ARAŞTIRMA MAKALESİ

# DEZENFORMASYONLA MÜCADELEDE BLOK ZİNCİR (BLOCKCHAIN) TEKNOLOJİSİ

**Yakup TOKTAY*, Ahmet GÜVEN****

Gönderim Tarihi: 17.01.2025 - Kabul Tarihi: 28.03.2025

Toktay, Y & Güven, A. (2025). Dezenformasyonla mücadelede blok zincir (blockchain) teknolojisi. *Etkileşim*, 15, 100-122.
https://doi.org/10.32739/etkilesim.2025.8.15.285

*Bu çalışma araştırma ve yayın etiğine uygun olarak gerçekleştirilmiştir.*

## Öz

Çağımızda doğru habere ulaşmanın önündeki en büyük engellerin başında dezenformasyon gelmektedir. Bu sebeple dezenformasyonla mücadele noktasında pek çok çalışma yapılmaktadır. Ancak insan emeğine dayanan ve dolayısıyla hem maddiyat hem de zaman açısından maliyeti yüksek olan geleneksel yöntemlerin etkisi sorgulanmaktadır. Bu çalışmanın amacı, geleneksel yöntemlere göre daha etkili olma kapasitesi taşıyan ve daha az maliyetli olan blok zincir teknolojisinin dezenformasyonla mücadele açısından potansiyelini tartışmaktır. Çalışma, blok zincir teknolojisinin; yanlış bilgi, sahte haber, manipülasyon ve propaganda gibi farklı dezenformasyon türlerinin önlenmesi ve yönetilmesinde sunduğu yenilikçi çözümlerin ne olduğu, yeni nesil dezenformasyon yöntemlerinin tespitinde hangi imkanları sunduğu ve geleneksel yöntemler ile hangi farklılıklara sahip olduğu sorularına odaklanmaktadır. Nitel yöntem, durum çalışması desenine göre tasarlanan çalışmada betimsel analiz yöntemi kullanılmıştır. Blok zincir teknolojisinin; değiştirilemez, şeffaf ve merkeziyetsiz olması, verilerin dağıtık tutulması, akıllı sözleşmelerle yürümesi, kriptografik güvenlik ve konsensüs mekanizmasına sahip olması sebebiyle dezenformasyonla mücadelede geleneksel yöntemlere üstünlük sağlayabileceği sonucuna ulaşılmıştır.

**Anahtar Kelimeler:** dezenformasyon, manipülasyon, blok zincir, haber doğrulama, enformasyon.

* Öğretim Görevlisi Doktor, Bandırma Onyedi Eylül Üniversitesi, Bandırma Meslek Yüksekokulu, Balıkesir, Türkiye.
ytoktay@bandirma.edu.tr, ORCID: 0000-0003-3253-9898
** Doçent Doktor, Bandırma Onyedi Eylül Üniversitesi, İletişim Fakültesi, Balıkesir, Türkiye.
aguven@bandirma.edu.tr, ORCID:0000-0002-2452-2992

RESEARCH ARTICLE

# COMBATING DISINFORMATION WITH BLOCKCHAIN TECHNOLOGY

**Yakup TOKTAY*, Ahmet GÜVEN****

Received: 17.01.20258 - Accepted: 28.03.2025

Toktay, Y & Güven, A. (2025). Dezenformasyonla mücadelede blok zincir (blockchain) teknolojisi. *Etkileşim*, 15, 100-122.
https://doi.org/10.32739/etkilesim.2025.8.15.285

*This study complies with research and publication ethics.*

## Abstract

Disinformation is one of the biggest obstacles to accessing accurate news in our age. For this reason, many efforts are being made to combat disinformation. However, the effectiveness of traditional methods, which rely on human labor and are therefore costly in terms of both time and money, has been questioned. The aim of this study is to discuss the potential of blockchain technology, which has the capacity to be more effective and less costly than traditional methods, in terms of combating disinformation. The study focuses on the questions of what innovative solutions blockchain technology offers in preventing and managing different types of disinformation such as misinformation, fake news, manipulation and propaganda, what opportunities it offers in detecting new generation disinformation methods and what differences it has with traditional methods. Descriptive analysis method was used in the study designed according to qualitative method, case study design. It was concluded that blockchain technology can provide superiority over traditional methods in the fight against disinformation because it is unchangeable, transparent and decentralized, data is kept decentralized, it works with smart contracts, has cryptographic security and consensus mechanism.

**Keywords:** disinformation, manipulation, blockchain, fact-checking, information.

* Lecturer (PhD), Bandırma Onyedi Eylül University, Bandırma Vocational School, Balıkesir, Türkiye.
ytoktay@bandirma.edu.tr, ORCID: 0000-0003-3253-9898
** Associate Professor/PhD, Bandırma Onyedi Eylül University, Faculty of Communication, Balıkesir, Türkiye.
aguven@bandirma.edu.tr, ORCID:0000-0002-2452-2992

**Giriş**

İnternet teknolojisinin ortaya çıkışı, insanların birbirleriyle iletişim kurma, bilgi alma ve haber tüketim alışkanlıklarını büyük oranda değiştirmiştir. Berners-Lee'nin mucidi olduğu ilk web, statik bir yapıya sahipti ve kullanıcıların sadece bilgiyi aramasına ve okumasına olanak tanımaktaydı. Dolayısıyla kullanıcılar kendilerine sunulanla yetinmek zorunda kalır ve içerik üretim sürecine dâhil olamazdı. Ancak sosyal ağların ortaya çıkışına zemin hazırlayan web 2.0 altyapısı, insanları salt tüketici konumdan üretici konuma, statik yapıdan dinamik yapıya dönüştürmüştür. Konvansiyonel medyanın aksine bilgi akışı ve kontrol mekanizmalarının merkezi olmadığı sosyal ağlarda kullanıcılar içerik üretim sürecine dahil olarak ürettikleri bilgileri rahatlıkla ağlar üzerinden senkron ya da asenkron bir şekilde ucuz ve hızlı olarak diğer kullanıcılarla paylaşabilmektedir. Popülaritesi artan sosyal medyanın kullanıcılara sunduğu bu olanaklar büyük bir problemi beraberinde getirmiştir. Bilgi akışının hiyerarşik yapıdan ziyade çoklu ve ağ tabanlı bir yapıya evrilmesi, sosyal ağlarda yalan ve yanlış bilginin dolaşımını artırarak gerçeklerin çarpıtılması ve kamuoyunun yanıltılması gibi sorunları ortaya çıkarmıştır. Kamuoyu algısının şekillendirilmesi noktasında sahte haberlerin gerçek olarak algılanmasının insanların siyasi tutumlarını etkilediği, politikacılara yönelik etkisizlik, yabancılaşma ve güvensizlik gibi tutumların gelişmesine sebebiyet verdiği ortaya koyulmuştur (Balmas, 2014, s. 447). Yine sahte haberlerin, seçim kampanyası sırasında siyasi kutuplaşmayı ve seçmenler arasındaki çatışmayı körüklediği ve seçmenlerin yanıltıcı siyasi ifadeler ve iddialardan kolayca etkilenebildiği belirlenmiştir (Zhang & Ghorbani, 2020, s. 2).

Sosyal ağlarla birlikte ortaya çıkan vatandaş gazeteciliği kullanıcıların da haber üretim ve dağıtım sürecine dahil olmasını sağlayarak habercilik pratiğini profesyonel bir meslek olmaktan çıkarmıştır. Ancak Virilio, mevcut durumu enformasyon devriminden ziyade "sistemli ihbarcılık devrimi" olarak nitelendirmektedir. Ona göre kullanıcıların sosyal ağlar üzerinde ortaya attığı söylenti ve iddialar, bir panik fenomeni yaratarak hakikatin doğasını ve basın özgürlüğünün temelindeki meslek etiğini yıkmaktadır (Virilio, 2003, s. 105). Değişen gazetecilik pratiğiyle birlikte doğrulama ve teyit platformlarının gerçeği ortaya çıkarabilme kapasitesinin çok üzerinde dezenformatif bilgi yayılımı gerçekleştiği ortadadır. Bu da yalan ya da yanlış bilginin, gerçeği aşarak onu geride bırakmasına sebep olmaktadır. Zira yapılan araştırma sahte haberlerin doğru bilgilerden altı kat daha hızlı bir şekilde yayıldığını ortaya koymuştur (Vosoughi ve diğerleri, 2018, s. 1149).

Gerçek ile kurgunun, bilgi ile eğlencenin birlikte sunulduğu medya ortamlarında veri doğrulama ve bilgi teyidine olan talepte de bir artış söz konusudur. Dolayısıyla yalan ve yanlışlar karşısında hızla büyüyen bir siyasi teyit hareketi de vardır. Ancak gerçeklik kontrol süreçlerinin otomasyonuna yönelik çabaların yetersiz kalması ve bu sürecin büyük ölçüde elle yapılan incelemelere dayandırılması hem zaman verimliliğini düşürmekte hem de işlemi oldukça

zahmetli hale getirmektedir. Bu durum dezenformatif bilginin gerçeği geride bırakmasındaki ana sebeptir.

Bu çalışma, dezenformasyonla mücadeledeki bu kısıtlılığa odaklanarak bilgi doğrulama ve teyit sürecinin blok zincir teknolojisiyle nasıl daha hızlı ve verimli hale getirilebileceği tartışmasına odaklanmaktadır. Bu çerçevede amaç soru cümleleri hazırlanmıştır:

1. Blok zincir teknolojisi, yalan ya da yanlış bilgi, sahte haber, manipülasyon ve propaganda gibi farklı dezenformasyon türlerinin önlenmesi ve yönetilmesinde hangi yenilikçi çözümleri sunmaktadır?

2. *Deepfake* (derin sahte) videolar, ses klonlama, otomatik metin, haber ve görüntü üretimi, botlar ve trol ağları, kişiselleştirilmiş dezenformasyon, algoritma manipülasyonu gibi yeni nesil dezenformasyon yöntemlerini tespit etmek ve önlemek için blok zincir teknolojisi hangi imkanları sunmaktadır?

3. Geleneksel dezenformasyonla mücadele yöntemleri ile blok zincir teknolojisinin sunduğu yenilikçi çözümler arasında ne gibi farklılıklar vardır?

Konu ile ilgili literatürdeki çalışmalar tarandığında Wang ve diğerlerinin (2023) yaptığı bir çalışmada blok zincir veri tabanı kullanılarak güvenilmeyen kaynaklardan gelen sahte haber verilerinin depolanması, izlenebilirliği ve doğrulanması üzerine bir araştırma yapıldığı ve haber verilerinin güvenli bir şekilde depolanması için bir model tasarlandığı görülmüştür. Başka bir çalışmada Birhade ve diğerleri (2023), bilgi sistemlerinin doğrulanması ve dezenformasyonla mücadelede blok zincir kullanımına ilişkin bir veri analiz süreci geliştirmeyi amaçlamışlardır. Blok zinciri ve dağıtık defter teknolojilerinin (DLT) kullanılarak sahte haber, dezenformasyon ve *deepfake* ile mücadeledeki potansiyelinin sorgulandığı çalışmalar mevcuttur (Fraga-Lamas & Fernandez-Carames, 2020; Shae & Tsai, 2019; Qayyum ve diğerleri, 2019; Hasan & Salah, 2019; Song ve diğerleri, 2019; Huckle & White, 2017; Shang ve diğerleri, 2018; Babar ve diğerleri, 2020; Meghana ve diğerleri, 2023).

Türkçe literatürde genel olarak blok zincir teknolojisini konu alan farklı alanlarda yapılmış çalışmalar mevcuttur. Doğrudan blok zincir ve dezenformasyon ilişkisi üzerine hazırlanmış bir çalışmaya rastlanmasa da konuya yakın bazı çalışmaları sıralamak mümkündür (Takan & Ergün, 2024; Türker & Tanyeri, 2024; Atalay, 2018; Önder & Koç, 2024). Bu durum çalışmanın özgünlüğünü ortaya koyarak ilgili alana katkı sağlaması bakımından önemlidir.

Nitel yöntem ve durum çalışması desenine göre tasarlanan bu çalışmada, blok zincir teknolojisinin dezenformasyonla mücadelede sağlayabileceği faydalar betimsel analiz gerçekleştirilerek ortaya konulmaya çalışılmıştır. Ayrıca geleneksel mücadele teknikleriyle yenilikçi çözümlerin arasındaki farklar da ortaya konmaya çalışılacaktır.

**Dezenformasyonla Mücadele**

Dezenformasyon çağdaş demokrasilerde dahi çözülmesi gereken başlıca problemlerden biridir. Her ne kadar etkisini yeni iletişim teknolojileriyle birlikte daha yoğun olarak gösterse de aslında yeni bir kavram değildir. Ancak özellikle internet ve sosyal ağların ortaya çıkışıyla birlikte kanun yapıcıların, ekonomistlerin ve akademik camianın dikkatini çeken konular arasına girmiştir çünkü dezenformasyon toplumsal bir patoloji durumuna yol açan toplumdaki güven ve kohezyonu parçalayarak sosyal çözülmeyi ortaya çıkarmaktadır. Dolayısıyla dezenformasyon günümüzde toplumsal bir sorun olarak kendini daha belirgin bir şekilde göstermektedir.

Dezenformasyon kelime anlamı itibarıyla "kasıtlı olarak yapılan aldatıcı bilgidir" (Bennett & Livingston, 2023, s. 3; Fallis, 2009, s. 410). Aldatıcı ya da yanıltıcı bilginin arkasında her zaman kötü niyet olmayabilir ancak ister bilinçsizce yapılan bir hatadan veya ihmalden yapılmış olsun isterse de bir önyargıdan kaynaklı olarak veya kasıtlı bir amaç uğruna yapılmış olsun yalan, yanlış ya da kirli bilgi, insanları yanlış yönlendirmektedir. Dezenformasyon yanlış bilgilendirmenin problemli biçimidir çünkü insanların yanlış yönlendirilmesi tesadüf değildir (Fallis, 2015, s. 402). İyi niyetli bir hatadan farklı olarak dezenformasyon, aktif olarak yanlış yönlendirme girişiminde bulunan birinden gelir (Piper, 2002, ss. 8-9). Dezenformasyon, sadece doğrudan zarar vermez aynı zamanda güveni aşındırıp bireyler arası etkili bilgi alışverişini engelleyerek topluma dolaylı yoldan da zarar verebilir.

Bilgi ve iletişim araçlarına olan erişim kolaylığı, insanları çoğu zaman kaynağını dahi bilmediği büyük bir enformasyon bombardımanına tutmaktadır. Bireyin gündelik yaşamının tümü, yoğun bir şekilde, hızla sunulan aşırı miktarda bilgiyle çevrelenmektedir. Bilginin miktarı ve yayıldığı ortamlardaki çeşitlilik arttıkça dezenformasyon miktarı da artmaktadır. Aynı zamanda dezenformasyon da her medya platformunda kendine özgü biçimlerde ortaya çıkarak toplumsal algıyı şekillendirmektedir. Ancak dezenformasyon, medya teknolojilerindeki yeniliklere hızla adapte olurken bu olgunun engellenmesine yönelik stratejiler hala ağırlıklı olarak geleneksel yöntemlerle sınırlı kalmaktadır. Geleneksel yöntemler içerisinde üç farklı dezenformasyonla mücadele yaklaşımından söz edilebilir.

**Profesyonel gerçeklik kontrolörleri**

Haber ya da haberlere konu olan bilgi, iddia ya da belgelerin gerçek olup olmadığının tespit edildiği doğrulama ve teyit süreci (*fact-checking*), esasında hesap verilebilir gazeteciliğin bir formu olsa da artık süreç, daha etkin bir şekilde bağımsız kuruluş ve organizasyonlarca yürütülmekte ya da yürütülmesi için fonlanmaktadır. Doğrulama (*fact-checking*) kuruluşları bünyesinde yetiştirdikleri teyitçiler ve gönüllülerle dezenformasyon savaşına girmektedir. Dünya çapında teyitçileri bir araya getirmeyi amaçlayan Uluslararası Doğrulama Ağı'na

(*International Fact-Checking Network*-IFCN) kayıtlı farklı ülkelerden 122 teyit platformu mevcuttur. Türkiye'de ise IFCN'nin belirlediği standartlara uyum sağlayan üç doğrulama platformu mevcuttur. Bunlar; *Teyit.org*, *Doğruluk Payı* ve *Doğrula* platformlarıdır.

Doğrulama (*fact checking*) platformları bilgi haber ya da iddiaların doğruluğunu teyit etmek için öncelikle güncel tartışmaların merkezindeki iddiaları veya sosyal medyada hızla trend olan ve şüphe uyandıran içerikleri ya da kullanıcılar tarafından ihbar edilen içerikleri incelenmek üzere toplamaktadır. Toplanan haber ve iddiaların ilk olarak kaynağına ve nerede ortaya çıktığına bakıldıktan sonra iddia edilen bilgiler akademik çalışmalar, resmi belgeler, uzman görüşleri alınarak karşılaştırma yapılmaktadır. Eğer incelemeye alınan iddia görsellik içeriyorsa o zaman fotoğraf ve videonun orijinal olup olmadığı, meta verileri, tersine görsel arama yapılarak görselin daha önce kullanılıp kullanılmadığı tespit edilmektedir. Ayrıca iddia edilen bilgi hakkında mantıksal çelişki olup olmadığı da kontrol edilmektedir. Tüm bu süreçlerin ardından raporlama işlemi yapılarak inceleme sonucunda başvurulan tüm kaynaklar raporda verilmekte ve kullanıcılarla paylaşılmaktadır. Ancak anlatılan bu süreç maliyetli ve titizlikle işlenmesi gereken bir süreç haline gelmektedir.

**Kullanıcı etkileşimli dezenformasyonla mücadele**

Bazı sosyal medya kuruluşları, dezenformasyonla mücadele merkezleri kurarak kullanıcı etkileşimlerinden faydalanıp potansiyel sahte haber ve içeriklerle mücadele tekniği geliştirmiştir. *Meta* şirketi çatısı altındaki *Facebook*, kullanıcılarından geri bildirim alarak potansiyel dezenformatif içerikleri işaretleme olanağı sunmaktadır (Shu ve diğerleri, 2020, s. 11). Bu yöntem esasında *Facebook* içerisindeki dezenformasyonla mücadele amaçlı kullanılan botlarının eğitilmesi anlamını taşır. Kolektif kullanıcı zekasından faydalanarak botlar kullanıcılardan gelen bildirimlerle eğitilir ve yazılımın bir kanaat oluşturması sağlanmış olur. Dezenformasyonla mücadelede kullanılan bu yöntem birçok sahte haber dedektörünün kullandığı tekniklerden biridir (Qian ve diğerleri, 2018, s. 3840).

Öte yandan dezenformasyonun kullanıcı tepkilerinde gözlemlenebilen korku, tiksinti ve şaşkınlık gibi duygu durumlarını tetiklediği gözlemlenmiştir. Gerçek haberlerde ise beklenti, üzüntü, neşe ve güven gibi duyguları harekete geçirmektedir. Kullanıcı merkeze alınarak dezenformasyonu tespit etmek amacıyla kullanılan tekniklerden bazıları bu araçları kullanmaktadır (Vosoughi ve diğerleri, 2018; Shu ve diğerleri, 2020, s. 11). Ancak bahsi geçen bu iki teknikte de doğrulama ve teyit işlemi "çapraz bilgelikten" yararlanarak herhangi bir destekleyici araç olmadan profesyonel olmayan topluluklarca gerçekleştirilmektedir. Bu geniş bir ölçeğe ulaşılabilmesi açından kıymetli lakin kullanıcıların partizanlaşmaya olan eğilimi nedeniyle istismara açık ve dolayısıyla etki düzeyi düşük bir yöntemdir (Buțincu & Alexandrescu, 2023, s. 3).

**Yarı ve tam otomatik doğrulama araçları**

Dezenformasyonla mücadele etmek üzere geliştirilen yarı ve tam otomatik olarak programlanan yapay zekâ araçları kirli bilginin tespit edilmesi, sınıflandırılması ve yayılmasının önlenmesinde kullanılmaktadır. Yarı-otomatik çalışan yapay zekâ araçlarında insan müdahalesi de sürece dahil edilmektedir. Yapay zekâ şüpheli gördüğü içerikleri işaretlemekte ancak iddianın değerlendirilerek teyit edilmesi bir uzman tarafından gerçekleştirilmektedir. *Duke Reporters' Lab* tarafından geliştirilen *ClaimReview*, şüpheli içerikleri tarayan ve bu iddiaları işaretleyerek doğruluğunu sınayan bir yarı otomatikleştirilmiş yapay zekâ aracıdır. Yine Avrupa Dijital Medya Gözlemevi (EDMO) tarafından tanıtılan *WeVerify deepfake* dedektörü, görsel konum tahmini, klonlanmış video arama, sosyal ağ analizi, görüntü doğrulama asistanı, bağlam toplama analizi gibi sunduğu hizmetlerle çevrim içi dezenformatif bilgileri tespit edebilen yarı otomatik sistemlerden biridir.

Tam otomatik çalışan doğrulama sistemlerinde ise insan müdahalesine ihtiyaç duyulmadan veri setleri analiz edilmekte, sınıflandırılmakta ve otomatik kararlar alınmaktadır. *Jigsaw* ve *Google* tarafından geliştirilen *Perspective API* makine öğrenmesini kullanarak toksik, yanıltıcı veya saldırgan içerikleri tespit ederek denetleyen, yayılmasını engelleyebilen tam otomatik sistemlerden biridir.

**Blok Zincirin Temel Özellikleri ve Dezenformasyonla Mücadeledeki Rolü**

Blok zincir, dağıtılmış cüzdan teknolojisinin bir alt kümesi olarak verilerin birden fazla veri deposu tarafından kaydedilip aynı anda paylaşıldığı bir yapıdır. Bu yapı, "düğüm" adı verilen dağıtılmış bilgisayar sunucuları ağı tarafından korunmakta ve kontrol edilmektedir. Sürekli büyüyen veri yapısını oluşturmak ve doğrulamak için, kriptografi olarak bilinen şifreleme yöntemlerini kullanarak belirli matematiksel algoritmalarla çalışmaktadır (Natarajan ve diğerleri, 2017; Huoben & Snyers, 2018, s. 15). Böylece güvenli ve şeffaf bir veri yönetimi sağlamaktadır.

Blok zincir, dağıtılmış bir veri tabanı olarak düşünülebilir; üyeler, bu veri tabanına bilgiler ekleyerek yeni bir veri bloğu veya düğüm oluşturmaktadır. Oluşturulan bu yeni düğüm, ağ içinde kriptografi kullanılarak şifrelenir ve yayınlanır (Natarajan ve diğerleri, 2017, s. 1). Her yeni düğüm doğrulandıktan sonra zincire eklenir ve bu süreç, aynı zamanda birden fazla dağıtılmış defterde kayıt altına alınarak güncellenir (BIS, 2021).

Blok zincir teknolojisi, sahip olduğu özellikler (Lin & Liao, 2017, s. 653; Buțincu & Alexandrescu, 2023, s. 4; Fraga-Lamas & Fernandez-Carames, 2020, s. 56) bakımından dezenformasyonla mücadelede yenilikçi çözümler sunabilir:

1. Değiştirilemez olması
2. Merkeziyetsiz olması

3. Şeffaf ve izlenebilir olması
4. Verilerin dağıtık olarak tutulması (DLT)
5. Otonom ve akıllı sözleşmeler
6. Kriptografik Güvenlik
7. Konsensus Mekanizması

Blok zincir içerisindeki düğümlere kaydedilen bilgiler depolandıktan sonra değişmez ve değiştirilemez, sonsuza kadar saklanır. Bu özellik sayesinde haber ve bilgilerin güvenilir olmayan kaynaklar tarafından değiştirilmesinin önüne geçilir ve yanlış bilgilendirme ve dezenformasyonun yayılmasını önler. Haberler blok zincire kaydedildiğinde ilgili içeriğin doğruluğu garanti altına alınmış olur. Zira blok zincir üzerinde saklanan değiştirilemez dijital varlıklar olan NFT'ler, bu teknolojinin temel özelliği olan değiştirilemez oluşu sayesinde güvenilirlik ve orijinalliklerini korumaktadırlar. Blok zincir üzerinde yapılan her bir işlem zaman damgası ile kaydedilmektedir. Bu özellik sayesinde haber ve içeriklerin ne zaman üretildiği, paylaşıldığı ya da değiştirildiği hakkında bilgiler vererek içeriklere yapılan müdahaleler rahatlıkla tespit edilebilmektedir. Örneğin derin sahtecilik yolu ile üretilen bir politikacıya ait bir videonun sosyal ağlarda dolaşıma sokulması halinde dijital bir imza olan zaman damgası sayesinde videonun gerçek konuşmadan daha sonra üretildiği ve dezenformasyon amacıyla oluşturulduğu rahatlıkla anlaşılabilir. Benzer şekilde haberlerin çıkış kaynağını görmek ve takip etmek için de zaman damgası mühimdir.

Blok zincir merkeziyetsizdir. Karar alma mekanizmaları konvansiyonel medyada olduğu gibi tek bir merkezden sağlanmaz, herhangi bir otorite ya da merkeze bağlı olmadan çalışan sistemlere sahiptir. Bir diğer ifade ile veri yönetimi ve hizmetler dağıtık defterlerde birden fazla kullanıcının düğümler aracılığıyla veri girişi yapabilmesini sağlamaktadır. Bu da blok zinciri sansüre karşı dirençli bir yapı haline getirmektedir. Zincir üzerindeki yapılan işlemler ağdaki diğer bilgisayarlarda da tutulduğu için *DDos* gibi olası siber saldırılara karşı daha dayanıklı hale getirir. Öte yandan blok zincir üzerinde yapılan işlemler isteyen herkesin görebileceği şekilde şeffaf, izlenebilir olarak tasarlanmıştır. Kullanıcılar spesifik bir işlem ya da veri setinin geçmişini inceleyebilmektedir. Düğümler üzerinde yapılan her işlem zaman damgasıyla birlikte kaydedilir. Böylece bilginin kaynağı, verinin ne zaman yüklendiği ve güncellendiği takip edilebilmektedir. Bu özelliğin dezenformasyonla mücadeleye katkısı son derece önemlidir. Örneğin sosyal ağlarda dolaşıma sokulan bir haberin doğruluğunu kontrol etmek isteyen bir kullanıcı, blok zincir içerisinde ilgili haber kaynaklarının izini sürebilir ve haber eğer zincire kaydedilmişse, kullanıcı haberin güvenilirliğini teyit edebilir. Veyahut bir ilaca ya da gıdaya dönük olarak yanıltıcı bilgiler ağlarda dolaşmaktaysa tedarik zinciri düğümlere kaydedilmiş olmak kaydıyla tüketiciler ilacın üretiminden dağıtımına kadar olan süreci blok zincirinden takip edebilir. İlacın hangi ülke ve fabrikada üretildiği, hangi parti numarasına sahip olduğu ve ne zaman piyasaya sürüldüğü gibi tüketicileri

yakından ilgilendiren bilgilere ulaşılabilmektedir. Örneklerden de anlaşılacağı üzere zincirlere işlenen verilerin kaynağı, kullanıcıların bu süreçleri şeffaf bir şekilde takip edebilmesi dezenformatif içeriklerin çürütülmesine katkı sağlamaktadır.

Blok zincirde verilerin dağıtık defterlerde tutulması (DLT-*Distributed Ledger Technology*) dezenformasyonla mücadeleye katkı sağlayan bir başka özelliktir. DLT'ler kullanılarak herhangi bir olayın kaynağı ve ilgili bilgi ve belgeler zincire kaydedilmiş ise kullanıcılar bu bilgi ve belgelere erişebilir ve belgelerin doğru olup olmadığını anında teyit edebilir. Elbette bu, bilgi ve belgelerin asıllarının zincire kaydedilmesiyle mümkündür.

Blok zincir teknolojisi akıllı sözleşmelerle belli koşullar sağlandığı takdirde otonom hareket eden yazılım kodlarına sahiptir. İnsan müdahalesine gerek kalmadan, belirlenmiş kurallar çerçevesinde otonom olarak işlem yapabilmektedir. Örneğin; blok zincirdeki akıllı sözleşme kullanılarak yapılan bir alışverişte mal sahibi mülkün tapusunu akıllı sözleşmeye yükler, alıcı da öncesinde belirlenmiş miktarı yatırırsa koşullar yerine getirilmiş olur ve sistem otonom çalışarak akıllı sözleşme otomatik olarak mülkün tapusunu alıcıya aktarır. Aksi durumda ise şartlar yerine getirilmediği için anlaşma otomatik olarak iptal edilir. Örneğin sosyal medyada seçimlerin tarihinin değiştiğine ilişkin şüpheli bir haber dolaşıma girmişse bir haber platformunun "seçim kurulunun resmi web sitesindeki duyurularla haberi doğrula" şeklinde bir komut girmesi dezenformasyonun önüne geçecektir.

Blok zincirde güvenlik, kriptografik *hash* fonksiyonları ile sağlanmaktadır. Bu da verilerin değiştirilmesini zorlaştırır. Veriler üzerinde değişiklik yapılmaya çalışıldığında zincir üzerindeki tüm blokların *hash*leri de değişmek durumunda kalacaktır. Bir haber kaynağı, makale ya da haberlerin doğruluğunu kanıtlamak için her makalenin *hash*'ini zincire kaydedip yayınlandığında o makalenin artık değiştirilemeyeceğini güvence altına almış olur. Bu sayede herhangi bir makale ya da haber üzerinde işlem yapılamayacağı için asıl kaynağa zarar verilememiş olur. Bu da dezenformasyonla erken mücadelede katkı sunabilecek önemli bir fonksiyondur. Kriptografik güvenlik aynı zamanda kullanıcılar ve eser sahiplerinin haklarını koruyan bir donanıma sahiptir. Şöyle ki eser sahipleri, eserlerinin kullanımlarını blok zincire kaydederek eserleri üzerinde hak sahipliği elde etmiş olur. Eserleri üzerindeki yanlış, eksik bilgilendirmeler veyahut izinsiz kullanımlarda eser sahipleri haklarını kolayca kanıtlayabilir.

Blok zincir teknolojisinde *Proof of Work* veya *Proof of Stake* gibi iki farklı konsensus mekanizması vardır. Her iki sistem de ağın katılımcıları arasındaki güveni oluşturmak ve blok zincirin merkeziyetsiz yapısını korumak için tasarlanmıştır.

*Proof of Work*'te kullanıcılar blok zincir üzerinde işlemleri doğrulamak ve yeni bloklar oluşturmak için karmaşık matematiksel problemleri çözerek iş kanıtı sağlamış olurlar. Çözülen problemler karşılığında madenciler kripto para

birimleriyle ödüllendirilir. *Proof of Stake*'te ise yeni blok oluşturulabilmesi ve işlemlerin doğruluğunun sağlanması için kullanıcıların ellerinde tuttukları kripto paraları belli süreler boyunca 'stake' edip kilitlemeleri gerekmektedir. 'Stake işlemi' madenciliğe alternatif olarak bloklar üretmekte kullanılır. Bu iki uzlaşı mekanizmasının dezenformasyonla mücadelede sağlayabileceği faydayı örnekle açıklamak gerekirse *Proof of Work* tabanlı çalışan bir haber sitesinde bir gazeteci eksik, sahte veya aldatıcı nitelikte bir haber yayınlamaya çalışarak zincirlere haberi yüklemeye çalıştığında bu haberin blok zincire eklenebilmesi için zincir üzerinde aktif olan diğer haber platformları ya da gazetecilerin de bu haberi doğrulaması gerekecektir. Neticede sistem uzlaşı ile çalışmaktadır. Gazeteci eksik ya da yanıltıcı bir haberi blok oluşturmak için eklemeye çalıştığı durumda diğer madenciler (doğrulayıcılar) bu işlemi reddedecektir. Kullanıcılar ağda anonim olarak varlık gösterdiklerinden ve birbirlerini tanımadıklarından dolayı kolektif bir şekilde hareket etme imkanları sınırlanmaktadır. Anonimlik, bireylerin kimliklerinin gizli kalmasını sağlayarak ortak bir eylem geliştirmelerini zorlaştırmaktadır. Bu durum, ağ içindeki koordinasyonun sınırlı olarak sağlanmasını mümkün kılmaktadır. Ayrıca doğrulayıcılar (madenciler) teyit ettikleri haber karşılığında ödüllendirilebilir. Veyahut sahte bilgiyi yaymaya çalışanlar ekonomik olarak cezalandırılabilir. Esasında bu sistem bilgi ya da haber doğrulama ve teyit işleminin topluma yayılması ve kullanıcıların da süreç içerisine entegre edilmesi açısında kıymetlidir. *Proof of Stake* sisteminde teminat olarak yatırılan miktar olduğu için kripto paraların kaybedilme riski katılımcıları sahte bilgi yaymaktan caydırır ve doğru bilgiyi yaymaya yönlendirir. Ancak teorik açıdan konsensüs mekanizmalarının manipüle edilmesi mümkündür. Saldırgan ya da manipülatör, madencilik sürecinde eğer ki çok büyük bir hesaplama gücü ve enerji kaynağına sahipse ve karmaşık matematik problemlerini hesaplama gücü toplamda yüzde 51'den fazlaysa hesaplama veya doğrulama çoğunluğunu elinde bulundurduğu için kendi istediği şekilde bloklar ekleyebilir ve doğrulama sürecini manipüle edebilir. Ancak yüzde 51 gibi bir oranda hesaplama gücünün olması yüksek maliyet ve enerji isteyen bir işlem olmakla birlikte böyle bir saldırı, saldırgan için de zararlı sonuçlar doğuracaktır çünkü başarılı bir yüzde 51 saldırısı, blok zincir üzerindeki güveni zedeleyeceği için kripto para birimin değerinde de ani bir düşüş yaşanacaktır. Bu durum, saldırganın elinde bulundurduğu kripto varlıkların değerini de düşüreceğinden ekonomik olarak kendi çıkarlarına zarar verebilecek bir hamle yapmış olur.

## Yöntem

Bu çalışmada nitel yöntem, tematik veri analiz çözümleme tekniği kullanılmıştır. Tematik analiz, araştırma sorularına yanıt bulabilmek ve veri setlerinden anlamlı bulgular ortaya çıkarabilmek için kullanılan bir veri çözümleme tekniğidir. Bu tekniğin sunduğu avantaj veri setlerindeki anlam örüntülerini, sistematik olarak tanımlayarak düzenlemeye imkân vermekte ve bunlara ilişkin iç görüler sunabilmektedir. Bu sayede en küçük boyutlardaki veri setini dahi düzenlemek ve derinlemesine betimlemek mümkün olmaktadır (Braun & Clarke, 2019, s. 883).

Analizin ilk aşamasında alan yazın taraması yapılarak konuyla doğrudan ilgili olan yayınlar saptanmış, bu çalışmalarda blok zincir teknolojisinin dezenformasyonla mücadelede sunabileceği faydalara dönük kodlar araştırılmıştır.

Araştırmanın ikinci safhasında temalar oluşturulmuştur. Temaların oluşturulma süreci tümevarımsal olarak gerçekleştirilmiş ve araştırma sorularına yanıt verebilecek nitelikteki yayınların içerisinden çıkarılmıştır. Meta-sentez yöntemi kullanarak blok zincir teknolojisinin dezenformasyonu önlemede kullanılabileceği konusunu araştırarak daha önce yapılmış çalışmaların sonuçlarını bütünleştiren Kayıhan (2025)'ın çalışması yol gösterici olmuştur. 2017'den 2024'e kadar olan yapılan bildiri, kitap bölümü ve makale olmak üzere 18 çalışmada blok zincir teknolojisinin haber doğrulama ve dezenformasyonla mücadelede sunduğu ve sunabileceği faydalar ortaya konulmuştur (Huckle & White, 2017; Sylim ve diğerleri, 2018; Qayyum ve diğerleri, 2019; Hasan & Salah, 2019; DiCicco & Agarwal, 2020; Jurado ve diğerleri, 2020; Buțincu & Alexandrescu, 2023; Liu, ve diğerleri, 2022; Torky ve diğerleri, 2019; Fraga-Lamas & Fernandez-Carames, 2020; Marbouh ve diğerleri, 2020; Arquam ve diğerleri, 2021; Agrawal, ve diğerleri, 2021; Upadhyay & Baranwal, 2021; Guerar & Migliardi, 2022; Panigrahi, ve diğerleri, 2022; Alexandrescu & Butincu, 2023; Petratos & Faccia, 2023). Nihai olarak temalar bahsi geçen kaynaklardan faydalanılarak oluşturulmuştur:

*Tablo 1. Tümevarımsal kodlar*

| Sıra | Temalar |
|---|---|
| 1 | Veri doğrulama |
| 2 | Veri güvenirliği |
| 3 | Zaman verimliliği |
| 4 | Veri erişimi ve şeffaflık |
| 5 | Dezenformasyon yayılımı |
| 6 | Kullanıcı katılımı |
| 7 | Maliyet |
| 8 | Veri analiz ve raporlama |
| 9 | Sorumluluk ve hesap verebilirlik |
| 10 | İş birliği ve ağ oluşturma |
| 11 | Yenilik |

## Bulgular ve Yorum

*Tablo 2. Dezenformasyonla mücadelede geleneksel yöntemlerle blok zincirin karşılaştırılması*

| ***Geleneksel yöntemler*** | ***Blok zincir teknolojisi*** |
|---|---|
| **1-Veri Doğrulama** | |
| Elle yapılan inceleme ve doğrulama süreçlerine dayanmaktadır. *Fact-checker* (Doğrulama Uzmanları) tarafından yürütülür. | Kayıtların farklı defterlerde tutulması ve şeffaf, izlenebilir veri yapısı ile otomatik doğrulama imkânı sunar. Herkesin erişebileceği değiştirilemez kayıtlar oluşturulur. |
| **2-Veri Güvenirliği** | |
| İncelemeler editoryal bir süzgeçten geçtiği için güvenilirlik medya ve kurumların yapısına bağlıdır. | Verilerin güvenliği, kriptografi ile sağlanır. Kriptografi sayesinde zincire kaydedilen verilerin değiştirilmesi imkansıza yakındır. Bir haber, kriptografi ile şifrelendiği taktirde üzerinde işlem yapılamayacağı için asıl kaynağa zarar verilemez ve dezenformasyon oluşumunun önüne geçilir. |
| **3-Zaman Verimliliği** | |
| Doğrulama süreçleri, elle yapılan incelemelere ve merkezi otoritelere bağlıdır. Bu durum, incelemelerin eşik bekçileri tarafından kontrol edilmesi nedeniyle işlemlerin yavaşlamasına ve zaman kaybına neden olmaktadır. Sonuç olarak, bilginin hızlı bir şekilde doğrulanamaması, dezenformasyonun yayılma hızını artırmaktadır. | Veriler anlık şekilde doğrulanabilir ve anlık veri güncellemesi mümkündür. Verilerin anlık şekilde doğrulanabilmesi zaman verimliliğini artırır. Blok zincirde merkezi bir otorite yoktur. Veriler merkezi bir yerde değil, dağıtık defterlerde kaydedilir ve doğrulanır. Bu, süreçlerin hızlanmasını sağladığı gibi verilerin izlenebilmesi ve şeffaflığı da artırır. |
| **4-Veri Erişimi ve Şeffaflık** | |
| Verilerin kontrolü ve denetimi merkezi otoritelerce yürütülür. Bu durum erişim kısıtlığına sebep olabilir. Ayrıca geleneksel mücadele yöntemlerinde şeffaflık eksikliği söz konusu olabilir. | Blok zincir açık kaynak kodlu olduğu için daha şeffaf bir yapı sunar. Blok zincire teyitçiler verilerini rahatlıkla kaydederek verilerinin takibini yapabilir. Her işlem herkes tarafından anlık bir şekilde izlenebilir. Okuyucular da istedikleri taktirde verileri anlık olarak kontrol ederek doğrulanmasına katkıda bulunabilir. |

| **5-Dezenformasyon Yayılımı** | |
|---|---|
| Şüpheli bilgilerin doğruluğunun kontrol edilmesi ve teyit edilmesi zaman aldığı için dezenformasyona karşı tepki almakta gecikilebilir. | Blok zincirin otonom çalışan akıllı sözleşmeleri doğrulama sürecini otomatikleştirebildiği için dezenformasyonla erken mücadele mümkündür. Öte yandan blok zincir kullanıcıları da istenildiği taktirde doğrulama süreçlerine katkıda bulunabildiği için sahte veya yanlış bir içerik tespit edildiğinde, bu durum hızlı bir şekilde paylaşılabilir ve düzeltilebilme imkânı vardır. |
| **6-Kullanıcı Katılımı** | |
| Geleneksel yöntemlerde bilgi doğrulama ve teyit işlemi çoğunlukla uzmanlar tarafından yapılır ve okuyucular sürece ya dahil edilmez ya da sınırlı olarak katkıda bulunurlar.<br><br>Okuyucular şüpheli bilgi ve içeriğe karşı teyitçilere geri bildirimde bulunabilir. Ancak ihbar edilen şüpheli bilginin incelenmesi zaman alacağı için geri bildirimlerin her birinin özel olarak incelenmesi mümkün gözükmemektedir.<br><br>Bu durumda bir filtreleme yapılarak dezenformasyonun yayılım hızı ve gündem belirleme yoğunluğu göz önünde bulundurularak bazı iddiaların peşine düşülür. | Blok zincir teknolojisi kullanıcılarına kaydettikleri verileri anlık bir şekilde izleyebilme imkânı sunmaktadır.<br><br>Kullanıcılar doğrulama sürecinin doğrudan içindedir. Örneğin; haber servisleri kaynağına ve doğruluğuna güvendiği haberleri blok zincir kullanarak habere ilişkin her türlü (rapor, röportaj, belge, görsel, video) veriyi bloklara kaydederse veriler zaman damgasıyla birlikte diğer okuyucuların görebileceği şekilde zincirde izlenebilir. Kullanıcılar da ilgili haberin zaman damgasına bakarak orijinal kaynağını görür ve teyit etmiş olur.<br><br>Öte yandan teyit merkezleri okuyucuları doğrulama süreçlerine katkıda bulunmaları karşılığında blok zincirin tokenleri ile onları ödüllendirebilir. |
| **7-Maliyet** | |
| Geleneksel dezenformasyonla mücadelede verilerin doğrulanması ve teyit edilmesi sürecinde birçok kişi aktif olarak rol alır. Editörler, denetleyiciler ve diğer personellere sürekli maaş ödemeleri yapılır, bu da maliyetleri artırır. Ayrıca incelemeler elle yapıldığı için hataya daha müsaittir. Hataların düzeltilmesi de bir maliyet ortaya çıkarmaktadır. Zira teyit platformları merkezi yönetimden ve vakıflardan alınan fonlar, hibe ve desteklerle faaliyetlerini yürütmektedir. | Blok zincirle yapılan doğrulamalarda insan gücü maliyetleri daha düşüktür. Doğrulama süreçleri otomatikleştirilebildiği için daha düşük işlem maliyeti ortaya çıkmaktadır. Ancak bazı blok zincir projelerinde kullanılan PoW (*Proof Of Work*) madencilik yapmaya yarayan uzlaşı mekanizması yüksek enerji tüketimine sebep olmaktadır. |

| **8-Veri Analiz ve Raporlama** | |
|---|---|
| Geleneksel dezenformasyonla mücadele tekniklerinde analiz ve raporlama süreçleri (veri toplama, işleme, analiz etme ve raporlama) birçok işlemden geçer. Bu süreçler insan hatasına açık olmakla beraber zaman alıcı ve zahmetlidir. | Blok zincirde veri analiz süreci otomatikleştirilebilir. Gerçek zamanlı raporlar hazırlamak mümkündür. Veriler anlık olarak izlenebildiği için karar alma süreçleri hızlıdır. |
| **9-Sorumluluk ve Hesap Verebilirlik** | |
| Doğrulama mekanizmaları merkezi bir otoriteye bağlıdır. Merkezi otoriteyi fonlayan kuruluşlar, otorite üzerinde tahakküm kurmak isteyerek doğrulama platformlarının bağımsız çalışmalarını engelleyebilir. Öyle ki Türkiye'de faaliyet gösteren bazı teyit kuruluşlarının siyasi partilerce fonlandığı bilinmektedir. Bu durum, teyitçilerin editoryal bağımsızlıklarına gölge düşürmektedir.<br><br>Merkezileşmiş doğrulama mekanizmalarında insan hatalarının sorumluluğundan ziyade organizasyonel sorumluluk ve hesap verilebilirlik vardır. | Blok zincir doğası gereği merkeziyetsiz olarak inşa edilmiştir. Herhangi bir otoriteye bağlı olmadığı için baskı altına alınması daha zordur.<br><br>Blok zincir de doğrulama süreci şeffaf bir şekilde paylaşılıp izlenebilir. İstenildiği taktirde tüm işlemler kullanıcıların gözleri önünde şeffaf bir şekilde ortaya konabilir. |
| **10-İş Birliği ve Ağ Oluşturma** | |
| İş birliği sınırlı ve okuyucu geri bildirimleri yeterince dikkate alınmaz ve okuyucular doğrulama sürecine çoğunlukla dahil edilmez. | Blok zincirde çok yönlü bir iletişim söz konusudur ve bir otorite etrafında olmadan eşit koşullarda etkileşimde bulunabilirler. Blok zincir farklı alanlara entegre çalışan bir sistemdir. Bir teyit kuruluşuyla sistemsel anlamda entegrasyon ve dolayısıyla iş birliği yapılabileceği gibi bir lojistik şirketiyle, eğitim kurumuyla da iş birliğine ve ağ oluşturmaya açıktır.<br><br>Blok zincirde kullanıcılar ve topluluklar teyit sürecine doğrudan ve dolaylı katkı sunarak iş birliğinin parçası olabilir. Ödül sistemiyle de kullanıcılar ödüllendirilebilir. |

| 11-Yenilik | |
|---|---|
| Geleneksel mücadele tekniklerinde yeniliklere daha yavaş adapte olunur.<br><br>Ses klonlama, *deepfake*, algoritma manipülasyonu gibi yeni tip dezenformasyonlara karşı mücadele teknikleri çoğunlukla yazılım kullanılmadan yapılmaktadır.<br><br>Dolayısıyla yeniliklere daha dirençli bir yapı vardır. | Blok zincir yeni gelişme ve projelere açık bir yapı sunar. Yapay zekâ, 5G, 6G, IoT gibi, teknolojinin diğer alanlarına entegre çalışan sistemleri vardır.<br><br>Yeni türden dezenformasyonlara karşı piksel analizi, renk ve doku analizi gibi gelişmiş inceleme ve analiz sistemleri vardır. |

*Tablo 2*'de dezenformasyonla mücadelede geleneksel tekniklerle blok zincir tabanlı sistemlerin karşılaştırılması yer almıştır. Karşılaştırması yapılan kodlar birbirleriyle ilişkili olduğu için sırasıyla yorumlamaktan ziyade harmanlanarak değerlendirilmiştir.

Haber ve veri doğrulama süreçlerinde geleneksel yöntemler, genellikle elle olarak yapılan incelemelere dayandığı için bu sürecin doğrulama uzmanları veya *fact-checker*'lar tarafından yürütülmesi insan faktörüne bağlı olarak hata riski taşıdığı görülmüştür. Çünkü insan doğası gereği politik, kültürel ve bireysel önyargılardan etkilenebilir. Bu da tamamen nesnel ve tarafsız bir değerlendirme yapmayı zorlaştırmaktadır. Lakin blok zincir teknolojisinin sunduğu yenilikçi teknikler doğrulama süreçlerini daha şeffaf, izlenebilir ve otomatikleştirebilmesi hem zaman ve maliyet açısından verimliliği artırmakta hem de doğrulama işlemlerini merkeziyetsiz bir yapıda gerçekleştirerek, insan müdahalesine dayalı hataları ve önyargıları minimize etmektedir. Bu sayede doğrulama süreçleri daha objektif ve şeffaf hale gelir, verilerin doğruluğu daha güvenli bir şekilde sağlanarak merkezi otoritenin etkisi azaltılmış olacaktır. Bunun, özellikle doğrulama süreçlerine güvenin artırılmasına ve manipülasyon risklerinin düşürülmesine yardımcı olacağı düşünülmektedir.

Geleneksel yöntemlerdeki incelemelerde verilerin güvenirliği editoryal süreçler ve kurumların sahiplik yapısına bağlı olarak değişmektedir. Bu durum doğrulama sürecinde veri güvenirliği sorununu karşımıza çıkarmaktadır. Netice itibariyle editoryal süreç içerisindeki tüm insan müdahaleleri, doğrulama süreçlerini manipüle edebilir. Hatta doğrulama yapan kurumun ekonomi politik yapısı, haber doğrulama sürecinde sansür uygulama riskini ortaya çıkarabilir. Çünkü bu tür yapılar, ekonomik veya ideolojik çıkarlar doğrultusunda belirli haberlerin doğruluğunu manipüle edebilir ya da sansürleyebilir. Böylece, haberin doğruluğu yerine, kurumun çıkarları doğrultusunda bir doğrulama süreci işleyecektir. Zira Türkiye'de, siyasi partilere yakın doğrulama kuruluşlarının varlığı, bu durumu daha anlaşılır kılmaktadır. Öte yandan blok zincir teknolojisi doğrudan merkeziyetsiz bir yapı üzerine bina edildiği için manipülasyon riski oldukça zordur. Blok zincirde verilerin güvenliği güçlü kriptografik algoritmalarla sağlandığı için verilerin değiştirilmesi veya manipüle edilmesi neredeyse imkânsız hale gelmektedir. Bu durum, verilerin güvenilirliğini artırarak haberin

asıl kaynağına zarar verilmesini engeller ve dezenformasyonun önlenmesine yardımcı olur. Verinin bütünlüğü, güvenilirliği ve doğruluğu bu şekilde güvence altına alınır. Öte yandan verilerin zincire kaydedilmesi ve akıllı sözleşmelerle otomatikleştirilebilen doğrulama süreçlerine sahip olması blok zinciri, insan ve kurumların ön yargı ve olası manipülatif işlemlerden koruyabileceği anlamına gelmektedir.

Geleneksel haber doğrulama süreçlerinde bilginin hızlı bir şekilde doğrulanamaması, dezenformasyonun yayılma hızını artırmaktadır. Doğrulama süreçlerinin elle yapılan incelemelere ve merkezi otoritelere dayandığı için oldukça maliyetlidir. Sürecin insan kaynağına dayalı olarak yürütülmesi hem zaman açısından verimsizdir hem de uzun vadede yüksek iş gücü maliyetlerine yol açmaktadır. Doğrulama süreçlerinin yavaş ilerlemesi, karar alma sürecinde gecikmelere ve dolayısıyla iş kayıplarına neden olduğu düşünülmektedir. Ancak, blok zincir teknolojisi doğrulama sürecini büyük oranda insan kaynağından bağımsız olarak yürütebileceği için maliyetleri düşürmektedir. Özellikle tekrarlayan işlerin otomatikleştirilmiş blok zincir akıllı sözleşmelerle yürütülmesi insan kaynağından doğan maliyetleri düşürdüğü gibi zaman verimliliği de sağlamaktadır. Verilerin anlık bir şekilde doğrulanabilmesini mümkün kılan blok zincir teknolojisi, dezenformasyonla erken mücadelede önemli bir rol oynayabilir. Haberler hızla yayıldıkça, yanlış bilginin doğruluğu da hemen kontrol edilmelidir. Blok zincir anlık veri doğrulama özelliği sayesinde, bilgi kaynağının doğruluğunu anında tespit ederek ve doğrulama sürecini hızlandırabilir. Bu sayede yanlış veya yanıltıcı bilgilerin yayılması önlenebilir.

Blok zincir, açık kaynak kodlu yapısı sayesinde daha şeffaf bir ortam sunmaktadır. Blok zincir üzerinde veriler, teyitçiler tarafından kolayca kaydedilip ve takip edilebilir. Ayrıca her işlem anlık olarak herkes tarafından izlenebilir ve isteyen kullanıcılar doğrulama sürecine katkı sağlayabilir. Bu sayede daha şeffaf bir veri erişimi sağlanabilir. Geleneksel yöntemlerde, bilgi doğrulama süreçleri, genellikle uzmanlar tarafından yapılır ve okuyucular doğrulama sürecine sınırlı katkı sağlamaktadır. Blok zincir teknolojisi ise kullanıcıların kaydettikleri verileri anlık olarak izleyebilmesini sağlamaktadır. Haber servisleri, güvenilir kaynaklardan aldıkları verileri blok zincir üzerinde zaman damgasıyla kaydederek doğrulama sürecini şeffaf hale getirebilir. Kullanıcılar da zaman damgası sayesinde orijinal kaynağa ulaşarak veriyi doğrulayabilir. Ayrıca teyit merkezleri, doğrulama sürecine katkı sağlayan okuyucuları 'blok zincir tokenleri' ile ödüllendirerek doğrulama süreçlerinde kullanıcı katılımını teşvik edebilir. Öte yandan geleneksel sistemde iş birlikleri ve okuyucu geri bildirimleri sınırlıdır. Zira bunlar zaman ve insan kaynağı isteyen kalemlerdir. Bu sebeple okuyucular doğrulama süreçlerine çoğunlukla dahil edilmemektedir. Ancak blok zincir, merkezi bir otorite olmadan, eşit koşullarda çok yönlü bir iletişim imkânı ile farklı iş sahaları arasında (teyit kuruluşları, lojistik şirketleri ve sağlık, turizm, teknoloji, eğitim kurumları) entegrasyon sağlama potansiyeli sunarak iş birliği yapma ve ağ oluşturma fırsatı sağlamaktadır. Kullanıcılar ve topluluklar, doğrulama sürecine doğrudan veya dolaylı katkı sağlayarak iş birliğinin parçası olabilmektedir.

Teyit işleminin son basamağı olan analiz ve raporlama süreci açısından da blok zincirin yenilikçi yaklaşımlar sunduğu görülmüştür. Özellikle veri analiz sürecinin otomatikleştirebilmesi ve eş zamanlı raporlar alabilmeyi mümkün kılan yapısı sayesinde anlık bilgi ve haber doğrulama raporları elde edilebilir. Bu da karar alma süreçlerini hızlandırarak dezenformasyonun önüne geçen önemli bir etkendir.

**Tartışma ve Sonuç**

Sosyal ağların oluşumunun arkasındaki web 2.0 teknolojisiyle birlikte kullanıcılar yalnızca bilginin salt tüketicisi olmaktan çıkmış, aynı amanda içerik üretim sürecine de aktif olarak katılmaya başlamıştır. Kullanıcıların içerik üretim sürecine dahil olması yalan, eksik veya yanıltıcı bilgilerin dolaşımını artırarak gerçeklerin çarpıtılması ve kamuoyunun yanıltılması gibi dezenformasyon ve manipülasyon sorunlarını da beraberinde getirmiştir. Dezenformasyonun kamuoyu algısının şekillendirilmesi noktasında yapılan çalışmalar gösteriyor ki sahte haberlerin insanların tutum ve eğilimlerini etkilediği ve politikacılara yönelik güvensizliği tetiklediği yine siyasi ve toplumsal kutuplaşmayı filizlendirerek seçmenler arasında çatışmaları körüklediği görülmüştür. Bu açıdan bakıldığında dezenformasyon toplumsal güveni ve kohezyonu parçalayarak sosyal çözülmeyi ortaya çıkaran toplumsal bir patolojik durumdur. Bu sebeple enformasyon bombardımanın en yoğun olduğu bu dönemde dezenformasyon farklı düzeylerde mücadele edilmesi gereken en önemli gündem maddesidir. Zira dezenformasyonun yıkıcı etkileri, birçok hükümet, ulusal ve uluslararası sivil toplum kuruluşları, üniversiteler ve doğruluk kontrolörlerinin dikkatini bu yöne çekmiştir. Enformasyon akışındaki yoğunluğun artışına bağlı olarak verilerin doğrulanması ve teyit edilmesine olan talep de büyük bir artış vardır. Birçok hükümet dezenformasyonla mücadeleyi yasal bir zemine oturtarak farklı önlem ve stratejiler geliştirmektedir. Ancak dezenformasyon, medya teknolojilerindeki yeniliklere hızla adapte olarak sürekli farklı maskelerle karşımıza çıkarken, bu sorunun önlenmesine yönelik stratejiler hâlâ büyük ölçüde geleneksel yöntemlerle sınırlı kalmaktadır. Gerçeklik kontrol süreçlerinin büyük ölçüde hala elle yapılan incelemelere dayandırılması hem zaman verimliliğini düşürmekte hem de işlemi oldukça zahmetli hale getirmektedir. Bu, dezenformatif bilgilerin gerçekleri geride bırakmasının temel sebeplerindendir. Bu çalışma dezenformasyonla mücadeledeki tam olarak bu kısıtlılıklara odaklanarak, bilgi doğrulama ve teyit sürecinin blok zincir teknolojisiyle nasıl daha verimli ve hızlı bir hale getirilebileceğini tartışarak sürece sunabileceği katkıları irdelemiş ve şu sonuçlar ortaya konulmuştur:

Blok zincir teknolojisi sahip olduğu özelliğin bir gereği olarak düğümlerine kaydedilen bilgiler değiştirilemez ve sonsuza dek saklanır. Bu sayede haber ve bilgilerin güvenilir olmayan kaynaklar tarafından değiştirilmesi engellenerek, dezenformasyonun oluşmasının ve yayılımının önüne geçilir. Yeni nesil dezenformasyon tiplerinden *deepfake*, ses klonlama, otomatik metin ve haber üre-

timi gibi sahte içeriklere karşı etkili bir mücadele sağlayabilir. Çünkü orijinal metin ya da video, blok zincire kaydedildiği taktirde belge niteliği taşıyan asıl kayıt zaman damgasıyla birlikte zincirde kayıtlı durduğu için haber ve içeriklerin ne zaman üretildiği, paylaşıldığı ya da güncellendiği hakkındaki meta veriler sağlanabildiği için orijinal içeriklere yapılabilecek müdahaleler tespit edilebilir. Özetle, blok zincir, görsel işitsel materyallerin orijinalliğini doğrulayabilir, içerikler oluşturulduğu andan itibaren blok zincire kaydedilirse değişiklikler izlenebilir böylece sahte içerikler tespit edilerek belgelendirilebilir.

Blok zincir tabanlı sistemler kimlik doğrulama amaçlı kullanabilir. Bu sayede dezenformasyonun kaynağı olabilecek sahte hesaplar, bot ve trol ağlarının tespit edilebilmesi sağlanabilir.

Merkeziyetsiz yapıya sahip olan blok zincir de karar alma süreçleri tek bir otoriteden sağlanmamaktadır. Verilerin yönetimi, dağıtık defterlerde birden fazla kullanıcı katılımı ile sağlanır. Haber ve içeriklere ilişkin verilerin aynı anda farklı defterlerde tutuluyor olması blok zinciri olası *Ddos* gibi siber saldırılara karşı dayanıklı yaptığı gibi sansüre karşı da dirençli bir yapı oluşturur. Öte yandan zincir üzerinde işlemler şeffaf ve izlenebilir şekilde tasarlanarak, okuyucular daha öncesinde kaydedilen haber ya da bilgilerin geçmişini, bilginin kaynağını ve güncellenme tarihi gibi verileri izleyebilir. Blok zincirin sunduğu bu özellik dezenformasyonla mücadelede kritik bir öneme sahiptir; kullanıcılar, sosyal medyada dolaşan haberlerin güvenilirliğini sistem sayesinde kontrol edebilir.

Blok zincir otomatik haber doğrulama için de bir potansiyel sunabilmektedir. Sistem akıllı sözleşmelerle belirli koşullar yerinde getirildiğinde otomatik çalışacak şekilde dizayn edildiği için bir haberin belirli tarih ve saat aralığında doğru olup olmadığı teyit edilebilir. Ancak zincire kasıtlı bir şekilde yanlış ya da yalan bilgiler kaydedilirse bu durum otomatik doğrulama süreçlerinin de manipüle edilmesine sebebiyet verecektir. Bu durumun önüne geçmek için içeriklerin yalnızca güvenilir ve doğrulanmış kaynaklar tarafından kaydedilmesi sağlanmalıdır. Yalnızca bazı medya kuruluşları ve Uluslararası Doğrulama Ağı'na kayıtlı doğrulama platformları tarafından veri girişinin yapılması bu durumun önüne geçecektir.

Blok zincir, verilerin güvenilirliği sağlamakta ve doğrulama süreçlerinde kullanıcıları sisteme dahil etmektedir. Madencilik (PoW) ya da 'stake' (PoS) gibi konsensüs mekanizmaları ile kullanıcılar doğrulama süreçlerinde katılarak sağladıkları fayda üzerinden ödüllendirilir. Blok zincirle çalışan doğrulama platformlarında kullanıcılar da dezenformasyonla mücadeleye katkı sunarak tokenizasyonlarla ödüllendirilebilir. Bu doğrulama süreçlerinde kullanıcıların katılımını teşvik edecektir.

Blok zincir anlık doğrulama raporları sunabilir ve zincirde kaydedilen verilerin izi rahatlıkla sürülebilir. Bu dezenformasyon erken tespiti için oldukça kıymetlidir.

Blok zincir gelişen bilgi ve iletişim teknolojilerine entegre çalışarak yapay zekâ, artırılmış gerçeklik, sanal gerçeklik, nesnelerin interneti, 5G, 6G gibi entegrasyonlarla dezenformasyonun yeni türlerine karşı ortaklık ve iş birliği içerisinde mücadele imkânı sunmaktadır. Zira dezenformasyonla mücadelede her ne kadar blok zincir yenilikçi çözümler getirmiş olsa bile kirli bilgi ile mücadelede tek başına kullanılabilecek bir sistem sunmamaktadır. Muhakkak yapay zekâ, makine öğrenmesi ile bütünleştirilerek kullanılması dezenformasyonla mücadelede daha büyük fayda sağlayarak ve daha güvenilir ve sağlam bir bilgi ekosisteminin inşasında önemli bir adım olacaktır.

Ortaya çıkan sonuçlar açıkça göstermektedir ki, blok zincir teknolojisi gerek dezenformasyonla erken mücadele de gerekse de dezenformasyonun tespiti ve yayılımında yenilikçi çözümler sunmaktadır. Geleneksel mücadele teknikleri ise dezenformasyonun hızına yetişememektedir. Bu sebeple doğruluk ve teyit platformları, haber servisleri blok zincir teknolojisinin sağladığı faydaları göz önünde bulundurup mevcut sistemlerini blok zincire entegre ederek ondan faydalanmalıdır. Dezenformasyonun yeni tiplerine karşı mücadelede inovatif çözümler geliştirilmeli yapay zekâ ve blok zincir teknolojisi birlikte kullanılmalıdır. Gelişmeler, dezenformasyon mücadelesinin sadece teyitçiler tarafından ele alınmasının yetersiz olduğunu göstermektedir. Etki boyutu, sorunun karmaşıklığı, bilgi akışındaki artan yoğunluk gibi faktörler dezenformasyonla mücadelede bilişim uzmanları, veri bilimciler ve diğer disiplinlerden uzmanların iş birliği yapmasını zorunlu kılmaktadır. Çünkü dezenformasyonun yıkıcı etkileri toplumun farklı kesimlerinde herkes tarafından derinden hissedilmektedir. Dezenformasyon toplumsal bir problem olduğuna göre mücadele de multidisipliner bir yaklaşım ile farklı aktörlerin iş birliğini gerektirmektedir. Örneğin, devlet kurumları, resmi bilgi kaynaklarının güvenilirliğini artırmak amacıyla blok zincir tabanlı doğrulama mekanizmaları oluşturabilir. Seçim süreçlerinde yayılan dezenformasyonu engellemek için kamu kurumları, resmi açıklamalarını blok zincir üzerinde kayıt altına alarak manipülasyonu önleyebilir. *Meta*, *X* veya *Google* gibi platformlar, blok zincir destekli bir doğrulama sistemi kullanarak kullanıcıların paylaştığı haberlerin güvenilirliğini artırabilir. Gazeteciler ve medya kuruluşları, blok zincir teknolojisini kullanarak içeriklerinin orijinalliğini kanıtlayabilir ve okuyucuların güvenini artırabilirler. Sivil toplum kuruluşları, medya okuryazarlığını artırmaya yönelik blok zincir tabanlı uygulamalar geliştirerek, kullanıcıların sahte haberleri tespit etmesine yardımcı olabilirler. Öte yandan hukuk çerçevesinde de düzenlemeler getirilerek, blok zincir tabanlı sistemlerin nasıl şekilleneceği, blok zincir tabanlı dezenformasyonla mücadele araçlarının etkinliği, düzenleyici çerçevelerin oluşturulmasını tartışmalı ve somut adımlar atılmalıdır. Blok zincir üzerinde saklanan bilgilerin kim tarafından doğrulanacağı ve yanlış bilgi yayılması durumunda kimin sorumlu tutulacağı belirlenmelidir. Dezenformasyonun küresel bir problem olduğu göz önüne alındığında, blok zincir tabanlı çözümlerin uluslararası düzeyde uygulanabilirliği değerlendirilmelidir. Dezenformasyonun hızı, yönü, miktarı, türleri göz önüne getirildiğinde bu mücadele sadece teyitçilerin sırtına bırakılmamalı,

devlet, özel sektör, sivil toplum kuruluşları, üniversiteler ve medya iş birliği yaparak sistematik yaklaşımlar geliştirilmelidir.

**Kaynakça**

Agrawal, P., Anjana, P. S., & Peri, S. (2021). DeHiDe: Deep learning-based hybrid model to detect fake news using blockchain. *Proceedings of the 22nd International Conference on Distributed Computing and Networking* (ss. 245-246). Association for Computing Machinery.

Alexandrescu, A., & Butincu, C. N. (2023). Decentralized news-retrieval architecture using blockchain technology. *Mathematics*, *11*(21), 4542.

Arquam, M., Singh, A., & Sharma, R. (2021). A blockchain-based secured and trusted framework for information propagation on online social networks. *Social Network Analysis and Mining*, *11*(1), 49.

Atalay, G. E. (2018). Blok zincir teknolojisi ve gazeteciliğin geleceği. *Stratejik ve Sosyal Araştırmalar Dergisi*, *2*(2), 45-54. https://doi.org/10.30692/sisad.440148

Babar, A., Shukla, A., Jagtap, N., Chaudhari, P., & Mithari, A. (2020). News tracing system using blockchain. *International Journal of Engineering Research & Technology*, *5*(2), 554-562.

Balmas, M. (2014). When fake news becomes real: Combined exposure to multiple news sources and political attitudes of inefficacy, alienation, and cynicism. *Communication Research*, 41(3), 430-454. https://doi.org/10.1177/0093650212453600

Bennett, W. L., & Livingston, S. (2023). A brief history of the disinformation age: Information wars and the decline of institutional authority. *Streamlining political communication concepts: Updates, changes, normalcies* içinde (ss. 43-73). Springer International Publishing.

BIS (Bank of International Settlements). (2015). Committee on payments and market infrastructures digital currencies. https://www.bis.org/cpmi/publ/d137.pdf adresinden erişilmiştir.

Birhade, K., Wani, N., Bhosale, S., Jadhav, P., & Raje, S. (2023). *Enhancing security and transparency: The role of blockchain in document verification.* SSRN 4659924.

Braun, V., & Clarke, V. (2019). Psikolojide tematik analizin kullanımı (S. N. Şad, N. Özer, ve A. Atli, Çev.). *Eğitimde Nitel Araştırmalar Dergisi - Journal of Qualitative Research in Education, 7*(2), 873-898. https://doi.org/10.14689/issn.2148-2624.1.7c.2s.17m

Buțincu, C. N., & Alexandrescu, A. (2023). Blockchain -based platform to fight disinformation using crowd wisdom and artificial intelligence. *Applied Sciences*, *13*(10), 6088.

DiCicco, K. W., & Agarwal, N. (2020). Blockchain technology-based solutions to fight misinformation: A survey. Disinformation, Misinformation, and Fake News in

Social Media. *Emerging Research Challenges and Opportunities*, 267-281.

Fallis, D. (2015). What is disinformation? *Library Trends*, *63*(3), 401-426.

Fraga-Lamas, P., & Fernandez-Carames, T. M. (2020). Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. *IT Professional*, *22*(2), 53-59.

Guerar, M., & Migliardi, M. (2022). TruthSeekers chain: Leveraging invisible CAPPCHA, SSI and blockchain to combat disinformation on social media. *International Conference on Computational Science and Its Applications* (ss. 419-431). Springer International Publishing.

Hasan, H. R., & Salah, K. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access*, 7, 41596-41606.

Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament. https://data.europa.eu/doi/10.2861/280969

Huckle, S., & White, M. (2017). Fake news: A technological approach to proving the origins of content, using blockchain. *Big Data*, *5*(4), 356-371.

Jurado, F., Delgado, O., & Ortigosa, Á. (2020). Tracking news stories using blockchain to guarantee their traceability and information analysis. *IJIMAI*, *6*(3), 39-46.

Kayıhan, B. (2025). Dezenformasyonun önlenmesine yönelik blok zinciri teknolojisinin kullanımı. *TRT Akademi*, *10*(23), 266-303. https://doi.org/10.37679/trta.1560520

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653-659.

Liu, Y., Hao, X., Ren, W., Xiong, R., Zhu, T., Choo, K. K. R., & Min, G. (2022). A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things. *IEEE Transactions on Computers*, *72*(2), 501-512.

Marbouh, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., ... & Ellahham, S. (2020). Blockchain for COVID-19: Review, opportunities, and a trusted tracking. *Arabian Journal of Science for Engineering*, *45*(12), https://doi.org/9895-9911 10.1007/s13369-020-04950-4

Meghana, G. R., Prashantha, G. R., Akshatha, P., Anisha, M., & Naveen, J. K. (2023). Tracing and tracking of fake news detection. *International Journal of Engineering Research & Technology, 11*(05).

Natarajan, H., Krause, S., & Gradstein, H. (2017). Distributed ledger technology and blockchain. *World Bank*. https://hdl.handle.net/10986/29053

Önder, B. A., & Koç, N. E. (2024). Disinformation with artificial intelligence in algorithmic societies: An analysis of political leaders. *Turkish Online Journal of Design Art and Communication, 14*(3), 629-647. https://doi.org/10.7456/tojdac.1464241

Upadhyay, A., & Baranwal, G. (2021). *Fake news detection using ethereum blockcha-*

*in*. In International Conference on Advanced Network Technologies and Intelligent Computing (pp. 142-152). Springer.

Panigrahi, S., Rai, A. K., Rajput A. K., Bhardwaj, A. (2022). Fake news detection using blockchain. *International Journal for Research in Applied Science and Engineering Technology. (IJRASET), 10*(3), 2442-2445.

Petratos, P. N., & Faccia, A. (2023). Fake news, misinformation, disinformation and supply chain risks and disruptions: Risk management and resilience using blockchain. *Annals of Operations Research*, *327*(2), 735-762.

Piper, P. S. (2002). Web hoaxes, counterfeit sites, and other spurious information on the Internet. Anne P. Mintz and Steve Forbes (Ed). *Web of deception: Misinformation on the Internet* içinde(ss. 1-22). CyberAge Books.

Qayyum, A., Qadir, J., Janjua, M. U., & Sher, F. (2019). Using blockchain to rein in the new post-truth world and check the spread of fake news. *IT Professional*, *21*(4), 16-24.

Qian, F., Gong, C., Sharma, K., & Liu, Y. (2018, July). Neural user response generator: Fake news detection with collective user intelligence. *IJCAI 18* içinde (ss. 3834-3840).

Shae, Z., & Tsai, J. (2019). AI blockchain platform for trusting news. *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* içinde (ss. 1610-1619). https://doi.org/10.1109/ICDCS.2019.00160

Shang, W., Liu, M., Lin, W., & Jia, M. (2018, June). Tracing the source of news based on blockchain. İçinde *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)* (ss. 377-381). *IEEE*.

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T. H., Ding, K., Karami, M., & Liu, H. (2020). Combating disinformation in a social media age. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(6), e1385.

Song, G., Kim, S., Hwang, H., & Lee, K. (2019, Ocak). Blockchain -based notarization for social media. *2019 IEEE International Conference on Consumer Electronics* (*ICCE*) içinde (ss. 1-2). IEEE.

Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. *JMIR research protocols*, *7*(9), e10163.

Takan, S., & Ergün, D. (2024). FAIR prensipleriyle uyumlu gözlemlenebilen ve izlenebilen sosyal medya tabanlı dijital habercilik veri modeli. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *39*(2), 1153-1166.

Torky, M., Nabil, E., & Said, W. (2019). Proof of credibility: A blockchain approach for detecting and blocking fake news in social networks. *International Journal of Advanced Computer Science and Applications*, *10*(12).

Türker, G. F., & Tanyeri, K. (2024). Blokzincir teknolojisi ile nesnelerin interneti tabanlı (IoT) sistemlerin veri güvenliğinin sağlanması. *Gazi University Journal of Science Part C: Design and Technology*, *1*(1).

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146-1151. https://doi.org/10.1126/science.aap9559

Virilio, P. (2003). *Enformasyon bombası* (K. Şahin, Çev.). Metis Yayınları.

Wang, X., Xie, H., Ji, S., Liu, L., & Huang, D. (2023). Blockchain -based fake news traceability and verification mechanism. *Heliyon*, *9*(7).

Yıldırım, A., & Şimşek, H. (2003). *Sosyal bilimlerde nitel araştırma yöntemleri.* Seçkin Yayınları.

Zhang, X., & Ghorbani, A. A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management*, *57*(2), 102025. https://doi.org/10.1016/j.ipm.2019.03.004

***Etik Kurul Onayı:*** Etik kurul onayına ihtiyaç bulunmamaktadır.
***Çıkar çatışması:*** Çıkar çatışması bulunmamaktadır.
***Finansal destek:*** Finansal destek bulunmamaktadır.
***Yazar Katkı Oranı:*** Y. Toktay (%50), A. Güven (%50)

***Ethics committee approval:*** There is no need for ethics committee approval.
***Conflict of interest:*** There are no conflicts of interest to declare.
***Financial support:*** No funding was received for this study.
***Author contribution rate:*** Y. Toktay (50%), A. Güven (50%)