İç Denetimin Blok Zincir Yoluyla Siber Güvenlik Yönetimine Adaptasyonu

Seval SELİMOĞLU [1]

Mustafa Hakan SALDI [2]

Özet

Çalışma, esas itibari ile blok zincir teknolojisinin altyapısındaki özelliklerin araştırılmasına yönelik olarak tasarlanmış olup, bu yeniliğin siber güvenlik süreçlerinde nasıl kullanılabileceği ve iç denetçilerin gelişmekte olan bu teknolojiye adaptasyonları için neler yapılabileceği üzerine bir dizi öneriler sunmak için geliştirilmiştir. Bu çerçevede, blok zincir teknolojisinin altyapısı kavramsal açıdan incelenerek, siber güvenlik kontrollerindeki uygulama alanları sınıflandırılıp, iç denetçilerin bu yeni disiplinlere hangi doğrultuda uyum sağlamaları gerektiği üzerine öneriler sunulmuştur. Çalışma keşifsel araştırma yöntemi üzerine kurgulanarak ikincil veri kaynaklarından çevrim içi araştırmalar, bilim literatüründe yer alan makaleler ve vaka çalışmaları doğrultusunda elde edilen bilgiler yoluyla oluşturulmuştur. Sonuç olarak, blok zincir teknolojisinin benzersiz altyapısı sayesinde siber güvenlik yönetiminde karşılaşılan rutin sorunların üstesinden gelinebilirken, organizasyonların denetim faaliyetlerini bu yönde iyileştirerek, risk kontrol süreçlerinin adaptasyonlarını sağlamaları gerekmelidir.

Anahtar Kelimeler: Blok Zincir Teknolojisi, Siber Güvenlik, İç Denetim, Risk Kontrol, Erişilebilirlik

The Adaptation of Internal Audit to Cyber Security Management by Blockchain

Abstract

The study is mainly designed to explore the characteristics of block chain technology infrastructure and to present a set of proposals for how to apply this innovation in cyber security processes and to offer which strategies can be utilized to adapt the internal auditors to this new technology. In this framework, recommendations are structured through the reviews of conceptual subjects of block chain technology and classifications of application fields in cyber security controls by proposing solutions for adapting internal auditors to new disciplines. The study is constructed via exploratory research method through the usage of secondary data sources that cover online researches, literature examinations and case studies. Consequently, while the routine problems which are being encountered in cyber security management can be overcome by the unique infrastructure of block chain technology, the organizations need to recover their audit activities in this direction with providing the adaptations of their risk control processes.

Keywords: Blockchain Technology, Cyber Security, Internal Audit, Risk Control, Availability

1. GİRİŞ

Blok zincir teknolojisi, şifreli algoritmalar vasıtası ile hesaplarda gerçekleştirilen tüm eş zamanlı finansal aktivitelerin, yetkili şahıslar veya kuruluşlar tarafından paylaşımdaki defter-i kebir üzerinden kontrol edilebilmesi fırsatını sağlamaktadır. Blok zincir sistemi, işlem bilgilerinin kişisel bilgisayarlar üzerinde güvenli bir biçimde korunarak sürekli olarak saklanmasına olanak tanımaktadır. Böylelikle, sistemde saklanan veriler yetkili taraflara dağıtılarak bilgiye erişim mekanizması da etkin ve verimli bir yaklaşımla sürdürülebilir kılınmaktadır. Bu bağlamda, blok zincir sistemi üzerinden herhangi bir işlem gerçekleştirildiğinde program kodları ile bloklar

Araştırma Makalesi / Research Article
Makale Geliş Tarihi / Submitted: 5.6.2022 Makale Kabul Tarihi / Accepted: 6.7.2022
[1] Prof. Dr., Anadolu Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Muhasebe ve Finansman Ana Bilim Dalı, Eskişehir/Türkiye, sselimoğlu@anadolu.edu.tr, http://orcid.org/0000-0003-1185-9980
[2] Sorumlu Yazar, Dr., Anadolu Üniversitesi Sosyal Bilimler Enstitüsü İngilizce İşletme Doktora Programı Mezunu, Endüstri Mühendisi, İstanbul/Türkiye, hamusaldi@hotmail.com, http://orcid.org/0000-0001-5043-4606
Atıf (Citation): Selimoğlu, S., ve Saldı, M., H. (2022). İç denetimin blok zincir yoluyla siber güvenlik yönetimine adaptasyonu. *Denetim ve Güvence Hizmetleri Dergisi 2*(2), 121-134.

üzerinde saklanan ve korunan veriler devreye girerek sürece giren aktivitenin güvenli, şeffaf ve hızlı bir biçimde erişimi olan kişi tarafından denetlenmesi alternatifini sunmaktadır. Blok zincir teknolojisinin verilerin korunması, erişimlerinin güvenli bir şekilde sağlanması ve dağıtılması üzerine getirdiği yenilikler zihinlere siber güvenlik süreçlerindeki kontrollerin bu sistemden hangi ölçüde etkileneceği ve iç denetçilerin bu değişime nasıl uyum sağlayabileceği sorularını getirmektedir.

Tüm bu sorular ışığında, blok zincir teknolojisinin temel kavramları, siber güvenlik süreçlerindeki aksamalara hangi çözüm önerilerinin sunulacağı ve iç denetçilerin bu değişime nasıl adapte olabilecekleri üzerinde durularak, akademisyenlerin ve endüstri uzmanlarının kafalarındaki soru işaretleri giderilmeye çalışılmıştır. Bu doğrultuda, öncelikle blok zincir teknolojisinin işleyiş mekanizması incelenerek siber güvenlik yönetimi ile bağı kurulmuştur, daha sonra ise iç denetçilerin bu yöndeki gelişim süreçlerinin nasıl tasarlanabileceği üzerine gözlemler yapılmıştır.

2. KAVRAMSAL ÇERÇEVE

Blok zincir teknolojisi, çağın öne çıkan yıkıcı yeniliklerinden biri olarak değerlendirilmesi açısından öncelikle kripto para olarak isimlendirilen dijital varlıklar doğrultusunda ilgi görmeye başlayan ve sonrasında ise altyapısında içerdiği kendine özgü mekanizması vasıtası ile dijital ortamlardaki herhangi bir değerin depolanması ve taşınması üzerine organizasyonlara sağladığı birçok fayda ile de kendisini hem kamu hem de özel kesim kapsamında kabul ettirmekte olan bir dijital dönüşüm aracıdır. Diğer taraftan, dijitalleşme doğrultusunda kat edilen mesafe ile birlikte, ulusların ve kurumların kritiklik derecesi yüksek olan ve hassas olarak nitelendirilen verilerin ve bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini kontrol etmeleri ve siber güvenlik altyapılarını geleceğe yönelik bir biçimde tasarlamaları gerekmektedir. Bu doğrultuda, herhangi bir kuruluşun siber uzayda karşılaşabileceği tehditlere karşı nasıl güncel kalabileceği, etkin bir siber güvenlik istihbarat sisteminin nasıl oluşturulacağı ve gelişen teknolojilere nasıl uyum sağlanacağı soruları zihinlerde ışık oluşturmaktadır. Ayrıca, blok zincir teknolojisi, bilhassa, kamu ve özel sektörler kapsamında hala ağırlıklı olarak kullanılmakta olan merkezi veri tabanlarının oluşturduğu risklerin de sorgulanmasının vaktinin geldiğinin habercisi olma özelliğindedir.

2.1. Blok Zincir Teknolojisi'nin Temelleri

2009 yılında, Satoshi Nakamoto isimli bir şahıs tarafından finansal piyasalardaki sorunlara çözüm getirmek için bir eşler arası elektronik nakit sistemi platformu veya bilinen ismiyle bitcoin geliştirilerek, herhangi bir finansal aracı kuruluşa gerek kalmadan çevrim içi ödemelerin gerçekleştirilmesi sağlanmaya başlanmıştır. Fakat, bu mekanizmadaki en büyük problem olarak gözlemlenen bir işlemde iki kez ödeme yapılma ihtimalinden sakınmak için ve bitcoinin dijital bir varlık olmasından dolayı kopyalanarak çoğaltılmasının zor olmamasının oluşturabileceği sorunlar nedeni ile blok zincir teknolojisi geliştirilmiştir. Buna rağmen, Nakamoto'nun orijinal raporunda blok zincir teknolojisinden bahsedilmezken, bu tabir sadece bitcoine ilişkin kaynak kodunun yorum bölümünde yer almaktadır (Gupta, 2018: 35).

Tablo 1. 2019 Yılı itibari ile Blok Zincir Teknolojisini İşletme Süreçlerinde Uygulayan Başlıca Kurumlar

Blok Zincir Teknolojisini En Çok Uygulayan Finansal Kurumlar	Proje Sayısı
Bankalar	411
Sigorta Şirketleri	40
Ödeme Sistemleri ve Finansal Teknoloji Hizmet Sağlayıcıları	33
Menkul Kıymet Ticaret Yapan Şirketler	16
Çeşitlendirilmiş Finansal Kuruluşlar	15

Kaynak: Statista Research Department, 2020

Blok zincir teknolojisi geleneksel internet işlemlerinden farklı olarak, merkezi olmayan veri tabanları vasıtası ile verilerin saklandığı, korunduğu, işlendiği, aktarıldığı ve erişilebildiği bir altyapıya sahip olması nedeni ile devletlerin ve kurumların kullanım alanlarına dâhil olmaktadır. Bu sistem, özellikle, siber güvenlik açısından hata toleranslarının asgari seviyelerde olduğu kritik altyapı endüstrilerinde hassas bilgilere erişimin kontrolü açısından mükemmele yakın süreç yönetimi olanakları sunmaktadır.

Bütün bunlar ile birlikte blok zincir teknolojisi birçok insanın kafasında hala soru işaretleri uyandırmaktadır. İşin aslına bakıldığında, bu teknoloji ile yeni tanışanlar için herhangi bir komisyon ücreti ödenmeden binlerce mil uzaklıktan fon transferi yapabilmenin mümkün olduğunu düşünmek gerçekten sıra dışı gibi gözükse de herhangi bir insanın kendi varlıklarının kontrolünü herhangi bir bankanın ya da aracı kuruluşun desteğini almadan dijital bir hesap vasıtası ile yapabilmesi bu teknoloji sayesinde mümkün kılınabilmektedir (Pathak, 2021). Aslında bütün bunlar, önceden bahsedildiği gibi, blok zincir teknolojisinin altyapısında yer alan merkezi olmayan veri tabanları ile gerçekleştirilebilmektedir. Bahsedilen nedenlerden ötürü, iki bin on dokuz yılındaki verilere göre blok zincir teknolojisi özellikle bankalar tarafından organizasyonel çözümlerde sıklıkla kullanılmıştır. Blok zincir teknolojisinin içinde barındırdığı altyapı sayesinde internete bağlı her bilgisayar veya elektronik ve komünikasyon cihazı ekosistemde erişilebilirlik yetkisine sahip olmak için bu sistemin temelini oluşturulan algoritmalar vasıtası ile oluşturulmuş düğümlerde yer alan uygulamaları edinmek zorundalardır. Kullanım durumlarına göre, bu cihazların sisteme katılımı sınırlandırılabilmektedir; örneğin, blok zincir tabanlı bir ekosistemde bankaları kapsayan bir düğümler kümesi oluşturulduğu varsayılırsa, bu küme içindeki herhangi bir bankanın kendi müşterilerine ait olan verileri gözetme ve işleme aktiviteleri, düğümlere erişimi sağlayan yazılım kodları vasıtası ile sağlanabilmektedir.

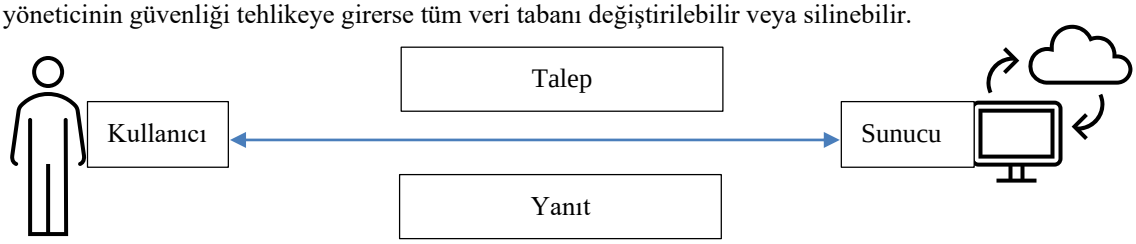
Dijital dönüşümün kendisini hayatın her alanında hissettirdiği çağın koşulları dikkate alındığında, blok zincir teknolojisinin neredeyse tüm sektörlerde kullanıma açık olmasının beraberinde birçok fayda getirdiği aşikardır. Örneğin, faaliyet giderlerinin minimize edilmesinde, siber güvenlik ile ilgili sorunların üstesinden gelinmesinde, kimlik ve erişim yönetimi ile ilgili problemlere çözümler üretilmesinde, kamu ve özel sektörler arasındaki uyumun sağlanmasında, lojistik yönetiminin iyileştirilmesinde ve yalınlaştırılmasında veya hastanelerin veri tabanlarındaki kayıt takip sistemlerinin daha korunaklı hale getirilmesinde bu teknolojinin içerdiği altyapı uygulanabilmektedir.

Tablo 2. Blok Zincir Sisteminin İşleyişi

İşlem Hazırlığı	İşlem Doğrulama	Blok Oluşturma	Blok Onaylama	Blok Zincirleme
Alıcı	Sıfır Güven Yaklaşımı	Düğümler	Yinelemeli Onay Süreci	Uzlaşma Mekanizması
Enformasyon	Düğüm	Ağ Sistemi	İş Kanıtı (Proof of Work) (PoW)	Blokların Onayı
Protokol Adresi	Şifreleme	Bitcoin	Hisse İspatı (Proof of Stake) (PoS)	Blokların Blok Zincir Sistemine Eklenmesi
Dijital İmza		Madenciler	Yetkilendirilmiş Hisse İspatı (Delegated Proof of Stake) (DPoS)	
İşlem Mesajı		Karmaşık Matematiksel Problemler	Pratik Bizans Hata Toleransı (Practical Byzantine Fault Tolerance) (PBFT)	

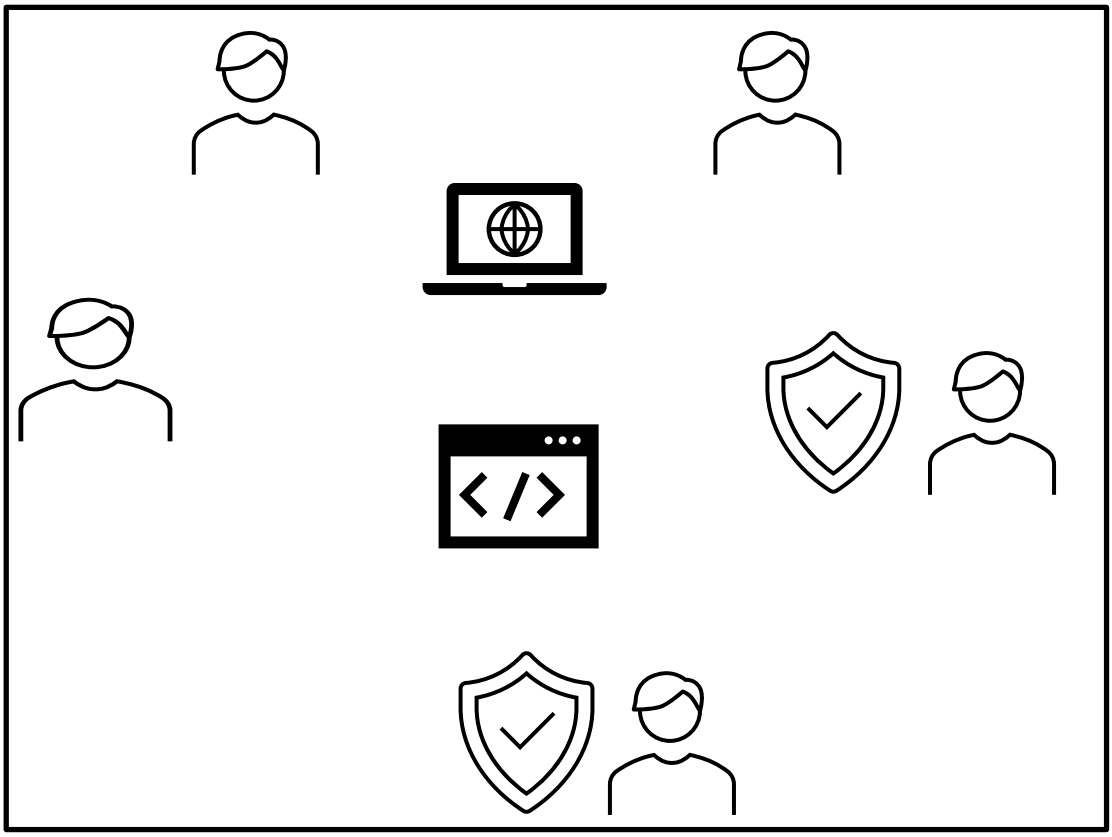
Kaynak: Gupta, 2018: 39-40.

Blok zincir sistemi tablo iki'de gösterimi yapılan basamaklar doğrultusunda performans gösterirken, bloklarla temsil edilen merkezi olmayan bir kayıt sisteminin çoklu veri tabanları üzerinden yetkisi olan şahıslar veya kurumlar vasıtası ile güncellenmesinin ve işletilmesinin sağlanması sonucunda sisteme dâhil edilmesi ile oluşturulan ağlardan meydana gelmektedir. Öncelikle, internet üzerinden verilerin nasıl erişilebilir hale geldiği açıklanacak olursa; merkezi bir sunucu üzerinden herhangi bir kullanıcının erişmek istediği veriye ulaşması istemci/sunucu (client/server) modeli vasıtası ile gerçekleştirilmektedir. Teorik olarak, bir sunucu herhangi bir kullanıcı makinesinden farklı değildir, ancak, pratikte, sunucunun amacı birçok kullanıcıya eş zamanlı olarak hizmet vermektir. Bütün bunlar ile birlikte, veri tabanının kontrolü atanmış bir yöneticiye bağlıdır ve bu nedenle eğer yöneticinin güvenliği tehlikeye girerse tüm veri tabanı değiştirilebilir veya silinebilir.



Şekil 1. Internet Vasıtası ile Geleneksel Veri Transferi
Kaynak: Gupta, 2018

Blok zincir ağı, düğüm olarak nitelendirilen birbirinden bağımsız makinelerden oluşturulan bir sistemdir. Geleneksel veri tabanlarında merkeziyetçi bir sistem ile depolanan verilerin suretleri blok zincir teknolojisinde yer alan düğümlerde birkaç ayrı veri tabanı olarak saklanabilmektedir. Bu sayede, herhangi bir düğümde problem oluşsa dahi, veriler, ayrık olarak farklı düğümlerde de tutulduğu için daha güvenli bir mekanizma ile depolanabilmekte ve işlenebilmektedir. Herhangi bir düğümün blok zincir ağına katıldığı an itibari ile sistemdeki defteri kebir kayıtları güncellenebilmektedir. Her düğüm geçerli olduğu bloklar kapsamındaki kayıtların idaresinden ve güncellenmesinden sorumlu olarak blok zincir ağındaki aktiviteler takip edilebilmektedir. Hesap kayıtlarının blok tabanlı bir sistem eşliğinde depolandığı her bir düğüm, hashing algoritması olarak tanımlanan ve sisteme dahil edilen ve her bir veriyi dizgiler halinde çıktıya çeviren matematiksel kural bütünlüğüne bağlanmaktadır. Sistem dahilindeki her bir bloğun oluşturulmasının sağlanması için çoklu işlemler birbirleri ile ilişkilendirilerek basit hali ile veri yapısı biçimselleştirilmektedir. Her kripto tedavülünün kendine özgü uzanımı ve blok zincir sistemi mevcut bulunmaktadır. Örneğin, bir bitcoin blok zincirindeki bir mega baytlık blok her on dakikada bir oluşturulurken, bir ethereum blok zincirindeki bir bloğun oluşturulma süresi ise on iki ile on dört saniye arasında değişmektedir ve her bir bloğun hacmi ise iki kilo bayt olarak tanımlanmaktadır. Blok zincir teknolojisindeki her bir blok daha detaylı bir biçimde değerlendirilecek olunursa, her bir blok bir blok başlığından (block head) ve bir blok gövdesinden (block body) oluşmaktadır. Bu bağlamda, her blok başlığı blok zincir içindeki spesifik bir bloğu tanımlarken, bünyesinde bir meta veri kümesini barındırmaktadır.



Şekil 2. Eşler Arası Blok Zincir Ağı
Kaynak: Gupta, 2018

- Version (Version): Yazılım ve protokol kademelerinin takip edildiği dört baytlık bir alandır.
- Zaman damgası (Time Stamp): Saniyelik zaman dilimlerinde blokların oluşumunu gösteren dört baytlık alandır.
- Önceki Bloğun Hash'i (Hash of the Previous Block): Zincirdeki önceki bloğun hash'ini gösteren otuz iki baytlık alandır.
- Tek Seferlik Kullanılan Numara (Number Only Used Once) (Nonce): Emek ispatı (Proof of Work) (PoW) algoritma sayacının izlenmesi için kullanılan dört baytlık alandır.

- Merkle Kök Ağacı (Hash of the Merkle Root): Herhangi bir blok işleminin merkle ağacının kökünde yer alan otuz iki baytlık alandır.
- Blok Gövdesi (Block Body): Bloğun bu bölümü bir dizi işlemi içermektedir. Bitcoin dünyasında, herhangi bir blokta ortalama beş yüzden fazla işlem gerçekleştirilir. Her işlem dijital ortamda imzalanarak gerçekleştirilir; aksi takdirde, geçersiz sayılır. Bu süreçlerin oluşturulması için gerçek bir işlem üzerinden özel bir şifre doğrultusunda algoritmalar vasıtası ile bir hashing fonksiyonu kullanılmaktadır (Gupta, 2018).

Şekil 3. Blok Zincir Sistemindeki Herhangi Bir Blokta Yer Alan Kısımlar

Kaynak: Gupta, 2018

2.2. Blok Zincir Teknolojisi'nin Siber Güvenlik Süreçlerine Etkisi

Öncelikle, siber güvenlik disiplinleri ile bu disiplinleri değerlendirmek doğrultusunda hazır bulunulması için gereken hususlar arasında önemli bir eşitsizlik olduğu öne sürülmektedir. Birçok şirket karşılaşacağı siber atakların ve güvenlik meselelerinin farkında olmasına rağmen, bu risklere karşı alınan önlemlerin tam olarak standartlaştırılamamasından ve bu ataklar neticesinde ortaya çıkan tahribatın bilgi sistemlerine etkilerinin kısa süre zarflarında onarılamamasından dolayı yetersiz kalmaktadır (Maleh, Baddi, Alazab, Tawalbeh, & Romdhani, 2021). Bunlara ilaveten, işletmelerin çoğu dışarıdan gelişen siber saldırılara karşı güvenlik sistemlerini hazır tutarlarken, bunlardan sadece az bir kısmının savunma mekanizması, kendi çalışanlarından kaynaklanabilecek kötü niyetli ataklara karşı güvenli sayılabilecek düzeydedir (Groenfeldt, 2014). Bilgisayar korsanlarının gerçekleştirdikleri siber saldırılar doğrultusunda güvenlik duvarlarını aşarak yerel alan ağlarına sızmaları sonucunda elde edebilecekleri önemli bilgileri korumak için bile bir oyun planı geliştirmenin tam olarak mümkün olmadığı koşullarda, kurumların bir de kendi çalışanları tarafından maruz kalabilecekleri risklere karşı önlem almalarının daha güç olduğu bariz biçimde anlaşılmaktadır. Bu gibi vakaların önlenmesinde kuşkusuz öncelikli olarak güvenlik altyapılarına yapılan yatırımların ölçeğini artırmak ilk sırada gelmektedir, çünkü güçlü bir bilgi sistemleri güvenliğine sahip olmak, bilgisayarların, ağların ve iletişim hatlarının hem kasıtlı olarak gerçekleştirilen saldırılara karşı savunulmasını hem de kaza sonucu oluşabilecek vakalara karşı sistemin çabuk toparlanabilmesini sağlamaktadır. Bilgisayar güvenliği geniş kapsamlı bir konu olduğundan, birçok tehdit unsurunun dikkate alınması gereklidir. Ancak, ne yazık ki, bu tehditlerin çoğu insan faktöründen kaynaklanmaktadır. Truva atı (trojan) bu tehditlerin en karmaşığı olarak dikkat çekmektedir. Bankalara yönelik olarak gerçekleştirilen siber saldırıların başında da Zeus ve SpyEye gibi truva atı familyasında kabul edilen kötü amaçlı yazılımlar gelmektedir. Herhangi bir truva atı saldırısı ile antivirüs kontrolüne yakalanılmadan sisteme sızılması ve bankaların hassas bilgilerine erişilmesi olasılıklar dahilindedir (Martino, 2013).

İşletmelerin kasıtlı veya kasıtsız olarak içeriden kaynaklı ataklara karşı siber güvenlik ölçümlerini yapabilmelerinin birkaç adet yolu bulunmaktadır (Tonsager, 2013). Yetkisiz erişimlere ve neticesinde ortaya çıkabilecek olası veri hırsızlığı vakalarına karşı organizasyonları koruyabilecek beş adet bilgi güvenliği ölçümü şu şekilde sıralanmıştır;

- Dahili Gizlilik ve Veri Güvenliği İlkeleri: İşletmelerin müşterilerinin ve çalışanlarının kişisel verilerini nasıl koruduğunu, ifşa ettiğini, kullandığını ve topladığını tanımlanmış ilkeler çerçevesinde belirlemelerinin, kimin gizlilik derecesi yüksek verilere ulaşması için yetkili olabileceği ve hassas sınıfında yer alan verilerin nasıl korunabileceği noktalarında kendilerine yardımcı olabileceği beklenmektedir (Tonsager, 2013).
- Internet Erişimi ve Kullanımı Politikaları: Doksanlı yıllarda birçok şirket, çalışanlarının internete ve bilgisayar ağlarına nasıl erişebilmeleri gerektiği üzerine çalışan politikaları oluşturmuşlardır. Buna rağmen, bu politikalar, eşler arası programlar ve üçüncü parti mobil uygulamalar gibi yeni teknolojilerin türemesi ile şirketlerin sır kapsamındaki bilgilerinin ifşa edilmesine yol açtıkları için güncellenmelidirler (Tonsager, 2013).
- Sosyal Medya Politikaları: Sosyal medya politikaları, genel olarak kurum çalışanlarının sosyal medyayı iş amaçları doğrultusunda nasıl kullanabilecekleri üzerine bir çerçeve sunarak, kişisel sosyal medya hesaplarının kullanılması için yönergeler ortaya koyar. Bu politikalar vasıtası ile çalışanlara, gizli veya tescilli şirket bilgilerinin ifşa edilmesini önlemek için sosyal medyayı kullanırken ihtiyatlı olmaları hususunda bilgilendirme yapılırken, işverenin de yasal mevzuata uyum süreci kontrol altında tutulmuş olunur (Tonsager, 2013).
- Hizmet Sağlayıcı Anlaşmalarında Güçlü Korumalar: Hizmet sağlayıcılar ile gerçekleştirilen gizlilik hükümleri ve ifşa etmeme anlaşmaları yaygın ve önemlidir. Ancak, gizlilik ve veri güvenliği hükümleri, bilhassa hizmet sağlayıcıların müşterilerin kişisel verilerini idare edebilecekleri durumlarda ek koruma sağlayarak güvenlik ihlali riskini minimum seviyelere çekebilir (Tonsager, 2013).
- Kendi Cihazını Getir Politikası: Çalışanlarına kendi akıllı telefonlarını, tabletlerini ve diğer cihazlarını kullanarak işlerinde kullandıkları elektronik posta adreslerine ve bilgisayar ağlarına ulaşmalarına izin veren işverenlerin sayısı gün geçtikçe artmaktadır. Hem işverenler hem de çalışanlar bu yaklaşımdan fayda sağlayabilirlerken, şirketlerin kendi cihazını getir politikasını uygularlarken, çalışanlarına yeterli bildirimde bulunduklarından ve uzaktan silme araçları gibi veri güvenliği önlemlerini aldıklarından emin olunması gerekmektedir (Tonsager, 2013).

Metinde bahsedilen, kurumların bilgi güvenliği kapsamında maruz kaldığı riskler bağlamında, blok zincir teknolojisinin kullanılmasının getireceği faydalar sıralanacak olunursa;

- Doğruluk: Herhangi bir blok zincir ağı dahilinde gerçekleştirilen tüm işlemler binlerce düğüm tarafından kontrol edilerek onaylanır. Bu sayede, herhangi bir hata yapılsa bile sistemdeki diğer cihazlar bu hatayı anında tespit edebilir. Ancak, herhangi bir hatanın anlaşılamaması için, ağ kapsamındaki cihazların en azından yüzde elli birinin eş zamanlı olarak aynı hatayı yapması gereklidir ki, böyle bir duruma, örneğin, Bitcoin gibi yüksek hacimli veriler ile işlem yapma kabiliyeti olan blok zincir ağlarında rastlanması söz konusu bile değildir (Pathak, Blockchain Technology: A Guide for Beginners, 2021).
- Adem-i Merkezileşme: Blok zincir ağları tek bir merkezden kontrol edilmez. Bu sayede, bilgi teknolojileri denetimlerinde ve sızma testlerinde sıklıkla karşılaşılan yetkilendirme ve erişilebilirlik sorunları ortadan kaldırılabilir, çünkü, sistem içerisindeki herhangi bir değişiklik anında her bir düğüme yansımaktadır (Pathak, Blockchain Technology: A Guide for Beginners, 2021).
- Değişmezlik: Güvenilir şifreleme mekanizması ve sistem içerisindeki blokların kronolojik olarak birbirlerine bağlanması sayesinde verilerin değiştirilmesi olanaklı değildir. Bu sayede, siber güvenlik uzmanlarının risk kontrollerinde karşılaştıkları ve veri bütünlüğünün ihlaline neden olan sorunlar tespit edilerek önlenebilmektedir. Örneğin, bir blok zincir ağında herhangi bir işlem yapıldığında, binlerce güçlü bilgisayar bu işlemi kontrol ederek kaydın geçerliliğini sorgular ve en son olarak bloğa ekler. Bu süreçlerde karmaşık hesaplamalar içeren algoritmalar kullanılarak yeni bir işlemin kaydının bloğa aktarılması için tekil bir hash kullanılmaktadır. Böylelikle, kötü niyetli bir yazılım vasıtası ile sistemdeki bilgileri değiştirmek isteyen siber korsanların yapacağı herhangi bir atak, blok zincir ağındaki tüm düğümlerde fark edilerek geçersizleştirilir ve bloklara eklenmeden saldırı kontrol altına alınmış olunur (Pathak, Blockchain Technology: A Guide for Beginners, 2021).

• Şeffaflık: Blok zincir ağları açık kaynak yazılım mimarisi üzerine geliştirildiği için herhangi bir merkeziyetçi otorite üzerinden işlem yapılmasına izin verilmemektedir. Sonuç olarak, geleneksel ağ mekanizmalarına kıyasla daha şeffaf bir yaklaşıma sahip olması sebebi ile bilgi teknolojisi denetçilerinin güvenlik açıklarını tespit etmeleri ve proaktif olarak çözüm önerileri sunmaları daha uygulanabilir hale getirilebilmektedir (Pathak, Blockchain Technology: A Guide for Beginners, 2021).

2.3. İç Denetçilerin Adaptasyonu

Büyük veri kümelerinin depolanmasını, işlenmesini, transfer edilmesini ve korunmasını kapsayan aktivitelerin, kurumların iş süreçlerinde egemen hale gelmesi ile birlikte, iç ve dış olarak tanımlanan geleneksel denetim yaklaşımları da ciddi ölçüde değişime uğramaktadır (Vasarhelyi & Halper, 1991). Herhangi yeni bir teknolojiye etkin bir biçimde adapte olmanın en iyi yolu bu yeniliklerin beraberinde getirdiği riskleri tanımlamaktır. Öte yandan, gelişen bir teknolojinin sadece uygulama olmanın ötesinde bir altyapı olma özelliği var ise, neden olabileceği koşulların daha detaylı incelenmesi gerekmektedir. Blok zincir teknolojisinin de organizasyonlara heyecan verici fırsatlar sunmasının yanında, denetim açısından spesifik zorluklar ve yeni gelişim alanları oluşturacağı belirlidir. Bu bağlamda, iç denetçilerin sadece bu riskleri anlamalarının yanında, organizasyonlara proaktif olarak danışmanlık yapmaları ve bu yeni altyapı ile ilgili ortaya çıkabilecek risklere karşı devletlerin ve işletmelerin kontrol çerçevelerini hazır bulundurmaları için yol göstermeleri gerekmektedir. Bahsedilen nedenlerden ötürü, blok zincir sistemlerinin kontrol altında tutulması için iç denetçilerin yeni yaklaşımlara yönelmesi beklenmektedir.

Blok zincir sisteminin getireceği değişim rüzgarlarının denetim açısından ortaya çıkarabileceği farklılıklar aşağıda belirtilen konular ile tasnif edilebilir;

• Yönetişim çerçevesi: Blok zincir ağları verilerin paylaşılma mekanizması açısından geleneksel sistemlerden farklıdır, bu nedenle, veri kümelerinde gerçekleştirilen işlemlerin onayı ve doğrulanması ile sisteme katılımı izin verilen şahısların ve kurumların bu faaliyetleri kontrol etme yöntemleri ile yönetişim süreçleri kapsamındaki politikaların ve prosedürlerin birbirleri ile uyumlu olması açısından risk unsurları oluşabilmektedir (Deloitte, 2021).
• Bilgi teknolojisi güvenliği: Blok zincir teknolojisi ile geliştirilen yeni altyapının korunması için bilgi teknolojisi kapsamındaki farklı katmanların değerlendirilmesi ve sürekli izlenmesi gereklidir. Aslında bu durum, kullanıcı erişiminin sağlanmasında ihtiyaç duyulan bilginin edinilmesi ve gerekenlerin yapılması üzerine bir kurgunun oluşturularak, şifre mekanizmalarının kontrolünün sağlanmasıdır. Blok zincir sisteminin asimetrik şifreleme uygulamaları üzerinden verilere erişimi sağlaması, aynı zamanda veri tabanlarında gerçekleştirilen herhangi bir değişikliğin de tüm sistem tarafından kontrol edilmesine olanak tanıyarak, bütünlük açısından da ağın daha güvenli bir biçimde denetlenmesini mümkün kılar. Ancak, yine de, blok zincir altyapısının bilgi güvenliği çözümlerine sunduğu önerilerin, kullanıcıların erişim izni süreçleri, sisteme erişebilen tüm katılımcılar açısından konsensüs mekanizmalarının etkinliği, şifrelerin türetilmesi, toplanması, depolanması, iyileştirilmesi ve yok edilmesi açısından özel anahtar yönetiminin etkinliği, sistemin çok yüksek işlem hacimlerindeki verimliliği açısından ölçeklendirilmesi ve verilerin mahremiyetinin korunması açısından yeni riskler oluşturabileceği de göz ardı edilmemelidir (Deloitte, 2021).
• Sızma Testi: Blok zincir tabanlı bir sistem, dağıtık defter kayıtlarının güncellenmesi için birden fazla katılımcının eş zamanlı olarak yüksek bağlantı frekanslarında iş birliği yapmasını sağlayan bir altyapı üzerinden işletilmektedir. Bu yüzden, böyle bir sistemin siber güvenlik açıkları açısından sürekli incelenerek, yeni altyapı bakımından herhangi bir ihlale sebep olmayacağının temin edilmesi kritik derecede önemlidir. Sonuç olarak, blok zincir sisteminin güvenlik ihlallerinin tespit edilmesinde, hızlı bir biçimde kontrol altına alınarak önlenmesinde ve onarılmasında, klasik sızma testlerine göre, etkin olup olmadığı daha detaylı bir biçimde değerlendirilmelidir (Deloitte, 2021).
• Yetenek yönetimi ve gelişimi: Blok zincir teknolojisinin getirdiği yenilikler ile birlikte iç denetçilerin ihtiyaç duyacağı yetkinlik setleri de farklı bir boyut kazanmakta ve bu altyapının nasıl kullanıldığına ilişkin eğitimlerin kurumlara entegre edilmesi nitelikli bir duruma gelmektedir (Deloitte, 2021).

Öncelikle, iç denetim perspektifinden, blok zincir tabanlı bir sistemin iç denetçilere sağlayacağı avantajlar şu şekilde sıralanabilir;

- Çevik analitik: Blok zincir ağında yetkilendirme prensiplerine göre karmaşık matematiksel algoritmalar vasıtası ile biçimselleştirilerek depolanan veri kümeleri gösterge panelleri ile güvenli bir şekilde güncellenebilmektedir (Deloitte, 2021).
- Eş zamanlı denetim: Blok zincir tabanlı sistemler geleneksel örneklem testinin haricinde yüzde yüz olarak ana kütle testine olanak tanırlar. Ayrıca, paylaşımda bulunan kayıt defteri vasıtası ile sisteme erişimi izin verilen tüm taraflar blok zincir ağında gerçekleşen işlemleri kontrol edebilirler. Örneğin, iç denetim departmanları, blok zincir ağındaki salt okunur bir düğümü gerçek zamanlı olarak izleyebilir, yapılan işlemleri takip edebilirler ve rutin olarak yönlendirilmesi gereken işlemleri veri analitiği araçları ile otomasyon sürecine dahil ederek kontrol aktivitelerini sağlayabilirler (Deloitte, 2021).
- Denetim döngüsünün kısaltılması: İç denetçiler anlamlı neticelere varılması doğrultusunda, verilerin toplanması, organize edilmesi ve arındırılması için ciddi ölçülerde zaman ve emek harcarlar. Herhangi bir blok zincir sisteminde, verilerin biçimselleştirilerek tutarlı bir şekilde saklanması ve bu verilere gerçek zamanlı olarak ulaşılma imkanının sunulması, iç denetçiler açısından oldukça önemli bir avantajdır. Bu sayede, daha hedefe yönelik, bilinçli ve planlı bir risk değerlendirmesi süreci mümkün kılınarak, zaman tasarrufu sağlanmaktadır. Bunlara ilaveten, iç denetçilerin, test operasyonlarında destekleyici belgelerin sağlanması için süreç sahiplerine güvenmeleri yerine, blok zincir üzerinden kendi elde ettikleri dokümanları takip ederek kontrol döngüsünü kısaltmaları ve verimliliği iyileştirmeleri sağlanabilir (Deloitte, 2021).
- Otomatikleştirilmiş sözleşme yaptırımı: Sözleşme şartlarına bağlılığının takip edilmesi bir hayli insan eylemini gerektiren ve hatalara açık bir süreçtir, bu nedenle sözleşme risklerinin uyumluluklarının kontrol edilmesinde iç denetçilerin olağan üstü efor ve dikkat sarf etmesi gerekmektedir. Üzerinde anlaşmaya varılan belirli iş koşullarına göre yürütülecek şekilde kodlanmış akıllı sözleşmeler bu süreci hızlandırabilmektedirler. Akıllı sözleşmeleri destekleyen blok zincir tabanlı bir sistemle, uyumluluk takipleri neredeyse tamamen otomatik hale getirilebilerek, denetçilerin odak noktalarının örneklem tabanlı bir test yönteminden daha değer katıcı bir yaklaşım olan otomatik işlevsellik testine dönüştürülmesi sağlanabilmektedir (Deloitte, 2021).
- Karşı taraflarla güvenilir mutabakatlar: Blok zincir sisteminde güvenli bir biçimde korunan verilerin tutarlı ve güvenilir olması sayesinde, bazı mutabakat denetimlerinin blok zincir ortamında test edilmesi gerekmeyebilir ve böylelikle iç denetçilerin diğer kontrollere odaklanması sağlanabilir (Deloitte, 2021).
- Verilerin hızlı bir şekilde kurtarılması: Blok zincir sisteminin benzersiz altyapısı sayesinde kayıtların birden fazla veri tabanında muhafaza edilmesi, verilerin tahrip edici bir olay sırasında ve sonrasında daha güvenli bir biçimde kurtarılabilmesine olanak tanımaktadır. Bu spesifik özellik sayesinde verilerin saklanması ve transfer edilmesi süreçleri daha düşük riskli kategorilerde değerlendirilebilmektedir (Deloitte, 2021).

Sonuç olarak, bu yeni altyapının merkezi bir otoriteye bağlı kalınmadan, daha güvenli bir kayıt sistemi sunularak, daha büyük ölçekli veri setlerinin anlamlı kılınması ile kontrol edilmesine olanak sağlaması, geleneksel iç denetim faaliyetlerinin değişimi üzerinde de yüksek bir potansiyele sahip olduğunu göstermektedir. Ancak, gelişen teknoloji ile ortaya çıkabilecek yeni risklerin de daha detaylı olarak değerlendirilmeye alınarak, denetim bazında yaşanacak uyum sağlama süreçlerinin daha etkin bir şekilde idare edilmesi gereklidir.

3. LİTERATÜR ARAŞTIRMASI

Literatürdeki araştırmaların derlenmesi ile oluşturulan plan çerçevesinde, bu çalışmanın blok zincir teknolojisindeki teknik altyapının siber güvenlik ve iç denetim açısından nasıl bir dönüşüm yaratabileceği konusu üzerine oluşturulmasına karar verilmiştir. Bu doğrultuda, çalışmanın amacı, blok zincir ağı yapılarının, geleneksel denetim enstrümanlarına tesirlerinin yanında, bilgi teknolojisi kontrolleri ve büyük verinin kullanımı açısından siber güvenlik yaklaşımlarına ve iç denetim yöntemlerine etkilerini incelemek olarak tanımlanmıştır. Geçmiş araştırma çalışmalarının ışığında, blok zincir teknolojisinin alt bileşenleri teknik konular ile birlikte incelenerek, yeni yapılacak çalışmalar için yol gösterici niteliğinde bir çalışma türetmek hedeflenmiştir.

Tablo 3. Kritik Literatür İncelemesi

Yazar ve Yıl	Makale Adı	Konu Kapsam	Sonuç
Rooney, Hugh; Aiken, Brian; Rooney, Megan; 2017	İç Denetim Blok Zincir'e Hazır mı? (Is Internal Audit Ready for Blockchain)	İç denetçilerin yönetişim, risk yönetimi ve kontrol alanlarındaki fonksiyonları blok zincir teknolojisi ile birlikte daha güvenli, şeffaf, hızlı ve etkin yöntemlerle dönüşüme ihtiyaç duymaktadır.	Blok zincir teknolojisi hükümetlerin ve diğer büyük organizasyonların yeniliğe yönelik dijital çözümler geliştirmesinde destekçi olurken, iç denetçilerin bilgi, yetkinlik ve diğer özelliklerini de sorgulamak gerektiğine de vesile olmuştur.
Risius, Marten; Spohrer, Kai; 2017	Bir Blok Zincir Araştırma Çerçevesi: Neyi Biliyoruz veya Bilmiyoruz, Buradan Nereye ve Nasıl Varırız? (A Blockchain Research Framework: What We (don't) Know, Where We Go From Here, and How We will Get There)	Blok zincir teknolojisi bozucu potansiyele sahip inovasyon araçları arasında yer almasına rağmen, kendisinden beklenen farkı oluşturamayabileceği yönünde fikirlerin de öne sürülmesine neden olmuştur ve bu doğrultuda blok zincir sisteminin genel araştırma çerçevesinden incelenmesi yapılmıştır.	Blok zincir teknolojisinin uygulanılabilirliği, kullanımı ve etkileri literatür çerçevesindeki çalışmalar açısından incelenerek gelecek araştırmalara ışık tutulmuştur.
Chedrawi, Charbel; Howayeck, Pierrette; 2018	Baş Temsilci Yaklaşımı ile Blok Zincir Çağında Denetim (Audit in the Blockchain Era within a Principal-Agent Approach)	Blok zincir ve denetim açısından bir model öne sürülerek, kurumlardaki geleneksel yönetişim yaklaşımlarına alternatif seçenekler sunulmuştur.	Düzenleyicilerin hem blok zincir teknolojisi için hem de denetçilerin yeni misyonu olarak görülen güvence misyonları için spesifik yasalar oluşturmaları gerekirken, denetçilerin de güvence rollerini taban alan birleşik bir blok zincir denetim sistemi kurmaları gerektiği üzerinde durulmuştur.
Uysal, Tuğba; Kurt, Ganite; 2018	Muhasebe ve Denetimde Blok Zinciri Teknolojisi	Blok zinciri teknolojisinin beraberinde getirdiği yeniliklere adaptasyon konusunda muhasebe ve denetim mesleğini icra eden kesimin yetkinliklerinin hangi yönde değişime uğrayacağı incelenmiştir.	Blok zincir teknolojisi muhasebe ve denetimin geleneksel fonksiyonlarına yeni faaliyet alanları açarak, muhasebe ve denetim mesleğine sahip kişilere bu teknolojik altyapının getirmekte olduğu ve getireceği farklılıklardan faydalar sağlama fırsatı sağlamaktadır.
Özdoğan, Burak; Karğın, Sibel; 2018	Blok Zinciri Teknolojisinin Muhasebe ve Finans Alanlarına Yönelik Yansımaları ve Beklentiler	Blok zinciri teknolojisi özet olarak tanımlanarak, muhasebe ve finans alanlarındaki kullanım fırsatları araştırılmıştır.	Muhasebe ve denetim uzmanlarının blok zinciri teknolojisi ile karşılaştıkları değişim rüzgarları doğrultusunda politikaların ve standartların yeniden değerlendirilmesi gerekmektedir.
Schmitz, Jana; Leoni, Giulia; 2019	Blok Zincir Teknolojisi Periyodunda Muhasebe ve Denetim: Bir Araştırma Gündemi (Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda)	Blok zincir teknolojisi muhasebe ve denetim mesleği açısından keşifsel olarak incelemeye tabi tutulmuştur.	Risk kontrolündeki yönetişim, şeffaflık ve güven meseleleri, blok zincir tabanlı teknolojilerin öncülüğündeki sürekli denetimler, akıllı sözleşme uygulamaları ve örnek teşkil eden dönüşümler ile muhasebecilerin ve denetçilerin rollerini etkilemiştir.
Liu, Manlu; Wu, Kean; Xu, Jennifer Jie; 2019	Blok Zincir Teknolojisi Muhasebeyi ve Denetimi Nasıl Etkileyecek: İzinsiz ve İzinli Blok Zincir Teknolojilerinin Kıyaslanması (How will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain)	Denetçilerin blok zincir teknolojisine adaptasyon sürecinin aşılmasına ve kendilerini blok zincir dönüşümünün birer stratejik ortağı olarak hissetmelerine yönelik spesifik önerilerde bulunulmuştur.	Blok zincir teknolojisi denetim endüstrisine somut farklılıklar getirerek, denetçilerin bu alandaki yönetişimin nasıl sağlandığına yönelik yetkinlikler kazanmaları için risk kontrol ve sürekli denetim uygulamalarında geleneksel rollerinin dışına çıkmalarının sağlanarak veri analitiği süreçlerine dahil olmaları gerektiği gerçeğini gün yüzüne çıkarmıştır.

Brender, Nathalie; Gauthier, Marion; Salihi, Arber; 2019	Blok Zincir Teknolojisinin Denetim Uygulamaları üzerine Potansiyel Etkisi (The Potential Impact of Blockchain Technology on Audit Practice)	İsviçre'deki denetçilerden alınan örneklem doğrultusunda gömülü teori (grounded theory) kullanılarak blok zincir teknolojisinin denetçilerin günlük aktivitelerine olan etkileri araştırılmıştır.	Bulgulara göre, küçük denetim firmaları yeni teknolojinin mesleğe pek fazla bir etkisinin olmayacağı yönünde görüş sunarlarken, öte yandan, gelecek süreçlerde, denetçilerin muhasebe odaklı aktivitelerden sıyrılarak bilgi teknolojileri ağırlıklı faaliyetlerde daha ağırlıklı olarak rol alacaklarını öne sürenler de olmuştur.
Karahan, Çetin; Tüfekçi, Aslıhan; 2019	Blok Zincir Teknolojisinin İç Denetim Faaliyetlerine Etkileri: Fırsatlar ve Tehditler	Blok zincir teknolojisinin iç denetim fonksiyonlarına potansiyel etkileri fırsatlar ve tehditler ikileminden değerlendirilmiştir.	İç denetçilerin blok zincir teknolojisindeki gelişmeleri yakından takip ederek kendilerini yeniliklere hazır konumda bulundurmaları gereklidir.
Demirhan, Habip; 2019	Vergi Denetiminde Yeni Bir Yaklaşım Olarak Blok Zinciri Teknolojisi	Vergi denetiminin geleceği blok zinciri uygulamaları çerçevesinden incelenmiştir.	Blok zinciri teknolojisi vergi denetiminde yüksek etkinliğe sahip olma potansiyeline sahip olması nedeni ile vergi toplama süreçlerini hızlandırarak kayıt dışı ekonomiye karşın aktif rol üstlenmeye hazırdır.
Ciğerci, İsmail; Eğmir, Rabia Tuğba; 2019	Kamu Mali Denetiminde Olası Blok Zincir Teknolojisinin Denetim Etkinliği Açısından Değerlendirilmesi	Blok zincir sistemi ile herhangi bir kamu mali denetim yapısının kurulup kurulamayacağı ve denetim faaliyetlerinin yürütülüp yürütülemeyeceği irdelenmiştir.	Kamu mali kontrollerinin blok zincir teknolojisi vasıtası ile gerçekleştirilmesi için bu sisteme uygun bilgi teknolojileri altyapısının tasarlanması ve mevzuat açısından yeni düzenlemelerin oluşturulması gerekmektedir.
Derrick, Bonyuet; 2020	Blok Zincir'e Genel Bakış ve Blok Zincir'in Denetim üzerindeki Etkisi (Overview and Impact of Blockchain on Auditing)	Blok zincir teknolojisi ile birlikte gelişen yeni risklerin ve fırsatların denetim mesleğine etkileri teknoloji perspektifinden derinlemesine araştırılmıştır.	Blok zincir teknolojisinin denetim mesleğine etkisinin minimal düzeyde olduğu gözlemlense dahi, bu teknolojinin müşterilerin işlerine etkisinin denetçiler tarafından kavranması gereklidir.
Dyball, Maria Cadiz; Seethmraju, Ravi; 2021	Blok Zincir Teknolojisinin Müşteriler Tarafından Kullanılmasının Denetim Riski ve Denetim Yaklaşımı üzerindeki Etkisi-Keşifsel Bir Çalışma (The Impact of Client Use of Blockchain Technology on Audit Risk and Audit Approach-An Explorative Study)	Denetim ortaklarını da kapsayan yirmi sekiz adet blok zincir hissedarı ile Avustralya Denetim Standardı ASA (Australian Auditing Standard) 315 doğrultusunda gerçekleştirilen yarı yapılandırılmış görüşmelerden yola çıkılarak bu yeni teknolojinin denetimler kapsamında yer alan risklerin tespit edilmesi ve değerlendirilmesi süreçlerindeki etkileri irdelenmiştir.	Blok zincir müşterilerinin işlemlerinin diğer müşterilerin aktivitelerine kıyasla daha riskli ve karmaşık süreçler içerdiği ortaya çıkarılmıştır.
Tusek, Boris; Jezovita, Ana; Halar, Petra; 2021	Hırvatistan'daki İç ve Dış Denetçilerin Blok Zincir Teknolojisinin Denetimi için Kullandıkları Analitik Prosedürlerin Farkları ve Önemleri (The Importance and Differences of Analytical Procedures' Application for Auditing Blockchain Technology Between External and Internal Auditors in Croatia)	İç ve dış denetçilerin blok zincir teknolojisi kontrolleri kapsamında yer alan faaliyetlerindeki farklar analitik prosedürlerin kontrol değişkeni olarak kullanılması doğrultusunda anket çalışmaları vasıtasıyla incelenmiştir.	İşletme süreçlerini blok zincir teknolojisi ile destekleyen şirketlerin verimlilikleri ve etkinlikleri denetim süreçlerinde ileri analitik prosedür uygulamalarının kullanılması ile geliştirilebilir.

4. ARAŞTIRMA

Çalışmada, blok zincir teknolojisinin siber güvenlik kapsamındaki kullanım alanları ve iç denetçilerin bu değişime adapte edilme süreçleri, keşifsel bir yaklaşım doğrultusunda bilgi edinme amacı ile değerlendirilmiştir.

4.1. Araştırmanın Konusu ve Amacı

Çalışmada, iç denetçilerin, siber güvenlik faaliyetlerinde kullanılabilen blok zincir teknolojisine uyum süreçleri araştırılarak, özellikle bilgi teknolojisi denetiminde rol alan ekiplerin bu yenilikten nasıl fayda sağlayabilecekleri ve hangi farklılıklar ile karşılaşabilecekleri kavramsal çerçeveden değerlendirilmek hedeflenmiştir. Çalışmada, ikincil veri kaynaklarından elde edilen bilgiler ile blok zincir teknolojisinin getirdiği yeniliklerin siber güvenlik kontrollerindeki uygulama sahalarının iç denetim fonksiyonlarına hangi yönde etki edeceği araştırılmıştır.

4.2. Araştırmanın Evreni ve Örneklemi

Araştırmada birincil veri kaynakları kullanılmadığı için örnekleme yapılmamıştır.

4.3. Araştırmanın Kısıtları

Çalışma sadece kavramsal çerçeveyi içermekte ve ikincil veri kaynaklarından oluşmaktadır.

4.4. Araştırmanın Hipotez Testleri

Nitel çalışmada ikincil veri kaynakları kullanıldığı için hipotez testlerine başvurulmamıştır.

4.5. Bulgular

Blok zincir teknolojisi, siber güvenlik ve iç denetim bağlamında gerçekleştirilen bu keşifsel çalışma ile literatürde yer alan araştırmalara farklı boyutlar kazandırılmak amaçlanmıştır. Özellikle, blok zincir sisteminin altyapısında içerdiği yeniliklerin kavramsal açıdan derinlemesine incelenmesi gerektiği gözler önüne serilerek, bu teknolojinin hangi prensipler üzerine oluşturulduğu, nasıl kullanıldığı ve teknik açıdan hangi fırsatları sunduğu hem temel olarak hem de siber güvenlik ve iç denetim açısından sorgulanmıştır. Aynı zamanda, bu yeniliğin sunduğu fırsatların yanında, oluşturabileceği riskler de kontrol çerçevesi perspektifinden incelenerek, geleceğe yönelik değerlendirmeler yapılmıştır. Özellikle, siber güvenlik kapsamında yapılan denetim faaliyetlerindeki geniş kullanım alanı ve verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasındaki eşsiz altyapısı ile blok zincir teknolojisi ister insanlardan ister de teknik meselelerden kaynaklı siber tehditlerin kontrol edilmesinde mükemmele yakın çözümler sunmaktadır. Bunların başında da, kritiklik derecesi yüksek bilgilerin ayrık olarak çoklu veri tabanlarında saklanması ve erişim mekanizmasının geleneksel ağ sistemlerine göre daha karmaşık süreçler içeren matematiksel algoritmalar vasıtası ile daha yüksek hızlarda türetilen şifreler doğrultusunda izin verilen kişilere dağıtılması ile sürekli kontrole fırsat tanıyan bir döngüye sahip olması bulunmaktadır. Ancak, denetim açısından da bahsedildiği gibi, blok zincir sistemi ile yönlendirilebilen, gerçek zamanlı kontrollerin sistemdeki güvenlik açıklarının ve olağan dışı durumların saptanmasındaki rolünün, geleneksel sızma testlerine kıyasla hangi oranda etkili olduğuna yönelik teknik çalışmaların yapılmasına mutlaka ihtiyaç duyulmaktadır. Bu bağlamda, simülasyon çalışmaları ve örnek olay modellemeleri ile bu yeniliğin testleri yapılarak geleceğe yönelik önerilerde bulunulabilir.

5. SONUÇ

Özellikle, bankalar gibi eş zamanlı işlemlerin sıklıkla gerçekleştirildiği kurumların, güvenlik altyapıları için daha çevik ve esnek iş yapış modelleri sunması nedeni ile denetçilerin bu yeni teknolojik altyapıya ısındırmaları sağlanarak, yetenekleri geliştirilmelidir. Önceden de belirtildiği gibi, blok zincir teknolojisi geleneksel denetim yaklaşımları için sunduğu bozucu fırsatların yanında, yönetişim açısından, risk değerlendirme standartları ve kontrol çerçevesi bağlamında daha çok yeni sayılmaktadır. Bu yüzden, kurumların bu altyapıya hangi ölçülerde sahip olabilecekleri konusunda yasal çerçevenin tasarlanması ve uygulanabilir hale getirilmesi gerekmektedir. Sonuç olarak, geleneksel denetim bazında yapılan faaliyetlerin odak noktası olarak değerlendirilen kritik verilere erişilebilirlik, kritik verilerin bütünlüğü, yönetişim, mevzuata uyumluluk, kritik verilerin gizliliği ve güvenliği ile değişim mühendisliği yaklaşımlarının uygulanması üzerine tanımlanan riskler blok zincir teknolojisi ile yapılan,

yapılıyor olan ve yapılacak kontrollerde de öncelikli yer almaktadırlar. Ancak, iç denetçilerin dağıtık defter teknolojisi ile gelen teknik donanıma kendilerini adapte ederek geleneksel kontrol yaklaşımlarına yenilikler katmaları gerekmektedir.

Hakem Değerlendirmesi: Dış bağımsız.

Çıkar Çatışması: Yazarlar çıkar çatışması bildirmemiştir.

Finansal Destek: Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

Etik Onay: Bu makale, insan veya hayvanlar ile ilgili etik onay gerektiren herhangi bir araştırma içermemektedir.

Yazar Katkısı: Seval Selimoğlu (%50), Mustafa Hakan Saldi (%50)

Peer-review: Externally peer-reviewed.

Conflict of Interest: The authors declare that there is no conflict of interest.

Funding: The authors received no financial support for the research, authorship and/or publication of this article.

Ethical Approval: This article does not contain any studies with human participants or animals performed by the authors.

Author Contributions: Seval Selimoğlu (50%) , Mustafa Hakan Saldi (50%)

KAYNAKÇA

Bonyuet, D. (2020). Overview and impact of blockchain on auditing. *The International Journal of Digital Accounting Research*, 31-43.

Brender, N., Gauthier, M., Morin, J.-H., ve Salihi, A. (2019). The potential impact of blockchain technology on audit practice. *Journal of Strategic Innovation and Sustainability, 14*, 35-59. Erişim adresi: https://articlegateway.com/index.php/JSIS/article/view/1370/1303

Chedrawi, C., ve Howayeck, P. (2018). Audit in the blockchain era within a principal-agent approach. *Conference: Information and Communication Technologies in Organizations and Society (ICTO 2018): "Information and Communications Technologies for an inclusive world".At: University Paris Nanterre - Pole Léonard de Vinci, Paris-France.* Paris: University Paris Nanterre.

Ciğerci, İ., ve Eğmir, R. T. (2019). Kamu mali denetiminde olası blok zincir teknolojisinin denetim etkinliği açısından değerlendirilmesi. *Maliye Dergisi, Temmuz-Aralık 2019*, (177), 203-217.

Deloitte. (2021). An ınternal auditor's guide to blockchain: auditing blockchain environments. Erişim adresi: https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html

Demirhan, H. (2019). Vergi denetiminde yeni bir yaklaşım olarak blok zincir teknolojisi. *Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 9*(18), 857-875. Erişim adresi: http://busbed.bingol.edu.tr/en/download/article-file/835623

Dyball, M. C., ve Seethamraju, R. (2021, Mayıs 19). The impact of client use of blockchain technology on audit risk and audit approach—An exploratory study. *International Journal of Auditing, 25*(2), 602-615.

Groenfeldt, T. (2014). *Forbes*. Enterprise tech. Erişim adresi: https://www.forbes.com/sites/tomgroenfeldt/2014/05/08/insiders-pose-a-serious-threat-to-corporate-information/?sh=2600bf965ca9

Gupta, R. (2018). *Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS Security Using Blockchain.* Birmingham: Packt Publishing.

Karahan, Ç., ve Tüfekci, A. (2019). Blokzincir teknolojisinin iç denetim faaliyetlerine etkileri: fırsatlar ve tehditler. *Denetişim*, (19), 55-72.

Leoni, G., ve Schmitz, J. (2019). Accounting and auditing at the time of blockchain technology: a research agenda. *Australian Accounting Review*, *29*(2), 331-342.

Maleh, Y., Baddi, Y., Alazab, M., Tawalbeh, L., ve Romdhani, I. (2021). *Artificial intelligence and blockchain for future cybersecurity applications.* Cham, Switzerland: Springer.

Manlu, L., Wu, K., ve Xu, J. J. (2019). How Will blockchain technology impact auditing and accounting: permissionless versus permissioned blockchain. *American Accounting Association, 13*(2), 19-29.

Martino. (2013). *IObit Forum*. IObit Forum. Erişim adresi: https://forums.iobit.com/topic/11210-28-types-of-computer-security-threats-and-risks/

Özdoğan, B., ve Karğın, S. (2018). Blok zinciri teknolojisinin muhasebe ve finans alanlarına yönelik yansımaları ve beklentiler. *Muhasebe ve Finansman Dergisi*(80), 161-176.

Pathak, A. (2021). *Blockchain Technology: a guide for beginners*. Erişim adresi:https://geekflare.com/finance/blockchain-technology-for-beginners/

Risius , M., ve Spohrer, K. (2017). A blockchain research framework: what we (don't) know, where we go from here, and how we will get there. *Business&Information Systems Engineering*, 385-409.

Rooney, H., Aiken, L. B., ve Rooney, M. (2017). Is Internal Audit Ready for Blockchain? *Technology Innovation Management Review, 7*(10), 41-44. Erişim adresi: https://timreview.ca/sites/default/files/article_PDF/Rooney_et_al_TIMReview_October2017.pdf

Statista Research Department. (2020). *Leading financial ınstitutions in practical ımplementation of blockchain technology in 2019, by number of projects.* Statista.

Tonsager, L. (2013). 5 Privacy and data security measures that can protect your company against trade secret theft. United States: Covington. Erişim adresi: https://www.insideprivacy.com/data-security/5-privacy-and-data-security-measures-that-can-protect-your-company-against-trade-secret-theft/

Tusek, B., Jezovita, A., ve Halar, P. (2021). The importance and differences of analytical procedures' application for auditing blockchain technology between external and internal auditors in Croatia. *Economic Research, 34*(1), 1385-1408.

Uysal, T. U., ve Kurt, G. (2018). Muhasebe ve denetimde blok zincir teknolojisi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 23*(2), 467-481. https://dergipark.org.tr/tr/download/article-file/1005745 adresinden alındı

Vasarhelyi, M. A., ve Halper, F. B. (1991). UNIX and the continuous audit of online systems. *Rutgers University*, 87-104.

SUMMARY

Blockchain technology provides the opportunity for authorized persons and organizations to control all simultaneous financial activities which are carried out in the accounts through the ledger which is shared with the permitted participants. Blockchain system allows for permanent protection of transacted information in terms of saving them securely in personal computers. Thus, the data, which are stored in the system, can be distributed to the authorized parties and the mechanism of access to the information can be processed sustainably with an effective and efficient approach. In this context, when any action is taken through the blockchain system, program codes and data which are stored and protected on the blocks come into play, and by this way, the audit of happenings in the transactions can be performed securely, transparently, and swiftly by the person who is authorized to monitor these events. The innovations, that blockchain technology has brought to the protection, secure access, and transfer of information have been raising question marks in minds to what extent the controls in cyber security processes have been affecting from this innovation and how the internal auditors can adapt to this change. Within this framework, the infrastructure of blockchain technology is going to be examined conceptually in order to classify its application fields in cyber security controls in terms of presenting recommendations for determining the direction in which the internal auditors should adapt to these new disciplines in this research project.

In this context, first of all block chain technology is deeply investigated through step by step approach from fundamental to advanced levels to understand the logic behind. After that, common cyber security issues are analyzed to be aware the differences between block chain technology infrastructure and traditional data base functions. Particularly, the security problems, which are caused from availability related item of CIA (confidentiality, integrity, and availability) triad in cyber risk management, are considered for how to benefit from block chain technology. Therefore, the processing mechanism of block chain technology is explored to frame the data protection part of this innovation. Because of these reasons, the research questions are defined as;

- Which features of block chain technology infrastructure do differ from traditional data base processes?
- How can the block chain technology be integrated to cyber security management?
- What are the pros and cons of block chain technology applications in cyber security operations?
- How can the internal auditors be adapted to this emerging technology?

According to the research problems, the main goal of the study is defined to investigate the conceptual framework that is related to block chain technology infrastructure, cyber security and internal audit field to show the link between these disciplines. Correspondingly, exploratory research method is applied by using secondary data sources which include online researches, literature reviews and case studies. In particular, since institutions such as banks, where concurrent transactions are frequently being carried out, offer more agile and flexible business models for their security infrastructures, their capabilities should be improved by ensuring that auditors should be adapted to this new technology.