry into world-leading position by 2025". Erişim tarihi, 12.11.2021, https://www.globaltimes.cn/page/202106/1225636.shtml.

Gray, Mark (2018). "Blockchain and Suitability for Government Applications". Public-Private Analytic Exchange Program, Erişim tarihi, 21.11.2021, https://www.dhs.gov/sites/default/files/publications/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf.

Hong, Iris (2021). "China sets goal to be blockchain world leader by 2025", Asia Financial. Erişim tarihi, 18.11.2021, https://www.asiafinancial.com/china-sets-goal-to-be-blockchain-world-leader-by-2025.

House Hearing (September 7, 2018). "Hearing Before the Subcommittee on Terrorism and Illicit Finance of the Committee on Financial Services" U.S. House of Representatives, One Hundred Fifteenth Congress, Second Session", Erişim tarihi, 08.09.2021, https://www.govinfo.gov/content/pkg/CHRG-115hhrg31576/html/CHRG-115hhrg31576.htm.

Hsu, Sara & Green, Gabrielle (2021). "Blockchain in China". Stimson Center. Erişim tarihi, 19.10.2021, https://www.stimson.org/2021/blockchain-in-china/.

IBM (2021). What is blockchain security? Erişim tarihi, 12.08.2021, https://www.ibm.com/topics/blockchain-security.

Jens Ducrée et al. (2021). "Unchaining Collective Intelligence for Science, Research, and Technology Development by Blockchain-Boosted Community Participation," Frontiers in Blockchain, cilt 4, no 6. https://doi.org/10.3389/fbloc.2021.631648.

Lin, Lian, Qichao, Zhu & Yu, Zhao (2016). "Blockchain technology and its potential military value[J]. National Defense Science and Technology, 37(02): pp. 30-34. / 廉蔺,朱启超,赵炤.区块链技术及其潜在的军事价值[J].国防科. Erişim tarihi, 13.11.2021, https://global.cnki.net/kcms/detail/detail.aspx?filename=GFCK201602007&dbcode=CJFQ&dbname=CJFD2016&v=.

Mathews, Jessica Tuchman (1989). "Redefining Security." Foreign Affairs 68, No 2.

Matisek, Jahara (2019). China Weaponizing Blockchain Technology For Gray Zone Warfare?, Global Security Review. Erişim tarihi, 17.11.2021, https://globalsecurityreview.com/china-weaponizing-blockchain-technology-gray-zone-warfare/.

Metry, Mark (2017). "Blockchain Technology is the Most Significant Invention since the Internet and Electricity". Erişim tarihi, 15.11.2021, https://markmetry.medium.com/blockchain-technology-is-the-most-significant-invention-since-the-internet-and-electricity-f2d44a631ef6.

Moran, Theodore (1990). "International Economics and National Security". Foreign Affairs, Citl 69, No 5.

Nabben, Kelsie (2020). "Trustless approaches to digital infrastructure in the crisis of COVID-19 Australia's newest COVID app. Home-grown surveillance

technologies and what to do about it," social science research network. Rochester, NY. doi: 10.2139/ssrn.3579220SSRN.

Nabben, Kelsie (2021). "Blockchain Security as 'People Security': Applying Sociotechnical Security to Blockchain Technology," Frontiers in Computer Science, cilt 2, no 62. https://doi.org/10.3389/fcomp.2020.599406.

Pan, David (2019). From Banking Giants to Tech Darlings, China Reveals Over 500 Enterprise Blockchain Projects, Coindesk. Erişim tarihi, 08.11.2021, https://www.coindesk.com/markets/2019/10/28/from-banking-giants-to-tech-darlings-china-reveals-over-500-enterprise-blockchain-projects/.

President of Russia (June 2, 2017). "Meeting with founder of Ethereum project Vitalik Buterin". Erişim tarihi, 28.11.2021, http://en.kremlin.ru/events/president/news/54677.

Ratcliffe, Susan (2016). "Roy Amara 1925–2007, American futurologist". Oxford Essential Quotations. 1 (4th ed.). Oxford University Press. doi: 10.1093/acref/9780191826719.001.0001.

Reserve Bank of Australia (2019). Submission to the senate select committee on financial technology and regulatory technology. Erişim tarihi, 09.11.2021, https://www.rba.gov.au/publications/submissions/payments-system/financial-and-regulatory-technology/index.html.

Reisman, R. J. (2019). Air traffic management blockchain infrastructure for security, authentication, and privacy. NASA Ames Research Center.

Roberts, Brad (1990). "Human Rights and International Security", Washington Quarterly, Cilt 13.

Sagolj, Damir (2019). China goes bullish on blockchain, Insider. Erişim tarihi, 08.11.2021, https://www.businessinsider.com/china-bullish-on-blockchain-xi-jinping-2019-10.

Singh, S., & Singh, N. (2016). "Blockchain: future of financial and cyber security," in 2016 2nd International Conference on Contemporary Computing and informatics IC3I, pp. 463–467. doi:10.1109/IC3I.2016.7918009.

Shen, Muyao (2018)." The Russian Military Is Building a Blockchain Research Lab", Coindesk. Erişim tarihi, 01.09.2021, https://www.coindesk.com/markets/2018/07/02/the-russian-military-is-building-a-blockchain-research-lab/.

The Third Prague 5G Security Conference, National Cyber and Information Security Agency (NÚKIB), 06 December 2021, Erişim tarihi, https://www.nukib.cz/en/infoservis-en/news/1779-the-third-prague-5g-security-conference-has-ended/.

Ullman, Richard H. (1983). "Redefining Security", International Security, Cilt 8, No 1. pp. 129-53.

Underwood, S. (2016). Blockchain beyond bitcoin. Commun. ACM. 59 (11), pp. 15–17. doi: 10.1145/2994581.

UNICEF Office of Innovation (2020). UNICEF funding opportunity for blockchain startups. Erişim tarihi, 12.11.2021, https://www.unicef.org/innovation/applyBlockchainCrypto.

U.S. Department of Defense (2020). "Report on Potential Uses of Blockchain by the U.S. Department of Defense", Value Technology Foundation. Erişim tarihi, 11.11.2021, https://www.crowell.com/files/Potential-Uses-of-Blockchain-Technology-In-DoD.pdf.

U.S. Department of Justice (2020). "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns" Erişim tarihi, 10.07.2021, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

Ünal, G. & Uluyol, Ç. (2020). Blok Zinciri Teknolojisi. Bilişim Teknolojileri Dergisi, 13 (2), 167-175 . DOI: 10.17671/gazibtd.516990

Vigna, Paul & Ostroff, Caitlin (2020). "Why Hackers Use Bitcoin and Why It Is So Difficult to Trace", The Wall Street Journal. Erişim tarihi, 15.11.2021, https://www.wsj.com/articles/why-hackers-use-bitcoin-and-why-it-is-so-difficult-to-trace-11594931595.

Wallace, Ed (2016). "We need to talk about blockchain", The Economist. Erişim tarihi, 20.09.2021, https://eiuperspectives.economist.com/technology-innovation/we-need-talk-about-blockchain.

Xinhua (2019). "Xi stresses development, application of blockchain technology" Erişim tarihi, 11.10.2021, http://www.xinhuanet.com/english/2019-10/25/c_138503254.htm.

Xuanzun, Liu (2019), "Chinese military could deploy blockchain management." Global Times, Erişim tarihi, 12.11.2021, https://www.globaltimes.cn/content/1170370.shtml