



Blockchain Tabanlı Bilimsel Veri Yönetimi: Açık Bilim ile Veri Güvenliği Arasındaki Etik Denge

Blockchain-Based Scientific Data Management and Ethical Standards

Eda KILIÇ¹, Hasan Tahsin KEÇELİGİL²

¹Ondokuz Mayıs Üniversitesi, Sağlık Bilimleri Fakültesi, Samsun

²Ondokuz Mayıs Üniversitesi Tıp Fakültesi ve Ali Fuad Başgil Hukuk Fakültesi, Samsun

ORCID:

E.K.: 0006-6666-8910

HTK.: 0000-0002-8256-8059

Corresponding Author:

Eda KILIÇ

Email:

24282344@stu.omu.edu.tr

Citation: Kılıç, E. ve Keçeliğil, H. T. (2026). Blockchain tabanlı bilimsel veri yönetimi: açık bilim ile veri güvenliği arasındaki etik denge. *Journal of Humanities and Tourism Research*, 16 (3), 400-418.

Submitted: 04.10.2025

Accepted: 25.07.2026

Özet

Bilimsel araştırmaların hızla dijitalleşmesi, veri üretimi, paylaşımı ve arşivleme süreçlerinde güvenlik, şeffaflık ve doğruluk ilkelerini önceleyen yeni bir yönetimi zorunlu kılmaktadır. Bu çalışma, blockchain teknolojisinin bilimsel veri yönetimine entegrasyonunu kavramsal çerçeve ve etik boyutlarıyla incelemektedir. Odak noktaları; veri sahipliği ve rıza yönetimi, onay/konsensüs mekanizmaları, kayıt zinciri güvenliği, denetim izleri (auditability) ve akademik gözetim süreçleridir. Çalışma ayrıca, açık/kamuya açık ve izinli/kapalı ağ yapılarını, büyük verinin zincire doğrudan yazımı yerine hash tabanlı referans mimarilerini, ölçeksellik ve birlikte çalışabilirlik sınırlamalarını, enerji tüketimi ve sürdürülebilirlik (proof-of-work) sorunlarını ve KVKK/GDPR uyumu bağlamında mahremiyetin korunmasını tartışmaktadır. Bulgular, blockchain'in veri manipülasyonunu azaltma, etik ihlalleri görünür kılma ve güvenilirlik ile izlenebilirliği artırma potansiyeline sahip olduğunu; ancak teknik, hukuki ve kurumsal uyum koşullarının belirleyici olduğunu göstermektedir. Sonuç olarak, standartlaşmış mimariler, etik yönergeler ve çok paydaşlı yönetimle desteklenen blockchain tabanlı sistemlerin, uzun vadede akademik güven ortamını güçlendirmesi ve bilimsel üretkenliği artırması beklenmektedir.

Anahtar Kelimeler: Blockchain Bilimsel Veri Araştırma Etiği, Siber Güvenlik, Dijitalizasyon ve Etik, Veri Güvenliği, Veri Yönetimi, Açık Bilim

Abstract

The rapid digitalization of scientific research demands a new governance model that prioritizes security, transparency, and accuracy across data production, sharing, and archiving. This study examines the integration of blockchain into scientific data management through a conceptual and ethical lens, focusing on data ownership and consent, consensus mechanisms, ledger security, audit trails, and academic oversight. It discusses open/public versus permissioned networks, the use of hash-based references instead of writing large datasets on-chain, scalability and interoperability constraints, energy consumption and sustainability (proof-of-work), and privacy protection within GDPR/KVKK compliance. Findings indicate that blockchain can reduce data manipulation, surface ethical breaches, and strengthen reliability and traceability, while technical, legal, and institutional alignment remain decisive. In conclusion, standardized architectures, ethical guidelines, and multi-stakeholder governance are expected to enable blockchain-based systems to reinforce academic trust and boost scientific productivity in the long term.

Keywords: Blockchain Scientific Data Research Ethics, Cybersecurity, Digitalization And Ethics, Data Security, Data Management, Open Science

1. GİRİŞ

Blok zincir teknolojisi; saydamlığı, güvenilirliği ve dayanıklılığı ile günümüz bilgi ve teknoloji alanında öne çıkan bir yapı haline gelmiştir. Türkiye açısından blok zincir teknolojisi, tarihi bir fırsat alanı sunmaktadır. Ülkemizde bu alana yönelik ilgi kademeli olarak gelişmiş, 2018 yılında Blockchain Türkiye Platformu (Blockchain, 2018) kurulmuştur. Kısa sürede elde edilen başarı ve küresel bir örnek halini alan yönetim modeli, bu süreçte önemli bir rol üstlenmiştir.

Literatürde, blok zincir teknolojinin finansal ve teknik yönleri detaylı bir şekilde araştırılmıştır, ancak bilimsel veri yönetimi ile etik yönetim arasındaki bağlantıyı kapsamlı olarak inceleyen çalışmalar oldukça kısıtlıdır. Bu araştırmanın ana sorunu, dijitalleşen bilimsel veri süreçlerinde güvenliğin, şeffaflığın ve etik denetimin nasıl sağlanabileceğidir. Bu çalışma, literatür taramasına dayalı bir kavramsal analiz olarak değerlendirilmiştir.

İlk olarak bilgi güvenliği için tasarlanan blok zincir, günümüzde farklı alanlarda kullanılmaktadır. Merkezi otoriteye gerek kalmaksızın para, mülk veya sözleşme verilerinin güvenli biçimde aktarımını mümkün kılmakta; gücün tek elde toplanmasını ve manipülasyon risklerini engellemektedir. Dağıtık sistemler fikri, internet altyapısının gelişmesiyle birlikte daha da uygulanabilir hale gelmiştir (Werbach, 2018).

İlk pratik blok zincir teknolojisini keşfeden Nakamoto'ya göre blok zinciri, yapılan işlemlerin ağdaki kullanıcılar tarafından kaydedilip paylaşıldığı dağıtık bir veri yapısıdır (Nakamoto, 2018). Pilkington ise blok zinciri "devrim niteliğinde ve temel bir teknoloji" olarak tanımlamakta; küresel ödemelerden kurumsal yönetime, demokratik katılımdan sermaye piyasalarının uzlaşmasına kadar geniş bir alanda işlev gördüğünü vurgulamaktadır. Kriptografi yöntemleriyle güvence altına alınan bu yapı, coğrafi ve politik sınırların ötesinde organik bir sistem olarak öne çıkmaktadır (Pilkington, 2016).

Nakamoto, blok zinciri teknolojinin yalnızca elektronik para dışında da kullanılabileceğine ilişkin çevrimiçi tartışmalar yürütmüştür. Elmas, hisse senedi, telif hakkı ya da konser bileti gibi değerli varlıklar da bu sistem üzerinden takas edilebilmektedir. Günümüzde verilerin de önemli bir değer haline gelmesiyle birlikte, dağıtık defterler güçlü veri süreçlerini merkezi yapılara bağlı olmaksızın yönetme olanağı sunmaktadır (Werbach, 2021).

Blok zincir teknolojisi; finans (Hyvarinen, 2017), yönetim (Alketbi vd., 2018) ve eğitim (Mahankali ve Chaudhary, 2020) sektörlerinde uygulanmaya başlanmıştır. Bu çalışmada ise blok zincir tabanlı bilimsel veri yönetimi ve etik standartlarla ilişkisi ele alınmaktadır. Blockchain teknolojinin giderek artan kullanımı, güvenlik konusunu finans, kamu yönetimi, eğitim ve veri yönetimi gibi her alan için kritik bir mesele haline getirmiştir. Blok zincir teknolojinin veri yönetimi ve etik standartlarla ilişkisi incelenmelidir (Cormen vd., 2009).

2. KAVRAMSAL ÇERÇEVE

2.1. Blok Zincir Nedir?

Blok zincir, dağıtık (decentralized), değiştirilemez (immutable) ve kriptografik olarak güvence altına alınmış bir veri kayıt sistemidir. Her veri bir blok halinde zaman damgasıyla zincire eklenmektedir. Bu yapı sayesinde veri bütünlüğü korunmaktadır, merkezi bir otoriteye ihtiyaç duyulmamaktadır ve bürokrasi azalmaktadır. Tüm işlemler şeffaftır, geriye dönük izlenebilir ve manipülasyona kapalıdır. Blok zincir güvenilirliği artırmak ve veri manipülasyonunu önlemek amacıyla merkezi olmayan bir sistemde kriptografik olarak bağlanmış ve değiştirilemez veri bloklarının oluşturduğu bir kayıt teknolojisidir (Werbach, 2021).

Blok zincir, verilerin sıralı şekilde bloklar halinde bir zincire eklenmesi esasına dayanmaktadır. Her bilgi bir blok olarak eklenmekte ve her blok kendinden önceki bloğa

bağlanmaktadır. Oluşturulan zincirde eklenen veriler sonradan değiştirilememekte ve silinememektedir. Bilgilere herkes erişebilmekte; ancak hiç kimse tek başına müdahalede bulunamamaktadır. Bu durum, özellikle bilimsel araştırmalar açısından merkeziyetsizliği ve doğrulayıcı paydaşların artması sebebiyle veriye olan güveni artırmaktadır. Blok zinciri, yapısı itibarıyla sayfaları güçlü bir yapıştırıcıyla birbirine eklenmiş dijital bir deftere benzetilebilmektedir. Herkes bu defteri görebilmekte fakat hiç kimse tek başına bir sayfayı silememekte ya da değiştirememektedir. Sayfaların üzerindeki bilgiler, 0–9 ve a–f karakterlerinden oluşan 64 haneli dijital bir şifreye dönüştürülmektedir. Her sayfanın eklenişi zaman damgası ile kaydedilmektedir. Bir bilgisayar korsanı, dijital şifreyle blok zincir üzerinde yazılmış metne erişse bile yalnızca hash fonksiyonlarının ürettiği şifreli verileri görebilmektedir. Hash fonksiyonlarının (Beyaznet, 2026; Whitebit, 2024)) geri döndürülemez yapısı nedeniyle, bu verilerden orijinal şifreye ulaşmak mümkün olmamaktadır. Dolayısıyla hash fonksiyonu, tıpkı parmak izi gibi benzersiz bir güvenlik sağlamaktadır. Girdi üzerinde en küçük bir değişiklik dahi yeni bir hash kodu üretmekte, bu da verinin bütünlüğünü kanıtlamaktadır. Blok zincir, herkesin görebildiği fakat kimsenin tek başına değiştiremeyeceği bir defter olarak düşünülmektedir. Kimin ne zaman ne eklediği kaydedilmekte ve bu sayede güvenlik ile şeffaflığın kritik olduğu bilimsel veri alanlarında işlevsellik kazanmaktadır. (Oracle, 2026; Vikipedi, 2026; Blokzincir Laboratuvarı, 2026)

Blockchain teknolojisi, bilgilerin depolanmasına ve aktarılmasına imkân tanıyan bir sistem olarak bilinmektedir. Blockchain’de kaydedilen bilgiler değiştirilememekte; bu değiştirilemezlik, düzenlenmek istenen alanlara erişim olanağını sınırlandırmaktadır. Bilgiler kopyalanamamakta; herkes tarafından görüntülenmekte, ancak hiç kimse tek başına kontrol edememektedir. Kimse tek başına kontrol edemediği için özgün bir biçimde çalışmayı zorlaştırmaktadır (Taşdan, 2024).

Blok zincir teknolojisinde veriler kronolojik sırayla kaydedilmekte ve tek bir merkezde tutulmamaktadır. Kayıtlar, milyonlarca kişisel bilgisayardan oluşan ağlarda şeffaf biçimde muhafaza edilmektedir. Bu nedenle hiçbir kişi ya da kurum kayıt defterine tek başına sahip olamaz; bu durum da blok zinciri oldukça güvenli bir sistem haline getirmektedir. Bir blokta yapılacak en ufak değişiklik, ilgili hash kodunu ve dolayısıyla kendisinden sonra gelen blokların bütünlüğünü bozmaktadır. Bu nedenle değişiklikler kolayca fark edilmekte ve sahte bilgi ya da belge üretilmesine imkân verilmemektedir. Ayrıca zincire bir blok eklenebilmesi için ağdaki kullanıcıların onayı gereklidir. Bu yapı, bilimsel verilerin doğrulanabilir ve şeffaf bir biçimde arşivlenmesini sağlamaktadır. Blok zincir, güvene dayalı geleneksel sistemlerin yerini, matematiksel olarak tanımlanmış ve mekanik biçimde uygulanabilen kurallarla almaktadır. Üçüncü taraf doğrulayıcıların ortadan kalkması, gücün merkezi otoriteden alınarak ağın geneline aktarılmasını sağlamaktadır. Blok zincir teknolojisi açık kaynaklıdır ve herkesin erişimine açıktır. Bu yapı, sansür ve müdahalelere karşı güçlü bir koruma sunmaktadır. Hiçbir hükümet ya da otorite tek başına kontrol sağlayamamaktadır (Werbach, 2021).

Ağ katılımcılarının bir alt kümesi olan madenciler, matematiksel problemleri çözerek zincire yeni blokların eklenmesini sağlamaktadır. Yeni bloklar karşılığında ödül olarak üretilen paralar, madencilerin adreslerine gönderilmektedir. Sistemdeki madencilik gücü arttıkça çözülmesi gereken problemler de zorlaşır ve ortalama blok oluşturma süresi yaklaşık on dakika olarak korunmaktadır. İlk dönemlerde ev bilgisayarlarıyla yapılan madencilik, zamanla artan zorluk derecesi sebebiyle özel donanımlar gerektirmeye başlamıştır. Bu süreç, kriptografik hash işlevinin geri döndürülemez niteliğini ve çarpışma direncini ortaya koymaktadır.

2.2. Blockchain Teknolojisinde Veri Yönetimi

Günümüzde bireysel madencilik, yüksek teknik bilgi ve güçlü donanım gerektirdiği için azalmış; kullanıcılar daha çok çevrimiçi ve çevrimdışı cüzdan hizmetlerini tercih etmeye başlamıştır. Veri yapıları, karmaşık ilişkileri düzenlemek ve hızlı erişim sağlamak için kritik öneme sahiptir.

Bilgisayar biliminde temel bileşenlerden biri olan veri yapıları, yazılım geliştirme süreçlerinde sistemlerin etkinliğini, esnekliğini ve verimliliğini artırmada belirleyici rol oynamaktadır. Blok zincirde, iki düğümün aynı anda farklı zincirler önermesi durumunda, en uzun zincir sistem tarafından kabul edilmektedir. Ancak ağdaki bilgisayar gücünün çoğunluğunu elinde bulunduran bir saldırganın sahte blok oluşturmasıyla “%51 saldırısı” meydana gelebilmektedir. Buna rağmen düğümler blok zincirini sürekli doğruladığı için, yeni blok eklendikçe önceki blokları değiştirmek giderek daha zor hale gelmektedir (Werbach, 2021).

Veri yapılarının etkin kullanımı, yazılımların karmaşık verilerle başa çıkabilme kapasitesini artırmaktadır. Soyut veri yapıları hem teorik hem de uygulamalı alanlarda önemlidir; verilerin organizasyonu, depolanması ve işlenmesini belirlemektedir. Bu nedenle veri yapılarının anlaşılması, verimli algoritmalar geliştirilmesi açısından elzemdir. Büyük veri analizi gibi çağdaş alanlar, etkili veri yapılarını zorunlu kılmaktadır (Temür, 2023). Diziler ve bağlı listeler, veri setlerini düzenli depolayarak hızlı erişim olanağı sağlamaktadır (Cormen, vd., 2009).

Blockchain teknolojisi, temel araştırmalarda da büyük bir potansiyel taşımaktadır. Matematiksel modelleme, simülasyon ve algoritma geliştirme gibi alanlarda bilimsel çalışmalara katkı sunabilmekte; hipotez geliştirme süreçlerine ivme kazandırmakta ve deneysel sonuçların doğruluğunu artırmaktadır. Ancak bu teknolojinin temel bilimlerde uygulanması, klasik yöntemlere kıyasla daha karmaşık süreçler gerektirmektedir. Blok zincir teknolojisinin bilimsel bütünlüğü koruma potansiyeli bulunsa da küresel eşitsizliklerin giderilmesine yönelik politikaların eksikliğinin (Cooper, 2023) etik ve etkin biçimde kullanılabilmesi için küresel iş birliğine ve eşit fırsatlar sağlayacak politikalara ihtiyaç vardır (Perkins, 2003).

Merkle ağacı (Vikipedi, 2024; Coino, 2025), verileri bir zincir üzerine güvenli ve verimli bir şekilde kaydetmek için kullanılan veri parçalama, kaydetme ve dağıtma potansiyeline sahip yapı modelidir. Sistem, orijinal işlemlere dayanarak o verilerin gerçekliğini doğrulama aracı olarak karma oluşturmak için bir algoritma ile işlem bloklarını çalıştırır. Sonunda tüm bu bloklar için bir karma oluşturulur. Oluşan bu yapıya Merkle ağacı denir (Kınacı, 2019, s. 12). Merkle ağacı, verilerin güvenli biçimde toplanmasını ve büyük veri setlerinin tek merkezde organize edilmesini sağlamaktadır. Bu yapı hem verimliliği artırmakta hem de veri güvenliğini güçlendirmektedir.

Blok zincir, maliyet ve siyasi nedenlerle mülkiyet kayıtlarının denetimini kolaylaştırabilmektedir. Mülkiyet konusunda hisse senedi sahipliğinde şeffaflık ve güvenilirliği artırdığı da gözlemlenmiştir. Teknik açıdan bir örüntüye sahip olsa da blok zincir, aynı zamanda sosyoteknik (insan [sosyal] ve teknoloji [teknik]) unsurlarının bir arada, birbirini etkileyerek işlediği karmaşık sistemler) bir altyapıya sahiptir. İş kanıtı, yatırım kararı, sistemin geliştirilmesi ve iyileştirilmesi gibi temel adımlar, teknolojiye yön veren insan faktörüne bağlıdır.

Kullanıcı ve işlem sayısı arttıkça blok zincirin boyutu da büyümekte, bu durum ölçeklenebilirlik sorununa ve performans düşüşüne yol açmaktadır (Swan, 2015). Blok zincir kullanımında uzun işlem süreleri ve farklı sistemler arasında birlikte çalışabilirlik ihtiyacı gibi zorluklar söz konusudur (Sharples ve Domingue, 2016). Ayrıca altyapı ve yönetim maliyetleri oldukça yüksektir; blok zincir uygulamaları ciddi finansal kaynak gerektirebilmektedir (Bore vd., 2017).

2.2.1. Etik Sorunlar

Kuçuradi, etik bilginin insan davranışını otomatik olarak belirlemediğini açıkça söyler: “Etik bilgi, insanın davranışını kendiliğinden belirlemez; davranışın belirlenmesi, kişinin durum bilgisine ve değer bilgisine bağlıdır.” (Kuçuradi, 1999, s. 23–24). Kuçuradi, “iyi”yi bilmenin “iyi”yi yapmayı garanti etmediğini ise şöyle açıklar: “İnsanın neyin iyi olduğunu bilmesi, onu iyi olanı yapmaya zorunlu olarak götürmez.” (Kuçuradi, 2003, s. 57).

Hızla değişen dünya, kişilerin ahlaki normlara bağlılığını da gevşetmiştir. Verilerin kolay ve hızlı bir şekilde değiştirilerek sonuca ulaşılması, ne yazık ki günümüz akademisinde kaçınılmaz hale gelmiştir. Bu çalışma kapsamında değerlendirilmektedir ki bilimde ahlaka aykırı davranışların önlenmesi; etkili bir eğitimle, verilerin gerektiğinde temin edilebilmesi için en az beş yıl boyunca saklanmasıyla ve genç bilim insanlarının basitten karmaşığa doğru ilerleyen çalışmalar yapmalarıyla mümkün olmaktadır. Ayrıca bilimsel özgürlük, araştırmacılar üzerindeki mali ve idari baskıların kaldırılmasıyla sağlanabilmektedir. Ancak, bu ütopya gibi görünen kriterler karşılanırsa bile, birey nihayetinde kendi menfaati ile vicdanı arasında bir tercih yapmak durumunda kalmaktadır. İşin özü şudur: Bilimde etik dışı davranışları tamamen ortadan kaldırmak için yapısal önlemler alınabilir; ancak nihai belirleyici yine bireyin vicdanıdır.

Başlangıçta bilgi güvenliği sistemleri için tasarlanan bu teknoloji, günümüzde kullanım alanlarını genişletmiştir. Dijitalleşmenin hız kazanmasıyla artan bu geniş veri hacmi ve veri balonuna erişimdeki kolaylık, kullanıcıları veri güvenliği tehlikesiyle karşı karşıya getirmektedir. Bu durum, bilimsel araştırmaların güvenilirliği, saydamlığı ve izlenebilirliğini önemli hale getirmektedir. Özellikle veri seçme, ekleme ve çıkarma yoluyla bilgilerin değiştirilmesi; verinin aslına benzetilerek yapılan düzmece işlemler ve etik dışı yöntemler, bilimsel ortamda güven sorununa yol açmaktadır. (Karagöz, 2019) Bu noktada merkeziyetsiz ve değiştirilemez izlenebilir kayıt sistemiyle blok zincir teknolojisi, bilimsel veri yönetiminde dikkatleri üzerine çekmektedir.

Veri gizliliği, erişim yetkilendirme zafiyetleri, kimlik doğrulama sorunları ve siber saldırılar bilişim teknolojilerinde karşılaşılan temel sorunlar arasında yer almaktadır (Subashini ve Kavitha, 2011). Siber saldırılar, hizmete erişimde aksamaların yanı sıra ekonomik kayıplara ve veri güvenliği açıklarına da yol açmaktadır (Sote Haber, 2022; Yaşar Üniversitesi-Haber, 2020). Bu nedenle güvenlik politikalarının geliştirilmesi ve yenilikçi çözümlerin uygulanması zorunlu olmaktadır. Yapılan çalışmalarda “Zero Trust Architecture” (Sıfır Güven Mimarisi) gibi güncel yaklaşımlar, veri güvenliğini daha kapsamlı bir şekilde ele almaktadır (Kindervag, 2010). Sıfır güven mimarisi yaklaşımı, doğrulanana kadar hiçbir bağlantının, kullanıcının veya varlığın güvenilir olmadığını varsayar. Buna karşılık, geleneksel çevre güvenlik paradigması, kimlikleri doğrulandıktan sonra bağlantılara güvenir ve tüm ağa erişim izni vererek kurumsal varlıkları potansiyel olarak siber suçlulara açık hale getirir. Dönüştürücü ve yoğun zaman alan sıfır güven projeleri, mevcut mimariyi temel alır ve yeniden işler (Trendmicro, 2026). Geleneksel güvenlik modelleri bir kuruluşun ağındaki her şeyin güvenilir olduğunu varsayarken, Zero Trust güvenlik mimarisi ister kurumsal ağ içinde ister dışında olsun, kaynaklara erişmeden önce her kullanıcının ve cihazın kimliğini doğrular. (Microsoft, 2026).

Blok zincir teknolojisi, geleneksel sistemlere kıyasla gelişmiş güvenlik önlemleri sunmasına rağmen siber saldırılara karşı tamamen bağışık değildir. Zincirde depolanan hassas bilgiler, yetkisiz erişimlere karşı hâlâ yeterince korunamamaktadır (Pilkington, 2016). Ayrıca teknolojinin henüz başlangıç aşamasında olması, kullanımının karmaşık algılanmasına ve kullanıcı güveninin tam anlamıyla oluşmamasına yol açmaktadır (Xu vd., 2019).

Blok zincir teknolojisinde veriler, hash kodları ile şifrelenerek kullanıcı gizliliği korunmaktadır. Gizlilik amacıyla her kullanıcının kimliği, bir kimlik numarası aracılığıyla güvence altına alınmaktadır. Blok zincirinde saklanan kayıtlar; savaşlar, doğal afetler ya da başka sebeplerle eğitim sisteminin kesintiye uğramasından bağımsız olarak kalıcı biçimde güvence altına alınabilmekte ve doğrulanabilmektedir (Loukil vd., 2021). Ağda kaydedilen öğrenme deneyimlerine ilişkin tüm bilgilere yalnızca özel anahtarlarına sahip kullanıcılar erişebilmektedir. Güvenlik ve şeffaflığın artması oranında maliyetler azalmaktadır; kötü niyetli kişiler ise tam özel anahtara sahip olmadan verilere erişememektedir. Böylece idari maliyetler ve bürokrasi azaltılarak öğrencilerin kayıtları ömür boyu sistemde tutulabilmektedir (Jirgensons ve Kapenieks, 2018).

Blok zincir teknolojisi, dijital sözleşmeler ve kâğıtsız işlemler aracılığıyla hizmet maliyetlerini önemli ölçüde düşürmekte; bilgi işleme için harcanan enerji ve zaman maliyetlerini azaltarak yeni bir dönemin kapısını aralamaktadır (Taşdan, 2024).

Literatür ışığında söylenebilir ki geleneksel araştırma yönetim sistemlerinde, benzer nitelikteki bilimsel çalışmaların eşzamanlı olarak yürütülüp yürütülmediğinin ya da araştırma süreçlerinde etik ihlallerin meydana gelip gelmediğinin nesnel biçimde saptanması çoğu durumda sınırlı kalmaktadır. Blok zincir teknolojisi, dağıtık ve değiştirilemez kayıt yapısı sayesinde bu sorunlara yönelik önemli bir çözüm potansiyeli sunmaktadır. Özellikle akıllı sözleşmeler aracılığıyla araştırma önerilerinin içerik ve süreç bilgilerinin güvenli biçimde kaydedilmesi, araştırma faaliyetlerinin doğrulanabilirliğinin artırılması ve üniversitelerde uygulanan araştırma teşvik mekanizmalarının daha şeffaf ve izlenebilir hâle getirilmesi mümkün olmaktadır. Blok zincir mimarisinde kullanılan açık anahtarlar, kriptografik yöntemlerle üretilen ve gerçek kişi kimlikleriyle doğrudan ilişkilendirilemeyen adreslerdir. İşlemler sistem üzerinde izlenebilir nitelikte olsa da kimlik bilgilerinin açıklanmasını gerektirmemesi nedeniyle veri sahiplerinin mahremiyeti korunmakta ve gizlilik ilkesi güvence altına alınmaktadır.

Blok zincir tabanlı sistemler, verilerin bütünlüğünü koruyarak araştırma süreçlerinde şeffaflığı sağlamakta; aynı zamanda etik standartların dijital ortamda izlenebilirliğini mümkün kılmaktadır. Konsensüs olmadan verilerde değişiklik yapmak imkânsız olmaktadır (Rodeck ve Curry, 2021). Bir başka avantaj olarak blok zincir, yolsuzluk ve bürokrasinin önüne geçerek girişimciliği özendirmektedir. Bu teknolojinin geleceği ümit verici görülmektedir (Mattila, 2016). Ayrıca veri işlemenin çoklu ortaklık organizasyonları için bir gereklilik haline geldiği ve yeni içgörülerin keşfine imkân sunduğu söylenebilmektedir.

Blok zincirde etik boyutlar özellikle önem taşımaktadır. Hassas veriler doğrudan blok zincir defterinde saklanmamalıdır; yalnızca kurcalamaya dayanıklı şekilde dağıtımına uygun veriler deftere eklenmelidir. Kullanıcı kimliği korunurken, yetkili kurumların yasadışı faaliyetleri araştırmasına da imkân tanıyacak şekilde tasarım yapılmalıdır. Yönetim gücü dağıtılmalı, karar yetkisi tek bir merkezde yoğunlaşmamalıdır. Oylama düğümlerini çalıştıran donanımlar kurcalamaya karşı güçlendirilmelidir. Kod kalitesi, sisteme dağıtılmadan önce titizlikle değerlendirilmelidir ve farklı blok zincir sistemleri arasında izlenebilirlik sağlanmalıdır. Blockchain sistemleri sürdürülebilir biçimde çalışmalı ve bu teknolojilerin toplumsal değerler üzerindeki etkileri sürekli olarak incelenmelidir.

Geriye dönük izlenebilirlik (auditability) sayesinde, hangi verinin ne zaman ve kim tarafından eklendiği ile hangi aşamalardan geçtiği zincir üzerinde kayıtlıdır. Blok zincir ağları kamuya açık (izin gerektirmeyen; public/permissionless) ve kapalı(özel/izinli) olmak üzere ikiye ayrılmaktadır. Bir blok zincir ağına katılım için başvuru yapılması gerekiyorsa veya açık/kamuya özel anahtarların belirli kişi ya da kuruluşlarca atanması söz konusuysa, bu otoriteler uygun buldukları kişilere yetki tahsis edebilirler (Martini & Weinzierl, 2017). Bu bağlamda bireyler, internet ortamında kendi özerk dijital alan oluşturma ve işlem yapma fırsatına sahip olmaktadır. Temel kullanım alanları arasında tedarik zinciri yönetimi, tapu ve nüfus kayıtları, hukuk sektöründe delil saklama, finansal takaslar ve dijital hak yönetimi (DRM) yer alır. Aynı şekilde, verilerin erişimine imkân sağlayan kamuya açık blok zincir uygulamaları da mevcuttur. (Bitcoin (BTC), Ethereum (ETH), Solana (SOL) ve BNB Smart Chain)

Blok zincir teknolojisi halen büyük ölçüde düzenlemelerden yoksundur ve eğitimde kullanımına ilişkin net yönergeler ile standartlar bulunmamaktadır. Akademik alanda uygulanabilmesi için gerekli altyapının oluşturulması ve mevzuatın düzenlenmesi gerekmektedir. Bu kapsamda personel eğitimi sağlanmalı veya dış merkezlerden uzman desteği alınmalıdır. Teknolojinin nasıl kullanılacağı, verilere kimlerin erişeceği ve verilerin nasıl yönetileceği

konularında kesinlik yoktur. Dolayısıyla akademide blok zincir uygulamalarının benimsenmesi; eğitim kurumları, öğrenciler, araştırmacılar ve devlet otoriteleri dahil olmak üzere farklı paydaşların iş birliğini zorunlu kılmaktadır (Taşdan, 2024).

EU Expert Group on Blockchain Ethics (EGBE, Blockchain Etiği Uzman Grubu), genel alanlarda yönergeler geliştirmiştir (EU Expert Group on Blockchain Ethics, 2026; Agerskov, 2024). Bu yapı, paydaşların sürece dahil edilmesine ve ayrımcılığın önlenmesine olanak tanımaktadır. Bununla birlikte, tasarımcıların sistemdeki güç dinamiklerinin nasıl evrimleşebileceğini ve istenmeyen sonuçların nasıl azaltılabileceğini sürekli değerlendirmeleri gerekmektedir. Ancak The European Blockchain Services Infrastructure (EBSI, Blok Zincir Hizmetleri Altyapısı)'na göre sistem özerk çalıştığından, uygulama sürecinde etik yönergelere, normlara ve değerlere ihtiyaç duyulmaktadır (The European Blockchain Services Infrastructure, 2026; Blockchain Türkiye, 2026, Aktaş & Tan & Arap, 2024).

Dijital ortamda var olan belgelerin kolayca müdahaleye açık olması, elektronik belgelerde mahremiyet ve güven sorunlarını gündeme getirmektedir (Haber ve Stornetta, 1991).

Bunun yanı sıra blok zincirin iş kanıtı (proof-of-work) yöntemi başka bir sorun teşkil etmektedir. Bu mekanizma yoğun işlem gücü gerektirdiğinden oldukça maliyetli hale gelmekte ve ciddi enerji israfına yol açmaktadır. Enerji tüketimi sorunu dijitalleşmenin etik boyutuyla doğrudan ilgilidir. Blok zincir değer kazandıkça madenciler, blok ödülleri elde edebilmek için daha fazla enerji harcamaya yönelmektedir. Artan enerji ihtiyacı, karbon salınımını yükseltmekte ve özellikle iklim değişikliğiyle mücadele edilen günümüzde ciddi bir sorun yaratmaktadır (Werbach, 2021; Aslan & Kasapbaşı, 2022; Küre Ansiklopedi, 2026; Ledger Academy, 2026).

2.3. Dijitalleşme ve Etik

Dijital teknolojilerin hızlı ilerlemesi, kişisel ve toplumsal hayatın birçok alanında kolaylıklar sağlamakla birlikte, aynı zamanda çeşitli etik sorunları da gündeme getirmektedir. Mahremiyetin ihlal edilmesi, yapay zekâ sistemlerinin şeffaflığını kaybetmesi, dijital dışlanma ve algoritmik ayrımcılık gibi sorunlar, dijitalleşmenin etik açıdan olumsuz bir yöne evrilmesine neden olmaktadır. Bu durum, dijitalleşmedeki gerileyici eğilimler olarak adlandırılmakta ve teknolojik yeniliklerin temel etik değerlerle çelişkili biçimde geliştiğini ortaya koymaktadır. Özellikle sağlık, kamu hizmetleri ve finans gibi alanlarda yapay zekâ tabanlı sistemlerin hızla yayılması; bireylerin kişisel verilerinin düzensiz biçimde işlenmesi ve algoritmik kararların toplumsal eşitsizlikleri artırması, etik riskleri daha görünür hale getirmiştir. Bu etik gerilemelere karşı güçlü, sürdürülebilir ve kapsamlı bir etik yapı inşa edilmelidir (Babaoğlu, 2025; Özcan, 2021; Aslan, 2022).

Etik yapının oluşturulması yalnızca teknolojinin güvenli ve yasal olmasına indirgenemez; bunun aynı zamanda adil, şeffaf ve insana odaklı bir tasarımı da içermesi gerekmektedir. Bu hedefe ulaşmak için öncelikle insan haklarına dayalı etik ilkelerin açık bir biçimde tanımlanması gerekmektedir. Mahremiyet, eşitlik, hesap verebilirlik, ayrımcılık yapmama ve özerklik gibi ilkeler her dijital uygulamanın temelini oluşturmalıdır. Bu ilkeleri takip eden aşama, yeni teknolojilerin uygulanmadan önce etik etki analizine tabi tutulmasını gerektirmektedir. Böylelikle, teknolojinin kimleri nasıl etkileyebileceği ve olası zararları önceden öngörülebilir. Ayrıca, dijital sistemlerin geliştirilmesi ve uygulanması süreçlerinde kurumsal etik komiteleri oluşturulmalı ve bu komiteler aracılığıyla etik denetim sürekliliği sağlanmalıdır. Bu komiteler, muhtemel ihlalleri tespit edip belgelemeli ve teknolojinin insan onuruna uygun biçimde kullanılıp kullanılmadığını denetlemelidir. Dijitalleşme süreci yalnızca teknik bir dönüşüm değil, aynı zamanda etik bir sınavdır. Ahlaki değerlerden uzaklaşmaların ve geriye gidişlerin önlenmesi yalnızca hukuk aracılığıyla değil; güçlü bir etik anlayışla mümkündür. Bu bağlamda dijital sistemlerin insan haklarına duyarlı, toplumsal adaleti gözeten ve şeffaf yapılarla desteklenmesi büyük önem

taşımaktadır. Etik altyapı, dijitalleşmenin yönünü belirleyen bir pusula işlevi görmeli; teknolojik gelişmelerin yalnızca neyin mümkün olduğunu değil, aynı zamanda neyin doğru olduğunu da sorgulamasını sağlamalıdır (Babaoğlu, 2025).

Dijital teknolojilerin hızlı gelişimi, insan yaşamında dönüştürücü etkiler yaratırken beraberinde etik açıdan geri gidişleri de gündeme getirmektedir. Regresif eğilimler; insan hakları, şeffaflık, eşitlik ve hesap verebilirlik gibi temel değerlerde gerilemeyi işaret etmektedir. Bu durum, teknolojik yeniliklerin toplumsal ve hukuksal düzenlemelerden daha hızlı ilerlemesi ya da kasıtlı olarak etik çerçevenin zayıflatılması sonucunda ortaya çıkmaktadır. Örneğin sosyal medya platformlarının konum, sağlık bilgileri ve özel yazışmalara aşırı erişim sağlaması, bireysel bağımsızlığı zayıflatan regresif bir eğilimi yansıtmaktadır (Tufekci, 2015; Sarı, 2024).

Özellikle dijital platformların (Google, Yahoo, Facebook vb.) gözetim kapitalizmi (kullanıcıların çevrimiçi davranışlarını, kişisel verilerini ve tecrübelerini rıza dışı toplayıp işleyerek, geleceğe yönelik tahmin ürünleri üretmesi ve bunları pazarlaması temeline dayanan ekonomik sistemdir) bağlamında dijital teknolojiler, bireylerin mahremiyetini aşındırmakta ve demokratik mekanizmaları zayıflatmaktadır (Zuboff, 2019). Bu etik gerilemelerin somut örneklerinden biri sosyal medya platformlarının veri toplama pratikleridir. Morozov (2011) ise dijital araçların otoriter rejimler tarafından kontrol ve manipülasyon için kullanılabilceğini vurgulamaktadır. Bu bağlamda etik altyapının yalnızca bireysel hakları değil, aynı zamanda toplumsal adalet, algoritmik şeffaflık ve veri adaleti gibi normatif ilkeleri de kapsamı gerekmektedir (Mittelstadt vd., 2016).

Dolayısıyla araştırma bulguları şunu göstermektedir: Dijital teknolojilerin sağladığı ilerlemeler ancak güçlü bir etik çerçeve ile desteklendiğinde toplumsal faydaya dönüşebilir. Aksi halde teknoloji, insanlığın gelişimine katkı sunmak yerine demokratik değerlerde gerileme ve toplumsal eşitsizliklerin derinleşmesi riskini barındırmaktadır.

Dijital teknolojilerin gelişimi beraberinde bireysel haklar ve özgürlükler açısından önemli tehditler doğurmaktadır. Özellikle veri gizliliğinin ikinci plana atılması, kullanıcı verilerinin çoğu zaman açık rıza olmaksızın toplanması, analiz edilmesi ve ticari amaçlarla paylaşılması, bireyin mahremiyetine doğrudan zarar vermektedir. Büyük veri şirketleri yalnızca kişisel bilgileri saklamakla kalmamakta, aynı zamanda bu verileri kullanıcıların davranışlarını yönlendiren bir araç olarak kullanmaktadır (Babaoğlu, 2025; Turancı, 2021; Zuboff, 2019).

Kara kutu problemi olarak tanımlanan yapay zekâ sistemlerinde şeffaflık ve hesap verebilirlik eksikliği, algoritmaların karar verme süreçlerinin kullanıcıya açıklanamaması (Yılmaz, 2025; Duran, 2025; Burrell, 2016; Kayacı, 2025) elde edilen sonuçların sorgulanamamasına ve insan kontrolünden uzaklaşılmasına yol açmakta, böylece etik hesap verebilirlik zayıflamaktadır. Örneğin, bir bankanın yapay zekâ destekli kredi değerlendirme sisteminin yalnızca sosyoekonomik geçmişe dayanarak ayrımcı kararlar alması, fakat bunun gerekçesini açıklamaması, teknolojik regresyonun somut bir örneğidir (O'Neil, 2016). Dijital teknolojiler, doğru etik altyapılar ve şeffaf mekanizmalar geliştirilmediği takdirde, bireysel hakları ihlal eden ve toplumsal adalet açısından gerilemeye yol açan regresif uygulamalara dönüşebilmektedir.

Etik yapının bir diğer önemli unsuru eğitimidir. Yazılım geliştiriciler, kamu yöneticileri ve dijital hizmet sağlayıcıları için dijital etik farkındalığını artırıcı programlar düzenlenmeli ve etik okuryazarlık güçlendirilmelidir. Böylece etik karar alma süreçleri bireysel düzeyde de desteklenmiş olur. Bununla birlikte mevcut hukuki düzenlemeler ile etik ilkeler arasında uyum sağlanmalıdır. Örneğin Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK, Kanun Numarası: 6698, Kabul Tarihi: 24/3/2016, Yayımlandığı Resmî Gazete: Tarih: 7/4/2016, Sayı: 29677) veya Avrupa Birliği'nde yürürlükte olan Genel Veri Koruma Tüzüğü (GDPR) gibi yasalar ile kurumsal etik kuralları arasında entegrasyon kurulmalıdır. Bu bütünleşik yapı yalnızca riskleri azaltmakla kalmayacak, aynı

zamanda dijital teknolojilerin toplumsal kabulünü ve güvenilirliğini de artıracaktır (Mevzuat Bilgi Sistemi, 2026; T.C. Dışişleri Bakanlığı, Avrupa Birliği Başkanlığı, 2026).

2.3.1. Dijital Erişimde Adaletsizlik (Dijital Uçurum)

Dijital uçurum kavramı, temel olarak bilgi ve iletişim teknolojilerine erişimi olanlar ile bu imkândan mahrum kalanlar arasındaki farkı ifade etmektedir. Bu bağlamda bilgisayarlar ve internet başta olmak üzere, cep telefonları (özellikle akıllı telefonlar) ve çeşitli dijital donanım ya da yazılımlar da kapsam dâhilindedir. Dolayısıyla dijital uçurum, yalnızca teknik bir erişim sorunu değil, aynı zamanda toplumsal ve bilgi eşitsizliği tartışmalarının merkezinde yer alan bir olgudur (Norris, 2001; van Dijk, 2020).

Toplumsal yaşamda kapsayıcılık ve dışlayıcılık kavramları, dijital uçurumun en görünür etkilerindendir. Özellikle kırsal bölgelerde yaşayan, düşük gelirli ya da yaşlı bireyler teknolojiye erişimden dışlanmakta; bu da dijital hizmetlerin yalnızca belli bir kesime fayda sağlamasına neden olmaktadır. Örneğin yalnızca çevrimiçi randevu sistemi üzerinden hizmet veren bir hastane, internet okuryazarlığı düşük veya hiç olmayan yaşlı bireyleri fiilen sağlık hizmetlerinden mahrum bırakabilmektedir. Bu durum, dijitalleşmenin toplumsal adalet ve eşitlik açısından regresif bir eğilim taşıdığını açıkça göstermektedir (Hargittai, 2002). Bu sebeple dijital teknolojilerin geliştirilmesi ve uygulanmasında yalnızca teknik altyapıya değil, aynı zamanda erişilebilirlik, eşitlik ve kapsayıcılık ilkelerine de önem verilmelidir. Aksi halde dijitalleşme, toplumsal faydayı artırmak yerine yeni ayrımcılık biçimlerini derinleştirebilmektedir.

2.4. Manipülatif Tasarımlar ve Algoritmalar

Dijital içeriklerin büyük bir kısmının, asıl haliyle sunulmak yerine, belirli amaçlar doğrultusunda değiştirilmiş veya dönüştürülmüş olmasına dijital manipülasyon denir. Dijital platformlar, kullanıcıların dikkatini daha uzun süre ekranda tutmak amacıyla bağımlılık yaratacı içerikler ve yönlendirici tasarımlar geliştirmektedir. Bu durum, bireylerin bilinçli tercihlerini zayıflatarak özgür irade ilkesini gölgelemektedir. Literatürde “karanlık desenler” (dark patterns) olarak adlandırılan bu uygulamalar, kullanıcıları istemedikleri kararlar almaya zorlayan manipülatif arayüz tasarımlarıdır. Örneğin abonelik iptali menülerinin kasıtlı olarak gizlenmesi ya da varsayılan ayarların reklamları kabul edecek biçimde düzenlenmesi, sepeti izinsiz ürünle doldurma, yanıltıcı buton renkleri (Confirmshaming) ve gizlilik ayarlarını karmaşıktırmak bu tür pratiklere tipik örneklerdir (Ünar, 2024; Gray vd., 2018; Mathur vd., 2019, Korkmaz & Sönmez, 2025).

Manipülasyon yalnızca görsel tasarımlarla sınırlı kalmamakta, algoritmik öneri sistemleri de kullanıcı davranışlarını yönlendirmektedir. YouTube veya TikTok gibi platformlarda öneri algoritmaları, kişileri sürekli içerik tüketmeye teşvik ederken, zaman zaman yanlış bilgi veya kutuplaştırıcı içeriklere maruz bırakabilmektedir (Narayanan vd., 2020).

Bu gelişmeler uluslararası alanda etik ve hukuki tartışmaları gündeme getirmiştir. Avrupa Birliği’nin Dijital Hizmetler Yasası (2022) manipülatif arayüzleri sınırlandırmayı hedeflerken, ABD Federal Ticaret Komisyonu (FTC, 2022) dark patterns uygulamalarını tüketici haklarını ihlal eden yanıltıcı pratikler olarak değerlendirmektedir. Manipülatif tasarımlar ve algoritmalar, kullanıcı deneyimini bozmanın ötesinde, bireylerin seçim özgürlüğünü ve etik sorumluluk ilkesini zedelemektedir. Bu nedenle dijital teknolojilerin tasarımında şeffaflık, kullanıcı özerkliği ve etik sorumluluk ilkelerinin merkeze alınması gerekmektedir (Turancı, 2021; Babaoğlu, 2025).

3. YAPAY ZEKÂ VE OTOMASYON İLE İŞGÜCÜ ADALETSİZLİĞİ

Yapay zekâ ve otomasyon teknolojilerinin hızla gelişmesi, üretim ve hizmet süreçlerinde insan emeğinin yerini alma potansiyelini beraberinde getirmektedir. Bu durum, verimlilik artışı sağlarken aynı zamanda iş gücü piyasasında işsizliğe, beceri uyumsuzluğuna ve gelir eşitsizliklerinin

derinleşmesine yol açabilmektedir (Brynjolfsson ve McAfee, 2014). Özellikle düşük vasıflı işlerde çalışan bireyler, yeterli yeniden eğitim ve dönüşüm desteği sunulmadığında, dijital dönüşüm sürecinde dışlanma riskiyle karşı karşıya kalmaktadır. Bu eğilim, sosyal adalet ve kurumsal sorumluluk açısından regresif bir durum yaratmaktadır. Örneğin sağlık sektöründe dijital hasta karşılama ve otomatik yönlendirme sistemlerinin kullanılması, destek personelinin işini kaybetmesine neden olabilmektedir. Benzer şekilde finans, lojistik veya müşteri hizmetleri gibi alanlarda yapay zekâ destekli otomasyon, kısa vadede maliyet avantajı sağlarken uzun vadede toplumsal istihdam sorunlarını derinleştirebilmektedir (Frey ve Osborne, 2017). Dolayısıyla, yapay zekâ ve otomasyonun yaygınlaşması yalnızca teknolojik bir dönüşüm değil, aynı zamanda etik ve toplumsal sorumluluk meselesidir. Bu sürecin adil yönetilebilmesi için politika yapımcıların, işletmelerin ve eğitim kurumlarının iş gücüne yönelik yeniden beceri kazandırma (reskilling) ve destek mekanizmaları geliştirmesi büyük önem taşımaktadır (Susskind ve Susskind, 2015).

3.1. Siber Güvenlik

Dijital teknolojilerin hızlı gelişimi, yalnızca teknik güvenlik sorunlarını değil, aynı zamanda ulusal ve uluslararası hukuk bakımından ciddi sorumluluk ve risk alanlarını da gündeme getirmektedir. Gelişmiş yapay zekâ sistemleri, devlet destekli siber aktörler, büyük teknoloji şirketleri ve organize hacker grupları; bireylerin temel hak ve özgürlüklerini, kamu düzenini ve kritik altyapıların bütünlüğünü tehdit edebilecek nitelikte faaliyetlerde bulunabilmektedir. Tarihsel olarak yaşamı kolaylaştırma amacıyla geliştirilen teknolojiler, günümüzde hem özel hukuk kişileri hem de kamu otoriteleri açısından sürekli değişen ve karmaşılaşan siber güvenlik yükümlülüklerini beraberinde getirmiştir. Öyle ki bu tehditler, bir veri ihlalinin ardından daha güçlü şifreleme yöntemlerinin geliştirilmesini zorunlu kılan teknik ve hukuki uyum süreçlerinden, kritik altyapıların hedef alınması hâlinde ortaya çıkabilecek uluslararası sorumluluk tartışmalarına kadar geniş bir yelpazede ortaya çıkmaktadır. Su ve enerji dağıtım sistemlerinin manipüle edilmesi, ulaşım ağlarının devre dışı bırakılması veya askerî tesislerin kontrolünün ele geçirilmesi gibi senaryolar hem ulusal güvenlik hukukunun hem de uluslararası siber çatışma hukukunun kapsamına giren yüksek riskli durumlar olarak değerlendirilmektedir. Bu bağlamda devletlerin, şirketlerin ve diğer dijital aktörlerin; özen yükümlülüğü, veri güvenliği tedbirleri, risk yönetimi ve kritik altyapıların korunmasına ilişkin hukuki sorumluluklarını yerine getirmeleri zorunluluk hâline gelmiştir.

Siber güvenlik alanında insan faktörü ile ilgili öne çıkan tespit şudur: Hem teknik savunma kapasitesinin etkinliği hem de hukuki sorumlulukların yerine getirilmesi açısından insan faktörü belirleyici bir unsurdur. Kurumsal yapılarda çalışanların görev bilinciyle hareket etmesi, bir veri ihlali meydana geldiğinde hızlı ve koordineli iletişim kanallarının işletilmesi, olay müdahale süreçlerinin hukuka uygun biçimde yürütülmesi ve aktif savunma stratejilerinin geliştirilmesi, modern siber güvenlik yönetiminin temel bileşenleri arasında yer almaktadır. Bununla birlikte, "hack-back" olarak adlandırılan karşı saldırı yöntemlerinin etik ve hukuki meşruiyeti, ulusal hukuk düzenleri ve uluslararası siber normlar bakımından hâlen tartışmalı bir alan olmaya devam etmektedir. Bu nedenle kurumların, hem bireysel gizliliğin korunmasına ilişkin yükümlülüklerini hem de siber savunma faaliyetlerinde orantılılık, hukuka uygunluk ve hesap verebilirlik ilkelerini gözetmeleri gerekmektedir. Ancak kabul edilmelidir ki, bir organizasyonun teknik kapasitesi ne kadar gelişmiş olursa olsun; güvenlik yazılımlarına, personel eğitimine, risk yönetimi süreçlerine ve kurumsal farkındalık programlarına yapılan yatırımlar tam güvenliği garanti etmemektedir. Kritik altyapıların dijital sistemlere bağımlı olması ve çoğu zaman internet bağlantısı üzerinden çalışması, bu sistemlerin mutlak güvenlik düzeyine ulaştırılmasını fiilen imkânsız kılmaktadır. Bu durum hem kamu otoriteleri hem de özel sektör açısından sürekli güncellenen bir özen yükümlülüğünü, çok

katmanlı savunma mimarilerinin uygulanmasını ve siber tehditlere karşı dinamik bir hukuki–teknik uyum sürecinin sürdürülmesini zorunlu hâle getirmektedir.

Dijital teknolojiler, daha önce hiç görülmemiş bir güç sunarken kullanıcıları aynı zamanda daha riskli bir duruma sokmaktadır. Yüksek iletişim kapasiteleri iş birliği ve ağ kurma fırsatları sağlarken, bu özellikler davetsiz misafirler için de açık kapı oluşturmaktadır. Veri miktarının ve manipülasyon kapasitesinin artması işlemleri hızlandırırsa da başarılı saldırılarda çalınabilecek veri miktarını da büyütmektedir. Karmaşık donanım ve yazılımlar büyük kapasite sunarken, aynı zamanda kırılgan olmaları davetsizlerin tespitini zorlaştırmaktadır. Dolayısıyla, siber sistemler fayda sağlarken aynı zamanda zayıflıklara ve tehditlere de kapı aralamaktadır. Ponemon Enstitüsü'nün araştırmalarına göre, ABD'deki şirketler sistemlerindeki bir sızmayı ortalama 20 günde tespit edebilmektedir. Güvenlik duvarları ve saldırı tespit sistemleri gibi güncel koruma araçlarının yanı sıra, karmaşık parolaların kullanılması, sık şifre değişikliği, verilerin şifrelenerek iletilmesi, güvenlik duvarlarıyla ağların ayrıştırılması, güncellemelerin zamanında yapılması, hassas sistemlere erişimlerin sınırlandırılması ve tedarikçilerin güvenlik denetiminden geçirilmesi siber hijyenin temel unsurlarını oluşturmaktadır. CEO'lar, bu önlemler sayesinde şirketlerini büyük zararlardan koruyabileceklerini düşünmektedir. Ancak siber hijyen, daha çok sıradan saldırılara ve amatör hackerlara karşı etkilidir. Michael Assante'nin ifadesiyle, "Siber hijyen sadece çevrimiçi şakaları bertaraf etmekte etkili olmaktadır. Ütopik bir dünyada mükemmel uygulansa bile saldırganların yalnızca %95'ini engelleyebilmektedir. Ancak gerçek dünyada belirli bir hedefe odaklanan yetenekli saldırganlar için sadece caydırıcı olabilmektedir" (IBM Security, & Ponemon Institute, 2023; Singer, P. W., & Friedman, 2014; SecureWorld, 2019; SANS Institute, 2019).

Ağ güvenliğinin temel bileşenlerinden biri olan Saldırı Tespit Sistemleri (Intrusion Detection Systems – IDS), kullanıcıların veya süreçlerin yetkisiz erişim girişiminde bulunup bulunmadığını belirlemek amacıyla ağ trafiğini ve sistem davranışlarını sürekli olarak analiz eden yapılardır. Bu sistemler, normal kullanıcı faaliyetlerini istatistiksel ve davranışsal modeller aracılığıyla sınıflandırarak, olağan dışı bir erişim örüntüsü ortaya çıktığında bunu potansiyel bir saldırı olarak işaretlemektedir. Atagün, Temür ve Biroğul'un (2024) da vurguladığı üzere, IDS modellerinin başarısı yalnızca saldırıların tespit edilmesiyle sınırlı değildir; aynı zamanda normal ve anormal erişim davranışlarının doğru biçimde ayrıştırılmasına dayanmaktadır. Bu nedenle modern IDS yaklaşımları, özellikle makine öğrenmesi ve açıklanabilir yapay zekâ tekniklerini kullanarak sınıflandırma süreçlerini daha şeffaf, yorumlanabilir ve güvenilir hâle getirmeyi amaçlamaktadır. Böylece sistem, hem yetkisiz erişim girişimlerini erken aşamada tespit edebilmekte hem de güvenlik yöneticilerine karar destek sağlayarak ağ bütünlüğünün korunmasına katkıda bulunmaktadır.

Siber güvenlik literatürü, kurumsal dijital varlıkların bütüncül biçimde haritalandırılmasını etkili risk yönetiminin temel aşamalarından biri olarak değerlendirmektedir. Bu kapsamda araştırmalar, bir organizasyonun yalnızca kendi bilgi işlem altyapısını değil; aynı zamanda üçüncü taraf tedarikçileri, dış hizmet sağlayıcıları, donanım ve yazılım bileşenlerini, üretim süreçlerini, kontrol ve otomasyon sistemlerini, fiziksel girdileri ve veri akışlarını ayrıntılı biçimde envanterleştirmesi gerektiğini vurgulamaktadır. NIST ve ENISA gibi kurumların yayımladığı rehberlerde, saldırganların çoğu zaman sistemler arasındaki geçiş noktalarını (pivot points) hedef aldığı, bu nedenle kurumların kendi ağ topolojilerini ve veri akışlarını tam olarak bilmemeleri hâlinde ciddi güvenlik açıklarının ortaya çıkabileceği belirtilmektedir. Bu çerçevede literatür, ekipmanlara kimlerin erişim sağladığı, ağlarda bilginin hangi yollar üzerinden aktığı ve bu bilgilerin hangi teknik ve idari kontrollerle korunduğu sorularının siber güvenlik yönetiminin merkezinde yer aldığını göstermektedir. Özellikle tedarik zinciri saldırılarının artması, dijital varlık envanterinin çıkarılmasını ve erişim yönetimi süreçlerinin güçlendirilmesini kurumsal güvenlik stratejilerinin vazgeçilmez bir bileşeni hâline getirmiştir (ENISA, 2021; NIST, 2018; NIST, 2015).

En gelişmiş siber güvenlik uygulamaları dahi, Kuzey Kore veya Rusya gibi yüksek kapasiteye sahip siber tehdit gruplarını durdurmakta yetersiz kalabilmektedir. Bu bağlamda, kritik işlevlerin dijital teknolojilere bağımlılığını ve internet bağlantısını sınırlandırmak riski azaltmanın etkili yollarından biridir. Verilerin %25'i iç kaynaklı tehditlerden etkilenmektedir. Sektörler arasında farklılıklar bulunmakla birlikte, sağlık hizmetleri ve kamu hizmetleri gibi hassas bilgilerin işlendiği alanlarda iç tehditlerin oranı yüksektir. Öte yandan, restoranlar ve mağazalar gibi sektörler daha çok dış saldırılara maruz kalmaktadır. Sağlık sektöründe siber saldırıların %50'sinden fazlası başarılı olurken, diğerleri engellenmekte veya başarısız olmaktadır. Tek tip bilgi içeren sektörler (ör. sağlık, konaklama ve gıda) daha etkili savunmalar geliştirebilmektedir; çünkü bu alanlarda saldırı motivasyonu ve hedefler daha açıktır. Siber saldırıların başlıca nedenleri arasında ayrıcalıkların kötüye kullanılması, web uygulaması hataları ve diğer teknik açıklar bulunmaktadır.

Literatür, siber saldırı ekosisteminin giderek çeşitlenen tehdit vektörleri üzerinden şekillendiğini göstermektedir. Accenture, McAfee ve IBM gibi kuruluşların yayımladığı küresel siber suç maliyeti raporlarında; kart kopyalama, kötü amaçlı yazılımlar, siber casusluk faaliyetleri, hizmet kesintileri, varlık hırsızlıkları ve ödeme noktası saldırılarının en yaygın saldırı kategorileri arasında yer aldığı belirtilmektedir. Sağlık sektörü özelinde yapılan analizler ise, Health-ISAC ve ENISA tarafından ortaya konulduğu üzere, sektörün yıllık ortalama siber suç maliyetinin diğer sektörlerle kıyasla belirgin biçimde yüksek olduğunu ve yaklaşık 13 milyon dolar seviyesine ulaştığını göstermektedir. Bununla birlikte NIST ve MITRE tarafından geliştirilen siber dayanıklılık çerçeveleri, modern sistemlerin saldırı anında dahi çalışmaya devam edebilmesini önemli bir ilerleme olarak değerlendirse de literatür bu durumun aynı zamanda kritik bir çelişkiyi ortaya çıkardığını vurgulamaktadır: Engelleme ve tespit kapasitesi artmasına rağmen, başarılı saldırıların yol açtığı operasyonel, finansal ve hukuki zararların azaltılmasında kurumların hâlâ yetersiz kaldığı görülmektedir. Bu nedenle güncel çalışmalar, yalnızca saldırı önleme odaklı güvenlik yaklaşımlarının değil, aynı zamanda zarar azaltma, iş sürekliliği, olay müdahalesi ve kurumsal dayanıklılık stratejilerinin bütüncül biçimde ele alınması gerektiğini ortaya koymaktadır. (Accenture, 2019; ENISA, 2023; National Institute of Standards and Technology, 2021).

Siber güvenlik literatürü, güvenliğin mutlak olarak sağlanabilecek bir durumdan ziyade, sürekli yönetilmesi gereken dinamik bir süreç olduğunu vurgulamaktadır. NIST ve ISO gibi uluslararası standart kuruluşları, hiçbir kurumun tüm siber riskleri tamamen ortadan kaldırmasının mümkün olmadığını; bu nedenle temel amacın riskleri kabul edilebilir ve yönetilebilir bir seviyeye indirmek olduğunu belirtmektedir. Bu çerçevede kurumsal aktörlerin risk algıları, sahip oldukları uzmanlık alanlarına göre önemli ölçüde farklılaşabilmektedir. Hukuk danışmanları siber güvenliği öncelikle mevzuata uyum, veri koruma yükümlülükleri ve hukuki sorumluluklar açısından değerlendirirken; bilgi güvenliği yöneticileri teknik açıklar, zafiyet yönetimi ve saldırı yüzeyinin azaltılması üzerinde yoğunlaşmaktadır. Risk yöneticileri ise risk transferi, sigorta mekanizmaları ve kurumsal risk iştahı gibi finansal araçları ön plana çıkarırken; finans yöneticileri siber saldırıların potansiyel ekonomik etkilerini, operasyonel kesintileri ve mali sürdürülebilirlik üzerindeki sonuçlarını dikkate almaktadır. Bu durum, siber güvenliğin yalnızca teknik bir mesele değil, aynı zamanda hukuki, yönetsel ve ekonomik boyutları olan çok disiplinli bir yönetim alanı olduğunu göstermektedir. (International Organization for Standardization, 2022; National Institute of Standards and Technology, 2018; World Economic Forum, 2022).

Tedarik zincirindeki yüklenici, danışman ve satıcıların süreçteki rollerinin farkında olmaları ve bilgilendirilmeleri gerekmektedir. Çalışanlar, siber güvenliğin en zayıf halkası olsa da kendilerine basit ve izlenebilir politikalar sunulduğunda kurumların en güçlü savunucuları haline gelebilirler. Bir hata durumunda güvenin yeniden tesisi için en etkili yol şeffaflıktır. Siber saldırıların tespiti, saldırı kaynağına ilişkin bilgi toplama ve önleyici karşı hamlelerin yapılması aktif siber

savunmanın kapsamına girmektedir. Denning ve Strawser'in ifadesiyle, "Aktif siber savunma, dost güçler ve varlıklara yönelik siber tehditleri ortadan kaldırmak, etkisiz hale getirmek veya zayıflatmak amacıyla kullanılan doğrudan savunma yöntemidir" (Denning, D. E., & Strawser, M. 2017; European Union Agency for Cybersecurity, 2018; European Union Agency for Cybersecurity, 2021).

3.2. Blok Zincir ve Yeni Güven Mimarisi

Blok zincirinde bazı bileşenler güvenilir olmasa dahi, sistemin bir bütün olarak sonucuna güven duyulabilmektedir. Sistem, her birey için ağ güvenliğini artırarak kişisel faydaları ortak yarara dönüştürmektedir. Geleneksel sözleşmeler, düzenlemelerin sürekli ilişkiler içinde ortaya çıktığını varsaymaktadır. Buna karşılık akıllı sözleşmeler, her bir işlemi bağımsız biçimde değerlendirmektedir. Blok zincir teknolojileri başarılı bir şekilde işlediği için hem değerli hem de cazip görülmektedir; ancak zamanla bu teknolojilerin kapsamı genişledikçe ve süreklilik kazandıkça verimliliğe ilişkin endişeler gündeme gelecektir (Werbach, 2021).

Blok zincir teknolojisi, güveni ortadan kaldıran değil, aksine güvenin niteliğini dönüştüren bir mimari olarak değerlendirilmektedir. Bu yapıda katılımcılar, merkezi bir otoriteye, aracı kurumlara veya bireysel aktörlere güvenmek zorunda kalmaksızın, dağıtık defter üzerinde tutulan kayıtların bütünlüğüne ve doğruluğuna güven duyabilmektedir. Werbach'ın belirttiği üzere, blok zincir sistemleri karşılıklı güvensizlikten sistemsel güven üreten yeni bir güven mimarisi ortaya koymakta; böylece bireysel çıkarlar, ağın bütününe yönelik ortak bir güvenlik faydasına dönüşmektedir. Bu çerçevede akıllı sözleşmeler, geleneksel sözleşmelerin süreklilik ve ilişkisellik varsayımlarından ayrılarak her bir işlemi bağımsız ve otomatik biçimde değerlendirmekte, böylece hukuki güvenlik ile teknik kesinliği bir araya getiren hibrit bir yapı sunmaktadır. Albert Wenger'in "mantıksal olarak merkezi, yapısal olarak dağıtık" şeklindeki tanımı ise blok zincirin hem tekil bir kayıt mantığına sahip olduğunu hem de bu kaydın çok sayıda düğüm tarafından senkronize biçimde tutulduğunu göstermektedir. Bu dağıtık yapı, devletlerin veya özel aktörlerin işlemleri tek taraflı olarak durdurma ya da değiştirme kapasitesini sınırlamakta; aynı zamanda yeni bağımsız uygulamaların, tahmin pazarlarının, merkeziyetsiz sosyal ağların ve hizmet ekonomisine katkı sağlayabilecek yenilikçi platformların gelişmesine olanak tanımaktadır. Bununla birlikte literatür, blok zincirin cazibesinin büyük ölçüde teknik işleyişindeki güvenilirlikten kaynaklandığını, ancak teknolojinin ölçeklenmesi ve yaygınlaşmasıyla birlikte verimlilik, yönetim ve hukuki uyum konularında yeni tartışmaların ortaya çıkacağını vurgulamaktadır (Werbach, 2018; Narayanan & Clark, 2017).

SONUÇ ve ÖNERİLER

Bu çalışmada, bilimsel veri yönetiminde güvenlik, şeffaflık, veri bütünlüğü ve izlenebilirlik sorunlarına çözüm olarak Blockchain teknolojisinin sunduğu potansiyel fırsatlar değerlendirilmiştir. Yapılan çalışmalar, merkeziyetsiz, değiştirilemez ve izlenebilir kayıt sistemleri aracılığıyla Blockchain'in, bilimsel araştırmalarda veri manipülasyonunu engelleme, etik ihlalleri azaltma ve veri paylaşımını teşvik etme gibi önemli katkılar sağladığını göstermektedir. Özellikle açık bilim hareketiyle birlikte artan şeffaflık beklentileri, Blockchain'in bu alandaki önemini daha görünür kılmıştır.

Bilimsel verilerin üretilmesinden analiz edilmesine, depolanmasından yayımlanmasına kadar olan tüm süreçlerde Blockchain tabanlı sistemlerin benimsenmesi, yalnızca araştırmacılar arasındaki güveni artırmakla kalmaz; aynı zamanda kurumsal iş birliklerinin daha sağlam temellere oturmasına da katkı sunar. Bununla birlikte, söz konusu teknolojinin etik standartların korunması ve akademik sahtekârlığın önlenmesi açısından önemli bir araç olabileceği vurgulanmaktadır. Bununla beraber, Blockchain'in bilimsel veri yönetimine entegrasyonu çeşitli teknik, hukuki ve

operasyonel zorlukları da beraberinde getirmektedir. Özellikle büyük veri setlerinin doğrudan blok zincirine yüklenmesi yerine hash tabanlı referans sistemlerinin kullanılması yönünde mimari çözümler geliştirilmesi gerekmektedir. Ayrıca kişisel verilerin korunması ve veri erişim politikalarının yeniden şekillendirilmesi de zorunludur. Blockchain teknolojisinin etik ve etkin kullanılabilmesi için küresel iş birliğine ve eşit fırsatlar sağlayacak politikalara ihtiyaç vardır (Perkins, 2003). Kullanıcı ve işlem sayısına bağlı ortaya çıkan ölçeklenebilirlik sorunu (Sharples ve Domingue, 2016) ayrıca altyapı ve yönetim faaliyetleri de (Bore vd, 2017) blockchain teknolojisini kullanırken tereddüt yaşamamıza sebep olmaktadır.

Sonuç olarak, Blockchain teknolojisi, bilimsel veri yönetiminde devrim niteliğinde etkiler yaratma potansiyeline sahip güçlü bir araçtır. Ancak bu potansiyelin hayata geçirilebilmesi için hem teknik altyapının güçlendirilmesi hem de bilimsel topluluklar ile yasal düzenleyicilerin bu yeni sistemleri benimsemesi gerekmektedir. Gelecekte yapılacak çalışmalar, teknolojinin farklı disiplinlerdeki bilimsel uygulamalarını derinlemesine inceleyerek Blockchain tabanlı veri yönetim sistemlerinin standardizasyonuna katkı sağlayacaktır.

Blockchain teknolojisi matematiksel modelleme, simülasyon ve algoritma geliştirme gibi alanlarda ilmi emeğe yardım etmektedir. Varsayım geliştirme prosesine hız kazandırır ve deneysel sonuçların doğruluğunu arttırmaktadır. Ancak blockchain teknolojisinin temel bilimlerde uygulanması klasik yöntemlere kıyasla daha karmaşık süreçler gerektirmektedir. Blockchain teknolojisinin bilimsel bütünlüğü koruma potansiyeli bulunsa bile küresel eşitsizliklerin giderilmesine yönelik politikalar artırılmalıdır. Blockchain teknolojisinin etik ve etkin bir şekilde kullanılabilmesi için küresel iş birliğine ve fırsatlar sağlayacak politikalara ihtiyaç vardır.

Blockchain teknolojisi halen büyük ölçüde düzenlemelerden yoksundur. Yasaların blockchain teknolojisine kapsama altına almasında fayda olacaktır. Blockchain teknolojisinin eğitimde kullanımına ilişkin net yönergeler ve standartlar bulunmamaktadır. Akademik alanda uygulanabilmesi için gerekli altyapının oluşturulması ve mevzuatın ayrıntılı biçimde düzenlenmesi gerekmektedir. Bu kapsamda personel eğitimi sağlanmalı veya bir dış merkezden uzman desteği alınmalıdır. Sistemdeki güç dinamiklerinin nasıl evrimleşebileceğini ve istenmeyen sonuçların nasıl azaltılabileceğini sürekli değerlendirmek gerekmektedir. Uygulama sürecinde etik yönergeler normlara ve değerlere ihtiyaç duyulmaktadır. Bireylerin kişisel verilerinin düzensiz biçimde işlenmesi ve algoritmik kararlarının toplumsal eşitsizlikleri artırması etik riskleri daha görünür hale getirmiştir. Bu etik gerilmelere karşı güçlü sürdürülebilir ve kapsamlı bir etik yapı inşa edilmelidir.

Yapay Zekâ Kullanım Beyanı

Bu çalışmanın hazırlanması sırasında yazarlar, konu ile ilgili daha çok kaynak bulabilmek, ulaştıkları ve yararlandıkları kaynakları teyit edebilmek, İngilizce özet yazmak amacıyla “Copilot” adlı yapay zekâ aracını kullanmıştır. Bu aracı/hizmeti kullandıktan sonra yazarlar, içeriği gerektiği gibi gözden geçirip düzenlemiş olup yayınlanan makalenin içeriğine ilişkin tüm sorumluluğu üstlenmektedir.

Teşekkür

Yüksek lisans eğitimim süresince bilgileriyle ve tecrübeleriyle yolumu aydınlatan, zor günlerimde desteklerini esirgemeyen danışmanın Sayın Prof. Dr. Hasan Tahsin KEÇELİGİL’e sonsuz teşekkürlerimi sunarım.

KAYNAKÇA

- Accenture. (2019). *The cost of cybercrime study*. Accenture Security.
- Agerskov, S. (2024). First Official EU Ethical Guidelines for Blockchain Systems. <https://dataethics.eu/first-official-eu-ethical-guidelines-for-blockchain-systems/> (E.T. 24.05.2026)
- Aktaş D, Tan E ve Arap İ. (2024). Avrupa Blok Zinciri Hizmetleri Altyapısının (EBSI) Süreç Analizi Modeli ile İncelenmesi. *Journal of Business Innovation and Governance*. 7(1), 1-26. <https://doi.org/10.54472/jobig.1491620>. <https://dergipark.org.tr/tr/pub/jobig/article/1491620> (E.T. 24.05.2026)
- Alketbi, A., Nasir, Q. ve Talib, M. A. (2018). Blockchain for government services — Use cases, security benefits and challenges. *15th Learning and Technology Conference (L&T)*, 112–119.
- Aslan, A. (2022). Dijital Hayattaki Etik İhlallerin Tespiti ve Analizi: Cambridge Analytica Veri Skandalı. *Journal of Media Literacy Studies*. 1(1), 57-61. <https://doi.org/10.5281/zenodo.7301585> <https://medyaokuryazari.org/wp-content/uploads/2022/11/6-Dijital%20Hayattaki%20Etik%20%C4%B0hlallerin%20Tespiti%20ve%20Analizi.pdf> (E.T. 24.05.2026)
- Aslan, M & Kasapbaşı, M.C. (2022). Blok Zinciri Platformları, Fikir Birliği Mekanizmaları ve Ağın Güvenlik Analizi. *Haliç Üniversitesi Fen Bilimleri Dergisi*, 5(1), 43-72, DOI: 10.46373/hafebid.1000108. <https://dergipark.org.tr/tr/download/article-file/1992054> (E.T. 24.05.2026)
- Atagün, E., Temür, G., & Biroğul, S. (2024). Application Of Explainable Artificial Intelligence In Intrusion Detection System Classification Using Boosting Algorithms. *Muğla Journal of Science and Technology*, 10(1), 1-7. <https://doi.org/10.22531/muglajsci.1343051> (E.T. 24.05.2026)
- Babaoğlu, C. (2025). *Yapay Zekâ Çağında Dijital Özerklik, Mahremiyet Erozyonu ve Algoritmik Hakimiyet*. SETA. https://www.setav.org/yapay-zeka-caginda-dijital-ozerklik-mahremiyet-erozyonu-ve-algoritmik-hakimiyet?utm_source=copilot.com (E.T. 23.05.2026)
- Beyaznet. (2026). *Hash Fonksiyonu (Özetleme Fonksiyonu) ve Birthday Attack*. https://www.beyaz.net/tr/guvenlik/makaleler/hash_fonksiyonu_ozetleme_fonksiyonu_ve_birthday_attack.html (E.T. 19.05.2026)
- Blockchain Türkiye Platformu. (2018). *Blockchain Türkiye*. <https://bctr.org/blockchain-turkiye-platformu-kuruldu-3821/> (E.T. 19.05.2026)
- Blockchain Türkiye Platformu. (2026). *Avrupa Blokzinciri Altyapısı (EBSI) devreye girdi*. <https://bctr.org/avrupa-blokzinciri-altyapisi-ebsi-devreye-girdi-14246/> (E.T. 24.05.2026)
- Blokzincir Laboratuvarı. (2026). *Blokzincir nedir?* https://blokzincir.bilgem.tubitak.gov.tr/blokzincir-nedir/?utm_source=copilot.com (E.T. 19.05.2026)
- Bore, N., Karumba, S., Mutahi, J., Darnell, S. S., Wayua, C. ve Weldemariam, K. (2017, Kasım). Towards blockchain-enabled school information hub. *Proceedings of the Ninth International Conference on Information and Communication Technologies and Development*, 1–4.
- Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. New York, NY: W. W. Norton & Company.
- Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12.
- Coino. (2025). *Merkle Ağacı (Merkle Tree) Nedir? Blokzincir Güvenliğinde Rolü ve Kullanımı*. <https://blog.coino.com.tr/tr/blog/merkle-agaci-merkle-tree-nedir-blokzincir-guvenliginde-rolu-ve-kullanimi> (E.T. 12.05.2026)
- Cooper. (2023). *Cooperatives: An Ownership Model for Digital Networks*. KPMG. Retrieved from <https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/cooperatives-path-to-compliance-web3.pdf> (E.T. 23.09.2026)

- Cormen, T. H., Leiserson, C. E., Rivest, R. L. ve Stein, C. (2009). *Introduction to algorithms* (4. Baskı). Cambridge, MA: MIT Press.
- Denning, D. E., & Strawser, M. (2017). Active cyber defense: Applying air defense to the cyber domain. *Joint Force Quarterly*, 85, 30–37. National Defense University Press.
- Duran, O. (2025). Yapay Zekâda Etik ve Toplumsal Etki: Şeffaflık, Hesap Verebilirlik ve İnsan Denetimi. *İstanbul Rumeli Üniversitesi İnsan ve Toplum Bilimleri Dergisi*, 1(2), 69-89.
- ENISA. (2018). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. *European Union Agency for Cybersecurity*.
- ENISA. (2021). Cybersecurity culture: Guidelines and best practices. *European Union Agency for Cybersecurity*.
- ENISA. (2021). Threat landscape for supply chain attacks. *European Union Agency for Cybersecurity*.
- ENISA. (2023). Healthcare cybersecurity: Threat landscape report. *European Union Agency for Cybersecurity*.
- EU Expert Group on Blockchain Ethics. (2026). *Official guidelines for blockchain systems within the European Union*. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/674507497/EU+Expert+Group+on+Blockchain+Ethics> (E.T. 24.05.2026)
- EU The European Blockchain Services Infrastructure. (2026). *What is EBSI*. <https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/447687044/Home> (E.T. 24.05.2026)
- Federal Trade Commission. (2022). *Bringing dark patterns to light*. FTC Report. Retrieved from <https://www.ftc.gov/reports/bringing-dark-patterns-light> (E.T. 19.05.2026)
- Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, 114, 254–280. <https://doi.org/10.1016/j.techfore.2016.08.019> (E.T. 19.05.2026)
- Goodrich, M. T. ve Tamassia, R. (2014). *Data structures and algorithms in Java* (6. Baskı). Hoboken, NJ: Wiley.
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–14). New York, NY: ACM. <https://doi.org/10.1145/3173574.3174108> (E.T. 19.05.2026)
- Haber, S. ve Stornetta, W. S. (1991). How to time-stamp a digital document. In A. J. Menezes & S. A. Vanstone (Eds.), *Advances in Cryptology – CRYPTO’90* (ss. 437–455). Berlin: Springer.
- Hargittai, E. (2002). Second-level digital divide: Differences in people’s online skills. *First Monday*, 7(4). <https://doi.org/10.5210/fm.v7i4.942> (E.T. 19.05.2026)
- Hyvarinen, A. ve Morioka, H. (2017). Unsupervised feature extraction by time-contrastive learning and nonlinear ICA. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics* (Cilt 54, ss. 460–469). PMLR.
- IBM Security, & Ponemon Institute. (2023). *Cost of a data breach report*. IBM Security.
- International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. ISO.
- Jirgensons, M. ve Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. *Journal of Teacher Education for Sustainability*, 20(1), 145–156.
- Kindervag, J. (2010). *Artık chewy merkezleri yok: Bilgi güvenliğinin sıfır güven modeli*. Cambridge: Forrester Research Inc. <https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf> (E.T. 19.05.206)
- Korkmaz, A & Sönmez, T. (2025). Türk Hukukunda Karanlık Tasarımlar (Dark Patterns). *AkdHFD*. 15(1), 669-697. <https://dergipark.org.tr/tr/download/article-file/4730014> (E.T. 19.05.206)
- Kuçuradi, İ. (1999). *Etik*. Türkiye Felsefe Kurumu Yayınları.
- Kuçuradi, İ. (2003). *İnsan ve değerleri*. Türkiye Felsefe Kurumu Yayınları.

- Küre Ansiklopedi. (2026). *İş Kanıtı (Proof of Work)*. <https://kureansiklopedi.com/tr/detay/is-kaniti-proof-of-work-59fda> (E.T. 23.05.2026)
- Ledger Academy. (2026). *İş İspatı (Proof of Work; PoW) Nedir?* <https://www.ledger.com/tr/academy/is-ispati-proof-of-work-pow-nedir> (E.T. 23.05.2026)
- Loukil, F., Abed, M. ve Boukadi, K. (2021). Blockchain adoption in education: A systematic literature review. *Education and Information Technologies*, 26(5), 5779–5797.
- Mahankali, S. ve Chaudhary, S. (2020). Blockchain in education: A comprehensive approach – Utility, use cases, and implementation in a university. In R. Sharma (Ed.), *Blockchain in education* (ss. 267–293). Cham: Springer.
- Martini, M. ve Weinzierl, Q. (2017). Die Blockchain-Technologie und das Recht auf Vergessenwerden: Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen. *Zeitschrift für Datenschutz*, 17, 1251–1260.
- Mathur, A., Acar, G., Friedman, M. G., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–32. <https://doi.org/10.1145/3359183> (E.T. 19.05.2026)
- Mattila, J. (2016). *The blockchain phenomenon: The disruptive potential of distributed consensus architectures*. Helsinki: The Research Institute of the Finnish Economy.
- Mayacı, M. (2025). Kamu Yönetiminin Şeffaflığından Algoritmaların Şeffaflığına Geçiş: Şeffaflığı Algoritmaların Opaklığı ve Kara Kutu Problemi Çerçevesinde Yeniden Değerlendirmek. *Abant Sosyal Bilimler Dergisi*, 25(2), 827-841, DOI: 10.11616/asbi.1658320. <https://search.trdizin.gov.tr/tr/yayin/detay/1334643/kamu-yonetiminin-seffafligindan-algoritmalarin-seffafligina-gecis-seffafligi-algoritmalarin-opakligi-ve-kara-kutu-problemi-cercevesinde-yeniden-degerlendirmek> (E.T. 19.05.2026)
- Microsoft. (2026). *Sıfır Güven Mimarisi Nedir?* https://www.microsoft.com/tr-tr/security/business/security-101/what-is-zero-trust-architecture?utm_source=copilot.com (E.T. 19.05.2026)
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. <https://doi.org/10.1177/2053951716679679>
- Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. New York, NY: PublicAffairs.
- Nakamoto, S. (2018). *Bitcoin: A peer-to-peer electronic cash system*. <http://citeseerx.ist.psu.edu/viewdoc/summary> (E.T. 20.05.2026)
- Narayanan, A., & Clark, J. (2017). Bitcoin’s academic pedigree. *Communications of the ACM*, 60(12), 36–45. <https://doi.org/10.1145/3132259> (E.T. 19.05.2026)
- Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark patterns: Past, present, and future. *Communications of the ACM*, 63(9), 42–47. <https://doi.org/10.1145/3397884> (E.T. 23.05.2026)
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. U.S. Department of Commerce.
- NIST. (2015). *Guide to industrial control systems (ICS) security (NIST SP 800-82 Rev. 2)*. National Institute of Standards and Technology.
- NIST. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. National Institute of Standards and Technology.
- Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge: Cambridge University Press.
- O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York, NY: Crown.

- Oracle. (2021). *Blok zinciri nedir?* https://www.oracle.com/tr/blockchain/what-is-blockchain/?utm_source=copilot.com (E.T. 19.05.2026)
- Özcan, N. (2021). Dijital Etik Üzerine Nitel Bir Araştırma. *Gençlik Araştırmaları Dergisi*, 9(25), 89-105. <https://dergipark.org.tr/tr/download/article-file/2008395> (E.T. 23.05.2026)
- P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- Pilkington, M. (2016). Blockchain technology: Principles and applications. In X. Olleross & M. Zhegu (Eds.), *Research handbook on digital transformations* (ss. 225–253). Cheltenham: Edward Elgar Publishing.
- Rodeck, D. ve Curry, B. (2021, Nisan 1). Digital currency: The future of your money. *Forbes*. <https://www.forbes.com/advisor/investing/digital-currency> (E.T. 19.05.2026)
- SANS Institute. (2019). Remembering Michael J. Assante. *SANS Institute*. <https://www.sans.org> (E.T. 19.05.2026)
- Sarı, S. (2024). Dijitalleşmenin Günlük Yaşama Etkileri: Teknolojinin Artan Rolü ve İnsan Deneyimi. *Medyabar*. <https://medyabar.com/makale/21359581/serdar-sari/dijitallesmenin-gunluk-yasama-etkileri-teknolojinin-artan-rolu-ve-insan-deneyimi> (E.T. 20.05.2026)
- SecureWorld. (2019). Remembering Michael Assante, one of cybersecurity's "great ones". *SecureWorld*. <https://www.secureworld.io> (E.T. 23.05.2026)
- Sharples, M. ve Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. *European Conference on Technology Enhanced Learning* (ss. 490–496). Cham: Springer.
- Sote Haber. (2022). *IBM Raporu: Siber Saldırılarından En Ağır Darbeyi Üretim Aldı*. <https://www.sotehaber.com/post/ibm-raporu-siber-saldirilardan-en-agir-darbeyi-uretim-aldi> (E.T. 19.05.2026)
- Subashini, S. ve Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1–11.
- Susskind, R., & Susskind, D. (2015). *The future of the professions: How technology will transform the work of human experts*. Oxford: Oxford University Press.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media.
- T.C. Cumhurbaşkanlığı, Mevzuat Bilgi Sistemi. (2026). *Kişisel Verilerin Korunması Kanunu*. <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf> (E.T. 21.05.2026)
- T.C. Dışişleri Bakanlığı, Avrupa Birliği Başkanlığı. (2026). *AB Genel Veri Koruma Tüzüğü (GDPR) Türkçeye çevrildi*. https://www.ab.gov.tr/ab-genel-veri-koruma-tuzugu-gdpr-turkceye-cevrildi_53650.html (E.T. 21.05.2026)
- Taşdan, M. (2024). Eğitim yönetiminde blokzincir kullanımı: Uygulama alanları, fırsatlar ve zorluklar. *Elektronik Sosyal Bilimler Dergisi*, 23(90), 821–833.
- Trendmicro. (2026). *Sıfır Güven Mimarisi Nedir?* https://www.trendmicro.com/tr_tr/what-is/what-is-zero-trust/zero-trust-architecture.html?utm_source=copilot.com (E.T. 21.05.2026)
- Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*, 13(1), 203–218.
- Turancı, E. (2021). Dijital Dünyada Kişisel Veri ve Etik: Gizlilik Politikası Bağlamında “#WhatsAppSiliyoruz” Krizinde Kullanıcı Tepkilerini Anlamak. *TRT Akademi-Dijital Hayat ve Etik*. 6(12), 272-295.
- Ünar, Ç. (2024). Yapay Zekâ Yasası Madde 5 Bağlamında Dark Pattern. *Beykent Üniversitesi Hukuk Fakültesi Dergisi*. 10(20), 211-230. <https://www.seckin.com.tr/kitap/beykent-universitesi-hukuk-fakultesi-dergisi-cilt-10-sayi-20-aralik-2024-mete-ozgur-falcioğlu-s-p-276523144> (E.T. 24.05.2026)
- van Dijk, J. A. G. M. (2020). *The digital divide*. Cambridge, UK: Polity Press.

- Vikipedi. (2024). *Merkle ağacı*. https://tr.wikipedia.org/wiki/Merkle_a%C4%9Fac%C4%B1 (E.T. 12.05.2026)
- Vikipedi. (2026) *Blok zinciri*. https://tr.wikipedia.org/wiki/Blok_zinciri?utm_source=copilot.com (E.T. 14.05.2026)
- Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
- Whitebit. (2024). *Blok Zincirinde Hash Nedir?* <https://blog.whitebit-tr.com/what-is-a-hash-in-blockchain/> (E.T. 15.05.2026)
- World Economic Forum. (2022). *Global cybersecurity outlook 2022*. World Economic Forum.
- Xu, M., Chen, X. ve Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, 5(1), 1–14.
- Yaşar Üniversitesi-Haber. (2020). *Siber Saldırılar Ekonomiye Büyük Zarar Veriyor*. https://haber.yasar.edu.tr/siber-saldirilar-ekonomiye-buyuk-zarar-veriyor/?utm_source=copilot.com (E.T. 21.05.2026)
- Yılmaz, M. A. (2025). *Yapay Zekâ ve Kara Kutu Problemi /Algoritmaların Görünmeyen Karar Mekanizması*. Maykairos Dijital. <https://www.maykairos.com/yapay-zeka-ve-kara-kutu-problemi-algoritmalarin-gorunmeyen-karar-mekanizmasi/> (E.T. 24.05.2026)
- Yu, X., Tang, C., Palensky, P. ve Colombo, A. W. (2021). Blockchain: What does it mean to industrial electronics? Technologies, challenges, and opportunities. *IEEE Industrial Electronics Magazine*, 16(2), 4–14.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: PublicAffairs.