

BLOKZİNCİR TEKNOLOJİSİNİN İÇ DENETİM FAALİYETLERİNE ETKİLERİ: FIRSATLAR VE TEHDİTLER

(BLOCKCHAIN TECHNOLOGY AND ITS IMPACTS ON THE INTERNAL AUDIT ACTIVITIES: OPPORTUNITIES AND THREATS)

Çetin KARAHAN* / Aslıhan TÜFEKÇİ**

ÖZ

Blokzincir henüz yasal düzenlemeleri ve standartları net biçimde ortaya konulmamış olmakla birlikte tüm dünyada hızla gelişen, hem kamu hem de özel sektör tarafından yakından izlenen ve mevcut iş süreçlerinde köklü değişikliklere sebep olması beklenen bir teknolojidir. 2008 yılında ilk ortaya çıkmasından bu yana uygulama sahası sürekli olarak genişleyen bu teknolojinin ortaya koyduğu dönüşümün iç denetimin temel fonksiyonları olan denetim ve danışmanlık faaliyetlerini de etkilemesi öngörülmektedir. Teknolojinin sunmuş olduğu işlem şeffaflığı, silinmesi ya da değiştirilmesi mümkün olmayan işlem kayıtları, güvenilir bir üçüncü taraf onayı ya da kontrolü olmadan işlem gerçekleştirme gibi özellikler ve sürekli denetime çok uygun altyapısı en önemli avantajlar olarak öne çıkmaktadır. Bunun yanında yönetim yapısının karmaşıklığı, teknolojinin anlaşılmasının güçlüğü, denetime olan bağımlılığı azaltma potansiyeli, mevcut sistemlerle entegrasyon problemleri ve yetersiz insan kaynağı gibi konular da riskli alanlar olarak değerlendirilmektedir. İç denetim faaliyetleri ve iç denetçi nitelikleri bakımından bu teknolojinin sunduğu fırsatlardan azami

düzeyle faydalanmak, riskleri de olabildiğince iyi yönetmek için iç denetçilerin blokzincir teknolojisi konusunda yeterli düzeyde bilgi sahibi olmaları, dönüşüm sürecinde aktif rol alarak başlangıç aşamasında gerekli kontrollerin tasarlanmasına yardımcı olmaları kritik öneme sahiptir.

Blokzincir teknolojisinin teknik altyapısı, kullanım alanları, avantaj ve dezavantajları, mevcut süreç ve sektörler potansiyel etkileri gibi birçok konuda çok sayıda çalışma olmasına karşın teknolojinin denetim mesleğine etkileri konusundaki çalışma sayısı kısıtlı ve daha çok muhasebe denetimleri odaklıdır. Bu çalışmada, kısıtlı sayıdaki bu çalışmalarla birlikte blokzincir teknolojisinin temel özelliklerinden bahsedilerek denetim mesleğine potansiyel etkileri konusunda daha geniş bir perspektif sunulması hedeflenmektedir.

Anahtar Kelimeler: Blokzincir, iç denetim, dağıtık kayıt defteri

JEL Kodlaması: H83, M42, O30.

ABSTRACT

Though the technical and legal regulations and international standards were not clearly defined yet, blockchain is a rapidly developing technology throughout the world. Both public and private sector are in hot pursuit of this newly emerging technology and it is expected to create radical changes in existing business processes. The transformation caused by this technology which has a constantly expanding field of application since the first emergence in 2008, is predicted to affect the fundamental functions of internal auditing: audit and consulting. The most outstanding advantages of this technology are transparency, immutability, eliminating intermediaries and the favorable infrastructure for continuous auditing. Besides these advantages, it has some shortcomings such as the complexity of governance structure, difficulty in understanding the concept, the potential for diminishing the dependancy on the audit, problems in integration with the existing systems and insufficient resources of talent. It is so critical for internal auditors to have adequate knowledge on blockchain technology for taking the maximum advantages

of the opportunities offered by this technology and for managing the risks as proper as possible. Another critical action is taking an active role in the transformation process for especially facilitating control design.

There are many researches on some specific topics of blockchain technology such as technical infrastructure of blockchain, use cases, advantages and disadvantages, potential impacts on existing business processes and sectors but the researches about the potential impacts on audit profession are very limited and mostly focused on accounting. In this paper, it is aimed to provide a wider perspective on the potential impacts of blockchain technology to the audit activities while referencing these limited researches and with the basic characteristics of blockchain.

Keywords: Blockchain, internal audit, distributed ledger

JEL Classification: H83, M42, O30.

*) İç Denetçi (CISA), T.C. Cumhurbaşkanlığı, Savunma Sanayii Başkanlığı, Ankara, Orcid:0000-0002-8697-9162, ckarahan@ssb.gov.tr

**) Doç. Dr., Enstitü Müdürü, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara, Orcid:0000-0002-8669-276X, asli@gazi.edu.tr

Yazı Gönderim Tarihi: 03.04.2019, Yazı Kabul Tarihi: 10.04.2019

1. GİRİŞ

Denetim mesleğinde teknolojik yeniliklerin kullanımı günümüzde hızla artmaktadır. 1970'lere kadar kâğıt, kalem ve hesap makinasından faydalanılıyorken günümüzde artık veri madenciliği, veri analitiği, sürekli risk izleme ve değerlendirme, blokzincir, yapay zeka gibi teknolojiler iç denetimde kullanılmaya başlanmıştır (Dai, 2017, s. 2).

Blokzincir teknolojisi ilk olarak 1 Kasım 2008 tarihinde, kriptografi, programlama ve matematik gibi konularda bilgi paylaşımları ve tartışmaların yürütüldüğü bir e-posta grubuna Satoshi Nakamoto takma adını kullanan bir üye tarafından gönderilen 'Bitcoin: Eşten-eşe Elektronik Nakit Ödeme Sistemi' başlıklı bir makale ile adını duyurmuştur. Aslında bu makalede blokzincir ifadesi doğrudan geçmemekte olup sistem tarif edilirken işlemlerin kaydedildiği yapı blok olarak, onaylanan her bir bloğun özel bir algoritma ile birbirine eklenmesi ise zincir olarak ifade edilmiş, blokzincir ifadesi daha sonra kullanılmaya başlanmıştır.

Son yıllarda gittikçe popülerliği ve bilinirliği artmakla birlikte henüz tam olarak potansiyeli ortaya çıkmamış olan blokzincir, ilk ortaya çıkmasının üzerinden on yılı aşkın bir süre geçmiş olmasına karşın henüz geniş kabul görmüş, üzerinde uzlaşmış standartları bulunan ve kendini tam olarak ispatlamış bir teknoloji değildir. Bununla birlikte, çok da uzak olmayan bir gelecekte finans başta olmak üzere birçok sektörü ve kamu tarafından sunulan hizmetleri derinden etkileyeceği konusunda artık çok da fazla şüphe kalmamıştır. Uygulama alanı ve araştırma konuları çok hızlı bir şekilde genişleyen blokzincir teknolojisi hem özel hem de kamu sektörü için yıkıcı bir teknoloji olarak nitelendirilmektedir. Kuşkusuz ki iç denetim faaliyetleri de bu değişim ve dönüşümden etkilenecek, teknolojinin iç denetim mesleğine olumlu ve olumsuz bazı yansımaları olacaktır.

Blokzincir teknolojisinin yakın gelecekte birçok sektörü etkilemesi, günümüzdeki birçok iş alanının ortadan kalkmasına ya da dönüşmesine sebep olması öngörülmekte olup bu nedenle de yıkıcı bir teknoloji olarak adlandırılmaktadır. Dünya üzerinde birçok devlet, uluslararası kuruluş ve özel sektör temsilcisi bu teknolojinin doğrulanması ve uygulanması için çalışmalar yürütmekte olup bazı ülkeler gerçek hayat

uygulamalarında bu teknolojiyi kullanmaya başlamışlardır.

Blokzincir teknolojisi, diğer sektörlerin yanı sıra muhasebe sektöründe de artan bir ilgi görmektedir. PwC bu teknolojiyi mevcut uygulamaları değiştirecek yeni nesil iş süreci geliştirme yazılımı olarak görmekte, Deloitte blokzincirin bireylerle işletmeler arasındaki işbirliğini, süreçlerin şeffaflığını büyük oranda artıracığını, bunun sonucunda da ekonominin verimliliği ve sürdürülebilirliğini geliştireceğini tahmin etmektedir (Dai, 2017, s. 59, 60).

Blokzincir teknolojisi ve iç denetim faaliyetlerine etkileri konusunda yapılmış olan akademik çalışmalar oldukça kısıtlı olup mevcut çalışmalar genel olarak muhasebe denetimleri ve mali denetimlere odaklanmıştır. Brender ve diğerleri (2018) blokzincir teknolojisinin yıkıcı etkileri konusundaki tartışmalarda denetim ve kontrol mesleklerinin pek ön plana çıkmadığını vurgulayarak bu teknolojinin denetim mesleği konusundaki yıkıcı etkisinin tam olarak öngörülemediği, daha küçük ölçekli denetim firmalarının ortaya çıkacak değişime ayak uydurabilmek için bir hazırlık yapmadıkları bulgularına ulaşmışlar, mesleğin muhasebeden daha çok Bilgi Teknolojileri (BT) alanına yöneleceğini ve denetçi profilinin değişmesinin beklendiğini belirtmişlerdir.

Birçok sektörde blokzincir teknolojisinin pilot uygulamaları geliştirilmiş ve teknolojinin kullanım senaryoları tartışılmış olmakla birlikte denetim alanındaki potansiyel katkıları henüz tam olarak değerlendirilmemiştir (Dai, 2017, s. 60).

2. BLOKZİNCİR TEKNOLOJİSİ

2008 yılındaki mali krizden sonraki Acil Ekonomik İstikrar Yasasının Amerikan mali sistemini çökmekten kurtardığı dönemde ortaya çıkan Bitcoin ile tarihte ilk defa maliyetli bir aracıya gereksinim duyulmadan birbirinden uzak ve birbirine güven duymayan iki taraf arasında güvenilir bir biçimde değer transferi gerçekleşmiştir (Catalini ve Gans, 2017, s. 1). Blokzincir, dijital bir varlık olan kripto para birimi Bitcoin'in temelini oluşturan teknolojidir.

Blokzincir teknolojisi için bankasız para, yöneticisiz şirket, politikacısız ülke benzetmesi yapılmaktadır

(Voshmgir, 2017). İlk ve en bilinen uygulaması Bitcoin olduğundan uzunca bir süre blokzincir sadece kripto paralarla ilgili bir terim olarak algılanmış, ancak zamanla algoritmanın içinde barındırdığı muazzam potansiyel fark edilmeye başlanmıştır. Satoshi Nakamoto (2008) bu sistemi herhangi bir finansal kuruluşun aracılığına ihtiyaç duyulmadan iki taraf arasında çevrim içi ödemeyi mümkün kılan tamamen eşten eşe bir elektronik para olarak tanımlamış, dijital imzanın bu sistemin bir parçası olduğunu, arada güvenilir bir üçüncü taraf olmadan birbirlerini tanımayan ve hatta birbirlerine güvenmeyen tarafların ihtiyaç duydukları güven mekanizmasının kriptografi ile sağlandığını, mükerrer harcama probleminin işlemleri kronolojik olarak sıralayan bir zaman damgası kullanılarak giderildiğini, kaydedilen işlemlerin geri döndürülmesinin hemen hemen imkansız olduğunu belirterek CoinMarketCap'ın 01.04.2019 tarihli verilerine göre (CoinMarketCap, 2019) toplam piyasa değeri yaklaşık 370 milyar dolar olan kripto para pazarının temelini atan sistemin teknik detaylarını 8 sayfalık makalesinde açıklamıştır.

Blokzincir teknolojisini üzerinde uzlaşmış tek bir tanımı bulunmamakla birlikte en temel ifadeyle tek bir kişi ya da kuruluşun kontrolünde olmayan, düğüm adı verilen çok sayıda bilgisayar tarafından yönetilen, işlemlerin doğrulanması için özetleme algoritmasını, onaylanması için ise mutabakat protokollerini kullanan, işlemleri zaman damgası ile sıralayan, onaylanmış işlemleri birbiri ardına kriptografi ve özetleme fonksiyonları ile bağlayarak tüm düğümlerde özdeş kopyasını tutan, içerdiği verilerin değiştirilmesi ve geriye çevrilmesi hemen hemen imkansız olan dağıtık bir veri kayıt sistemidir.

2008 yılında ilk ortaya çıkmasından bu yana blokzincir teknolojisi, 1.0, 2.0 ve 3.0 olarak üç evrede gelişim göstermiştir. Blokzincir 1.0 bilinen en yaygın örneği Bitcoin olan kripto para işlemlerinin gerçekleştirildiği, dijital para transferi ve dijital ödemeler gibi finansal uygulamaları içeren ilk dönemdir. Blokzincir 2.0, 2013 yılı sonlarında Ethereum adlı blokzincir platformunun ortaya çıkması ile ortaya atılan 'akıllı sözleşmeler' kavramının varlıkların dijital olarak transferinde kullanılmaya başlandığı dönemdir. Bu dönemde bilgisayar kodları biçiminde hazırlanarak belirli koşullar gerçekleştiğinde kendiliğinden çalışan sözleşmelerle blokzincir teknolojisini yıkıcı etkileri

ve kullanım alanları daha da genişlemiştir. Blokzincir 3.0 ise üzerinde net bir uzlaşma ve tanım bulunmamakla birlikte teknolojinin ölçeklenebilirlik problemlerinin giderilebildiği, finansal uygulamalarının ötesindeki uygulamaların geliştirildiği evredir.

Blokzincirin en önemli karakteristiklerinden biri dağıtık ve paylaşılan yapısıdır. Bu nedenle, blokzincire dayalı sistemler mevcut araçların sebep olduğu maliyetleri ve ihtilafları ortadan kaldırma potansiyeline sahiptir. Böylelikle daha fazla veri bütünlüğü, dağıtıklık ve aracıya gerek duyulmayan bir güven ortamı ile daha düşük işlem maliyetleri vadetmektedir (Berryhill, Bourgerly ve Hanson, 2018, s. 11).

Blokzincir aslında tek bir kavram değildir. İlk ortaya çıktıktan sonra birçok yönden gelişmiş, farklı şekiller almış ve sınırsız kullanım senaryolarına hitap etmiştir (Lyons, Courcelas, Grandsenne, Carrel ve Timsit, 2018, s. 6). Blokzincir teknolojisini ilk ve en tanınan örneği olan *Bitcoin* özetleme, dijital imza, iş ispatı ve eşten eşe ağlar gibi çok büyük teknolojileri bir arada kullanmaktadır. Bunlardan hiçbiri yeni bir teknoloji olmamakla birlikte, bu mevcut teknolojilerin kombinasyonu blokzincirde yepyeni fonksiyonlar yaratmıştır (Nomura Research Institute, 2016, s. 13).

Casey ve Vigna (2018) blokzinciri "bilgisayar düğümlerinden oluşan bir ağda kopyaları kaydedilen, sürekli biçimde güncellemelerin bir yazılım yönlendirmeli mutabakatla belirlendiği, birbirlerine ardışık olarak bağlı ve kriptolojik olarak güvenliği sağlanmış, dijital imza ile kanıtlanabilir, dağıtık, sadece kayıt eklemeye izin verilen bir kayıt defteri" olarak tanımlamaktadır.

Blokzincir teknolojisinde veriler gruplanarak bloklar biçimde toplanır, işlem zamanlarına göre sıralanır ve daha sonra kriptografi kullanılarak bu bloklar birbiri üzerine eklenir. Her bir blok kendisinden önceki bloğun dijital bir parmak izine benzeyen özet değerini içerdiğinden bir bloktaki en küçük bir değişiklik kendisinden sonraki tüm blokların yapısını değiştirir. Böylelikle eski bir veriyi değiştirmek, takip eden tüm bloklardaki verileri değiştirmeyi ve bu değişikliği ağdaki tüm kullanıcılarda kaydedilen kopyalarda yinelenmeyi gerektirir ve bu da pratikte çok zor bir işlemdir. Tamamlanan her blok ile birlikte en güncel zincir ağdaki tüm katılımcılar tarafından kendilerine kopyalanır. Herhangi bir katılımcıda hatalı, manipüle edilmiş ya da bozulmuş bir veri zincirinin bulunması

sistemi tehlikeye atmaz. İşlemi tamamlanan her bir blok ayrıca kendi zaman damgasını alır ve böylelikle bilgilerin bir sıra dahilinde kaydı sağlanarak çifte kayıt engellenir.

Blokzincirde güvenin inşa edilebilmesi için kimlik (kim kimdir?), sahiplik (kim neye sahiptir?) ve doğrulama (gerçek nedir?) biçiminde üç kilit unsur bulunmaktadır. Blokzincir kullanıcıların kimliklerini kolaylıkla ispatlamalarına, dijital varlıkların sahipliğinin korunmasına ve yüksek maliyetli bir aracı olmadan işlemlerin doğrulanmasına izin verir. Blokzincir kimlik problemini dijital imza kullanımıyla, sahiplik problemini kriptografik özetleme ile, doğrulama problemini ise program kodu aracılığı ile gerçekleştirilen ağdaki düğümlerin çoğunluğunun mutabakatını gözetken konsensüs mekanizmasıyla çözmektedir (Galen vd., 2018, s. 7, 8).

Blokzincir teknolojisini tarihçesinden bahsedilirken haklı olarak Bitcoin ile başlanmakta birlikte 1970'li yıllara kadar yalnızca silahlı kuvvetler ve istihbarat servislerince kullanılan ancak 1976'da ilk defa herkese açık olarak kriptografi ve veri şifreleme konusunda iki makale yayınlayan Whitfield Diffie ve Martin Hellman ile 1980'lerin sonlarında bir grup yazılımcı aktivistin oluşturduğu bir e-posta grubu ile başlayıp 1992 yılında bir grup halini alan şifre anarşistlerinden de (*cypherpunks*) mutlaka bahsedilmelidir. Güven ve Şahinöz (2018) blokzincir teknolojisini meydana getirdiği dönüşümü Avusturya asıllı Amerikalı iktisatçı J. A. Schumpeter'in 'her yeni icat yapıcı bir yıkıcılık barındırır' sözüne atıfla yaratıcı yıkım olarak tanımlamakta, kripto para, blokzincir teknoloji devrimi ve Bitcoin konusunda konuşulan ne varsa *Cypherpunks* adıyla bilinen bir avuç aktivist ile başladığını ileri sürmektedir.

Cypherpunk grubunun içerisinde *WikiLeaks* kurucusu Julian Assange, *BitTorrent*'in yaratıcısı Bram Cohen, Bitcoin'in kurucusu Satoshi Nakamoto, ünlü kriptograf Hal Finney, Philip Zimmermann, Nick Szabo gibi birçok önemli isim bulunmaktadır (Cybersalon, 2013). Satoshi Nakamoto Bitcoin'i tasarlarlarken aslında yeni bir keşifte bulunmamış, kendisinin de içinde bulunduğu *Cypherpunks* grubunun diğer üyelerinin çalışmalarından, kriptografiden, oyun teorisinden, eşten eşe ağlardan, açık anahtarlı şifrelemeden, özetleme algoritmalarından ve dağıtık mimarilerden fay-

dalanarak birçok farklı çözümü tek bir çatı altında, açık kaynak kodlu bir yazılımda toplayarak neredeyse kusursuz bir sistemi ortaya koymuştur.

Onbirinci Kalkınma Planı hazırlıkları kapsamında hazırlanmış olan özel ihtisas komisyonu ön raporunun bir kısmında da blokzincir teknolojisinden kısaca bahsedilmektedir (Onbirinci Kalkınma Planı Kamuda Kurumsal Yönetimde Yeni Yaklaşımlar Özel İhtisas Komisyonu, 2017):

“Özellikle son dönemde bitcoin gibi sanal para birimlerinin kullanımı ile gündeme gelen blok zinciri teknolojileri, aracı kurumların varlığını yazılım teknolojilerine dayalı bir kayıt sistemiyle geçersiz kılan yeni bir olanak sunmaktadır. Bu güvenilir kayıt sisteminin bireyler ve kurumlar arasındaki her tür kayıt sistemine uygulanabileceği düşünülmektedir. Bu alandaki gelişmeler bankacılık sisteminden kamudaki kayıtlara kadar çok geniş bir yelpazede tartışılmaktadır. Kamu yönetiminde bu teknolojilerin hangi alanlarda ve nasıl kullanılabileceğine ilişkin ciddi tartışmalar sürmektedir.”

2.1. Blokzincir teknolojisini çalışma prensibi ve temel özellikleri

Blokzincir, veri bütünlüğünü sağlayan zincir şeklinde kayıt imzalama, verinin dağıtık biçimde bulunması ve sadece mutabakatla kayıt oluşturulabilmesi şeklinde üç temel kavramın birleşimi olarak tanımlanabilir. Bu üç maddeden en önemlisi ise mutabakat kısmıdır (T2 Yazılım A.Ş., Bankalararası Kart Merkezi A.Ş., 2018, s. 14).

Dijital bir sistem üzerinde mutabakat yapısı yazılımsal açıdan garanti altına alınmalıdır. Blokzincir teknolojisi bu noktada verinin iletişim ağları üzerinden, dağıtılmış şekilde saklanmasını ve bu süreç içinde verinin tüm noktalarda aynı kaldığına dair mutabakat yapılmasını sağlamakta, herkesin kendi verisini şifreleyeceği, böylelikle bu veriyi sadece kendisinin kullanacağı ve izin vermesi halinde diğer tarafların bu veriye erişebileceği bir yapı sunmaktadır (Usta ve Doğantekin, 2017, s. 45).

Blokzincir ve Dağıtık Kayıt Defteri Teknolojisi (*Distributed Ledger Technology – DLT*) bazen eşanlam-

lı olarak kullanılmakla birlikte tam olarak aynı şey değildir. Dağıtık Kayıt Defteri Teknolojisi gizli ya da herkese açık kayıtların ve bilginin dağıtılmasını sağlayan teknolojileri tanımlayan şemsiye bir kavramdır. Blokzincir ise ilk tam fonksiyonel Dağıtık Kayıt Defteri Teknolojisidir ve çok daha kapsamlı olan bu teknolojinin bir alt kategorisidir (Thake, 2018). Her blokzincir bir dağıtık kayıt defteridir ancak her dağıtık kayıt defteri bir blokzincir olmayabilir.

Blokzincir temel olarak sürekli büyüyen bir kayıtlar listesidir. Sadece veri eklemeye izin veren yapısı nedeniyle veri tabanına sürekli yeni kayıtlar eklenirken daha önce girilmiş olan verilerin silinmesi veya değiştirilmesi mümkün değildir. Bu özellikleri nedeni ile blokzincir teknolojisi olayların kaydı, kayıtların yönetilmesi, işlemlerin proses edilmesi, varlıkların izlenmesi ve oy kullanma konuları için çok uygundur (Ray, 2018).

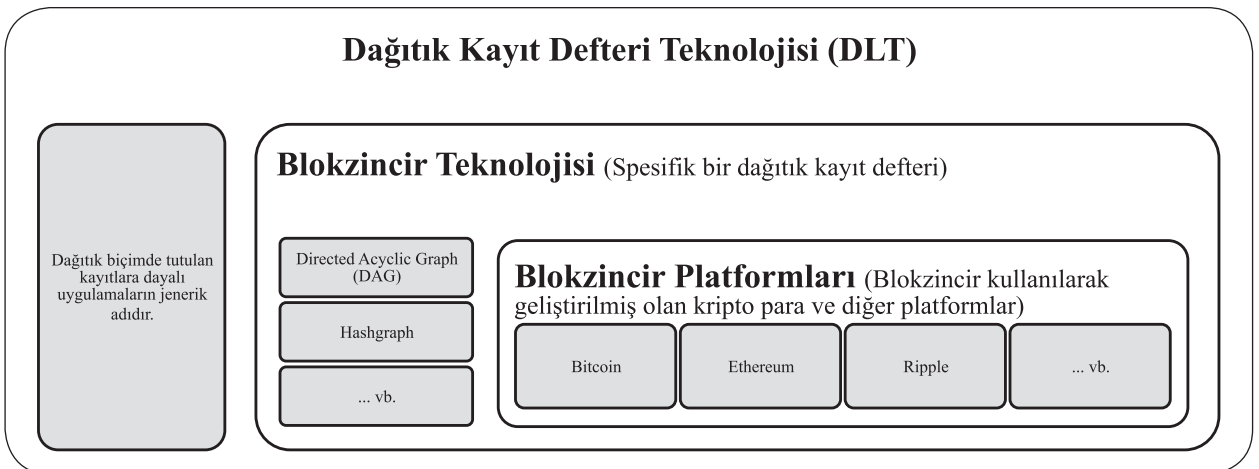
Aşağıda verilmiş olan Şekil 1'de Bitcoin, blokzincir ve dağıtık kayıt defteri arasındaki ilişki gösterilmiştir.

Blokzincir teknolojisinde tüm bilgi blok adı verilen veri yapısında tutulur. Her bir blok işlem bilgileri ile birlikte kendinden önceki bloğun referans değerini de içinde barındırır. Blok içinde cevabı sadece ilgili bloğa özgü çözülmesi oldukça zor matematiksel bir bulmaca bulunur. Bu matematiksel problemin cevabı bulunmadan ağa yeni bir blok gönderilemez. Bu problem çözme süreci madencilik olarak adlandırılır

ve madenciler soruyu ilk çözen olmak için yarışır. Çözümü ilk bulan madenci işlem doğrulama karşılığında ödül kazanır (teşvik mekanizması). Tüm işlem bilgileri, önceki bloğun referans değeri, zaman damgası ve işlem doğrulama için kullanılacak özel bir değer (*nonce* değeri) bir bloğu oluşturur ve bir özetleme algoritması ile tüm bu bilgilerin özet değeri (*hash*) alınarak o bloğun referans değeri oluşturulur. Blok içerisindeki verilerdeki en küçük bir değişiklik bile referans değerini değiştireceğinden bu değişiklik kendinden sonraki tüm blokları etkiler. Blokzincir ağındaki tüm katılımcılar (düğüm) tüm bloklardan oluşan zincirin tamamını kendilerine kopyalarlar. İşlemlerin gerçekleşmesi için oyun teorisine dayalı bir mekanizma ile uzlaşa sağlanması gerekir. Ağdaki her uç hem sunucu hem de istemcidir ve her birinde özdeş kopyalar tutulur. Açık anahtarlı kriptolama ve kriptolojik özetleme fonksiyonlarının kullanımıyla gizlilik ve şeffaflık sağlanır. Aşağıda verilmiş olan Şekil 2'de blokzincirin temel çalışma adımları basit biçimde verilmiştir:

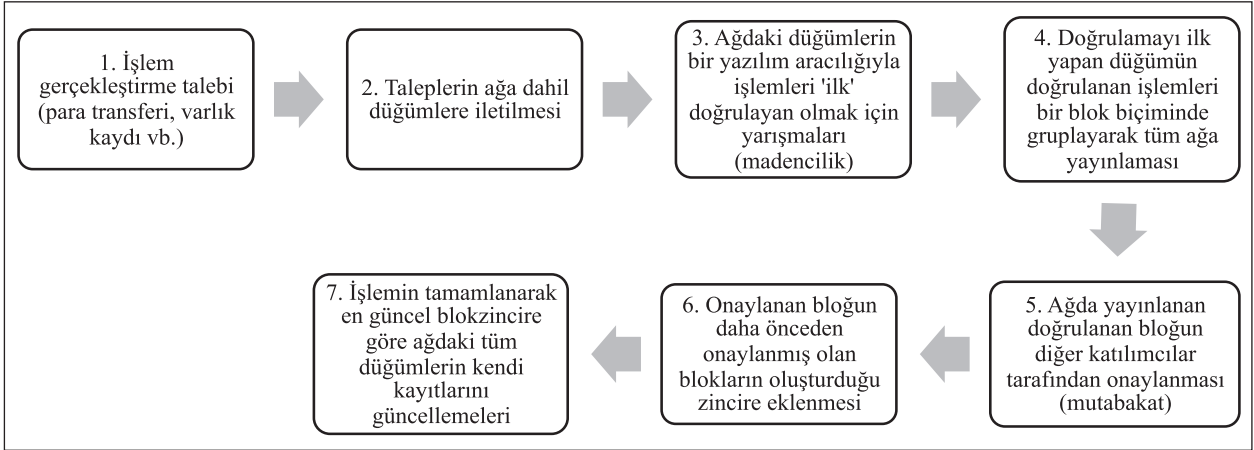
Blokzincir genellikle kayıt defterinin görünürlüğü ve erişim haklarının açıklığı bakımından kategorize edilmekte olup yaygın olarak görünürlük bakımından özel ve açık blokzincirler, erişim hakları bakımından da izin gerektiren ve gerektirmeyen blokzincirler olarak adlandırılmaktadır. Sadece yetkilendirilmiş kullanıcıların işlem geçmişi kayıtlarını görebildiği blokzincirler özel, sadece yetkilendirilmiş kullanıcıla-

Şekil 1. Dağıtık Kayıt Defteri Teknolojileri, Blokzincir ve Bitcoin Arasındaki İlişki



(Chartered Accountants Australia and New Zealand, 2017'dan uyarlanmıştır.)

Şekil 2. Blokzincir Teknolojisinin Temel Çalışma Adımları



(Yazarlar tarafından oluşturulmuştur.)

rın blokların geçerliliğinin onaylanması ve işlemlerin gerçekleştirilmesi ve doğrulanması mekanizmasında yer alabildiği blokzincirler de izin gerektiren blokzincirler olarak adlandırılır.

Deloitte 2019 yılı Mart ayında yayınlamış olduğu finans alanında blokzincirin kullanılması konulu rehberde bu teknolojinin finans alanında tanımlanmış olan süreçleri yeniden şekillendireceğini vurgulamakta, blokzinciri bir veya birden fazla tarafça kullanılan mevcut uygulamalar (Kurumsal Kaynak Planlama –ERP– sistemleri gibi) ile entegre olabilen dağıtık ve paylaşılan bir kayıt defteri olarak tanımlamaktadır. Kurumsal kullanım için tasarlanan özel blokzincir ağlarında ağa katılım izne tabi olup katılımcıların kimlikleri kriptografik anahtarlarla kontrol edilmektedir. Herhangi bir işlem bir blokzincir üzerinde kaydedilmeden önce mutabakat durumunu değerlendiren bir protokolle katılımcıların işlemin geçerliliğini doğrulamaları gerekir. Bir bloktaki her veri şifrelenmiştir ve her bir blok bir önceki bloğa benzersiz bir tanımlayıcı (hash – özet değeri) ile bağlanır. Blokzincirde kaydedilen işlemler ağ katılımcılarının bilgisayarlarında neredeyse eş zamanlı olarak güncellenir ve dağıtılır. Böylece blokzincir ağındaki her bir katılımcıda aynı veri kaydı bulunur. Eğer herhangi biri bloktaki veriyi değiştirmeye çalışırsa diğer katılımcılar blokları birbirlerine bağlamakta kullanılan özetleme mekanizması vasıtasıyla uyarılırlar.

Blokzincir teknolojisi bilgisayar bilimleri, kriptografi ve ekonomi alanlarının üzerine inşa edilmiştir. Bu teknoloji konusunda derinleşmek için bilgi sahibi olunması gereken konular temel olarak bilgisayar bilimleri alanında veri yapıları, kriptografi, dağıtık

sistemler, ağ kurma, ekonomi alanında oyun teorisi, makroekonomi ve mikroekonomi başlıkları altında toplanmakta olup bunların yanında Bitcoin'in teknik altyapısı ile Ethereum ve akıllı sözleşme programlama konuları hakkında da bilgi sahibi olunmalıdır (Qureshi, 2018).

2.2. Blokzincir teknolojisinin avantajları ve problemleri alanlar

Blokzincir teknolojisinin tasarımı itibarıyla sunduğu en önemli avantajlar kayıtlı verilerin değiştirilememesi, tamamlanan her bir bloğun oluşturduğu zincirin ağdaki her bir katılımcıda özdeş ve eşzamanlı olarak dağıtık biçimde tutulması, işlemlerin doğrulanması ve onaylanması için merkezi bir otoriteye gereksinim duyulmaması ve herhangi bir kopyadaki bozulmuş ya da manipüle edilmiş veriyi içeren zincirin sistemi tehlikeye atmaması (güvenilirlik) biçimindedir.

Teknolojinin ortaya çıkışı sürecinin altında yatan felsefe açık bir toplum için bireylerin mahremiyetinin korunması, şeffaflığın artırılarak merkezi otoritelere ve araçlara olan bağımlılığın ortadan kaldırılması ve üçüncü bir tarafa ihtiyaç olmadan tamamen kriptolojiye ve açık kaynak kodlu yazılımlara dayalı bir güven mekanizmasının inşa edilmesidir. İlk olarak Bitcoin ile ortaya konulan sistem bu felsefe ile hedeflenen temel unsurları başarıyla yerine getirmiştir.

Şeffaflık, gizlilik, dağıtık yapı ve güvenliğe ilave olarak blokzincir teknolojisinin sağladığı bazı önemli avantajlar aşağıdaki biçimde sıralanmaktadır:

- Aracılara gereksinim duyulmaması sonucunda işlem maliyetlerinde azalma,
- Çok düşük miktarda ödeme ve transfer işlemlerini gerçekleştirebilme,
- Bankacılık sistemine dahil olmayan insanların finansal işlemlerden faydalanabilmesi için bir ortam sağlama (sosyal yardımların bankacılık sistemini kullanmadan blokzincir ile dağıtılabilmesi gibi),
- Gizli ve özel anahtarlı şifreleme ile insanların kendi verilerini yönetebilmeleri,
- Farklı birimler arasında veri paylaşımını kişisel mahremiyeti ihlal etmeden sağlayan yapı,
- Küçük ve orta ölçekli işletmelerin yerel ve ulusal yönetimlerle daha kolay iletişim kurabilmeleri,
- Yenilikçi fikirler ve projeler için kaynak toplamayı kolaylaştırması,
- Veri koruma maliyetinin düşürülmesi.

Blokzincir teknolojisi ihtilafların giderilmesi ve farklı birimler arasında mutabakat işlemlerinin yürütülmesi gibi manuel faaliyetleri azaltma veya ortadan kaldırma avantajını sunmaktadır. Kayıtların geriye dönük olarak değiştirilememesi, her işlemin birden fazla tarafça doğrulanması ve onaylanması gerekliliği bir taraftan geleneksel sistemlere göre etkinliği azaltırken bir taraftan da işlemlerde şeffaflığın artması, faaliyetlerin basitleşmesi ve yolsuzlukların en aza indirilmesi gibi avantajlar sunmaktadır (Chartered Accountants Australia and New Zealand, 2017).

Blokzincir yeni bir teknoloji olmasının ötesinde ölçeklenebilirlik, veri gizliliği, yetki/yargı uyumsuzlukları ve dış kaynaktan temin edilen hizmetlere ilişkin sözleşmelerin performanslarından emin olunmaması gibi genel riskler taşımaktadır. Özellikle yetki problemleri blokzincirin dağıtık otonom kuruluşlara sahip olma özelliği yüzünden büyük kaygı doğurmakta, bir veri ihlali veya yasal bir anlaşmazlık durumunda yasal sorumluluğun kimde olacağı ve yetki sınırları ile ilgili düzenleme ve yasalarla nasıl başa çıkılabileceği soruları akla gelmektedir (Chalker, 2018).

Chalker (2018) diğer teknik riskleri; hesap güvenliği, akıllı sözleşmelerdeki kodlama hataları, iş süreçlerinin entegrasyon ihtiyacı, veriye ve şifreleme anahtarlarına erişim ve izinler, gerçek iş uygulamalarının azlığı biçiminde sıralamaktadır. Greenspan (2016) blokzincir ile klasik veri tabanlarının farklarını dört temel başlık altında değerlendirerek blokzincirin

aracı ve merkezi otoriteyi ortadan kaldırması, yüksek hata toleransı (dayanıklılık) bakımlarından veri tabanlarının ise performans ve mahremiyet bakımından daha avantajlı olduğunu belirtmiştir.

Teknolojinin anlaşılmasının güçlüğü blokzincirin popülerleşmesinin önündeki bir diğer engeldir. Blokzincirin algoritmaları ve çalışma prensibi önemli miktarda sistem ve güvenlik bilgisi gerektirmektedir. Bu nedenle yöneticiler, muhasebeciler ve denetçiler bu teknolojiyi doğru ve etkin biçimde kullanabilmek için eğitim almalıdırlar (Dai, 2017, s. 82).

Değiştirilemezlik özelliği blokzincirin en temel ve en faydalı özelliği olmakla birlikte aynı zamanda pratik uygulamalarda en önemli kısıtlılığdır. Blokzincir temel olarak hangi bilginin ilave edildiğini gösteren bir listedir. Günümüzde kamuda kullanılan geleneksel veri tabanlarından farklı olarak blokzincire eklenen bir verinin silinmesi mümkün değildir. Karar vericiler blokzincirin bu avantajının veri güncelleme ve silmenin imkansız hale gelmesine ağır basıp basmadığına karar vermeli, değiştirilemezlik özelliğinin kullanmak istedikleri alanda uygulanabilir olup olmadığını değerlendirmelidirler (Yaga, Mell, Roby ve Scarfone, 2018, s. 34).

Değiştirilemezlik özelliği nedeniyle kişisel bazı bilgiler blokzincirde kaydedilirse unutulma hakkı gerçekte uygulanamaz. Bununla birlikte, devletlerin tutmuş oldukları kimlik bilgisi ya da adli kayıtlar gibi bilgiler unutulma hakkı kapsamında olmayıp bu bilgilerin silinmesi talep edilemez. Ayrıca, çoğu kamu sektörü blokzincir uygulaması izin gerektiren yapıdadır ve sadece yetkilendirilmiş kamu çalışanları erişimi kontrol edebilirler (Berryhill, Bourgerly ve Hanson, 2018, s. 29). Açık ağlarda veri paylaşan blokzinciri uygulamalarının hayata geçirilmesi halinde şifreleme metotlarının kullanıcı gizliliğini sağlama garantisi verilmelidir. Kişisel bilgilerin depolanmasının muhtemel olduğu durumlarda gizlilik ve mahremiyet en önemli önceliktir. Kurallar ve kanunlar bu tip bilgilerin korunması konusunda çok katıdır.

Kamu ve özel sektör kuruluşları genellikle büyük miktarda veriyi belgeler, görüntüler, videolar ve uygulamalar gibi farklı biçimlerde depolamak için veri tabanları kullanmaktadırlar. Blokzincir ise daha genel olarak bir işlemler listesidir ve çoğunlukla akıllı sözleşmeleri yönlendirmek ve çalıştırmak için küçük veri parçalarını içerirler. Genel veri depolama için tasarlanmamıştır (Yaga vd., 2018, s. 34). Bununla birlikte,

eğer işlem kayıtlarının güvenilir ve dağıtık biçimde yürütülmesi hedefleniyorsa blokzincir teknolojisi uygulanabilir bir çözümdür. İhtiyaçları giderecek, geleneksel veri depolama çözümleri ile blokzincir teknolojisini bir arada kullanan hibrit bir yaklaşım da pekala mümkündür. Sadece veri depolamak için bir çözüm aranıyorsa blokzincir teknolojisi uygun olmayabilir.

Blokzincir platformlarını en güçlü kılan özelliklerin başında kriptografi gelmektedir. Bu kapsamda kullanılan şifreleme yaklaşımları oldukça güçlü olsa da, kuantum bilişim (*quantum computing*) gibi alanlardaki gelişmelerle birlikte bu konuda gelecekte çeşitli zafiyetler görülebileceği düşünülmektedir. Bu sistemlerin kabul edilebilir sürelerde günümüzün gelişmiş ikili şifreleme yöntemlerini kırması mümkün olacaktır. Bu blokzincir dünyası için hemen değil ama uzun vadede bir risk oluşturmaktadır (Usta ve Doğantekin, 2017, s. 105)

Belirli bir merkezi otoriteye bağlı olmaması istenmeyen durumlar ortaya çıktığında (hesaplara erişim şifresinin unutulması, hatalı işlemler vb.) kime başvurulacağı sorusunu ortaya çıkarmaktadır. Yazılım kodu geliştiricileri, blokzincir tasarımında doğrulama ve onaylama adımlarından sorumlu yetkili düğümler, kullanıcılar ve diğer karar vericilerin koordinasyonu konusunda henüz bir standart bulunmamaktadır.

Blokzincir teknolojisi ile ilgili yasal düzenleme ve standartlar henüz gelişim aşamasındadır. Akıllı sözleşmelerin hukuki altyapısı ve bağlayıcılığı, blokzincir denetim izlerinin mahkemelerde delil olarak kullanılıp kullanılamayacakları ve bu teknolojinin kullanımının bazı alanlarda zorunlu olup olmaması gibi konuların cevapları henüz belirsizliğini korumaktadır. Sistem dönüşümü için yüksek yatırım gereksinimi ve yeterli nitelikte insan kaynağının yetersizliği de diğer belirsizlik alanlarıdır.

Bu ölçüde hızlı bir büyüme bilgi teknolojileri karar vericilerinin karar vermesini güçleştirmektedir. Blokzincir teknolojisinin veya işlettiği ağın geniş kabul görmüş standartları bulunmamaktadır. Birçok blokzincir tedarikçisi küçük firmalar olduklarından bilgi teknolojileri ve satın alma birimleri için bu firmalarla birlikte proje yürütme kararı çok zordur. Aynı zamanda gizlilikle ilgili riskler de bulunmaktadır (Cheng, Daub, Domeyer ve Lundqvist, 2017).

İşlemlerin mutabakat algoritması ile doğrulanmadan önce tüm ağda dağıtılması gerektiğinden bant genişliği bir diğer önemli konudur. Kullanıcıların sayısı ve bunun sonucunda da işlem sayıları arttıkça daha iyi bir ağ bağlantısı gerekmektedir. İyi bir ağ bağlantısı ve büyük depolama kapasitesi etkin bir kayıt yönetimi gerektirmekte, daha fazla enerji tüketimi ve maliyete sebep olmaktadır (Brender, Gauthier, Morin ve Salihi, 2018, s. 10). 30 Mart 2019 tarihi itibarıyla Bitcoin'in tahmin edilen yıllık elektrik tüketimi 52 terawatt/saat¹ olup bu miktar 5 milyona yakın Amerikan hanesinin ve Bangladeş gibi bazı ülkelerin elektrik tüketimine ve dünyanın elektrik tüketiminin %0,24'üne eşittir (Digiconomist, 2019). Ticari işler için ihtiyaç duyulan yüksek hacimle çok kısa zaman içerisinde başa çıkma kabiliyeti bakımından halihazırda kullanılan veritabanı sistemlerinin gerisindedir.

Ölçeklenebilirlik bir sistemin boyutunda veya hacminde meydana gelen değişim sonucunda o sistemin fonksiyonlarını aynı biçimde sürdürebilmesidir. Blokzincirde katılımcı sayısı arttıkça ölçeklenebilirlik problemi ortaya çıkabilmektedir. Tasarımı gereği bir blokzincir kayıt defteri ilk bloktan itibaren bütün işlemleri içermektedir. Bu nedenle kullanıcı ve işlemlerin sayısı arttıkça kayıt defterinin boyutu da büyümektedir. Bitcoin platformunda saniyede en fazla yaklaşık 7 işlem gerçekleştirilebilmektedir. Bu problem büyük oranda herkese açık olan blokzincirler için geçerli olup bazıları saniyede binlerce işlem gerçekleştirebilen özel blokzincirlerde bu problem çözülmüştür (Brender vd., 2018, s. 10).

Blokzincir teknolojisinde kullanılan açık-özel anahtar yapısındaki özel anahtarın saklanması kullanıcının sorumluluğundadır. Özel anahtarın kaybedilmesi ya da erişim şifresinin unutulması durumunda kullanıcının elinde şifrelenmiş işlemlerin sahipliğini doğrulayacak hiçbir bilgi kalmamaktadır. Bu nedenle bu anahtarların kaybedilmesi ilişkili varlığın da kaybedilmesi anlamına gelmektedir (Usta ve Doğantekin, 2017, s. 106).

Blokzincir teknolojisi yüksek güvenli işlemleri vadedmesine karşın yolsuzlukları tamamen ortadan kaldıramaz. Yanlışlıkla veya bilinçli olarak hatalı ya da yetkisiz bir adrese değer transferi yapıldığında bu işlemi tersine çevirmek imkansızdır. Blokzincir

1) Bir watt'ın 1 trilyon katına denk düşen terawatt büyük barajların üretimini ve ulusal çapta enerji tüketimini ölçmek için kullanılacak kadar büyük bir elektrik ölçü birimidir. Örneğin dünyanın en büyük hidroelektrik santrallerinden biri olan Atatürk Barajı'nın yıllık elektrik üretimi 8,9 terawatt civarındadır (Radore, 2017).

teknolojisini kullanan kuruluş bir ortalama saldırısına maruz kalırsa blokzincirin merkezi bir yönetimi olmadığı için bu olayın raporlanacağı bir dolandırıcılık departmanı yoktur. Özel anahtar kaybedilirse bu anahtarla ilişkili hesaba (ve varlığa) erişim artık mümkün olmaz (Psaila, 2017, s. 3)

Blokzincir teknolojisi her ne kadar klasik sistemlerdeki güvenilir bir aracı ihtiyacını ortadan kaldırıyor olsa da bazı durumlarda, özellikle akıllı sözleşme kullanımında bazı güvenilir bilgilere erişilmesi gerekmektedir, bu durum da blokzincir teknolojisinin en temel özelliklerinden biri ile çelişkili bir durum ortaya çıkarmaktadır (İlkbahar, 2019). Bu çelişkili duruma örnek olarak belirli bir sıcaklık değerinin sağlanmasına yönelik olarak programlanmış bir akıllı sözleşmenin esas alacağı sıcaklık değerinin güvenilir bir kaynaktan sağlanması ihtiyacı verilebilir.

Teknolojinin finans ve sağlık kuruluşları gibi sektörlerce gerçekten çekicilik kazanması için birçok problemle başa çıkılmalıdır. Bunlar arasında veri güvenliği ve gizliliği, teknik uzman havuzunun yetersizliği, mevzuat ve uygunluk gereksinimlerinin bu yeni teknolojiye uygulanması bulunmaktadır. Bu güçlükler teknoloji olgunluğa eriştikçe giderilecek olup blokzincir teknolojisini kendi kuruluşlarında deneyimleyen geliştiricilerin dikkatini çekmeyen bir başka konu vardır: denetim güçlüğü. Blokzincir çözümleri geliştiren inovasyon ve strateji ekipleri ile yapılan çalışmalar sonucunda dört ana sorun tespit edilmiştir (Smith, 2018):

- Blokzincir oldukça yeni bir konudur. İlk uygulamanın üzerinden sadece 10 yıl geçmiştir ve birçok uygulama henüz olgunlaşmamıştır. Aksine, yönetimlerin güven duydukları sistemler on yıllardır denenmiştir ve bunları uygun biçimde kullanmak için spesifik kılavuz ve prensipler bulunmaktadır. Denetim ekiplerinin bu sistemden nasıl tam katkı elde edebileceği konusunda uzmanlıkları bulunmamaktadır.
- Bu yeni teknolojinin içerdiği kontroller geleneksel kontrollerden oldukça farklıdır ve denetçilerin blokzinciri kimin kontrol ettiği, sisteme kimlerin erişim sağladığı, sunucuların nerede bulunduğu, hangi fiziksel ve dijital kontrollerin bulunduğu, faaliyetleri kimin izlediği, teknolojinin gerçekten de iddia edildiği biçimde çalışıp çalışmadığı gibi sorular sormaları gerekmektedir.
- Blokzincir teknolojisi konusunda teknik uzmanlık

zayıftır. Blokzincir deneyimine sahip BT birimi sayısı çok azdır. 2017 Küresel Dijital IQ Anketi'nde finans servisleri yöneticilerinin %86'sı kuruluşlarında henüz yeterli blokzincir yetkinliğinin geliştirilmediğini ifade etmiştir. İç Denetim ekiplerinde bu sayı çok daha azdır.

- Blokzincir teknolojisinin ilk öne çıkan uygulaması Bitcoin olduğundan teknoloji konusunda olumsuz bir önyargı bulunmaktadır. Blokzincir teknolojisinin Bitcoin'den daha önemli bir konu olduğuna inanmakta genelde güçlük çekilmektedir.

Tüm bu teknik sıkıntılara ilave olarak PwC (2018) ve Deloitte'a (2018) göre blokzincirin kabulünün önündeki en büyük engel yasal düzenlemelerdeki belirsizliktir. Sistemlerin amaçlandıkları biçimde çalıştılarından emin olunabilmesi için gerekli standartlar ve kontroller henüz yetersizdir. Örneğin; Avrupa Birliği'nde blokzincir projelerinin Genel Veri Koruma Kanunu (GDPR) gerekliliklerini nasıl karşılayabileceği henüz net değildir.

2.3. Blokzincir teknolojisinin kullanım alanları

Blokzincir teknolojisinin kullanım alanları farklı birçok yerde listelenmekle birlikte bu liste her geçen gün uzamakta, sürekli yeni kullanım alanları ortaya çıkmaktadır. Bu nedenle, sunulan her liste daima eksik olacaktır (Filipowski, 2018). Blokzincirin kamuda kullanımında üç konu öne çıkmaktadır: kimlik yönetimi, tapu kayıtları ve elektronik oylama (Killmeyer, White ve Chew, 2017, s. 14-15). Berryhill, Bourgerly ve Hanson (2018) blokzincir konusundaki gelişmelerin yoğunlukla finans alanında yaşandığını ancak kamu sektöründe de son dönemde hızlı bir gelişim gösterdiğini öne sürerek kamu alanında yürütülen projelerde en sık rastlanan konuların dijital kimlikler, kişisel kayıtlar (sağlık, mali bilgiler), tapu kaydı, sosyal yardımların takibi, tedarik zinciri olduğunu belirtmektedir.

Nagpal (2017) blokzincirin çok faydalı olacağı üç konuyu; verinin aslına uygunluğu ve doğrulanması, akıllı varlık yönetimi ve akıllı sözleşmeler olarak sıralamaktadır.

Avrupa Parlamentosu'na sunulmak üzere 2017 yılında hazırlanmış olan raporda blokzincir teknolojisinin kullanımının öne çıktığı ve gelecekte de kullanım potansiyelinin yüksek olduğu konular dijital paralar, dijital içerikler ve telif hakları yönetimi, patentler,

elektronik oylama, akıllı sözleşmeler, tedarik zinciri yönetimi ve merkezi olmayan özerk kuruluşlar olarak belirtilmiştir (Boucher, Nascimento ve Kritikos, 2017).

Maupin (2018) göre hesap verebilir, güvenli, denetlenebilir ve şeffaf yapısı ile blokzincir teknolojisi tüm dünya vatandaşları için kapsayıcı küresel bir dijital ekonomi inşa edilmesi için kilit konumdadır. Devletlerin, vatandaşlarının sınır ötesi ekonomik işbirliğine inançlarını tesis etmeleri ve herkesin faydasına olan küresel ekonominin sağlanması için blokzincir kritik bir role sahiptir. Maupin bu teknolojinin ekonomik direncin geliştirilmesi, finansal kapsamın geliştirilmesi, vergilendirme, ticaret ve yatırım, istihdam, iklim, sağlık, sürdürülebilir gelişim ve kadının güçlendirilmesi gibi alanlara odaklanan politik amaçlar doğrultusunda kullanılmasını önermektedir.

Dünyadan kullanım örnekleri ve halihazırda yürütülmekte olan çalışmalar değerlendirildiğinde blokzincir teknolojisinin kullanılabilir olduğu konularda dijital kimlikler ve sertifikalar (yeterlilik belgeleri, lisanslar vb.), kişisel kayıtların tutulması ve yönetimi (sağlık bilgileri, sigorta, mali vb.), finansal hizmetler ve bankacılık, tapu kayıtları ve gayrimenkul işlemleri, tedarik zinciri yönetimi, varlık izleme ve envanter tutma, sosyal yardımların dağıtılması, hak sahiplikleri, telif hakları ve patentler, sözleşme ve tedarikçi yönetimi, yenilenebilir enerji, oy verme, kitlesel fonlama aracı olarak kullanım ve sadakat programları öne çıkmaktadır.

3. BLOKZİNCİR TEKNOLOJİSİ VE İÇ DENETİM

Teknolojinin içinde gömülü biçimde bulunan şeffaflık, izlenebilirlik, değiştirilemezlik ve kural ve prosedürlerin entegrasyonu özellikleri süreçleri ve bilgi üretimini zenginleştirerek denetim ve kontrol prosedürlerini önemli ölçüde değiştirmekte, hatta bazı durumlarda işe yaramaz hale getirmektedir. Aynı zamanda bu özellikler denetçiler için en iyi uygulamaların yeniden tasarlanması, kural ve prosedürlerin güncellenmesi, yeni standartların tanımlanması gibi fırsatlar da yaratmaktadır (Brender vd., 2018, s. 3).

Blokzincir teknolojisi birçok kamu hizmeti için güvenli, şeffaf, hızlı ve düşük maliyetli çözümler vadetmekte olup kurumları için maksimum katkıyı sağlamayı amaçlayan iç denetçiler için de bazı fırsatlar

ve zorluklar ortaya çıkarmaktadır. Bu zorlukların üstesinden gelmek ve fırsatlardan faydalanmak için iç denetim birimleri denetçilerin hem blokzincir teknolojisi hem de blokzincir projeleri konusunda iyi biçimde eğitilmelerini sağlamalıdır (Rooney, Aiken ve Rooney, 2017, s. 41).

Blokzincir ile geliştirilen uygulamaların sayısındaki artış kayıt saklamayı gerektiren her şeyde olduğu gibi iç denetimi de etkileyecektir. İç denetim blokzincirin teknik mimarisinin detaylı analizini gerçekleştirmek için hazırlıklı olmalı, yeterli düzeyde şeffaflığı gerçekleştirmek ve blokzincir uygulamalarının amaçlandığı biçimde çalıştığını doğrulamak için stratejiler geliştirilmelidir (Pelletier, 2018).

İç denetim bakış açısı ile blokzincire dayalı uygulamalarda devrimsel olan şey bilgi ve işlemlere ilişkin gerçeğin bulunmasında yepyeni bir yaklaşım sunmasıdır. Blokzincirin ortaya çıkmasına dek gerçeğin kanıtı spesifik kayıt defterlerinin ya da veritabanlarının tutulmasına dayanan bir sistem ve bu sistemi yöneten güvenilir bir üçüncü taraf iken blokzincir ile bu yapı kökünden değişmektedir.

3.1. Blokzincir teknolojisinin iç denetim faaliyetlerine ve iç denetim mesleğine potansiyel etkileri

Denetim mesleğine özgü olarak blokzincir teknolojisi değiştirilmesi mümkün olmayan bir kayıt defteri ve gerçek zamanlı olarak işlemlerin tüm anakütlesi üzerinde testleri gerçekleştirme fırsatı sunmaktadır. Bu nedenle, blokzincir konusunda danışmanlık ve güvence hizmetleri sunan büyük dörtlü (*Deloitte, EY, KPMG ve PwC*) olarak da bilinen firmaları da içeren geniş bir kitlenin ilgisini çekmektedir (Sheldon, 2018, s. 1). Örneğin; PwC (2018) tarafından henüz patent süreci devam etmekte olan bir risk çerçevesi ve sürekli denetim yazılımını içeren 'Blokzincir Doğrulama Çözümü' adı verilen bir çerçeve geliştirildiği duyurulmuştur.

Sheldon'a (2018) göre blokzincir kullanımı kuruluşların güçlü BT yönetişimine ihtiyaç duyduğu gerçeğini değiştirmeyecek, hatta bazı durumlarda bu yönetişim çok daha karmaşık bir hale gelecektir. Sheldon (2018) "Özel ve İzin Gerektiren Blokzincir Denetiminde Bilgi Teknolojileri Genel Kontrolleri" başlıklı çalışmasında blokzincir denetimleri için BT genel kontrollerini üç kategoride incelemiştir: (1) Program Geliş-

tirme ve Değişiklik Yönetimi, (2) Bilgisayar İşlemleri, (3) Programlara ve Veriye Erişim.

Blokzincir tasarımındaki değişiklikler mutabakat protokolü, iletişim protokolü, akıllı sözleşmeler, dağıtık uygulamalar (Dapps) veya programın kaynak kodu ile gerçekleştirilebilir. Birden fazla kuruluşun katılımıyla oluşturulmuş olan konsorsiyum tipi blokzincir ağlarında bu tasarım değişiklikleri konusunda tüm üyelerin mutabakatı ve değişikliklerin hedeflenen biçimde uygulandığından emin olunmasını sağlayan bir mekanizmanın bulunması gerekmektedir. Denetçiler bu nedenle değişikliklerin kabul edilmesi ve kabulden sonra uygulanması konusunda üyelerin mutabakatlarına ilişkin mekanizmanın tasarımını ve işleyişini dikkate almalıdırlar.

Kuruluşlar blokzincir kullanmaya başladıkça eski sistemlerinden ve hatta üçüncü taraf bulut esaslı sistemlerden veri toplanması ve bu verilerin işlenmesinde bir geçiş dönemi yaşanacaktır. Bu sistemler blokzincirle bir arayüz oluşturacak, nihai olarak blokzincire yüklenen verileri üreteceğinden eski uygulamalar ve süreçlere ilişkin mevcut politika ve prosedürlerin sürdürülmesi ve hatta daha da geliştirilmesi gerekecektir. Blokzincire kaydedilen veriler artık değiştirilmeye karşı korumalı olsa da blokzincirin dışında iken genel BT risklerine karşı hala savunmasızdır. Verilerin bir üst sistemden blokzincire iletimindeki geçiş arayüzü bu yeni ortamdaki en hassas kontrol noktalarından biri olacaktır. Denetçilerin, kendine özgü BT ortamında bu veri geçişinin en kontrollü biçimde nasıl yapılabileceğinin belirlenmesi konusunda sorumlu birimlerle birlikte çalışmaları gerekecektir. Blokzincir iş sürekliliği ve felaket kurtarma planlaması konusundaki birçok endişeyi giderme potansiyeline sahiptir. Denetçiler, blokzincir arayüzü görevini üstlenen eski sistem erişilemez olduğunda hangi prosedürlerin izleneceğini görmek için iş sürekliliği/felaket kurtarma planlarını değerlendirmek isteyecektir (Sheldon, 2018, s. 7,8,9).

Kripto paraların ortak problemi özel bir anahtarla ilişkilendirilmiş dijital varlıklara bu anahtarın kaybedilmesi halinde erişilememesidir. Bu nedenle, blokzincir üzerinde dijital varlık hareketini kontrol etmek için açık ve gizli anahtar kullanılıyorsa denetçiler bu anahtarların saklanma sürecini ve özel anahtarın çalınması ya da başkası tarafından ele geçirilmesi halinde bu anahtarla ilişkili dijital varlığın kontrolünü yeniden ele geçirme sürecini ve anahtarla ilişkilendirilmiş varlıklara erişmeye artık gereksinim duyulma-

dığında bu varlıkların güvenliğinin sağlanması konusunu da dikkate almalıdırlar (Sheldon, 2018, s. 9).

Blokzincir güvenli veri işleme, değiştirilemez kayıtlar ve sağlam yapısı ile yeni bir teknoloji olmakla birlikte halen BT altyapısının bir bileşeni olduğu akıldan çıkarılmamalıdır. Etkin BT genel kontrolleri olmadan blokzincir tarafından üretilen verilerin güvenilirliği tam olarak sağlanamayacağından mutlaka düzgün işleyen BT genel kontrolleri ile desteklenmelidir.

Blokzincirde tutulan verilere dayanarak karar alan kullanıcılar verinin nasıl kontrol edildiği, sorgulandığı ve hedeflenen kapsama ne derecede uygun olduğunun anlaşılması konusunda çok dikkatli olmalıdır. İç denetçiler de hizmet sundukları tarafları blokzincirin her sorunun çözümü olmadığı konusunda uyarmalı, blokzincirin sağlayacağı katkının paylaşılan bir veri tabanı ya da bir ERP sisteminden fazla olduğundan emin olunmasının önemini vurgulamalıdırlar (Sheldon, 2018, s. 11). Blokzincir teknolojisi halen tam olgunlaşmamış ve gelişimini devam ettiren bir teknolojidir. Karar vericiler bu noktada teknolojiden faydalanmak konusunda erken davrananlardan veya kendini ispatlamış teknolojik çözümleri kullanmaya devam ederek bu yeni teknoloji için bekle ve gör yaklaşımını benimseyenlerden olmak konusunda bir karar vermelidirler.

Brender ve diğerlerinin (2018) İsviçre'deki 23 denetim firmasından 34 mali ve BT denetçisi ile yüz yüze görüşme yolu ile yaptıkları anket sonucunda denetçilerin hemen hemen tamamının orta vadede denetim mesleğinde bir değişim olmasını bekledikleri, yarısından fazlasının ise denetim fonksiyonlarının çok daha fazla BT yönelimli olacağını bekledikleri sonucuna ulaşmıştır. Görüşülen bazı denetçiler denetçilerin programlama gibi spesifik BT yeteneklerine sahip BT mühendis denetçileri olacakları hipotezini öne sürmüşler, hatta bir kısmı 'blokzincir denetçisi' ifadesinden bahsetmiştir.

Brender ve diğerlerine (2018) göre denetim mesleği bir dönüm noktasındadır ve teknolojinin bu konudaki potansiyel yıkıcı etkileri tam olarak tahmin edilememektedir. Daha küçük ölçekli denetim firmaları bu değişikliklerle yüzleşmek için yeterli donanıma sahip değildir. Bu yıkıcı etkiler denetim mesleği paradigmasını daha fazla BT odaklı olacak biçimde değiştirecek, dolayısı ile denetçilerin profili de değişecektir.

Birçok denetçiye göre yeni denetim ve muhasebe standartları ve yeni gelişmeler konusunda güncel ka-

linmaya gerek duyulmakta, dahası BT yeteneklerinin geliştirilmesi gerekmektedir. Denetçilerin büyük bölümünün daha derin BT kabiliyeti konusunda eğitim ihtiyacı bulunmaktadır. Denetçiler kodlama, özetleme algoritmaları, kriptografi, akıllı sözleşmelerin teknik ve hukuki boyutu gibi konularla yeteneklerini genişletmeli, özellikle yeni ortaya çıkan yönetim problemlerini anlamak için kendilerini güncellemelidirler (Brender vd., 2018, s. 17, 22; Chalker, 2018).

İç denetim mesleğinin üst yönetime destek verme fonksiyonu dikkate alınarak blokzincir risklerini izlemek ve değerlendirmek için yeterli kaynaklara sahip olunup olunmadığı konusu değerlendirilmelidir. Bu kaynaklar ilave personel, dış kaynaktan temin edilecek uzmanlar, BT veya siber güvenlik birimleriyle daha yakın ilişkiler veya denetim personelinin gerekli eğitimi almaları için sağlanacak ilave bütçe olabilir (Kelly, 2019, s. 3).

Blokzincir teknolojisinin denetim mesleğine potansiyel etkileri değerlendirilirken iki farklı durum göz önünde bulundurulmalıdır; denetlenen tarafın blokzincir teknolojisini iş süreçlerinde kullanmaları sonucunda blokzincir sisteminin denetlenmesi ihtiyacı ve teknolojinin bir denetim aracı olarak kullanılması.

Dikkate alınması gereken bir diğer konu bazı durumlarda birden fazla kuruluşla işbirliği içinde çalışma ihtiyacıdır. Blokzincirlerin her biri kendi yönetim yapısına sahiptir ve bir blokzincir birden çok kuruluşa ait çok sayıda paydaşı içerebilir. Bu durumda, tüm paydaşların gereksinimlerinin karşılanıp karşılanmadığından emin olmak için farklı kuruluşlardaki iç denetçilerin birlikte çalışmaları gerekecektir (Rooney, Aiken ve Rooney, 2017, s. 42).

Doğanay'a (2019) göre gelişen teknolojilerle birlikte iş dünyası iki önemli riskle karşı karşıya kalmıştır; yeni teknolojilerin tam olarak anlaşılıp uygulanamaması, dijitalleşmenin beraberinde getirdiği siber risklerin anlaşılabilmesi. Bu durum denetim mesleği için de geçerlidir.

Chalker (2018), uygun yönetim, risk yönetimi ve kontrollerin başlangıçta inşa edilmesinin bir problem ortaya çıktıktan sonra uygulamaktan çok daha kolay olduğu düşüncesinden hareketle denetçilerin blokzincir süreçlerine erkenden dahil olmaları gerektiğini düşünmektedir. Blokzincir uygulamaları kurumun geleneksel BT yapısının dışında gerçekleşebileceğinden denetçiler, kurum BT organizasyonunun çok daha ötesine bakmalıdırlar.

3.2. Blokzincir teknolojisinin iç denetim faaliyetlerine sunduğu fırsatlar

Unerman ve O'Dwyer (2004), 2001 yılındaki *Arthur Andersen* ile bağlantılı *Enron* skandalı gibi bazı olumsuz tecrübelerin sadece bu firmaları değil küresel denetim endüstrisini olumsuz etkileyerek bu mesleğin en önemli varlığı olan kamu güveninin zedelenmesine yol açtığını belirtmektedir. Bu güvenin yeniden sağlanması için muhasebe ve denetim standartları gibi yeni düzenlemeler getirilmiş, bu düzenlemelerin getirdiği zorunluluklar firmalar için bazı işlemlerin karmaşıklığının artması, kontrol faaliyetlerinin ve raporlamaların maliyetlerinin yükselmesine neden olmuştur. Günümüzde, blokzincir teknolojisi kurumsal işletmelere dijital etkileşimlerini veya işlem kayıtlarını şeffaf, güvenli, denetlenebilir, etkili ve kesintilere karşı dayanıklı bir biçimde gerçekleştirme imkanı sunmaktadır.

Bu teknolojinin verilere daha etkin bir biçimde erişimi mümkün kılacağı açıktır. Herhangi bir varlığın ya da belgenin kodlanabilmesi veya bir kayıt defteri aracılığı ile referanslanabilmesi denetçilerin ve muhasebe çalışanlarının işlerini kolaylaştıracak, manuel işlemleri azaltacak, tüm işlemlerin izlenebilirliğini sağlayacaktır (Schatsky ve Muraskin, 2015, s. 2,3). Büyük uluslararası denetim firmaları bir denetimi gerçekleştirmek için gerekli olan zaman ve maliyetin kayda değer miktarda azalacağını öngörmektedir (Brender vd., 2018, s. 7). Bu teknoloji ile günümüz sistemlerinde her gün rutin olarak yürütülen bazı işler -farklı sistemlerdeki kayıtların mutabakat işlemleri gibi- gereksiz hale gelecektir (Rooney, Aiken ve Rooney, 2017, s. 42).

Blokzincir, bilgisayar işlemleri ile ilgili birçok riski azaltma ya da ortadan kaldırma potansiyeline sahiptir. Birçok kuruluş veri yedeklemesi için iç kontroller ve süreçlere sahiptir. Blokzincir ile veriler kalıcı bir kayıt defterinde depolandığından artık veri yedeklemeye gerek kalmayacaktır. Bir düğümle ilgili bir ihlal gerçekleştiğinde kalan diğer düğümlerde de kayıt defterinin tamamı, ilgili protokoller ve kaynak kodları bulunduğundan işlemler devam edecektir (Diedrich, 2016).

Blokzincirde işlemlerin grup işleme (*batch processing*) ile yayınlanması için bir çizelgeleme gereksinimi de yoktur. İşlemler iletişim ve mutabakat protokolleri tarafından belirlenen biçimde neredeyse gerçek zamanlı olarak gerçekleştirilir ve kaydedilir. Blokzincir

felaket kurtarma bakımından da önemli avantajlar sunmaktadır. Coğrafi olarak farklı bölgelerdeki düğümde tutulan kayıtlar bir felaket durumunda çalışmaya devam edecektir. Felaket durumu sona erdiğinde bundan etkilenen düğümler yeniden blokzincir ağına dahil olarak en güncel kayıtları kendilerine kopyalayabilirler (Diedrich, 2016).

Blokzincirin kayıtların değiştirilemezlik özelliğinden dolayı kaydedilen verilerin korunması için ilave kontrollere gerek yoktur. Tüm işlemlere ait kayıtlara anlık olarak erişilebilir. Tüm işlemler ayrıca otomatik olarak teknolojinin kendisi tarafından doğrulanarak onaylanmaktadır. Bu nedenle denetçilerin temel odak noktaları zaten teknoloji tarafından yerine getirilen, işlemlerin mevcudiyetini, kanıtların bulunmasını, doğruluğunu ve tamlığını garanti etmek olmayacaktır (Sheldon, 2018, s. 10; Brender vd., 2018, s. 20). Blokzincir teknolojisi eski verilerin silinmesi veya değiştirilmesine ilişkin riskleri de hemen hemen ortadan kaldırmaktadır. Bir blok onaylanıp zincire eklendikten sonra zincirdeki eski verilerin değiştirilmesi blokzincir ağındaki düğümler değişiklik konusunda tamamen mutabık olmadıkça imkansızdır.

Blokzincir teknolojisi şeffaf bir teknolojidir, maliyetleri düşürebilir, daha hızlı ve daha ucuz biçimde işlemler gerçekleştirebilir. Ayrıca asla değiştirilmesi mümkün olmayan işlem kayıtları sunarak denetim izlerini (*log*) otomatik hale getirmektedir. Bu durum denetimlerin gelecekte daha etkin biçimde gerçekleştirilmesi için bir fırsattır (Whitehouse, 2018). Kelly'ye (2019) göre blokzincir teknolojisi tam potansiyelini yansıttığında her çeşit işlem için kusursuz ve değiştirilmesi mümkün olmayan bir şeffaflık sağlayacak, tüm endüstrinin çalışma şeklini değiştirecek, hatta denetim mesleğini dönüştürecektir.

Kelly (2019) ve Rooney ve diğerleri (2017) blokzincir teknolojisi ile tüm işlemlere her an ulaşılabilirliğinden örneklemeye ihtiyaç duyulmayacağını ileri sürmektedir.

Blokzincir teknolojisinin iş süreçlerinde kullanımının denetim iş yükünü azaltması ve bu ve benzeri teknolojilerin denetimlerde daha yoğun kullanılması ile denetçilerin daha fazla katma değer sağlayıcı faaliyetlere odaklanmaları da mümkündür. Operasyonel ve finansal bilgilerin blokzincire sürekli olarak kaydedilmesi sayesinde bu bilgi istendiği anda analiz edilebilir ve gerçek zamanlı denetimler gerçekleştirilebilir.

Psaila (2017) blokzincir teknolojisinin denetim bakımından fırsatlarını kaydedilen verilerin değiştirilememesi, işlemlerin sürekli olarak doğrulanabilmesi ve şeffaflık, doğrulama sürecinin otomasyonunun denetim ortamında maliyet etkinliği sağlaması, örneklem seçimi yerine tüm anakütlenin denetlenebilmesi ve sağlanan güvencenin artması, sürekli denetimi mümkün kılması biçiminde sıralamaktadır.

Nesnelerin interneti gibi diğer bazı teknolojilerle birlikte kullanıldığında blokzincir teknolojisi bazı fiziksel varlıkların hareketlerinin de gerçek zamanlı olarak izlenebilmesini mümkün kılmaktadır. Bu teknoloji ile aynı zamanda, neredeyse gerçek zamanlı olarak kullanıcı rolleri ve taleplerine göre farklı biçimde içerikleri düzenlenmiş olan blokzincir kayıtlarını yöneticiler, denetçiler ve diğer bazı paydaşlar gibi ilgili taraflara sürekli olarak yayınlamak da mümkündür (Dai, 2017, s. 60, 61).

Tysiac (2018) blokzincirin yaygınlaşması ile denetçiler için akıllı sözleşme denetçisi, konsorsiyum blokzincirlerin kontrol etkinliğinin denetimi, katılım için izin gerektiren blokzincirlerde erişim izni yöneticisi, blokzincir ağı katılımcılarının arasındaki olası ihtilaflar için arabulucu gibi yeni rollerin ortaya çıkabileceğini öne sürmektedir.

Blokzincir teknolojisi ile tutulan muhasebe kayıtları sayesinde herhangi bir kişi istediği zaman işlemleri bir gelir tablosu ve bilanço biçiminde toplayabilir ve firma veya denetçileri tarafından hazırlanan üç aylık mali durum raporlarının beklenmesi gerekmez. Mali raporlamadaki bu radikal değişikliğin bir maliyeti olmakla birlikte çok önemli iki katkısı bulunmaktadır: Onaylı bilgilerin dışarıya açılmasıyla firmanın verilerinin doğruluğuna duyulan güvenin artması, firmanın kayıtları ve belgelerinin doğruluğu konusunda güvence vermek için işe alınan ve yolsuzluğa da açık bir süreç yürüten yüksek maliyetli denetçilere gerek kalmaması (Yermack, 2017, s. 24).

Yermack'a göre (2017) blokzincirde gerçek zamanlı tutulan kayıtlar sayesinde şüpheli varlık transferleri ve çıkar çatışması anlamına gelebilecek bazı diğer işlemlerin anında fark edilmesi sağlanabilecek, gerçek zamanlı muhasebe kayıtlarının tutulabilmesi ile denetim firmalarının rolleri azalacak, bu teknolojiye dayanan akıllı sözleşmelerin kullanımıyla finansal problemlerin beklenen maliyetleri ve dava açma ihtiyacı azalacaktır.

Blokzincire dayalı sürekli denetim kavramı bu otonom ve kendi kendini düzenleyen paradigma içerisinde denetim mesleğinin rolü ile ilgili tartışmaları da beraberinde getirmektedir. Denetçilerin işlemlerin doğruluklarına dair güvence verme rolleri azalsa da hükümleri, görüşleri ve içgörülerini çok daha gerekli hale gelecektir. Denetimin odağı kayıtların izlenmesi ve doğrulanmasından sistemik değerlendirme, risk değerlendirme, önleyici denetimler ve yolsuzlukların tespiti gibi daha karmaşık analizlere doğru kayacaktır (Dai, 2017, s. 76).

Blokzincir önemli ancak düşük değerli olan doğrulama zamanında kayda değer miktarda azalmaya neden olarak denetçilerin zamanlarını blokzincirin kullanımını konusundaki yönetim rollerinin değerlendirilmesi, "akıllı" ve "gerçek zamanlı" denetimlerin gerçekleştirilmesi, blokzincir sonrası çağda diğer karmaşık iç kontrol mekanizmaları ve risk yönetimi stratejisi konularında tavsiyelerde bulunmak gibi katma değeri daha fazla olan alanlara tahsis edebilirler. Bu, iç denetçilerin kuruluşlardaki güvenilir danışmanlar olma fonksiyonlarını pekiştirecektir (Yeung, 2017).

Kelly'ye (2019) göre yönetim kurulları hızlı bir biçimde blokzincir ile kripto paralar arasındaki farkları, blokzincir tasarım tiplerinin birbirlerinden farklarını öğrenmeli, teknoloji risk komitesi oluşturulması veya yeni ortaya çıkan teknolojiler ve blokzincir konusunda yetkin yeni yöneticilere yönetim kurullarında yer verilmesi konusunu dikkate almalıdırlar. Burada, iç denetim birimlerinin bu kavramlar hakkında yeterli düzeyde bilgi sahibi olarak yeni ortaya çıkan riskler ve teknolojinin detayları konularında üst yönetime eğitim ve danışmanlık vermek üzere hazırlıklı olmaları hem denetim mesleği hem de hizmet verilen kuruluş için önemli bir fırsattır.

3.3. Blokzincir teknolojisinin iç denetim faaliyetleri bakımından risk ve tehditleri

Geçmişte, ERP ve EDI (Electronic Data Interchange - Elektronik Veri Alışverişi) gibi yıkıcı teknolojiler kurumların verimliliğine önemli katkıda bulunmuş, maliyetleri düşürmüştür. Bununla birlikte teknolojik karmaşıklık, önemli miktarda finansal yatırım ve zaman gereksinimi, teknolojinin diğer paydaşlara yaygınlaştırılmasındaki güçlükler ve süreçlerde değişiklik gerekliliği gibi unsurlar bu yeni teknolojilerin benimsenmesini engelleyebilmektedir (Dai, 2017, s. 79).

Blokzincir teknolojisi kuruluşların iş görme biçimlerinde büyük değişiklikler gerçekleştirmek konusunda büyük vaatler sunmanın yanında üst yöneticiler ve yönetim kurulları için bazı sorunlara yol açma potansiyelini de taşımaktadır. Teknolojinin yol açacağı dönüşümün neler olabileceği konusunda hiç kimsenin gerçekten bilgisi bulunmamaktadır. 1994 yılındaki internet veya 2005 yılındaki sosyal medyayı hatırlamak gerekirse; herkes teknolojinin bazı büyük ve önemli etkilerinin olacağını bilmekte, ancak hiç kimse bunun nasıl olacağını kesin olarak bilememektedir (Kelly, 2019, s. 1).

Protiviti'nin 2019 yılında kurumsal riskler konusunda yapmış olduğu ankette yönetim kurulu başkanları ve diğer üst yöneticilerin en büyük endişesinin inovasyon ve yeni teknolojileri kucaklamakta yetersiz kalmak olduğu ortaya çıkmıştır (Kelly, 2019, s. 1). Karar vericilerin blokzincir teknolojisini de içeren yeni teknolojiler konusunda karşı karşıya oldukları en önemli risk temkinli davranmaları durumunda teknolojinin gerisinde kalmaları ve fırsatları kaçırmaları, öte yandan erken davranarak bu fırsatları yakalamak stratejisini seçmeleri durumundaysa olumsuz bir senaryoda gereksiz yatırım yapılması ve kaynakların israf edilmiş olması durumudur. Bu riskleri en uygun biçimde yönetebilmek için konu hakkında yeterli ve güncel bilgiye sahip olarak ilerlemeleri yakın biçimde takip etmek gerekmektedir.

Blokzincir teknolojisi genellikle önemli depolama ve hesaplama kaynaklarına ihtiyaç duyduğundan, büyük şirket sistemlerinde benimsenmesi, daha büyük depolama sistemlerinin öngörülen gelişimine, veri iletimi için daha geniş bant genişliğine ve hesaplama gücünün önemli ölçüde genişlemesine bağlı olacaktır (Dai, 2017, s. 80).

Deloitte Kanada'dan muhasebeye blokzincir teknolojisinin kullanımını konusunda çalışan kıdemli danışman Spoke (2015) blokzincir teknolojisinin sağladığı otomatik üçüncü taraf doğrulaması ile finansal işlemlerin testi için denetime olan bağımlılığı azaltacağını düşünmektedir.

Blokzincir ve veri analitiği, süreç otomasyonu, dijitalleşme, robotlaşma, yapay zeka (AI) gibi teknolojiler farklı karakteristiklere sahip olmalarına ve her birinin denetim mesleğine potansiyel etkileri farklı olmasına karşın önemli denetim standartları kurumları (IA-ASB ve PCAOB) bu teknolojileri birbirinden ayırt

etmeden yeni teknolojileri araştırmak için çalışma grupları kurmaktadır (Brender vd., s. 15). Denetim standartları bakımından bu tip bir ayırımın yapılması gelecekteki bu teknolojileri içeren denetim faaliyetlerinde bazı güçlüklerle ve standart olmayan uygulamalara yol açabilecektir.

Büyük dörtlü olarak bilinen firmaların dışındakiler henüz bu konu ile ilgili çalışmaya başlamamış olup bekle ve gör stratejisini izlemektedirler. Deneyimsiz denetçiler tarafından yürütülen testler ve manuel süreçlerin otomatik hale gelmesiyle artık günümüzdeki kadar yeni mezun denetçi (*junior*) ihtiyacı kalmayacaktır. Artık daha uzman, daha deneyimli profesyoneller aranacaktır. Bu durum da denetim organizasyonundaki piramit yapısını ve firmaların kariyer planlamalarını etkileyecektir. İşe yeni alınan denetçilerin kıdemli denetçiliğe yükselmeleri süreci olumsuz etkilenecektir (Brender vd., 2018, s. 18).

Blokzincirin başarılı bir biçimde adaptasyonu çalıştığı ortamın güvenliğine yüksek derecede bağlıdır. Makul düzeyde güvence verebilmek için, denetim süreçleri iç BT kontrollerinin işletim etkinliğinin değerlendirilmesi yönünde bir değişim göstermek zorundadır (Psaila, 2017, s. 3). Bu dönüşümün sağlanabilmesi için denetim birimlerinin insan kaynağının yeterliliğinin değerlendirilmesi ve bu doğrultuda güçlendirilmesi gerekmektedir.

Blokzincirin sunduğu fırsatlardan en büyük kazancın sağlanması bu teknolojinin geniş biçimde kabul görmesi ile mümkün olacaktır. Birçok blokzincir platformu veri güvenliğinin sağlanabilmesi için büyük miktarda depolama alanı ve hesaplama gücüne ihtiyaç duymaktadır. Çok hacimli kurumsal verilerin böyle bir sistemde tutulması oldukça zorlu ve potansiyel olarak da pahalı olabilir (Dai, 2017, s. 81).

Güvenilir bir blokzincirde yer alan işlemin doğrulanarak onaylanması kesin mali durum açıklamaları için yeterli bir kanıt olabilir ancak işlemin doğası gereği yeterli bir denetim kanıtı işlevi görmeyebilir. Yani, blokzincir üzerinden bir değer transferi yapıldığında değer teslim edildiği doğrulanabilir ancak bu değer karşılığında teslim edilmesi gereken ürünün teslim edilip edilmediği belirlenemeyebilir. İlave olarak, blokzincirin yönetimi denetlenen tarafından kontrol edilmiyor da olabilir (Tysiac, 2018; Bible vd., 2017).

Bu konuyu karmaşıklaştıran bir diğer husus da blokzincirin tek bir ürün veya uygulama olmamasıdır. Henüz kabul edilmiş standartları bulunmamaktadır ve blokzinciri kullanan 20 kuruluşa gidilse belki 16'sında farklı tip yazılım ve yarım düzine farklı mimari ile karşılaşılacaktır (Whitehouse, 2018).

Bazı yayınlarda blokzinciri teknolojisinin muhasebe denetmenlerince yürütülen mali durum tabloları denetimlerine ihtiyacı ortadan kaldıracığını iddia edilmektedir. Tüm işlemler geri döndürülemez ve değiştirilemez bir blokzincirde saklandıktan sonra denetim veya denetçiye gerek kalmayabileceği öne sürülmektedir (Bible, Raphael, Taylor ve Valiente, 2017).

Denetçiler hangi düğümlerin mutabakat mekanizmasına katıldıklarını, mutabakat mekanizmasını, işlemleri doğrulayan düğümlerin hesaplama güçlerinin dengeli dağıtılıp dağıtılmadığını, tek bir düğüm ya da küçük bir grubun usulsüzlük ya da %51 saldırısı ile zararlı faaliyetlerde bulunma risklerini değerlendirmelidir (Sheldon, 2018, s. 5). Bu konuları değerlendirmek için derinlemesine teknik bilgi ve denetçilerin bu güne kadar aşına olmadıkları bazı konularda yetkinlik kazanmaları gerekecektir.

4. SONUÇ VE ÖNERİLER

Henüz kamu uygulamaları oldukça kısıtlı, kamudaki bilinirliği nispeten az ve yakın gelecekte operasyonel kamu hizmetlerini üstlenme beklentisi düşük olmakla birlikte, teknolojinin bu güne kadar ivmesi sürekli artan gelişim hızı göz önüne alındığında, blokzincir teknolojisinin getireceği dönüşüme karşı hazırlıklı olunması, bu dönüşümün fırsatlarının kaçırılmaması ve risklere karşı gerekli tedbirlerin alınabilmesi için çok önemlidir. Bu hazırlığın etkin biçimde yapılabilmesi için de ön şart teknoloji hakkında yeterli düzeyde bilgi sahibi olmak ve dünyadaki gelişmeleri yakından takip etmektir.

Bu teknoloji, tüm sektörleri olduğu gibi kaçınılmaz olarak denetim faaliyetlerini de etkileyecektir. Bu etki hem olumlu hem de olumsuz unsurlar içermektedir. Denetim faaliyetleri bakımından blokzincir teknolojisinin sunduğu fırsatlar sürekli ve gerçek zamanlı denetimleri mümkün kılması, kaydedilen verilerin

silinmemesi ve değiştirilememesi nedeniyle güvenilir kanıtlar sunması, manuel işlemleri azaltması, tüm anakütleli denetleme imkanı vererek örneklem seçme gerekliliğini ortadan kaldırması, denetimin iş yükünü azaltarak denetçilerin katma değer sağlayıcı diğer faaliyetlere daha fazla odaklanmalarını sağlaması biçiminde özetlenebilir. Öte taraftan, bu teknolojinin denetim faaliyetleri bakımından potansiyel tehdit içeren özellikleri ise tasarımı ve mimarisi nedeniyle anlaşılmasının güçlüğü, süreçlerin yeniden tasarlanmasını gerektirmesi, yönetim yapısının karmaşıklığı, denetlenebilmesi ve denetimlerde kullanılabilmesi için teknik bilgi gerektirmesi, denetim sürecinde daha çok rutin testleri gerçekleştiren deneyimsiz denetçilere olan ihtiyacı ortadan kaldırması ve henüz mevzuatının ve standartlarının bulunmaması biçimindedir.

Uluslararası iç denetim standartları uyarınca (2120 – Risk Yönetimi ve 2130 - Kontrol) iç denetim faaliyeti, kurumun yönetim süreçlerinin, faaliyetlerinin ve bilgi sistemlerinin maruz kaldıkları riskleri değerlendirmek ve bu risklere karşılık olarak tasarlanmış kontrollerin etkinlik ve verimliliklerini değerlendirerek etkin kontrollerin tasarlanması ve uygulanması konusunda kurumlarına yardımcı olmak zorundadır. Bu standart gereğince, iç denetim birimleri blokzincir gibi teknolojilerin stratejik ve operasyonel risklerini değerlendirmeli, bilgilerin güvenilirliği ve doğruluğunun, faaliyetlerin etkinliği ve verimliliğinin, mevzuat, politika ve prosedürlere uyumun sağlanması için gerekli kontrollerin tasarlanmasında yönlendirici ve kolaylaştırıcı rol üstlenmelidirler.

Risk ve kontrollere yönelik rollerinin yanı sıra iç denetim birimleri kurum içerisinde münferit olarak yürütülen ve üst yönetimin dikkatini çekmemiş olan çalışmalar varsa bunları tespit ederek üst yönetimi bilgilendirebilir, konu hakkındaki yetkinlik düzeyine paralel olarak bu çalışmaları değerlendirebilir, kurumsal risk yönetimi ve stratejik yönetim kapsamında blokzincir teknolojisinin dikkate alınması için gerekli kurul ve birimleri bilgilendirebilir. Bu bağlamda bu teknolojiye ilişkin çalışmalarda öncü rol üstlenmek iç denetim birimleri ve iç denetim faaliyetleri konusunda kurumlardaki farkındalığın artırılması, itibarın ve danışmanlık fonksiyonunun geliştirilmesi bakımlarından bir fırsat olarak değerlendirilmektedir.

Üst yönetim ve karar alıcılar, blokzincir teknolojisini kullanacak kuruluşların tedarikçisi konumunda bulunan işletmelerin zorlanabilecekleri konular, ihtiyaç duyulabilecek yeni teknolojiler, eski teknolojilere entegrasyon, ihtiyaç duyulacak nitelikli insan kaynağı, en uygun kullanım alanları konularına cevap bulmak konusunda önemli bir sorumluluk yüklenmektedirler. Bu sorumluluk ve karar alma konusundaki iyimser öngörü karar verici konumdaki yöneticilerin blokzincir teknolojisi konusunda yeterli bilgilerinin olduğu varsayımına dayanmaktadır. İç denetim fonksiyonu, üst yönetimi bu kararlarda destekleyici bir rol üstlenebilir.

İç denetim birimleri olarak teknolojinin mesleğe etkilerine karşı hazırlıklı olunması bakımından iç denetimin kurumdaki blokzincir projelerine dahil edilip edilmediği, kurumdaki bu projelerden haberdar olup olunmadığı, bu teknolojinin nasıl ve nerede kullanılabileceği, sunacağı fırsatların ve getireceği risklerin neler olduğu sorularına cevap aranması gerekmektedir.

İç Denetim Standartlarına göre (1210 – Yeterlilik) iç denetçiler bireysel görevlerini yerine getirebilmek için gerekli bilgi, yetenek ve diğer vasıflara sahip olmak zorundadır. Bu standart doğrultusunda, blokzincir teknolojisinin geniş kabul görebilerek yaygınlaşmasından önce iç denetim birimleri iç denetçilerin bu yeni teknoloji konusunda eğitim almalarını sağlamalıdır. Konu hakkında belirli bir yetkinliğe eriştikten sonra görev yaptıkları kurumlarda olası blokzincir uygulamalarının planlama aşamalarına dahil olarak uygulamanın yönetim, risk yönetimi ve kontrollerin henüz tasarım aşamasında sisteme entegre edilmesini sağlamalıdır. Teknolojinin büyük avantajlar sağlayacağı beklentisi ile birlikte blokzincirin kurumdaki belirli süreçler için en uygun seçim olup olmadığı da değerlendirilerek teknolojinin kullanılma kararı konusunda azami mesleki özen gösterilmelidir. Aşırı temkinli davranarak fırsatları kaçırmak ile çok aceleci davranıp gereksiz maliyetlere neden olmak arasındaki denge çok iyi kurulmalıdır. Bu dengenin kurulması için en kritik nokta ise teknoloji konusunda yeteri kadar bilgi edinerek karar vermeyi destekleyici donanımın sahip olmaktır. İç denetçiler bu yeni teknolojiye karşı açık ve kucaklayıcı olmalı, getireceği problemlerle birlikte fırsatları da anlayarak gelecekteki yıkıcı değişikliklere karşı hazırlıklı olmalıdır.

Kaynakça

- Berryhill, J., Bourgerly, T., & Hanson, A. (2018). *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector*, OECD Working Papers on Public Governance, No. 28. Paris: OECD Publishing. <http://dx.doi.org/10.1787/3c32c429-en> adresinden alındı.
- Bible, W., Raphael, J., Taylor, P., & Valiente, I. O. (2017). *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession*. Toronto: Deloitte Development LLC.
- Boucher, P., Nascimento, S., & Kritikos, M. (2017). *How blockchain technology could change our lives*. Brussels: Scientific Foresight Unit (STOA), European Parliament.
- Brender, N., Gauthier, M., Morin, J.-H., & Salihi, A. (2018). *The Potential Impact of Blockchain Technology on Audit Practice*. Geneva: University of Applied Sciences and Arts Western Switzerland.
- Casey, M., & Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. New York: St. Martin's Press.
- Catalini, C., & Gans, J. (2017). Some Simple Economics of the Blockchain. *Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16*.
- Chalker, A. (2018, 6 12). *Why Internal Auditors Must Care About Blockchain*. 3 25, 2019 tarihinde The Protiviti View: <https://blog.protiviti.com/2018/06/12/internal-auditors-must-care-blockchain/> adresinden alındı.
- Chartered Accountants Australia and New Zealand. (2017). *The Future of Blockchain: Applications and Implications of Distributed Ledger Technology*. Sydney: Chartered Accountants Australia and New Zealand.
- Cheng, S., Daub, M., Domeyer, A., & Lundqvist, M. (2017, 2). Digital McKinsey. *Using blockchain to improve data management in the public sector*.
- CoinMarketCap. (2019, 4 1). *Coin Market Capitalization*. 3 22, 2019 tarihinde <https://coinmarketcap.com/coins/views/market-cap-by-total-supply/> adresinden alındı.
- Cybersalon. (2013, 9 5). *Cyberpunks, Bitcoin & the Myth of Satoshi Nakamoto*. 5 16, 2019 tarihinde Cybersalon: <http://cybersalon.org/cyberpunk/> adresinden alındı.
- Dai, J. (2017, 10). A Dissertation for the degree of Doctor of Philosophy. *Three Essays on Audit Technology: Audit 4.0, Blockchain, and Audit App*. New Jersey: The State University of New Jersey.
- Deloitte. (2018). *Breaking blockchain open Deloitte's 2018 global blockchain survey*. Deloitte Development LLC.
- Deloitte. (2019). *Unleashing blockchain in finance*. Deloitte Development LLC.
- Diedrich, H. (2016). *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*. Wildfire Publishing.
- Digiconomist. (2019, 3 30). *Bitcoin Energy Consumption Index*. 3 31, 2019 tarihinde Digiconomist: <https://digiconomist.net/bitcoin-energy-consumption> adresinden alındı.
- Doğanay, S. (2019, 3 15). Yeni ve gelişen teknolojilerin yarattığı dönüşüm. Türkiye Kimya Petrol Lastik ve Plastik Sanayii İşverenleri Sendikası. 3 2019 tarihinde <https://kiplars.org.tr/dr-sertac-doganay-ile-gelisen-teknolojiler-uzerine-konustuk/> adresinden alındı.
- Galen, D., Brand, N., Boucherle, L., Davis, R., Do, N., El-Baz, B., . . . Lee, J. (2018). *Blockchain for Social Impact Moving Beyond the Hype*. Stanford: Stanford Graduate School of Business.
- Greenspan, G. (2016, 3 17). *Blockchains vs centralized databases*. 3 27, 2018 tarihinde <https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/> adresinden alındı.
- Güven, V., & Şahinöz, E. (2018). *Blokzincir, Kripto Paralar, Bitcoin*. İstanbul: Kronik Kitap.
- İlkbahar, R. (2019, 3 5). *Araştırma Şirketlerinin Gözünden Blokzincir'in Geleceği*. Medium: <https://medium.com/@recepilkbahar/arastirma-sirketlerinin-gozunden-blokzincirin-gelecegi-5bc15045bc50> adresinden alındı.
- Kelly, M. (2019, 2). Boards Look to Harness Blockchain Disruption. *Tone at the Top*. The Institute of Internal Auditors.
- Killmeyer, J., White, M., & Chew, B. (2017). *Will blockchain transform the public sector?* Deloitte University Press.
- Lyons, T., Courcelas, L., Grandsenne, J., Carrel, E., & Timsit, K. (2018). *Blockchain Innovation in Europe*. European Union Blockchain Observatory and Forum.
- Maupin, J. (2018). *The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All*. Max Planck Institute.
- Nagpal, R. (2017, 9 9). *#8 Steps to Build a Blockchain Solution*. 6 1, 2018 tarihinde Entrepreneur - Start, run and grow your business: <https://www.entrepreneur.com/article/300077> adresinden alındı.

- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- Nomura Research Institute. (2016). *Survey on Blockchain Technologies and Related Services FY2015 Report*. Tokyo: Japan's Ministry of Economy, Trade and Industry (METI).
- Onbirinci Kalkınma Planı Kamuda Kurumsal Yönetimde Yeni Yaklaşımlar Özel İhtisas Komisyonu. (2017). *Onbirinci Kalkınma Planı Kamuda Kurumsal Yönetimde Yeni Yaklaşımlar Özel İhtisas Komisyonu Ön Raporu*.
- Pelletier, J. (2018, 4 5). *A Blockchain Primer for Internal Audit*. 3 26, 2019 tarihinde IA Online: <https://iaonline.theiia.org/blogs/Jim-Pelletier/2018/Pages/A-Blockchain-Primer-for-Internal-Audit.aspx> adresinden alındı.
- Psaila, S. (2017). *Blockchain: A game changer for audit processes?* Malta: Deloitte.
- PwC. (2018). *Global blockchain survey*. PricewaterhouseCoopers Limited.
- PwC. (2018, 3 6). *PwC Blockchain Validation Solution*. 3 14, 2019 tarihinde PwC: Audit and assurance, consulting and tax services: <https://www.pwc.com/us/en/about-us/new-ventures/pwc-blockchain-validation-solution.html> adresinden alındı.
- Qureshi, H. (2018, 1 28). *The authoritative guide to blockchain development*. 5 31, 2018 tarihinde freeCodeCamp: <https://medium.freecodecamp.org/the-authoritative-guide-to-blockchain-development-855ab65b58bc> adresinden alındı.
- Radore. (2017, 1 31). *Elektrik ve Elektrik Birimleri Nelerdir?* 3 31, 2019 tarihinde Radore Blog: <https://radore.com/blog/elektrik-birimleri-nelerdir.html> adresinden alındı.
- Ray, S. (2018, 2 19). *The Difference Between Blockchains & Distributed Ledger Technology*. 2 10, 2019 tarihinde Towards Data Science: <https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92> adresinden alındı.
- Rooney, H., Aiken, B., & Rooney, M. (2017). Q&A. Is Internal Audit Ready for Blockchain? *Technology Innovation Management Review*, 7(10): 41-44.
- Schatsky, D., & Muraskin, C. (2015). *Beyond bitcoin Blockchain is coming to disrupt your industry*. Deloitte University Press.
- Sheldon, M. D. (2018, 12 5). *A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit*. *American Accounting Association Journal*.
- Smith, A. M. (2018, 3 15). *The blockchain challenge nobody is talking about*. 3 26, 2019 tarihinde PwC Next in Tech: <https://usblogs.pwc.com/emerging-technology/the-blockchain-challenge/> adresinden alındı.
- Spoke, M. (2015, 6 11). *How Blockchain Tech Will Change Auditing for Good*. 3 25, 2019 tarihinde CoinDesk: <https://www.coindesk.com/blockchains-and-the-future-of-audit> adresinden alındı.
- T2 Yazılım A.Ş., Bankalararası Kart Merkezi A.Ş. (2018). *Keşif: Blockchain'in Sırları BBN Faz 1*. İstanbul: Bankalararası Kart Merkezi A.Ş.
- Thake, M. (2018, 2 8). *What's the difference between blockchain and DLT?* 2 10, 2019 tarihinde Medium: <https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd> adresinden alındı.
- Tysiac, K. (2018, 3 15). *How blockchain might affect audit and assurance*. 3 22, 2019 tarihinde Journal of Accountancy: <https://www.journalofaccountancy.com/news/2018/mar/how-blockchain-might-affect-audit-assurance-201818554.html> adresinden alındı.
- Unerman, J., & O'Dwyer, B. (2004). Enron, WorldCom, Andersen et al.: a challenge to modernity. *Critical Perspectives on Accounting*, 15, 971-993.
- Usta, A., & Doğanekin, S. (2017). *Blockchain 101*. İstanbul: Kapital Medya Hizmetleri A.Ş.
- Voshmgir, S. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, Vol.26, 499-509.
- Whitehouse, T. (2018, 4 3). *Auditors develop early plans for how to audit blockchain*. 3 24, 2019 tarihinde Compliance Week: https://www.complianceweek.com/news/news-article/auditors-develop-early-plans-for-how-to-audit-blockchain#.W_R1cOgzY2w adresinden alındı.
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. United States National Institute of Standards and Technology.
- Yermack, D. (2017, 1). Corporate Governance and Blockchains. *Review of Finance*, 7-31.
- Yeung, E. (2017, 6 9). *Blockchain 101 for Internal Audit*. 3 22, 2019 tarihinde LinkedIn: <https://www.linkedin.com/pulse/blockchain-101-internal-audit-eric-yeung/> adresinden alındı.