

Blok Zincir ve Çapraz Zincir Teknolojilerinin Gelecek Muhtemel Uygulama Alanları

Tibet Tebriz URMAK

Bağımsız Araştırmacı, İstanbul, Türkiye

Orcid Numarası: 0000-0001-9303-2893

Geliş Tarihi: 21.07.2022

***Sorumlu Yazar e mail:** tibet.urmak@gmail.com

Kabul Tarihi: 07.09.2022

Atf/Citation: Urmak, T. T. (2022). “Blok Zincir ve Çapraz Zincir Teknolojilerinin Gelecek Muhtemel Uygulama Alanları”, *Haliç Üniversitesi Sosyal Bilimler Dergisi* 2022, 5(2). 271-303

Öz

“Şansölye Bankalar için İkinci Kurtarma Paketinin Eşiğinde”. Bitcoin’in “Genesis Blok” olarak adlandırılan doğum belgesi diyebileceğimiz ilk bloğunda yer alan bu ilginç mesajın neden yerleştiği halen bilinmemektedir. Buna rağmen Bitcoin ile ilgili bildiğimiz kesin bir şey varsa o da, başta finansal konular olmak üzere birçok sektöre getirdiği yenileşimci başarımlardır. İlgi, halen ağırlıklı olarak Bitcoin’in üzerinde olmasına rağmen, Bitcoin’in altında yatan blok zinciri ve onun farklı endüstri ve iş kolları arasında aracılık hizmeti sağlayan çapraz zincir teknolojisi, dünya gündemini bir hayli meşgul etmektedir. Eşsiz bir yapıya sahip olan blok zinciri teknolojisi şüphesiz insanlığın geleceğinin kaçınılmaz bir parçasıdır. Bu inceleme yazısında; Bitcoin’in altında yatan blok zinciri teknolojisi ve tamamlayıcısı olarak geliştirilen çapraz zincir teknolojisinin mevcut ve gelecek kullanım alanlarına değinilerek gelecek beklentilerinin neler olduğu tartışılmaktadır. Araştırmanın nihai amacı olarak, blok ve çapraz zincir teknolojilerinin gündelik hayatta olası ve gelecek kullanım alanları üzerinden bir farkındalık yaratma düşüncesi benimsenmiştir. Bu bağlamda geniş çaplı bir literatür çalışması yapılmış ve konu güncel örneklerle açıklanmıştır.

Anahtar Kelimeler: Blok Zincir, Çapraz Zincir, Bitcoin. Fütüroloji

Possible Future Application Areas of Blockchain and Cross-Chain Technologies

Abstract

“Chancellor on the Brink of Second Bailout for Banks”. It is still unknown why this interesting message has been placed in the first block of Bitcoin which is called the “Genesis Block”. However, if there is one thing we know for sure about Bitcoin, it is the innovative achievements it has brought to many sectors, especially financial issues. Although the interest is still predominantly on Bitcoin, both the blockchain underlying Bitcoin and its Cross-chain technology which helps it maintain intermediary services among different industries and business lines, occupy the world agenda. Blockchain technology, which has a unique structure, is undoubtedly an inevitable part of the future of humanity. In this review article; current and future uses of cross-chain technology which has been developed to complement the blockchain technology underlying Bitcoin, and future expectations thereupon are discussed. As the ultimate aim of the research, the idea of raising awareness on the possible and future uses of Blockchain and Cross-chain technologies in daily life has been adopted. In this article, a comprehensive literature explanation and analysis with current examples.

Keywords: Blockchain, Cross-Chain, Bitcoin, Futurology

1. Giriş

İnsanlık, var olduğu ilk çağdan itibaren veri üretmektedir. Ürettikleri bu verileri kimi zaman mağara duvarlarına, kimi zaman hayvan derilerine, kimi zaman da sözlü gelenekler ile kuşaktan kuşağa aktararak saklamışlardır. İnsanlık tarihinde yaşanan değişim ve gelişmelere bağlı olarak, bu verilerin saklanma yöntemleri değişmiş, zaman içerisinde de işlenerek anlamlı bir hale getirilip “bilgi” olmuştur. İnsanlık, bilgi sayesinde geçmiş tecrübe ve deneyimlerinden yola çıkarak, kendisine bir gelecek projeksiyonu inşa etmiştir. Bu noktada bilgi için “herhangi bir nesnenin veya sürecin tüm özellikleri ile birlikte kodlanmış halidir” demek mümkündür (Şengör, 2019: 20). Bilginin anlamlı bir bütüne dönüşmesi ise kişinin çevresiyle olan etkileşim sürecinde, nesnelere

algıladığı etkilerin sonucunu yorumlamasıyla ilişkilendirilmektedir (Russell, 1905: 480-481). Bu ilişkilendirme, bilimin doğası gereği kendisini sürekli düzelterek geliştirmesine benzetilebilir. Bu sayede insanoğlu, hem daha çok bilgi öğrenebilir hem de öğrendiği bilginin bir karşılığı olarak daha çok ilerleyebilir (Urmak, 2021: 69). Yine de ilkel mağara dönemlerinden beri çeşitli yöntemler ile günümüze kadar saklanarak aktarılan ve işlenerek anlam kazanan bilgi; bugün şüphesiz bizim için bu tanımlardan biraz daha fazlasını ifade etmektedir. Öyleyse, sadece dış uyaranlardan alınan uyarıcıların yanına tecrübe ve deneyimi de katarak bir bilgi tanımı yapmak daha doğru olacaktır. 20. yüzyılın son çeyreğinde bilgisayar teknolojilerinde yaşanan hızlı ilerleme, bugün gündelik hayatımızda kullandığımız birçok teknolojinin bizim için sıradan hale gelmesini sağlamıştır. Bu teknolojik gelişmeler sayesinde, gündelik hayat biz insanlar için daha konforlu ve daha kolay bir hale gelmiştir. Hızla gelişen teknoloji, yeni buluş ve ihtiyaçların da önünü açmıştır. Söz konusu durum, dünyada bilginin en başından beri var olan önemini herkes tarafından daha anlaşılır bir noktaya taşımakla kalmamış, bilgiyi günümüzün en kıymetli hazinesi olarak konumlandırmıştır. Bu hazine, günümüz dünyasında etkisini her alanda sonuna kadar hissettirmektedir. Bu etkiler, dâhil oldukları her sektörü kökten etkilemekle kalmamış, adeta oyunun kurallarını o sektör adına yeniden yazmıştır. Teknolojinin bu denli belirleyici ve kural koyucu olduğu günümüzde bu ilerlemelere ayak uydurmak; başta devletler, hükümetler ve işletmeler için var olma ile var olmama arasındaki keskin çizgiyi belirlemektedir.

Çalışmanın ilerleyen bölümlerinde, blok zinciri ve çapraz zincire ilişkin bilgiler açıklanarak gelecekte uygulamaya konması muhtemel blok zinciri çalışma alanlarına değinilmiştir. blok zinciri, çapraz zincir ve Bitcoin konuları akademik açıdan değerlendirildiğinde bu alanda yapılan akademik yayınların oldukça sınırlı olduğu görülmektedir. Yine benzer bir şekilde blok zinciri ve çapraz zincir arkasında yatan “teknoloji” ve “yeni dünya” anlayışından çok, kripto paraların sadece

finansal varlık olarak incelendikleri görülmüştür. Araştırmanın içeriğini oluşturan bilgilerin daha anlaşılabilir olması için teknik açıklamalar görsellerle desteklenmiştir.

2. Blok Zincir

Blok zincir teknolojisi; 2008 yılında, bugün hala gerçek kimliğini bilmediğimiz Satoshi Nakamoto mahlazlı bir kişi veya bir grup tarafından, kendi dijital para birimleri olan Bitcoin'i üretmek için geliştirilmiştir. "Bitcoin; Eşler arası elektronik nakit sistemi" adı ile Ekim 2008'de, sadece dokuz sayfalık bir makale olarak dünyaya duyurulmuştur. Bu makale, blok zinciri teknolojisinin manifestosu olarak kabul edilmektedir. Makalede, bilgilerin birbirlerini tanımayan taraflar arasında dağıtık yapıdaki çevrimiçi kayıt defteri üzerinden son derece güvenilir bir paylaşım esasına dayandığı anlatılmaktadır. Yani eşlerin tümü, çevrimiçi dağıtık kayıt defterinin kendisine ait bir kopyasına sahip olmakta ve bu kopyaların hiç birinin adem-i merkeziyetçi bir yapı tarafından saklanmasına veya korunmasına ihtiyaç duymadan, güvenli bir şekilde kullanılmasına olanak sağlamaktaydı. Bu dağıtık çevrimiçi mutabakat yapısı, adem-i merkeziyetçi bir yapıya ihtiyaç duymayan blok zinciri felsefesinin temelini oluşturmaktadır. Genel bir tanım üzerinden blok zinciri, internet üzerinde çalışan bir ağ üzerindeki veri veya bilginin kamuya açık bir çevrimiçi kayıt defteri şeklinde çalışmasını sağlayan bir teknolojidir. Blok zincirinde asıl çığır açan yenilik ise kamuya açık bu kayıt defteri yapısının, şifreli bir şekilde birbirine bağlanması ve üzerindeki veri veya bilgiyi değiştirilemez kılmasında yatmaktadır (Atabaş, 2018: 11). Sahip olduğu bu başarımı sayesinde blok zinciri teknolojisi, bireylerin şeffaflık anlayışlarına hitap etmektedir. Bu şeffaflık anlayışı; dağıtık defter yapısı sayesinde şifreli bir veri tabanının, paydaşlar arasında bir mutabakata (konsensüs) varılarak veri tabanının herkesçe son halini içermesidir (Özcan, 2021: 2). Bu şeffaf çevrimiçi defter yapısı, birçok otorite tarafından günümüzün

en büyük olaylarından birisi olarak tanımlanmaktadır. Bu bakış açısı üzerinden blok zinciri için daha geniş ve daha teknik bir tanım yapacak olursak; üçüncü taraflarca tahrif edilemez bir veri modelinin istenildiği zaman istenilen yere kolayca transfer edilerek paylaşılmasını içeren bir tür çevrimiçi dağıtık defter yapısıdır demek doğru olacaktır (Kshetri, 2017: 68). Yine bu yapı, sanılanın aksine, sadece kripto para ve NFT (Değiştirilmesi Mümkün Olmayan Dijital Varlık) olarak tabir edilen eserlerde kullanılmamaktadır. Bir blok zinciri yapısı, barındırdığı veriyi istem dışı herhangi bir müdahaleye maruz bırakmayacak şekilde kendi veri tabanına kodlamaktadır. Yine de bu kazuistik yapısına rağmen bir blok zinciri yapısı güncellenemez veya üzerinde modifikasyon yapılamaz yapılar değildir. Zaman içerisinde teknik iyileştirmeler veya kavramsal değişiklikler gibi konularda güncelleme yapma yoluna gidilebilecek yapılardır. Günümüzde blok zinciri yapılarına ekseriyetle transfer verimliliği, veri kullanım, kriptografi, depolama yönetimi gibi alanlarında çalışma ve düzeltmeler yapılmaktadır (Drescher, 2017: 236-239).

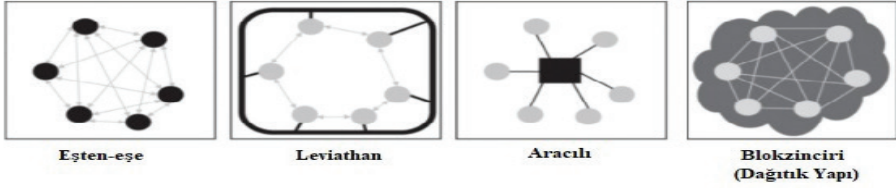
İşleyen bir blok zinciri ağında, veriyi içeren her alan “blok” olarak tanımlanmakta ve bu blok, çalışma prensibi olarak sıralı eylem dizisi oluşturulacak şekilde kodlanarak, kendinden önceki blokların tamamlanması prensibiyle çalışmaktadır. Bu yolla tamamlanmış verilerin oluşturdukları blokların toplamı zincir yapısını yani blok zincirini oluşturmaktadır (Fanning ve Centers 2016: 53-54). Bu yapının asıl başarımı, zincirleme bir reaksiyon ile birbirine bağlı ve kusursuz bir şekilde işleminde yatmaktadır. Bu sayede blok zinciri içerisinde kodlanan dağıtık kayıt defteri teknolojisi, merkezi bir otoritenin desteklemesine veya korumasına ihtiyaç duymadan eşler arası şifreleme, doğrulama ve mutabakat gibi işlemleri son derece hızlı ve düşük maliyetlerle mümkün kılmaktadır. Bu anlayışla inşa edilen “güvencesiz güven mimarisi” olarak da adlandırılan bu çevrimiçi dağıtık kayıt defteri yapısı, sadece ağın kendisini güvenli olarak kabul

etmektedir. Bu yapılar, akıllı sözleşmelerle de desteklenmişlerdir. Akıllı sözleşmeler, bir başka blok zinciri başarımı olan Ethereum altyapısında Solidity programlama dilinde oluşturulmuş kontratlardır. Akıllı sözleşmeler, belirli bir durumun veya görevin ifa edilmesi için geliştirilmiş uzlaşma protokolleri kullanan ve blok zinciri üzerinde çalışan programlardır. Çalışma şekilleri belirli bir koşulun sağlanmasına bağlıdır. İşlem için istenilen koşullar sağlandığı takdirde otomatik olarak gerçekleşen akıllı kontratlar; blok zinciri ağında gerçekleşen işlemlerin devamlılığını, şeffaflığını ve güvenilirliğini sağlayan programlardır (Wang vd., 2021: 1-2).

2.1. Blok Zincir Ağ Yapısı

Her ne kadar blok zinciri ağ yapısı barındırdığı özellikler açısından eşsiz olsa da insanlık tarihi boyunca blok zinciri teknolojisi geliştirilene kadar, zamanının gereksinim ve ihtiyaçlarına göre ortaya çıkmış ve kullanılmış başka ağ yapıları da mevcuttur. Bu ağ yapıları ve özelliklerine kısaca değinmeden hemen önce, blok zinciri ağ yapısında olan ama tarih boyunca geliştirilen diğer ağ yapılarının hiçbirisinde olmayan bir özellik olarak karşımıza çıkan “zincir” terimine değinmek, konunun daha net anlaşılması açısından şüphesiz faydalı olacaktır. Zincir terimiyle ifade edilen bu özelliği, Iansiti ve Lakhani 2017 senesinde yayımladıkları “The Truth About Blockchain” adlı makalelerinde “bir blok zinciri ağı üzerinde işlenmiş tüm bilgilerin kusursuz bir kronolojik sırayla tutulması ve bu kronolojik olarak saklanmış bilgilerin kendinden önce işlenmiş bilgilerle arasındaki kusursuz lineer ilişkiyi göstermesi” şeklinde tanımlamışlardır. Bu özelliği sayesinde blok zinciri ağ teknolojisi; ağ üzerinde gerçekleşen tüm işlemleri kusursuz bir şekilde saklayarak, diğer tüm ağ yapılarından net bir şekilde ayrılmaktadır. Öte yandan, blok zinciri ağ teknolojisi geliştirilene kadar sırasıyla; eşten-eşe, Leviathan ve aracılı ağ yapı modelleri kullanılmıştır. Bu ağ yapıları sayesinde insanlar mal, hizmet ve bilgi transferi gibi işlemleri kolayca

yaparak, sosyal ve ekonomik hayatın işleyişini devam ettirmişlerdir. Blok zinciri ağ yapısı ile birlikte eş zamanlı olarak halen kullanılan bu ağ yapılarına, blok zincirinin ve arkasındaki felsefenin daha iyi anlaşılması açısından değinecek olursak;



Şekil 1. Ağ Yapıları

Kaynak: Werbach, 2018: 42

İlk ağ yapısı olan eşten-eşe güven mimarisinin geçmişi insanlık tarihiyle yaşıttır. Bu yüzden bilinen ilk ağ yapısı demek mümkündür. Bu yapı içerisinde eş veya yakın statüye sahip taraflar, paylaşımlarını kendi aralarında karşılıklı güvene dayalı bir ilişki içerisinde ve yine kendi belirledikleri otonom kurallar çerçevesinde yürütürler. Bu ağ yapısı ağırlıklı olarak, merkezi regülasyon sağlayan otorite yapılarından uzakta çalışmayı tercih eder. Bu tip yapılar sıklıkla kendi özdenetim ve esnekliklerini kendileri sağlamakla birlikte, günümüzde halen kullanılmaktadır. İkinci güven mimarisi olan Leviathan, İngiliz filozof ve politikacı Thomas Hobbes'ın 1651 yılında kaleme aldığı "Leviathan" adlı kitabındaki hukuk devletinin esaslarını belirlediği, devletin ülke içerisinde gerçekleşen her türlü işleyişi tekelinde topladığı ağ yapısıdır. Her türlü anlaşmazlık, ortaklık veya yetki devri konuları bürokratik yollarca belirlenir. Bu tip ağ yapılarını sıklıkla işlem garantili paylaşım gerçekleştirmek isteyen kişi ve kurumlar tercih etmektedir. Üçüncü güven mimarisi olan aracılı yapı; sosyal normlar veya merkezi otoriteleri kapsamayan, bunların yerine aracı kurumlar

üzerinden işlemlerin yürütüldüğü yapılardır. Bu tip yapılarda araçlar, tarafları bir araya getirerek işlemlerin yapılmasını sağlamaktadır. Aracı üzerinden işleyen yapıların tercih edilmesinin asıl nedeni güvendir. İşlemlerde aracılık hizmeti sunan yapı, her iki taraftan geçici olarak vekâletini üstlenerek olası bir aksaklık durumunda her iki tarafın kayıplarını karşılamakla yükümlüdür. Son ağ yapısı olan blok zinciri, modern güvencesiz güven mimarisidir. Hiçbir otoriteye bağlı olmayan bu yapı özünde çevrimiçi bir kayıt defteridir. Bu aşamada blok zincirini diğer güven mimarilerinden farklı kılan da otoriteye tabi olmayan, kendi iç dinamikleriyle kendi güvenliğini sağlayan bir yapı içermesidir. Bu yapı üç temel unsur üzerinde şekillenmektedir. İlk unsur olan “özerklik” zincir ağı üzerinde tutulan, istisnasız her veriyi güvenli bir şekilde istenilen yere aktarabilme ve gereksinimler çerçevesinde güncelleyebilmeyi içermektedir. Yapılan tüm bu işlemler için ne merkezi bir otoriteye ihtiyaç duymakta ne de merkezi bir otoritenin izni gerekmektedir (Lin ve Liao, 2017: 653). Gerçekleşen her bir işlem, eşten-eşe olarak tabir edilen blok zinciri ağı üzerinde bulunan çok sayıda bilgisayar arasında eş zamanlı bir kopya yaratıp saklama yöntemine dayanmaktadır. Gerçekleşen her bir işlem, istisnasız ve hatasız bir şekilde ağ üzerinde bulunan kullanıcıların kendi kayıtlarında kalmaktadır. İkinci unsur olan “şeffaflık” ise, zincir ağı üzerinde bulunan verilerin kayıtlarının “düğüm” olarak adlandırılan, her bir kullanıcı için şeffaf olup istenildiği zaman verilerin geriye dönük olarak doğrulanabilmesidir. Sahip olduğu bu şeffaflık özelliği sayesinde bir blok zinciri ağı güvenilir kabul edilmektedir (Ünal ve Uluyol, 2020: 168). Üçüncü unsur olan “değiştirilemezlik” sayesinde bir blok zinciri ağı üzerindeki veriler, hiçbir şekilde değiştirilemez veya silinemez (Tanrıverdi vd., 2019: 205). Bu sayede, yapılan her kayıt sonsuza kadar saklanabildiği gibi, tüm siber tehditlere karşı tamamen güvenlidir. Blok zinciri ağ yapısı, sahip olduğu bu üç unsurdan dolayı dünya genelinde kullanıcılar tarafından son derece güvenli bulunmaktadır. Yine başta kriptografi uzmanları olmak üzere, kullanıcılar üzerinde sağladığı güvenin bir sonucu olarak blok zinciri

ağı üzerinde geliştirilen birçok uygulama her geçen gün artmakta ve kullanılmaktadır. Bunlarla beraber “şimşek ağ (Lightning Network)” olarak adlandırılan başta bir kavram daha başlıca blok zinciri ağlarına dâhil olmuştur. Şimşek ağ teknolojisi, bir blok zinciri ağı üzerindeki ödeme ve ölçeklendirme gibi işlemlerin hızlandırılmasını sağlayan, yardımcı bir ağ teknolojisidir. Şimşek ağ teknolojisi, blok zinciri ağları üzerindeki iş yükünü hafifleterek daha hızlı işlem yapabilir hale getirmiştir (Lightning Network, 2016).

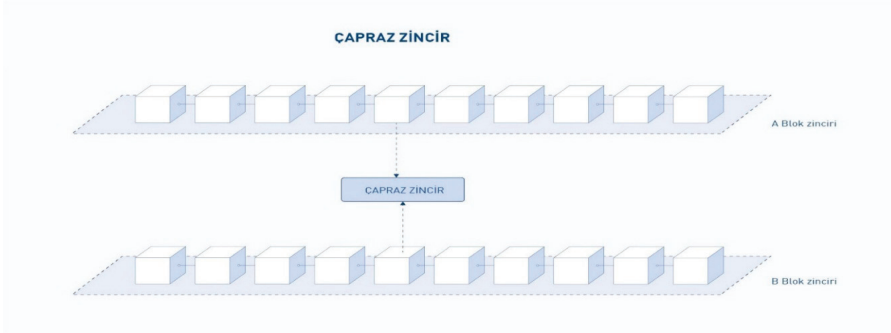
3. Çapraz Zincir

Modern, güvencesiz güven mimarisinin potansiyelini şimdiden fark etmiş birçok sektör ve endüstri dalı vardır. Blok zinciri üzerinde geliştirilmiş yapıların maliyet, şeffaflık ve güvenlik noktasında sağladıkları verimden istifade etmek isteyen birçok endüstri dalı bu teknolojiyle ilgilenmeye başlamıştır (Fairfield, 2005: 1047-1048). Ancak blok zinciri mimarisi üzerinde şekillendirilmiş uygulamaların sektör, uygulama ve iş dallarının çeşitliliği nedeniyle ihtiyaç ve amaçlarına yönelik birbirinden farklı yönetim modellerinde kodlanmış olmaları da yeni bir sorunu gündeme getirmiştir. Bu sorun, blok zincirleri arasında kesintisiz bir şekilde eş güdümü sağlayarak farklı endüstriler ve iş planları arasında aracılık ederek birbirinden farklı blok zinciri mimarilerini tek bir zincir gibi çalıştıracak bir ağ mimarisi gereksinimidir. Bu aşamada çözüm olarak yeni bir zincir teknolojisi olan “çapraz zincir teknolojisi” sunulmuştur. Çapraz zincir teknolojisinin amacı; farklı blok zinciri ağları üzerinde bulunan uygulamalardan gelen veri ve bilgileri, belirli zincir protokolleri üzerinden iletmek ve ağlar arasında karşılıklı mutabakatı sorunsuz bir şekilde gerçekleştirerek sürekliliği devam ettirmektir (Yu vd., 2020: 2; Hoffman, 2014). Yani çapraz zincir ağları; farklı fikir ve uzlaşma protokolleri üzerinde çalışmak üzere kodlanmış, blok zincirleri ağları arasında ortak fikir ve uzlaşma protokollerini benimseyecek şekilde güvenlik ve devamlılığı sağlayan köprü ağlardır. Her ne kadar basit

bir işlevi varmış gibi gözükse de, farklı blok zincir ağları arasında etkileşimi ve yönetişimi sağlamak düşünüldüğü kadar kolay bir iş değildir.

3.1. Çapraz Zincir Ağ Yapısı

Blok zincirleri, yönetim doğaları gereği karmaşık ve sarmal yapılardır. Zincir üzerinde bulunan blokların her bir düğümü için sadece tek bir doğrulama düğümü yetmemekle birlikte, birleştirilmek istenilen zincirlerden tamamen bağımsız, yani merkeziyetsiz bir doğrulama ağına daha ihtiyaç duyulmaktadır. Bu yüzden çapraz zincir ağları günümüzde her ne kadar kullanılmaya başlansa da uygulamaya konulan projelerin çoğu yoğun bir geliştirme/iyileştirme aşmasındadır (Deng vd., 2018: 146-148). Dahası, çapraz zincir ağları doğaları gereği daha ölçeklenebilir paralel doğrulama ağları üzerinden çalışmaya uygundur. Bu sebeple ağırlıklı olarak merkeziyetsiz finans, borsa ve token takas işlemleri yapan borsa hizmetleri sunmaktadır. Yine doğaları gereği zincir üzerinde bulunan blokların sayıları arttıkça verimlilik ve performans da eşzamanlı olarak yükselmektedir (Jiang vd., 2019: 16-17). Ölçeklenebilir ve dağıtık yapısı sayesinde zincir üzerinde gerçekleşen işlemler blok zincirine göre daha basit gerçekleşmektedir. Akıllı sözleşmeleri gereği, tamamen eşzamanlı iletişime dayalı bir protokol kullanmadıkları için, bir dereceye kadar merkezi sayılmaktadırlar. Veri yönetim ve iletim alanlarında sahip oldukları verimlilik sayesinde, zincirler arası ticari antlaşmaları tek taraflı olarak hızlı bir şekilde gerçekleştirmektedir. Bu da finans ve borsa hizmeti veren kurumların çapraz zincir teknolojisini tercih etmelerinin bir diğer nedenidir (Herlihy vd., 2021: 1-2).



Şekil 2. Güvencesiz Güven Mimarisi

Kaynak: under.orosfeoconskee.tk

Şekil 2 incelendiğinde iki farklı protokol çerçevesinde kodlanarak oluşturulmuş blok zincirine köprülük/ aracılık sağlayan çapraz zincir ağ modeli görülmektedir. Daha önce aktarıldığı gibi çapraz zincirler, farklı blok zincirleri arasındaki veri ve bilgilerin aktarılmasında kullanılmaktadır. Çapraz zincir mimarileri, mutabakat veya aktarım kanalları için üçüncü bir tarafa ihtiyaç duymamaktadır. Zincirler arası transfer ve etkileşimlerde eğer üçüncü bir tarafa ihtiyaç duyuluyor olsaydı, bu durum blok zincirinin altında yatan felsefeye ve gereksinime ters bir durum oluşturuyor olurdu. Bu anlamda düşünüldüğünde çapraz zincir de, öncülü olan blok zinciri teknolojisi gibi tamamen merkeziyetsiz bir yapıya sahiptir. Günümüzde, başta zincirler arası transfer ve köprü yapılarının etkileşimi, yönetişimi ve güvenliği gibi alanlarda, başta Avalanche, Cosmos, Wanchain ve Polkadot gibi projeler çeşitli çalışmalar yürütmektedir. Bu proje uygulayıcıları sayesinde başta DeFi (Merkezi Olmayan Finans) kuruluşları dijital varlıkları birbirleri arasında kolayca transfer edebilmektedir.

4. Mutabakat, Bizans Generalleri Problemi ve Bizans Hata Toleransı

Mutabakat, dağıtık yapıdaki ağ ve yazılım teknolojilerinin en büyük sorunlarından birisidir. Geçmiş blok zinciri teknolojilerinden çok daha öncesine dayanan mutabakat sorunu, zaman içerisinde değişik teoriler içerisinde ele alınmıştır. Bunların en çok bilinenleri yemek yiyen filozoflar, fırıncı algoritması, uyuyan berberler ve sigara içenler problemleridir. İsmi geçen bu problemler, güvenilirlik ve hata toleransını içinde barındıran sistem tasarımlarında kullanılmaktadır (Dursun, 1993: 64). Blok zinciri, içeriğinde bulundurduğu tüm veri ve bilgileri paydaşlarında barındırmaktadır. Süregelen blok zinciri yapısı, paydaşlar üzerinden devam ettiği için de mutabakatlara engel olabilecek anlaşmazlıklar, ihanetler ve hatalı işlemler olabilir. Bir ağ yapısı üzerinde bulunan paydaşlara ilişkin bu tip anlaşmazlıkları ve bu duruma bağlı oluşabilecek problemleri Akkoyunlu vd. 1975 yılında yayınladıkları “Some Constraints and Tradeoffs in the Design of Network Communications” adlı makalelerinde ele almışlardır. İlerleyen senelerde, dağıtık bir ağ mimarisi üzerinde mutabakat ve paydaşlara bağlı olarak yaşanabilecek sorunları Lamport, vd. 1982 yılında yazdıkları “The Byzantine Generals Problem” adlı makalede “Bizans Generalleri Problemi” ve “Bizans Hata Toleransı” teoremlerini tanımlayarak literatüre kazandırmışlardır. Lamport; karar verici, merkezi bir otoritenin olmadığı bir durumda taraflar arasındaki güvenin nasıl ve ne kadarlık bir yanılma payıyla oluşturulabileceğini ele alarak, kabul edilebilir bir hata payı üzerinden bir çözüm algoritması üretmiştir. Makalede geçen senaryo daha kolay anlaşılması için Şekil 3 üzerinde anlatılmıştır.



Şekil 3. Güvencesiz Güven Mimarisi

Kaynak: phemex.com

Aynı şehri ele geçirme emri alan bir grup general ve emirlerindeki orduları, şehri farklı cephelerden kuşatmışlardır. Kuşatma farklı cephelerden gerçekleştirildiği için generaller arasında bir hayli mesafe bulunmaktadır. Generallerin bazıları, aldıkları emire rağmen şehri ele geçirmeyi istememektedirler. Bu aşamada ortak bir karar üzerinden bir mutabakatın sağlanması için generallerin hemfikir olması gerekmektedir. Yani kesin bir mutabakat, başarılı bir saldırı için şarttır. Problem, generallerin birbirlerinden uzak olmaları, hepsinin aynı fikirde olmaması, kendi içlerinde bir hain barındırmaları ve kendi aralarındaki mesajların aslına uygun iletilip iletilmediği üzerine kuruludur.

Problemi, veri ve bilgi iletiminin yürütüldüğü ağ yapısı üzerinden düşünürsek; merkezi bir karar alıcı yapı olmadan, sadece hatalı, yanıltıcı ve eksik bilgilerin olabileceğini göz önünde tutarak, katılımcıların çoğu tarafından bir mutabakata varılamaması durumunu kapsamaktadır. Hem çoğunluğun kabul ettiği görüşleri yansıttığı için, hem de blok zinciri temelli kodlandığı için Bitcoin, ağ üzerinde işlem

yapan kullanıcıların ortak mutabakatıdır diyebiliriz. Blok zinciri ağı üzerinde iletilen verinin alıcıya ulaşmaması veya hatalı ulaşması durumunda bile mutabakat sağlanabilmesi noktasında kabul edilen çözüm ise “Bizans Hata Toleransı” olarak tanımlanmaktadır. Bizans hata toleransı, Bizans generalleri problemi çözümünde olası hataları minimuma indirgeyerek mutabakata varılması için geliştirilmiş bir yöntemdir. Böylelikle Satoshi Nakamoto, blok zinciri çözümü ile dağıtık ve çoğunluğun mutabakatına dayalı olarak çalışan ve merkezi bir otoritenin sağlamasına ihtiyaç duymayan bu tasarımı, yani “iş kanıtı” tasarımını kullanmıştır. Geçmiş Nakamoto’dan ve Bitcoin’de eskiye dayanan iş kanıtı, bir bilgisayarın belirlenen bir hedef için çalıştığını gösterdikten sonra sağlamasını yapan bir yöntemdir. İş kanıtı kavramı, ilk kez istenmeyen e-postalarla mücadele etmek için Cynthia Dwork ve Moni Naor adlı iki bilgisayar bilimci tarafından 1992 yılında geliştirilmiş bir protokoldür (Naor ve Dwork, 1992: 139). Bilgisayarlar, teknik donanımları sayesinde kendilerine verilen işlemleri çok kısa sürelerde gerçekleştirebilirler. Örneğin e-posta göndermek için programlanan bir bilgisayar, kısa süre içerisinde bir başka bilgisayara milyonlarca e-posta göndererek karşıda bulunan bilgisayarı iş göremez hale kolayca getirebilir. Bu tip sabotaj faaliyetlerinin önüne geçmek adına iş kanıtı yöntemi, e-postaları gönderen bilgisayarın bir süre sonra gönderdiği e-postaları doğrulamasını, yani yaptığı işi kanıtlamasını ister. Bu aşamada gönderdiği e-postaların doğrulamasını yine kendisi yapan bilgisayar bu işlem içinde enerji ve zaman harcayacak ve amacı dışında e-posta gönderemeyecektir. Bu şekilde iş kanıtı sağlanmış olacaktır (Liu vd. 2006: 2-3). İş kanıtı yaklaşımı sayesinde Nakamoto “Bizans Generalleri” problemine kavramsal olarak alternatif bir çözüm üretmiştir (Antonopoulos, 2017: 4). Blok zinciri tabanlı olarak sunulan bu çözüm yoluna “Nakamoto mutabakatı” demek doğru olacaktır. Şüphesiz Nakamoto mutabakatının insanlığa ettiği en büyük hediye, kurumsal aktörlerin dâhil olduğu güven mimarilerini bitirmesidir. Blok zinciri üzerinde yapılan bir işlemin fiziksel

dünyada karşılığının olduğunu bilmek, kurumsal bir otoriteye ihtiyaç duymadan paydaşlar arasındaki ilişkiye, yani blok zincirine güvenmek demektir.

5. Blok ve Çapraz Zincir Mevcut ve Gelecek Uygulama Alanları

Çalışmanın önceki bölümlerinde bahsedildiği gibi blok zinciri teknolojisi, günümüzde ağırlıklı olarak “Coin” ve “Token” olarak adlandırılan sanal paralarda kullanılmaktadır. Türünün ilk örneği olan “Bitcoin” ise herkes tarafından bilinen bir sanal paradır. Bu makalenin hazırlandığı sırada on binden fazla sanal para birimi bulunmaktadır. Bu sanal paraların toplam piyasa değeri 2 trilyon doların üzerindedir (CoinMarketCap, 2022). Sanal paralar dışında blok ve çapraz zincir teknolojileri, güven ve mutabakat gereksinimi gereken konularda sıklıkla kendisine kullanım alanı bulmakla birlikte; hızlı transfer, doğrulama, şeffaflık ve mutabakat gerektiren farklı sektörlerde kullanılması öngörülmektedir. Araştırmanın bu bölümünde blok ve çapraz zincir teknolojilerinin gelecekte kullanılması muhtemel alanlarına değinilecektir.

5.1. Nesnelerin İnterneti (Iot)

Fiziksel veya sanal olarak tanımlanması mümkün her türlü nesnenin; uygun girdi ve çıktı donanımı ve akıllı ara yüzü sayesinde internet ve internet benzeri bilgi ağlarıyla bütünleşerek çalışmasını ve bu süreç boyunca da bir takım standart ve ileri düzey protokolle yönetilmesi, nesnelerin interneti (Iot) olarak tanımlanmaktadır (Kranenburg, 2008). Nesnelerin interneti sayesinde, internete bağlı cihazlara uzak coğrafi konumlardan erişmek ve erişilen cihaza görev tanımlamak mümkündür. Bu entegrasyon sayesinde, verilen görevin takibi de anlık olarak yapılabilmektedir (Al Fuqaha vd., 2015: 2347; Atzori vd., 2010: 2787). Nesnelerin interneti sayesinde, günlük hayatımızda kullandığımız nesnelere, yine kendisi gibi internete bağlı diğer nesnelere

ile veri alışverişi yapmakta ve ortaya işlenmeyi bekleyen devasa bir veri kütlesi çıkartmaktadır. Özellikle makine öğrenmesi, büyük veri ve yapay zekâ gelişimi gibi alanlarda fayda sağlayan, nesnelere internetiyle birlikte elde edilen veriler, anlamlı bir hale getirilerek bilgiyi oluşturmada ve nihai sonuç olarak otonom bir akıllı dünyayı yaratma konusunda kilometre taşı görevi görmektedir.

Günümüzde, farklı alanlarda üretim gerçekleştiren birçok elektronik aygıt bulunmaktadır. Bu üreticiler, kendi marka ürün grupları için teknolojik aygıt üretmektedirler. Üretilen bu teknolojik cihazların birçoğunda da nesnelere internetini destekleyecek donanım ve ara yüz yazılımları bulunmaktadır. Bu kadar farklı üretici ve ürünün olduğu endüstride, nesnelere interneti için ne yazılım olarak, ne de donanım olarak bir standart bulunmamaktadır. Her üretici, kendi ara yüz yazılım ve donanımı üzerinden akıllı cihazlar geliştirmektedir. Yani her üretici, kendi uzak bağlantı servis ve yazılımını kullanmaktadır. Blok zinciri teknolojisi sayesinde, yazılım ara yüzleri standart bir yapıya kavuşabilir. Bu sayede başta yazılım güncellemeleri olmak üzere, tüm yazılımlarla ilgili konular tek merkezden ele alınarak yönetilebilir. Bu yöntemle blok zinciri teknolojisinin en büyük avantajı olan veri bütünlüğü ve veri entegrasyonu verimli olarak kullanılabilir. blok zincirinde yer alan akıllı sözleşmeler, İot aygıtlara entegre edilerek bu aygıtların kendi akıllı sözleşmeleri olabilir. Böylelikle alanda bir standart oluşturulabilir. Bu sayede hem güvenlik sorunları ortadan kaldırılabilir hem de kişi veya kurumlara sağlanan erişim koşulları detaylı bir şekilde yapılandırılarak rol ve yönetim karmaşaları engellenebilir.

5.2. Kitleli Fonlama Hareketleri

İnternetin ve bağı alt teknolojilerinin gelişmesiyle birlikte, hayatımıza farklı çözümler ve olanaklar dâhil olmuştur. İnternet kullanıcılarının ortak paylaşımlarıyla yarattıkları olanakların başında gelen Web 2.0

teknolojisi, kitlesel fonlama anlayışını hayatımıza sokmuştur (O'Reilly, 2009: 24-28). İşletme veya bireysel girişimlerin; başta ürün, herhangi mevcut duruma ait alternatif çözüm veya hizmet üretip satmak için internet üzerinden açık çağrı yaparak toplulukların üretilen çözüm veya hizmete ilişkin fikirlerini, isteklerini öğrenmeye çalışmasıdır. Sıklıkla bu tür organizasyonların sonucunda onayı alınan ürün, çözüm veya hizmetin sunulabilmesi için karşılıksız bedel toplanmaktadır (Kleeman, 2008: 5-6). Blok zinciri üzerinden başta girişimciler olmak üzere kitlesel fonlama yöntemi ile finans desteği aramakta olan birçok işletme ve kuruluşa hızlı bağış yapılabilir. Üstelik bu bağışlar doğrudan gönderici ve alıcı arasında gerçekleşeceğinden aracılara ödenecek komisyon ücretleri de ortadan kalkacaktır. Bu sayede bağış hedefi koyarak başlayan projeler, hem transfer hızlarından dolayı çok kısa zaman dilimlerinde gereken bağışları toplayacak, hem de aracılara komisyon ücretleri ödemedikleri için hedef bağış tutarlarını çok kısa zamanda ulaştıracaklardır. Yine benzer şekilde sivil toplum örgütleri, sosyal sorumluluk projeleri ve bireysel bağış kampanya sahipleri blok zinciri üzerinden komisyonsuz şekilde bağış ve fonlarını kolayca toplayabileceklerdir.

5.3. Tedarik Zinciri Yönetimi

Tedarik zinciri; tedarikçileri, lojistik hizmeti sunanları, üreticileri ve perakendecileri kapsayan ve bu paydaşlar arasında mal, hizmet, hammadde ve bilgi akışının süregeldiği bir döngüdür (Kopczak, 1997: 227). Tedarik zinciri yönetimi ise; üretimi biterek mamul olmuş ürünün nihai kullanıcı veya müşteriye ulaştırılmasına yönelik yürütülen ağ faaliyetlerinin koordinasyon ve yönetimidir. Bu süreç içerisinde hammadde, üretim, montaj, sipariş ve sipariş takibi, ulaştırma, depolama ve dağıtım gibi çok önemli iş fonksiyonlarının yönetimi sağlanmaktadır (Hervani vd., 2005: 331). Ayrıca hatasız işleyen bir tedarik zinciri yönetimiyle işletmeler, pazar üzerindeki rekabet güçlerini arttıracak yeni stratejilere daha fazla vakit

ayırabilmektedirler (Tan vd., 1998: 2-3). Ancak işletmeler için önemli olan tedarik zinciri yönetiminin geleneksel yapısı gereği, yapısal bazı aksaklıkları bulunmaktadır. Doğası gereği ağırlıklı olarak kendi iç akış dinamikleriyle ilgilenen bu süreçte, mevcut dinamikler her aşamada karışık entegrasyon ve bilgilendirme süreçleri ortaya çıkartmaktadır. Tüm bunlar da işletmelere maliyet ve verimlilik noktalarında çeşitli handikaplar yaratmaktadır (Usta ve Doğanekin, 2017: 74). Konuya tedarik zinciri yönetimi konusundan bakıldığında blok zinciri teknolojisi, sahip olduğu anlık veri iletimi ve şeffaflık sağlama özellikleri sayesinde; başta hatalı sevk işlemleri, olası gecikmeler, ön görülemeyen olumsuzluklar ve bunlara bağlı olarak oluşabilecek depolama ve taşıma maliyetlerinin önüne geçerek istenilen etkinlik ve verimliliği sağlayabilecek altyapıdadır. Yine orijinallik gerektiren ürünlerde, blok zinciri sayesinde ürünün imalat aşamasından son kullanıcı satış sürecine kadar olan tüm süreç, şeffaf ve değiştirilemez bir şekilde kayıt altına alınarak kolayca takip edilebilir. Bu sayede, ürünün orijinallik ve menşesine ilişkin tüm şüpheler ortadan kaldırılabilir ve ürünün orijinalliği doğrulanabilir. Üretimin, sevkiyatın ve miktarın her aşamada şeffaf olarak denetlenebilmesi sayesinde oluşan alıcı- satıcı güveniyle başta haksız kazanç sağlama, stokçuluk ve karaborsacılık gibi meşru olmayan faaliyetlerin kolayca önüne geçilebilir. Son olarak kusursuz işleyen bir blok zinciri takip envanter sistemi, geri dönüşüme tabii olan atıkların takibini kolaylaştırarak çevresel kaygıların önemsendiği yeşil tedarik zinciri kavramına da hizmet edebilir.

5.4. Siber Güvenlik

İlerleyenteknolojiylebirliktehergünyenikavramlarlakarşılaşmaktayız. “Siber Uzay” kavramı da bunlardan birisidir. İlk kez Amerikalı bilim kurgu yazarı William Gibson tarafından 1982 yılında yayımlanan “Burning Chrome” adlı kitapta geçen bu kavram, ilerleyen senelerde çevrimiçi küresel bilgi ağı olan interneti ve içinde elektronik ağ-ortam bulunan tüm yapıları tanımlamak için kullanılmıştır. Günümüzde siber

uzay kavramı, akademik anlamda dört çerçevede ele alınmaktadır. Bunlar; fiziksel altyapı, mantıksal yapı, bilgi ve insandır. Siber güvenlik unsurunu oluşturan bu kavramlardan fiziksel altyapı unsuru; ağ kabloları, uydular, ağ yönlendirme anahtarları (switch) ve diğer bilişim teknolojisi cihazlarını kapsamaktadır. Mantıksal yapı ise akıllı telefon işletim sistemi ve uygulamaları, bilgisayar işletim sistemleri ve yazılımları kapsamaktadır. Bir diğer unsur olan bilgi, bilgisayar ve bilgisayar bileşenleri arasında belirli iletişim protokolleriyle iletilen, fotoğraflar, metinler ve dosyalardır. Son unsur olan insan ise, tüm bu sistemler üzerinde bilgiyi kullanan, yayan, manipüle eden ve bu vasıta ile iletişimi sürdüren beşeri canlılardır (Clemente, 2015: 163-164). Siber uzay içerisinde tutulan, işlenen, dağıtılan ve kullanılan her türlü verinin parça ve anlam bütünlüğünün korunması, başka taraflarca sabote edilmesi veya istem dışı el değiştirmesinin önlenmesi, siber güvenlik olarak tanımlanmaktadır (Craig vd., 2014: 14-15). Bir diğer tanıma göre ise siber güvenlik; bilgi-iletişim ağlarında bir topluluğun veya ulusun bilgilerini, varlığını ve devamlılığını korumak için yine bilgi iletişim ağlarında yapılan her türlü koruma ve önlem faaliyetlerinin tümüdür (Canongia ve Mandarino, 2014: 60-61). Görüldüğü üzere siber güvenlik kavramı hem teknik, hem de beşeri yönleri olan bir kavramdır. Bu da tıpkı blok zinciri teknolojisi gibi inter disiplinler bir bilimsel yaklaşım anlayışıyla kavranıp incelenmesi gerekliliğini ortaya koymaktadır. Günümüzde, siber güvenlik gibi kavramlar hayatımıza dâhil oldukça veri ve bilgi güvenliği gibi kavramlar daha da önem kazanmaktadır. Freedom House isimli Amerika menşeli bir sivil toplum organizasyonunun “Freedom On The Net 2020” isimli raporuna göre internet üzerindeki veri ve bilgilerin %90’a yakını üçüncü taraflarca çevrimiçi olarak takip edilip, izlenmektedir. Konuya bu açıdan bakıldığında, hali hazırda noktadan noktaya güvenli veri ve bilgi iletişim ve paylaşım protokollerinde revizyona gidilmesi siber güvenlik anlamında kaçınılmazdır. Özellikle günümüzde, verilerin iletişimi veya noktadan noktaya aktarımında VPN veya SSL gibi internet üzerinden şifrelenmiş güvenli iletişim

protokolleri kullanılmaktadır. Fakat bu protokoller merkezi bir yapının ya üzerinde ya da birden çok merkezi yapının arasında çalışmaktadır. Blok zinciri teknolojisinin bir nimeti olarak, tamamen merkeziyetsiz ve anonim bir yapıda VPN hizmeti verilerek normal internet ağı üzerinden gerçekleşen ağ trafiği, hiçbir log kaydı olmadan eşler arası ve anonim bir şekilde tüm veri oluşturucular arasında gerçekleştirilmesi sağlanabilir. Yine blok zinciri teknolojisinin “Hash” adı verilen algoritmaları sayesinde ağ üzerinden geçen her türlü veriyi uçtan uca şifrelemek, saklamak ve dağıtmak mümkündür. Bu sayede ağ üzerinde gerçekleştirilecek tüm iletişim protokolleri, blok zinciri teknolojisinin merkeziyetsiz veritabanı özelliği sayesinde dışarıdan hiçbir müdahale ve riske maruz kalmadan eşler arasında güvenli bir şekilde kullanılabilir.

Blok zinciri teknolojisinin siber güvenlik alanında bir diğer olası kullanım alanı da DNS’ler olabilir. Bilindiği üzere DNS’ler internet ağında sınıflandırma, bölme ve adresleme işlemlerini yürüten, hiyerarşik yapıda çalışan adresleme/adlandırma sistemleridir. Daha basit bir tabirle, tarayıcıya girilen erişim adresini, bilgisayar tarafından anlaşılabilir bir IP protokolüne çeviren rehberdir. Bugün kullandığımız DNS yapıları, internet teknolojisiyle yaşıt olduğu ve tek bir merkezi otorite tarafından atandıkları için olası arıza, bakım ve yönetim noktasında tek elden kontrol edilmektedir. Bu yüzden başta DDOS saldırıları ve artan internet trafiklerinden olumsuz etkilenmekte, yavaşlamakta ve hatta tamamen hizmet dışı kalabilmektedir. Blok zinciri tabanlı olası DNS çözümleri, başta eşten eşe çalışma yöntemiyle blok zinciri üzerine kayıt edilen alan adlarının yedeklenmesini, yönetilmesini ve çözümlenmesini tek merkezli bir yapıdan çıkartıp birden çok eş zamanlı çalışan dağıtık bir yapıya dönüştürülebilir. Bu sayede blok zinciri üzerine kurulu DNS’ler olası siber saldırı ve artan internet trafiklerinden etkilenmeden çalışmayı sürdürebilir. Son olarak da blok zinciri üzerinde projelendirilecek merkeziyetsiz depolama çözümlerinden bahsetmek mümkündür. Özellikle son yıllarda küresel

olarak bilgisayar ve cluster mimarideki verilere karşı yapılan fideye amaçlı siber saldırıların artmasıyla birlikte, başta hükümetler ve işletmeler veri güvenliklerini sağlamak için alternatif arayışlara girmişlerdir (Sharma ve Shanker, 2002). Bu noktada veriyi (yedekler dâhil) tek bir depolama merkezinde tutmak yerine, veriyi parçalar halinde bir blok zinciri ağı veya birden çok blok zinciri ağı üzerinde kriptografik metotlarla şifreleyerek tutmak daha işlevsel ve güvenli olacaktır. Yakın gelecekte, tıpkı torrent veya emule dosya paylaşım programlarının çalışma prensibindeki gibi, veri güvenliklerini sağlamak isteyen kurum ve kuruluşlar; verilerini blok zinciri üzerinde parçalar halinde saklama yoluna giderek, kendi siber güvenliklerine kendilerinin sağlaması oldukça olasıdır. Hatta torrent, emule vb. popüler dosya paylaşım programlarında olduğu gibi veriyi sürekli dağıttık bir zincir ağ yapısı üzerinde saklamak, gerektiği zaman erişime açmak gibi P2P mantığıyla çalışan yollara gidilmesi ihtimal dahilindedir. Blok zinciri teknolojisiyle siber güvenlik alanında yapılabilecekler elbette burada sayılanlardan çok daha fazlasını içermektedir. İlerleyen zamanlarda ülkelerin; kendi blok zinciri tabanlı ulusal siber güvenlik modellerini ve stratejilerini yaratarak, küresel anlamda siber riskleri azaltma yoluna gitmeleri de bir hayli olasıdır.

5.5. Büyük Veri ve Öngörüleme (Tahminleme)

Yazının icadından başlayarak, bilgisayarlın gündelik hayatın her alanında kullanmasıyla birlikte, çeşitli yöntem ve metotlarla elde edilen veriler zaman içerisinde birikerek “Büyük Veri” kavramını oluşturmuştur. İlk olarak 1990’larda başta ekonomik toplantılar olmak üzere ortaya çıkan bu kavram zaman içerisinde bilimsel toplantıların da konusu olmaya başlamıştır. 2010 yılına gelindiğinde ise resmi olarak literatüre girmiş ve birçok çevre tarafından tanınmaya başlanmıştır (Manyika vd., 2011). Büyük veri kavramı, günümüzde bu kadar ilgi görmesine rağmen, genel kabul görmüş bir tanımı bulunmamasıyla birlikte, yaygın olarak kabul gören tanımı “alışıla gelen veri işleme

metotlarıyla işlenerek anlam kazandırılmayan verilerin, yüksek hacimli bir şekilde oluşturdukları ham yığınlardır” şeklindedir (Kaur ve Sood, 2017: 1-2). Daha sade bir tanıma göre ise; “basit bir şekilde irdelenemeyen ve işlenip bilgi haline dönüştürülemeyen verilerdir” (Fisher vd., 2012: 53). Büyük verinin günümüzde astronomi, finans, sağlık hizmetleri, nesnelere interneti, yaşam bilimleri, sosyal medya, telekomünikasyon, lojistik ve kamu hizmetleri gibi farklı ve sürekli veri birikimi sağlayan kaynakları bulunmaktadır (Bhadani ve Jothimani, 2016: 7). Bu veriler, çeşitli yöntem ve metotlar ile işlenerek anlamlı hale getirilip “bilgi” haline gelmektedir. Hatta bilgi kavramı Portsmouth Üniversitesinde fizikçi olarak çalışan Dr. Melvin Vopson’a göre maddenin beşinci hali bile olabilir. Dr. Melvin Vopson, tüm temel parçacıkların bilgi depoladığı ve bu bilgini fiziksel bir kütlesi olduğu yönündeki çalışmalarını sürdürmektedir. Yine Dr. Melvin Vopson’ın bir diğer iddiası, bilginin evrenin temel yapı taşı olduğu ve fiziksel bir kütlesi olduğu yönündedir (Vopson, 2019: 9).

Öngörüleme, bir diğer deyişle tahminleme ise; yordama ve doğruyu yakınsamaya yönelik olarak elde edilen veriler ışığında, gelecekte olması muhtemel olayları, geçmişteki veriler sayesinde modelleyerek tahmin etme veya olası en yakın senaryoda bilmeyi amaçlamaktadır. Ağırlıklı olarak borsa-finance, üretim, envanter ve personel seçimi gibi konularda öngörüleme modelleri kantitatif değerler üzerinden hesaplanmaktadır. Şimdiye kadar sadece işletmelerin kendi bünyelerinde, kendileri ve ilgilendikleri pazarlar için büyük veri gibi veri yığınlarını işleyerek öngörüleme elde ettikleri analizler, blok zinciri teknolojisiyle son kullanıcılarının kolayca erişimine açılabilir. Makine öğrenmesi algoritmalarının işlediği veriler sayesinde spordan finansa, seçim sonuçlarından şans oyunlarına ve hatta bilimsel yayınlara kadar birçok alanda kaliteli veriler analiz edilerek anlamı bir hale getirilip öngörülebilir bilgiler elde edilmesi bunun da blok zinciri tabanlı küresel merkezi olmayan öngörüleme modelleri hizmeti veren pazarlara dönüştürülmesi oldukça olasıdır. Yakın gelecekte gerçekleşme

ihtimali olan bu küresel öngörülemez pazar hizmeti sayesinde, veri yönetişiminin yeni bir boyuta geçmesi oldukça olasıdır.

5.6. Merkeziyetsiz (Dağıtık) İnternet

Bilindiği üzere internet birçok bilgisayar sisteminin TCP/IP protokolü ile birbirine küresel çapta bağlandığı bir iletişim ağıdır. Bu ağ sayesinde bizler her türlü bilgiye hızlı, kolay ve ucuz bir şekilde ulaşabilmekteyiz (Parlak, 2005: 10). İlk olarak 1950'lerde paket ağ olarak tabir edilen Amerikan kamu binalarında küçük ve yerel ağlarda kullanılmaya başlanmıştır. 1960'ların başında Amerika Birleşik Devletleri Savunma Bakanlığı tarafından organize edilen çalışmalar neticesinde ilk ağ protokolü olan ARPANET, yani ilk internet hayata geçirilmiştir (Atta, 2018: 12-13). 1990'da Avrupa Nükleer Araştırma merkezi (CERN); bugün ev, işyeri ve mobil cihazlarımızda kullanmaya başladığımız internetin ilk hali sayılabilecek World Wide Web (www) kavramını icat etmiştir (Castells, 2003: 7). Bu yıllar, internetin ilk defa belirli bir grup veya zümre dışında kamuya açıldığı, dönemin imkânları dâhilinde imkân sahiplerinin kullandığı dönemdir. Bu dönemde web siteleri ağırlıklı olarak text (alt metin) metinlerden ibaretti. Bununla birlikte web siteleri içerikleri sadece internet erişimi olan çok az sayıda uzman tarafından koordine edilmekteydi. Bu özellikleriyle ilk web ağı için; salt okunur, statik bir yapıya sahipti demek şüphesiz doğru olacaktır. Günümüzde bu dönem için literatürde Web 1.0 tanımlaması yapılmaktadır. Mevcut kullandığımız ve hayatımıza sosyal ağ kavramını da sokan Web 2.0, sadece kullanıcıların bilgi almak yerine kendilerinin de bir takım bilgiler oluşturup internet ortamında yayımlayabildikleri dönemin başlangıcıdır. Yapılan bilgi paylaşımı ile birlikte oluşan etkileşim, interaktiflik ve daha işbirlikçi içerikleri görselleştirme ve değerlendirme gibi imkânların sunulduğu bir yapıyı hayatımıza sokmuştur (Ajjan ve Hartshorne, 2008: 71-72). Web 3.0, blok zinciri üzerinden çalışan merkeziyetsiz uygulamaları tanımlamak için kullanılmaktadır. İçeriğinde; dosya paylaşımından

kripto para birimlerinin transferlerini sağlayabilen protokolleri barındıran bir yapıdır. Mevcut internet sisteminin kimlik kanıtlamaya gerek duymayan bir türü olarak adlandırılabilen bu yapı, blok zinciri ve çapraz zincir teknolojisi düşünüldüğünde muhtemelen yakın gelecekte ara geçiş dönemi olarak anılacaktır. Tüm bu özelliklerine rağmen Web 3.0 çalışması için mevcut TCP/IP tabanlı geleneksel internet altyapısına ihtiyaç duyulmaktadır. Yani her ne kadar Web 3.0 için merkeziyetsiz ibaresi geçse de sonuçta internet bir “Ağlar Ağı”dır ve internet üzerindeki tüm ağlar birbirinden bağımsız gibi gözükse de aslında belli protokoller seviyesinde hepsi birbirine bağlı olarak çalışmaktadır. Bu aşamada ister adına Web 4.0 diyelim ister “Merkeziyetsiz İnternet” TCP/IP tabanlı bir altyapıdan farklı, tıpkı üçüncü taraf ve kurumların aradan çıktığı, üçüncü parti bilindik internet teknolojilerinin de olmadığı bir yapı, yakın gelecekte blok zinciriyle mümkün olabilir. Bilindiği üzere SpaceX firması, uzaya gönderdiği Starlink uyduları ile uzaydan dünyanın birçok yerine internet hizmeti sunmaya başladı (Harris, 2018: 10-11). Bu uydular, interneti dünyadan almaktadır. Dünyadan aldıkları interneti tekrar dünyadaki müşterilerine aktararak bir aracılık görevi görmektedirler. Şimdi bu uyduların yakın gelecekte dünya yörüngesindeki sayılarının, dünyadaki her kullanıcıya internet hizmeti verebilecek kadar yeterli sayıya ulaştığını, yeterli teknik depolama donanımıyla desteklenerek mevcut internet üzerindeki tüm veri ve bilgileri içerdiklerini düşünelim. Dağıtık yapıdaki blok zinciri teknolojisiyle kendilerine bir ağ kurduklarını ve bu ağı da yeryüzündeki internet kullanıcılarına “merkeziyetsiz internet hizmeti” şeklinde sunduklarını farz edelim. Blok zinciri teknolojisi üzerinden gerçekleşebilme ihtimali olan bu gelecek senaryosunda küresel merkeziyetsiz bir bilgi ağını yani tamamen merkeziyetsiz interneti gerçekleştirmek olasıdır. Yine bu ağın kendi üzerinde merkeziyetsiz çalışan programlar, artevrenler (metaverse), oyunlar, sosyal ağlar, e-ticaret siteleri, finans merkezleri ve dosya paylaşım platformları sayesinde tamamen merkeziyetsiz bir siber uzaya dönüşmesi de olasıdır. Böyle bir yapı üzerinden oluşturulmuş bir sosyal medya

platformu, sansürlenemeyen ve küresel çapta dünyanın en özgürlükçü sosyal medya platformu olmaya adaydır. Yaratacağı politiktik, sosyal, ekonomik ve stratejik güç sayesinde paha biçilmez bir güç olması muhtemeldir. Yine dağıtık yapıdaki bir sosyal medya ağının başta pazarlama olmak üzere derin sosyal etkilerinin de olması muhtemeldir.

5.7. Tersine Mühendislik

Geçmiş sanayi devrimine kadar uzanan tersine mühendislik kavramı, insanı yapımı herhangi bir şeyden bilgi veya tasarım planlarının çıkarılmasıdır. Günümüzde tersine mühendislik kavramı ise endüstriyel ürünleri parçalarına ayırarak çalışma mantığını anlamaya yönelik işlemektedir. İlerleyen teknolojisinin bir sonucu olarak tersine mühendislik işlemleri gündelik kullandığımız elektronik cihazlardan gelişmiş bilgisayar yazılımlarına kadar her alanı kapsayacak şekilde genişlemiştir (Eilam, 2011: 3-4). Araştırma geliştirme faaliyetlerinin süreleri ve maliyetleri göz önüne alındığında, özellikle ulusal güvenlik alanında savunma veya saldırı teçhizatlarının eşdeğer bir örneğini oluşturmak veya üzerinde değişiklik yapabilecek kadar çalışma şeklini anlamak, tersine mühendislik alanının ilgilendiği konuların başında gelmektedir (Rekoff, 1985: 244-245). Dahası, tersine mühendislik işlemleri ticari veya askeri üstünlük sağlamak için sıklıkla devletlerin başvurduğu yollardan birisidir. Askeri alanda (haber alma-savunma-saldırı), yazılım ara yüzlerinde, endüstriyel ürünlerin güvenlik analizlerinde, araştırma-geliştirme işlemlerinde ve rekabetçi teknik zekâ eğitimlerinde sıklıkla tersine mühendislik çalışmaları yürütülmektedir. Günümüz dünyasında NATO ve eski doğu bloğu ülkeleri teknolojik olarak birbirlerine zıt ve olası bir savaş tehdidi karşısında mukavemet veya üstünlük sağlamak amaçlı, birbirlerinden farklı savaş donanım ve teknolojileri geliştirmektedir. Bu durum savunma sanayi anlamında yürütülen tersine mühendislik faaliyetlerinin önünü iyice açmıştır. Millî ve yerli savunma sanayisinin bir ülke için ne denli önemli olduğunun daha iyi anlaşılması için konuya kendi ülkemizden bir

örnek verecek olursak Türkiye, özellikle son yıllarda yaptığı savunma sanayii yatırımlarının karşılığını uluslararası alanda fazlasıyla almaktadır. Konunun en bariz örneği İkinci Karabağ Savaşıdır. Türk milli savunma sanayisinin geliştirdiği İHA ve SİHA'ların savaşta etkin olarak kullanılmasının, savaşın Azerbaycan Cumhuriyeti lehine sonuçlanmasında büyük katkısı olmuştur (Erarslan ve Özdemir, 2021: 317). Buradan da anlaşılacağı üzere, konvansiyonel savunma sistemleri yerine modern savunma sistemlerinin önemi giderek artmaktadır. Pahalı araştırma ve geliştirme maliyetleri olan savunma ekipmanlarının, başta karşıt ülkelerin veya istenmeyen grupların ele geçirmesiyle birlikte yazılım ve donanım tabanlı bilgilerinin tamamen veya kısmen deşifre edilmesi bir ülkenin isteyeceği en son şeydir. Amerika Birleşik Devletleri Deniz Havacılık Komutanlığı 2018 yılında ITAMCO isimli yine Amerikan Birleşik Devletleri menşeli bir üretim ve teknoloji firmasıyla blok zinciri tabanlı projelerin geliştirilmesi konulu bir antlaşma yaptı (Woodfield, 2019: 8). Yapılan antlaşmanın içeriği kamuoyuna açıklanmasa da muhtemelen su altı ve hava dronlarının iletişim ve işletim sistemlerinin yazılımları üzerine olduğu tahmin edilebilir. Bilindiği üzere günümüzde, su altı ve hava dronları geleneksel iletişim ve işletim sistemi yazılımları ile çalışmaktadır. Bu tip yazılım ve donanımları tersine mühendislik yöntemleri ile kırıp deşifre etmek kolaydır. Fakat blok zinciri tabanlı bir yazılımı kırmak kolay değildir. Bu konuda yapılan araştırmalar devam etmekle birlikte, yakın zamanda Maryland Üniversitesi'nden teorik fizikçi ve kuantum mekaniği uzmanı Dr. Sarma, MIT Technology Review'da yayınladığı makalesinde, kuantum bilgisayarlarının blok zinciri yapılarını kırmaktan çok uzakta olduğunu ve mevcut blok zinciri teknolojisinin de muazzam bir bilimsel başarımla olduğu şeklinde tanımlamıştır (Technologyreview, 2022). Günümüzde kuantum bilgisayarları üzerinden, kuantum blok zinciri yapılarının oluşturulmasıyla ilgili kavramsal çalışmalar da sürdürülmektedir. Victoria Üniversitesinden Dr. Rajan ve Dr. Visser, tamamen kuantum bilgisayarları üzerinde geliştirilmiş bir kuantum blok zinciri yapmışlardır (Rajan ve Visser

2019: 5-9). Araştırmalarına göre geleneksel blok zinciri gibi kuantum blokzincileri de kuantum bilgisayarlarıyla yapılmak istenilen tersine mühendislik ve korsanlık girişimlerine karşı koyarak, güvenli bir yapı oluşturmaktadır. Konuya ister geleneksel ister kuantum blok zinciri teknolojisi açısından bakalım, blok zinciri yapıları için son derece güvenilir yapılar demek doğru olacaktır. Ayrıca kuantum blok zinciri teknolojisi kendisine yeni uygulama alanları buldukça tıpkı geleneksel blok zinciri teknolojisinde olduğu gibi, bize yeni araştırmaların kapılarını açacaktır.

6. Sonuç ve Öneriler

Bu sistematik derleme çalışmasında blok zinciri ve çapraz zincir teknolojisi her yönüyle kapsamlı bir şekilde irdelenmiştir. Konu; tarihi gelişim süreci, teknik detayları ve altyapısıyla birlikte gelecek olası iştirak ve kullanım alanlarıyla açıklanmaya çalışılmıştır. Blok zinciri ve çapraz zincir uygulamaları hâlihazırda kullanılıyor olsa bile çoğu uygulama, ya gelişme ya da olgunlaşma aşamasındadır. Dahası, blok zinciri üzerinden gerçekleştirilmesi muhtemel hizmet ve uygulamaların bu araştırmada belirtilenlerle sınırlı kalmayacağı da aşikardır. Çünkü zincir teknolojileri bir tür gelecek teknoloji yatırımlarıdır. Ayrıca bu yatırımlar tek bir dijital dönüşüm değil topyekûn bir dönüşümün üst bileşenleridir. Başta vatandaşlık hizmetleri, e-devlet uygulamaları, enerji verimliliği, muhasebat uygulamaları, eğitim faaliyetleri, hukuk uygulamaları, akıllı yapı ve şehirler, pazarlama faaliyetleri, sağlık uygulamaları, seçim ve referandum çalışmaları olmak üzere birçok potansiyel uygulama alanını barındıran zincir teknolojisi topyekûn bir ekosistem dinamiğidir. İlk etapta insanlara karmaşık veya güvensiz bir yapı gibi gelse de, zamanla merkezizetsiz yapının kaotik bir yapı olmadığı; aksine işletmeler, kurumlar ve hatta devletlerin kullanabileceği ucuz, hızlı, şeffaf ve organizasyonel bir yapı olduğu anlaşıldıkça blok zinciri ve çapraz zincir üzerine kurulu projeler yaygınlaşacak ve genel olumsuz kanı mutlaka olumluya dönecektir.

Önümüzdeki kısa vadeli süreçte birçok hizmet, ürün ve çözümün altyapısı blok zinciri tabanlı olarak yürütülmeye başlanacak ve kayda değer ilerlemeler sağlanacaktır. Bu alanda yapılacak projeler ve denemelerin desteklemesiyle de blok zinciri teknolojisi, akademik anlamda da inter disiplinler olarak kendine yer bulacak ve gerçek potansiyelini gösterecektir.

Bununla birlikte konunun sosyolojik boyutu daha çok üzerinde durulması gereken bir konudur. Hızla yaşanan sosyokültürel dönüşüm ve değişim, bireyler üzerinde dijital bir bilişsel evrim baskısı yaratacak; bunun tabii bir neticesi olarak da dogma ve değer yargıları arasında belirgin farklılıklar gözlenecektir. Toplumların yaşadıkları ve karşılaştıkları gelişmeler doğrudan doğruya toplumların kurumsal hafızlarına etki etmektedir. Bu sayede toplumsal öğrenme eylemi gerçekleşmiş olup, toplu adaptasyon ve toplu kabul süreci başlamaktadır. Yukarıdaki cümlede belirtildiği gibi toplumsal dogma ve değer yargıları böyle köklü değişimler için mutlaka üzerinde durulması gereken noktalardır. Söz konusu çalışmada blok zinciri teknolojisinin gelecek için tek bir sorun çözücü alternatif olduğu fikri ve anlayışı kesinlikle çıkarılmamalıdır. Zira her ne kadar yapısı itibarıyla kusursuz gibi gözükse de ilerleyen zamanlarda karşıya karşıya kalacağı kusur ve zorlukları olması ihtimal dâhilindedir. Yine bu kusur ve zorlukların aşılması da oldukça olası bir durumdur. Yine unutulmamalıdır ki geleneksel yapı ve anlayışları ortadan kaldıran bu teknoloji gerekli dönüşüm ivmesini yakaladığı takdirde küresel olarak gelir sağlayan aracı kişi ve kurumları tamamen ortadan kaldıracak güçtedir.

Çalışmada, blok zinciri teknolojisinin geleceğe ilişkin kullanım alanları üzerine bir değerlendirme yapılmıştır. Şüphesiz önümüzdeki on yıl içerisinde, başta devletler olmak üzere birçok kurum ve organizasyonun gündelik hayatta kullanıma geçeceği blok zinciri teknolojisi, hayatımızın vazgeçilmez bir parçası olarak insanlık

tarihinde yerini alacaktır. Çalışmanın genel bir sonucu olarak, blok zinciri teknolojisi dünyada hızla yer edinirken, ülke olarak biz de kendimizi bu teknolojiye hazırlamalıyız. Sadece blok zinciri teknoloji kullanıcısı olarak değil, blok zinciri tabanlı araştırma, geliştirme ve uygulamacısı olarak ulusal anlamda bu teknolojiye hazırlık yapmalıyız. Bu bağlamda, başta kodlama ve yazılım geliştirme işlemlerinin ortaöğretime kadar genişletilmesi, yükseköğretimde blok zinciri derslerinin verilmesi, akademik araştırmaların artırılması ve blok zinciri üzerine çalışma yapan ve çeşitli faaliyetler yürüten işletmeler ve kurumların düzenli olarak finanse edilmesinin olumlu sonuçlar sağlayacağı düşünülmektedir. Sonuç olarak bu çalışma; blok zinciri teknolojisinin gelecek olası muhtemel kullanım alanlarını detaylı ve sade bir üslupla anlatılarak konu ile ilgili araştırma yapacaklara aktarmayı hedeflemiştir. Elde edilen sonuçlar geniş alanyazından erişilebilen bilgilerle harmanlanarak yorumlanmış ve ortaya bir gelecek öngörüsü konulmuştur. Bu sayede içerik, kapsam ve proje açısından alanyazınına katkı sağlayacağı düşünülmektedir.

Kaynakça

- Ajjan, H. ve Hartshorne, R. (2008). Investigating Faculty Decisions to Adopt Web 2.0 Technologies: Theory and Empirical Tests. *The Internet and Higher Education*, 11(2), 71-80. Doi: 10.1016/j.iheduc.2008.05.002.
- Akkoyunlu, E. A., Ekanadham, K. ve Huber, R. V. (1975). Some Constraints and Tradeoffs in the Design of Network Communications. In *Proceedings of the fifth ACM symposium on Operating systems principles* (pp. 67-74).
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. ve Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials*, 17(4), 2347-2376. Doi: 10.1109/COMST.2015.2444095.
- An Approach of Secure Two-Way-Pegged Multi-Sidechain, (Mayıs, 2022). Erişim Adresi <http://www.under.orosfeoconskee.tk>, (Erişim Tarihi: 01.05.2022)
- Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Inc.

- Atabaş, H. (2018). *Blokzinciri Teknolojisi ve Kripto Paraların Hayatımızdaki Yeni Yeri*. İstanbul, Ceres Yayınları.
- Atzori, L., Iera, A. ve Morabito, G. (2010). The Internet of Things: A Survey. *Computer Networks*, 54(15), 2787-2805. Doi: 10.1016/j.comnet.2010.05.010.
- Bhadani, A. K. ve Jothimani, D. (2016). Big Data: Challenges, Opportunities, and Realities. In *Effective Big Data Management and Opportunities for Implementation* (pp. 1-24). IGI Global.
- Byzantine Fault Tolerance: How Blockchain Solves Byzantine Generals Problem, (2022, Nisan). Erişim Adresi <http://www.phemex.com.com>, (Erişim Tarihi: 25.04.2022)
- Canongia, C. ve Mandarino, R. (2014). Cybersecurity: The New Challenge of The Information Society. In *Crisis Management: Concepts, Methodologies, Tools and Applications* (pp. 60-80). Hershey, PA: IGI Global. Doi.org/10.4018/978-1-4666-4707-7.ch003.
- Castells, M. (2003). Internet, Libertad y Sociedad: Una Perspectiva Analítica. *Polis. Revista Latinoamericana*, (4). Doi: 10.32735/S0718-6568/2003-N4-208.
- Clemente, D. (2015). Fundamentals of Cyber Security, A Biennial Collection of Analysis on International Agreements for Security and Development. *Vertic (Verification, Research, Training and Information Centre)*, Chapter 10.
- CoinMarketCap: Cryptocurrency Prices, Charts and Market Cap, (2022, Mart). Erişim Adresi <http://www.coinmarketcap.com>, (Erişim Tarihi: 28.03.2022)
- Craiggen, D., Diakun-Thibault, N. ve Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10). Doi: 10.22215/timreview/835.
- Deng, L., Chen, H., Zeng, J. ve Zhang, L. J. (2018). Research on Cross-Chain Technology Based on Sidechain and Hash-Locking. In *International Conference on edge Computing* (pp.144-151). Springer, Cham. Doi: 10.3390/en13040881.
- Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress.
- Dursun, H. (1993). Bizans Generalleri Problemi. *Tübitak Bilim ve Teknik Dergisi*, Ankara, TÜBİTAK Yayınları
- Dwork, C. ve Naor, M. (1992). Pricing Via Processing or Combatting Junk Mail. In *Annual international cryptology conference* (pp. 139-147). Springer, Berlin, Heidelberg. Doi: 10.1007/3-540-48071-4_10.
- Eilam, E. (2011). *Reversing: Secrets of Reverse Engineering*. John Wiley Sons.
- Erarslan, F. ve Özdemir, F. N. (2021). Azerbaycan-Türkiye İlişkilerinde Önemli Bir Kavşak: İkinci Karabağ Savaşı. *Türk Dünyası Araştırmaları, Türk Dünyası Araştırmaları*, 129(255), 315-334.
- Fairfield, J. A. (2005). Virtual Property. *BUL Rev.*, 85, 1047.

- Fanning, K. ve Centers, D. P. (2016). Blockchain and its Coming Impact on Financial Services. *Journal of Corporate Accounting Finance*, 27(5), 53-57. Doi: 10.1002/jcaf.22179.
- Feeley, G. (1982). *Burning Chrome* by William Gibson (Book Review). *Foundation*, 97.
- Fisher, D., DeLine, R., Czerwinski, M. ve Drucker, S. (2012). Interactions With Big Data Analytics. *Interactions*, 19(3), 50-59. Doi: 10.1145/2168931.2168943.
- Freedom On The Net 2020, (2022, Mayıs). Erişim Adresi <http://www.freedomhouse.org.com>, (Erişim Tarihi: 15.05.2022)
- Harris, M. (2018). Tech Giants Race to Build Orbital Internet [News]. *IEEE Spectrum*, 55(6), 10-11. Doi: 10.1109/MSPEC.2018.8362213.
- Herlihy, M., Liskov, B. ve Shrira, L. (2021). Cross-chain Deals and Adversarial Commerce. *The VLDB Journal*, 1-19. Doi: 10.1007/s00778-021-00686-1.
- Hervani, A. A., Helms, M. M. ve Sarkis, J. (2005). Performance Measurement for Green Supply Chain Management. *Benchmarking: An International Journal*. Doi: 10.1108/14635770510609015.
- Hobbes, T. (1969). *Leviathan*, 1651. Menston: Scholar P.
- Hoffman, R. (2014). The Future of the Bitcoin Ecosystem and “Trustless Trust”– Why I Invested in Blockstream. *LinkedIn Pulse*, 17(11), 573-587.
- Iansiti, M. ve Lakhani, K., (2017). The Truth About Blockchain. *Harvard Business Review*, 95(1), 118-127.
- Jiang, Y., Wang, C., Wang, Y. ve Gao, L. (2019). A Cross-chain Solution to Integrating Multiple Blockchains for IoT Data Management. *Sensors*, 19(9), 2042. Doi: 10.3390/s19092042.
- Kaur, N. ve Sood, S. K. (2017). Dynamic Resource Allocation for big Data Streams Based on Data Characteristics (5 V s). *International Journal of Network Management*, 27(4), e1978. Doi: 10.1002/nem.1978.
- Kleemann, F., Voß, G. G. ve Rieder, K. (2008). Un (der) Paid Innovators: The Commercial Utilization of Consumer Work Through Crowdsourcing. *Science, Technology Innovation Studies*, 4(1). Doi 5-26. 10.17877/DE290R-12790.
- Kopczak, L. R. (1997). Logistics Partnerships and Supply Chain Restructuring: Survey Results From the US Computer Industry. *Production and Operations Management*, 6(3), 226-247. Doi: 10.1111/j.1937-5956.1997.tb00428.x.
- Kranenburg, R., V. (2008). A Critique of Ambient Technology and The “All-Seeing Network of RFID. Institute of Network Cultures.
- Kshetri, N. (2017). Can Blockchain Strengthen The Internet of Things?. *IT professional*, 19(4), 68-72. Doi: 10.1109/MITP.2017.3051335.
- Lamport, L. ve Fischer, M. (1982). *Byzantine Generals and Transaction Commit Protocols* (Vol. 66). Technical Report 62, SRI International.

- Li, D., Yu, J., Gao, X. ve Al-Nabhan, N. (2020). Research on Multidomain Authentication of IoT Based on Cross-Chain Technology. *Security and Communication Networks*, Doi: 10.1155/2020/6679022.
- Lin, I. C. ve Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.*, 19(5), 653-659. Doi: 10.6633/IJNS.201709.19(5).01.
- Liu, D. ve Camp, L. J. (2006, June). Proof of Work can Work. In *WEIS*, England: Robinson College, University of Cambridge.
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. ve Hung Byers, A. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.
- O'reilly, T. (2009). *What is Web 2.0*. O'Reilly Media, Inc.
- Özcan, D. (2021). *Blokzincir Mimarisi ve Merkezi Olmayan Uygulamalar*. Pusula.
- Parlak, A. ve Balık, H. H. (2005). *İnternet ve Türkiyede İnternetin Gelişimi*. Bitirme Ödevi, Fırat Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Bölümü, Elazığ.
- Quantum Computing Has a Hype Problem, (Haziran, 2022). Erişim Adresi <http://www.technologyreview.com>, (Erişim Tarihi: 22.06.2022)
- Rajan, D. ve Visser, M. (2019). Quantum Blockchain Using Entanglement in Time. *Quantum Reports*, 1(1), 3-11. Doi: 10.3390/quantum1010002.
- Rekoff, M. G. (1985). On Reverse Engineering. *IEEE Transactions on Systems, Man, and Cybernetics*, (2), 244-252. Doi: 10.1109/TSMC.1985.6313354.
- Russell, B. (1905). On Denoting. *Mind*, 14(56), 479-493. Doi: 10.1093/mind/XIV.4.479.
- Sharma, N. ve Shanker, R. (2022, March). Analysis of Ransomware Attack and Their Countermeasures: A Review. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 1877-1883). IEEE. Doi: 10.1109/ICEARS53579.2022.9751949.
- Şengör, A. M. (2019). *Bilimin Büyüsü*. İnkılap Kitabevi, İstanbul.
- Tan, K. C., Kannan, V. R. ve Handfield, R. B. (1998). Supply Chain Management: Supplier Performance and Firm Performance. *International Journal of Purchasing ve Materials Management*, 34(3), 1-29.
- Tanrıverdi, M., Uysal, M. ve Üstündağ, M. T. (2019). Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), 203-217. Doi: 10.17671/gazibtd.547122.
- The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, (2022, Şubat). Erişim Adresi <http://www.lightning.network.com>, (Erişim Tarihi: 11.02.2022)
- Urmak, T.T. (2021). *Marka İmajının Marka Tercihinde Üzerindeki Etkisinde Elektronik Ağızdan Ağıza Pazarlamanın Aracılık Rolü: Bilişim Sektöründe Bir Uygulama*. Doktora Tezi, Haliç Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

- Usta, A. ve Dođantekin, S. (2017). *Blockchain 101*. İstanbul: MediaCat Kitapları.
- Ünal, G. ve Uluyol, Ç. (2020). Blok Zinciri Teknolojisi. *Bilişim Teknolojileri Dergisi*, 13(2), 167-175. Doi: 10.17671/gazibtd.516990.
- Van Atta, R. H. (2018). DARPA–The Innovation Icon at 60. *DARPA 60 years 1958-2018*.
- Vopson, M. M. (2019). The Mass-Energy-Information Equivalence Principle. *AIP Advances*, 9(9), 095206. Doi: 10.1063/1.5123794.
- Wang, Z., Jin, H., Dai, W., Choo, K. K. R. ve Zou, D. (2021). Ethereum Smart Contract Security Research: Survey and Future Research Opportunities. *Frontiers of Computer Science*, 15(2), 1-18. Doi: 10.1007/s11704-020-9284-9
- Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.
- Woodfield, D. (2019). *The Emerging Impacts of Blockchain Technology on DOD Asset Cyber Security*. Air Command and Staff Coll Maxwell AFB al Maxwell AFB United States. Air Command and Staff College Air University.

