T.C.
ANKARA ÜNİVERSİTESİ
Bilgi Yönetim Sistemleri Belgelendirme ve
Bilgi Güvenliği Merkezi (BİL-BEM)

BİLGİ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ

Editörler
Bahattin YALÇINKAYA
M. Altay ÜNAL
Burcu YILMAZ
Fahrettin ÖZDEMİRCİ

Ankara • 2019

Ücretsizdir

T.C.
ANKARA ÜNİVERSİTESİ YAYINLARI No: 676
Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi
(BİL- BEM) Yayınları No: 5

BİLGİ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

eBelge- eArşiv- eDevlet- Bulut Bilişim-Büyük Veri- Yapay Zekâ

Editörler

Bahattin YALÇINKAYA
M. Altay ÜNAL
Burcu YILMAZ
Fahrettin ÖZDEMİRCİ

Ankara- 2019

BİLGİ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

eBelge- eArşiv- eDevlet- Bulut Bilişim-Büyük Veri- Yapay Zekâ

Ankara Üniversitesi BİL-BEM, 2019.

ISBN: 978-605-136-472-8
e.ISBN: 978-605-136-473-5

1. Baskı: Ankara, 2019

Ankara Üniversitesi Yayınları No: 676
Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi Yayınları No: 5

Bilgi Yönetimi ve Bilgi Güvenliği: eBelge- eArşiv- eDevlet- Bulut Bilişim- Büyük Veri- Yapay Zekâ/ Editörler Bahattin YALÇINKAYA, Mehmet Altay ÜNAL, Burcu YILMAZ ve Fahrettin ÖZDEMİRCİ.- -Ankara, 2019.
xii. 508 s.; 16x23,5 cm.
Kaynakça var.

1. Elektronik Belge Yönetimi. 2. Bilgi Yönetimi. 3. Bilgi Güvenliği
I. YALÇINKAYA, Bahattin. II. ÜNAL, Mehmet Altay. III. YILMAZ, Burcu. IV. ÖZDEMİRCİ, Fahrettin.

İletişim:

Ankara Üniversitesi
Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi (BİL- BEM)
Gölbaşı 50. Yıl Yerleşkesi BEYAS Binası 06830 Gölbaşı/ ANKARA
e-Posta: bilbem@ankara.edu.tr Web: http://bilbem.ankara.edu.tr
Tlf: (0312) 484 51 89

Baskı Yeri:
Ankara Üniversitesi Basımevi
İncitaşı Sokak No. 10, 06510, Beşevler/ ANKARA
Tel: 0312 213 66 55
Basım Tarihi: 27.12.2019

Editörler ve Bilim Kurulu

Editörler

Bilim Kurulu

Kitapta yer alan çalışmalar çifte körleme yöntemiyle Bilim Kurulu tarafından değerlendirilmiştir.

Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı[16]

Influence of Blockchain Technology to the Success of Protecting the Trustworthiness of Electronic Records

Niyazi ÇİÇEK
İstanbul Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Özhan SAĞLIK
Bursa Uludağ Üniversitesi

Öz

İnternetin keşfinden sonraki önemli gelişmelerden biri olarak değerlendirilen blokzincir teknolojisi, ilk başlarda daha çok altın, para vb. gibi değerli varlıkların transferi sırasında ortaya çıkan kayıt bilgilerinin teyit edilip kanıtlanması için kullanılmış, bu uygulamadan sağlık, telif hakları ve maliye gibi alanlarda da yararlanılabileceği görülmüştür. Bu teknoloji, elektronik ortamdaki bir kaydın güvenilirliğini merkezi bir otoriteye ihtiyaç duymadan, çevrimiçi bir ortamda dağıtarak sağladığı için böyle bir uygulamadan elektronik şekilde üretilip transfer edilen, dosyalanıp arşivlenen belgelerin güvenilirliğini kontrol etmek için de yararlanılabileceği düşünülmektedir. Bu konuda literatüre girmiş yabancı dilde yayınlanan çalışmalar bulunmaktadır. Fakat blokzincir teknolojisi kullanarak oluşturulan belgelerin arşivsel bağı nasıl kurulacak, özgünlüğü nasıl muhafaza edilecek ve güvenilirliği nasıl korunacak gibi soruların, Türkiye'de yeteri kadar tartışılmadığı görülmektedir. Çalışmanın amacı, bu teknolojinin elektronik belgelerin güvenilirliğinin başarılı bir şekilde korunmasına yapacağı olumlu ve olumsuz etkileri, Türkiye koşullarında incelemektir. Çalışmanın kapsamı blokzincir teknolojisinin belge yönetimi alanında kullanılabilirliğiyle sınırlandırılmıştır. Bu teknolojinin kullanıldığı belge yönetim sistemlerinde belgeler, iz değerleri (hash) aracılığıyla muhafaza edilmektedir. Durum böyle olunca, belgelerin bütünlüğünün korunabileceği savını ileri sürmek mümkündür. Bununla birlikte, elektronik belge yönetimi sistemlerinde belgelerin ait oldukları faaliyet ve fonksiyonla ilişkisi kurularak arşivsel bağın muhafaza edilmesi ve kontekstin korunmasında çeşitli sorunların yaşandığı bilinmektedir. Ayrıca, sistem kriterlerinin doğru işletilmediği elektronik belge yönetimi sistemlerinde belgenin bütünlüğü ve tamlığının da ciddi olarak zarar görme ihtimali yüksektir. Bu durumda, blokzincir teknolojisi elektronik belgelerin güvenilirliğinin başarılı bir şekilde korunması için nasıl kullanılabilir ve hangi yönleri geliştirilebilir soruları sorulmaktadır. Böyle bir teknolojinin gelişmekte olması nedeniyle çalışmada nitel araştırma yöntemi kullanılmış, durum çalışması

[16] Bu çalışma, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Bölümünde Prof. Dr. Niyazi Çiçek'in danışmanlığında yürütülmekte olan Özhan Sağlık'ın "Arşivlenen Elektronik Belgelerin Delil Değerinin Güvenilirlik Açısından İncelenmesi" adlı teze dayanılarak hazırlanmıştır.

benimsenmiştir. Literatürdeki kaynaklardan yararlanılmış; ayrıca 4 saha uzmanıyla da görüşme yapılmıştır. Çalışma neticesinde blokzincir teknolojisi kullanılarak elektronik belgelerin güvenilirliğinin başarılı bir şekilde korunabileceğini söylemenin erken olduğu, yeni bir takım çalışmalara ihtiyaç bulunduğu görülmüştür. Buna rağmen sorunun uygulamalı çalışmalar yapılarak ortadan kalkabileceği; böylece, bu teknolojinin elektronik belgelerin güvenilirliğini başarılı bir şekilde korunmasına önemli katkılar yapabileceği kanaatine varılmıştır. Çalışmadan, belge yönetiminde kullanılacak blokzincir teknolojisinin güvenilirlik bakış açısıyla incelenmesi yönünde bir farkındalık oluşturması beklenmektedir.

Anahtar kelimeler: *Blokzincir, e-belgelerin güvenilirliği, erişim güvenliği*

Abstract

Blockchain technology which is considered to be one of the significant developments after the discovery of internet has been used to verify and give a proof of registration information during the transfer of valuable assets such as gold, money etc. at first. This application can be used in areas such as health, copyrights and finance. This technology can ensure the trustworthiness of the record in the electronic media by distributing on-line and without need to the central authority so it has been thought that an application like this can be used to control trustworthiness of born and transferred electronically, foldered and archived records. There are studies published in a foreign language in the literature, but it has seen that the questions like how the archival bond established, authenticity maintained and trustworthiness protected of the records created by using the blockchain technology have not debated much in Turkey. Researching the positive and negative effects of this technology on protecting the trusworthiness of e-records successfully in the conditions of Turkey is the aim of the study. The scope of the study is limited to the availability of blockchain in records management. In the records management systems where this technology is used, the records are kept by hash values. In these circumstances, it is possible to argue that the integrity of the records can be preserved. However, in electronic records management systems, it is known that various problems are experienced in maintaining the archival bond and preserving the context by establishing the relationship between records and the activity and function they belong to. Also, in electronic records management systems where the system criteria are not operated correctly, the integrity and accuracy of the records likely to be seriously damaged. In this case, the question of how the blockchain technology can be used to protect the trustworthiness of e-records successfully and which aspects of it can be improved have been asked. Due to the development of such a technology, a qualitative research method used and case study was adopted. Resources in the literature have been utilized and 4 experts were interviewed. As a result of the study, it is early to say that the trusworthiness of electronic records can be successfully protected by using blockchain technology and new researches are needed have been found. Nevertheless, the problem can be solved by performing practical studies; thus, this technology can make essential contributions to the protecting trustworthiness of e-records successfully have been reached as a conclusion. It has been expected from the study to create awareness of investigating the adoption of blockchain technology in the records management with the viewpoint of trustworthiness.

Keywords: *Blockchain, trustworthiness of e-records, access security*

1. Giriş

Bilgi teknolojisinin gelişmesiyle kâğıttan elektroniğe kayan belgelerle ilgili tartışılan konulardan biri de özgünlük ve güvenilirlik meselesidir. Elektronik belgelerin güvenilirliği konusunda hukukçular birtakım yeni tanımlar ve kriterler geliştirirken yazılımcılar da farklı uygulamalarla sahaya ışık tutmaktadır. Bunlardan biri de belgeyi hazırlayan, imzalayan, dağıtan, işlemini gerçekleştirip dosyalayan paydaşların merkezi bir otoriteden bağımsız olarak kendi ağlarında da belgeyi tutabildiği, bu süreçlerin kaydının ve iz değerlerinin ilk işlem gördüğü şekliyle takip edilebildiği bir sistem olan dağıtık defter teknolojisidir (DDT). Bu teknoloji üzerinde önemli çalışmalar yapılıp uygulama daha da geliştirilmiş ve blokzincir adıyla bildiğimiz bir yapı ortaya çıkmıştır. Hazırlayan ve üretici gibi bütün belge paydaşlarının işlemlerini bir iz değeri olarak takip edebilme imkânı veren blokzincir teknolojisinin, bir elektronik belge için onun delil değerini koruyan e-imza, e-mühür veya KEP gibi güvenilirlik unsuru katan bir mekanizma olarak kullanılabileceği düşünülmektedir.

Dağıtık defter, bir ağdaki katılımcılar tarafından bağımsız olarak tutulan ve güncelleştirilen bir veritabanıdır. DDT'de tutulan kayıtlar, merkezi bir makam tarafından üretilmeyip ağdaki katılımcıların oluşturdukları düğümler tarafından meydana getirilir ve saklanırlar. Bu nedenle DDT, internetin keşfinden sonraki en önemli gelişmelerden biri olarak değerlendirilmektedir (Berryhill, Bourgery ve Hanson, 2018, s. 10). Verilerin güvenilirliğinin nasıl sağlanacağı sorusu üzerine blokzincir teknolojisi geliştirilmiş, bu da daha çok kullanılan bir DDT haline gelmiştir.

Blokzincir teknolojisi, ilk olarak kripto paraların transferinde kullanılmış, kişisel sağlık kayıtları ile vergi kayıtları gibi mali içerikli belgelerin üretilip saklanmasında da tercih edilmeye başlanmıştır. Bu teknolojinin, belgelerin bozulmadan saklanmasını mümkün kılarak güvenilirliği koruduğu iddia edilmektedir (Lemieux, 2016a). Fakat belgelerin bütünlüğü nasıl kontrol ediliyor, tamlık nasıl denetleniyor ve özgünlük nasıl sağlanıyor gibi soruların ülkemizde yeteri kadar tartışılmadığı görülmektedir.

Bu çalışma, blokzincir teknolojisinin e-belgelerin güvenilirliğinin başarılı bir şekilde korunmasına yapacağı olumlu ve olumsuz etkileri incelemeyi amaçlanmaktadır. Çalışmanın problemi ise şöyle belirtilebilir: "Blokzincir teknolojisinde belgelerin bütünlüğünü sağlıklı bir şekilde koruyacak araçların geliştirildiği görülse de özgünlük ve tamlığı yeteri kadar koruyacak mekanizmaların henüz oluşturulamadığı gözlenmektedir. Bu durumun belgelerin güvenilirliğinin başarılı bir şekilde korunması noktasında yeteri kadar sağlıklı sonuçlar oluşturmayacağı düşünülmektedir". Çalışmada, "blokzincir teknolojisinin elektronik belgelerin güvenilirliğinin başarılı bir şekilde korunması için geliştirilmeye açık yönleri bulunmaktadır hipotezi" benimsenmiştir. Örgütlerde arşivcilik ve belge yönetimi fonksiyonları

uygulanırken özellikle elektronik belgelerin güvenilirliğinin sağlanmasında blokzincir tekniklerinden daha fazla yararlanılabileceği düşünülmektedir. Çalışmanın soruları ise bu teknolojide e-belgelerin bütünlüğü nasıl korunuyor, tamlık nasıl denetleniyor ve özgünlük nasıl sağlanıyor şeklindedir.

E-belgelerin güvenilirliğinin başarılı bir şekilde korunmasında bu teknolojinin karşılaştığı problemlerin açıklanması da bu yazının hedefleri arasındadır. Çalışmada yöntem olarak nitel araştırma yöntemi benimsenmiştir. Belgelerin güvenilirliğinin başarılı bir şekilde korunması meselesinin betimlenmesi hedeflendiğinden, yazıda nitel araştırma türü olarak "durum çalışması" kullanılacaktır. Literatürdeki kaynaklar incelenmiş ve bu konuda çalışma yapan uzmanlarla görüşmeler gerçekleştirilmiştir. Literatür, "blokzincir" (blockchain), "güvenilirlik" (trustworthiness), "özgünlük" (authenticity), "bütünlük" (integrity), "tamlık" (accuracy), "arşivsel bağ" (archival bond) anahtar kelimeleri ışığında taranmıştır. Saha uzmanlarıyla yapılan görüşmelerde örneklem seçilirken kişilerin çalıştıkları ya da araştırma yaptıkları kurumlarda blokzincir teknolojisini arşiv ve belge yönetiminde kullanmalarına dikkat edilmiştir. Bu bağlamda görüşmeler, blokzincir teknolojisinin e-belgelerin güvenilirliğinin tespitinde kullanılması yönünde çalışmalar yapan British Columbia Üniversitesi Kütüphane, Arşiv ve Bilgi Çalışmaları Okulu öğretim üyesi Prof. Dr. Victoria Lemieux, İngiliz Milli Arşivinde blokzincir teknolojisinin arşivcilik pratiklerini nasıl etkileyeceğini araştıran projenin araştırmacılarından Dr. Alex Green (Archangel, 2019), oluşturulan bir dokümanın farklı ülkelerde de delil değeri taşıması için blokzincir altyapısı kullanarak Proofstack (2019) adında bir mekanizma geliştiren Kadir Kurtuluş ve belgem.io (2019) adında kurumlardan eğitim alan bireylerin edindikleri sertifikayı blokzincir altyapısı kullanarak saklayan ve paylaşan bir proje geliştiren Bankalararası Kart Merkezi çalışanları ile gerçekleştirilmiştir. Bu yazı hazırlanırken, özellikle Lemieux'in çalışmalarından büyük ölçüde yararlanılmıştır.

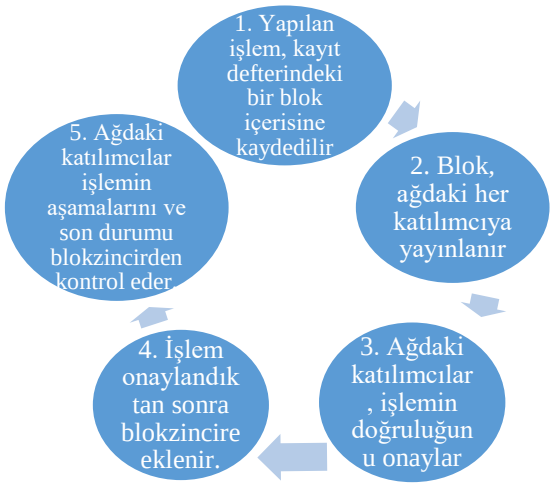
Makalede girişin ardından ilk kısmında dağıtık kayıt defteri ve blokzincir teknolojisinin açıklanmasına gayret edilmiştir. İkinci kısımda, elektronik belgelerin güvenilirliği meselesinin analiz edilmesine çalışılmıştır. Son kısımda ise bu yazının asıl temasını oluşturan blokzincirin e-belgelerin güvenilirliğini nasıl başarılı bir şekilde koruyabileceği ile ilgili tartışma ve açıklamalara yer verilmiştir. Değerlendirme ve sonuç kısmında elde edilen bilgilerin tartışılıp muhtemel çalışmaların dile getirilmesine gayret edilmiştir. Çalışmadan, yeni araştırmalara kaynaklık etmesi beklenmektedir.

2. Dağıtık Defter ve Blokzincir Teknolojisi

DDT, farklı birimler, ülkeler ve kurumların gerçekleştirdiği işlemlere dair kayıtların merkezi olmayan bir ağda paylaşılmasını mümkün kılmaktadır. İşlemler, katılımcıların onayını aldıktan sonra birbiri ardına devam eden defterlere kaydedilir. Burada otorite kabul edilen bir kayıt söz konusu

değildir; farklı yerlerdedir, ama üretilen kayıtların hepsi birbirinin aynısıdır (Berryhill ve diğerleri, 2018, s. 11-12). Mesela belediye, üniversite ve kalkınma ajansının yer aldığı bir süreçte gerçekleştirilen işlemler neticesinde imzalanarak oluşan belgeler defterlere kaydedilir ve bu defterler her kurumun kendi ağında birebir kopyası çoğaltılarak saklanır. Bu teknolojinin dikkat çeken özelliği, ağ kapsamında merkezi bir yapının bulunmamasıdır. Yapılmak istenen güncellemeler, yani oluşturulan yeni işlemler kararlaştırılan kurallar çerçevesinde bağımsız olarak her katılımcı tarafından oluşturulup veri tabanına kaydedilir (Buchman, Rathgeb, Baier, Busch ve Margraf, 2017, s. 745). Merkezi ağ yapılarında verilerin başka kişilerin eline geçme ihtimali daha kuvvetli olduğundan dağıtık veri tabanlarının kullanılması yönünde bir eğilim görülmektedir (Durbilmez ve Türkmen, 2019, s. 34). Dağıtık kayıt defterinin en çok kullanılan türü olarak dikkat çeken blokzincir teknolojisinde oluşturulan veriler kriptoloji kullanılarak şifrelenmektedir (Lemieux, 2016).

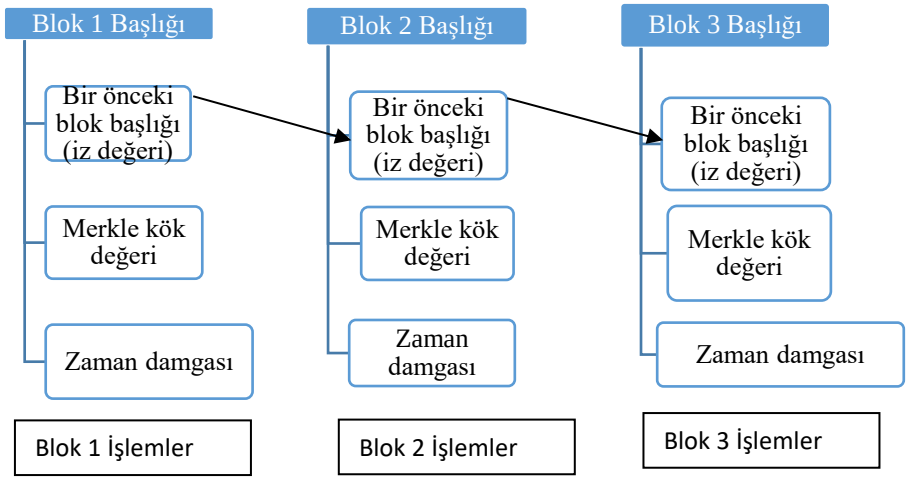
Blokzinciri anlatan ilk çalışmalardan biri bitcoin adlı kripto parayı takma adıyla tanıtan Satoshi Nakamoto'nun makalesidir (Nakamoto, 2008). Satoshi, burada doğrudan blokzincirden bahsetmese de kripto paraların kullandığı yapı blokzinciri gündeme getirmiştir. Makalede bu teknolojiyle güvenilir üçüncü taraflara ihtiyaç duymadan, işlem yapılabileceği belirtilmektedir. İşlemler bir blokzincir ağında yapılmaktadır ve ağdaki katılımcılar tüm işlem geçmişini görebilmektedir (Nakamoto, 2008). Dağıtık defter yapısı sayesinde işlemlerin anlık olarak kaydedilmesi, gerçek zamanlı olarak izlenmesi ve kontrol edilmesi imkânı oluşmaktadır. Böylece, kayıtların güvenilirliğine katkı yapıldığı belirtilmektedir (Hyla, 2019, s. 3). Çünkü, blokzincirlere eklenen işlemlerin, sonradan değiştirilemeyeceği dile getirilmektedir (Galiev ve diğerleri, 2019, s. 84). İşlem oluşturma süreci aşağıdaki şekille şöyle gösterilebilir (Canaday, 2017; Sayarlıoğlu, 2018):



Şekil 1. Blokzincirde İşlem Oluşturma Süreci

Blokzincir, üretilen bir veriyi belirlenen kurallar çerçevesinde kaydeden, bu kayıtları pek çok farklı noktayla paylaşabilen ve bu süreçte verilerin güvenilirliğini koruyan bir teknoloji olarak öne çıkmaktadır. Verilerin değiştirilemezliği, güvenliği, onaylanabilirliği, dayanıklılığı ve şeffaflığı bu teknolojinin öne çıkma nedenleri arasında gösterilmektedir (Birleşmiş Milletler, 2018, s. 5-6). Bu uygulamada verilerin saklandığı yapılar, blok olarak adlandırılmaktadır. Tamamlanan bloklar birbiri ardına bir zincir halkası gibi eklenir ve blok zincirler oluşturulur. Her blok, zaman damgası alarak oluşturulduğu ana dair tarih ve saat bilgilerine sahip olur. Böylece, her biri kendi imzasına sahip, belirli bir zamanda kaydı oluşturulan veri blokları sıra ile arka arkaya dizilmiş bloklardan meydana gelen bir zincir oluşturulur (Hofman, Lemieux, Joo ve Batista, 2019, s. 248).

Bloklardaki içeriğin değiştirilememesi için kriptografik özetleme ve zaman bilgisi kullanılmaktadır. Bloklar, kendi içerisinde üretilmiş veriler ve başlıktan oluşur. Blok başlığı bir önceki bloğa ait iz değeri (hash), blok içerisindeki verilere ait Merkle kök değeri ve zaman bilgisini içermektedir. Bu durumda, bir yerde olabilecek değişiklik, otomatik olarak diğerlerini de etkileyecektir. Durum böyle olunca, blok içerisindeki verilerin değişmesi için hem hedeflenen blok hem de ondan sonra gelen tüm blokların değişmesi gerekmektedir. Bu değişikliğin gerçekleşme ihtimali bulunsa da pratik olarak mümkün olmayacağı ifade edilmektedir (Zikratov, Kuzmin, Akimenko, Niculichev ve Yalansky, 2016, s. 538). Blokzincirin bu özelliği belgelerin delil değerinin korunmasında kullanılabilecek temel paradigma olarak görünmektedir. Bu paradigma aşağıdaki şekille şöyle gösterilebilir (Lemieux, 2016):



Şekil 2. Blok Yapısı

Sahada pek çok farklı blokzincir türü bulunduğu bilinmektedir. Örneğin kayıtlı verileri okumak ve bu ağın mutabakat sürecine uygun olarak yeni bloklar ekleyebilmek için izin gerekmiyorsa, bu türe "bütünüyle izin gerektirmeyen blokzincir ağları" adı verilmektedir. Buna kripto para alım-satımları örnek verilebilir. Kayıtlı verileri okumak için izin gerekmiyor, fakat ağın mutabakat yapısına uygun olarak yeni bloklar ekleyebilmek için izin gerekiyorsa, bu türe "kısmen izin gerektirmeyen blokzincir ağları" denilmektedir. Bu ağ türüne müzik eseri sahiplerinin eserlerini çeşitli mercilerin onayından sonra yükledikleri platformlar örnek verilebilir. Aynı zamanda bu iki ağ türü *açık ağlar* olarak adlandırılmaktadır (Usta ve Doğantekin, 2018, s. 32). Bununla birlikte bazı kurumlar halka açık blokzincir ağlarında verilerini tutmayı tercih etmeyebilir. Bu noktada onlar için geliştirilen çözüm özel blokzincir ağlarıdır. Kayıtlı verileri okumak için izin gerekiyor fakat mutabakat sürecine dâhil olduktan sonra yeni bir blok oluşturmak için izin almak gerekmiyorsa kısmen izin gerektiren blokzincir ağları, her iki süreç için de izin almak gerekiyorsa bütünüyle izin gerektiren blokzincir ağları kullanılmaktadır. Kısmen izin gerektiren blokzincir ağlarına banka şubelerinin havale yapabilmeleri için sisteme dâhil edilirken onay veren bankalar, bütünüyle izin gerektiren yapılara ise belge üreten kamu kurumları örnek verilebilir (Berryhill ve diğerleri, 2018, s. 18-19; Usta ve Doğantekin, 2018, s. 33-34).

Blokzincirlerdeki katılımcılar, birer düğüm (node) olarak adlandırılmaktadır (Yaga, Mell, Roby ve Scarfone, 2018, s. 3). Her blokzincir, ağdaki düğümlerin blokzincirde nasıl işlem oluşturup blok ekleyeceği ve bu işlemlerin nasıl doğrulanacağına ilişkin kendi kurallarına ve algoritmalara sahiptir. Blokzincirlerde düğümlerin blok eklemeleri için mutabakat yaklaşımı sergilemeleri gerekmektedir. Bu noktada, emeğin ispatı (proof of work), sahipliğin ispatı (proof of stake) ve yetkinin/kimliğin ispatı (proof of authority/identity) şeklinde üç türle karşılaşılmaktadır (Berryhill ve diğerleri 2018, s. 47-48). Emeğin ispatında bir düğüm için yeni bir blok oluşturmak istediğinde, diğer düğümlerin onayı gerekir. Bu işleme madencilik denilmekte olup, madenci işlevindeki düğüm, sürece onay vermelidir. Bu onaydan sonra, blok ağdaki yerini almaktadır. Sistemin yapısal özelliği gereği düğümler, tüm işlemler ve bir önceki bloktaki iz değerlerinin korunduğunu kontrol etmekle yükümlüdürler (Yaga ve diğerleri, 2018, s. 20-22). Buna kripto paralar örnek verilebilir. Ağa katılanlara bir teşvik verilmektedir. Bu teşvik ağa düğüm ekleme karşılığında bir kripto para birimi elde etme veya veri girişi yaparak sürekli sistemde kalma gibi maddi ya da maddi olmayan bir şekilde gerçekleşebilir. Mesela bazı kripto para birimlerinde halka açık torrent (sel)[17]

[17] Torrentler, verilerin paylaşılma miktarıyla verilere erişim hızının doğru orantılı olduğu bir yapıdır. Bu nedenle, sel yani torrent olarak adlandırılmıştır. BitTorrent ise sabit bir sunucuya sahip olmadan bağımsız sunucu tanımlama dosyaları aracılığıyla torrent sistemidir. BitTorrent'te herkes birer sunucu olarak sisteme katılabilir.

dosyaları kullanılmakta ve işlemlerde sınırsız üstveri girişi yapılabilmektedir. Varlıklarla ilgili veriler ve üstveriler BitTorrent aracılığıyla saklanmaktadır. Uçtan uca protokolünün yani torrent gibi merkezi bir koordinasyona ihtiyaç duyulmayan yapının benimsendiği sistemde, uçlar kripto para düğümlerinin yaptığı işlemleri dağıtık defterlere kaydetmektedir. Bu uçlar, dünyanın herhangi bir yerinde bulunabilirler. Uçlar verileri indirerek BitTorrent ağına katılmaya devam etmektedir (Lemiuex, 2017, s. 2276).

Sahipliğin ispatı mutabakat yaklaşımında blok üretim ve geçerlilik onay mekanizması, bloğu üreten makinenin ilgili blokzincir ağı üzerinde sahip olduğu pay ile ilişkilendirilir (Usta ve Doğantekin, 2018, s. 123). Bu aşamada kullanılan bir diğer yöntem de Practical Byzantine Fault Tolerance (PBFT) Müsamaha Gösterilen Pratik Bizans Hatası olarak Türkçe'ye çevirilebilecek bir yöntemdir. Bu yapı adını, Bizanslı generallerin kullandığı bir yöntemden almaktadır. Bizans İmparatorluğu'nda, imparatordan gelen emirlerin gerçek olup olmadığını anlamak için generallerin kullandığı oldukça basit ve etkili bir yöntem kullanılmaktaydı. İmparator, ordusuna bir emir vereceği zaman bunu generallere ulaştırmak için birden fazla ulak yollamakta ve generaller de emri aldıklarında kendi aralarında ulaklar ile bu emirleri paylaşmaktaydılar. Bu süreç içinde eğer imparatordan gelen emir ulakların çoğunluğu tarafından doğrulanmış ise bu emrin doğru olduğu kabul edilmekte; aksi takdirde tekil emirlere itimat edilmemekteydi (National Archives and Records Administration [NARA], 2019, s. 5). Bu çözüm, blokzincir teknolojisinde şöyle kullanılmaktadır: Ağ yapısına dâhil olan doğrulayıcı rolüne sahip her makine için özel bir açık-gizli anahtar ikilisi mevcuttur. Her makine diğer makinelerin açık anahtar bilgisine sahip olup kendisine gelen işlem bilgisini, kendi üzerinde tutulan veri yapısını kullanılarak kontrol eder; onayladığı bir işlemi gizli anahtarıyla imzalayarak ağda paylaşır. Eğer bir işlem, belirli bir sayıda makine tarafından onaylanmış ise mutabakat sağlanmış kabul edilir ve bu işlem ağ tarafından geçerli işlem olarak tanımlanır. Bu yaklaşım kapsamında ağa dâhil olan tüm doğrulayıcı makinelerin birbirinden haberdar olması ve ağa dâhil olacak yeni bir doğrulayıcının merkezi bir yapı tarafından onaylanması gerekmektedir. Bu nedenle açık yapılar yerine daha çok özel yapılar içerisinde kullanılmaktadır (Dini ve diğerleri, 2018).

Yetkinin ya da kimliğin ispatı mutabakat yaklaşımında ise tarafların gerçek dünyadaki kimlikleri bilinmektedir. Düğümlerin, işlem yapmak için blokzincir ağındaki kimliklerini doğrulamaları gerekir. Burada, düğümlerin yeni bir blok yayınlaması kimliklerini ya da yetkilerini ispat etmeleriyle mümkündür (Yaga ve diğerleri, 2018, s. 23). Elektronik belgelerin güvenilirliğinin başarılı bir şekilde korunması için kullanılacak blokzincirlerde yetkinin ve sahipliğin ispatı mutabakat yaklaşımından yararlanılabileceği düşünülmektedir.

Blokzincir teknolojisinin yolsuzluğu engelleme, şeffaflığı hâkim kılma, daha sağlıklı belge yönetimi gibi faydalarının yanı sıra yeteri kadar olumlu

görülmeyen kullanımları da söz konusudur. Blokzincir teknolojisinin, merkezi bir otoriteye ihtiyaç duymadan tabandaki herkesin sürece eşit şekilde katılımını öngören bir yapıyı gündeme getirerek güveni sağladığı iddia edilmektedir. Burada güven, sürece katılanların şahitliğine göre şekillenmektedir (Atalay, 2018, s. 49). Bu teknoloji ile işlem yapabilme yetkisi devletler tarafından önceden verilmiş noter, tapu müdürlüğü gibi bir yetkiliye eskisi kadar ihtiyaç duyulmayacağı, evlilik akdi, mal alım-satımı, para transferi gibi işlemlerin muhataplar tarafından blokzincirde gerçekleştirilebileceği ifade edilmektedir (Uysal ve Aldemir, 2018, s. 517; Atalay, 2018, s. 49; Yermack, 2017, s. 9). Ticari faaliyetlerin gerçekleştirildiği Bitnation adlı uygulamada insanların belirledikleri kurallar dâhilinde mal alım satımı yaparak ekonomiye katıldıkları görülmektedir. Bu uygulamanın sermayenin sınırsız bir serbestlik içerisinde dolaşımına izin veren küçük devletler veya kişilerin bir araya gelerek oluşturduğu otonom cemaatlere izin vererek serbest bir pazar oluşturma hedefinde olduğu anlaşılmaktır (Atalay, 2018, s. 49; Bitnation, 2019). Tüm bu uygulamaların küresel düzeydeki faaliyetlere daha çok yarar sağladığı görülmektedir.

Bundan dolayı, Dünya Bankası, Microsoft, IBM gibi küresel çapta iş yapan kurumların blokzincir teknolojisini destekledikleri görülmektedir (Blockchain Türkiye Platformu, 2019). Bu kurumların sermayenin sınırsız ve kuralsız bir şekilde dolaşmasını savunduğu bilinmektedir. Bu anlayış, günümüz yönetim sisteminde pek çok neoliberalizm taraftarlarınca da savunulmaktadır. Fakat neoliberalizmin iflas ettiği çeşitli mecralarda belirtilmiş (Guardian, 2016; Medium, 2018; Guardian, 2018), Uluslararası Para Fonu dergisinde de neoliberalizmin sosyal eşitliği ve kalkınmayı sağlayamadığı dile getirilmiştir (Ostry, Loungani ve Furceri, 2016). O halde, küresel düzeyde iş yapan sermaye sahiplerinin mevcut konumlarını korumak için yeni bir yaklaşım bulması bir gereklilik haline gelmiştir. Devletlere ihtiyaç duyulmadan da işlemler yapılabileceğine yönelik söylemle öne çıkan yaklaşımın teknoloji dünyasındaki karşılığının blokzincir teknolojisi olduğu düşünülmektedir (Herian, 2018, s. 165-166). Bunun sebebinin de bu teknolojinin faaliyetler sırasında ortaya çıkan idari işlemlerin ve buna bağlı olarak üretilen belgelerin delil değerini her koşulda koruyabilme gücüdür. Olumlu ve olumsuz tarafları olsa da, üstte açıklanmaya çalışılan tüm bu argümanlar, kamuda oluşan elektronik belgelerin güvenilirliğinin korunmasında blokzincir teknolojisinden yararlanılabileceği öngörülmektedir.

3. Elektronik Belgelerin Güvenilirliği

Hukuki işlemlerin sonucunda oluşup bir hakkın ya da yetkinin varlığını ispat eden belgeler (Çiçek, 2009) de birer delildir ve diğer tüm deliller gibi belgelerin de güvenilir olması beklenir. Güvenilirlik, güven duygusundan kaynaklanmaktadır ve kamu belgelerinin güvenilirliği hukukun kanıtlama

gücü tanıdığı unsurlardan beslenmektedir (Elitaş, Aydemir, Elitaş, 2009, s. 38). Belge yönetiminde bu unsurlar, sabit bir form, değişmeyen içerik ve tanımlanabilir bir kontekst şeklinde belirlenmiştir (INTERPARES, 2008, s. 106). Söz konusu unsurlar korundukça belgelere duyulan güven de artacaktır. Çünkü güven, paylaşılan değerler arttıkça oluşmaktadır (Fukuyama, 2005, s. 26). Ortamı ne olursa olsun bu unsurlar korunduğu sürece belgeler güvenilir kabul edilir.

Kâğıt ortamdan gelen alışkanlıkla olsa gerek güvenilirlik konusunda ciddi çalışmaları bulunan Luciana Duranti, sadece belgenin ilk üretildiği halinin orijinal olduğunu ifade etmekte; elektronik ortamda belgenin orijinalinin bulunmadığını dile getirmektedir. Belgenin ilk temsilinden sonra kaydedilen versiyonlarının birer kopya olduğunu belirtmekte ve belgeleri güvenilir yapan unsurların korunamayacağını, bu unsurların yeniden oluşturulabileceğini ifade etmektedir (Duranti, 2009). Bu nedenle belgenin saklanan hali ve sunulan hali arasında bir ayrım yapılmaktadır. Belgenin saklanan hali, depolama sistemlerinde muhafaza edilen ve üzerinde işlem yapılabilen belgeleri; belgenin sunulan hali ise belgenin saklanan halinin işlenmiş ya da görselleştirilmiş bir şekilde kişilerin erişimine sunulan belgeleri ifade etmektedir. Belgelerin saklanan halini muhafaza etmenin temel nedeni belgenin sunulan halini aslına sadık kalarak yeniden oluşturabilmektir (INTERPARES, 2008, s. 120-121).

E-belgelerin sunulabilmesi için saklanan belgenin birtakım işlemlere tabi tutulması gerekir. Saklanan belge, belirlenen kurallar çerçevesinde sunulabilir hale getirilerek erişime açılır. Yani saklanan belge ile sunulan belge farklı özelliklere sahiptir. Sunulan belgenin, belge olarak değerlendirilebilmesi için belgenin ilk oluştuğu andan itibaren yeniden üretilebilmesi gereklidir. Saklanan belgelerle ilgili verilerin form verisi, içerik verisi, oluşma verisi ve kurallardan teşekkül ettiği anlaşılmaktadır. Bu veriler aracılığıyla saklanan belgeler tanımlanır ve sunulan belgeler oluşturulur (Duranti ve Thibodeau, 2006, s. 57-58).

E-belgelerin ait olduğu kurumsal fonksiyonu yansıtabilmesi ve prosedürlere uygun olarak üretilmesi güvenilirlik analizinin önemli adımlarındandır. Bu analiz için uluslararası düzeyde çeşitli projeler gerçekleştirilmiş ve güvenilirliğin unsurları araştırılmıştır. Belgelerin güvenilirlik analizi özgünlük, tamlık ve gerçeklik unsurları kapsamında yapılmaktadır (INTERPARES, 2008). Belgenin, belge olduğuna duyulan güven ve bozulma ya da tahrif olmaktan uzak bir şekilde özniteliklerinin korunması şeklinde ifade edilebilen özgünlük (Rogers, 2015, s. 35), tanımlanabilirlik ile bütünlük olmak üzere iki aşamada incelenmektedir. Tanımlama, belgenin karakteristik özelliklerini belirterek belgenin diğer belgelerden ayırt edilmesini sağlama olarak ifade edilebilir. Bu karakteristik özelliklere, belgedeki kişiler, üretim tarihi, iletim tarihi, konu, arşivsel bağ, dosya kodu ve belgenin ekleri örnek

verilebilir. Belgenin kimliğini oluşturan bu unsurlar belgenin iç ve dış kaynaklı elemanlarında ya da üstverilerde açık bir şekilde belirtilmiş olabilir veya belgenin kontekstinde örtük bilgi şeklinde yer alabilir (INTERPARES, 2002, s. 155-156).

Belgenin bütünlüğü ise belgenin tüm yönleriyle bozulmamış ve değiştirilmemiş olmasını ifade eder. Fakat bu durum, belgenin ilk üretildiği haliyle mevcut olması anlamına gelmemektedir. Kâğıt ortamında belgeler, zaman içerisinde ısı, nem, kâğıt yapısı gibi koşulların etkisiyle bozulabilmekteydi. Elektronik ortamda ise taşıyıcı ortamın kırılganlığı, teknolojik eskimeler ve sistemlerin kendine has özellikleri belgelerin bütünlüğünü olumsuz etkileyebilmektedir. Belgenin bit dizisi gibi fiziksel bütünlüğünü oluşturan unsurların zarar görmesi mümkündür. Fakat belgede verilmek istenen mesaj, gerekli olan açıklama notları ve dokümanter form elemanlarının değişmemesi gerekir. Belgenin bütünlüğü, üstveriler ve kontekstte yer alan bulgularla analiz edilebilir (INTERPARES, 2002, s. 156). Bununla birlikte, belgelerin bütünlüğü bozulduysa onun güvenilirliğinden bahsetmek de mümkün olmayacaktır.

Bütünlük anlayışı, tanımlanabilirlikle birlikte zaman içerisinde belgelerin özgünlüğünü tesis etmek ve değerlendirmek fikrinin temelini oluşturmuştur. Kâğıt belgeler döneminde, bütünlük kontrolü kayıt defterlerine girilen sayılar, belge içeriklerinin listelenmesi ve dosyalardaki belge sayıları dikkate alınarak yapılmaktaydı. Elektronik belgeler döneminde ise belgelerin oluştuğu ve muhafaza edildiği yapılar ile bilgi sistemlerinin güvenilir bir şekilde çalışması şeklinde genişleyen bir bütünlük anlayışı görülmektedir. Bu dönemde bütünlüğü sağlamak için erişim kontrolleri, kullanıcı onayı, denetim günlükleri, sistemin normal koşullarda çalıştığını gösteren dokümantasyonlar, mutat bakımlar ve sistem güncellemeleri gibi çeşitli araçlar kullanılmaktadır (Lemieux, 2017a, s. 43).

Bir belgenin özgünlüğünü ileri sürebilmek için muhteva ettiği hukuki işlemin gerçekleştiğinin kanıtlanması gerekir. Özgünlük, belgenin iletimi ve korunması aşamasındaki denetimler ile birlikte belge üretildikten, alındıktan veya dosyasına kaldırıldıktan sonra da değiştirilmediğini, müdahaleye uğramadığını veya sahteciliğe maruz kalmadığını gösteren yöntemlerin benimsenmesi aracılığıyla korunabilir. Kâğıt belgelerde belgenin ilk üretildiği formu ve üretilip dosyasına kaldırıldığındaki hali muhafaza edilirse belgelerin özgünlüğünün korunduğu ileri sürülebiliyordu. Fakat sayısal belgelerin kırılganlığı ile kullanılan donanım ve yazılımların hızlı bir şekilde bozulması, teknolojik dönüşüm ve belgelerin aslına sadık kalarak yeniden üretilme (reprodüksiyon) süreçlerinin otonom bir şekilde tasdik edilmesi aracılığıyla belgelerin kopyalanması ve göç ettirilmesini gerekli kılmıştır (Rogers, 2015, s. 35). Zaman içerisinde belgelerin bütünlüğünü korumanın sıklıkla sayısal korumanın (digital preservation) kapsamına girdiği görülmüştür.

Sayısal koruma dünyasında tek başına belgenin bit yapısının korunması bütünlüğün muhafazası için yeterli kabul edilmemektedir. Bit yapısı aracılığıyla e-belgedeki yetki veya haklar görünür olsa da belgenin semantik yapısında yaşanacak bir kayıp, belgenin okunabilirliği ve erişilebilirliğini olumsuz etkileyebilecektir. Mesela bir tapu kaydının bit akışı ve bu akışı okunabilir hale getiren yazılımlar kolayca korunabilir; fakat esas olarak bitlerin önemini ve mahiyetini anlamak için belgeyi okunabilir hale getiren kontekst bilgisinin korunması gereklidir. Kontekst bilgisinin korunmasıyla belge, yetki vermek veya bir hakkın varlığını ispat etmek gibi toplumdaki karşılığını kaybetmeyecektir.

Belgenin okunabilirliğine, dönüştürülebilirliğine ve etkisine zarar vermeyecek derecede yaşanan bit kayıpları göz ardı edilebilmektedir (Lemieux, 2017a, s. 43-44). Fakat bitler çok iyi korunsa da belgenin okunabilirliği ve toplumdaki karşılığı zarar görebilir. İşte bu durum, arşivcilik dünyasında belgenin üretildikten sonra da bütünlüğünün korunma gereksinimini oluşturmaktadır. Bu nedenle, elektronik belgelerin geleceğe aktarılması, kontekst, içerik ve belge bileşenlerinin muhafaza edilmesinin yanı sıra arşivsel bağın korunmasını da gerektirir. Bu bağ aracılığıyla belgeler tanımlanarak bütünlük koruma altına alınabilir (Lemieux, 2017a, s. 45).

Belgelerin güvenilirliğini korumak için gerekli olan diğer özellikler ise tamlık (accuracy) ve gerçekliktir (reliability). Tamlık arz eden bir belge, kesin, doğru, hakikate uygun ve tahrifattan uzak olmalıdır. Tamlık, belgelerin sürekli işlem gören yapısıyla ilişkili olup hukuki sonuç meydana getirebilmek için belgenin üreticisi ve idari-hukuki sistem tarafından ihtiyaç duyulan tüm elemanların varlığını ifade etmektedir. Bu yüzden tamlık, belgenin iç kaynaklı bir unsuru olup belgenin resmi şekliyle de ilgilidir. Belge, üretilme gerekçesi olan hukuki prosedüre ve görmesi gereken idari işlem türüne göre belge vasfı kazanır. Mesela, bir tapu devri sözleşmesi imza ve tarih içermezse tamamlanmış kabul edilemeyecektir (INTERPARES 2, 2008). Burada, imza ve tarihin yanı sıra tapu devir sözleşmesinin geçerliliği için işlemin yetkili bir otorite olan tapu müdürlüğünde yetkili memur nezaretinde yapılması gerekir.

Belge, hukuki prosedürler neticesinde oluşturulur ve hukuki bir işlem ihtiva eder. Bu hukuki işlemin de işlemi gerçekleştirmeye yetkili kişiler tarafından ortaya konulması gerekir. Bununla birlikte, belge ile içerdiği hukuki işlem arasında bir uyumluluk aranır. Mesela, tapu devri sözleşmesinde, sözleşmenin bu işlemi yapabilmek için yetkili kılınmış olan tapu müdürlüğündeki yetkili kişiler tarafından gerçekleştirilmiş olması gerekmektedir. Bursa'daki tapu işlemleriyle yetkili bir müdürlüğün İstanbul'daki tapu işlemleriyle ilgili bir tasarrufu söz konusu olamayacaktır. Ayrıca, tapu devir işlemlerini gerçekleştirmekle yetkili kılınmamış kişilerin bu işlemlerde imzasının bulunması belgenin gerçekliğinden şüpheye düşülmesine neden olacaktır (INTERPARES 2, 2008). Gerçeklik, belge formunun tamlığına ve belgenin

üretim prosedürlerindeki kontrol düzeyine ait bilgiye dayanarak değerlendirilmektedir. Bu kontroller, belgenin üretimi ve alımı, dosyasına kaldırılması ve belgedeki kişilerin yetkilerini içermektedir. Ne kadar katı ve ayrıntılı kurallar konulup bu kurallar rutinleştirilirse belgenin gerçekliği o derece güçlenecektir (Rogers, 2015, s. 34-35). Belge formunun tamlığı ise belgeyi hukuki bir sonuç doğurmaya elverişli hale getirecek entelektüel formun tüm elemanlarının mevcut olmasını ifade etmektedir. Belge formu ve üretim prosedürleri aracılığıyla belgenin üreticisinin sorumluluğu ve üretiminde rol alan kişiler de incelenir. Bu nedenle, gerçeklik analizinde imza ve tarihin oldukça önemli bir yeri vardır. Tarih, belgeyi sorumlusuyla ilişkilendirip belgedeki irade beyanının zamanını ortaya koymakta; imza ise belgenin içeriğine hukuki bir sonuç katarak belgeyi irade beyanının kimlik tespitine elverişli hale getirmektedir. (Rogers, 2015, s. 34-35). Bu nedenle, belgedeki kişi ile imzanın uyumlu olması gerekmektedir. Aynı zamanda belgeyi düzenleyen onu düzenleme yetkisine sahip olmalıdır (Çiçek, 2009, s. 97-98).

Özgünlük, belgenin üretim prosedürlerinin tamamlanmasından sonra tahrif edilmediğini, değiştirilmediğini ve özniteliklerini korunduğunu göstermektedir. Belgenin gerçekliği, onun üretim safhasındaki koşullarına bağlıyken, özgünlüğü onun korunmasıyla ilgili şartlara bağlıdır. Güvenilir bir belge ise hem özgün hem de gerçek olmalıdır (Hofman ve diğerleri, 2018, s. 1653).

Kurumsal belgeler, bir işlemin sonucunda oluşarak bir faaliyete kaynaklık eder ve sonradan başvurulmak üzere dosyasına kaldırılır. Çünkü belgenin hangi faaliyetle ilişkili olduğu, kim tarafından saklandığı ve aynı faaliyet sonucunda oluşan diğer belgelerle arasında sınırları belirli bir ilişki söz konusudur. Bu ilişki arşivsel bağ olarak adlandırılmaktadır. Arşivsel bağ, bir kontekst bağlamında belgenin sadece üretilme ve kullanılma durumuyla ilişkili olmayıp dosya, seri ve fon gibi ait olduğu kümeyi de tanımlamaktadır. Bu bağı incelemeden bir belgenin sahih mi yoksa sahte mi olduğunu iddia etmek oldukça zordur. Bu inceleme için belgenin provenansı analiz edilir. Bu analizde, bir faaliyetin sonucunda oluşan belgelerle, bu belgelerin üreticisi, muhafaza edeni ve arasındaki ilişki sorgulanır (Çiçek, 2011; Çiçek ve Sağlık, 2017).

Arşivsel bağı güçlendirmek için geliştirilecek prosedürler, gerçeklik ve özgünlüğü ciddi bir şekilde korumaktadır. Bu prosedürlerin ilki belge yönetim sisteminin devreye alınmasıdır. Belge yönetimi sürecinde güncel belgelerle, arşivlenmiş belgelere yapılacak muameleler birbirinden ayrılmıştır. Belgeyi üretenler, belgeye ihtiyaç duyulduğu sürece onun gerçekliği ve özgünlüğünü sağlamakla görevliyken; arşivciler belgenin özgünlüğünü zaman içerisinde muhafaza etmekle yükümlüdür. Gerçeklik, belgenin üreticisinin belgedeki kişiler üzerindeki kontrolü, belgenin üretim süreci ve belge formunun

tanımlanmasıyla ilgili prosedürel ve teknolojik denetimlerle korunabilir. Özgünlük ise belgenin doğru kontekstine yerleştirilmesi, başarılı bir şekilde iletilip muhafaza edilmesi, arşive devredildiğinde güvenilir bir üçüncü tarafa devredilmesi ile arşivsel tanımlama aracılığıyla entelektüel kontrolü sağlayan prosedürel ve teknolojik yöntemler aracılığıyla gösterilir (Rogers, 2015, s. 36-37).

Belgenin üretimi, kullanımı, teknolojik göçü, korunması ve erişimi sırasında değişmediğini gösterecek unsurlar özgünlüğün yapısını oluşturmaktadır. O halde, özgünlüğü değerlendirebilmek için gerekli olan unsurlar neler olabilir sorusu hâlâ geçerlidir. Özgünlük, belgenin zaman içerisinde bozulmadığına dair karine öne sürülerek gösterilir. Eğer belgenin özgünlüğünden şüpheye düşülürse, tanık, bilirkişi veya belgenin üretim ve koruma koşulları değerlendirilmektedir (Rogers, 2015, s. 54-56).

Kâğıt belgelerde düzenleyen, mesajı fiziksel bir taşıyıcıya bir kalem ya da başka bir araçla doğrudan yazar ve imzalardı. Belge, ortamı değişmediği için özgün olarak kabul edilirdi. Belgenin özgünlüğünden şüpheye düşüldüğünde ise tanık dinlenir veya belirlenen kurallar dâhilinde fiziksel inceleme yapılırdı. Bu kurallar, kâğıt belgeler için oldukça iyi işlemekteydi. Fakat bilgi çağına geldiğimizde bilginin karmaşıklığı belgelerin değerlendirilmesinde geçerli olan kuralları da etkilemiş; pek çok ülkede özgünlük krizi ile karşı karşıya kalınmıştır. Bunun için hukuk düzenleri yeni yöntemleri benimsemek zorunda kalmıştır. Bu yöntemler yazılımlar, üstveriler, log kayıtları gibi hususların incelenmesi olarak öne çıkmaktadır. Peki, üretilen sayısal delillerin geçerliliği nasıl gösterilecek, sürekli gelişen teknolojide malzemelerin kimliği ve bütünlüğü nasıl değerlendirilecektir (Rogers, 2015, s. 57-59). Acaba, blokzincir teknolojisi bu soruna bir çözüm getirebilir mi sorusu akla gelmektedir.

4. Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğini Korumadaki Rolü

Blokzincir teknolojisinin elektronik belge yönetimindeki kullanımı üzerine ciddi çalışmaları olan Victoria Lemieux, blokzincir teknolojisinin kullanıldığı belge yönetimi sistemlerini üç türde sınıflamaktadır. Bunlar, ayna (mirror), sayısal belge (digital record) ve aidiyet (tokenized) blokzincirleri şeklinde ifade edilebilir (Lemieux, 2017, s. 2273). Ayna türü blokzincirlerde, belgeler sayısal ya da fiziki olarak mevcut olmakla birlikte, bloklar bu belgelerin iz değerlerinden oluşmaktadır. Bu türde, belgeler blokzincirlerde üretilmemektedir. Bloklar, asıl belgelerin kriptografik yansımalarından meydana gelmektedir. Bu nedenle Lemiux, bu türü ayna olarak nitelendirmiştir. Buradaki temel amaç, belgelerin hesaplanan iz değeriyle, blokzincirlere yüklenen iz değerlerinin karşılaştırılarak bütünlüğün korunup

korunmadığını incelemektir. Eğer iz değerleri örtüşmezse, belgenin bir değişikliğe uğramış olabileceği düşünülecektir (Lemieux, 2017).

Bununla birlikte, benzer bir sistem belge yönetimindeki başarılı faaliyetleriyle bilinen Estonya'da da görülmektedir. Bu ülkede, sağlıkla ilgili belgeler, hasta verileri, hastalarla belgeler arasındaki ilişkiler ile tüm kayıtlar ve verilerin denetim günlükleri bir veri tabanına yüklenmektedir. Belgeler, eXtended Markup Language (XML) formatında saklanmakta ve e-imza ile imzalanarak sistemdeki iz değeri ağacında muhafaza edilmektedir. Yeni oluşturulan belgeler ve denetim günlüklerinin de iz değeri oluşturulup iz değeri ağacına eklenmektedir. Tüm hareketler kayıt altına alınıp düz metin olarak Structured Query Language (SQL) formatında kaydedilmekte ve tek bir log kaydı olarak sistemden dışarıya aktarılmaktadır. Her iş günü yaklaşık 40 bin doküman üretilmekte ve değiştirme, ekleme gibi yaklaşık 1 milyon işlem gerçekleşmektedir (Lemiuex, 2017).

Sistemden dışarı aktarılan log kaydının da iz değeri oluşturulur. Bu iz değeri sistem içerisindeki iz değeri ağacına eklenir. Bir iz değeri ağacı, 1000 iz değerini kapsamaktadır. İz değerinin en tepesi bir dakikalık aralıklarla blokzincir ağına yüklenir. Böylece, üretimden hemen sonra üçüncü tarafların da kayıtları onaylaması mümkün hale gelir. Bu yöntemde belgelerin blokzincir ağında arşivlendiği iddia edilse de, belgelerin orijinali blokzincirlerde üretilip muhafaza edilmediği için bu iddianın gerçeği pek yansıtmadığı söylenmektedir. Bir sayısal koruma teorisine göre, belgelerin bulunduğu bir düğümde sorun oluşursa, iz değerlerinin kopyası başka bir düğümde de mevcut olmalıdır. Sistem, pratikte kayıt defterlerinin tüm kopyasının bütün ya da yeterli sayıda düğümlerde bulunması esasına dayanmaktadır. Eğer geriye tek bir düğüm sağlam kalırsa bu düğümün bütünlüğüne zarar gelip gelmediğini incelemek pek mümkün olmayacaktır (Lemieux, 2017).

İngiliz Milli Arşivi de blokzincir teknolojisinin arşivlerde kullanımı yönünde ARCHANGEL adında bir proje yürütmektedir. Bu projeyi de ayna türü blokzincirler arasında sınıflandırmak mümkündür. ARCHANGEL'in diğer örneklerden farklı bir özelliği dikkat çekmektedir. Bir belge dağıtık deftere yüklenirken o belgenin iz değeriyle birlikte, ileride yapılacak bir sorgulamada belge oluşturulduğundaki iz değerini yeniden üretmek için gerekli olan kodun iz değeri muhafaza edilir. Belge, sisteme yüklendiği gibi elektronik imzaya dair iz değeri dağıtık defterlere kaydedilmektedir. Bu iz değerinin ilerleyen zamanlarda da değişmediğinin gösterilmesiyle özgünlüğün ve belgelerin tahrif edilmediğinin gösterilebileceği ifade edilmektedir (Collomosse ve diğerleri, 2018). Bu husus, belgelerin içeriğinin değişmediğinin göstergesi olarak kabul edilebilir ve özgünlüğün bir şartı olan bütünlüğün sağlandığı ileri sürülebilir. Tanımlamanın arşivsel bağın kurulup gösterilmesiyle gerçekleştiği göz önüne alındığında, ARCHANGEL Projesinde arşivsel bağa

ilişkin bir yaklaşım görülememektedir. Bu nedenle, belgenin özgünlüğünün yeteri kadar sağlıklı korunduğunu ifade etmek pek mümkün görünmemektedir.

Belgenin sisteme yüklenmesiyle birlikte format tanımlama aracı, belgenin türünü (Portable Document Format [PDF], WORD gibi) belirler. Burada belge dosyasının adı gibi format tanımlama aracının sağladığı üstveriler de kullanılır. Belgedeki imza, iz değeri algoritmasıyla birlikte belgeden ayrı olarak da blokzincirlerde saklanır. Kullanılan iz değeri algoritmalarının geliştirilebileceğinin ifade edilmesi dikkat çekmektedir. İmza, dosya adı ya da tek biçim tanımlayıcı, içeriğin iz değeri, arşivcinin notu, yükleme tarihi, versiyon bilgisi gibi üstverilerle birlikte blokzincirlere kaydedilir. Bu veriler son blokla ilişki kurularak blokzincirde saklanır (Collomosse ve diğerleri, 2018).

ARCHANGEL'de Etherium dağıtık defter yapısının benimsendiği görülmektedir. Gerçekleştirilen işlemlerin onaylanması için ağdaki düğümlerin bir kriptografik bulmacayı çözmesi gerekmektedir. Çünkü ağdaki diğer düğümlerin işlemlerin onayı için bir mutabakata varması beklenir. Sistemin farklı arşivlerin sürece dâhil olduğu ve emeğin ispatı şeklinde çalışan özel düğümlerle korunabileceği ifade edilmektedir. Eğer kamuya açık bir yapı kullanılacaksa akıllı sözleşmelerin tercih edilmesi önerilmektedir. ARCHANGEL Projesinin şu an için eksik yanları olsa da, blokzincir teknolojisinin arşivcilerin iş pratiklerini değiştireceği öngörülmektedir (Collomosse ve diğerleri, 2018).

Bununla birlikte, İngiliz Milli Arşivlerinin video kayıtları üzerine yaptığı bir çalışma dikkat çekmektedir. Anayasa Mahkemesindeki duruşma görüntüleri için kullanılabileceği belirtilen bu uygulamada video kayıtlarının bütünlüğü blokzincir teknolojisi kullanarak korunmaktadır. Burada, daha çok videoların tahrif edilmemesi ve kimden neşet ettiğine dair bilginin korunmasına yönelik bir yaklaşım sergilendiği görülmektedir (Bui ve diğerleri, 2019). Söz konusu kayıtların bütünlüğü ve gerçekliğinin korunduğu dile getirilebilir. Video kayıtlarıyla ilgili uygulamada akıllı sözleşmeler de kullanıldığı için, bu uygulamayı ayna ve sayısal belge türü blokzincirler içerisinde sınıflamak mümkündür.

Sayısal belge türünde ise belgeler akıllı sözleşmeler olarak zincirlerde üretilmektedir. Bu tür, geleneksel sayısal belge üretiminden farklılık arz etmektedir. Geleneksel yöntemlerde, belgeler merkezi bir veritabanında ya da bulut tabanlı platformlarda üretilirken, blokzincirde merkezilik yerine dağıtık bir yapı benimsenmektedir. İsveç'teki tapu kayıtları örneğinde bu blokzincir türü görülmektedir (Lemiuex, 2017, s. 2274). Bir tapu satışı söz konusu olduğunda, satıcı, ilanını sistemde paylaşır; alıcı bu ilana teklif verir. Alıcı ile mutabakata vardıktan sonra banka, satıcının yeterli bakiyesi olup olmadığını kontrol eder. Yeterli bakiye varsa miktarı alıcıya iletir ve tapu müdürlüğü de

bu satışı onaylar. Sayısal belge türündeki blokzincirde geleneksel belge yönetiminde pek görmediğimiz akıllı sözleşmelerin tamamlanmasıyla süreç sona ermektedir (Lemiuex, 2017, s. 2274). Burada, bu tipe sayısal belge türü dense de akıllı sözleşmeler türü olarak adlandırmanın daha gerçekçi olacağı düşünülmektedir.

Bu noktada akıllı sözleşmelerin geçerliliğinin henüz delil hukuku tarafından kabul edilmemiş olması, geçerlilikleri hakkında yeteri kadar inceleme yapılmaması gibi sorunlar dikkat çekmektedir. Bununla birlikte, akıllı sözleşmelerde neyin belge olarak değerlendirileceği de sorgulanmaktadır. Çünkü bu akıllı sözleşmelerde işlem bittikten sonraki süreç derleme kodlarına yazılmaktadır. İşlem yapmak isteyen tarafın iradesinin çeşitli aracılarla sunumu mu, betik (script) mi yoksa derlenmiş kodların mı belge olarak kabul edileceği yönünde bir belirsizlik görülmektedir (Lemiuex, 2017, s. 2275). Bununla birlikte, Ethereum protokolü üzerinde tanımlı 19.366 akıllı sözleşmeden 8.833 tanesinde, sözleşmenin yönlendirilmesi sonucunda kazanç elde edilebilecek güvenlik açıklarının olduğu tespit edilmiştir (Luu, Chu, Olickel, Saxena ve Hobor, 2016, s. 255). Öyle anlaşılıyor ki, akıllı sözleşmelerin belge yönetimindeki uygulaması için daha çok pratik yapmak gerekecektir.

Bir diğer uygulama olan aidiyet türü blokzincir uygulamasında ise yeni bir arşivcilik paradigmasının geliştirildiği görülmektedir. Lemieux, bu tür için "tokenized" ifadesini kullanmaktadır. Türkçe karşılık olarak jeton anlamına gelen bu ifadenin meselenin mahiyetini tam olarak karşılayamadığı düşünülmektedir. Bu nedenle, herhangi bir varlığın blokzincir ağındaki aidiyeti söz konusu olduğu için bu uygulamanın aidiyet türü blokzincir olarak adlandırılmasının daha uygun olacağı kanaatine varılmıştır. Sistemde sadece belgeler değil, varlıklar da kripto paralarla ilişkilendirilerek zincirlerde temsil edilmekte ve saklanmaktadır. Bu varlıklar araziler, içecekler, pırlantalar, sanat eserleri gibi pek çok şey olabilir (Lemiuex, 2017, s. 2275).

Belge tanımının kapsamı gelişen teknolojiyle birlikte değişmektedir. Blokzincir teknolojisiyle birlikte, ev, para, kalem gibi akla gelebilecek tüm malzemeler sadece bir madde gibi değerlendirilmemiş; sanal bir aidiyet haline dönüştürülmüştür. Bu aidiyetlerle ilgili yapılan işlemler blokzincir teknolojisinde tek bir kayıtta toplanmış ve söz konusu malzemeler bir belge haline gelmiştir. Bu durumun pek de yeni olmadığı düşünülmektedir. Arşiv biliminin teorisyenlerinden Hilary Jenkinson, sergilenen ürünler gibi gelecekte başvuru kaynağı olarak kullanılmak üzere arşive kaldırılan ve resmi işlemlerin bir parçası olan fakat yazılılık içermeyen nesnelerden söz etmektedir. Apoletler, bir mektubun ekinde gönderilen hediyeler, portreler, insan saçları, kırbaçlar, üzerine nefret söylemleri kazılan madeni paralar, kanser tedavisi için gönderilmiş tozlar vb. de bir arşivin parçası

olabilmektedir. Arşivcilerin, yazılı kayıtları muhafaza etmeden önce sembolik objeleri koruma altına aldığı bilinmektedir. Bu duruma hükümdarlığın ya da adaletin sembolü olarak kılıçlar ve miğferlerin saklanması örnek verilebilir. Bununla birlikte, tarafların kendilerini bir bölgenin lideri olduğunu göstermek amacıyla 12. yüzyılda birbirlerine bıçaklar hediye ettiği bilinmektedir. Ayrıca bir arazinin belirli bir kişiye ait olduğunu belirtmek için kişiye ait bir sembolün (bıçak, bardak vb. gibi) kullanıldığı belirtilmektedir (Lemieux, 2017).

Brezilya'daki tapu kayıtlarının yönetiminde bu tür bir blokzincir uygulaması görülmektedir. Burada araziler bir varlık olarak değerlendirilmektedir. Bu varlıklar ve bunlarla ilgili işlemleri içeren arazi devirleri blokzincir ağına kaydedilmektedir. Araziler, bloklarda bir jetona dönüştürülmüş ve bu jetonların alım-satımı kripto paralarla gerçekleştirilmektedir (Lemiuex, 2017, s. 2275-2276). Fakat yetkililer, sistemi pahalı bulmuş ve bu uygulamayı mevcut belgelerin yarısını dikkate alarak gerçekleştirmiştir (Flores, Lacombe ve Lemieux, 2018, s. 10).

Blokzincir teknolojisinde de e-imzalar önemli bir rol oynamaktadır. Pek çok ülkedeki e-imza uygulamalarında, e-imzaların sertifika geçerlilik süreleri vardır ve bu geçerlilik süreleri belge arşive devredildikten sonra son bulabilir. Bu süre sonunda belgenin tekrar imzalanması gerekmektedir. Bu sürecin sonunda belgenin koruma zincirinin kesintiye uğraması ihtimali vardır. Blokzincir teknolojisinde ise bir sertifikalandırma otoritesine ihtiyaç duyulmamakta, özel ve açık anahtarlar sistem içerisinde kendiliğinden oluşmaktadır (Lemieux, 2016a). Fakat, sertifikalandırma otoritesi kullanarak e-belgeleri blokzincirlerde oluşturan uygulamalar da görülmektedir (Galiev ve diğerleri, 2019). Tataristan Cumhuriyeti'ndeki bu uygulamada arşive devredilen e-belgelerin iz değerleri ve zaman damgaları oluşturularak blokzincir ağında saklanmaktadır. Böylece, belgeler kriptografik olarak koruma altına alınmakta ve belgelerin özgünlüğü muhafaza edilmektedir (Galiev ve diğerleri, 2019, s. 87). Bu örnekte bir sayısal koruma projesi olarak blokzincir teknolojisinin kullanıldığı görülmektedir (Lemiuex, 2017, s. 2277). Lemieux, belge yönetimindeki blokzincir uygulamalarını üç türde derlemişti; sayısal koruma projesi olarak blokzincir uygulamasının dördüncü bir tür olarak değerlendirilebileceği düşünülmektedir.

Belgelerin bütünlüğünün korunması blokzincir teknolojisinin en önemli faydalarından biri olarak kabul edilmektedir. Blokların zamana göre oluşturulması, işlemlerin kriptografik araçlarla doğrulanması ve dağıtık mimari, belgelerin bozulmadan uzak olması yönünde ciddi kazanımlar sağlamaktadır (Lemiuex, 2017a, s. 10). Bununla birlikte, blokzincir, belgelerin gereksiz yere çoğaltılmasını engellemekte ve hangi belge sahihtir

sorununu ortadan kaldırmaktadır. Çünkü, sistemde yapılan tüm işlemler aynı belge üzerinde gerçekleşmektedir (Berryhill ve diğerleri, 2018, s. 14).

Belgelerin güvenilirlik unsurlarından biri olan tamlığa ilişkin yaklaşımlar da blokzincir uygulamalarında görülmektedir. Tamlık, veri üzerindeki teknik ve prosedürel denetimlere bağlıdır. Sistem kontrolleri ve denetim günlükleri ile tamlığı artırmak mümkündür. Blokzincir teknolojisi sayesinde daha güçlü bir kalite kontrolünün gerçekleşebileceği öngörülmektedir. Mesela, Brezilya'daki uygulamada, kâğıt ortamında olup elektroniğe aktarılan tapu kaydının iz değeri oluşturularak bu kayıt blokzincirdeki kaydın iz değeriyle karşılaştırılır. İz değerlerinin örtüşmesiyle de blokzincire eklenen kayıtların tamlığı denetlenir. Bu denetleme işleminin yapıldığına dair bir üstveri, blokzincirdeki belgeye eklenebilir (Flores ve diğerleri, 2018, s. 18-19).

Tüm bunlara karşın blokzincir teknolojisinin e-belgelerin tamlığına zarar verebilme ihtimali de söz konusudur. Bir blokzincir ağında, her blok, çeşitli işlemlere ait iz değeri ve diğer bilgilerle birlikte bloğun belirli bir tarihten önce oluştuğunu gösteren zaman damgasını içerir. Bazı sistemlerde, bloklardaki zaman damgaları, işlemlerin kronolojik sırasının ispatı için kullanılan jetonların üretimini düzenlemesini de mümkün kılmaktadır. Düğümler, düğüm uçlarının yaptığı işlemlerdeki ortalama zamana göre zaman damgasında yer alan tarih ve saat bilgilerini hesaplayabilmektedir. Blokzincir teknolojisinin sağlıklı çalışabilmesi ve zaman damgası hatalarının önlenmesi için tüm düğümlerin önceki işlemlerin zamanını da muhafaza etmesi gerekir. Aksi takdirde zaman damgası doğru tarihi göstermeyebilir. Düğümlerin normal koşullarda çalıştığı durumlarda bile düğümlerdeki ağ zamanı yavaşlatılabilir veya hızlandırılabilir. Bu durumda, zaman damgasının sağlıklı sonuçlar vermeyeceği düşünülmektedir. Bununla birlikte, izin gerektiren blokzincir ağlarında tek bir düğümün kontrolü ele alması muhtemeldir. Bu tür durumlarda bloklardaki hatalı veya istenmeyen işlemlerin düzeltilmesi söz konusu olsa da, mezkûr hatalı işlem geçersiz olacağından onun hatasını düzelten işlem de geçersiz olacaktır (Lemieux, 2017a, s. 46). Bu sorunun aynı faaliyet ya da işlem kapsamında oluşan belgelere arşivsel bağ ile ilgili bilgilerin eklenmesiyle çözülebileceği ifade edilse de mevcut blokzincir uygulamalarının bu konuda yetersiz kaldığı belirtilmektedir (Lemiuex, 2017a, s. 47).

Belgelerin güvenilirliği için gerekli olan unsurlardan biri de kontekstir. Blokzincir uygulamalarında, iz değeri oluşturulan belgelerin ait olduğu kontekstle ilişkilendirilmesine yönelik girişimlerin mevcut olduğu görülmektedir. Bunun için her bir iz değerine tekil bir numara verilerek denetim günlükleri aracılığıyla belgenin ait olduğu kaynak gösterilmektedir. Burada bir yan zincir oluşturulmakta ve dağıtık defterdeki belgelerin arşivsel bağı da bu zincirle birlikte hareket etmektedir. Bir diğer yöntem ise aynı işlem ya da faaliyet sonucu oluşan belgelerin iz değerini bir üst belgede toplayarak

tekrardan bu belgenin iz değerini oluşturmaktır. Bu yöntemde oluşan üst belgenin iz değeri, yapılan işlemlerin yer aldığı belgelerin iz değerlerini elediği için daha önce yapılan işlemlerin kimliği kaybolmuş olacaktır. Bu durumda üst belgeyi oluşturan belgeler ve bu belgelerin iz değerleri de ortadan kaybolmaktadır (Lemiuex, 2017a, s. 9).

Bununla birlikte, vaka dosyalarını oluşturan belgelerin durumu merak konusudur. Bu durumda, vaka dosyasındaki belgeleri blokzincir ağına eklerken gerçekleştirilen işlemler sonucunda oluşan belgelerin iz değerini hesaplayıp faaliyetin tamamlanmasını beklemenin verimli bir çözümü gündeme getirmeyeceği ifade edilmektedir. Çünkü bir faaliyetin tamamlanması aylar hatta yıllar sürebilir. Bu sorunu çözmek için bazı kripto para uygulamalarında görülen OP_Return fonksiyonunun işlemler arasındaki arşivsel bağı kurabileceği ifade edilmektedir. OP_Return betik kodunun işlemlere ait üstverileri belirlemede kullanılabileceği söylenmektedir. Fakat OP_Return kodu, kripto para işlemlerinin bir parçası olmadığı için doğrulamak noktasında sorunlar çıkabilmektedir. Ayrıca, arşivsel bağ, belgenin ait olduğu kontekstle ilişkilendirilen ve belgenin tanımlanması için kullanılan ontolojiler aracılığıyla da kurulabilmektedir. Ontolojilerin ayrı bir semantik etiket olarak bloklara eklenebileceği belirtilmektedir. Ontolojilere yapılacak referansların, gerçekleştirilen işlemlere ait verilerle birlikte iz değeri hesaplanıp bu bilgiler zincirlerde saklanabilir (Lemiuex, 2017a, s. 9).

Arşivsel bağın blokzincirlerde kurulmasının önemli bir önkoşulu kayıt defterlerindeki belgelerin önceden tanımlanmasıdır. Bunun için her işlem tek bir iz değeri ile ilişkilendirilir. Diğer taraftan, mantıksal olarak kayıt defterleriyle ilişkili olan fakat bloklarda tutulmayan belgeler için bunun nasıl yapılacağı merak edilmektedir. Blokzincirlerde tutulmayan belgelere de bir iz değeri verilmekte ve bu iz değerine bloklarda bağlantı yapılmaktadır. Sağlık kayıtlarının onamı örneğinde, bir onam cüzdanı kullanılmaktadır. Kişilerin verdiği tüm onamların görülebildiği bu cüzdanın arşivsel bağın korunması için de değerlendirilebileceği düşünülmektedir (Hofman ve diğerleri, 2018, s. 1654-1655).

Özgünlüğün bileşenleri, bütünlük ve tanımlama ile gösterilir. Tanımlama, belgenin sorumlusunun kimliklendirilmesi ve arşivsel bağın kurulması ile gerçekleşir. Bütünlük ise belgenin üretiminden sonra da eksiksizliğini muhafaza etmesidir. Belgenin sorumlusunun gerçekliği imzalar aracılığıyla gösterilir. Bu nedenle imza özgünlüğün gösterilmesinde en önemli araçlardan biridir. Blokzincirlerde belgenin sorumlusu belgeyi özel anahtarıyla imzaladıktan sonra bu imza inkâr edilememelidir. Mevcut blokzincir uygulamalarında açık anahtar alt yapısının ve role dayalı kontrollerin uygulandığı görülmektedir. Bununla birlikte, erişim kontrolleri de yetkisi olmayan kişinin bir belgeyi imzalayabilme ihtimalinin önüne geçebilmek için kullanılan bir yöntem olarak karşımıza çıkmaktadır (Hofman ve diğerleri, 2018, s. 1653).

Estonya'daki uygulamada görülen Merkle ağaç yapısından e-belgelerin güvenilirliğinin başarılı bir şekilde korunması noktasında ciddi olarak faydalanılabileceği düşünülmektedir. Merkle ağaç yapısında en alttaki verilerden yukarıya doğru bir özetleme değeri üretilerek tüm yapı için bir özetleme değeri oluşturulabilir (Usta ve Doğantekin, 2018, s. 114). İşlem-faaliyet-fonksiyon hiyerarşisi içerisinde belge-dosya-seri ve birim yapısını ele alalım. Her belge için bir özetleme değeri oluşturulup, belgelerin ait olduğu dosya için de bir özetleme yapısı meydana getirilir. Dosyaların ait olduğu seriler için de tek bir özetleme yapısı tesis edilebilir ve bu seriler de birimler çatısı altında birleştirilip bir özetleme değerine sahip olur. Bu birimler yine birleşerek kurumu oluşturur ve kuruma bir özetleme değeri tevdi edilir. Merkle ağaç yapısına arşivsel bağla ilgili ontolojilerin semantik bir etiket olarak eklenmesi kontekstin korunmasını mümkün kılabilir.

Sağlık verilerinin onamına dair belgelerin blokzincir teknolojisi kullanılarak paylaşılması ve saklanılmasına dair prototip geliştiren bir çalışma dikkat çekmektedir. Bu çalışmada, hatalı bilgiler içeren belgelerin düzeltilmesi meselesinin nasıl gerçekleşeceği sorgulanmış ve arşivsel bağ tesis edilirse bağlantılar kurularak doğru bilgi içeren belgenin sisteme eklenebileceği belirtilmiştir. Bir elektronik mesajın bileşenleri önceden belirlenmemiş ve üretim prosedürleri kontrol edilmemişse elektronik olarak mühürlenmiş ya da zaman damgası almış olsa dahi mesajın gerçek olamayacağı ifade edilmektedir (Hofman ve diğerleri, 2018, s. 1652). O halde, blokzincir teknolojisi kullanılarak elektronik belgelerin güvenilirliğinin başarılı bir şekilde korunması için arşivcilik ve belge yönetimi ilkelerinin benimsenmesi gerektiği anlaşılmaktadır.

5. Değerlendirme

Arşivler, Roma Hukuku'na göre senetlerin bozulmadan korunduğu, güvenilir delillerin sağlandığı ve bir hafıza merkezi olan kamusal alanlar olarak kabul edilmektedir. Arşivlerin, başka bir ortamda üretilmiş belgelerin delil teşkil etmesi ya da gelecek kuşaklara bir miras olması amacıyla özgünlüklerini muhafaza etmek gibi sadece kendisinin sahip olduğu bir rolü bulunmaktadır. Bu nedenle asırlardır teoriler, metodolojiler ve uygulamalar geliştirilmekte ve arşivlerin kendisine devredilen belgelerin özgün olduğunu beyan etmekten ziyade, zaman içerisinde belgelerin özgünlüğünü garanti edecek uygun metodolojileri kullanmak gibi bir görevi ön plana çıkmıştır. Bunun için arşivlerin şeffaflık, güvenlik ve dayanıklılık gibi üç temel kriteri karşılaması gerekmektedir. Şeffaflık, sürece güvenilir üçüncü tarafların katılımıyla, güvenlik belgelerin bilerek veya bilmeyerek değiştirilmemesiyle, dayanıklılık ise belgelerin kontekstinin tanımlanıp yansıtılmasıyla sağlanmaktadır (Guo, Fang, Pan ve Li, 2016, s. 171-172). Bu çalışmada, söz konusu üç kriterin

blokzincir teknolojisi kullanılarak sağlıklı bir şekilde sağlanıp sağlanamayacağı incelenmiş ve mevcut örnekler kapsamında değerlendirildiğinde blokzincir teknolojisinin arşivcilik ve belge yönetimi disiplinlerinin bakış açısıyla yeteri kadar yorumlanmadığı görülmüştür. Bu nedenle, geliştirilmesi gereken yönleri olduğu öne çıkmıştır. Bu yönler aşağıda ifade edilmektedir.

Türkiye'de blokzincir konusunda önemli girişimleri olan ProofStack'in kurucusu ve Avrasya Blockchain ve Dijital Para Araştırmaları Derneği Yönetim Kurulu üyesi Kadir Kurtuluş, belge yönetimi için geliştirilecek blokzincirlerin Bitcoin, Ethereum, Ripple gibi protokollere bağımlı olmaması gerektiğini dile getirmektedir. Bu protokollerde oluşacak sorunların belgeleri de olumsuz etkileyeceğini ifade etmektedir (Kurtuluş ile yapılan görüşme, 2019). Bu nedenle, mevcut teşvik sistemleri ve alınıp satılabilir protokollere dayanarak geliştirilecek blokzincir teknolojisinin belge yönetiminde yeteri kadar sağlıklı işletilemeyeceği düşünülmektedir. Ekonomik Kalkınma ve İşbirliği Örgütünün (Organisation for Economic Co-operation and Development [OECD]) toplu taşımada blokzincir teknolojisinin kullanımına dair hazırladığı raporda da devletlerin kendi protokollerini hazırlaması önerilmektedir (OECD, 2018, s. 9). Bununla birlikte, mevcut blokzincir sistemlerinde, sistemin devamlılığı için taraflara çeşitli teşvikler verildiği bilinmektedir. Teşviğe dayalı bir sistemin de blokzincirin başarısına olumsuz etki edebileceği ifade edilmektedir (Lemiuex, 2017, s. 2273-2274).

Dağıtık, merkezi olmayan büyük ölçekli bir mimaride, bağlı her bir makinedeki blok yapısının her zaman tutarlı olması beklenemez. Sistem içerisinde yakın zamanlı paralel blok üretimi, blokların ağ üzerindeki makinelere farklı zamanlarda iletilmesi gibi nedenlerden dolayı, ağa bağlı makineler üzerinde farklı blok sıralamasına sahip düğümlerin bulunması karşılaşılan bir durumdur. Bu durumu çözebilmek için makineler her zaman "en uzun blokzincir kaydı geçerlidir" mantığı ile hareket edip bu kaydı genişletmek amacı ile işlem yaparlar. Bir makineye yeni bir blok aday olarak iletildiğinde, öncelikle bloğun içeriği incelenerek geçerlilik kontrolü yapılır. Sonrasında ise blokun bağlı olduğu üst blok bulunarak blokzincir ağına eklenir. Bu durumda üç farklı davranış şekli söz konusudur: Gelen blok, en uzun blok yapısının sonuna eklenir. Burada bloğun ilişkili olduğu üst blok, geçerli en uzun blokzincir kaydının son bloğudur. Gelen blok yapısının bağlı olduğu üst blok, en uzun blokzincir kaydı yapısında sonuncu blok değilse ana blokzincir yapısı üzerinde çatallaşma (fork) oluşur ve bu dallara "ikincil zincir" (secondary chain) adı verilir (Usta ve Doğantekin, 2018, s. 126).

Bir ikincil zincir, o an olmasa da zamanla "en uzun zincir" özelliğine sahip olabilir. Bu durumda kendisi ana blokzincire dönüşürken, o esnada geçerli olan ana blokzincirin artık bir ikincil zincir olarak değerlendirilmesi mümkündür. Bununla birlikte, gelen bloklar bilinen bir zincir yapısında ise bu

blokların bağlı olduğu üst blok bulunmaz ve bu durumda söz konusu bloklar "yetim" (orphan) olarak adlandırılır. Bu tarz bloklar, genelde birbirini takip eden hızlı blok üretimi durumlarında, blokların ilgili makineye ağ yapısındaki gecikmeler gibi nedenlerden dolayı ters sıralama ile varmasından dolayı oluşabilir. Bu tarz bloklar, genel olarak ilgili üst blokları ilgili makineye gelinceye kadar makine üzerinde ayrı bir havuz yapısında tutulurlar (Usta ve Doğantekin, 2018, s. 127). Bu husus, blokzincir teknolojisinin geliştirilmesi gereken yönlerinden biri olarak kabul edilmektedir. Belge yönetiminde kullanılacak blokzincir ağında çatallaşmaya, ikincil zincir oluşumuna ve yetim bloklara izin verilmemelidir.

Bununla birlikte, karşılaşılan diğer sorunlar herhangi bir kişi ya da kurumun blokzincirdeki kayıtları tahrif etme ihtimalin olabildiği, sistemin devamlılığının kim tarafından sağlanacağı, düğümler arasındaki blok farklılıklarında hangi bloğun delil olarak kabul edileceği (Lemiuex, 2017a, s. 10), yanlışlıkla bir varlığı temsil eden jetonun ya da kripto paranın el değiştirmesi ihtimali, özel anahtarların kaybı ve hangi sayısal koruma teknolojisinin kullanılacağı (Lemiuex, 2017, s. 2277) şeklinde belirtilmektedir. Diğer taraftan, işlem performansının düşüklüğü, yüksek yatırım gereksinimi, güncelleme sonrasında eski versiyona sahip kullanıcıların yeni blokzincir ağı oluşturma ihtimali, 0 ve 1'lerden oluşan şifreleme algoritmalarının quantum teknolojisiyle çözülebilme ihtimali (Usta ve Doğantekin, 2018, s. 100-101) önemli sorunlar arasındadır. İngiliz Milli Arşivinde blokzincir kullanımı üzerine araştırmalar yapan Alex Green, mevcut şifreleme algoritmaların geliştirilmesi yönünde çalışmaların olduğunu ifade etmiştir (Green ile yapılan görüşme, 2018; Green, 2018). Sayısal koruma konusunda önemli çalışmaları bulunan David Rosenthal ise SHA 256 algoritmasına dayanması, önerilen sistemlerde kripto para teşvikinin kullanılması, kripto paraların Hollanda kadar enerji harcaması gibi meselelerden dolayı blokzincir teknolojisinin sürdürülebilir olmadığını belirtmektedir (Rosenthal, 2018). Bunun yanı sıra, ciddi enerji kullanımı (Berryhill ve diğerleri, 2018), aradaki adam, sybil ve SYN saldırısı, kodlama hataları, zamanlama hataları ve saldırılar blokzincir teknolojisinin diğer zayıf yönleri arasında gösterilmektedir (Lemiuex, 2017a, s. 10).

Ayrıca, belgelerin bütünlüğü için kullanılan Bizans Generalleri Yöntemi'nin tekrardan kurgulanması gerektiği öne sürülmektedir. Bu yöntemde bir düğüm ağa mesaj iletir, bu mesajı alan ana düğüm ya da diğer düğümler mesajı yayınlardı. Yeterli sayıda düğümlerin mesajları doğrulaması neticesinde işlemler onaylanmaktaydı. Düğüm sayısı ne kadar fazlaysa, belgelerin tahriften uzak olma ihtimali de o kadar yüksekti. Fakat mesajı doğrulayan düğüm sayısı azsa, bir saldırganın ağdaki işlemlerin doğrulanması aşamasında kontrolü ele geçirmesi ve belgelerin orijinalliğini tahrif etmesinin mümkün olduğu dile getirilmektedir. Bununla birlikte kullanılan sistemlere bağlılığın da bütünlüğü etkileyebileceği ifade edilmektedir. Belgenin mahiyetinde bir

değişiklik olmasa da yedekleme gibi durumlarda belgenin iz değerlerinde yaşanabilecek eşleşmeme ihtimalinin dikkate alınması gerektiği belirtilmektedir (Hofman ve diğerleri, 2018, s. 1655).

Blokzincirlerdeki işlemler zamana göre düzenlenmiş ve zaman damgasıyla kaydedilmiş olsalar da, üretilen bu zaman damgalarının senkronizasyon problemi veya kullanılan takvimle ilişkili olmama gibi durumları söz konusudur. İşlemlerin onaylanma zamanı ile işlemlerin gerçekleşme zamanı arasında da bir gecikme söz konusu olabilir. Bunun için işlemler ile takvim zamanı arasında ek bir ilişki kurulmalıdır (Flores ve diğerleri, 2018, s. 22). Bu sorunların zamanla çözümlenebileceği düşünülse de bu konuda ciddi çalışmaların yapılması gerekli görülmektedir. Bu çalışmalara rehberlik edecek öneriler ise aşağıda belirtilmektedir.

Belgelerin kullanım ömrünü artıracak uygun ve güvenilir idari bir kontekst ve ortam sunmak için tasarlanmış faaliyetler olarak tanımlanabilecek sayısal koruma bit yapısı ve semantik bütünlük, format ve ortam sürdürülebilirliği ile bilgi güvenliğini konu edinir. Arşivsel bağın kurulmasıyla gösterilebilecek semantik bütünlük, belge tahrif olursa ortadan kalkacak ve belgenin geçmişteki olayların delili olma niteliği son bulacaktır. Bit bütünlüğünün bozulması ise iz değerlerinin karşılaştırıldığı durumlarda problemli sonuçlar oluşturabilir. Sayısal korumanın başarılı olması için belgelerin tahrif edildiği mevcut sistemlerde çözümler geliştirmektense, bir sayısal koruma sisteminin geliştirilebileceği önerilmektedir (Hofman ve diğerleri, 2018, s. 1655-1656).

Blokzincir sistemlerinde hangi kişilerin hangi belgede işlem yapabileceği sıkı bir şekilde önceden belirlenmeli ve bunun aksine izin verilmemelidir. Çünkü, anahtara sahip olan kişiler o anahtara tanımlanan yetkileri gerçekleştirebilecektir. Anahtar yönetimi, anahtarların değişimi, saklanması, kullanımı ve yenilenmesini içermelidir. Blokzincir sisteminin bu anahtarların çalınmasına veya erişilememe durumuna karşı alınması gereken güçlü önlemlerin bulunması gereklidir. (Hofman ve diğerleri, 2018, s. 1654-1655). Böylece, belgelerin gerçekliği artabilir.

Blokzincir teknolojisinde güvenilir merkezi üçüncü taraflara ihtiyaç duyulmadığı görülmektedir. Bu teknoloji, sayısal koruma pratiklerindeki aidiyet kuran ve kurmayan sayısal koruma modellerini yeniden gündeme getirmektedir. Sayısal koruma konusundaki çalışmalarıyla bilinen Peter Van Garderen bazı merkezi olmayan otonom koleksiyonların mevcut olduğunu ve bu koleksiyondaki sayısal bilgi nesnelerinin tarafların haricindeki güvenilir bir muhafızın (arşivci) kontrolüne ihtiyaç duymadan katkı sunma, temsil etme ve geliştirme teşvikiyle de saklanabileceğini ifade etmektedir. Merkezi olmayan otonom koleksiyonların merkezi kurumsal arşivlerdeki kaynak kısıtlılığı, siyasi müdahaleler ve bir ülkenin sömürdüğü topluluklarla ilgili belgeleri saklaması, yok etmesi gibi durumları ortadan kaldırabileceği söylenmektedir (Lemieux, 2017, s. 2277). Bu noktada özel kurumlarda

üretilen dokümanların da blokzincir teknolojisiyle milli hafızanın bir unsuru olarak değerlendirilebileceği düşünülmektedir. Devlet Arşivleri Başkanlığının bu konuda ciddi çalışmalar yapabileceği öngörülmektedir.

ABD Milli Arşivinin de blokzincir teknolojisinin belge yönetimindeki kullanımı üzerine araştırmalar yaptığı görülmektedir. Bu konuda bir rapor hazırlanmıştır. Raporda, e-belgelerin güvenilirliğinin nasıl korunacağına ilişkin bir yaklaşım görülemese de bazı önemli sorular gündeme getirilmiştir. Bu sorular şöyle belirtilebilir: "*NARA, blokzincir ağında sadece belgelerin tasfiyesiyle görevlendirilmiş müstakil bir düğüm olarak mı yer alacak yoksa belgelere erişebilmek için blokzincirin bir parçası mı olacaktır? Bir kuruma ait bloklar, NARA'nın bloklarına transfer edilebilecek midir? Bir blokzincir ağındaki belirli kısımları transfer etmek mümkün olacak mıdır*?" (NARA, 2019, s. 10-11). Bu aşamada milli arşivlerin rolü nasıl olacak, tüm kurumlar arşivlerin oluşturacağı blokzincir ağında mı belgelerini üretecek gibi soruların tartışılması gerekli görülmektedir.

6. Sonuç

Blokzincir teknolojisi verilerin değiştirilemezliği, güvenliği, onaylanabilirliği, dayanıklılığı ve şeffaflığını sağladığı iddiasıyla son yıllarda oldukça öne çıkmıştır. Bu çalışmada, söz konusu teknolojinin elektronik belgelerin güvenilirliğinin başarıyla korunmasındaki rolünün incelenmesi yönünde çaba gösterilmiştir. Blokzincir teknolojisi, kurulan sistemler sağlıklı çalıştığı takdirde belgelerin gereksiz yere çoğaltılmasını engellemekte ve hangi belge sahihtir sorununu ortadan kaldırmaktadır. Çünkü sistemde yapılan tüm işlemler aynı belge üzerinde gerçekleşmektedir. Bununla birlikte, belgelerin bütünlüğünü koruması en önemli kazanımları arasında kabul edilmektedir.

Bu kazanımlarına rağmen, arşivcilik ve belge yönetiminde kullanılacak blokzincir teknolojisinin ciddi olarak geliştirilmesi gereken yönleri olduğu görülmüştür. Blokzincir teknolojisinde belgelerin tamlığına zarar verme ihtimali mevcuttur. Bununla birlikte, belgelerin konteksti ve arşivsel bağının korunamaması söz konusudur. Bunun için blokzincir teknolojisinin arşivcilik ve belge yönetimi bakış açısıyla şekillendirilmesi gerekli görülmektedir. Bir belgenin kuruma ait bir işlem neticesinde oluştuğunu kanıtlamanın yolu, belgenin aynı işlem kapsamında üretilen diğer belgelerle arasındaki ilişkinin kurulmasıdır. Arşivsel bağ olmadan bir bilginin ya da verinin belgeye dönüşümünden söz etmek pek mümkün görünmemektedir. Arşivsel bağ, aynı faaliyet sonucunda oluşan belgeler arasındaki ilişki ağını açıklar (Hofman ve diğerleri, 2018, s. 1654; Lemieux, 2017b, Lemieux, 2016a).

Kâğıt ortamdaki belgelerde arşivsel bağın kurulması dosya kodlarıyla gerçekleştirilmekteydi ve aynı faaliyet kapsamında oluşan belgeler aynı dosyaya kaldırılırdı. Böylece dosya yapısına bakarak arşivsel bağ

incelenebilirdi. Fakat elektronik ortamda arşivsel bağın korunması daha çok titizlik gerektiren bir adım olmuştur. Bunun için üstveriler kullanılsa da belge ile ait olduğu işlem, faaliyet ve fonksiyonla ilişkili olan diğer belgeler arasında bir bağ kurulmalıdır. Bu bağ, blokzincirlerin yapısında da yer almalıdır (Hofman ve diğerleri, 2018, s. 1654-1655).

Bununla birlikte, sistemde belge üretimini kontrol etmek amacıyla kullanılacak, belgelerin fiziksel ve entelektüel formlarının tanımlanması için gerekli olan özellikleri inceleyen prosedürlerin devreye alınması gereklidir. Bu prosedürlerin belge üretiminin kontrol etmek amacıyla kullanılması beklenmektedir. Böylece, sistemler güvenilir belge üretebilir (Hofman ve diğerleri, 2018, s. 1656). Bu noktada, diplomatik analiz yöntemlerinden faydalanılabileceği düşünülmektedir. Aynı tür ve kaynağa ait belgelerin form elemanlarının birbirine benzerlik göstermesi güvenilirliğin gereklerindendir. Blokzincirlerdeki kayıtlarda bu gerekliliğin nasıl sağlanacağı konusunda çeşitli tereddütler bulunmaktadır. Bu nedenle, yeterli standartlaşmanın sağlanamadığı ifade edilmektedir (Flores ve diğerleri, 2018, s. 22). Hangi teknoloji kullanılırsa kullanılsın belge yönetimi ilkelerinin geçerliliğini koruyacağını ileri sürmek mümkün görünmektedir. Blokzincir teknolojisinin elektronik belgelerin güvenilirliğinin başarılı bir şekilde korunması için bu ilkeleri takip etmenin gerekli olduğu anlaşılmaktadır.

Blokzincir teknolojisinde kripto para olarak da işlem gören Bitcoin, Ethereum, Ripple gibi protokoller kullanılmaktadır. Bu protokollerin uzun vadede ne kadar sürdürülebilir olacağı merak edilmektedir. Ayrıca, protokoller arası geçişlerde bu geçişin sorunsuz gerçekleşmesi dikkatle incelenmesi gereken bir meseledir. Bu nedenle açık kaynak kodlu protokollerin geliştirilmesi yönünde ciddi çaba gösterilmesi gerekli görülmektedir. Bu konuda önemli araştırmaların yapılması temenni edilmektedir. Bu kanaatimiz blokzincir uygulamaları konusunda önemli çalışmaları bulunan British Columbia Üniversitesi Kütüphane, Arşiv ve Bilgi Çalışmaları Okulu öğretim üyesi Prof. Dr. Victoria Lemieux ile paylaşılmıştır (Lemieux ile görüşme, 2017).

Blokzincir teknolojisinin merkezi bir otoriteye ihtiyaç duymaması nedeniyle kamu kurumlarına eskisi kadar ihtiyaç duyulmamasına neden olacağı ifade edilmektedir. Fakat bu yaklaşımın tersine bir sonuç oluşması da muhtemeldir. Günümüzde, elektronik arşivlemeyi yeteri kadar başarılı yürütemeyen devletlerin blokzincir teknolojisi aracılığıyla başarısını artırabileceği tahmin edilmektedir. Bu kanaatin ciddi olarak denenmesi için devlet arşivlerinde blokzincir teknolojisinin kullanımına yönelik çalışmaların yapılmasına ihtiyaç duyulmaktadır. Bununla birlikte, blokzincir teknolojisinde devlet arşivlerinin konumu ne olacaktır, üretilen belgeler arşivlere nasıl devredilecektir gibi soruların ciddi olarak tartışılması bir gereklilik olarak karşımıza çıkmaktadır.

Ülkemizde özel kurumlarda üretilen belgelerin devlet arşivlerine devri konusunda yeteri kadar sağlıklı sonuçların elde edilemediği bilinmektedir. Bu noktada blokzincir teknolojisinden faydalanılabilir mi, özel kurumlarda üretilen belgeler blokzincir teknolojisi kullanılarak devlet arşivlerinin emanetine daha sağlıklı bir şekilde alınabilir mi gibi sorular akla gelmektedir. Bu soruların incelenmesi için konu hakkında ciddi çalışmaların yapılmasına ihtiyaç duyulmaktadır.

Türkiye'de blokzincir teknolojisinin arşivcilik ve belge yönetimindeki kullanımı üzerine yeteri kadar araştırma yapılmadığı gözlenmektedir. Bu alanda yapılacak araştırmalar sadece arşivciler ve belge yöneticileri tarafından değil, bilgi teknolojileri uzmanlarının da katkısıyla gerçekleşmelidir. Bu konudaki araştırmalar için TÜBİTAK Bilgem'de oluşturulan Blokzincir Laboratuvarının önemli bir katkı sağlayacağı düşünülmektedir. Burada gerçekleştirilecek araştırmalarda kamu ve özel sektör işbirliğinin sağlıklı sonuçlar oluşturacağına inanılmaktadır.

Kaynakça

ARCHANGEL (2019). *Trusted Digital Archives*. 28 Eylül 2019 tarihinde http://www.archangel.ac.uk adresinden erişildi.

Atalay, G. E. (2018). Blokzincir Teknolojisi ve Gazeteciliğin Geleceği, *Stratejik ve Sosyal Araştırmalar Dergisi*, 2(2), 45-54.

Bankalararası Kart Merkezi (2019). *Belgem.io*. 28 Eylül 2019 tarihinde https://bkm.com.tr/belgem-io-herkes-icin-blockchain/ adresinden erişildi.

Berryhill, J., Bourgery, T. ve Hanson, A. (2018). *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector*. OECD.

Birleşmiş Milletler. (2018). The Future is Decentralised. 16 Haziran 2019 tarihinde https://www.undp.org/content/dam/undp/library/innovation/The-Future-is-Decentralised.pdf adresinden erişildi.

Bitnation. (2019). Bitnation Web Sayfası. 16 Haziran 2019 tarihinde https://tse.bitnation.co/ adresinden erişildi.

Blockchain Türkiye Platformu. (2019). *Blockchain Türkiye Platformu Web Sayfası*. 7 Eylül 2019 tarihinde https://bctr.org/ adresinden erişildi.

Buchmann, N., Rathgeb, C., Baier, H., Busch, C. ve Margraf, M. (2017). Enhancing Breeder Document Long-Term Security Using Blockchain Technology. *International Computer Software and Applications Conference*, 2, 744–748.

Bui, T., Cooper, D., Collomosse, J., Bell, M., Green, A. Sheridan J., Brown, A. (2019). ARCHANGEL: Tamper-proofing Video Archives using Temporal Content Hashes on the Blockchain.CVPR Blockchain Workshop, 17 Haziran 2019, Long Beach, Amerika Birleşik Devletleri [ABD] içinde, 7 Eylül 2019 tarihinde https://arxiv.org/abs/1904.12059 adresinden erişildi.

Canaday, H. (2017). *Blockchain in MRO Could Happen Sooner Than You Think*. 28 Eylül 2019 tarihinde https://www.mro-network.com/big-data/blockchain-mro-could-happen-sooner-you-think adresinden erişildi.

Collomosse, J., Bui, T., Brown, A., Sheridan, J., Green, A., Bell, M., Fawcett, J., Higgins, J. ve Thereaux, O. (2018). ARCHANGEL: Trusted Archives of Digital

Public Documents. *Proceedings of the ACM Symposium on Document Engineering*.

Creswell, J. W. (2016). *Araştırma Deseni: Nitel, Nicel ve Karma Yöntem Yaklaşımları*. Selçuk Beşir Demir (Yay. haz.). 3. baskı. Eğiten Kitap Yayıncılık.

Çiçek, N. (2009). *Modern Belgelerin Diplomatiği*. İstanbul: Derlem Yayınları.

Çiçek, N. (2011). Elektronik Belgelerin Diplomatik Analizi ve Arşivsel Bağın Kurulmasındaki Önemi: Türkiye'deki Uygulamalar Işığında Bir İnceleme. *Bilgi Dünyası*. 12(1), 87-104.

Çiçek, N. ve Sağlık, Ö. (2017). e-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme. Özdemirci, F. ve Akdoğan, Z (Yay. haz.). *Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar* içinde (257-276). Ankara Üniversitesi.

Dini, A. T., Abete, G. E., Colombo, M., Guevara, J., Hoffmann, M. B. S. ve Abeledo, C. M. (2018). Analysis of Implementing Blockchain Technology to the Argentinian Criminal Records Information System. *Congreso Argentino de Ciencias de La Informatica y Desarrollos de Investigacion* içinde.

Duranti, L. ve Thibodeau, K. (2006). The Concept of Record in Interactive, Experiential and Dynamic Environments: The Views of INTERPARES. *Archival Science*, 6, 13-68.

Duranti, L. (2009). From Digital Diplomatics to Digital Records Forensics. *Archivaria*, 68, 39-66.

Durbilmez, S. E., Türkmen, S. Y. (2019). Blockchain Teknolojisi ve Türkiye Finans Sektöründeki Durumu. Finans Ekonomi ve Sosyal Araştırmalar Dergisi, 4(1), 30–45.

Elitaş, C., Aydemir, O. ve Elitaş, B. L. (2009). Muhasebe Açısından Kamu Güveni: Türk Ceza Kanunu'nun İncelenmesi. *Mali Çözüm Dergisi*, 93, 29-44

Flores, D., Lacombe, C. ve Lemieux, V. (2018). *Real Estate Transaction Recording in the Blockchain in Brazil*. 6 Ağustos 2019 tarihinde http://blogs.ubc.ca/recordsinthechain/files/2018/01/RCPLM-01-Case-Study-1_v14_English_Final.pdf adresinden erişildi.

Fukuyama, F. (2005). *Güven: Sosyal Erdemler ve Refahın Yaratılması*, çev. Ahmet Buğdaycı, 3. baskı, İş Bankası Yayınları.

Galiev, A., Prokopyev, N., Ishmukhametov, S., Stolov, E., Latypov, R. ve Vlasov, I. (2019). Archain: A Novel Blockchain Based Archival System. *Proceedings of the 2nd World Conference on Smart Trends in Systems, Security and Sustainability*, 308–312.

Green, A. (2018, 5 Haziran). Trustworthy Technology: The Future of Digital Archives? [Blog Yazısı]. Erişim Adresi: https://blog.nationalarchives.gov.uk/trustworthy-technology-future-digital-archives

Guardian (2016). The Death of Neoliberalism and the Crisis in Western Politics. 16 Haziran 2019 tarihinde https://www.theguardian.com/commentisfree/2016/aug/21/death-of-neoliberalism-crisis-in-western-politics adresinden erişildi.

Guardian (2018). Seven signs of the Neoliberal Apocalypse. 16 Haziran 2019 tarihinde https://www.theguardian.com/commentisfree/2018/apr/27/seven-signs-of-the-neoliberal-apocalypse adresinden erişildi.

Guo, W., Fang, Y., Pan, W. ve Li, D. (2016). Archives as a Trusted Third Party in Maintaning and Preserving Digital Records in the Cloud Environment. *Records Management Journal*, 26(2), 170-184.

Herian, R. (2018). Taking Blockchain Seriously. *Law Critique*, 29, 163-171.

Hofman, D., Shannon, C., McManus, B., Lam, K., Assadian, S., Ng, R. ve Lemieux, V. L. (2018). Building Trust Protecting Privacy Analyzing Evidentiary Quality in a Blockchain Proof-of-Concept for Health Research Data Consent Management. *IEEE 2018 International Congress on Cybermatics, 30 Temmuz-3 Ağustos 2018, Halifax, Kanada* içinde (1650-1656).

Hofman, D., Lemieux, V. L., Joo, A. ve Batista, D. A. (2019). The Margin Between the Edge of the World and Infinite Possibility: Blockchain, GDPR and Information Governance. *Records Management Journal*, 29(1-2), 240-257.

Hyla, T., Pejaś, J. (2019). eHealth Integrity Model Based on Permissioned Blockchain. *Future Internet*, 11(3), 1-14.

International Research on Permanent Authentic Records in Electronic Systems [INTERPARES]. (2002). *Findings on the Preservation of Authentic Electronic Records*.

INTERPARES. (2008). *INTERPARES 2: Experiential, Interactive and Dynamic Records*. Ed. Duranti, L. ve Preston, R.

Lemieux, V. (2016). *Blockchain Technology for Recordkeeping Help or Hype ? Blockchain Technology for Recordkeeping*. Montreal: Social Sciences and Humanities Research Council of Canada.

Lemieux, V. L. (2016a). Trusting Records: Is Blockchain Technology the Answer? *Records Management Journal*, 26(2), 110-139.

Lemieux, V. L. (2017). A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation. Nie Jian-Yun ve diğerleri (Yay. haz.). *IEEE International Conference on Big Data, 11-14 Aralık 2017, Boston, ABD* içinde (2271-2278).

Lemieux, V. L. (2017a). Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework. *Future Technologies Conference, 29-30 Kasım 2017, Vancouver, Kanada* içinde (41–48). Vancouver: The Science and Information Organization.

Lemieux, V. L. (2017b). Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective. *European Property Law Journal*, 6(3), 392-440.

Luu, L., Chu, D. H., Olickel, H., Saxena, P. ve Hobor, A. (2016). Making Smart Contracts Smarter. *23rd ACM Conference on Computer and Communications Security Hofburg Palace, Vienna, Austria*, 24-28 Ekim 2016. 16 Haziran 2019 tarihinde https://eprint.iacr.org/2016/633.pdf adresinden erişildi.

Medium (2018). The Death of Neoliberalism. 16 Haziran 2019 tarihinde https://medium.com/@beyondsatire/a-brief-history-of-neoliberalism-46c1fc0aa89b adresinden erişildi.

Nakamoto, Satoshi. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 16 Haziran 2019 tarihinde https://bitcoin.org/bitcoin.pdf adresinden erişildi.

National Archives and Records Administration [NARA] (2019). *Blockchain White Paper*. NARA.

OECD. (2018). *Blockchain and beyond: Encoding 21st Century Transport*. OECD: International Transport Forum.

Ostry, J. D., Loungani, P. ve Furceri, D. (2016). Neoliberalism: Oversold?. *IMF Finance & Development*, 53(2), 38-41.

Proofstack (2019). *Proofstack Web Sayfası*. 28 Eylül 2019 tarihinde https://tr.proofstack.io/about.html adresinden erişildi.

Rogers, C. (2015). *Virtual Authenticity: Authenticity of Digital Records from Theory to Practice.* Doktora Tezi. British Columbia Üniversitesi.

Rosenthal, D. (2018, 15 Şubat). Do You Need a Blockchain? [Blog Yazısı] Erişim Adresi: https://blog.dshr.org/2018/02/do-you-need-blockchain.html

Sayarlıoğlu, A. (2018). *Herkes için Blok-Zincir*. 28 Eylül 2019 tarihinde https://medium.com/@ahmet.sayarlioglu/herkes-i%C3%A7in-blok-zincir-blokchain-1c85eb3a0bee adresinden erişildi.

Uysal, U. T., Aldemir, C. (2018). Dijital Kamu Mali Yönetim Sistemi Ve Blok Zinciri Teknolojisi. *Muhasebe ve Vergi Uygulamaları Dergisi*, 11(3), 505–522.

Usta, A ve Doğantekin, S. *Blockchain 101*. 2. baskı. İstanbul: Bankalararası Kart Merkezi.

Yaga, D., Mell, P., Roby, N. ve Scarfone, K. (2018). *Blockchain Technology Overview*. 7 Eylül 2019 tarihinde https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf adresinden erişildi.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 7-31.

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V. ve Yalansky, L. (2017). Ensuring Data Integrity Using Blockchain Technology. *Conference of Open Innovation Association*, 534–53.