Kamu Ekonomisi ve Kamu Mali Yönetimi Dergisi, Cilt: 4 | Sayı: 2/ Ekim 2024

Journal of Public Economy and Public Financial Management, Volume: 4| Issue: 2| October 2024

DİJİTAL DÖNÜŞÜM SÜRECİNDE BLOK ZİNCİRİ: TEORİK YAKLAŞIMLAR VE SEKTÖREL UYGULAMALAR

Çağdaş TÜRKOĞLU[1]
Rukiye ÇELİK[2]

Makale İlk Gönderim Tarihi / Recieved (First): *23.10.2024,* ***Makale Kabul Tarihi:*** *26.10.2024*

Atıf/©: Türkoğlu, Ç., Çelik, R. (2024). Dijital Dönüşüm Sürecinde Blok Zinciri: Teorik Yaklaşımlar ve Sektörel Uygulamalar. *Journal of Public Economy and Public Financial Management,* 4(2), 83- 111.

Özet

Blok zinciri teknolojisi, dijital dönüşüm sürecinin önemli bir parçası olarak çeşitli sektörlerde artan bir şekilde kullanılmaktadır. Merkezi olmayan yapısı sayesinde veri güvenliği, şeffaflık ve değiştirilemezlik gibi özellikler sunarak geleneksel sistemlere kıyasla birçok avantaj sağlayabilmektedir. Özellikle finans, sağlık, lojistik, eğitim ve eğlence alanlarında verilerin güvenli depolanması, işlemlerin hızlandırılması ve maliyetlerin azaltılması adına dikkat çeken uygulamalar geliştirilmiştir.

Bu makalede, blok zincirinin teknik yapısı, kriptografik temelleri, dağıtık defter teknolojisi ve uzlaşma mekanizmaları gibi temel unsurlar ele alınmıştır. Ayrıca, bu teknolojinin farklı sektörlerdeki kullanım alanları ve sunduğu avantajlar üzerinde durulmuştur. Ayrıca, yapay zeka entegrasyonu ile birlikte blok zinciri teknolojisinin veri güvenliği ve otomasyon süreçlerinde daha güçlü çözümler sunabileceği vurgulanmıştır.

Blok zincirinin gelecekteki potansiyeli, mevcut sistemleri iyileştirmekle sınırlı kalmayıp yeni iş modelleri yaratma kapasitesine de dayanmaktadır. Merkezi olmayan finans uygulamaları, akıllı sözleşmeler ve dijital kimlik doğrulama gibi yenilikler, blok zincir teknolojisinin daha yaygın bir şekilde benimsenmesine yardımcı olmaktadır. Bu teknoloji hızla gelişirken birçok sektörde yenilikçi çözümlerin ortaya çıkması ve dijital dünyanın yapısında köklü değişikliklerin meydana gelmesi beklenmektedir.

Anahtar Kelimeler: Blok Zinciri Teknolojisi, Dijital Dönüşüm, Yapay Zeka

BLOCKCHAIN IN THE DIGITAL TRANSFORMATİON PROCESS: THEORETİCAL APPROACHES AND SECTORAL APPLİCATİONS

Citation/©:Türkoğlu, Ç., Çelik., R. (2024)BlockchaınınTheDıgıtalTransformationProcess: TheoreticalApproachesandSectoral Applications. *Journal of Journal of Public Economy and Public Financial Management,* 4(2), 83- 111.

Abstract

Blockchain technology is increasingly being utilized across various sectors as a key component of the digital transformation process. Its decentralized structure offers advantages such as data security, transparency, and immutability, making it superior to traditional systems in many aspects. Notable applications have been developed in areas such as finance, healthcare, logistics, education, and entertainment to securely store data, accelerate transactions, and reduce costs.

This article examines the fundamental elements of blockchain technology, including its technical structure, cryptographic foundations, distributed ledger technology, and consensus mechanisms. Additionally, the usage areas of this technology in different sectors and the advantages it offers are explored. Furthermore, it has been emphasized that the integration of artificial intelligence with blockchain technology can provide stronger solutions in data security and automation processes.

The potential of blockchain extends beyond improving current systems, as it has the capacity to create new business models. Innovations like decentralized finance (DeFi) applications, smart contracts and digital identity verification

[1]Öğr. Gör., Isparta Uygulamalı Bilimler Üniversitesi, cagdasturkoglu@isparta.edu.trOrcid: 0000-0002-2507-7544
[2]Doç. Dr., Süleyman Demirel Üniversitesi, rukiyecelik@sdu.edu.tr, Orcid: 0000-0002-2538-0228

are driving the wider adoption of blockchain technology. As this technology rapidly evolves, it is expected to lead to the emergence of innovative solutions across many sectors and bring about fundamental changes to the structure of the digital world.

Keywords: BlockchainTechnology, DigitalTransformation, ArtificialIntelligence

1. GİRİŞ

Teknolojinin hızla gelişmesi ve internetin yaygınlaşmasıyla birlikte, dijitalleşme hayatımızın her alanına nüfuz etmiş, geleneksel yöntemleri geride bırakarak yeni bir dönüşüm yaratmıştır. Bu dönüşümün temelinde, bilgi ve iletişim teknolojilerinin hızla gelişmesi yatmaktadır. Özellikle internetin yaygınlaşması, veri depolama ve işleme kapasitesinin artması, bulut bilişim ve yapay zeka gibi teknolojilerin gelişimi, dijital dönüşümün itici güçleri arasında yer almaktadır. Dijital dönüşümün toplumsal etkileri de oldukça geniş kapsamlıdır. Eğitimden sağlığa, kamu hizmetlerinden eğlence sektörüne kadar birçok alanda dijitalleşme, bireylerin yaşam kalitesini artırmakta ve yeni fırsatlar sunmaktadır. Ancak dijital dönüşümün getirdiği fırsatların yanı sıra, bazı zorluklar ve riskler de bulunmaktadır. Özellikle siber güvenlik tehditleri, kişisel verilerin korunması ve dijital eşitsizlik gibi konular, dijitalleşmenin olumsuz yanları olarak öne çıkmaktadır.

Teknoloji insan hayatını kolaylaştırırken, insanların yaşamlarında gizlilik ve güvenlik gibi önemli soruyu da beraberinde getirmiştir. Nesnelerin interneti(farklı cihazların birbirine internet üzerinden bağlanarak veri paylaşımı ve iletişim kurmasını sağlayan bir ağ yapısı) ile ilgili birçok endişe mevcuttur. İnternet tabanlı teknoloji insanlar tarafından kullanıldıkça yeni veriler oluşmakta, cihazlar üzerinde bilgi üretilmekte ve diğer insanlarla paylaşılmaktadır. Nesnelerin internetinin gelişimi ve hayatımıza entegrasyonu, bu teknolojinin ne kadar güvenli olduğu sorusunu da gündeme getirmektedir. Ayrıca gizlilik, başka bir önemli soruyu da beraberinde getirmiştir. Bu yüzden çevrimiçi gizlilik ve güvenliğin sağlanması için çeşitli tasarım yöntemleri, güvenlik ve koruma yöntemleri kullanılmaktadır.

Günümüzde sosyal medya, e-posta programları, iletişimle ilgili yazılımlar, e-sağlık, e-devlet, özel uygulamalar, e-ticaret siteleri ve lojistik gibi farklı alanlarda veri transferleri sürekli yapılmaktadır. Bu transfer süreçlerinde bazı kullanıcılarda güvenlik endişeleri oluşabilmektedir. Blok zinciri teknolojisi ise sağladığı olanaklar ve çeşitlenebilen uygulamalar aracılığıyla yüksek derecede güvenlik ve verimlilik sağladığı düşünülmektedir. Blok zinciri teknolojisinin merkezi olmayan yapısı, verilerin şeffaf olarak saklanması ve değiştirilemeyecek bir biçimde kaydedilmesi gibi özellikleri sayesinde birçok ihtiyacın karşılanmasında önemli bir araç olarak kullanılmasına imkan tanıyabilmektedir. Blok zinciri, işlemlerin kullanıcılara açık bir biçimde gerçekleştirildiği merkezi olmayan bir sistemde saklanmasını sağlayan yeni bir teknolojidir. Bu sistem merkezi olmayan bir defter ile uygulanmaktadır. Merkezi olmayan defter teknolojisi sayesinde veriler kalıcı ve değiştirilemeyecek şekilde saklanmaktadır. Güvenlik, şeffaflık ve değiştirilemezlik sayesinde birçok farklı alanda kullanılan bu teknoloji günümüzdeki uygulamalarda karşılaşılan birçok soruna da çözüm sağlayabilmektedir.

Bu çalışmanın ana sorunu, dijital dönüşüm sürecinde blok zinciri teknolojisinin teorik temelleri ve sektörel uygulamalarıyla ilgili eksiklerin giderilmesi olarak ele alınmıştır. Ara sorunlar ise blok zincirinin farklı sektörlerdeki etkileri, potansiyel zorluklar ve entegrasyon süreçleri üzerinedir. Çalışmanın amacı, blok zinciri teknolojisinin mevcut yapısını, teorik alt yapısını ve

sektörel kullanım alanlarını açıklamak, özellikle yapay zeka ile entegrasyonun bu alandaki yeniliklere nasıl katkı sağlayabileceğini ortaya koymaktır. Literatürdeki teorik alt yapı, blok zincirinin merkeziyetsizlik, veri güvenliği ve şeffaflık gibi temel özelliklerine dayanmaktadır. Çalışmanın ana varsayımları, blok zincirinin gelecekte birçok sektörde köklü değişiklikler yaratacağı ve iş süreçlerini dönüştüreceği yönündedir. Çalışma iddialarını, blok zincirinin merkezi olmayan finans, akıllı sözleşmeler ve dijital kimlik doğrulama gibi yeniliklerin yaygınlaşmasıyla desteklemektedir. Araştırma soruları, blok zincirinin farklı sektörlerde nasıl ve ne ölçüde kullanılabileceğine odaklanmaktadır. Yöntem olarak literatür taraması ve sektör bazlı uygulamalar incelenmiştir. Çalışmanın sonuç bölümünde, blok zinciri teknolojisinin sağladığı avantajlar ve çözülmesi gereken zorluklar ele alınmıştır. Özellikle veri güvenliği, maliyet düşürme ve işlem hızlandırma alanındaki bulgularla iddialar desteklenmiştir. Tartışmalı konular ise enerji tüketimi ve yasal düzenlemeler üzerine yoğunlaşmaktadır. Çalışmanın önerileri, sektörlerin blok zinciri teknolojisine yönelik farkındalıklarını artırmaları ve regülasyonlarla birlikte bu teknolojinin daha etkin kullanılabilmesi için iş birliğinin güçlendirilmesi üzerinedir.

Blok zinciri teknolojisi özellikle finans, bankacılık, kamu yönetimi, sağlık ve mesleki hizmetler gibi farklı sektörlerde uygulanabileceği için büyük ilgi görmektedir. Fakat, blok zinciri yeni bir teknoloji olması sebebiyle sürekli değişmekte ve gelişmektedir. Blok zinciri konusundaki bilgi ve öngörü eksikliği bankacılık sektörü dışında diğer sektörlerde nasıl bir çalışma mekanizması olduğunun farkında olmaması sebebiyle bu teknolojinin değerinin açıklığa kavuşturulmasına halen ihtiyaç duyulmaktadır. Tüm bunlardan hareketle bu çalışmada, blok zinciri teknolojisinin teknik boyutu incelenecek olup, sektörlerdeki uygulamalarla birlikte potansiyel kullanım alanları incelenecektir.

2. BLOK ZİNCİRİ TEKNOLOJİSİ

Blok zinciri kavramı, ilk olarak 1990'ların başında, dijital belgelerin saklanması için merkezi kontrol olmadan güvenliği sağlamak amacıyla veri yapıları ve algoritmalar önerilerek ortaya atılmıştır (Bayer vd,, 1993: 329). Stuart Haber ve W. Scott Stornetta'nın yayınladığı bir araştırma makalesinde, dijital belgelerin doğruluğunu ve bütünlüğünü sağlamak için zaman damgası kullanma yöntemi önerilmiştir. Bu makalede, verilerin güvenli ve merkezi olmayan bir şekilde depolanması için blok zinciri kullanma fikri özetlenmiş ve daha sonra blok zinciri teknolojisi olarak bilinecek olan kavramın temelleri atılmıştır (Haber, Stornetta, 1991). Ancak, 2009 yılında Bitcoin'in ortaya çıkışına kadar blok zinciri teknolojisi geniş çapta ilgi görmemiştir. Blok zinciri kavramı ilk kez teorik olarak 2008'de SatoshiNakamoto takma adını kullanan bir kişi tarafından kaleme alınan Bitcoin makalesinde ele alınmıştır (Nakamoto, 2008).Makalede adı doğrudan belirtilmese de, kriptografik yöntemlerle birbirine bağlı bloklar dizini şeklinde tanımlanarak kripto paranın temel bileşeni olarak sunulmuştur (Nakamoto, 2008:6)SatoshiNakamotoise blok zincirinin gelişim tarihinde en etkili figürlerden biri olmuştur. Gizemli bir şekilde Bitcoin'in yaratıcısı olan bu kişi, dünyayı merkezi olmayan dijital para ve ona dayalı blok zinciri teknolojisi ile tanıştırmıştır. Nakamoto'nun Bitcoin ile ilgili teknik incelemesi, birçok başka blok zinciri projesinin ve kripto para biriminin geliştirilmesine öncülük etmiş olup onu blok zinciri teknolojisinin gelişiminde önemli bir figür haline getirmiştir (Sanka, 2021: 188-189). Bitcoin, finansal özellikleri ve yarattığı ekonomik değer nedeniyle dikkat çekmiş ve finans sektöründe önemli bir başarı elde etmiştir. Bu gelişmeye bağlı olarak,

Bitcoin'in temel bileşeni olan blok zinciri teknolojisi de önem kazanmış ve birçok farklı alanda kullanılabilir olduğu kabul edilmiştir (Ünsal ve Kocaoğlu, 2018: 54).Blok zinciri, özel sektörden kamu sektörüne, bireylerden devletlere kadar her türlü kişi ve kuruluşun yakın gelecekte hayatının bir parçası olması beklenen yeni bir teknolojik altyapı olarak değerlendirilmektedir (Metin, Arslan, 2018: 151).

2. BLOK ZİNCİRİ TEKNOLOJİSİNİN MİMARİSİ

Hızla ilerleyen teknoloji çağında, blok zinciri güvenli ve şeffaf işlem arayışına önemli bir yenilik getirmiştir. Bu yenilikçi yaklaşım, işlemlerin yapısına benzersiz seviyede güvenlik, şeffaflık ve verimlilik ekleyerek finanstan tedarik zinciri lojistiğine kadar birçok sektörde işlem yönetiminin temel değişimini sağlamıştır. Bu dönüşümün merkezinde ise blok zincirinin merkeziyetsiz yapısı bulunmaktadır. Blok zinciri, merkezi olmayan bir yapıyı benimseyen yenilikçi bir teknolojidir. Merkezi veri tabanı mimarisinden farklı olarak kayıtları yönetme yeteneğine sahiptir. Blok zincirinde bilgiler, birbirine bağlı ve eşit boyutlara sahip bloklardan oluşan zincirimsi bir yapı içinde depolanmaktadır.

Bu sistemdeki düğüm ağı (bilgisayarlar), verileri belirli yöntemlerle paylaşmakta ve ağ üzerinde gerçekleştirilen tüm değişiklikler bu düğümler tarafından ortaklaşa tamamlanmaktadır. Teknolojinin en önemli özelliklerinden biri ise çeşitli kullanıcı gruplarına olanak tanımasıdır.Kullanıcılar arasında işlem yapılabilirken, aynı anda tek ve zamana karşı tutarlı bir "akıllı defter" (blok zinciri sisteminde verilerin şeffaf ve değiştirilemez şekilde kaydedildiği merkezi olmayandefter yapısı) üzerinden anlaşma sağlanmaktadır. Üstelik bunun için herhangi bir merkezî otoriteye ihtiyaç duyulmamaktadır. Ayrıca her yeni eklenen halka ile bütünlüğünü korumaktadır. Bu da onu güvenilir hale getirmektedir. Genellikle aracısızlaştırıcı özelliği sayesinde aracıların işlevini ortadan kaldırdığı düşünülmektedir (Christidisand, Devetsikiotis, 2016: 2296-2297).

Blok zinciri, merkezi olmayan defter teknolojisi olarak da bilinmektedir. Ancak, blok zinciri, bu teknolojinin daha özel bir durumudur. Merkezi olmayan defter teknolojisi, verilerin depolanmasına ve kaydedilmesine olanak tanıyan bir teknoloji türünü ifade ederken, blok zinciri bu teknolojinin bir çeşididir. Blok zinciri, zincir benzeri bir yapıda birbirine bağlı bloklar içermekte ve güvenlik için kriptografik anahtarlar kullanmaktadır. Blok zincirinin kayıtları, zincir benzeri bir yapıda saklanmaktadır. Her blok, bir önceki bloğun karmasını içeren bir blok başlığına sahiptir ve blok gövdesi ile saklanmaktadır. İşlemler, Merkle ağacı adı verilen özel bir yapıda kodlanarak saklanmaktadır (Zheng vd., 2017: 558). Temel olarak, bir sistemde gerçekleştirilen her işlem, kriptografik olarak şifrelenmiş parçalar halinde depolanmaktadır. Bir sonraki blok, önceki blok hakkında bilgi içererek zinciri oluşturmaktadır. Blok zincirindeki her blok, benzersiz bir hash (karma) olarak adlandırılan karma işlevini kullanmaktadır. İşlem verileri, bir önceki bloğun karma işlevini içermektedir. Bu, başlangıç bloğu olarak bilinmektedir (Puthalvd, 2018: 20). Bir alt blok, bir sonraki bloğu oluşturmak için kimlik doğrulaması gerektirmektedir.

Blok zinciri, işlemlerin yönetilmesinde protokoller ortaya çıkarak veri kaynağı, işlem, blok oluşturma, uzlaşma,bağlantı ve arayüz modülünden oluşmaktadır.

Blok zincirinin dağıtılmış ve paylaşılan veri tabanlarının oluşturulmasını sağlayan veri kaynağı modülü, bu sistemdeki verilerin blok zinciri kullanıcıları tarafından bozulmasını veya değiştirilmesini engellemektedir. Herhangi bir verinin transfer edilebilmesi için gerekli bilgilerin yer aldığı bir veri kaydının oluşturulması zorunludur ve işlem modülü, bu veri kayıtları üzerinde uzlaşma sağlayarak veri transferini gerçekleştirmektedir (Elbüz vd., 2023: 515).

İşlem modülü, blok zincirindeki tüm işlemleri izler ve her düğüme yeni bir blok eklenmesini sağlamaktadır. Bu bloklar, sistemin bütünlüğünü koruyarak zincirden geri alınamaz veya silinemez. Tüm işlemler, merkezi olmayan bir yapıya sahip dağıtık bir defterde kaydedilmektedir. Bu defter, blok zinciri ağına dahil olan tüm düğümler tarafından güncellenmekte ve doğrulanmaktadır, böylece verilerin güvenliği ve şeffaflığı sağlanmaktadır. Merkezi bir otoritenin bulunmadığı bu süreç, kullanıcıların işlemleri güvenli bir şekilde gerçekleştirmesine olanak tanımakta ve herhangi bir müdahale veya değişiklik yapılmasını engellemektedir.Böylece, zincirdeki tüm işlemlerin kopyalarının saklanması kolaylaşmaktadır. Ayrıca kullanıcılar çevrimdışı olsa bile tekil deftere erişebilmektedir. Blok zinciri ağında geçmişte yapılan tüm işlem kopyalarını barındırdığı için geriye dönük erişim mümkündür (Uysal, Kurt, 2018: 470).

Blok oluşturma modülü, gerçekleştirilen işlemlerin detaylarını ve bilgilerini içeren blokların özet değerlerini oluşturmakta ve bu blokları birbirine bağlayarak zincire yeni bir blok eklenmesini sağlamaktadır. Bu süreç, işlemlerin güvenli bir şekilde doğrulanması ve blok zincirinin bütünlüğünün korunması için kritik bir rol oynamaktadır. Özet değerleri sayesinde her blok, zincirdeki bir önceki blokla kriptografik olarak bağlantı kurmakta, bu da verilerin değiştirilemezliğini ve güvenliğini sağlamaktadır.Gerçekleştirilen işlemler bu bloklar içinde kaydedilirken kriptografik özetlerile tarihsel kayıtları içermektedir. Bir bloğun içerisindeki işlem kısmında ise kontrol başlığı, işlemlerin özet değeri ve zaman damgası bulunmaktadır (Yener, 2020: 12).

Uzlaşı modülü, her işlemin geçerliliğini doğrularken bloklar arasında bağlantı kurmaktadır. Bu modül, ağdaki tüm üyelerin blok zinciri kopyalarının kimliğini doğrulamasını sağlamaktadır. Blok zincirinde yapılan her değişiklik, tüm düğümlere iletilmekte ve düğümlerden gelen yanıtlar doğrultusunda ya onaylanmakta ya da reddedilmektedir. Bu süreç, blok zincirinin güvenliğini ve bütünlüğünü korumada kilit bir rol oynamaktadır. Birçok uzlaşı algoritması mevcuttur (Kösesoy, 2019: 6). En yaygın uzlaşıalgoritmaları arasında PoS (Proof of Stake), PoW (İş İspatı), DPoS (Yetkilendirilmiş Hisse İspatı) ve PBFT (Uygulamalı Bizans Hata Toleransı) yer alır (Mingxiaovd., 2017: 2568). Bu algoritmalar arasındaki temel fark, onaylanan işlemler için oy verme ve ödül alma yöntemleridir. Bitcoin gibi birçok kripto para birimi PoW kullanmaktadır. Kullanılacak uzlaşımodülü, blok zincirinin amacına göre seçilmektedir (Sikorskivd., 2017: 237).Örneğin, PoW algoritmasına dayalı madencilik işlemi yüksek enerji tüketimi ve uzun işlem süresi gerektirirken, PoS daha düşük maliyet ve enerji tüketimi sunmaktadır(Kösesoy, 2019: 6).

Bloklardaki işlemleri izleyerek akıllı sözleşmelere gerçek zamanlı veri sağlayan bağlantı ve arayüz modülü, blok zinciri platformları arasında güvenli ve verimli iletişim kurma ihtiyacından

doğmuştur (Dutta vd., 2020: 6). Bu modül, finans sektöründen tedarik zinciri yönetimine kadar birçok alanda önemli etkiler yaratmaktadır. Farklı blok zinciri ağları arasında kesintisiz iletişim ve iş birliği sağlaması, verimliliği artırarak maliyetleri düşürmekte ve güvenliği güçlendirmektedir. Ancak, bu modülün geliştirilmesiyle ilgili bazı zorluklar da bulunmaktadır. En büyük sorunlardan biri, farklı blok zinciri ağları arasında standart protokoller ve birlikte çalışabilirlik standartlarının eksikliğidir. Evrensel bir çerçeve olmadan, platformlar arasında sorunsuz iletişim sağlamak hala önemli bir zorluk olarak devam etmektedir. Blok Zincirleri Arası İletişim (IBC) protokolü gibi birlikte çalışabilirlik standartları oluşturma çabaları ise sürmektedir (Wang,Wu, 2021: 4;Essaid vd., 2023: 21).

3. BLOK ZİNCİRİNİN ÇALIŞMASI

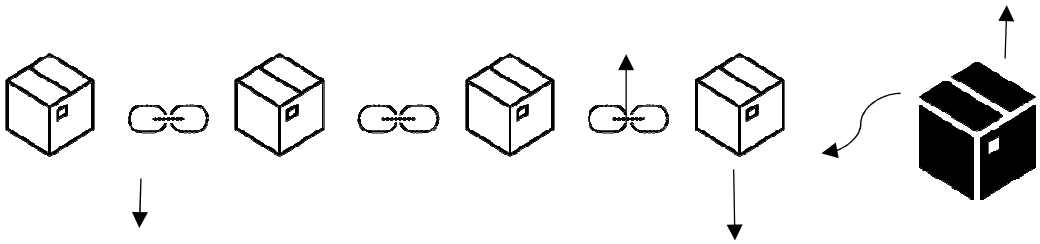
Blok zincirinin merkezi olmayan yapısı, verilerin merkezi bir sunucu yerine bir bilgisayar ağı üzerinde depolanmasına olanak tanıyarak, verilerin değiştirilmesine ve bilgisayar korsanlığına karşı dirençli hale gelmesini sağlamaktadır. İşlemler, karmaşık kriptografik algoritmalar kullanılarak doğrulanmakta ve doğrulanan her işlem, zincirdeki bir bloğa eklenmektedir. PoW veya (PoS) gibi mutabakat mekanizmaları, ağ katılımcıları arasında işlemlerin geçerliliği konusunda uzlaşma sağlamaktadır (Saad, Radzi, 2020: 27). Bir blok zincirinin süreci dört adımda açıklanabilir.

Bir kullanıcı, işlemlerini imzaladıktan sonra komşu düğümlere iletmektedir. Kullanıcılar, ağ ile etkileşim kurmak için ayrı bir özel/genel anahtar çifti kullanmaktadır. Kullanıcının benzersiz özel anahtarı, işlemi imzalamak için kullanılmaktadır. Diğer tüm düğümler, imzayı doğrulamak amacıyla genel anahtara erişebilmektedir. Bu imzalanmış işlem, ağdaki en yakın düğümlere gönderilmektedir. Komşu düğümler, bu işlemi genel anahtarı kullanarak doğrulamaktadır. İşlem tüm ağa yayılmaktadır. Madencilik işlemiyle bir blok oluşturulmaktadır. Gerçekleştirilen işlemler, zamana göre belirli bir sırayla blokta toplanmaktadır. Bu süreç madencilik olarak adlandırılmaktadır. Algoritma, işlemleri sıralamakta ve bloğun içine kilitlemektedir. Bloğun doğrulanma süreci tamamlanmaktadır. Bloğun ve bir önceki bloktaki referansın yer aldığı zincir kontrol edilmektedir. Eğer bloklar arasındaki ağ anahtarı doğruysa, ağ bloğu zincire eklemektedir. Aksi takdirde, blok reddedilmektedir.

Dört aşamanın sonucunda kimliği doğrulanmış zaman damgalı bir kayıt oluşur. Merkezi bir otoriteye ihtiyaç duymayan ağ ile güvenli bir zincir oluşmaktadır (Christidis, Devetsikiotis, 2016: 2293).

Laurance (2017: 12) blok zincirinin, kriptografik olarak birbirine bağlı bir dizi işlem içeren bloklardan oluştuğunu açıklamaktadır. Bloklar, zincirler ve ağ; her blok zincirin üç temel bileşenini oluşturmaktadır. Belirli bir zaman dilimindeki tüm defter kayıtları "blok" adı verilen bölümlerde toplanmaktadır. Zincirler ise bu oluşturulan blokların birbirine kriptografik olarak bağlanmasını ifade etmektedir. Her bloğun kopyası alınarak ağa gönderilir ve böylece verilerin doğruluğu sağlanmış olmaktadır. Yeni üretilen tüm bloklar, kronolojik sırayla zaman damgalarıyla birbirine bağlanır ve bu yapıya 'blok zinciri' denir. Bir blok zincirin yapısı Şekil 1'de gösterildiği gibidir.

Şekil 1: Blok Zincirinin Yapısı



Kaynak: Hadi vd., 2019: 4050.

Şekil 1'e göre, ağdaki bir kullanıcı bir işlem yaptığında öncelikle bu işlemin protokol kurallarına uygun olup olmadığı belirlenmelidir. Eğer işlem kabul edilirse, yeni bir blok oluşturulmakta ve işleme alınmaktadır. Hesaplama gücü kullanılarak yapılan işlemler tek bir blokta toplanıp şifrelenmektedir.Yeni blok ise tüm işlemler tamamlandıktan ve zaman damgası eklendikten sonra zincirin sonuna eklenmektedir (Reynavd., 2018: 174).

4. BLOK ZİNCİRİNİN BİLEŞENLERİ

Blok zincirinin bileşenleri genel olarak merkezi olmayan defter teknolojisi, kriptografi ve kriptoloji, özetleme fonksiyonu, Merkle ağacı ve asimetrik şifrelemedir.

4.1. Merkezi Olmayan Defter Teknolojisi

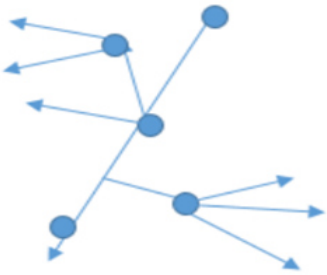
Sisteme dahil olan tüm kullanıcıların aynı verilere dahil olarak bu kayıtları bilgisayar sunucuları aracılığıyla saklamaları şeklinde tanımlanabilmektedir. Merkezi olmayan defter teknolojisinin diğer kayıtlardan en belirgin farkı ağ yapılarıdır. Günümüzde üç tür ağ yapısı bulunmaktadır. Bu ağ yapıları verilerin saklanmasına göre farklılık göstermektedir. Mevcut ağ yapıları Şekil 2, 3 ve 4'teki gibi özetlenebilir.

Şekil 2: Tek Merkezli Ağ Yapısı

Kaynak: Duman, 2023:196.

Tek merkezli ağ yapısındaki tüm veriler merkezi bir tabanda kaydedilerek işlem gerçekleşmektedir. Veriye erişebilmek için merkezi nokta ile bağlantı kurularak işlem yapılmaktadır. Merkezi sistemlerde, veriler tek bir merkezde saklanır ve bu merkezin bilgiyi değiştirme veya silme yetkisi vardır. Bu tür tek merkezli yapılar, sadece bir kontrol merkezi olduğu için kolayca yönetilip denetlenebilir. Ancak merkezde meydana gelen herhangi bir sorun tüm sistemi etkileyebilir (Montresor, 2008: 111-113).

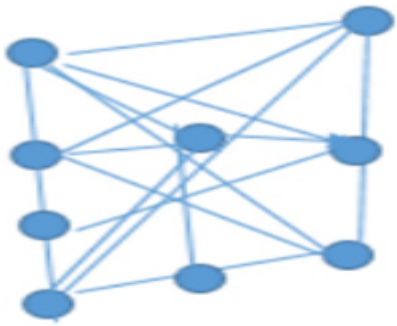
Şekil 3: Çok Merkezli Ağ Yapısı



Kaynak: Duman, 2023:196.

Çok merkezli ağ yapısı, birden fazla merkezi sunucunun bulunduğu bir tür ağdır. Bu ağlarda, sunucular genellikle farklı konumlara yerleştirilmekte ve bu sunucular arasında belirli düzeyde veri alışverişi yapılabilmektedir (Tüfenk, 2023: 35).Çok merkezli veri tabanında, veriler önceden belirlenen veri merkezlerine kaydedilerek işlem yapılmaktadır. Veri merkezleri arasında uyum sağlanarak veri güvenliği temin edilmeye çalışılmaktadır.

Şekil 4: Merkezi Olmayan Ağ Yapısı



Kaynak: Duman, 2023:196.

Merkezi olmayan defter teknolojisi, blok zinciri teknolojisinin gelişimiyle birlikte ortaya çıkmıştır. Blok zinciri, ağda depolanan verilerin doğruluğunu sağlamak için kriptografiden yararlanırken; merkezi olmayan defter teknolojisi ise bu doğruluğu korumak amacıyla dağıtılmış veri tabanı sistemlerinden faydalanır. Bu teknoloji, işlem maliyetlerini düşürmekle kalmaz aynı zamanda işlemlerin hızını artırmakta ve güvenlik seviyesini yükseltmektedir (Tapscott, Tabscott, 2016). Merkezi olmayan yapıyı hiçbir kurum veya birey tarafından kontrol edemez. Bu özellik, verilerin daha güvenli ve şeffaf biçimde saklanmasını mümkün kılmaktadır. Blok zinciri teknolojisiyle birlikte verilerin tüm düğümler arasında güncellenmesini, doğrulanmasını ve onaylanmasını kolaylaştırmaktadır (Narayanan,Clark, 2017: 40). Ayrıca blok zinciri anonimlik sağlamaktadır. Hiç kimse gerçek bilgileri ile işlem yapmamaktadır. Bunun yerine sistemin oluşturduğu sayısal kimlikler kullanılmaktadır.Merkezi olmayan sistem sayesinde ise herhangi bir veri hatasında sistemin tamamen çökmesi gibi sorunlar önlenmektedir (Elbüz vd., 2023: 511).

Merkezi olmayan defter teknolojisinin potansiyel avantajları arasında işlem maliyetlerini düşürmesi, işlemlerin hızını artırması, veri güvenliğini ve şeffaflığı yükseltmesi ile veri sahipliği sorunlarını çözmesi yer almaktadır. Kripto para birimleri ve ödeme sistemleri, akıllı sözleşmeler, dijital kimlikler, tedarik zinciri yönetimi gibi çeşitli alanlarda; ayrıca enerji sektörü, sağlık hizmetleri sektörü gayrimenkul piyasası, oy kullanma sistemleri ve sigorta endüstrisi de dahil olmak üzere birçok kullanım olanağı bulunmaktadır (Blossey vd., 2019: 6891). Ancak kara para aklama ve terörizmin finansmanı gibi yasadışı faaliyetlerle ilişkilendirildiği için eleştirilere maruz kalmıştır. Bazı blok zinciri ağlarında yapılan işlemler takma adlarla gerçekleştirilebildiğinden bu teknolojinin yasa dışı amaçlar doğrultusunda kötüye kullanılabilme ihtimali konusunda kaygılar oluşmuştur. Bu zorlukların üstesinden gelebilmek adına hükümetler teknoloji geliştiricileri ve ilgili paydaşlar arasında düzenleyici çerçevelerin oluşturulması iş birliği sağlanarak çözümler sağlanmaktadır (Scholl, Bolivar, 2019 : 604).

4.2. Kriptografi ve Kriptoloji

Kriptografi, şifreli bir metni orijinal haline dönüştürme yöntemidir. Kriptoloji ise iletişimde veri güvenliğini sağlayan kripto cihazlarının algoritmik emniyetini inceleyen ve matematik temelli

bilgisayar mühendisliği ile fizik ve istatistik gibi alanları içine alan disiplinler arası bir bilim dalıdır (Akleylek vd., 2011: 713). Kriptografinin amacı, bilginin sadece belirlenen kullanıcı tarafından erişilebilmesini sağlamaktır. Bilgi şifrelendikten sonra anlamsız hale gelen sayısal verilere dönüştürmektir. Tarih boyunca birçok uygarlık tarafında kullanılan kriptografinin basit biçimleri Roma döneminde görülmeye başlanmıştır. Julius Caesar'ın mektuplarını harf kaydırma tekniği kullanarak gizlemesi buna örnek olarak verilebilmektedir. Günümüz modern kriptografisi oldukça karmaşık olsa da kökenleri bu eski uygulamalara dayanmaktadır (Atabaş, 2018: 20-21).

Blok zinciri teknolojisinde kullanıcı isimleri sisteme dahil edilmemektedir. Hesaba ait tanımlanan adresler, yani kriptografik adreslere karşılık gelen ve yalnızca kullanıcıya ait olan özel bir anahtar bulunmaktadır. Herhangi bir transfer sırasında kullanıcının karşı tarafa bu adresi göndermesi yeterlidir. Fakat geliştirilecek bir iletişim aracı ile veri tabanında hangi adresin hangi kişiye ait olduğunun tespit edilmesi mümkündür. Önemli olan nasıl bir sistem tasarlanmak istendiği ile ilgilidir. Bu sistemler herkese açık olabileceği gibi özel anahtarlar aracılığıyla girilen, üyelik oluşturularak kullanıcı bilgilerinin saklandığı bir sistem de olabilmektedir(Ber, 2022: 8). Kriptografi ile ilgili yapılan işlemler bir algoritma tarafından eşler arası (P2P) tarafından yönetilen bir ağa dayandığından, verilerin içeriklerinin yasa dışı olup olmadığını belirlemek son derece güçtür. Devletlerin bu konuda yapılan işlemlere ilişkin tüm şüpheli işlem raporlarını talep edeceği bir kurum bulunmamaktadır. Blok zinciri ağı üzerinden yapılan işlemlere ilişkin hizmet sağlayıcıların şüpheli işlemleri adli ve idari makamlara bildirmesi durumunda tespiti mümkündür. Dolayısıyla sorumluluklarını yerine getirmeyen hizmet sağlayıcılarına ilişkin faaliyet izni verilmesi önemli bir nokta olarak görülmektedir (Balcı ve Çakır, 2021: 45-46).

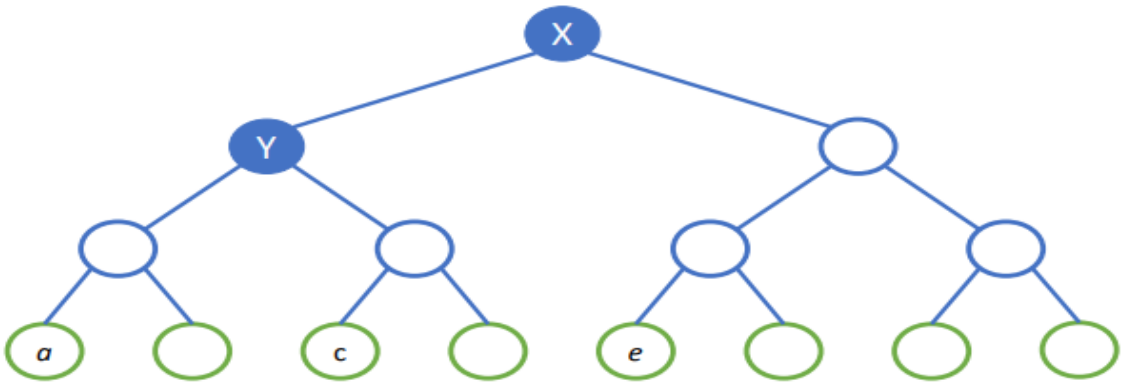
4.3. Özetleme Fonksiyonu

Özetleme fonksiyonları, matematiksel algoritmaları kullanarak blok verilerini sıkıştırmakta ve bu öze dönüştürülmüş biçimde bir araya getirmektedir. Bu süreç sayesinde her bloğun kendisinden önceki bloğun özetiyle ilişkili olduğu blok zinciri sistemi içerisinde birleşik temsil sağlanmaktadır. Böylelikle herhangi bir blok üzerinde değişiklik yapıldığında tüm zinciri etkileyen durumlar meydana gelmektedir. Çünkü diğer blokların özetleri de buna bağlı olarak değişime uğramaktadır. Özetleme fonksiyonları, özellikle hem müdahale girişimlerine karşı koruma sağlamakta hem de doğruluklarının güvencesini sunmaktadır. Dolayısıyla modifikasyon veya veri değiştirme çabalarına direnmektedir. Blok zinciri teknolojisi kullanıldığında, herhangi bir blokta yapılan en küçük bilgi güncellemesi tüm sisteme yansımaktadır. Bu durum da blok özetlerinin güvenilirliğini artırarak oldukça önemli hale getirmektedir (Nadia vd., 2018: 2).Özetleme fonksiyonu, tüm veri setini girdi olarak alır ve belirli işlemlerden sonra sabit bir hane sayısına sahip bir çıktı oluşturmaktadır. Girdideki herhangi bir değişiklik, çıktıda farklı bir değere yol açmaktadır. Aynı verinin özeti her seferinde aynıdır. Bu fonksiyon sayesinde verinin sürekliliği ve doğrulaması sağlanmış olmaktadır (Tüfekci, Karahan, 2019: 163).

4.4. Merkle Ağacı

Merkle ağacı veya Merkle kökü olarak bilinen bu bileşenin amacı, büyük verileri kümelendirerek hızlı ve güvenli doğrulama sağlamaktır. Bir blok zincirinde birçok veri bloğu bulunmaktadır. Bu blokların özet bilgilerinin bir araya getirilip paketlenmesiyle tek bir özet oluşmakta ve bunaMerkle ağacı denir (Drescher, 2017: 124-126). Şekil 5'te kısaca bir Merkle ağacının örneği gösterilmektedir.

Şekil 5: Merkle Ağacı Yapısı



Kaynak: Wallez vd., 2022: 1219.

Merkle ağacı, ters çevrilmiş bir ağaç şeklinde olup "yaprak düğümleri" olarak adlandırılan altta yer alan katmanları işlem sonunda oluşan karma değerlerini ifade etmektedir. Bu karma değerler Merkleağacının dallarını oluşturmakta ve en yüksek karma değer ise "Merkle kökü" olarak adlandırılmaktadır. Merkle ağacı, blok zinciri teknolojisindeki şifreleme süreçlerinin güvenliğini sağlamaktadır (Yakupoğlu, 2016: 4).

Blok zinciri teknolojisinde bir verinin orijinal konumdan gelip gelmediğin doğrulanması için dijital imzalar kullanılmaktadır. İşlemler, dijital imzalar doğrulandıktan sonra başlatılmaktadır. Bir dijital imzanın doğrulama süreci ve imzalama süreci olmak üzere iki aşaması bulunmaktadır. Gönderici, bir işlemi imzalamak isterse, öncesinde gönderdiği işleme ilişkin özet bir değer türetilmektedir. Bu karma değeri, özel bir anahtar kullanılarak şifrelenir ve orijinal veri ile alıcı tarafa dahil edilmektedir. Alıcı taraf ise şifrelenmiş karma değeri alınan verilerden elde edilen karma değeri ile karşılaştırarak işlemin gerçekliği kontrol edilmektedir(Efe, 2021: 98).

Merkle Ağaçları, büyük veri kümelerinin verimli bir şekilde doğrulanmasını sağlamaları nedeniyle önemli avantajlar sunmaktadır. Çok miktarda bilgiyi tek bir karma değerinde toplayarak veri bütünlüğünün hızlıca teyit edilmesine olanak tanımaktadır. Bu yetenekleri, blok zincirlerinin vazgeçilmez parçalarından biri haline gelmelerine katkıda bulunmuştur. İşlemlerin etkili biçimde doğrulanmasına ve kayıt altındaki verilerin değiştirilemezliğine destek olmuştur. Ayrıca Merkle Ağaçları, dağıtık sistemlerin etkin senkronizasyonunu kolaylaştırmaktadır.

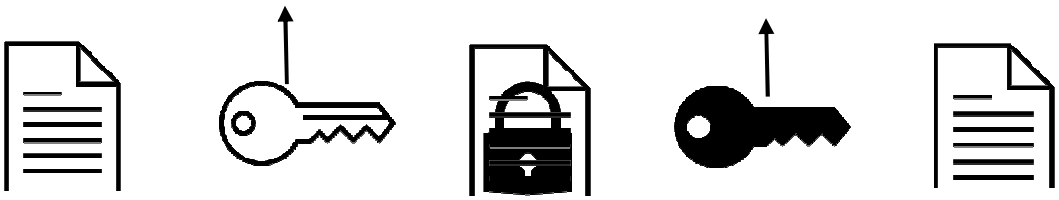
Birden fazla tarafın aynı veri kümesinin farklı kısımlarını barındırdığı durumlarda tutarsızlıkların tespitini sağlamakta ve bu sayede dağıtılmış kopyaların güncellenmesi ile uzlaşılma sürecini hızlandırmaktadır. Özellikle eşler arası (kullanıcıların doğrudan birbirine bağlandığı)ağlar ve merkezi olmayan yapılarda bu özellik oldukça değerlidir (Bosamina, Patel, 2018: 295).

4.5. Asimetrik Şifreleme

Asimetrik şifreleme, simetrik olmayan algoritmalar kullanılarak yapılan bir şifreleme ve çözme sürecidir (Yerlikaya vd., 2006: 3). Bu süreçte taraflar iki farklı anahtar kullanılmaktadır.

Anahtarlardan biri diğerinden tamamen farklıdır. Şifrenin çözülebilmesi için bu iki anahtarın birlikte kullanılmasına ihtiyaç vardır. Açık anahtar, şifrenin oluşturulmasında kullanılan ve herkesle paylaşılabilen anonim bir unsur olarak tanımlanmaktadır. Özel anahtar ise yalnızca sahibine ait olup gizli tutulan ve şifreyi çözme işlevi gören unsurdur. Özelden elde edilen bir açık kendi başına sorun yaratmamakta, ancak özel bilgiyle birleştiğinde veri çözümüne yol açabilmektedir(Şat, 2019: 124). Blok zinciri teknolojisinde işlemler dijital imza ile onaylanarak özel olarak tamamlanmaktadır. Ardından da halka açık olan doğrular sayesinde bilgilerin kaynağını ve değişime uğramadığını garanti edecek şekilde kontrol edilmektedir (Tapscott, Tapscott, 2016). Sonrasında bloklara eklenen içerikler işlem teyidi almaktadır.Asimetrik şifreleme çalışma sistemi Şekil 6'teki gibidir.

Şekil 6: Asimetrik Şifreleme



Kaynak: Maqsoodvd., 2017: 443.

Simetrik şifreleme işleminde, hem veriyi şifrelemek hem de çözmek için tek bir gizli anahtar kullanılmaktadır. Bu yöntem, matematiksel olarak daha az karmaşık olup yaygın şekilde tercih edilmektedir. Simetrik şifrelemede işlemin tamamlanmasının ardından gizli anahtarın alıcıya gönderilmesi gerekir ki böylece hızlıca çözülmektedir (Kodaz,Botsalı, 2010:12). Asimetrik şifrelemeye bakıldığında ise Şekil 4'te görüldüğü üzere açık ve kapalı olmak üzere iki farklı anahtarla simetriğe göre farklı bir sistemde çalışmaktadır. Asimetrik yöntemin en belirgin özelliği verinin üçüncü taraflarla paylaşılabilmesidir. Burada ya kapalı anahtara başvurulur ya da veri matematiksel yollarla çözülmektedir. Tablo 1'de her iki yöntemin özellikleri özetlenmiştir.

Tablo 1: Simetrik ve Asimetrik Şifreleme Özellikleri

Özellik	Asimetrik Şifreleme	Simetrik Şifreleme
Gizlilik	Sağlanır	Sağlanır
Bütünlük	Sağlanır	-
Kimlik Doğrulama	Sağlanır	-
İnkar Edilemezlik	Sağlanır	-
Performans	Yavaş	Hızlı
Güvenlik	Anahtar Uzunluğu Etkilidir	Anahtar Uzunluğu Etkilidir

Kaynak: Kodaz, Botsalı, 2010: 20.

Tablo 1'e dayanarak, her iki şifreleme yöntemi de gizlilik sağlamaktadır ve güvenlik düzeyleri anahtar uzunluğuna göre değişiklik göstermektedir. Ancak asimetrik şifreleme, simetrik şifrelemeye kıyasla bütünlük, kimlik doğrulama ve inkar edilemezlik gibi özellikler sunmaktadır. Buna karşılık, simetrik şifrelemenin performansı daha hızlıdır.

Günümüzde, bir verinin güvenli bir şekilde saklanması, iletilmesi ve kullanılması kadar hızlı ve etkili biçimde gerçekleştirilmesi de büyük önem taşımaktadır. Bu tür durumlarda simetrik ve asimetrik sistemlerin birleşimiyle oluşan hibrit sistemlerden faydalanılır. Hibrit sistemlerin avantajları ve dezavantajları değerlendirildiğinde; dijital imza veya anahtarsız şifreleme gibi işlemler genellikle asimetrik sistemlerle yapılırken, yüksek hacimli verilerin işlenmesinde ise simetrik sistemler kullanılmaktadır (Şahin, 2015: 30).

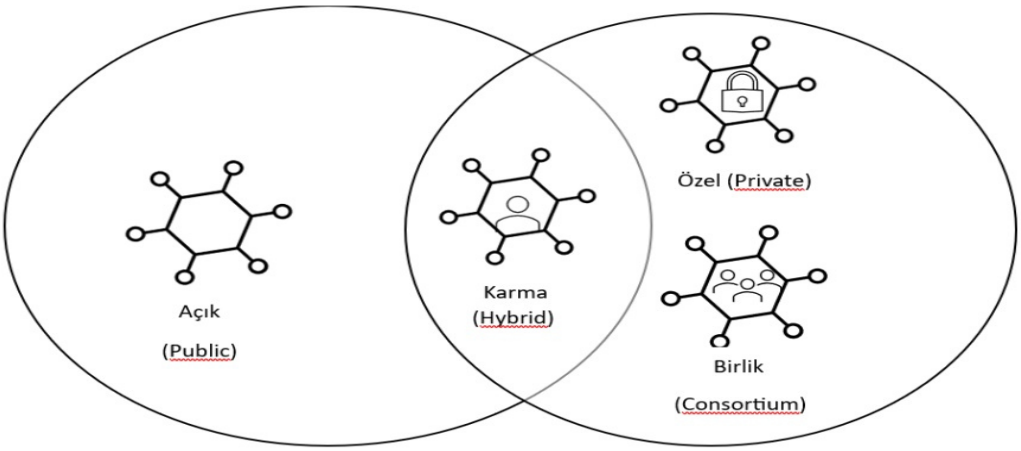
5. BLOK ZİNCİRİ TÜRLERİ

Blok zinciri, veri güvenliği ve şeffaflık sağlamak için merkeziyetsiz bir yapı sunan bir teknoloji olarak, çeşitli kullanım alanlarına ve gereksinimlere göre farklı türlerde geliştirilmektedir.

Her bir tür, belirli bir amaca hizmet ederek işlem hızları, güvenlik seviyeleri ve erişim kontrolü gibi önemli özellikler açısından farklılık göstermektedir.

Yapısı ve çalışma şekline göre blok zinciri türleri dört grupta sınıflandırılmaktadır. Blok zinciri türleri Şekil 7'teki gibidir.

Şekil 7: Blok Zinciri Türleri



Kaynak: Wegrzyn ve Wang, 2021.

5.1. Açık (Public) Blok Zinciri

Açık blok zinciri türünde, herkes bilgilere erişilip işlemler gerçekleştirilmektedir. Açık blok zincirleri, herhangi bir kişinin kayıtları okuyabildiği ve işlem gönderebildiği sistemlerdir. Ayrıca, katılımcılar mutabakat sürecine dahil olarak hangi blokların ve işlemlerin deftere (veri kayıtlarının tutulduğu merkeziyetsiz sistem) eklenip ekleneceğine karar verilmektedir.

Açık blok zinciri türünde herkes bilgilere erişebilmekte ve işlem yapabilmektedir. Açık blok zincirleri, herhangi bir kişinin kayıtları okuyabildiği, işlem gönderebildiği blok zincirleridir. Herhangi bir katılımcı, blokların ve işlemlerin deftere eklenip eklenmeyeceğini belirlemek için mutabakat sürecine katılabilmektedir. Açık blok zincirler, herkese açık olan ve merkezi olmayan sistemlere ihtiyaç duyan uygulamalar için uygundur. Bitcoin ve Ethereum bu tür blok zincirinin iyi bilinen örnekleri arasındadır (Zheng vd., 2018: 357).

5.2. Özel Blok Zinciri

Özel blok zinciri, yalnızca belirli bir kuruluş veya kullanıcı grubuna erişim imkanı tanıyan ve özel bir şifreyle girilebilen bir türdür. Bu tipteki blok zincirleri genellikle belli izin seviyelerine ihtiyaç duyan kullanıcılara hitap etmekte ve sınırlı erişim sağlamaktadır. Açık blok zincirlere kıyasla daha merkeziyetçi ve kontrollü yapılardır (Yang vd., 2020: 2).

Özel blok zincirleri, daha küçük ağ boyutları ve daha az uzlaşma protokolü gereksinimi nedeniyle ölçeklenebilirlik açısından avantaj sunmaktadır. Bu özellikler sayesinde, özel blok zincirleri yüksek işlem hacmine ulaşabilmekte ve işlemler hızla tamamlanmaktadır. Ayrıca erişimin belirli bir katılımcı grubuyla sınırlanması yoluyla gizlilik artmaktadır. Bu durum da hassas bilgilerin işlendiği sektörlerde cazip hale gelmektedir. Ancak özel blok zincirlerinin farklı platformlar veya standartlarla uyumsuzluğu diğer özel ya da açık blok zinciri sistemlerine

entegrasyon konusunda zorluk yaratabilmektedir (Yang vd., 2020: 2). Böyle durumlarda, amaçlara yönelik olarak birlik (konsorsiyum) blok zinciri teknolojisi tercih edilebilmektedir.

5.3. Birlik Blok Zinciri

Birlikblok zinciri, çeşitli işlem alanlarında süreçleri doğrulamak, iş birliği yapmak ve ortak hareket etmek amacıyla oluşturulan bir blok zinciri ağı türüdür (Yagavd., 2018: 34). Bu tip bir ağın hedefi, katılımcıların güvenli ve güvenilir bir ortamda etkileşimde bulunmalarını ve işlemler gerçekleştirmelerini sağlamaktır. Birlik blok zincirinde yer alan düğüm sayısı ise yalnızca birliğe üye olan kişilerle sınırlıdır (Wang, Zhang, 2021: 2976).

Birlik blok zincirleri, birden fazla paydaş arasında iş birliğine ihtiyaç duyan çeşitli sektörler üzerinde önemli etkiler yaratmaktadır. Bu tür blok zinciri sayesinde tüm taraflar, işlemleri güvenilir ve şeffaf şekilde takip edebilmekte, orijinalliği doğrulanabilmekte ve düzenlemelere uyumu garanti altına alabilmektedir. Böylelikle verimsizliklerin azaltılması sağlanırken dolandırıcılığın önüne geçilebilmektedir (Dibvd., 2018: 51).

5.4. Karma Blok Zinciri

Karma blok zinciri, izinli ve izinsiz blok zincirlerinin avantajlarını bir araya getiren yenilikçi bir çözüm sunmaktadır. Hem açık hem de özel blok zincirlerin faydalarını bütünleştirmek üzere tasarlanmıştır. Karma yapıları sayesinde bazı verilerin genel olarak paylaşılmasına izin verirken, diğerlerini gizli tutarak yalnızca yetkili kişilere açmaktadır. Bu sayede belirli kişiler için işlem sınırları koyarak güvenilir bir platform sağlamaktadır (Vurdu, 2021: 927-928). Ayrıca ihtiyaç duyulduğunda karma blok zincirlerine yeni katılımcılar eklenebilmektedir. Bu esneklik ağı genişletme imkanı tanımakta ve kullanım alanını artırmaktadır.

6.BLOK ZİNCİRİNİN ÖZELLİKLERİ

Bir blok zincirinin çeşitli özellikleri vardır. Bu özellikler arasında güvenlik, gizlilik, ademi merkeziyetçilik, kalıcılık, uçtan uca iletişim ve aracısızlaştırma olarak sıralanmaktadır.

6.1. Güvenlik

Blok zinciri, mevcut verileri sonradan değiştirilemeyecek biçimde kaydederek güvenli bir teknoloji haline gelmiştir. Gerçekleşen işlemlerin ağ tarafından doğrulanması, sistem bütünlüğünü sağlamakta ve koruma altına almaktadır. Bu sayede güvenlik temin edilmektedir. Blok zinciri dışındaki altyapılarda ise tüm kişisel verileri toplayabilecek üçüncü bir tarafından kontrolü söz konusudur. Ancak blok zinciri, bu aracı kaldırarak doğrudan aktarımı mümkün kılarak güveli bir paylaşım ortamı yaratmaktadır. Dijital ortamlardaki veri miktarının sürekli artışı kullanıcılar arasında çeşitli güvenlik endişelerine neden olmaktadır. Örneğin, Facebook gibi büyük sosyal ağlardan biri 300 petabayt kişisel veriyi topladıktan sonra bunu üçüncü taraflarla paylaşıp ciddi anlamda güven sorunları oluşturmuştur (Stephen, Alex, 2018: 5). Böylece kullanıcıların kişisel verileri kötü amaçlı kullanıma açık hale gelmiştir ki bu durum da blok zincirini daha da önemli kılmıştır.

Blok zinciri güvenliği, mevcut sınırlamaları ele almayı ve blok zinciri sistemlerinin genel güvenliğini iyileştirmeyi amaçlayan devam eden araştırma ve geliştirmelerle gelişen bir alandır. Gizlilik özelliği de blok zinciri teknolojisinde güvenliğin artırılmasında önemli bir rol oynamaktadır.

6.2. Gizlilik ve Şeffaflık

Bir blok zinciri, işlemleri güvence altına almak ve bilgilere erişimi kontrol etmek için kriptografik yöntemler kullanmaktadır. Güvenli ve gizli işlem imkanları sağlamak adına açık anahtarlar ile özel anahtarlar blok zincirde yer alırken, katılımcıların kimlikleri genellikle gizlenmektedir. Bazı durumlarda ise, blok zinciri ağlarına yalnızca belirlenen grupların ulaşabileceği şekilde izin kısıtlamaları getirmektedir. Bu da ağa dahil olabilecek kişileri ve veriye erişebilecek olanları sınırlandırarak mahremiyeti artırmaktadır. Bazı blok zinciri platformlarında, ek bir mahremiyet seviyesi sağlamak amacıyla gizlilik odaklı teknolojiler veya sıfır bilgi ispatları kullanılmaktadır (Zhang vd., 2019: 12-14). Katılımcılar bu tekniklerle spesifik detaylara girmeden işleme dair geçerliliği doğrulama imkânı bulmaktadır. Blok zincirin sunduğu mahremiyetle şeffaflığın etkisi oldukça geniş kapsamlıdır. Bir yandan bireylerin kişisel bilgilerini koruyabilmeleri, kullanıcı güvenini artırmakta ve veri ihlallerine karşı önemli bir avantaj sağlamaktadır. Bu durum, günümüz dijital dünyasında endişelerin büyük olduğu göz önüne alındığında oldukça değerlidir. Söz konusu protokoller sayesinde örneğin sıfır bilgi kanıtlarının yardımıyla kişiler sadece gerekli görüldüğünde bilgilerinin paylaşılmasına onay vermektedir. Böylelikle dolandırıcılık risklerini asgariye indirmektedir (Halpin, Piekarska, 2017:2). Gizlilik öncelikli kripto paralar aracılığıyla finansal hizmetlerden yararlanmanın yanı sıra para transferleri gerçekleştirip merkezi otoritelere bağımlılık olmaksızın ticaret yapılması mümkün hale gelmektedir.

6.3. Ademi Merkeziyetçilik

Blok zincirlerinin temel özelliklerinden biri olan güvenlik ve gizliliğin yanı sıra, bu sistemin merkeziyetsiz yapısı da ön plandadır. Blok zincirleri bilgileri tek bir merkezde toplamak yerine, ağdaki tüm düğümlere dağıtmaktadır. Bilgilerin tüm düğümlerde bulunması nedeniyle hiçbir otorite ağı kontrol edememekte veya veriyi değiştirememektedir. Bu sebeple daha güvenli bir ağ oluşturulmaktadır (Yiannas, 2018: 48).

Merkezi otoriteye güvenin olmadığı ve denetimin politik etkenlerden bağımsız tutulması gereken durumlarda, ademi merkeziyetçilik önemli hale gelmektedir. Blok zinciri ise yapısı gereği bilgileri merkezi bir alanda depolamamakta, dolayısıyla herhangi bir otoritenin müdahalesine açık değildir (Eroğlu, 2023: 188).

6.4. Kalıcılık ve Geri Döndürülemezlik

Blok zinciri teknolojisinin önemli bir özelliği, depoladığı verilerin kalıcılığını ve değiştirilemezliğini sağlamasıdır. Blok zinciri teknolojisinin dayanıklılığı ve güvenilirliğini sağlayan temel özellikler arasında kalıcılık ve geri döndürülemezlik bulunmaktadır. Kalıcılık, bir işlemin blok zincirine kaydedildikten sonra değiştirilemeyeceği veya silinemeyeceği anlamına gelmektedir. Bu durum, kriptografik karma fonksiyonlarının kullanılmasıyla birlikte

blokların ardışık ve sabit bir yapıda birbirine bağlanması sayesinde sağlanmaktadır. Geridöndürülemezlik ise, bir işlem onaylandıktan sonra onu iptal etmenin neredeyse imkansız hale geldiğini ifade etmektedir. Bu da işleme olanak tanımamaktadır. Güvenin, güvenliğin ve şeffaflığın kritik önem taşıdığı çeşitli endüstri kollarında geniş çapta etkileri vardır (Aggarwall, Kumar, 2021: 173-176).

Ağ üzerindeki her işlemin ağ boyunca dağıtılmış bloklar şeklinde doğrulanması ve kaydedilmesi gerektiği için gerçekleşen işlemlerde değişiklik yapılması oldukça zordur. Ayrıca, tamamlanan her blok diğer düğümler tarafından doğrulandığı için bu işlemlerin incelenebilmesi mümkündür. Bu sayede herhangi bir değişiklik kolayca tespit edilebilmektedir (Zheng vd., 2018: 357).

6.5. Uçtan Uca İletişim

Uçtan uca iletişim, blok zincirinin bir özelliği olarak aracıya ihtiyaç duymadan iki ya da daha fazla taraf arasında doğrudan ve güvenli bilgi alışverişini ifade etmektedir. Örneğin finans sektöründe Bitcoin ve diğer kripto para birimleri, dijital varlıkların aracı bankalar olmaksızın direkt transfer edilmesini sağlamaktadır. Geleneksel bir iletişim sisteminde ise katılımcılar arasındaki etkileşimi yöneten ve kolaylaştıran aracılar veya merkezi platformlar bulunmaktadır. Bu platformlar taraflar arasında güvenilir işlemlerin gerçekleştirilmesi için gerekli altyapıyı sağlamaktadır. Blok zincirinde ise merkezi bir platform bulunmayıp uçtan uca iletişim sağlamaktadır (Kfouryvd., 2019: 110162).

7. BLOK ZİNCİRİ TEKNOLOJİSİNİN KULLANIM ALANLARI

Güvenli, şeffaf ve verimli sistemler oluşturabilme potansiyeline sahip blok zinciri teknolojisi son yıllarda çeşitli sektörlerde yaygın olarak kullanılmaktadır. Kripto paralar başta olmak üzere bankacılık, sigortacılık, lojistik, tedarik zinciri yönetimi gibi alanların yanı sıra medya, eğlence sektörü, oyun dünyası ile eğitim ve sağlık hizmetlerinde de kullanım imkânı bulmuştur.

7.1. Kripto Paralar

Kripto paralar, fiziksel bir varlığı olmayan ve herhangi bir merkez bankasının kontrolü altında bulunmayan dijital yapılardır. Taraflar arasında hızlı, güvenli ve düşük maliyetli transfer imkanları sunan sanal para niteliğindedir (Şahin, 2018: 899-900).Kripto para birimleri, mevcut finansal sistemin tersine belirlenmiş zaman dilimlerinde daha az üretilmek üzere tasarlanmış olup, bu yaklaşımın amacı piyasa değerini oluşturmak ve belirli fiyat seviyelerinde istikrar sağlamaktır (Kesebir, Günceler, 2019: 611).

Kripto paraların yasal durumu ülkeden ülkeye farklılık göstermektedir. Birçok ülke kripto paralara resmi bir statü tanımazken, bazıları bu varlıkları kontrol altına almak için hukuki düzenlemeler yapmıştır. Örneğin; Arjantin, Paraguay ve Uruguay ile Lüksemburg ve Malta gibi ülkelerde Bitcoin ve diğer kripto para birimlerinin kullanımına yasal olarak izin verilmektedir (Lubis, Pratama, 2023:33). El Salvador ise 2021 yılında Bitcoin'i resmi para birimi olarak kabul eden ilk ülke olmuştur (Bibi, 2023:2).

Kripto para birimlerinin ve blok zinciri teknolojisinin sağladığı birçok avantaj bulunmaktadır. İlk olarak, maliyetlerin düşmesi ve işlem sürelerinin kısalması önemli bir kazanım olarak öne

çıkmaktadır. Geleneksel finans sistemlerinde gerçekleştirilen işlemler, çeşitli aracılara bağlı olduğu için genellikle yüksek maliyetlere ve uzun bekleme sürelerine yol açmaktadır. Ancak, kripto para birimleri aracılığıyla gerçekleştirilen işlemler, merkeziyetsiz yapıları sayesinde daha hızlı ve düşük maliyetli hale gelmektedir.

Bir diğer avantaj ise uçtan uca/kişiler arası şifrelemenin sağlanmasıdır. Bu özellik, kullanıcıların işlemlerinin güvenliğini artırarak, verilerin yalnızca ilgili taraflar arasında paylaşılmasını mümkün kılmaktadır. Böylece, bilgi güvenliği sağlanırken, kullanıcıların gizlilikleri de korunmaktadır.

Uluslararası para transferlerini kolaylaştırmak da bu teknolojinin önemli bir özelliğidir. Geleneksel sistemlerdeki karmaşık süreçler ve yüksek ücretler göz önüne alındığında, kripto para birimleri ile yapılan transferler, hızlı ve maliyet etkin bir alternatif sunmaktadır. Bu durum, özellikle sınır ötesi ticaret yapan işletmeler için büyük avantajlar sağlamaktadır.

Ayrıca, kripto para birimlerinin bir diğer önemli avantajı, geleneksel finansal aracılara olan bağımlılığı azaltmasıdır. Bankalar ve diğer finansal kuruluşlar, işlemlerin gerçekleştirilmesinde önemli bir rol oynamaktadır. Ancak kripto para birimleri, merkeziyetsiz yapıları sayesinde bu aracıları ortadan kaldırmakta ve kullanıcıların doğrudan birbirleriyle işlem yapmalarına olanak tanımaktadır. Bu da işlemlerin daha hızlı ve daha az maliyetle gerçekleştirilmesini mümkün kılmaktadır (Drescher, 2017; Doğan, 2020: 861).

Yukarıda belirtilen olası faydaların yanı sıra, kripto paralarla ilgili bazı potansiyel zorluk ve tehlikeler de bulunmaktadır. Öncelikle, fiyatlardaki dalgalanma önemli bir sorun teşkil etmektedir. Kripto para birimlerinin değerleri, piyasa koşullarına bağlı olarak aniden değişebilmekte ve bu durum, yatırımcılar için ciddi kayıplara yol açabilmektedir. Özellikle spekülasyon amacıyla yapılan işlemler, yatırımcıların daha büyük riskler almasına neden olmakta ve bu da piyasanın istikrarsızlaşmasına katkıda bulunmaktadır.

Bir diğer zorluk, acil fon gereksinimleri durumunda kripto paraların kağıt veya madeni paraya dönüştürülememesidir. Kripto paralar, dijital varlıklar olarak varlık gösterdiği için, acil bir durumda nakit paraya çevrilmeleri zaman alabilir veya bazı durumlarda mümkün olmayabilir. Bu, kullanıcıların finansal esnekliklerini kısıtlamakta ve acil durumlarda zorluklar yaşamalarına yol açmaktadır.

Ayrıca, kripto paraların özel şirketler tarafından üretilmesi ve merkez bankalarının düzenleyici bir rol üstlenmemesi, sektördeki belirsizlikleri artırmaktadır. Bu durum, kullanıcıların güvenliğini tehdit etmekte ve dolayısıyla kripto paraların benimsenmesini olumsuz yönde etkilemektedir. Merkez bankalarının düzenleyici müdahale eksikliği, piyasanın daha az denetlenen ve daha riskli bir ortam haline gelmesine neden olmaktadır.

Bununla birlikte, kripto paralar, haksız kazanç sağlama ve kara para aklama gibi yasadışı faaliyetlere de zemin hazırlamaktadır. Anonimlik sunan bu dijital varlıklar, kötü niyetli kişilerin yasa dışı işlemler gerçekleştirmelerine olanak tanımakta ve bu da kripto para ekosisteminin güvenilirliğini sarsmaktadır. Ayrıca, kripto paralar siber saldırılara hedef olma riski taşımakta ve kripto borsaları ile cüzdanlar, bilgisayar korsanları tarafından sıkça hedef alınmaktadır. Bu tür saldırılar sonucunda kullanıcıların varlıkları kaybolabilmekte, bu da kullanıcıların güvenliğini tehdit etmekte ve kripto para piyasasına olan güveni azaltmaktadır (Chakravaramvd., 2020: 752-754).

Bitcoin dışında, piyasada en çok ilgi gören ve tanınan kripto para birimleri arasında Ethereum, Ripple, Solano, Cardano, Avax ve Dogecoin gibi yüksek piyasa değerine sahip kripto para birimleri de bulunmaktadır. Bu kripto paraların her biri belirli projeler etrafında geliştirilmiş olup özgün amaçlara sahiptir. Kripto paralar madencilik olarak bilinen bir süreçle üretilmektedir. Bilgisayarlar yardımıyla karmaşık matematiksel problemleri çözerek yeni blokların eklenmesini içermektedir. Kullanıcılar bu işlem sonucunda ödül kazanarak kripto paraelde etmektedir. Oluşturulan kripto paraların saklanması için çeşitli cüzdan türleri mevcuttur: çevrimiçi cüzdanlar, çevrimdışı cüzdanlar, donanım ya da kağıt üzerindeki şekillerde olmaktadır (Rajasekaranvd., 2022: 52).

7.2. Bankacılık ve Sigortacılık

Blok zincirinin sağladığı güvenli yapı sayesinde, bankacılık sektöründe kullanımı giderek yaygınlaşmakta ve blok zinciri tabanlı hizmetler sunulmaktadır. Bitcoin'in ortaya çıkmasıyla birlikte paranın tamamen dijital ortamda işlem görmesi, bankacılık alanında blok zinciri kullanımını önemli hale getirmiştir. Bankacılıkla ilgili çalışmalarda öncelikli olarak kripto para birimlerinin alım satımına odaklanılmıştır. Ayrıca Forex piyasasında da bu değerli varlık olan kripto para birimleri kullanılmaya başlanmıştır. Bu tür uygulamalarla amaçlanan, banka dünyasında kripto paraların nakde çevrilmesi ve ödemelerin resmi kurumlara iletilmesidir. Günümüzde finansal kuruluşlar arasında yer alan bankalara karşı duyulan güvensizlik artış göstermiştir. Bu sebeple daha güvenilir alternatif sistemlerin arayışı blok zincirine ilgiyi artırmaktadır (Takaoğlu vd., 2019: 271).

Bankacılık sektöründe, blok zinciri tabanlı birçok proje bulunmaktadır. Örneğin, dünya çapında en büyük bankalardan biri olan JP Morgan, Ethereum tabanlı Metaverse platformunda ilk banka olma unvanını kazanmıştır. Fiziksel bir mekânı olmadan faaliyet gösteren bu banka bekleme salonları sunacak, müşterilerin birbirleriyle tanışmasına imkân sağlayacak ve sınır ötesi para transferlerinin yanı sıra finansal varlık yönetimi desteklerini içeren çeşitli bankacılık hizmetlerini sanal dünyada gerçekleştirebilmektedir(Başar, 2023:144). Benzer şekilde Çin Halk Cumhuriyeti'nde de özellikle ödeme işlemlerinde blok zincirinin kullanıldığı görülmektedir. "Gachain" adlı projeyle elektronik faturalama ve vergi sistemini entegre ederek potansiyel vergi kaçakçılığının önlenmesi hedeflenmiş olup bu yolla hem vergi tahsilatının hızlandırılması hem de kayıt dışı ekonominin engellenmesi amaçlanmaktadır (Demirkan, 2021:80).

7.3. Lojistik ve Tedarik Zinciri

Blok zinciri, lojistik ve tedarik zinciri sektöründe geleneksel sistemleri ve süreçleri dönüştürme potansiyeli nedeniyle büyük ilgi görmektedir. Tedarik zinciri paydaşları, blok zincirini şeffaflık eksikliklerini giderebilecek, verimsiz takip sorunlarını çözebilecek ve sahte ürünlerle mücadele edebilecek bir teknoloji olarak değerlendirmektedirler.

Lojistik ve tedarik zincirinde blok zincirin etkisi oldukça geniş kapsamlı olup, sektörün çeşitli yönlerini kapsamaktadır. Bu teknolojinin önemli avantajlarından biri şeffaflık ve izlenebilirliği artırmasıdır. Blok zinciri sayesinde, tedarik zinciri paydaşları malların hareketini kolayca takip edip doğrulayabilmektedir. Bu da düzenlemelere uyum sağlama imkânı sunarken dolandırıcılığı önleyici bir rol oynamaktadır. Artan şeffaflık ise farklı tedarik zinciri aktörleri arasında daha

fazla güven ve iş birliğini teşvik ederek anlaşmazlıkların ve gecikmelerin azalmasına yardımcı olmaktadır (Hellanivd., 2021: 1-2).

Blok zinciri, sahte ürün riskini azaltarak tedarik zincirinin güvenliğini artırma kapasitesine sahiptir. Ürün bilgilerini ve işlemleri değiştirilemez bir defterde kaydederek paydaşlar, malların gerçekliğini ve kökenini doğrulayabilmektedir. Böylelikle sahte ürünlerin dolaşımını önleyebilmekte ve tüketici güvenliği sağlanmaktadır. Ek olarak, blok zinciri lojistik ve tedarik zincirindeki verimliliği artırarak maliyetleri düşürme potansiyeline de sahiptir (Modgil, Sonwaney, 2019: 1).

Lojistik ve tedarik zinciri alanında blok zincirinin geliştirilmesi ve yaygınlaştırılmasında önemli bir rol oynayan isimlerden biri, Danimarkalı denizcilik devi Maersk'tir. IBM ile iş birliği yapan Maersk, 2018 yılında küresel tedarik zincirlerini dijitalleştirmek ve kolaylaştırmak amacıyla Trade Lens platformunu hayata geçirmiştir. Trade Lens, gerçek zamanlı görünürlük sunarak tek bir doğruluk kaynağı sağlamaktadır. Bu sayede tedarik zinciri süreçlerinin verimliliğini artırmakta ve güvenli hale getirmekte olup evrak işlerindeki karmaşıklığı azaltırken gecikmeleri de minimize etmektedir (Jovanovicvd., 2022). Bu alanda etkisi olan diğer kişi ise Frank Yiannas'tır. Yiannas'ın katkıları sayesinde gıda izlenebilirlik sistemlerinde büyük ilerlemeler kaydedilmiş. Blok zinciri teknolojisinin benimsenmesinde destekçi olmuştur. Uyguladığı blok zinciri tabanlı sistemlerle gıdaların kaynaklarının takip edilmesini sağlayarak israfı önlemeyi hedeflemektedir (Difrancescovd.,2023:629).

Gelecekteki gelişmeler açısından, lojistik ve tedarik zinciri alanında blok zincirinin sürekli genişleme ve yeniliklere açık olduğu görülmektedir. Bu alandaki potansiyel ilerlemelerden biri de Nesnelerin İnterneti (IoT) cihazlarının blok zinciri teknolojisi ile entegrasyonudur. Fiziksel cihazların blok zinciri ağlarına bağlanmasıyla birlikte malların gerçek zamanlı olarak takip edilmesi mümkün hale gelebilmektedir. Böylelikle tedarik zincirinde şeffaflık ve verimliliği daha fazla artırabilmektedir (Hussain vd., 2021: 1). Ayrıca, akıllı sözleşmelerin yükselişi lojistik ve tedarik zincirlerinde önemli bir değişiklik olarak değerlendirilmektedir. Akıllı sözleşmeler, anlaşmaların koşullarını otomatik biçimde doğrulayan ve uygulayan kendi kendini yöneten dijital kontratlardır. Blok zinciri ile entegre edilen akıllı sözleşmelere sayesinde ödeme işlemleri, sigorta talepleri gibi süreçler otomatikleştirilebilirken paydaşlar arasındaki güveni güçlendirmektedir (Hassan vd., 2021: 2-3).

7.4. Medya, Eğlence, Oyun

Blok zincirinin yenilikçi çözümleri medya, eğlence ve oyun sektörlerinde kayda değer bir dönüşüm sağlamaktadır. Bu sektörde blok zinciri teknolojisinin etkisi geniş kapsamlı ve dönüştürücü bir nitelik taşımaktadır. Ürettiği en önemli avantajlardan biri, gelişmiş güvenlik ve şeffaflık sunmaktadır. Blok zinciri, merkezi olmayan defterlerin kullanımıyla içerik üreticileri, dağıtıcılar ve tüketiciler arasındaki kayıtların bozulmadan korunmasını sağlayarak güveni artırmaktadır (Bhowmik, Feng, 2017: 5).

Blok zinciri teknolojisi, dijital varlıkların oluşturulmasına ve yeni gelir modellerinin geliştirilmesine zemin hazırlamıştır. Son yıllarda NFT'ler (değiştirilemez tokenler), blok zinciri

aracılığıyla büyük ilgi görmektedir. Bu tür tokenler, sanatçıların ve yaratıcı bireylerin dijital eserlerini belirli bir formatta parçalara ayırarak dijital varlıklar haline getirip satmalarına olanak tanımakta, sanat ve koleksiyonculuk alanında yenilikçi bir kapı açmaktadır (Düzenli,Perdahçı, 2023: 167). Ayrıca Decentraland ile TheSandbox gibi blok zincir tabanlı platformlar sayesinde oyuncular sanal varlıklara sahip olma, bunları alıp-satma veya takas etme imkanı bulmaktadır. Böylece oyun dünyasında farklı fırsatlar ortaya çıkarmaktadır (Casale-Brunetvd., 2023: 2).

Diğer yandan bu teknoloji geleneksel aracı kurumlarda da değişikliklere yol açmaktadır. Blok zinciri içerik doğrulama ve dağıtım süreçlerinde merkezi kuruluşlara duyulan ihtiyacı ortadan kaldırarak içerik üreticilerinin kitleleriyle doğrudan iletişim kurabilmelerine imkan tanımaktadır. Bu durum, maliyet tasarrufunu artırarak özellikle müzik sektöründe teliften az pay alan sanatçılara güç kazandırabilmektedir (Arcos, 2018: 441).

Medya, eğlence ve oyun alanında blok zincirinin tüm potansiyelini ortaya çıkarmak ve bu sektörleri merkezi olmayan, dijitalleştirilmiş yapıya dönüştürmek için sektörler arası sürekli yenilik ve iş birliği gerekmektedir.

7.5. Eğitim

Eğitim sektöründe blok zincirinin etkisi oldukça geniş kapsamlıdır. Veri güvenliği, kimlik hırsızlığı ve eğitim kayıtları üzerindeki merkezi kontrol gibi sorunlara çözüm sunarak öğrenme ve kimlik bilgileri gibi birçok alanda önemli potansiyellere sahiptir. Geleneksel eğitim sistemleri genellikle merkezi veri tabanlarına dayanmaktadır. Bu da siber saldırılara ve veri ihlallerine karşı savunmasız kılmaktadır. Blok zinciri ise verilerin birden fazla düğüme dağıtılması sayesinde doğal olarak daha güvenli hale gelmektedir. Her işlem şifrelenip zaman damgasıyla işlendiği için önceki işlemlerle bağlantılı olmaktadır. Böylece şeffaflık ve değişmezlik garanti edilmektedir (Maulanivd., 2021:137).

Blok zinciri eğitim alanında kimlik bilgilerini kolayca doğrulama ve onaylama imkanı sunmaktadır. Günümüzde eğitim sertifikalarının ve diplomaların doğrulanması, birçok kurumla iletişime geçmeyi gerektirmektedir. Bu da zaman alıcı bir süreçtir. Blok zinciri sayesinde bu kayıtlar dijital olarak saklanıp yetkili kişiler tarafından anında kontrol edilebilir hale gelmektedir. Böylece idari yükler hafifletilirken sahte sertifika riski de ortadan kaldırmaktadır (Fedorova,Skobleva, 2020: 568).

Veri gizliliği ve standardizasyonla ilgili zorluklar sürerken, blok zinciri eğitim sektöründe öğrencileri güçlendirme, veri güvenliğini artırma ve daha verimli ile şeffaf bir eğitim platformu oluşturma potansiyeline sahiptir. Teknoloji ilerledikçe paydaşların iş birliği yaparak bu zorlukları birlikte aşmaları, blok zincirinin eğitimin geleceğini şekillendirmede tam potansiyelini ortaya koyabilecektir.

7.6. Sağlık

Günümüzde sağlık sektöründe, artan maliyetler ve rekabetin yanı sıra hasta memnuniyeti, mahremiyet ihlalleri ve hizmet sunucularına yapılan geri ödemelerdeki aksaklıklar gibi birçok önemli sorun bulunmaktadır. Sağlığın ertelenemez bir ihtiyaç olması sebebiyle kaliteli sağlık

hizmeti sunumu, alıcıların en temel beklentileri arasında yer almaktadır. Modern ağ yapılarının teknolojide yaygınlaşmasıyla birlikte hizmet kalitesinde iyileşme beklenirken aynı zamanda kötü amaçlarla kullanılabilecek sağlık bilgisi güvenliği sorunu da ortaya çıkmaktadır. Bu nedenle, mevcut veya olası riskleri değerlendirip karşılaşılan problemleri çözen, değişime uyum sağlayabilen, teknolojiye ayak uyduran, rekabet gücünü artıran, maliyetleri düşüren ve hasta memnuniyetini ön planda tutan sistemlerin benimsenmesi kaçınılmaz hale getirmektedir (Reda vd., 2020; Aytekin, Ayhan, 2022: 61).Sağlık bilgi teknolojileri, karar verme ve örgütsel operasyonların merkezinde bulunduğu için verimlilik, kalite, güvenlik ve maliyet gibi unsurları etkilemektedir (Karaçadır, 2023: 13). Blok zinciri, sağlık alanında veri güvenliği ve bütünlüğü sağlama konusunda önemli bir altyapı sunmaktadır. Bu teknoloji, sağlık hizmetlerinin yönetimi, tıbbi kayıtların korunması ve veri paylaşımı gibi birçok alanda avantajlar sağlamaktadır. Sağlık sektöründeki blok zincirinin en kritik uygulamalarından biri ise hasta verilerinin güvenli şekilde saklanmasıdır. Geleneksel yöntemler genellikle merkezi olup siber saldırılar ve ihlaller karşısında savunmasız olabilirken, blok zincirinde kullanılan merkezi olmayan defter teknolojisi ile bilgiler daha güvenli olarak saklanmaktadır.Böylece bu yapı hastaların hassas kişisel sağlık bilgileri üzerindeki olası tehditleri veya ihlalleri önlemeye yardımcı olmaktadır (Pilaresvd., 2022: 2).

Blok zinciri teknolojisi, sağlık hizmetlerinde geniş ve önemli kullanım alanlarına sahiptir. Bu teknoloji, veri güvenliğini artırma, hasta verilerinin paylaşımını kolaylaştırma ve ilaç takibini garanti altına alma gibi konularda büyük avantajlar sağlamaktadır. Dolayısıyla blok zinciri yalnızca kripto para birimlerinde değil, pek çok farklı alanda da işlevsel olan bir teknolojidir. Merkezi olmayan yapısı sayesinde şeffaflık sağlayan bu sistem aynı zamanda değiştirilemezlik özelliği ile dikkat çekerken dağıtık ve otomatik özellikleriyle de etkili çözümler sunmaktadır (Kasula, 2023: 2). Güvenli bir yapı oluşturan blok zincirinin birçok sektörde dönüşüm yarattığı gözlenmektedir. Gelecekte de bu yenilikçi teknolojinin kullanım alanlarının daha fazla yayılacağı öngörülmektedir.

8.BLOK ZİNCİRİ VE YAPAY ZEKA ENTEGRASYONU

Dijital çağda, blok zinciri ve yapay zeka teknolojileri en önemli iki yenilikçi güç olarak dikkat çekmektedir. Her bir teknoloji kendine has avantajlar sunmaktadır. Ancak birlikte kullanıldıklarında daha etkileyici ve yaratıcı sonuçlara ulaşmak mümkün olmaktadır. Blok zinciri, endüstriyel sektörler için verilerin güvenli bir şekilde saklanmasını sağlayan değiştirilmez kayıt mekanizmasıdır. Yapay zeka ise büyük veri miktarlarını analiz ederek anlamlı bilgiler üretme kapasitesini artırmakta ve bu sayede otomatik karar verme süreçlerini desteklemektedir (Hussain, Al-Turjman, 2021: 7-8).

Yapay zeka algoritmalarının öğrenimi ve kullanımında genellikle büyük miktarda veriye ihtiyaç duyulmaktadır. Bu nedenle, bu verilerin güvenliği ve değiştirilemez olması çok önemlidir. Blok zinciri teknolojisi burada önemli bir rol üstlenmektedir. Çünkü veriler blok zinciri üzerinde saklanarak manipülasyon riskleri en aza indirilirken yetkisiz erişimlere karşı da koruma sağlanmaktadır. Böylece yapay zeka modellerinin dayanıklılığı artmaktadır (Tagdevd., 2021: 52810). Blok zinciri ve yapay zekanın entegrasyonu, veri yönetiminde önemli iyileştirmeler sağlamaktadır. Bu entegrasyon, veri güvenliğini artırarak manipülasyonu zorlaştırmakta ve

işlemlerin doğruluğunu kalıcı olarak kaydedilmektedir. Yapay zeka, veri analizi ve işleme süreçlerini otomatikleştirerek zaman tasarrufu sağlamakta ve karar verme süreçlerini hızlandırmaktadır. Ayrıca, müşteri davranışlarını anlamada yardımcı olurken, insan hatalarını minimize ederek veri kalitesini artırmaktadır. Blok zinciri, değiştirilemez veri kayıtları sunarken, yapay zeka özel çözümlerle işlemleri daha güvenli ve etkili hale getirmektedir. Bu şekilde, veri yönetimindeki sorunlar çözülmekte ve mevcut noksanlıklar giderilmektedir. Özellikle sağlık sektörü bu entegrasyondan büyük ölçüde yararlanabilmektedir. Hastaların verileri blok zinciri ile güvenli ve değişmez bir şekilde saklanırken, yapay zeka algoritmaları bu verileri analiz ederek hastalıkların erken teşhisini sağlayabilmekte ve kişiye özel tedavi planları oluşturulmasına olanak tanımaktadır (Shaikvd., 2022: 2). Finans sektöründe blok zinciri ve yapay zekanın birleşimi önemli fırsatlar sunmaktadır. Blok zinciri, güvenli ve şeffaf finansal işlemler sağlarken, yapay zeka bu verileri analiz ederek dolandırıcılığın tahmin edilmesi ve önlenmesine yardımcı olmaktadır. Bu durum, finansal hizmetlerin daha güvenilir ve etkili hale gelmesini desteklemektedir. Örneğin, bir kredi risk değerlendirme süreci blok zincirinde kaydedilmiş olan güvenli veri kullanılarak yapay zeka algoritmaları ile daha doğru bir şekilde gerçekleşebilmektedir (Adeyeri, 2024: 29).

Blok zinciri ve yapay zekanın entegrasyonu, birçok sektörde büyük dönüşüm potansiyeline sahip olup veri güvenliği ve yönetimi konularında önemli iyileştirmeler sağlamaktadır. Bu entegrasyonun başarıyla uygulanabilmesi için teknik zorluklar ile düzenleyici engellerin aşılması gerekmektedir. Gelecekte bu iki güçlü teknolojinin birleşimi, daha akıllı, daha güvenli ve daha verimli sistemlerin geliştirilmesine öncülük edecektir.

SONUÇ VE TARTIŞMA

Blok zinciri teknolojisi, dijital dönüşüm sürecinde güvenlik, şeffaflık ve merkeziyetsizlik gibi özellikleriyle çeşitli sektörlerde büyük bir potansiyel sunmaktadır. Bu makalede blok zincirinin teknik altyapısı, mimarisi ve uygulama alanları ele alınmış olup özellikle finans, sağlık, lojistik ve eğitim gibi alanlardaki mevcut ve olası kullanımları vurgulanmıştır. Kripto paralar, düşük işlem maliyetleri ve merkeziyetsizlik sağlarken, piyasa dalgalanmaları ve düzenleme eksiklikleri yatırımcıları zorlayabilmektedir. Bankacılıkta blok zinciri, aracılara bağımlılığı azaltarak güvenli ve hızlı işlemler yapılabilmesini sağlarken, lojistikte şeffaflık ve izlenebilirlik sunarak maliyetleri düşürebilmektedir. Medya ve eğitim sektörlerinde veri doğrulama ve doğrudan kitlelerle iletişim imkânı tanıyabilen blok zinciri, sağlıkta ise hasta verilerinin güvenliğini güçlendirebilmektedir. Blok zincirinin sunduğu yenilikçi çözümler, sektörel dönüşüm yaratabilirken adaptasyon sürecinde bazı düzenleyici ve operasyonel zorluklar içerebilmektedir. Bu teknolojiveri güvenliğini artırma, işlemleri hızlandırma ve maliyetleri düşürme avantajları sağlamakla birlikte aynı zamanda merkezî otoritelerin bulunmadığı güvenli ile şeffaf bir dijital ekosistem oluşturabilme yeteneğine de sahiptir. Ancak bu teknoloji henüz gelişim aşamasında olup, birlikte çalışabilirlik ve enerji tüketimi konularında çözüm gerektiren sorunlarla karşı karşıyadır. Kripto para ve blok zinciri alanında, farklı platformların entegre çalışabilmesi için açık standartlar geliştirilmesi, ekosistemin genişlemesine ve kullanım kolaylığının artmasına katkı sağlayabilir. Ayrıca, enerji tüketimi konusundaki sorunların çözümü için, yenilenebilir enerji kaynaklarının kullanımını teşvik eden uygulamalar ve daha az enerji tüketen blok zinciri algoritmaları üzerine yapılan araştırmalar desteklenebilir. Böylece, bu

teknolojinin sürdürülebilir büyümesi sağlanabilir ve kullanıcılar için daha erişilebilir bir sistem oluşturulabilir.

Sonuç olarak, blok zinciri teknolojisi dijital dönüşümde değişim yaratma potansiyeline sahiptir. Türkiye özelinde değerlendirildiğinde ise, bu teknolojinin uygulanmasına yönelik önemli adımlar atılmış olup yasal düzenlemeler, teknik çalışmalar ve örnek projelerle desteklenmektedir. Türkiye'de yapılan yasal düzenlemeler arasında kripto varlıkların hukuki statüsünün belirlenmesi ve finansal işlemler için güvenlik protokollerinin geliştirilmesi yer almaktadır. Ancak bu düzenlemelerin etkinliği, teknolojinin hızla gelişmesi karşısında zaman zaman yetersiz kalabilmektedir. Ayrıca, düzenlemelerin verimliliğini artırmak için sektörler arası iş birliği ve yenilikçi yaklaşımlarla mevzuatın güncellenmesi önem taşımaktadır. Bu adımlar, blok zincirinin Türkiye'deki uygulama alanlarını genişleterek teknolojinin dijital dönüşümde daha güçlü bir rol oynamasını sağlayabilir. Türkiye Cumhuriyeti Merkez Bankası ve Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) gibi kurumların, blok zincirinin finans ve dijital varlıklar üzerindeki kullanımına yönelik oluşturduğu yasal çerçeveler, ülkemizdeki düzenleyici altyapının güçlendirilmesi adına önem taşımaktadır. Ayrıca, özellikle finans sektörü ve kamu kurumlarında blok zinciri teknolojisinin kullanımını teşvik eden projeler dikkat çekmektedir. Örneğin, Türkiye Cumhuriyeti Merkez Bankası'nın dijital para projeleri, bankaların blok zinciri tabanlı ödeme sistemlerine yönelik çalışmaları Türkiye'de blok zincirinin sektörel adaptasyonuna ilişkin somut örnekler sunmaktadır. Ancak bu teknolojinin tam anlamıyla benimsenebilmesi için sektörel farkındalığın artırılması ve hem yasal hem de teknolojik altyapıların güçlendirilmesi gereklidir. Gelecekte daha fazla sektörde uygulanabilir olması beklenen blok zincirinin geliştirilmesi ve yaygınlaştırılması, güvenli, hızlı ve merkeziyetsiz bir dijital dünya oluşturmak için kritik öneme sahip olabilecektir. Özellikle Türkiye'de blok zinciri adaptasyonunun daha geniş sektörlere yayılabilmesi adına, çeşitli düzenleyici çerçevelerin uluslararası iş birliğiyle şekillendirilmesi, teknolojinin güvenlik ve enerji verimliliği gibi kritik konularda daha da iyileştirilmesi gerekmektedir.

KAYNAKÇA

Adeyeri, T. B. (2024). Blockchainand AI Synergy: Transforming Financial Transactionsand Auditing. *BlockchainTechnologyand Distributed Systems, 4*(1), 24-44.

Aggarwal, S., & Kumar, N. (2021). Architecture of Blockchain. In*Advances in Computers, 121*, 171-192. Elsevier.

Akleylek, S., Yıldırım, H. M., & Tok, Z. Y. (2011). Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta. *13. Akademik Bilişim Konferansı Bildirileri*, 713-718.

Arcos, L. C. (2018). TheBlockchainTechnology on The Music Industry. *BrazilianJournal of Operations andProduction Management, 15*(3), 439-443.

Atabaş, H. (2018). Blokzinciri Teknolojisi ve Kripto Paraların Hayatımızdaki Yeni Yeri: Dijitalleşen Finans-Ekonomi-Sağlık-Eğitim-İş Dünyası. İstanbul: Ceres Yayınları.

Aytekin, M., & Ayhan, E. (2022). Sağlık Sektörü Uygulamaları, Blockchain Teknolojileri ve Sektörel Etkileri. Ankara: Nobel Yayınları.

Balcı, M., & Çakır, K. (2021). Kripto Paraların Karapara Aklama Yöntemi Olarak Kullanılması. *Ceza Hukuku Dergisi, 16*(46), 311-332.

Başar, R. (2023). Dijital Dönüşümde Güncel Yaklaşımlar: Türkiye ve Dünya Örnekleri. İ. Çevik Tekin (Ed.), *Yönetim Bilişim Sistemleri: İşletmelerde Dijital Dönüşüm Yönetimi* içinde (ss. 125-162). Gaziantep: Özgür Yayınları.

Bayer, D., Haber, S., &Stornetta, W. S. (1993). ImprovingtheEfficiencyandReliability of Digital Time-Stamping. In*Sequences II: Methods in Communication, Security andComputerScience* (ss. 329-334).

Ber, A. S. (2022). Blokzincir (Blockchain) Teknolojisi Kapsamında Elektronik Çek. *Journal of Marine andEngineeringTechnology, 2*(1), 1-20.

Bhowmik, D., & Feng, T. (2017). The Multimedia Blockchain: A Distributed andTamper-Proof Media Transaction Framework. *22nd International Conference on DigitalSignalProcessing (DSP)*, 1-5.

Bibi, S. (2023). Money in The Time of Crypto. *Research in International Business and Finance, 65*, 1-15.

Blossey, G., Eisenhardt, J., &Hahn, G. J. (2019). BlockchainTechnology in SupplyChain Management: An Application Perspective. *Proceedings of the 52nd Hawaii International Conference on SystemSciences*, 6885-6893.

Bosamia, M., &Patel, D. (2018). CurrentTrendsandFutureImplementationPossibilities of The Merkel Tree. *International Journal of ComputerSciencesandEngineering, 6*(8), 294-301.

Casale-Brunet, S., Mattavelli, M., &Chiariglione, L. (2023). ExploringBlockchain-BasedMetaverses: Data Collection andValuation of Virtual Lands Using Machine Learning Techniques. *Digital Business, 3*(2), 100068.

Chakravaram, V., Ratnakaram, S., Agasta, E., &Vihari, N. S. (2020). Cryptocurrency: ThreatorOpportunity. *3rd International Conference on Communications andCyberPhysicalEngineering*, 747-754.

Christidis, K., &Devetsikiotis, M. (2016). Blockchainsand Smart ContractsforThe Internet of Things. *IEEE Access, 4*, 2292–2303.

Demirkan, G. (2021). Blokzincir ve Teknolojik Determinizm (Yayımlanmamış yüksek lisans tezi). İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Dib, O., Brousmiche, K. L., Durand, A., Thea, E., &Hamida, E. (2018). ConsortiumBlockchains: Overview, Applications andChallenges. *International Journal on Advances in Telecommunications, 11*(1), 51-64.

Difrancesco, R. M., Meena, P., & Kumar, G. (2023). How BlockchainTechnologyImprovesSustainableSupplyChainProcesses: A Practical Guide. *Operations Management Research, 16*(2), 620-641.

Doğan, Ş. (2020). Dijital Çağda Paranın Dönüşümü: Kripto Para Birimleri ve Blok Zinciri (Blockchain) Teknolojisi: Üniversite Öğrencilerine Yönelik Bir Araştırma. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi, 8*(3), 859-870.

Drescher, D. (2017). Using the Data Store. In*Blockchain Basics*. Apress, Berkeley, CA.

Duman, M. Ç. (2023). Sürdürülebilir İşletmeler İçin Yeni Bir Çözüm Olan Blok Zinciri Teknolojisi Üzerine Sistematik Bir İnceleme. *İzmir İktisat Dergisi, 38*(1), 192-214.

Dutta, P., Choi, T. M., Somani, S., &Butala, R. (2020). BlockchainTechnology in SupplyChain Operations: Applications, ChallengesandResearchOpportunities. *TransportationResearchPart E: LogisticsandTransportationReview, 142*, 2-33.

Düzenli, K., &Perdahçı, N. Z. (2023). Metaverse ve NFT'ninMimarîğe Etkileri: Geleceğin Yapıları Nasıl Şekillenecek? *Eksen Dokuz Eylül Üniversitesi Mimarlık Fakültesi Dergisi, 4*(2), 165-182.

Efe, D. (2021). Büyükşehirlerde Blokzincir Teknolojisinin Kullanımı: Denizli Büyükşehir ve Gidiş-Geliş Kuşağı Örneği (Yayımlanmamış yüksek lisans tezi). Pamukkale Üniversitesi, Denizli.

Elbüz, A., Osmanoğlu, M., & Tanrıöver, Ö. (2023). Blok Zinciri Tabanlı İdeal Bir Veri Ticareti Platformunun Tasarımı İçin SysML Tabanlı Bir Yaklaşım. *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 39*(1), 509-519.

Eroğlu, A. (2023). Kamu Mali Denetiminin Dijitalleşmesi: Blokzincir Teknolojisinin İncelenmesi. *Alanya Akademik Bakış Dergisi, 7*(1), 187-207.

Essaid, M., Kim, J., &Ju, H. (2023). Inter-BlockchainCommunication Message Relay Time Measurementand Analysis in Cosmos. *AppliedSciences, 13*, 11135.

Fedorova, E. P., &Skobleva, E. I. (2020). Application of BlockchainTechnology in HigherEducation. *EuropeanJournal of ContemporaryEducation, 9*(3), 552-571.

Haber, S., &Stornetta, W. S. (1991). How to Time-Stamp a DigitalDocument. *Journal of Cryptology*, 437-455.

Hadi, F. A., Hussein, A. R., Rashed, J. R., Awi, N. S. A., &Albehadili, H. (2019). A Vision of BlockchainTechnologyandIts Integration WithIoT: Applications, Challenges, andOpportunities; FromtheAuthenticationPerspective. *Journal of TheoreticalandApplied Information Technology, 97*(15), 4048-4060.

Halpin, H., &Piekarska, M. (2017). Introductionto Security andPrivacy on theBlockchain. *2nd IEEE EuropeanSymposium on Security andPrivacy*, Paris.

Hassan, A., Ali, M. I., Ahammed, R., Khan, M. M., Alsufyani, N., &Alsufyani, A. (2021). SecuredInsurance Framework Using Blockchainand Smart Contract. *Scientific Programming, 2021*(1), 6787406.

Hellani, H., Sliman, L., Samhat, A. E., &Exposito, E. (2021). On Blockchain Integration withSupplyChain: Overview on Data Transparency. *Logistics, 5*(3), 46.

Hussain, A. A., & Al-Turjman, F. (2021). ArtificialIntelligenceandBlockchain: A Review. *Transactions on EmergingTelecommunications Technologies, 32*(9), 1-26.

Hussain, M., Javed, W., Hakeem, O., Yousafzai, A., Younas, A., Awan, M. J., &Zain, A. M. (2021). Blockchain-BasedIoTDevices in SupplyChain Management: A SystematicLiteratureReview. *Sustainability, 13*(24), 13646.

Jovanovic, M., Kostic, N., Sebastian, I. M., &Sedej, T. (2022). Managing a Blockchain-Based Platform EcosystemforIndustry-WideAdoption: The Case of TradeLens. *TechnologicalForecastingandSocialChange, 184*, 121981.

Karaçadır, V. (2023). *Sağlık Bilgi Teknolojileri Kullanım Niyeti*. İstanbul: Eğitim Yayınevi

Kasula, B. Y. (2023). The Role of BlockchainTechnology in Securing Electronic HealthRecords. *Transactions on LatestTrends in ArtificialIntelligence, 4*(4), 1-6.

Kesebir, M., & Günceler, B. (2019). Kripto Para Birimlerinin Parlak Geleceği. *Iğdır Üniversitesi Sosyal Bilimler Dergisi, 17*, 605-625.

Kfoury, E. F., Gomez, J., Crichigno, J., Bou-Harb, E., &Khoury, D. (2019). Decentralized Distribution of PCP MappingsOverBlockchainforEnd-to-EndSecure Direct Communications. *IEEE Access, 7*, 110159-110173.

Kodaz, H., & Botsalı, F. M. (2010). Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması. *Selçuk Teknik Dergisi, 9*(1), 10-23.

Kösesoy, İ. (2019). Nesnelerin İnterneti Güvenliğinde Blok Zinciri Uygulamaları. *Veri Bilimi Dergisi, 2*(1), 1-9.

Laurance, T. (2017). *BlockchainforDummies*. John WileyandSons, New Jersey.

Lubis, N. I., &Pratama, A. (2023). Perkembangan Sistem AdministrasiPajakBerbasisBlockchain. *AccumulatedJournal, 5*(1), 27-41.

Maqsood, F., Ahmed, M., Ali, M. M., &Shah, M. A. (2017). Cryptography: A Comparative Analysis for Modern Techniques. *International Journal of Advanced ComputerScienceand Applications, 8*(6), 442-448.

Maulani, G., Gunawan, G., Leli, L., Nabila, E. A., &Sari, W. Y. (2021). DigitalCertificateAuthoritywithBlockchainCybersecurity in Education. *International Journal of Cyberand IT Service Management, 1*(1), 136-150.

Metin, T., & Arslan, İ. (2022). Blockchain ve kamu sigortası. In O. Yılmaz, B. T. Kaplan, & M. Kaplan (Edt.), Blockchain Teknolojileri ve Sektörel Etkileri (ss. 151-166). Ankara: Nobel Yayınları.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., &Qijun, C. (2017). A Review on ConsensusAlgorithm of Blockchain. *IEEE International Conference on Systems, Man andCybernetics (SMC)*, 2567-2572.

Modgil, S., &Sonwaney, V. (2019). Planning the Application of BlockchainTechnology in Identification of CounterfeitProducts: SectorialPrioritization. *IFAC-PapersOnLine, 52*(13), 1-5.

Montresor, A. (2008). Decentralized Network Analysis: A Proposal. *In 2008 IEEE 17th Workshop on Enabling Technologies: InfrastructureforCollaborative Enterprises*, 111-114.

Nadiya, U., Mutijarsa, K., &Rizqi, C. Y. (2018). BlockSummarizationandCompression in Bitcoin Blockchain. In*2018 International Symposium on Electronicsand Smart Devices (ISESD)*, 1-4. IEEE.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Erişim adresi: https://static.upbitcare.com/931b8bfc-f0e0-4588-be6e-b98a27991df1.pdf (Erişim tarihi: 06.07.2023).

Narayanan, A., & Clark, J. (2017). Bitcoin'sAcademicPedigree. *Communications of the ACM, 60*(12), 36-45.

Pilares, I. C. A., Azam, S., Akbulut, S., Jonkman, M., &Shanmugam, B. (2022). AddressingtheChallenges of Electronic HealthRecords Using Blockchainand IPFS. *Sensors, 22*(11), 4032.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). TheBlockchain as a Decentralized Security Framework FutureDirections. *IEEE Consumer Electronics Magazine, 7*(2), 18-21.

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A ComprehensiveSurvey on BlockchainTechnology. *SustainableEnergy Technologies andAssessments, 52*, 1-13.

Reda, M., Kanga, D. B., Fatima, T., &Azouazi, M. (2020). Blockchain in HealthSupplyChain Management: State of Art ChallengesandOpportunities. *ProcediaComputerScience, 175*, 706-709.

Reyna, A., Martin, C., Chen, J., Soler, E., & Diaz, M. (2018). On BlockchainandIts Integration withIoT: ChallengesandOpportunities. *FutureGenerationComputerSystems, 88*, 173-190.

Saad, S. M. S., &Radzi, R. Z. R. M. (2020). ComparativeReview of theBlockchainConsensusAlgorithmBetweenProof of Stake (POS) andDelegatedProof of Stake (DPOS). *International Journal of Innovative Computing, 10*(2), 27-32.

Sanka, A. I., Irfan, M., Huang, I., &Cheung, R. C. (2021). A Survey of Breakthrough in BlockchainTechnology: Adoptions, Applications, ChallengesandFutureResearch. *Computer Communications, 169*, 179-201.

Scholl, H. J., &Bolívar, M. P. R. (2019). Regulation as BothEnabler of TechnologyUseand Global CompetitiveTool: TheGibraltar Case. *Government Information Quarterly, 36*(3), 601-613.

Shaik, T., Tao, X., Higgins, N., Li, L., Gururajan, R., Zhou, X., &Acharya, U. R. (2023). Remote PatientMonitoring Using ArtificialIntelligence: CurrentState, Applications, andChallenges. *WileyInterdisciplinaryReviews: Data Miningand Knowledge Discovery, 13*, e1485.

Sikorski, J. J., Haughton, J., & Kraft, M. (2017). BlockchainTechnology in theChemicalIndustry: Machine-to-Machine Electricity Market. *AppliedEnergy, 195*, 234-246.

Stephen, R., & Alex, A. (2018). A Review on Blockchain Security. *IOP Conference Series: MaterialsScienceandEngineering, 396*(1), 012030.

Şahin, F. (2015). Modern Blok Şifreleme Algoritmaları. *İstanbul Aydın Üniversitesi Dergisi, 7*(26), 23-40.

Şahin, O. N. (2018). TMS ve TFRS Işığında Muhasebe, Vergi ve Denetim Açısından Bitcoin ve Diğer Kripto Para Birimleri. *Muhasebe ve Bilim Dergisi, 20*(4), 898-923.

Şat, N. (2019). Blokzincir (Blockchain)'in Kamu İdaresine Olası Etkileri Üzerine. *Amme İdaresi Dergisi, 52*(4), 117-147.

Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D., & Rahman, M. H. (2021). BlockchainandArtificialIntelligenceTechnology in E-Health. *EnvironmentalScienceandPollutionResearch, 28*, 52810-52831.

Takaoğlu, M., Özer, Ç., & Parlak, E. (2019). Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulama Alanları. *Uluslararası Doğu Anadolu Fen Mühendislik ve Tasarım Dergisi, 1*(2), 260-295.

Tapscott, D., &Tapscott, A. (2016). *BlockchainRevolution: How theTechnologyBehind Bitcoin is Changing Money, Business, andthe World*. PenguinRandom House, New York.

Tüfekci, A., & Karahan, Ç. (2019). Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirinin Kullanım Durumu. *Verimlilik Dergisi, 4*, 157-193.

Tüfenk, M.B. (2023), Uluslararası Ticarette Blockchain Teknolojisi Üzerine Genel Bir Bakış, *Gümrük Ticaret Dergisi*, 10(33), 31-42.

Uysal, T. U., & Kurt, G. (2018). Muhasebe Denetiminde Blok Zinciri Teknolojisi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 23*(2), 467-481.

Ünsal, E., & Kocaoğlu, Ö. (2018). Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri. *Avrupa Bilim ve Teknolojisi Dergisi, 13*, 54-68.

Vurdu, S. A. (2021). Dış Ticarette Blokzincir Uygulamaları. *Sosyal, Beşeri ve İdari Bilimler Dergisi, 4*(9), 924-936.

Wallez, T., Protzenko, J., Beurdouche, B., &Bhargavan, K. (2022). TreeSync: AuthenticatedGroup Management for Messaging Layer Security. *32nd USENIX Security Symposium*, 1217-1233.

Wang, D., & Zhang, X. (2021). SecureRide-Sharing Services Based on a ConsortiumBlockchain. *IEEE Internet of ThingsJournal, 8*(4), 2976-2991.

Wang, R., &Wu, Y. (2021). Application of BlockchainTechnology in SupplyChain Finance of BeibuGulfRegion. *Mathematical Problems in Engineering*, 5556424.

Wegrzyn, K. E., & Wang, E. (2021). Types of Blockchain: Public, Private, orSomething in Between. Erişim adresi: https://www.foley.com/insights/publications/2021/08/types-of-blockchain-public-private-between (Erişim tarihi: 13.07.2023).

Yaga, D., Mell, P., Roby, N., &Scarfone, K. (2018). BlockchainTechnologyOverview. *NationalInstitute of StandardsandTechnologyInternal Report*. Erişim adresi: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf.

Yakupoğlu, C. (2016). A ComparativeStudy of Bitcoin andAlternativeCryptocurrencies (Yayımlanmamış doktora tezi). Yıldırım Bayezit Üniversitesi, Ankara.

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G., & Chen, S. (2020). PublicandPrivateBlockchain in Construction Business Processand Information Integration. *Automation in Construction, 118*, 1-21.

Yener, E. (2020). Dijital Girişimcilikte Blok Zincir Teknolojilerinin Rolü ve Bir Model Önerisi: Blok Zincir Tabanlı İkinci El Araç Alım Satım Platformu (Sechandchain) (Yayımlanmamış yüksek lisans tezi). İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Yerlikaya, T., Buluş, E., & Buluş, N. (2006). Kripto Algoritmalarının Gelişimi ve Önemi. *Akademik Bilişim Konferansları*, 9-11.

Yiannas, F. (2018). A New Era of FoodTransparency Powered byBlockchain. *Innovations: Technology, Governance, Globalization, 12*(1-2), 46-56.

Zhang, R., Xue, R., &Liu, L. (2019). Security andPrivacy on Blockchain. *ACM Computing Surveys, 52*(3), 1-34.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of BlockchainTechnology: Architecture, Consensus, andFutureTrends. *IEEE International Congress on Big Data*, 557–564.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). BlockchainChallengesandOpportunities: A Survey. *International Journal of Web and Grid Services, 14*(4), 325-375.