**Kütüphane, Arşiv ve Müze Araştırmaları Dergisi**
**Library, Archive and Museum Research Journal**
e-ISSN: 2718-0832
*Cilt/Volume: 5, Sayı/Issue: 1 (2024), 1-35*
https://dx.doi.org/10.59116/lamre.1357399

İSTANBUL MEDENİYET ÜNİVERSİTESİ

Araştırma Makalesi – Research Article
*Geliş Tarihi / Received: 08.09.2023 Kabul Tarihi Accepted: 31.10.2023*

# Arşivcilik ve Belge Yönetimi Faaliyetlerinde Blokzincir Teknolojisi: Bilgi Güvenliği Bağlamında Bir Değerlendirme

## Blockchain Technology in Archiving and Records Management Activities: An Evaluation in Terms of Information Security

Fatih SÜKÜT*

**ÖZET**

Arşivcilik ve belge yönetimi faaliyetleri yürüten kurumlar, hizmetlerini gereğince yerine getirilebilmek adına günümüz teknolojilerinin sunduğu imkânları faaliyetlerine yansıtmaya çalışılmaktadırlar. 2008 yılı itibariyle ilk olarak kripto para birimleri ile ünlenen blokzincir teknolojisi de bu kapsamda farklı alanlarda faaliyet gösteren kurumların ilgi alanına girmiş teknolojilerden biridir. Söz konusu teknoloji özellikleri sayesinde arşivcilik ve belge yönetimi de dâhil farklı alanlarda araştırma ve uygulamalara konu olmuştur. Teknolojinin ilgili alanlarda kullanımına yönelik çeşitli metodolojik ve uygulamalı çalışmalar yapılmış ve yapılmaya devam edilmektedir. Elektronik ortamda yürütülen arşivcilik ve belge yönetimi faaliyetleri için en önemli konunun bilginin güvenliği ve belge sayısındaki artışa bağlı olarak belgenin yönetimi olduğu göz önüne alındığında blokzincir teknolojisinin, bu alanda da kullanılabilecek bir araç olduğu değerlendirilebilir. Bu kapsamda bilginin / belgenin özgünlüğü, güvenirliliği, bütünlüğü ve kullanılabilirliği ilkeleri doğrultusunda blokzincir teknolojisinin arşivcilik ve belge yönetimi faaliyetlerine muhtemel katkısının araştırılması, bu faaliyetlerin geliştirilmesi açısından önem kazanmaktadır. Çalışmada, belge tarama nitel araştırma yöntemi ile blokzincir teknolojisinin arşivcilik ve belge yönetimi faaliyetlerinde kullanımına yönelik araştırmalar ve uygulamalar irdelenmekte, ulusal ve uluslararası bilgi güvenliği ve belge yönetimi standartları bağlamında blokzincir teknolojisinin ilgili faaliyetlere / hizmetlere sağlayacağı katkı ve olası zafiyetler ortaya konmaktadır. Bilgi güvenliği özelinde sürdürülen çalışmanın alanyazınına katkı sağlayacağı öngörülmektedir.

***Anahtar Kelimeler:*** *Blokzincir Teknolojisi, Arşivler, Arşivcilik, Belge Yönetimi, Bilgi Hizmetleri.*

**ABSTRACT**

Archiving and records management institutions are trying to incorporate the possibilities offered by today's technologies into their activities in order to provide their services properly. Blockchain technology, which first came to prominence in 2008 with cryptocurrencies, is one of the technologies that has attracted the interest of institutions. Thanks to the characteristics it offers, this technology has been the subject of research and applications in various fields, including archiving and records management. Various methodological and applied studies have been and are being carried out on the use of this technology. Considering that the most important issue for archiving and records management activities in the electronic environment is the security of information and the management of records, depending on the increase in the number of records, it can be considered that blockchain technology is a tool that can also be used in this field. In this context, it is important to explore the possible contributions of blockchain technology to activities in line with the principles of originality, reliability, integrity and usability of the information or records. In the study, research and applications for the use of blockchain technology in related activities will be examined using the document scanning method from qualitative research methods. And the contribution and possible weaknesses of blockchain technology in the context of national and international information security and records management standards will be revealed. It is expected that the study conducted in the context of information security will contribute to the literature.

***Keywords:*** *Blockchain Technology, Archives, Archiving, Records Management, Information Services.*

*Dr. Öğrencisi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi Anabilim Dalı, e-posta: fatihsukut@gmail.com, ORCID: https://orcid.org/0000-0001-6395-8812

## 1. GİRİŞ

Bilgi ve iletişim teknolojileri 21. yüzyıl ile birlikte belirgin gelişmeler kaydetmiştir. Özellikle son 20 yılda ortaya çıkan gelişmeler ile insanlık farklı bir boyuta taşınmıştır. Bu süreçte akıllı telefon, saat ve ev eşyaları, 3 boyutlu yazıcılar, sürücüsüz otomobiller, insansız hava araçları, birden fazla kullanımlı roketler, güneş panelleri, yapay zekâlı ya da insansı robotlar, dokunmatik ekranlar, wifi teknolojisi, artırılmış gerçeklik teknolojisi, gen düzenlemesi, blokzincir teknolojisi gibi konularda yenilikler ve önemli gelişmeler ortaya çıkmıştır (Arslan, 2020, s. 83, ss. 87-89). Bu gelişmelere en önemli katkılardan birini de kuşkusuz kablosuz haberleşme teknolojilerindeki ilerlemeler sağlamıştır. 5G kablosuz haberleşme teknolojisi, bu bağlamda ortaya çıkan en yeni teknolojidir. Bu teknolojiye ilişkin hizmetlerin sunumuna yönelik çalışmalar dünya genelinde son hız devam etmektedir. 2028 yılı itibariyle dünyadaki tüm mobil aboneliklerinin %55'inin ulaşabilir olacağı tahmin edilen 5G teknolojisi, hali hazırda dünyanın farklı gelişmiş ülkelerinde kullanılmaktadır (Bilgi Teknolojileri ve İletişim Kurumu (BTK), 2018, s. 25, s. 41; Arslan, 2020, s. 83, ss. 92-93; BTK, 2023a; Turkcell, 2022). 5G teknolojisinin kullanımının yaygınlaşması ile birlikte yakın gelecekte dünyada ve ülkemizde veri indirme hızlarının Gbit/s seviyelerine yükselmesi, gecikme sürelerinin 4.5G'ye oranla asgari düzeye inmesi (bir ile on milisaniye sürelerde gecikmeler), bu sayede örneğin uzaktan cerrahi müdahalelerin daha mümkün ve yaygın hale gelmesi ve (bir baz istasyonunun kapsamına daha fazla cihazın girebilecek olması sebebiyle) çeşitli alanlarda daha fazla cihazın aynı anda, kalite sorunu yaşamadan işlem yapabilmesi beklenmektedir (Turkcell, 2022). Kablosuz internet kullanımının yaygınlaşmasına vesile olan bu teknolojiler, bilgi ve iletişim teknolojilerinin insan hayatının her aşamasında kendisine yer bulmasına da yardımcı olmaktadır. Örneğin BTK'nın 2022-4. Çeyrek Pazar Verileri Raporu'na göre ülke genelinde 19 milyonu sabit, 71,7 milyonu mobil olmak üzere toplam 90,6 milyon geniş bant internet abonesi bulunmaktadır. Bunun yanı sıra aynı dönemde toplam mobil abone sayısı 90,3 milyon olmuştur (BTK, 2023b, ss. 8-9). Bu sayı bir önceki yılın aynı döneminde 86,3 milyondur (BTK, 2022, ss. 7-8). Ayrıca bilgi ve iletişim teknolojilerinin kullanımı dünya genelinde de günbegün artmaktadır. Ekonomik Kalkınma ve İşbirliği Örgütünün (OECD) "Hanehalkı ve Bireyler Tarafından Bilgi ve İletişim Teknolojilerine Erişim[1]" başlıklı dinamik tablosunda oranların yıllar itibariyle artarak ilerlediği açıkça görülmektedir (OECD, 2023).

Toplumsal tabanda bilgi ve iletişim teknolojilerinin kullanımındaki artış olumlu görünse de kullanıcılar ve büyük veriye sahip kurumlar açısından yanında bazı tehditleri de barındırdığı bir gerçektir. Bunlar arasında (1) verilerin yönetilememesi, bu sebeple kaybolma veya istendiğinde erişilememe ihtimali, (2) kullanıcıların özel hayatlarının gizliliği ve kişisel verilerinin korunması kapsamında verilerin üçüncü, yetkisiz ya da kötü amaçlı kişilerin eline geçme ihtimali, (3) verilerin içeriklerinin değiştirilme ihtimali, (4) verilerin alıverişi veya aktarılması gibi işlemler esnasında dışarıdan müdahalelere açık olması gibi farklı bilgi güvenliği tehditleri bulunabilmektedir (Lemieux, 2017a, s. 420; Zikratov ve diğerleri, 2017, s. 535; BTK, 2019). Dijital

[1] ICT Access and Usage by Households and Individuals.

varlıkların ya da elektronik belgelerin (e-belge) el değiştirmesi, alakalı olmayan kişilerin / kurumların eline geçmesinin engellenmesi ve bu varlıkların ya da belgelerin benzersizliklerinin/tekliklerinin kanıtlanması süreçlerinde güvenlik zafiyeti oluşması, bilgisayar ve iletişim teknolojilerini kullanan bireyler ve kurumlar arasında geçmişten bu yana güvensizlik, hoşnutsuzluk ve mağduriyet yaratmaktadır. Hükümetler bu tehditleri ortadan kaldırmaya yönelik Bilgi Edinme Hakkı Kanunu (örneğin Birleşik Krallık Bilgi Edinme Hakkı Kanunu, 2000 - Freedom of Information Act, 2000; Türkiye Cumhuriyeti 24/10/2003 tarihli ve 4982 sayılı Bilgi Edinme Hakkı Kanunu) gibi farklı mevzuat çalışmaları yapsalar da söz konusu mevzuatın uygulanmasındaki yetersizlikler ve teknolojik gelişmelere ayak uydurulmasındaki (bürokratik) aksaklıklar internet kullanıcılarının güvenlik tehditleri karşısında yeterince korunamamalarına yol açmaktadır. Bu minvalde çok sayıda dolandırıcılık haberi ile de karşılaşılmaktadır (NTV Haber, 2019; Emniyet Genel Müdürlüğü, 2022; Türk Ekonomi Bankası, 2022). Hayatın farklı alanlarında karşılaşılan ve çalışma içerisinde bölüm bölüm bahsedilen bilgi güvenliği sorunları, hâlihazırda yüksek miktarda ve çeşitli veri kaynağı barındıran kütüphane ve arşivler gibi bilgi merkezleri (İngiliz Ulusal Arşivleri, 2023a; İngiliz Ulusal Arşivleri, 2023b) özelinde de üzerinde durulan bir konudur (Özdemirci, 2009; Özdemirci, 2019; Bilgi Yönetimi ve Bilgi Güvenliği…, 2019).

Bu aşamada, elektronik ortamda bulunan varlıkların yönetimi ve güvenliklerinin sağlanmasında blokzincir teknolojisi bir araç olarak sunulmakta ve kullanılmaktadır. Blokzincir teknolojisi 90'lı yılların başında ele alınan dağıtık defter teknolojisine (DDT) dayanır (Stuart ve Stornetta, 1991, s. 100; Stuart ve Stornetta, 1999, s. 30; BlockstreetHQ Team, 2018). DDT, kayıtları birbirinden bağımsız kullanıcılar tarafından tutulan bir veri tabanı olarak tanımlanabilir (Çiçek ve Sağlık, 2019, s. 143). İlk olarak kripto para transferlerinde kullanılan blokzincir teknolojisi, üçüncü tarafları aradan çıkararak iki taraf arasında dijital varlık alışverişi yapılmasına imkân veren, bu işlemler esnasında güven sorununu ortadan kaldıracak şekilde kullanıcıların elektronik imzalarını (e-imza) içeren, şifreleme teknikleri ile işlem yapabildikleri ve kanıta dayalı bir teknoloji olarak lanse edilmektedir (Stuart ve Stornetta, 1991, s. 102; Nakamoto, 2008). Sağlık kayıtlarının sahipleri tarafından tercihli sunulmasından, tapu kayıtlarının transferi ve saklanması ile dijital varlıkların aracısız değiş tokuşuna kadar farklı alanlarda kullanılan blokzincir teknolojisi, arşivlerde ve belge yönetimi faaliyetlerinde de kullanılmakta ya da kullanılmasına yönelik çalışmalar (Hoy, 2017; Lemieux, 2017a; Lemieux, 2017b; Çiçek ve Sağlık, 2019; Kim, 2020; Metin, 2021) sürdürülmektedir. Arşivler ve belge yönetimi faaliyetlerinde bulunan kurumlarda blokzincir teknolojisinin kullanımı ile bilgi ve belge hizmetleri ve bu hizmetlere ilişkin kayıtları, bu kayıtlara veya yapılacak işlemlere özgü doğrulanabilir zaman damgalarını[2] ve kullanıcı kayıtlarını içeren blokzincir ağları kurulabilir, belgeler bu vasıtayla kullanıcı özelinde paylaşılabilir, bu sayede arşivler veya ilgili kurumlar arası kaynak alışverişlerinde kolaylık ve güvenlik sağlanabilir.

Çalışmada arşivcilik ve belge yönetimi faaliyetleri ile blokzincir teknolojisi arasındaki ilişki kuramsal olarak

[2] "Zaman damgası" kavramı dipnot 7'de açıklanmıştır.

ele alınmıştır. Konu üzerine literatürde yer alan araştırmalar incelenmiştir. Bu kapsamda arşivlerde ve ilgili diğer kurumlarda veya bilgi merkezlerinde blokzincir teknolojisi konusunda hâlihazırda gerçekleştirilen projeler ve uygulamalar araştırılmış, blokzincir teknolojisinin söz konusu faaliyetlere sağladığı veya sağlayacağı katkılar ve bilgi güvenliği bağlamında ortaya çıkabilecek muhtemel açık alanlar (zafiyetler) "TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı" ile "ISO 15489-1 Belge Yönetimi Standardı"na bağlı olarak "TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı" doğrultusunda irdelenmiştir. Araştırma sonunda ortaya çıkan bulgular değerlendirilmiş, sonuç ve öneriler ile çalışma sonlandırılmıştır. Konu bağlamında çalışmanın gelecek araştırmalara ışık tutacağı, katkı sağlayacağı öngörülmektedir.

Çalışmamızda nitel araştırma yöntemlerinden doküman analizi diğer bir ifadeyle belge incelemesi yöntemi kullanılmıştır. Araştırma kapsamında niteliklerine göre yazı ve görsel-işitsel temelli dokümanlar ele alınmıştır (Kıral, 2020, ss. 173-174). Blokzincir, dağıtık defter teknolojisi, (elektronik) belge yönetimi, bilgi yönetimi, bilgi güvenliği, arşivler, bilgi merkezleri ve arşivcilik kavramları literatür taraması esnasında kullanılan anahtar kelimeler olmuştur. Blokzincir teknolojisine yönelik somut araştırmaların dayandığı 90'lı yıllardan günümüze kadar olan süreç kaynak / araştırma zaman aralığı olarak belirlenmiştir. Araştırma kapsamında erişilen ulusal ve uluslararası basılı ve elektronik kaynaklar: (1) Gözden Geçirme (yüzeysel inceleme), (2) Okuma (ayrıntılı inceleme) ve (3) Yorumlama yöntemleri doğrultusunda analiz edilmiştir (Kıral, 2020, s. 181).

## 2. BLOKZİNCİR TEKNOLOJİSİ

2008 yılında Satoshi Nakamoto adlı bir internet kullanıcısı genel olarak tarafların herhangi bir aracıya ihtiyaç duymadan kendi aralarında güven sorunu teşkil etmeyecek, kullanıcıların e-imzalarını içeren, şifreleme teknikleri ile kanıta dayalı bir ödeme sistemi önermiştir. Bu sistemde kullanılacak dijital para biriminin adını da "Bitcoin" olarak ifade etmiştir. Ortaya atılan bu sistemin odak noktasında elektronik ödeme olmasına rağmen geri planında, işlemlerin güvenli bir şekilde gerçekleştirilmesini sağlayan blokzincir teknolojisi yer almaktadır (Nakamoto, 2008).

Dağıtık defter sistemine dayanan blokzincir teknolojisi ve buna ilişkin akademik çalışmalar 2008 yılı öncesine dayansa ve Bitcoin'in geliştirilmesinden önce var olsa da teknolojinin toplumun geniş bir kesimi tarafından fark edilmesi, konu üzerine yapılan ar-ge çalışmalarının artması, yaygınlaşması ve daha somut çıktılara dönüşmesi, Bitcoin'in 2008 yılında ortaya çıkışıyla başlamıştır (Usta ve Doğantekin, 2018, s. 9, ss. 23-24; Çiçek ve Sağlık, 2019, s. 145; Çetin, 2020, ss. 65-66). Çalışmanın "Blokzincir Teknolojisinin Yapısı" başlığı altında dağıtık defter teknolojisine ilişkin daha detaylı açıklama yer almaktadır.

Blokzincir kavramı, uluslararası literatürde İngilizcesiyle "blockchain" olarak ifade edilmektedir. Ülkemizde ise "blokzincir", "blokzinciri" ve "blok zinciri" gibi farklı söylem ve yazım şekillerinde kullanılmaktadır. Bu çalışmada ise verilerin kaydedildiği blokların birbirine zincirlenmesi / eklemlenmesi sonucunda zincirlenmiş

bloklar silsilesinin ortaya çıkması sebebiyle "blokzincir" şeklinde kullanılmıştır.

Felsefe olarak blokzincir, merkezi otoriteyi aradan çıkararak kişiler arası ilişkilerin veya operasyonların (çevrim içi alışveriş, arşivleme, depolama vb.) üçüncü bir kişi veya kurum olmaksızın, güvene dayalı gerçekleştirilmesini hedeflemekte ve sağlamaktadır (Sert, 2020).

Kavramsal tanım olarak blokzincir; "*verilerin, bir önceki blokla, kriptografik doğrulama yapan, zaman mühürlü, sadece dosya yazım yetkisi olanlar tarafından değiştirilebilen, şifreleme anahtar yöntemi ile bağlanan, dağıtılmış veri tabanı teknolojisi"* olarak tanımlanmaktadır (Çetin, 2020, s. 66).

Ayrıca TÜBİTAK BİLGEM Blokzincir Araştırma Laboratuvarına göre; internet ortamında dijital varlıkların kişiler arası transferine imkân sağlayan ve merkezi olmayan bir kriptografik kayıt defteri (TÜBİTAK, 2018), Amerikan Kütüphane Derneğine (ALA) göre; verileri kriptografik doğrulamaya sahip, zaman damgalı, türüne göre yalnızca şifreleme anahtarlarına sahip olanlar tarafından değiştirilebilen, yazılabilen ve önceki bloklarla / kayıtlarla bağlantılı bloklar halinde düzenlenen dağıtık bir veri tabanı teknolojisi olarak ifade edilmektedir (ALA Blockchain, 2017).

Blokzincir teknolojisi sayesinde veriler matematik fonksiyonları kullanılarak şifrelenir ve yalnızca belirli yazılımsal anahtarlarla açılabilir. Böylece veriler güvenli ve / veya özel kılınır (Hughes, 1993).

Bunun yanında blokzincir teknolojisi sayesinde yukarıda bahsedilen elektronik ödeme sisteminde yapılan işlemlerin geri döndürülme ihtimali yok denecek kadar azdır. Örneğin bir kullanıcının sahip olduğu bir varlığı veya bilgiyi başka bir kullanıcıya aktardıktan sonra bu işlemi tersine çevirmesi veya geri döndürmesi, bir işlem birden fazla kullanıcı tarafından teyit edildiğinden ve geri döndürülmesi istendiğinde yine aynı teyit sürecinin gerçekleşmesi gerekeceğinden oldukça zordur. Bu konu çalışma içerisinde Şekil 2 bağlamında açıklanmıştır. Diğer taraftan gerçekleştirilen işlemin geri döndürülemiyor olması duruma göre faydalı olarak da değerlendirilebilir. Örneğin yapılan işlemlerin zaman damgalı kayıtları bloklarda kronolojik olarak saklandığından çift ödeme gibi hatalı işlemler engellenmektedir (Nakamoto, 2008; Usta ve Doğantekin, 2018, s. 145).

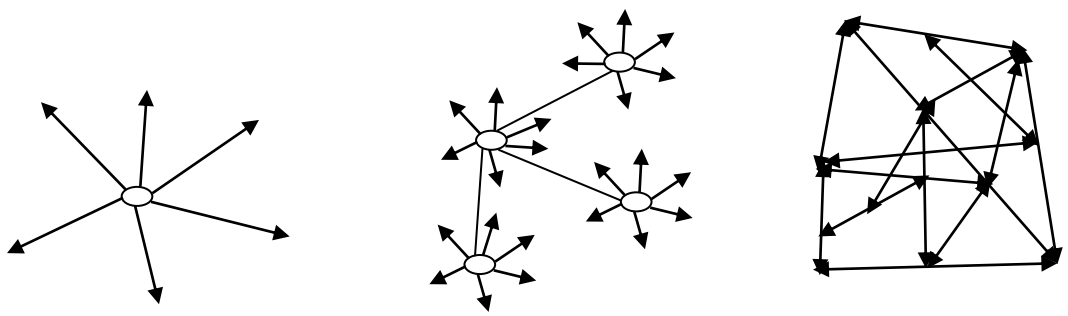
Blokzincir ağı düğümlerden (node) oluşmakta ve her bir düğüm bir bilgisayara karşılık gelmektedir. Bilgisayardan kastedilen ise IP adresi[3] değil işlemcidir. Bunun sebebi, birden fazla IP adresine sahip bilgisayarın ağda bulunan, çoğunluğun oluşturduğu blokları hileyle kendi iradesi doğrultusunda değiştirebilme ihtimalinin bulunmasıdır.

[3] IP (İnternet Protokolü) adresi, bir bilgisayar ağında iletişim için internet teknolojisini kullanan bir bilgi iletişim aygıtının tanımlayıcı numarasıdır. Bu adres, söz konusu cihazın hangi hizmet sağlayıcısını veya hizmet ağını kullandığını ve internete hangi konumdan bağlandığını gösterir (Chip Online, 2022).

Ağda yer alan düğümlerin yarısından fazlası doğru bilgiyi[4] teyit ettiği sürece sistemin üçüncü kişiler tarafından bertaraf edilmesi veya ağı kendi çıkarları doğrultusunda yönlendirmesi mümkün olamamaktadır[5]. Bu durum doğru bilgiyi teyit eden düğümler arasındaki işbirliğini önemli kılmaktadır. Ayrıca bir ağda ne kadar çok düğüm bulunursa ağ o kadar merkezi olmayan bir yapıya sahip olur ve doğru bilgiyi teyit edecek düğümlerin %50'den fazla olma ihtimali artar. Burada sürecin güvenliği, emeğin / iş kanıtı (proof of work) yöntemi[6] ile sağlanmaktadır. Emeğin kanıtı, özetleme işlemi sonucunda ortaya çıkan özet kodun bulunabilmesi için başına belirli sayıda 0 bit olan bir değerin konarak ilgili özet değerin taranması ve bulunması işlemidir. Emeğin kanıtı ile düğümlerin işlem geçmişi tüm kullanıcılara açıktır ve herkesçe izlenebilmektedir. Bu sayede sistemde yapılan işlemlerin düğümler tarafından teyit edilerek devamlılığı sağlanabilmektedir (Nakamoto, 2008; ARMA International Educational Foundation (AIEF), 2019, ss. 12-14; Demirkan, 2021, ss. 45-47).

## 2.1.Blokzincir Teknolojisinin Yapısı

Veri tabanları aşağıda gösterildiği gibi üç şekilde ifade edilebilir:




**Şekil 1.** Blokzincir Ağ Yapısı

- *Merkezi yapı*, kişiler veya kurumların kayıtları kendi bünyelerinde veya kontrolleri altında tuttuğu yapıyı temsil eder. Bu sayede ilgili kayıtlar üzerinde hüküm kurma veya ilgili kayıtlar doğrultusunda işlem gerçekleştirme hakkı da bu kayıtları elinde bulunduran kesimlerce saklı tutlmaktadır (TÜBİTAK, 2018; Ünal ve Uluyol, 2020, s. 172; AIEF, 2019, s. 10; Yapıcı ve diğerleri, 2021, s. 460).

[4] Bizans Hata Toleransı (Byzantine Fault Tolerance), bilgisayar terminolojisinde dağıtık sistemlerde fikir birliğini tesis etmeye yönelik zorluğu ifade etmede kullanılan bir kavramdır. Kavram, Bizans generalleri tarafından ulaklar vasıtasıyla gönderilen saldırı veya geri çekilme emirlerinde fikir birliğine varılmasını ele alır. Emirlerin ilgiliye ulaşmaması, hatalı ulaşması veya emri alanın aksi yönde davranması durumularında ortaya çıkabilecek olumsuzlukları engellemeye yönelik bir durumdur. Ulaklar tarafından iletilen emirleri alanların en az yarıdan fazlasının iletilen emir üzerinde mutabık kalarak hareket etmesini ve bu sayede yanlış davranışın önüne geçilmesini konu alır. Özetle mevcut yapıyı oluşturan kullanıcıların yarıdan fazlasının fikir birliğinin olduğu durumlarda emir doğru kabul edilir ve harekete geçilir. Fikir birliğinin olmadığı durumlarda ise sistem %51 saldırısına (bkz. Dipnot 5) açık hale gelebilir (Güven ve Şahinöz, 2018, ss. 63-64; AIEF, 2019, ss. 13-14; Demirkan, 2021, ss. 48-49).

[5] "%51 Saldırısı" olarak bilinen bu konuya çalışmanın ileriki safhalarında değinilmiştir.

[6] "Emeğin / İş İspatı" yöntemi dışında "Sahiplik İspatı" ve "Yetki İspatı" gibi farklı yöntemler de bulunmaktadır. Çalışmanın ileriki safhalarında bu konuya değinilmiştir.

- *Sorumluluğu dağıtılmış yapı*, kayıtların daha önceden belirlenmiş veri tabanlarına yerleştirildiği yapıdır. Kendi içinde uyumlu çalışan bu veri tabanları ile veri güvenliği büyük ölçüde sağlanmış olur (AIEF, 2019, s. 10; Yapıcı ve diğerleri, 2021, s. 460).
- *Dağıtık yapı* ise blokzincir yapısının merkeziyetsiz olması anlamına gelir. Yani bir devlet, hükümet, organ, kurum, birim veya kişiye bağlı olmayan bir yapıyı ifade eder. Bu tür yapılarda veri tabanını oluşturan kayıtların kopyaları farklı kullanıcıların elinde bulunur. İlgili kayıtlar üzerinde inisiyatif kullanılabilmesi için -protokole göre değişkenlik göstermekle beraber- kayıtları elinde bulunduran kullanıcıların çoğunluğunun veya tamamının kayıt üzerinde aynı düşüncede veya ortak paydada buluşması gerekir. Bu sayede belirli bir kişi veya zümre söz konusu kayıtlar ya da veri tabanı üzerinde tek başına bir yetki veya hükme sahip olamamaktadır (TÜBİTAK, 2018; AIEF, 2019, s. 10; Ünal ve Uluyol, 2020, s. 172; Yapıcı ve diğerleri, 2021, s. 460).

Merkezi olmayan dağıtık yapıdaki blokzincir teknolojisi iki temel kavramdan oluşmaktadır: (1) Blokları oluşturan kayıtlar ve (2) Blokzinciri oluşturan bloklar (TÜBİTAK, 2018).

Kayıtlar, ilgili blokta yer alan her türlü veridir ve blokzincir sisteminin tasarım şekline göre değişebilmektedir. Sanal para birimleri için para transfer bilgileri, ürün veri tabanı için ürün veya demirbaş bilgileri ya da herhangi bir şirkete bağlı müşterilerin bilgileri bu verilere örnek verilebilir (TÜBİTAK, 2018; Çetin, 2020, s. 67). Bloklar ise yukarıda bahsedilen kayıtların belirli aralıklarla yazıldığı defterlerdir. Bu defterlerin ne kadar kayıt içereceği ve bu kayıtların hangi işlemden geçtikten sonra blokları oluşturacağı sistemin tasarımına göre farklılık gösterebilir. Bloklar oluşturulurken sanal imza ve kriptografik algoritmalar kullanılmaktadır. Bir önceki bloğun özet algoritması (hash / özet değer)[7] ile bir sonraki bloğun özet algoritması birbirine bağlanmaktadır. Bu sayede bloklarda geriye dönük bir kaydı silme, değiştirme, çoğaltma veya ekleme ve çıkarma işlemleri yapılamamaktadır. Yapılmak istenmesi durumunda ise geçmiş işlemi teyit eden tüm kullanıcıların sonradan yapılan işlemi de teyit etmesi gerekmektedir ki bu daha önce de ifade edildiği üzere neredeyse imkânsızdır (TÜBİTAK, 2018; Çiçek ve Sağlık, 2019, ss. 146-147).

Brownworth tarafından oluşturulan blokzincir yapısında (Şekil 2); blokların (block) sırasını gösteren bir sayı ya da karakter, yalnızca bir kez kullanılabilen ve bir değeri ifade eden bir sayı (iz değeri / nonce[8]), kayıt altına alınan verinin girildiği bir alan (veri ve üst verisi / merkle kök değeri), önceki bloğun verisinin şifrelenerek

[7] Özet Algoritması (Hash / Zaman Damgası / Özet Değer / Güvenli Hash Algoritması (Security Hash Algorithm)), bir takım harf ve rakamlardan oluşan, elektronik bir veri için parmak izi olarak tanımlanabilir. Bloğa kaydedilen her bir karakterin ve bu kapsamda içeriğin hash değeri farklıdır, tektir ve değişmezdir (Brownworth, 2016). Hash Algoritması, türü fark etmeksizin verinin veya belgenin özgünlüğünü kanıtlamak için kullanılır. Bu algoritma belge, resim, metin veya yalnızca bir harf için aynı uzunlukta (64 karakter) sayı ve harflerden oluşan bir çıktı yaratır (Şekil 2'de bir örneği görülebilir) (Güven ve Şahinöz, 2018, s. 45). Blokzincir teknolojisinde ABD'nin şifreleme konusunda uzman olan Ulusal Güvenlik Ajansı (NSA-National Security Agency) tarafından geliştirilmiş olan SHA-256, SHA-512 gibi güvenlik algoritmaları kullanılmaktadır. Blokzincir ağının ilk bloğunda (buna Genesis blok da denir) önceki hash değeri (previous) olmadığı için bu alan 0000… şeklinde başlar (bakınız Şekil 2).

[8] Nonce, madencilik sürecinde sayaç olarak kullanılan tek kullanımlık rastgele bir sayıyı ifade eden değer (Güven ve Şahinöz, 2018, s. 62).

rakamlara döküldüğü bir sayı ya da karakter kümesi (prev) (zaman damgası / hash / özet değer / parmak izi) ile cari blokta yer alan verinin rakamlara döküldüğü veya çevrildiği bir diğer sayı kümesi yer almaktadır. Bir blok oluşturulduğunda "Mine[9]" butonuna basılarak bloğun benzersiz bir "nonce" ve "hash" değeri alması sağlanır. Bu şekilde bloklar silsile halinde blokzincirini oluşturmaktadır (Brownworth, 2016; Çiçek ve Sağlık, 2019, s. 146):

| Block | # | 1 |
|---|---|---|
| Nonce | 11316 | |
| Data | | |
| Prev | 00000000000000000000 | |
| Hash | 000000015783b764259b38 | |
| Mine | | |

| Block | # | 2 |
|---|---|---|
| Nonce | 35230 | |
| Data | | |
| Prev | 000000015783b764259b38 | |
| Hash | 00000011656a5d65465f65s | |
| Mine | | |

| Block | # | 3 |
|---|---|---|
| Nonce | 12937 | |
| Data | | |
| Prev | 00000011656a5d65465f65s | |
| Hash | 00000016sd6w9s55a2666d1 | |
| Mine | | |

**Şekil 2.** Blok Yapısı

Bir blokzincir yapısı aşağıdaki adımlar doğrultusunda oluşmaktadır (Çiçek ve Sağlık, 2019, s. 145):

- Yapılan işlemler, kayıt defterindeki bir blok içerisine kaydedilir,
- Blok, ağdaki her katılımcıya yayınlanır,
- Ağdaki katılımcılar tarafından işlemin doğruluğu teyit edilir[10],
- İşlem tüm katılımcılar tarafından onaylandıktan sonra zincire eklenir,
- Ağdaki katılımcılar tarafından işlemin aşamaları ve zincirin son hali kontrol edilir.

## 2.2.Blokzincir Teknolojisi Mutabakat Yapıları

Blokzincir ağlarının tümü dağıtıktır (merkezi olmayan) ve değişmezlik, güvenlilik ve güvenirlik özelliklerine sahiptir (Zhang, 2019, s. 279). Buna rağmen hepsinin ortaya çıkış amaçları veya projeleri farklı olabilir. Bu farklılıklara müzik eseri sahiplerinin eserlerinin yer aldığı platformlar, kripto para alışverişlerinde kullanılan platformlar veya öğrenci bilgilerinin veya insan kaynakları departmalarının kayıtlarını içeren platformlar örnek verilebilir. Her bir blokzincir ağı, proje amacına uygun olarak kendi içinde farklı özellikleri barındırabilir. Farklı amaçlar doğrultusunda o ağa özgü belirlenen kurallar uygulanır. Bu kurallar sayesinde çift harcamaların veya olası saldırıların önüne geçilerek dağıtık defterlerin bütünlüğü ve güvenliği

[9] To Mine: Kazımak, çıkarmak (Cambridge Dictionary, 2023).

[10] Teyit işlemi, blokzincirde bir önceki bloğa ait hash değerinin bir sonraki bloktaki değer ile doğrulanması şeklinde yapılmaktadır. Fakat bu işlemin bir blokzincir ağındaki blok sayısının fazlalığı düşünüldüğünde her blok için tek tek yapılması mümkün değildir. Örneğin Bitcoin blokzincir ağında 30.08.2023 tarihi itibariyle oluşturulmuş blok sayısı 805.520 adettir (13.05.2022 tarihinde bu sayı 736.325'tir) (Bitcoin (BTC) price stats…, 2022). Bu sebeple bu hash değerlerinin doğrulanmasında *Merkle Kök Değeri* kullanılmaktadır. Merkle Kök Değeri, blok içerisine kaydedilen hash değerlerinin ikişerli gruplar halinde ve yukarılara çıktıkça katlanarak toplanmasıyla hesaplanır. Ters ağaç şeklinde tasavvur edilebilecek bu yapının en üstüne gelindiğinde, tüm hesaplamalar yapıldıktan sonra Merkle Kökü ortaya çıkmış olur. Daha sonraki onay süreçlerinde artık blokların hash değerleri değil ortaya daha önce çıkarılmış olan Merkle Kök değerleri kullanılır. Böylece zaman tasarrufu sağlanmış olur (Güven ve Şahinöz, 2018, ss. 56-60).

sağlanabilir. Kurallar ise mutabakat algoritmaları aracılığıyla uygulanır. Ağda bulunan düğümlerin, blokları güncellemek için fikir birliğine varmaları, fikir birliğinin oluşturulması içinse ağın kurallarının önceden belirlenmiş olması gereklidir. Bu kuralların uygulanmasında mutabakat algoritmaları kullanılır.

Mutabakat algoritmaları, düğümler tarafından işlem oluşturulma ve bu işlemlerin doğrulanma şekillerini belirlemektedir. Bu algoritmaları kısaca tanımlayacak olursak:

- *Emeğin kanıtı / İş kanıtı algoritması*, en yaygın kullanılan algoritmadır. Bir düğüm yeni bir blok oluşturmak istediğinde diğer tüm düğümlerin onayını alması gerekir. Bu onay esnasında tüm düğümler bir bloğun önceki blok ile olan bağını yani özet değerlerini kontrol etmek ve bu doğrultuda işleme onay vermekle yükümlüdür. Bu sayede işlem kesinleşir ve ilgili bloklar meydana gelir. Bu bloklar matematik işlemlerinin çözümü ile oluşur. Bu faaliyete madencilik, işlemi yapanlara da madenci denir (Güven ve Şahinöz, 2018, ss. 64-67). Emeğin kanıtı algoritması, madencilerin matematik problemilerini çözmeleri neticesinde ilgili kripto para birimi ile ödüllendirildikleri mekanizmadır. Yapılan işin kanıtı olarak ödül kullanıcılara aktarılır. Bu algoritmanın sorunu, problem çözümünde yoğun enerji kullanımı ve yüksek nitelikte bilgisayar donanımı gerektirmesi sebepleriyle işlem maliyetlerinin yüksek olmasıdır (National Institute of Standards and Technology (NIST), 2018, ss. 19-21; Çiçek ve Sağlık, 2019, ss. 147-148; Lemieux, 2016, s. 13; Metin, 2021, ss. 68-69).
- *Sahipliğin kanıtı / Teminat kanıtı algoritması / Varlığın kanıtı,* yeni bir bloğu yaratacak kullanıcının blokzincir ağı ile ilişkili kripto varlıktan belirli oranda sahip olması veya ilgili varlığı belirli oranda taahhüt etmesi beklenir. Diğer bir deyişle, kullanıcıların herhangi bir veri veya belge için çevrim içi dağıtık bir varlığın sahibi olduklarını kanıtlaması gerekir. Bu sayede blokzincir ağındaki belgeleri güvenli ve anonim bir şekilde onaylayabilirler. Algoritmanın işleyişi gereği, emeğin kanıtı algoritmasına göre daha az işlem ve enerji gerektirir. Bu sebeple maliyeti düşüktür (NIST, 2018, ss. 21-23; Çiçek ve Sağlık, 2019, s. 148; Demirkan, 2021, ss. 47-48; Metin, 2021, ss. 70-71).
- *Yetkinin kanıtı / Kimliğin kanıtı algoritması*, bu algoritmada düğümlerin gerçek dünyadaki kimlik bilgileri bilinmektedir. Her işlem öncesi düğümlerin kimlik bilgilerini doğrulamaları gerekmektedir. Doğrulamalar neticesinde düğümler tarafından yeni bloklar yaratılabilir (NIST, 2018, s. 23; Çiçek ve Sağlık, 2019, ss. 148-149).
- *Delege edilmiş hisse kanıtı algoritması*, ilgili blokzincirde yer alacak blokları doğrulamak için belirli bir grubun diğer tüm düğümler adına delege edilmesi / belirlenmesi anlamına gelir. Seçme işlemi sahip olunan hisse veya kripto para birimi başına oy şeklinde gerçekleşir (NIST, 2018, s. 25; AIEF, 2019, ss. 12-13; Metin, 2021, ss. 71-72).

Genellikle her blokzincir ağında farklı ve tek bir mutabakat yapısı kullanılmaktadır. Örneğin Bitcoin blokzincir ağında emeğin kanıtı, Ethereum blokzincir ağında sahipliğin kanıtı gibi. Fakat son zamanlarda blokzincir ağlarındaki riskleri daha da azaltmak veya en aza indirgemek için hibrid mutabakat yapılarının kullanımı da ortaya çıkmıştır. Bu kapsamda örneğin Decred[11] adlı blokzincir ağı emeğin kanıtı ve sahipliğin kanıtı mutabakat yapılarını bir arada kullanmaktadır. Her iki yapının olumlu taraflarını barındıran bu ağın işleyişinde düğümler tarafından öncelikle emeğin kanıtı kapsamında madencilik yapılarak blokların oluşması sağlanır, daha sonra sahipliğin kanıtı kapsamında söz konusu blokların düğümler tarafından onaylanıp onaylanmamasına karar verilir (Sharma, 2020).

### 2.3.Blokzincir Teknolojisi Türleri

Blokzincir teknolojisi, türleri bakımından bazı kaynaklarda açık ve özel olmak üzere ikiye (Çiçek ve Sağlık, 2019, s. 147; Metin, 2021, s. 73), bazı kaynaklarda ise genel (açık-public), izinli (permissioned) ve özel (gizli-private) olmak üzere üçe (Bhatia ve Wright de Hernandez, 2019, s. 76; National Archives and Records Administration (NARA), 2019, s. 6) ayrılmaktadır. *Açık blokzincir ağları*, "bütünüyle izin gerektirmeyen ağlar" ve "kısmen izin gerektirmeyen ağlar", *özel blokzincir ağları* ise, "kısmen izin gerektiren ağlar" ve "bütünüyle izin gerektiren ağlar" olmak üzere iki kısımda değerlendirilmektedir (Çiçek ve Sağlık, 2019, s. 147; Metin, 2021, ss. 73-75). *Açık ağlar*, herkesin katılabildiği ve genellikle çok fazla katılımcının dâhil olduğu ağlardır. Bu ağlar, yaygın olarak kripto para birimlerinin kullanıldığı ağlardır. *İzinli ağlar*, belirli kesimlere yöneliktir. Bankalar tarafından kendi aralarında güncel nakit rezervleri gibi hassas bilgilerin paylaşılması amacıyla kurulan ağlar buna örnek verilebilir. *Özel ağlar* ise sıkı denetim altında olan ve genellikle gizli veya korumalı bilginin paylaşıldığı ağlardır. Bu ağlar çoğunlukla kurumlar arasında güvenilir ve özel işlemler için kurulmaktadır (Bhatia ve Wright de Hernandez, 2019, s. 76; NARA, 2019, ss. 6-7).

### 2.4.Blokzincir Teknolojisinde Güvenlik

Blokzincir ağlarında güvenliğin ve gizliliğin sağlanması için şifreleme işlemleri çift aşamalı yani asimetrik olarak yapılır. Asimetrik şifreleme ile birbirine bağlı veya birbirini tamamlayıcı nitelikte iki anahtarla güvenliğin derecesi artırılabilmiştir. Bu anahtarlardan birincisi *genel (açık) anahtardır* (public key) ve veriyi ya da mesajı şifrelemede kullanılır. Genel ve özel anahtar oluşturmak için e-imza[12] gereklidir. Diğeri ise *özel (gizli) anahtardır* (private key) ve bu anahtarı oluşturmak için güvenli hash algoritması kullanılır. Açık anahtar ile şifrelenen veri / mesaj özel anahtar ile çözülür. Gizli veriyi gönderen kişi, karşı tarafın açık anahtarını alır, bloğu / kaydı bu açık anahtar ile şifreler böylece belgeyi göndermiş olur. Karşı taraf ise gelen gizli veriyi özel anahtarı ile açar (Güven ve Şahinöz, 2018, ss. 45-49; Metin, 2021, ss. 52-53).

[11] https://decred.org/

[12] E-imza, üretilen belgenin / içeriğin özgün olduğu ve belirli bir kişiye ait olduğunun teyit edildiği anlamını taşır. Gizli anahtar ile oluşturulan belge elektronik imzalanmış anlamına gelir. Gizli anahtar ile belgeyi hazırlayan kullanıcı açık anahtarını mesajı iletmek istediği (karşı) tarafa verir. Karşı taraf bu anahtar ile mesajın içeriğine erişebilir (Güven ve Şahinöz, 2018, ss. 48-49).

Blokzincir ağlarındaki madencilik işlemleri eş zamanlı olarak farklı düğümler tarafından yapıldığından bazen farklı düğümler aynı sonuca aynı zamanlarda erişir ve bu sayede iki veya daha fazla blok aynı anda oluşur. Bu duruma *çatallaşma (forking)* denir (Güven ve Şahinöz, 2018, ss. 68-71). Çatallaşma ile oluşan ana blok dışındaki blok(lar) *ikincil zincir (secondary chain)* olarak adlandırılır (Lemieux, 2017a, s. 426; Çiçek ve Sağlık, 2019, s. 162). Çatallaşma kendi içinde aşağıdaki gibi farklılaşmaktadır (Güven ve Şahinöz, 2018, ss. 69-74; NIST, 2018, ss. 28-30; Metin, 2021, ss. 80-83):

- Gönüllü Çatallaşma (Soft Forking),
- Zorunlu Çatallaşma (Hard Forking),
- Yetim Blok (Orphan Block).

Blokzincir teknolojisi her ne kadar dağıtık yapıda kurgulansa ve tüm katılımcıların onayı ile işlemler güvenlik doğrulamaları ve e-imza ile gerçekleştirilse de bazı güvenlik sorunlarını da bünyesinde barındırmaktadır. Bu sorunlar başlıklar halinde aşağıdaki gibidir (Lemieux, 2017a, ss. 420-423):

- %51 Saldırısı ya da Güvenlik Açığı (51% Attack),
- Kullanıcıların özel anahtarlarının fiziki veya elektronik ortamda başkalarının eline geçmesi,
- Kullanıcıların açık ve özel anahtarlarının savaş, doğal afet, yanlışlıkla silinme veya elektrik kesintisi gibi sebeplerle kaybolması (Cryptographic Key Loss),
- Mutabakat Mekanizmasının Geciktirilmesi (Timing Errors and Attacks) (Güven ve Şahinöz, 2018, ss. 63-64; Metin, 2021, ss. 77-78),
- Ortadaki Adam Saldırısı (Man-in-the Middle Attacks),
- SYN Saldırısı (SYN Flood Attacks),
- Çift Harcama (Double-Spending),
- Sybil Saldırısı (Sybil Attacks).

## 2.5.Blokzincir Teknolojisinde Uygulama Örnekleri

2008 yılından bu yana popülerliği artan blokzincir teknolojisinin yukarıda bahsi geçen bazı sorunları olsa da teknolojik potansiyelinin yüksek olduğu ve yakın gelecekte farklı alanlarda uygulanabilir türlerinin geliştirileceği ile ilgili olumlu düşünceler ve gelişmeler de bulunmaktadır. Örneğin 2017 yılında yapılan bir çalışmada, blokzincir teknolojisinin güncel yaşama adaptasyonunun blokzincir 1.0, 2.0 ve 3.0 olmak üzere üç aşamadan oluştuğu ve 2017 öncesinde teknolojinin birinci aşamasında olduğu ifade edilmektedir. Çalışmaya göre *blokzincir 1.0*, çevrim içi kripto paralar aşamasıdır ve en büyük örneği her gün binlerce işlem yapılan güncel Bitcoin sistemidir (Bitcoin (BTC) price stats…, 2022). *Blokzincir 2.0* (güncel olarak içinde

bulunduğumuz aşama olarak da ifade edebiliriz), bu aşamada akıllı sözleşmeler kurulmaktadır. Ayrıca finansal kayıtlar, kamu belgeleri ve mülkiyet kayıtları da bu aşamada tutulmaktadır veya tutlmasına yönelik çalışmalar yapılmaktadır. *Blokzincir 3.0*'da ise blokzincir teknolojisi bilim, tıp ve eğitim alanına doğru genişleyecektir. Bu aşamada, kurumlar ve şirketler tarafından sahip olunan gizli ve kontrollü bilgi, açık ve dağıtık hale gelecektir. Örneğin hasta bilgilerinin yer aldığı sistemin blokzincir ağında kurulması ve hangi bilgilerin paylaşılabileceğine hastaların kendilerinin karar vermesi gibi (Hoy, 2017, ss. 275-276).

Sağlık alanındaki çalışmalara ilişkin örnek bir uygulama hâlihazırda bulunmaktadır. Çiçek ve Sağlık'ın Lemieux'den aktardığına göre; Estonya'da, hasta verilerinin de yer aldığı sağlık kayıtları bir veri tabanına yüklenmekte, bu kayıtlar eXtended Markup Language (XML) formatında e-imza ile imzalanarak iz değerleri yapısında saklanmaktadır. Bu şekilde oluşturulan tüm kayıtlar aynı şekilde muhafaza edilerek iz değerleri alınmaktadır. Bu işlemlerin tüm kayıtları Structured Query Language (SQL) formatında, kütük dosyası (log kaydı) olarak system dışına çıkarılmakta ve güvenli ortamlarda muhafaza edilmektedir. Bu şekilde günlük 40 bin doküman ve yaklaşık bir milyon işlemin gerçekleştirildiği ifade edilmektedir (Çiçek ve Sağlık, 2019, s. 155).

İsveç Tapu Dairesinde (Lantmäteriet) ise tapu işlemlerinin özel bir blokzincir ağından yürütülmesi ile ilgili bir pilot çalışma yapılmıştır. Bu kapsamda bir yıl içerisinde kâğıt masraflarından yaklaşık 106 milyon Amerikan Doları tutarında tasarruf sağlanmıştır. Aynı zamanda dolandırıcılık ihtimali sıfıra indirilmiş ve tapu işlemlerindeki hız oldukça artmıştır[13] (Lemieux, 2017a, ss. 408-410). Projedeki uygulamaya göre tapu işlemi şu şekilde gerçekleşmektedir: Bir tapu sözleşmesi esnasında satıcı ilanına alıcı teklif verir, alıcı ile satıcı alışverişte anlaşır, banka alışveriş için yeterli alıcı bakiyesini teyit eder, banka miktarı satıcıya iletir ve tapu müdürlüğü alışverişi tasdik eder. Burada blokzincir teknolojisi kapsamında akıllı sözleşmeler kullanılır (Çiçek ve Sağlık, 2019, s. 156).

Akıllı sözleşmeler, iki taraf arasında sözleşmeye konu eylemleri otomatikleştiren komut dosyalarıdır. Bu sözleşmeler, yasal dil, ilave şartlar veya anlaşmalar içermez. Sözleşmelerin içerisinde, belirtilen koşullar oluştuğunda / karşılandığında eylemlerin otomatik olarak gerçekleşmesini sağlayan kodlar bulunmaktadır (NIST, 2019, s. 32). E-belge türü olarak blokzincirlerde üretilen bu sözleşmeler, fiziki raflarda saklanan geleneksel sözleşmelerden farklı olarak dağıtık halde blokzincirler içerisinde saklanmaktadır. Bunun yanında akıllı sözleşmeler, dünya genelinde henüz hukuki anlamda geçerli bir delil niteliğinde belge olarak görülmemektedir. Ayrıca bu sözleşmelerin bilgisayar teknolojileri kapsamında teknik anlamda (hangi tür kodların belge olarak kabul edileceği ile ilgili) henüz üzerinde mutabık kalınamamış noktaları bulunmaktadır. Daha da önemlisi örneğin Ethereum protokolünde tanımlı akıllı sözleşmelerde güvenlik açıklarının olduğu da tespit edilmiştir (Çiçek ve Sağlık, 2019, s. 157).

[13] İsveç Krallığı, blokzincir teknolojisi ile tapu kayıt işlemlerini sürdürmeyi planlasa da diğer taraftan İsveç Savunma Bakanlığı'nın kendi sorumluluk alanı çerçevesinde arazi işlemlerinde ıslak imza almasını gerektiren mevzuat halen yürürlüktedir (Lemieux, 2017a, s. 418).

Tapu kayıt işlemlerinin blokzincir ağına taşınması ve o platformdan sürdürülmesi ile ilgili başka bir pilot proje 2016 yılında ABD'nin Georgia Eyaleti tarafından yürütülmüştür. Proje kapsamında gayrimenkullerin alım satım işlemleri ile ilişkili kredi ve noter işlemlerinin blokzincir ağı üzerinden yürütülmesi planlanmıştır. Bunun dışında sağlık hizmetleri kayıtlarının ve yeni arsaların blokzincir ağlarına kaydedilmesi ve işlemlerin buralardan yürütülmesi gibi farklı birçok proje, dünyanın farklı bölgelerindeki hükümetler tarafından hâlihazırda planlanmaktadır (Lemieux, 2016, s. 12).

Bu kapsamda University of British Columbia ve CNPQ UFSM Ged/A Digital Records Research Group şemsiyesi altında, altı araştırmacı tarafından, 2017 Mayıs-Eylül tarihleri arasında, "Zincirdeki Kayıtlar[14]" projesine bağlı olarak Brezilya'nın Pelotas Belediyesi'nde, "Brezilya'da Tapu İşlemlerinin Blokzincirde Saklanması" konulu bir pilot çalışma gerçekleştirilmiştir. Proje;

- tapu işlemlerinde blokzincir teknolojisinin nasıl kullanıldığı,
- hangi blokzincir platformunun kullanıldığı,
- blokzincir teknolojisinin hangi yönleriyle tapu işlemlerine katkı sağladığı,
- blokzincir teknolojisinin kullanımı sebebiyle karşılaşılan hukuki konular,
- blokzincir teknolojisinin Brezilya vatandaşlarına katkısı / etkisi,
- blokzincir teknolojisinin tapu işlemlerinin doğruluğunun sağlanmasını ve kayıtların uzun süreli korunmasını nasıl etkilediği

gibi başlıklar çevresinde yürütülmüştür. Araştırmada blokzincir teknolojisi aracılığıyla gerçekleştirilen tapu işlemlerine ilişkin kayıtların kanıt olarak kabul edilebilirliği, doğruluğu, bütünlüğü ile uzun vadeli muhafaza ve erişilebilirliği irdelenmiştir. Bu sebeple esasen arşivsel bakış açısıyla bir değerlendirme de yapılmıştır. Değerlendirme neticesinde, tapu işlemlerinde blokzincir teknolojisinin kullanılmasının verimlilik, işlem sürelerinde kısalma, maliyetlerde azalma, işlem güvenliğinde artış gibi potansiyel faydaları bulunsa da teknik anlamda (kütük dosyası gibi) halen daha geliştirilmesi gereken taraflarının olduğu, hukuki anlamda kanıt niteliğine henüz haiz olamayacağı (mevzuat değişiklikleri gerektireceği), ilgili dosyalara uzun vadeli erişimde sorunların çıkabileceği tespit edilmiştir. Ayrıca tapu işlemlerinde şeffaflığın ve kamu hesap verebilirliğinin şu an tam olarak tesis edilemeyeceği belirtilerek bunun vatandaşların hak kaybına uğramasına sebep olabileceği ifade edilmiştir. Ayrıca hukuki, idari ve işlem usulleri bağlamında güncel süreçlerde değişiklikler yapılması gerekeceği belirtilmiştir. Fakat bu sorunlar sebebiyle blokzincir teknolojisinin kullanımının geriye bırakılması yerine geliştirilmeye dönük bu tür çalışmaların daha fazla yapılmasının faydalı olacağı da ifade edilmiştir (Lemieux ve diğerleri, 2018, ss. 16-17, s. 31).

Tapu işlemleri özelinde blokzincir teknolojisinde değinilmesi gereken bir husus daha bulunmaktadır.

[14] Records in the Chain.

Blokzincir teknolojisinde oluşturulacak akıllı sözleşmeler ile yapılacak tapu işlemleri sonucu oluşacak blokzincir ağı, aynı mülke ilişkin daha sonra kurulacak yeni bir akıllı sözleşme ve bu kapsamda yapılacak işlem sonucunda aynı ağda mecburi bir çatallaşmayı ortaya çıkarabilir. Mecburi çatallaşmada iki farklı ağ işlemlerine devam eder. Bu durumun tapu kayıtlarında karmaşa ortaya çıkabileceği endişeleri bulunmaktadır (Bhatia ve Wright de Hernandez, 2019, s. 79). Fakat çözüm olarak tapu işlemlerine ilişkin kayıtlarda doğruluk, şeffaflık ve güvenliğin sağlanması, mülk sahipliğinin ve işlem doğruluğunun teyit edilmesi için parallel bir blokzincir ağının ya da platformun daha kurulabileceğinden bahsedilmektedir (Lemieux ve diğerleri, 2018, s. 8).

Bu yöntem çatallaşma sonucunda ortaya çıkan farklı ağlardan hangisinin (geçmişten gelen) gerçek ağ olduğunu ortaya çıkarmak için de kullanılabilir. Fakat bu kez de farklı platformların oluşması ve bunların konuşabilirliği sorunu ortaya çıkabilir. Örneğin tapu işlemlerinde kullanılmak üzere ilgili kamu kurumu tarafından geliştirilecek platformun Ethereum, Hyperledger, Bitcoin gibi diğer platformlar (NARA, 2019, 7-8) ile konuşabilir olması, mutabakat yapılarının belirlenmesi konuları gündeme gelecektir. Yukarıda bahsedilen Brezilya örneğinde de buna dikkat edilerek proje kapsamında bir platform geliştirilmiş, ancak çalışma sonucunda ilgili platformun ulusal tapu işlemlerinin gerçekleştirilmesinde gerekli temel özellikleri barındırması, diğer platformlarla konuşabilirliği, kayıtların başka platformlara kayıpsız ve sorunsuz aktarılabilirliği ile mutabakat yapılarının dikkate alınması gerektiği özellikle belirtilmiştir. Buna ragmen halen daha mutabakat yapıları bazında geliştirilmesi gereken hususların olduğu da ifade edilmiştir (Lemieux ve diğerleri, 2018, ss. 10-16, ss. 24-25).

Diğer taraftan eş zamanlı olarak blokzincir teknolojisi tabanlı arama motorları da geliştirilmektedir. Semantik web ve ilgili konularda faaliyet gösteren Aviv Digital[15] adlı şirketin kurucu üyesi ve teknoloji konusunda yaygın blog platformu Medium.com'da yayınlanan "*Blockchain-Based Search Engines: All You Need to Know"* adlı makalenin yazarı Rithesh Raghavan'a göre blokzincir tabanlı arama motorlarının çalışma mantığı şu şekildedir; kullanıcı blokzincir tabanlı bir arama motorunda bir anahtar kelimeyi aratır, arama motoru sonuçları göstermek için ağda yer alan dağıtık defterlerin tamamını araştırır ve kullanıcının karşısına getirir. Bu arada aramanın ayrıntıları şifrelenir ve dağıtık defterlerde saklanır. Blokzincir teknolojisinin felsefesine uygun olarak ağda yer alan her bir düğüm arama hizmetine katkı sağlamış olur. Bu arama motorları, diğer blokzincir uygulamalarında olduğu gibi merkezi bir kontrol mekanizmasına sahip değildir. Herhangi bir şirket kullanıcıların verilerine, arama geçmişlerine veya ilişkili bilgilerine erişim sağlayamamaktadır. Kullanıcıların verileri şifrelenmiş şekilde blokzincir ağında muhafaza edilmektedir (Raghavan, 2019). Böylece kullanıcılar Google, Microsoft veya Yandex gibi arama motoru şirketleri yerine verilerini kendileri kontrol edebilmektedirler. En popüler blokzincir tabanlı arama motorları arasında Nebulas[16], Presearch[17],

[15] https://avivdigital.in/.
[16] https://www.nebulas.io/docs/NebulasTechnicalWhitepaper.pdf.
[17] https://whitepaper.io/coin/presearch.

DeSearch[18], BitClave Decentralized[19], YaCy Project[20] ve FAROO (SeekStorm[21]) bulunmaktadır (Rezaee ve diğerleri, 2021, s. 2).

Son olarak içerisinde barındırdığı özellikler sayesinde farklı alanlarda faaliyet gösteren çok uluslu şirketlere veya farklı iş süreçlerine yönelik esnek çözümler üretebilen Arweave ve Hyperledger adlı teknolojilerden de bahsetmek gerekir:

a) Arweave, merkezi olmayan bir blokzincir depolama ağıdır. Bu ağ, sisteme bağlı olan ve ilave sanal depolama alanı bulunan kullanıcıların alanlarını ağdaki diğer kullanıcıların kullanımına açar. Sistem, açık defter teknolojisinde kalıcı ve dağıtık / merkeziyetsiz bir veri depolama ağı olarak tanımlanır. 2018 yılı Haziran ayında resmi olarak faaliyete geçen projede, kullanıcılar kendi sayfalarını oluşturabilir ve içerisinde kalıcı olarak dosyalarını depolayabilir. Sistem, ağda yer alan verilerin süresiz olarak saklanması için kullanıcılarına / madencilerine token kazandırmakta ve "AR" adlı kripto para ile ödeme yapmaktadır. Diğer blokzincir teknolojilerinin aksine bu teknolojide kullanıcılar çatallaşmaya giderek kendi çatallarını oluşturup buradan işlem yapmaya devam ettikçe ilave token kazanabilmektedir. Bu sayede daha adil bir ödül kazanma süreci ortaya çıkması hedeflenmektedir. Projede ayrıca kullanıcıların web uygulamaları geliştirebileceği ve ifade özgürlüğüne sahip dijital sayfa ve uygulama alanı olarak tanımlanan PermaWeb adlı bir web aracı ile kullanıcıların katkılarıyla gelişecek kolektif bir bilgi merkezi olarak tanımlanan ArWiki adlı bir diğer paylaşım platform bulunmaktadır (Arweave, 2023; The Arweave Project, 2023).

b) Hyperledger, 2015 yılında Linux Vakfı tarafından duyurulan açık kaynak kodlu bir blokzincir projesidir. Amacı, farklı alanlarda iş odaklı kullanılabilecek blokzincir çerçeveleri oluşturmak, bu işlemleri mali ve teknik yönden desteklemek, ilgililerde blokzincir teknolojisi konusunda farkındalık yaratmak ve onları eğitmek için tarafsız, açık ve topluluk odaklı alt yapılar sağlamaktır. Hyperledger, kripto paralara konu olmayan bir proje olarak tarif edilmektedir. Hyperledger'i diğer projelerden ayıran bazı özellikleri şu şekilde tanımlanabilir: (1) İzinli bir blokzincir ağıdır ve kimlik yönetimi modülü ile kimlik doğrulaması yapılmasını gerektirir. (2) Ağ üzerinden kullanıcı grubu tanımlanarak veri gizliliği sağlanabilir. (3) Modüler bir mimariye sahiptir ve kullanıcılar ihtiyaçları doğrultusunda istedikleri modülleri kendi araçlarında kullanabilirler. Bu sebeple farklı sektörlerden kullanıcı ihtiyaçlarına yanıt verebilecek esnekliğe sahiptir. (4) Java, Go, NodeJS gibi farklı yazılım dilleri ile geliştirmeye açık bir teknolojidir. (5) Tüm işlemler ücretsizdir. Herhangi bir lisanslama ücreti bulunmamaktadır. (6) Kullanıcılar izinli işlem yapabildiklerinden açık blokzincir ağlarına göre daha hızlı işlem yapılabilme kapasitesine sahiptir (Hyperledger, 2023a). İşlemlerin kullanıcıdan kullanıcıya aracısız ve güvenlik odaklı gerçekleştirilmesi amacıyla kullanılan blokzincir teknolojisi ile açık kaynak kodlu bir yapı sunan Hyperledger projesinin yanyana gelmesi işlem güvenlikleri açısından soru

[18] https://medium.com/bitclave/desearch-feature-release-dev-update-f2ee2d43be96.
[19] https://medium.com/bitclave.
[20] https://yacy.net/.
[21] https://seekstorm.com/.

işaretleri doğursa da bu teknolojinin izinli, kullanıcıları önceden belirlenmiş ve kimlik kontrollü bir ağ olması söz konusu soru işaretlerini ortadan kaldırmaktadır.

Hyperledger teknolojisi ile (1) sözleşme süreçlerinin kısaltılması, kâğıt bazlı işlemlerin ortadan kaldırılması, dijital sistemlere güvenin artırılması, uzaktan çalışmanın kolaylaştırılması ve bu sayede zamandan, kâğıt israfından ve maliyetten tasarruf edilmesi, (2) blokzincir protokollerinin geliştirilmesi, şirketlerde açık kaynak statejilerinin yaygınlaştırılması ve bu sayede akıllı nesneler arasındaki işlem ve ödeme hızlarının artırılması, (3) küresel çapta şirketler arasında iş akışlarının otomatize edilmesi, ilişkileri temelinde küresel çapta şirketlerin birbirlerine daha hızlı bağlanması, birbirleriyle daha hızlı iletişim kurabilmesi ve veri paylaşımlarında güvenli ve özel ağların kurulması, bu sayede şirketler arasında kolay ve sürekli iletişimin sağlanması, güvenli ve özel veri depolama alanlarının yaratılması, (4) sigortacılar için raporlamanın kolaylaştırılması, düzenleyiciler için doğru ve zamanında raporlama yapılabilmesi ve bu raporlamalardan işe değer katan yeni içgörülerin kazanılması, böylece daha çok kaydın daha kısa zamanda gözden geçirilebilmesi, piyasa düzenleyiciler tarafından piyasa bilgilerinin doğru zamanda görülebilmesi, toplu ve otomatik veri akışının gerçek zamanlı ve verimli şekilde sağlanması, büyük sigorta şirketlerinin yıllık raporlama maliyetlerinden milyonlarca Amerikan Doları tasarruf edebilmesi vb. çok çeşitli konularda Fujitsu, Hitachi, Bosch, Walmart, Honeywell, British Columbia, Tech Mahindra gibi küresel çapta faaliyet gösteren farklı şirketler iş ve teknoloji geliştirmektedir (Hyperledger, 2023b).

Sonuç olarak blokzincir teknolojisinde sistem kişilere veya kurumlara bağlı değildir. Bunun yerine sistemin işleyişi için belirlenen mutabakat algoritmalarına ve her halükârda ağda yer alan tüm düğümlere bağlıdır. Bu sayede merkezi otorite ihtiyacı ortadan kalkmakta, kullanıcılar kendi ihtiyaçlarını kendileri çözebilir hale gelmektedir. Ethereum, Everledger gibi teknolojilerin[22] akıllı sözleşme oluşturma imkânları da bu serbestide önemli rol oynamaktadır. Zincir teknolojisinde dağıtık yapının bulunması, onay mekanizmasının algoritma doğrultusunda birden fazla veya her bir düğüme dayanması, matematik işlemlerinin zorluğu ve çift aşamalı şifreleme özellikleri ile işlemlerin anonim olarak yapılabilmesi gibi özellikler blokzincir ağında bulunan kullanıcıların mahremiyetini ve ağda yapılan işlemlere güveni bir ölçüde sağlanmıştır.

Bunların yanında blokzincir teknolojisinin arama motorları dışında bankacılık ve para transfer işlemleri, kıymetli evrakın oluşturulması ve muhafazası, elektronik ticaret ve ödeme işlemleri, hisse senetlerinin arzı ve ticareti, noter işlemleri, kişiler arası borçlanma ve dağıtık kredi arzı veya temini, bağışlar, bulut teknolojileri ve güvenli depolama[23] ve Web 3.0 teknolojilerinde de kullanılmaya başlandığını ifade etmek söz konusu güveni göstermesi açısından doğru olacaktır (TÜBİTAK, 2018; Raghavan, 2019).

[22] Bu teknolojilerin özelliklerine çalışmanın ilerleyen bölümlerinde değinilmiştir.

[23] Uluslararası kripto varlıkları piyasasını takip eden ve bu doğrultuda kullanıcılarına piyasa analizi, açık kaynak kod geliştirme gibi çeşitli hizmetler sunan Gecko Labs adlı şirketin web sitesinde "veri depolama" (storage) etiketine sahip blokzincir ağı ve / veya kripto para birimlerinin (örneğin; FIL, HOT, SOUL, BLZ vb.) 31.08.2023 tarihindeki toplam piyasa değeri 4,13 milyar Amerikan Doları civarındadır (Top storage coins…, 2023).

# 3. ARŞİVCİLİK VE BELGE YÖNETİMİNDE BLOKZİNCİR TEKNOLOJİSİNİN KULLANIMI VE BİLGİ GÜVENLİĞİ

Günümüzde e-devlet hizmetlerinin gelişmesiyle e-belgelerin kullanımı da artmıştır. Fakat teknoloji ilerledikçe elektronik ortamdaki risklerin paralel oranda artması bu alandaki faaliyetlerin geliştirilmesini elzem kılmaktadır. Bu durum arşivcilik ve belge yönetimi faaliyetlerinin bilgi ve iletişim teknolojilerindeki gelişmeler doğrultusunda düzenlenmesi ve gelişen dinamikler çerçevesinde sunulabilmesi için blokzincir gibi yeni nesil teknolojilerin arşivlerde muhtemel kullanım alanlarının tartışılmasını önemli kılmaktadır. Bu kapsamda çalışmada, blokzincir teknolojisi konusunda arşivcilik ve belge yönetimi bağlamında hâlihazırda gerçekleştirilen projeler ve uygulamalar incelenecek, blokzincir teknolojisinin bu faaliyetlere muhtemel katkıları ve bu faaliyetlerde bilgi güvenliği bağlamında ortaya çıkabilecek muhtemel zafiyetler TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, ISO 15489-1 Belge Yönetimi Standardı ve TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi Standardı doğrultusunda irdelenecektir.

## 3.1.Arşivcilik, Belge Yönetimi ve Blokzincir Teknolojisi

Arşivcilik ve belge yönetimi faaliyetlerinde dünyada önde gelen kurum, kuruluş ve araştırmacılar tarafından bu alanlar ile blokzincir teknolojilerini bir araya getiren çeşitli projeler veya çalışmalar planlanmakta ya da gerçekleştirilmektedir. Çalışma kapsamında öne çıkanlar incelenerek aşağıda sunulmuştur:

a) Birleşik Krallık Ulusal Arşivi (The National Archives) tarafından geliştirilen ARCHANGEL adlı bir proje bulunmaktadır. İngilizce kelime açılımı "Trusted Archives of Digital Public Documents" (Kamuya Açık Elektronik Belgelerin Güvenilir Arşivleri) olan bu proje; kamu arşivlerinde saklanan e-belgelerin uzun süreli bütünlüğünün sağlanması amacıyla oluşturulan merkezi olmayan bir platform olarak tanımlanmaktadır. Bir başka ifadeyle proje, kamu arşivlerindeki e-belgelerin kaynağını, bütünlüğünü doğrulamak ve sürekliliğini sağlamak için oluşturulmuş bir platformdur. Platform, hızlı bir dönüşüm ve değişim içerisine giren elektronik dünyanın gereklerine uygun olarak arşivcilik faaliyetlerinin adaptasyonunu amaçlamaktadır. Bu kapsamda güncel uygulamalardan farklı olarak merkezi olmayan bir güven modeli oluşturmak amacıyla kaynak içeriğini dağıtık defter teknolojisiyle birleştirmeyi planlamaktadır. Blokzincir teknolojisini kullanarak dijital verilerin güvenliğini ve belgelerin bütünlüğünü sağlayarak gelecek nesillere aktarmayı hedefleyen ARCHANGEL projesi, bu sayede blokzincir teknolojisinin kullanımı ile muhafaza altına alınan belgelerin tahrifata maruz kalmasının engellenebileceği görüşünü savunmaktadır (ARCHANGEL Trusted Digital Archives (ARCHANGEL), 2018).

Projede ayrıca veri tabanında yer alan video kayıtların formatlarının değiştirilse dahi izlerinin sürülebilmesi, içeriklerinin izinsiz değiştirilmesi durumunda bunların belirlenmesi veya içerik değiştirilmesinin önüne

geçilmesi amacıyla SHA-256 güvenlik algoritması ile PROV Standardının[24] kullanılması olasılıkları araştırılmaya devam etmektedir. Projede blokzincir teknolojilerinden Ethereum altyapısını kullanılmıştır. Bu kapsamda odak çalışma grubu belirlenmiş, grup vasıtasıyla e-belgelerin ilgili ağa aktarılması ve sonrasında bu belgelerin yönetimi amaçlı uygulamalar gerçekleştirilmiştir. Oluşturulan ağda yer alan belgelerin aranması ve doğrulanması için çalışmaların devam etmesi gerektiği belirtilmektedir. Bu kapsamda örneğin ağda yer alan kullanıcılara belge doğrulama faaliyetleri (madenciliği) sebebiyle çeşitli rozet vb. ödüller ile ödeme yapılmasının bu işlemleri teşvik edeceği, blokzincir teknolojisinin arşivlerin dijital dönüşüm sürecinde yararlı olabileceği fakat bu teknolojinin tam anlamıyla arşivcilik faaliyetlerinde kullanılması için henüz erken olduğu ve bu alanda daha çok araştırmanın yapılması gerektiği belirtilmektedir (ARCHANGEL, 2018; Green ve diğerleri, 2018, s. 6; Bell ve diğerleri, 2019, ss. 5-7).

b) Alanda etkin bir diğer kuruluş olan Amerikan Kütüphaneciler Derneği (ALA) web sayfasında "geleceğin kütüphanesi" (library of the future) olarak adlandırılan bir bölüm bulunmaktadır. Bu bölümde kütüphanecilik alanı ile ilgili güncel eğilimler paylaşılmaktadır. Burada ALA tarafından "blokzincir" konusu da işlenmiş ve bir rapor hazırlanarak kullanıcılara sunulmuştur. Rapora göre blokzincir teknolojisinin olumlu ve olumsuz özellikleri aşağıda ifade edilmiştir (American Library Association (ALA), 2017):

- Blokzincir teknolojisinin belge saklamaya uygun yapısı gereği, kamu kayıtlarının veya tarihi belgelerin mevcut belge saklama yöntemlerine bir alternatif olarak devletlerin ilgili kurumları tarafından blokzincir teknolojisine aktarılabilir.
- Blokzincir teknolojisi belge aktarma, depolama ve saklama gibi işlemlere ait maliyetleri düşürebilir. Belgenin doğruluğunu kanıtlayacak yöntemleri sunabilir ve herhangi bir sabotaj veya doğal afet durumunda söz konusu belgelerin yok olmasını engelleyebilir.
- İzin gerektirmeyen veya kısıtlandırılmamış blokzincir ağlarında izin gerektiren veya özel blokzincir ağları bulundurulabilir. Bu ağlara erişim ve bunlar üzerinde değişiklik yapma yetkisi belirli kullanıcılara tanımlanabilir. Bu sayede yetkisiz kullanıcıların yetkileri dışındaki belgelere erişimleri kısıtlanabilir.
- Blokzincir teknolojisinin dağıtık yapıdaki çalışma mantığı sebebiyle farklı bölgelerde veya konumlarda (mevcut Elektronik Belge Yönetim Sistemleri gibi) aralıksız ve yüksek miktarda elektrik enerjisine ihtiyaç duyulabilir (Fernandez, 2021, s. 9).
- Blokzincir teknolojisinin bilgisayar ve ağ depolama araçlarına gereksinim duyması sebebiyle maliyet anlamında her kurum için uygun olmayabilir.

[24] PROV (Provenans) Standardı, Dünya Çapında Ağ Konsorsiyumu (World Wide Web Consortium (W3C)) tarafından geliştirilen bir standarttır. Web'te yer alan içeriğin bütünlüğünü koruyarak değiş tokuşunu / alışverişini veya aktarımını desteklemeye yönelik bir veri modelidir. Kullanıcı nezdinde ilgili kaynağın kalitesi ve güvenirliliği hakkında bir değerlendirme oluşturmak için söz konusu içeriğin üretilmesinde yer alan varlık, kişi veya faaliyetler hakkındaki bilgileri içerir (World Wide…, 2013).

Aynı raporda blokzincir teknolojisinin hâlihazırda çözüm olarak kullanıldığı girişimlerden de bahsedilmektedir (ALA, 2017):

- Ethereum, geliştiricilerinin akıllı sözleşmeler oluşturabilmeleri için blokzincir ağında kendi uygulamalarını yazmalarına izin vermektedir. Bu akıllı sözleşmeler ile kullanıcılar, borçlarının veya bu türdeki işlemlerinin kayıtlarını tutabilmekte, belirli zamanda veya belirli olaylar gerçekleştiğinde daha önceden belirlenen işlemlerin gerçekleştirilmesi için talimatlar verebilmektedir.
- Everledger, bu veri tabanı teknolojisi ile kullanıcılar değerli varlıkların izini sürebilmektedir. Bir milyondan fazla elmasın kimlik numarası söz konusu sistemde bulunmaktadır. Bu sayede kullanıcılar, elmasların nereden çıkarıldığını ve çalıntı olup olmadığını kontrol edebilmektedir. Ethereum ve Everledger'in sunduğu akıllı sözleşme oluşturma imkânları sayesinde kullanıcılar borsa fiyatları, hava durumu bilgileri veya son dakika haberleri gibi farklı ve sistem dışı veriler ile akıllı sözleşmelerini ilişkilendirebilmektedir. Böylece kullanıcılar tarafından talimatı verilen dış veriler ile sözleşmelerinde yazan koşullar eşleştiğinde sözleşmelerin gerçekleşmesi sağlanmaktadır.
- Verisart, bu sistem sayesinde kullanıcılar blokzincir teknolojisini merkezi olmayan bir sanat veri tabanı olarak kullanabilmektedir. Bu zincirde kayıtlı her sanatsal parçaya eşsiz bir doğrulama kodu atanmakta ve bu sayede alıcılar ve ürün sahipleri söz konusu sanatsal parçaların doğruluğunu teyit edebilmekte ve kaynağını görebilmektedir.
- Block Verify, bu araç yüksek değere sahip ürünlerin doğruluğunun teyit edilebilmesine, alışverişlerin kayıtlarının tutulmasına, çalıntı ürünlerin izlerinin sürülmesine, sahte işlemlerin ve yine sahte ilaçların belirlenmesine olanak sağlamaktadır.
- Microsoft firması tarafından açık kaynak kodlu "Coco Framework Project" adlı bir proje geliştirilmiştir. Bu proje kapsamında Microsoft, şirketlerin bağlantılı oldukları veya birlikte iş yaptıkları tedarikçiler, müşteriler ve diğer üçüncü kişiler ile aralarındaki operasyonları veya işlemleri takip edebilecekleri kendi blokzincir ağlarını kurmalarına yardımcı olmaktadır.
- IBM, kendi adını taşıyan "IBM Blockchain" adlı blokzincir ağını kurmuştur. IBM blokzincir projesi kapsamında iki pilot çalışma gerçekleştirilmektedir. Birincisi, bankaların kullanımına yönelik hazırlanmış ve müşterilerin veri paylaşımını azaltmayı ve bu kapsamda kimlik doğrulamasını kolaylaştırmayı hedefleyen bir proje, ikincisi ise sosyal, çevresel veya ekonomik bir değeri olan ve kişiler, şirketler, aileler veya özel topluluklar tarafından edinilebilen ve yeşil (çevreci) varlık[25] olarak.

[25]Yeşil Varlık, çevreye duyarlı iş ve işlemlerde kullanılmak üzere finansal kuruluşlar tarafından sunulan çevreci faaliyetleri destekleyici ürünlerdir. Örneğin; yatırım fonları, yeşil kamu fonu, karbon fonları, afet bonosu fonları. Ayrıca rüzgâr çiftlikleri, güneş enerji parkları ve biyo-yakıt tesislerinin kurulumu ve karbon ayak izini düşürücü faaliyetlerin gerçekleştirilmesi için sağlanan finansman, bu kapsamda verilen krediler, destekler ve teşvikler, yapılan araç, ev-bina, iş ve karbon sigortaları gibi. Bu finansman türleri ve varlıklar, günümüzde sürdürülebilir kalkınmanın önemli bir ayağını oluşturmaktadır (Kuloğlu ve Öncel, 2015, s. 3, s. 6).

da tanımlanan varlıkların ticaretinin yapılabildiği bir platformdur.

- Sony şirketi, öğrenci bilgilerinin yer aldığı bir blokzincir veri tabanı üzerine çalışmalar yapmaktadır. Bu veri tabanında öğrencilerin kayıt belgeleri, derse devam durumları, aldıkları sonuçlar, dereceler veya notları ve öğretmenler tarafından planlanan ders programları bulunmaktadır. Bu bilgilerin, ilgili öğrencilerin bir sonraki aşamada gidecekleri okulların veya (öğrenimlerinin son aşamalarında bulunmaları halinde ise) işe başlayacakları kurum ile paylaşılabileceği ve bu sayede öğrenci geçmişinin tek elden ve doğruluğu teyitli olarak ilgili makamlara sunulabileceği bir platform hedeflenmektedir.
- Southern New Hempshire University, çok sayıdaki mezununun sahip olduğu geleneksel belgelerinin üstünde genişletilmiş bir tanıtım kartı niteliğinde blokzincir tabanlı elektronik bir veri tabanı oluşturmayı planlamaktadır. Söz konusu platform, mezunların öğrencilik hayatı boyunca sahip olduğu notlar, diplomalar veya yeterlilikler gibi bilgi ve belgeler dışında öğrencilerin yaşam boyu öğrenme odaklı edindikleri sertifikalar, dâhil oldukları etkinlikler, kazandıkları deneyimler ve başarılar gibi genel bir akademik belge niteliğindedir.

Blokzincir teknolojisi ile kullanıcılar veya tüm insanlık yakın gelecekte daha kolay bir şekilde kişisel verilerini, doğum ve ölüm belgelerini, tapu kayıtlarını, sahip oldukları diğer kayıtları, varlıkları veya belgeleri muhafaza edebilecek ve dış dünyadan koruyabileceklerdir. Aynı zamanda istedikleri kurum veya kuruluş (hastane, işveren, banka vb.) ile istedikleri kadarını, istedikleri süre zarfı için paylaşabileceklerdir. Öte yandan Ethereum ve Everledger gibi hizmetlerdeki akıllı sözleşme özellikleri, bir kullanıcının bir ürüne kaç kez erişebileceğini, bu ürünü kaç kez paylaşabileceğini veya kopyalayabileceğini kontrol ederek en nihayetinde içeriğe ve fikri mülkiyete erişim şekillerini de bir dönüşüm içerisine sokacaktır. Fakat bu nokta arşiv belgelerinin telif hakkı bağlamında kullanımını, hatta veri tabanlarının kullanımını etkileyebilir. Sonuç olarak bulunduğumuz dönem için hükümetler veya kamu kurumları blokzincir teknolojisine karşılıklı tartışma veya fikir alışverişi bazında ilgi ve alaka göstermektedir. Bu sürecin resmi düzeyde daha somut hale getirilmesi ve gerekli adımların atılması blokzincir teknolojisine kamu uyumunu kolaylaştıracaktır (ALA, 2017).

c) Avrupa Birliği'nin (AB) ilgili kuruluşlarının da blokzincir konusunda çeşitli çalışmaları bulunmaktadır. Bunlardan birisi DECODE[26] adlı bir projedir. Bu proje ile AB üyesi ülkelerde yaşayan vatandaşların verilerinin yer aldığı bir blokzincir veri tabanı kurulmak istenmektedir. Bu veri tabanında AB vatandaşlarının, kişisel verilerinin ve özelliklerinin, yeterliliklerinin kurum, kuruluş ve özel şirketlerle ne kadarının paylaşılıp paylaşılmayacağının seçebilmesi sağlanacaktır. Böylece kişisel verilerin korunmasının yanı sıra kamu kurum ve kuruluşları ile özel şirketlerin vatandaşlara yönelik hizmet ve ürün geliştirmelerinin

[26] The European Union's Decentralised Citizen Owned Data Ecosystem (DECODE). https://decodeproject.eu/.

devamlılığının da sağlanması hedeflenmektedir. Bu kapsamda örneğin Barcelona ve Amsterdam şehirlerinde pilot projeler gerçekleştirilmiştir (The European Unions's…, 2017).

d) Amerikan Saint Jose State University'de (SJSU) School of Library and Information Science bölümünün müdürü Prof. Dr. Sandra Hirsh'in Institute of Museum and Library Services tarafından ödüllendirilen blokzincir teknolojisi konulu projesi bulunmaktadır[27]. Proje, kütüphane hizmetlerinin geliştirilmesinde blokzincir teknolojilerinin kullanılması için blokzincir teknolojilerinde uzman kişiler ile kütüphane profesyonellerini buluşturan bir platform kurulması üzerinedir. Proje kapsamında blokzincir teknolojisi ile kütüphanelerdeki potansiyel uygulama alanlarını buluşturmayı amaçlayan bir web sitesi kurulmuş[28], Haziran 2018'de blokzincir standartları, yasal sorunlar, güvenlik sorunları ile kimlik doğrulama ve koruma konularında "Kütüphane 2.0" başlıklı sanal bir konferans düzenlenmiştir. Ağustos 2018'de, alanında uzman 26 katılımcıyla "kütüphanelerde blokzincir uygulamaları için fırsatlar" konulu bir "Blokzincir Ulusal Forumu" gerçekleştirilmiştir (San Jose State University (SJSU), 2017).

2019 yılının ikinci çeyreğinde kullanıcılara, bilgi profesyonellerine ve ilgililere blokzincir üzerine çevrimiçi kurs (MOOC-Massive Open Online Courses) verilmiştir. Bu kurs içeriklerine ilgili üniversitenin "SJSU ScholarWorks" başlıklı web sayfasından[29] halen erişim sağlanabilmektedir. Öğrenciler bu kurslarda Hyperledger[30] kullanarak blokzincir oluşturmayı öğrenebilmektedirler (SJSU, 2022).

Diğer taraftan proje kapsamında blokzincir teknolojisinin kütüphanecilik ve belge yönetimi için potansiyel yararları ve sorunlar ile buralarda kullanım alanları belirlenmiştir (Zhang, 2019, ss. 279-280):

1) Potansiyel yararları:

- Belgelerin bütünlüğü ve değişmezliği,
- Güvenilirlik ve yasal kanıt oluşturabilirliği,
- Belgelerin birden fazla kopyasının bulunması,
- Tüm düğümlerce teyit gerektiren bir ağ olması,
- Veri tabanı açısından gizlilik ve performans sunması.

2) Potansiyel sorunlar:

- Dağıtık yapının bir sahibinin veya otoritesinin olmaması,
- Ağın yüzde ellisinden fazlasını kontrol eden düğümlerin saldırısına uğraması halinde verilerin kaybolabilmesi,

[27] Proje kütüphaneler ile blokzincir teknolojisini bağdaştırmasına rağmen arşivcilik ve belge yönetimi ile bağdaştırılabilecek alanları bulunması sebebiyle çalışmaya dâhil edilmiştir.
[28] https://ischoolblogs.sjsu.edu/blockchains/.
[29] https://scholarworks.sjsu.edu/.
[30] Bakınız madde (e).

- Ağdaki sürecin ve üst verilerin yönetimine ilişkin dokümantasyon eksiklerinin bulunması,
- Gereken teknolojinin her kullanıcının karşılayabileceği seviyenin üzerinde bir maliyete sahip olması,
- Depolama kapasitelerinin yetersiz ve ağdaki işlem hızlarının yavaş kalabilmesi.

3) Potansiyel kullanım alanları:

- Dijital koruma ve izlemede,
- Nesneleri, araçları ve hizmetleri paylaşabilecek topluluk temelli koleksiyonlarda,
- E-belgelerin kurumlar arası ödünç sistemlerinde,
- Kimlik bilgilerinin doğrulanması işlemlerinde,
- Kurum kartı oluşturulmasında,
- Provenansın ve özgünlüğün önem arz ettiği arşivlerde veya koleksiyonlarda,
- Kurum faaliyetleri sonucunda oluşan belgelerin muhafazasında,
- Kurumsal veri yönetiminde,
- Fikri mülkiyet haklarının gözetimi veya korunmasında.

SJSU'nun proje kapsamında hazırlanan "*bilgi profesyonelleri için blokzincirler*" başlıklı web sayfasında blokzincir teknolojisinin kütüphanelerde somut kullanım alanları aşağıdaki başlıklarda ifade edilmiştir (SJSU, 2017; Çetin, 2020, s. 70):

- Kütüphaneler için geliştirilmiş üst veri sistemlerinin kurgulanması,
- Dijital hakların korunması,
- Kişiler ve / veya kurumlar arası dijital veri veya ürün paylaşımı,
- Şehir yaşamının blokzincir teknolojileriyle geliştirilmesinde katkı sağlayıcı rol oynanması,
- Kişilere becerileri veya aldıkları çevrim içi eğitimlere karşılık olarak dijital rozetler verilmesi (bu sayede beceri, başarı, yetkinlik ve kalite doğrulanabilir ve bunlara ilişkin bir havuz oluşturulabilir).

e) Blokzincir teknolojisi ile bağlantılı olarak değiştirilemez para / token (Non-Fungible Token-NFT) teknolojisi de arşivcilik ve belge yönetiminin ilgi alanına girmektedir. NFT, blokzincir teknolojisiyle dağıtık defterlerde depolanan sanal, benzersiz ve değiştirilemez dijital varlık olarak tanımlanabilir (LaFountain, 2021, s. 22). Herhangi bir sanatsal ürün, video oyunu, video kesiti, fotoğraf, resim, simge vb. ürün NFT olarak adlandırılabilir (BTC Türk Bilgi Platformu, 2021; Fernandez, 2021, s. 7). NFT'ler aracılığıyla dijital varlıklar üzerinde hak sahipliği, dijital varlığın değeri ve benzersizliği belgelendirilmektedir. Benzersizliği ve bütünlüğü blokzincir teknolojisi ile güvence altına alınan NFT'lere ilişkin işlemler (NFT'lerin yaşam

döngüleri boyunca) dağıtık defterlerde kaydedilmekte, izlenmekte ve korunmaktadır (LaFountain, 2021, s. 22).

Dijital varlıkların sahipliğini, benzersizliğini ve bütünlüğünü kanıtlamada kullanılan NFT'lerin yüksek işlem ücretleri ve yavaş işlem hızları gibi sorunları bulunmaktadır. Ayrıca, NFT sanal müzayede veya değişim platformlarının birçoğu Ethereum tabanlıdır. Bu platformlarda işlem (aracılık) maliyetleri oldukça yüksektir ve işlem hacmine göre miktarlar anlık olarak değişkenlik gösterebilmektedir. Söz konusu platformlarda tercihli işlem hızları da sunulmaktadır. Fakat alternatif olarak sunulan işlem hızlarında da maliyetler oldukça yüksektir. NFT'lerin bir diğer olumsuz veya eksik tarafı da özellikle finans, teknoloji veya kripto paralar bağlamında ulusal mevcut yasal düzenlemelerin eksik olması veya hiç olmamasıdır (LaFountain, 2021, s. 25). Arşivcilik bağlamında NFT'lerin kullanım alanları aşağıdaki gibi açıklanabilir:

- Nadir veya benzersiz belgelerin NFT'leri yaratılarak kullanıcılara bu ürünler sunulabilir. Bu sayede kullanıcılara farklı bir platform üzerinden de kullanıcı hizmeti verilmiş olur (Fernandez, 2021, s. 8; LaFountain, 2021, s. 23):
- Bağışçılar para bağışlamak veya çek yazmak (daha çok ülkemiz dışında, dünyanın farklı bölgelerinde geçerli) gibi geleneksel yöntemler yerine arşivlere NFT ürünlerini teklif edebilir (ilgili ülkede bulunan mevuzatın imkân vermesi halinde) (LaFountain, 2021, s. 23):
- İlgili ülke mevzuatının izin vermesi halinde arşivler tarafından gelir amaçlı NFT'ler üretilerek elektronik platformlardan müzayede şeklinde satışlar yapılabilir (Fernandez, 2021, s. 8; LaFountain, 2021, s. 23).

Dijital varlık haklarının korunmasında somut bir araç olarak kullanılabilecek NFT teknolojisinin temel ortaya çıkış nedenleri kişilerin benzersiz dijital varlıklara sahip olmak, bu varlıkları diledikleri gibi satmak ve bu varlıklardan asgari kârı elde etmek istemeleridir. Bu doğrultuda NFT'lerin arşivler bağlamında kullanım alanları veya yararları oldukça tartışmalıdır. Zira arşivlerdeki amacın burada yer alan varlıkların zarar görmesinin engellenerek olabildiğince fazla kullanıcıya sunulması veya kullandırılması olduğu düşünüldüğünde NFT'lerin bu amacın tam tersine hizmet ettiği görülmektedir. Bu kapsamda dijital varlık haklarının korunması dışında NFT kullanımının arşivlerde henüz yaygın bir kullanım alanı bulabileceği söylenemez (Fernandez, 2021, ss. 8-9).

Öte yandan tüm bu olumlu ve olumsuz örnekler sonucunda Lemieux'nun "*Evaluating the use of blockchain in land transactions: An archival science perspective"* adlı çalışmasında da belirttiği üzere; blokzincir tabanlı kayıt tutma sistemlerinin günümüzün koşulları için henüz yeni, standardizasyon olarak eksik, pilot projeler bağlamında aynı tür ve kaynaktaki kayıtlar arasında bile içerisinde tutarsızlıkları barındıran fakat bunlara rağmen gelişme olasılığı yüksek bir teknoloji olarak tanımlanmasında halen bir sakınca bulunmamaktadır (Lemieux, 2017a, s. 439).

### 3.2.Bilgi Güvenliği ve Blokzincir Teknolojisi

Son dönemde basılı, elektronik ve hibrit olarak oluşturulan belgelerin özellikle kamu kurumlarında elektronik ortamda yaratılması yönünde bir yönlendirme bulunmaktadır. Bu kapsamda 10 Haziran 2020 tarihinde Resmi Gazete'de yayımlanan "*Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik*"te yer alan şu ifade bu durumu desteklemektedir: Madde 4 (1) "Kamu kurum ve kuruluşlarınca resmî yazışmalar, elektronik ortamda e-Yazışma Teknik Rehberi'ne uygun olarak hazırlanan ve güvenli e-imza ile imzalanan belgelerle yapılır" (Resmi Yazışmalarda…, 2020). Bu süreç, kullanımı artarak devam eden e-belgelerde bilgi güvenliği konusunun daha somut ele alınmasını gerektirmektedir. Bu kapsamda oluşturulan ulusal ve uluslararası standartlar konuyu hem bilgi ve belge yönetimi hem de bilgi güvenliği açısından değerlendirmek için en doğru yol olacaktır.

TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardına göre bilgi güvenliği ilkeleri *gizlilik, bütünlük, kullanılabilirlik* başlıklarından oluşmaktadır (Güler ve Furat, 2022, s. 81; Türk Standartları Enstitüsü (TSE), 2022). Bu ilkeleri bozacak nitelikte durum veya davranışlar ise bilgi güvenliği ihlali anlamına gelmektedir.

Uygulamada bilgilerin elektronik ortamda depolanması veya sunucular / kullanıcılar arasında aktarımı esnasında yetki ve amaç dışı kullanımı veya yetkisiz kişilerin bu bilgilere erişimi bir bilgi güvenliği sorunu olarak değerlendirilir. Bunun yanında bilgi sistemlerinde gizlilik ihlalleri, bilgi bütünlüğünün bozulması, bilginin değiştirilmesi veya imhası, bilgiye yetkisiz erişim, bilginin yetkisiz kullanımı veya izinsiz ifşası gibi başlıklar da bilgi güvenliğinin konusunu oluşturmaktadır. Bilgi güvenliği ihlalleri, bilgi bütünlüğünün bozulması veya erişilebilirliğinin kısıtlanması halleri, yetkisiz veya üçüncü kişilerin bilgiye müdahalesi ile olabileceği gibi bilgi teknolojilerindeki değişimler kaynaklı da olabilir. Özetle bilgi güvenliği, bu gibi ihlalleri engellemeye yönelik faaliyetleri kapsamaktadır (Güler ve Furat, 2022, s. 81).

Arşivler bağlamında değerlendirildiğinde ise somut çıktılara ulaşabilmek açısından belge yönetimi ile bilgi güvenliği kavramları birlikte değerlendirilmelidir. Konuyu hem ulusal hem de uluslararası bağlamda değerlendirmek amacıyla TS ISO/IEC 27001, TS ISO 15489 ve TS 13298 Standartlarını *bilgi güvenliği* kavramı üzerinden bağdaştırdığımızda belgenin *özgünlüğü (orijinalliği), güvenirliliği (erişim hakları), bütünlüğü* ve *kullanılabilirliği (kullanım)* ilkeleri karşımıza çıkmaktadır (Lomas, 2010, s. 190; International Organization of Standardization (ISO) 2016; Güler ve Furat, 2022, s. 80; TSE, 2022).

Bir belgenin geçerliliğini belgenin *değişmezliği* ve *bütünlüğü* sağlar. İlgili belgeye sahip olan kurum, kuruluş veya kişinin *tarafsız* ve *güvenilir* olması ancak bu değişmezlik ve bütünlük özelliklerini belgelerinde barındırıyor olmasına bağlıdır. E-belgeler, kısa zamanlarda *büyük hacimlerde* üretilmektedir. Aynı zamanda *soyut* olmaları sebebiyle içeriği değiştirilmeye oldukça müsaittir. Bunun yanında *elektronik kayıt ortamları* ve *belge formatları* gün geçtikçe eskimektedir. Bu ve çalışmanın çeşitli bölümlerinde belirtilen benzer

özelliklerinden dolayı belgeler bilgi güvenliği açısından aşağıda belirtilen riskleri barındırması kaçınılmazdır (Collomosse ve diğerleri, 2018, s. 1; Güler ve Furat, 2022, s. 81; TSE, 2022):

- Belgelere müdahale edilmesi, belge içeriklerinin izinsiz, olağan durumlar dışında değiştirilmesi, belgelerin uygun olmayan tarafların eline geçmesi, yok edilmesi, uygun olmayan şartlarda bulundurlması ve içeriklerinin anlaşılamaz, eksik veya erişilemez duruma veya forma dönüşmesi / dönüştürülmesi, zaman geçtikçe (doğal yollarla) kayıt ortamlarında bozulma ve bu sebeplerle içeriğine erişilememesi.

### 3.2.1. Bilgi Güvenliği Bağlamında Arşivcilik ve Belge Yönetiminde Blokzincir Teknolojisi

TS ISO/IEC 27001 Standardında bilgi varlıkları için bir üst başlıkta belirtilen ilkelere ilave olarak belgenin özgünlüğü, hesap verebilirliği, inkâr edilemezliği ve güvenilirliği gibi özellikler de alt detayda açıklanmaktadır (Güler ve Furat, 2022, ss. 82-84).

TS 13298 no.lu Belge Yönetim Standardına göre ise belgenin *özgünlüğü, güvenirliliği, bütünlüğü* ve *kullanılabilirliği* belgenin geçerliliği için gerekli ilkelerdir. Bu ilkeler ışığında bir belgenin yok edilmemiş, içeriğinin tam ve değiştirilmemiş olması, yani oluşturulduğu haliyle kaydedilmiş ve muhafaza altına alınmış olması gerekir. Bu sayede belgenin *özgünlüğü* korunmuş olur. Belgenin bir diğer özelliği olan *güvenilirliği*, belgenin bütünlüğünün bozulmamış olması, belgenin oluşturulduğu formda bulunması ve içeriğinin değiştirilmemiş olması ile sağlanır. Belgenin *bütünlüğü*, belge içeriğinin konu bağlamından kopmamış olması (arşivsel bağının korunmuş olması), tamlığının bulunması (yazı ve altında imza bulunması gibi) ve üst verisi ile tanımlanabilir veya tamamlanabilir olması gibi özellikler ile sağlanabilir. Arşivsel bağ, konu birliği olan kayıtlar arasındaki ilişkiyi açıklar (Çiçek ve Sağlık, 2019, s. 165). Bu özellikleri yitiren belgeler güvenirliğini de yitirmiş olur. Belgenin erişilebilir olması, içeriğinin açık ve anlaşılır olması sayesinde ise belge *kullanılabilirliği* sağlanmış olur. Bu özelliklere haiz bir belge bir anlamda hukuki delil niteliğini de korumuş sayılır (Çiçek ve Sağlık, 2019, s. 152; Güler ve Furat, 2022, ss. 81-82; TSE, 2022).

Çalışma kapsamında belge yönetimi bağlamında bilgi güvenliği ilkelerini (1) belgeye erişim haklarını (*gizlilik*), (2) belgenin doğruluğunu ve tamlığını (*bütünlük*), (3) belgenin bulunduğu yerin belirli, içeriğinin anlaşılır, talep edildiğinde erişilebilir ve kullanılabilir olduğunu (*kullanılabilirlik / erişilebilirlik / süreklilik)*, (4) belgeyi oluşturan kişinin, belgenin oluşturulduğu tarihin ve içeriğinin gerçek ve doğru olduğunu (*orijinallik*) açıklayan ilkeler şeklinde ifade edebiliriz.

Bu doğrultuda blokzincir teknolojisinin bilgi güvenliği bağlamında ***Güvenilirlik*** */ Gizlilik / Erişim Hakları,* ***Özgünlük*** */ Orijinallik,* ***Bütünlük*** */ Tamlık* ve ***Kullanılabilirlik*** */ Erişilebilirlik / Süreklilik* ilkeleri çerçevesinde arşivlere sağladığı veya sağlayacağı katkılar ile arşivler açısından oluşturacağı zafiyetler aşağıda

iki başlık halinde açıklanmaktadır[31]:

1) Katkı Sağlayabileceği Özellikler

Blokzincir teknolojisinin dağıtık defter yapısına dayanması, üretilen verinin ve işlemlerin kurallar çerçevesinde kaydedilmesi (e-imza niteliğinde kullanıcı bazında özel anahtar ile imzalanması), bu işlem ve içeriklerin şeffaf, işlemlere özgü zaman damgaları sayesinde teyit edilebilir, değiştirilemez, anlık olarak izlenebilir olması ve özet değerleri vasıtasıyla muhafaza altında olması arşivler ve belge yönetimi açısından olumlu özelliklerdendir. Bunun yanında açık ve özel ağlar kurgulanabilmesi sayesinde amaca özgü ağların tasarlanabilmesi ve bu ağlarda bulunabilecek kullanıcıların ve yetkilerinin belirlenebilmesi yukarıdaki ilkelere ayrı ayrı katkı sağlamaktadır (Lemieux, 2017b, ss. 41-46; Çiçek ve Sağlık, 2019, ss. 143-148).

Ağda yer alacak belgelerin varsa üst verileri ve e-imzaları gibi belgeyi tamamlayıcı bileşenleri ile birlikte üretiminden itibaren kullanımı, teknolojik dönüşümü (tür, format vb.) ve erişimi aşamalarında herhangi bir değişime uğrama ihtimalleri dağıtık defter yapısı sayesinde engellenmektedir (Lemieux, 2017b, ss. 42-43, s.46; Çiçek ve Sağlık, 2019, ss. 152-153).

Özet değerleri aracılığıyla bir belgenin veya kaydın içinde bulunduğu bağlam ortaya çıkarılabilmektedir. Merkle ağaç yapısı sayesinde en alttaki kayıttan en yukarıdaki kaydı kapsayacak şekilde bir iz değeri oluşturularak konu birliği olan kayıt kümesinin özet değeri çıkarılabilmektedir. Bu imkân belgelerin arşivsel bağlarının korunmasını ve belgelerin bağlamı çerçevesinde değerlendirilmesini sağlamaktadır (Usta ve Doğantekin, 2018, s. 114). Ağda oluşturulan bloklar özet değerleri ile birbirine bağlı ve özel anahtarlar ile kilitli olması sebebiyle ağ içerisinde yer alan kayıtların silinmesi, değiştirilmesi, çoğaltılması veya söz konusu bloğa başka bir kayıt eklenmesi veya bloktan bir kaydın çıkarılması engellemektedir. Zaman damgalı kayıtlar bloklarda kronolojik olarak saklandığından işlemlerin çiftlenmesi gibi hatalı işlemler de engellenmektedir (TÜBİTAK, 2018; Çiçek ve Sağlık, 2019, s. 158-161).

Dağıtık yapı sebebiyle blokzincir ağları herhangi bir kişi veya kuruma bağlı değildir. Bu tür yapılarda veri tabanını oluşturan kayıtların kopyaları farklı kullanıcıların elinde bulunur. Bu özellik olağan dışı durumlarda veya afet zamanlarında arşivlere ait kayıtların kaybolmasını engellemektedir (TÜBİTAK, 2018; AIEF, 2019, s. 10; Ünal ve Uluyol, 2020, s. 172; Yapıcı ve diğerleri, 2021, s. 460).

Arşivler NFT'ler aracılığıyla, kullancıların yaptıkları işlem başına rozet veya token kazanmalarını, bu sayede kullanıcı katkısı ile veri tabanının dinamik kalmasını sağlayabilmektedir (ARCHANGEL, 2018; Green ve diğerleri, 2018, s. 6; Bell ve diğerleri, 2019, s. 7; LaFountain, 2021, s. 23). Ülke mevzuatı ve ödeme yöntemlerinin izin vermesi durumunda NFT'ler aracılığıyla bağış toplanabilmekte, arşivler özelinde kıymetli NFT ürünleri geliştirilerek elektronik müzayede (e-müzayede) yoluyla bu ürünler satılabilmekte ve buralara kaynak yaratılabilmektedir. NFT'ler sayesinde ayrıca dijital varlık haklarının korunması garanti altına

[31] Bazı olumlu ve olumsuz özellikler birden fazla ilkeyi kapsayabileceğinden ilkeler bazında ayrım yapılmamıştır.

alınabilmektedir (Fernandez, 2021, ss. 8-9).

Elektronik kaynakların arşivler veya ilgili kurumlar arasında aktarımının daha hızlı ve daha az maliyetle yapılabilmesi olanağı bulunmaktadır. Bu sistem sayesinde kurumlar arasında ödünç verme sistemlerinin kolaylaştırılması da mümkün hale gelmektedir. Bunlara destek olacak şekilde mutabakat yapıları belirlenebilir. Buna göre (varlığın kanıtı algoritması kullanılarak) işlem, zaman ve enerji maliyetleri azaltılabilir ve (kimliğin kanıtı algoritması kullanılarak) işlem doğrulukları artabilir (Lemieux, 2016, s. 13; NIST, 2018, ss. 21-23; LaFountain, 2021, s. 25).

Sanal kullanıcı kimlik (tanıtım) kartı oluşturularak kullanıcı bilgileri ve kullanıcıların bilgi veya arşiv kullanım verilerine erişim sağlanabilmesi, bu sayede kullanıcılara özgü hizmet geliştirilebilmesi imkânları bulunmaktadır. Ayrıca kullanıcıların bu kartlar ile farklı kurumlardan herhangi başka bir işleme ihtiyaç kalmadan hizmet alabilmeleri sağlanabilmektedir (ALA, 2017; Zhang, 2019, s. 280).

Dijital varlıkların korunarak gelecek nesillere aktarılması, kişiye ve topluluğa özel veri tabanlarının oluşturulması, kurumsal veri yönetimi ve -ülke mevzuatı izin vermesi durumunda- ağda bulunan kayıtların hukuki delil niteliğinde kullanılması bu teknoloji sayesinde mümkün kılınmaktadır (ALA, 2017; ARCHANGEL, 2018; Çiçek ve Sağlık, 2019, s. 152; Zhang, 2019, s. 279). Bu imkân ile "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" kapsamında kamuda ıslak imzalı gönderilen çok gizli, gizli ve hizmete özel damgalı belgelerin blokzincir ağlarından elektronik olarak gönderilmesi sağlanabilir.

Son olarak blokzincir ağlarında yüksek depolama ihtiyacı doğabilmekte[32] ve bu kapsamda maliyetler artabilmektedir. Bunun önüne geçebilmek adına ilgili blokzincir ağı, ağda bulunan kullanıcıların depolama alanlarını belirli teşviklerle kullanılabilir şekilde düzenleyebilmektedir. Bu sayede ağın dinamik kalması ve aynı zamanda kullanıcı katkısı ve ilgisi canlı tutulabilmektedir (LaFountain, 2021, s. 23; Hyperledger, 2023b; The Arweave Project, 2023).

2) Açık Konular (Zafiyet İhtimalleri)

Blokzincir teknolojisinin kuralları doğru tanımlanmadığı veya doğru uygulanmadığı durumlarda belgelerin tamlığına yönelik tehditler ortaya çıkabilmektedir. Tamlığın tam anlamıyla korunamadığı, yani bir belgenin üreticisi veya hukuki delil niteliğini sağlayacak tüm özelliklerini barındırmaması hallerinde bilgi / belge güvenirliliği de zarar görmektedir (Çiçek ve Sağlık, 2019, s. 152).

Bunun yanında ağda bulunan belgelerin arşivsel bağının net olarak ortaya çıkarılmasında eksiklikler oluşabilmektedir. Arşivsel bağın kurulabilmesi için gerekli üst verinin, belge işlem zamanlarının ve diğer işlemlere ilişkin kayıtların, olağan blok kayıtlarından farklı bir koruma yöntemine ihtiyaç duyması gerekebilir Bu durum çatallaşmaya sebep olabilmektedir (Lemieux, 2017b, s. 47).

[32] Bitcoin blokzincir ağının 30 Ağustıs 2023 tarihi itibariyle büyüklüğü 507,19 GB'tır (YCharts, 2023).

Merkeziyetsiz sistemde yer alan düğümlerin yarısından fazlasının dürüst olmadığı varsayımında sistemin üçüncü kişiler tarafından manipüle edilmesi mümkün hale gelebilmektedir. Ayrıca dağıtık yapıda veri tabanında yer alan kayıtlarda herhangi bir kişi veya kurumun tek başına bir inisiyatifi veya sahipliği bulunmadığından verilerin güvenliği tehdit altındadır (Güven ve Şahinöz, 2018, ss. 63-64; AIEF, 2019, ss. 13-14; Demirkan, 2021, ss. 48-49).

Blokzincir teknolojisinde işlem maliyetleri (NFT işlemleri de dâhil) artabilmektedir. Bununla beraber mutabakat yapısının gerçekleştirilmek istenen faaliyet çerçevesinde belirlenmediği durumlarda, örneğin işlem yoğunluğu sebebiyle işlem sürelerinde dramatik yavaşlamalar ortaya çıkabilmektedir. Bu kapsamda "varlığın kanıtı" ve "kimliğin kanıtı" mutabakatları arşivler açısından daha uygun mutabakat yapıları olarak öne çıkmaktadır. Birinde düğümlerin kimlik bilgileri belirlidir ve kimlik doğrulamaları ile işlem yapılabilmektedir. Diğerinde ise düğümlerin elinde bulunan varlıklar sayesinde ağda işlem yapabilmeleri imkânı doğmaktadır (Lemieux, 2016, s. 13; NIST, 2018, ss. 21-23; LaFountain, 2021, s. 25).

Son olarak, ağdaki süreç ve işlemlere ilişkin dokümantasyonun eksiklikler barındırabileceği, donanım gereksinimlerinde yüksek maliyetlerin ortaya çıkabileceği, tüm kullanıcıların bu ihtiyaçları karşılayabilecek imkânda olamayabileceği, yine ağda yüksek miktarda depolama alanı ihtiyaçlarının ve bu kapsamda maliyetlerin ortaya çıkabileceği, işlem hızlarının değişkenlik gösterebileceği, yoğunluk olduğu zamanlarda işlem hızlarının oldukça düşebileceği, özellikle madencilik işlemlerinde yüksek miktarlarda enerji ihtiyacının ortaya çıkabileceği, akıllı sözleşmelerde güvenlik açıkları ihtimalleri, bu ağlarda yer alan kayıtların hukuki anlamda kanıt niteliğinde kullanılamayabileceği (mevzuat değişiklik ihtiyaçları), farklı platformların oluşması ve bunların konuşabilirliğinde ya da kayıtların farklı platformlara aktarılmasında sorunların ortaya çıkabileceği gibi farklı sorun, ihtiyaç ve maliyetler bu teknolojinin mevcut şartlarda yaygınlaşmasının önündeki engeller olarak ifade edilebilir (ALA, 2017; Lemieux ve diğerleri, 2018, ss. 10-17, ss. 24-25, s. 31; NIST, 2018, ss. 19-21; Çiçek ve Sağlık, 2019, s. 157; Zhang, 2019; Fernandez, 2021, s. 9).

## 4. SONUÇ VE ÖNERİLER

### 4.1.Sonuç

Çalışmamız kapsamında *bilgi güvenliği bağlamında arşivcilik ve belge yönetiminde blokzincir teknolojisi* konusu nitel araştırma yöntemlerinden doküman analizi doğrultusunda kuramsal olarak ele alınmış, literatür taraması yapılmış, ilgili kavramların tanımı ve teknoloji özellikleri açıklanmış, mevcut ve olası uygulamalarda kullanım alanları irdelenmiştir. Bilgi güvenliği bağlamında arşivcilik ve belge yönetiminde blokzincir teknolojisini değerlendirebilmek adına ulusal ve uluslararası bilgi ve belge güvenliği standartları (TS ISO/IEC 27001, TS ISO 15489 ve TS 13298) ele alınmıştır. Bilgi güvenliği ve belge yönetimi kavramları bilginin / belgenin *özgünlüğü*, *güvenirliliği*, *bütünlüğü* ve *kullanılabilirliği* ilkeleri temelinde bağdaştırılmıştır. Akabinde blokzincir teknolojisinin teknoloji özellikleri ve sunduğu imkânlar ile söz konusu

ilkelerin gerektirdiği asgari şartların karşılıklı değerlendirmesi yapılarak teknolojinin ilgili faaliyetlere katkı sağlayabileceği özellikler ve zafiyet ihtimalleri ayrı ayrı açıklanmaya çalışılmıştır.

Sonuç olarak özellikleri sebebiyle verilerin bütünlüğünü, değişmezliğini, doğruluğunu, şeffaflığını ve tarafsızlığını sağlaması beklenen blokzincir teknolojisinin, potansiyel kullanım alanları öngörülmesi sebebiyle arşivcilik ve belge yönetimi faaliyetlerinde de kullanılabilirliğine yönelik araştırmaların bulunmasına rağmen bunların özellikle uygulamada henüz yeterli sonucu ve güveni vermediği belirlenmiştir. Arşivlerde riske edilemeyecek tek, nadir veya hayati öneme sahip kaynaklar veya kayıtlar bulunmaktadır. Bunun yanında elektronik doğan belgelerin oransal olarak arttığı da bir gerçektir. Bu durum yaygın kullanım alanı ve potansiyeli bulunan blokzincir teknolojisinin şu aşamada arşivcilik ve belge yönetimi faaliyetlerinde kullanımına temkinli yaklaşılmasını gerektirmektedir. Fakat temkinli yaklaşım, teknolojinin kullanım alanlarının zamanla artacağı gerçeğini de değiştirmemektedir. Blokzincir teknolojisi üzerine hem ulusal hem de uluslararası platformlarda yapılacak araştırmaların veya pilot çalışmaların artırılması (konu muhteviyatı sebebiyle disiplinler arası araştırmacıların birlikte çalışması gerektirebilir), gelişen teknolojik imkânların değerlendirilmesi ve bunların etkin kullanımının sağlanması bu alandaki faaliyetlerin çeşitlendirilmesi ve çağa ayak uydurulması açısından önem arz etmektedir.

## 4.2.Öneriler

Blokzincir teknolojisinin arşivler nezdinde mevcut kullanımının kısıtlı olması, arşivlerin bu teknoloji konusunda geleceğe dönük hazırlıklı olmalarına engel değildir. Arşivler ve ilgili kurumların faaliyetlerinin sürdürülebilirliğini bugünden sağlamak amacıyla aşağıda belirtilen öneriler birer önlem olarak değerlendirebilir:

- Arşivler ve ilgili kurumların bir kısım faaliyetlerinin yakın gelecekte blokzincir ağı üzerinden gerçekleştirilebileceği düşünülmektedir. Bu sebeple bu alanda çalışanların blokzincir teknolojileri konusunda farkındalıklarının oluşturulması ve varsa becerilerinin veya yetkinliklerinin geliştirilmesi gerekir (bu kapsamda ulusal bazda blokzincir teknolojisi üzerine araştırmalar yapan ve bir amaçları da toplumda bu konuda farkındalık yaratmak olan TÜBİTAK BİLGEM Blokzincir Araştırma Laboratuvarı, Blockchain Türkiye Platformu gibi farklı dernek, vakıf veya kuruluşlardan ya da blokzincir kulüplerinden (örneğin İstanbul Teknik Üniversitesi bünyesinde kurulmuş İTÜ Blockchain Kulübü)[33] destek alınabilir),
- Uygulama açısından bakıldığında bu tür kurumlarda bulunan kayıtlar (kullanıcı kayıtları dâhil) doğrulanabilir zaman damgaları ile blokzincir ağlarında saklanabilir. Kayıtlar veya bilgi hizmetleri bu ağlar vasıtasıyla kullanıcılar ve diğer kurumlar ile buluşturulabilir. Benzer işlevde veya ilişkili kurumlar, bu ağlar vasıtasıyla kaynak alışverişinde bulunabilir,

[33] https://blokzincir.bilgem.tubitak.gov.tr/, https://bctr.org/ ve https://itublockchain.com/.

- Arşivlere veya başka kurumlara güvenli (özel) veri aktarımı hatları kurulabilir,
- Kurumlar nezdinde bulunan kayıtların (envanter) takibinde kullanılabilir,
- Everledger ve Block Verify gibi sistemlerin sunduğu hizmetler arşiv faaliyetlerine örnek teşkil edebilir. Benzer sistemler ile değerli belgelerin / varlıkların izleri sürülebilir, tek ve nadir olan belgelerin / varlıkların kimlik numaraları sisteme kaydedilip, çoğaltılmalarının veya kopyalanmalarının önüne geçilebilir, bu sayede fikri mülkiyet hakları korunabilir,
- Değerli belgelerin kaynakları tanımlanabilir ve sahte olup olmadıkları belirlenebilir,
- Belgelerin tahrifatı engellenebilir veya tespit edilebilir,
- Kullanıcılara bilgi hizmetlerinden yararlanma sıklıkları vb. konular ışığında çevrim içi rozetler verilebilir. Bu rozetler ile farklı kaynaklara seçimli erişim hizmetleri sunulabilir. Kullanıcılar ile arşivler veya kurumlar arasında etkileşim ile kullanıcı sayıları artırılabilir, kullanıcıların ağlarda etkin rol oynamaları sağlanabilir,
- Kullanıcı paylaşımına konu olmayan kurum idari kayıtları özel bir blokzincir ağında tutulabilir,
- Arşivlerde bulunan belgeler / kayıtlar için üst veri sistemleri geliştirilebilir, özet değerler kümesi oluşturularak bu belgeler arası arşivsel bağ kurulması sağlanabilir,
- Veri tabanı özet değerleri farklı formatlarda indirilip kütük dosyaları şeklinde özel blokzincir ağlarında muhafaza edilebilir,
- Kullanıcıların doğrulanabilir kullanıcı kimlik kartı (merkezi olmayan bir kart) ile konuma bağlı kalmaksızın tüm arşivlerden veya ilgili kurumlardan ve bu kartın olası diğer avantajlarından yararlanması sağlanabilir,
- NFT'ler sayesinde dijital varlık mülkiyet hakları güvence altına alınabilir.

## KAYNAKÇA

American Library Association (ALA) (2017). Blockchain. Erişim adresi: https://www.ala.org/tools/future/trends/blockchain. Erişim tarihi: 10.01.2022.

ARCHANGEL Trusted Digital Archives (ARCHANGEL) (2018). Erişim adresi: https://www.archangel.ac.uk/. Erişim tarihi: 18.01.2022.

ARMA International Educational Foundation (AIEF) (2019). Blockchain technology and record keeping. Research Project Report, 30 May 2019. Prepared by Victoria L. Lemieux, Ph.D; Darra Hofman, JD, MSLS; Danielle Batista, BARM, MIS; and Alysha Joo, MASLIS: ARMA Canada Region.

Arslan, H. (2020). Bilişim teknolojilerinin dünü, bugünü ve geleceği. *Bilişim teknolojileri ve iletişim: Birey ve toplum güvenliği* içinde 81-93. Şeker, M. ve Korkut, C. (Ed.). Türkiye Bilimler Akademisi: Bilim ve Düşünce. ISBN: 9786052249482. https://doi.org/10.53478/tuba.2020.010

Arweave (2023). Erişim adresi: https://www.arweave.org/. Erişim tarihi: 04.07.2023.

Aviv Digital Institute (2022). Erişim adresi: https://avivdigital.in/. Erişim tarihi: 13.05.2022.

Bell, M., Green, A., Sheridan, J., Collomosse, J., Cooper, D., Bui, T., Thereaux, O., Higgins, J. (2019). Underscoring archival authenticity with blockchain technology. *Insights*, 32 (21), 1-7. https://doi.org/10.1629/uksg.470

Bhatia, S. ve Wright de Hernandez, A.D. (2019). Blockchain is already here. What does that mean for records management and archives?. *Journal of Archival Organization*, 16 (1), 75-84. https://doi.org/10.1080/15332748.2019.1655614

*Bilgi Edinme Hakkı Kanunu* (2003). Kanun Numarası: 4982, Resmi Gazete: 25269, 24 Ekim 2003. Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4982.pdf

Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2018). *5G ve ötesi beyaz kitap*. Erişim adresi: https://www.btk.gov.tr/uploads/announcements/5g-ve-otesi-beyaz-kitap/beyaz-kitap-son.pdf. Erişim tarihi: 25.06.2023.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2019). İnternetin riskleri ve zararları. Erişim adresi: https://internet.btk.gov.tr/internetin-riskleri-ve-zararlari. Erişim tarihi: 25.06.2023.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2022). 2021-4. Çeyrek Pazar Verileri Raporu. Erişim adresi: https://www.btk.gov.tr/uploads/pages/pazar-verileri/2021-4-pazar-verileri-raporu.pdf. Erişim tarihi: 25.06.2023.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2023a). 5G zirvesi BTK ev sahipliğinde düzenlendi. Erişim adresi: https://www.btk.gov.tr/haberler/5g-zirvesi-btk-ev-sahipliginde-duzenlendi. Erişim tarihi: 25.06.2023.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2023b). 2022-4. Çeyrek Pazar Verileri Raporu. Erişim adresi: https://www.btk.gov.tr/uploads/undefined/ceyrek-raporu-2022-4-c-eyrek-22-03-23-kurumdisi.pdf. Erişim tarihi: 25.06.2023.

Bilgi yönetimi ve bilgi güvenliği: eBelge-earşiv-edevlet-bulut bilişim-büyük veri-yapay zekâ (2019). B. Yalçınkaya, M. A. Ünal, B. Yılmaz ve F. Özdemirci (Ed.). Ankara Üniversitesi Yayınları. https://doi.org/10.33721/by.987197

BitClave Decentralized (2019). *Medium.com.* Erişim adresi: https://medium.com/bitclave Erişim tarihi: 08.05.2022.

Bitclave's Desearch Feature Release (Dev Update) (2018, Ağustos 1). *Medium.com.* Erişim adresi: https://medium.com/bitclave/desearch-feature-release-dev-update-f2ee2d43be96 Erişim tarihi: 10.05.2022.

Bitcoin (BTC) price stats and information (2022). Erişim adresi: https://bitinfocharts.com/bitcoin/. Erişim tarihi: 13.05.2022.

BlockstreetHQ Team (2018). *Before blockchain, there was distributed ledger technology* [Blog yazısı]. Erişim adresi: https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011 Erişim tarihi: 01.05.2022.

Brownworth, A. (2016). *Blockchain 101 - Görsel Demo* [Youtube]. Erişim adresi: https://www.youtube.com/AndersBrownworth

BTC Türk Bilgi Platformu (2021). *NFT Türleri: NFT dünyasının favorileri*. Erişim adresi: https://www.btcturk.com/bilgi-platformu/nft-turleri-nft-dunyasinin-favorileri/ Erişim tarihi: 09.07.2023.

Cambridge Dictionary (2023). *İngilizce-Türkçe Sözlük. Cambridge University Press & Assessment 2023*. Erişim adresi: https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce-t%C3%BCrk%C3%A7e/mine Erişim tarihi: 30.06.2023.

Chip Online (2022). *IP adresim nedir?*. Erişim adresi: https://www.chip.com.tr/ip-adresim-nedir Erişim tarihi: 13.05.2022.

Collomosse, J. Bui, T., Brown, A., Sheridan, J., Green, A., Bell, M., Fawcett, J., Higgins, J., Thereaux, O. (2018). *ARCHANGEL: Trusted Archives of Digital Digital Public Documents*. Canada: Halifax. Erişim adresi: http://personal.ee.surrey.ac.uk/Personal/J.Collomosse/pubs/Collomosse-DocEng-2018.pdf Erişim tarihi: 18.01.2022.

Çetin, B. (2020). Blokzincir teknolojisi bilgiye erişimde nasıl kullanılır? Mevcut durum ve potansiyeller. *Türk Kütüphaneciliği*, *34*(1), 65-70.

Çiçek, N. ve Sağlık, Ö. (2019). Blokzincir teknolojisinin elektronik belgelerin güvenilirliğinin korunmasında başarıya katkısı. *Bilgi yönetimi ve bilgi güvenliği: ebelge-earşiv-edevlet-bulut bilişim-büyük veri-yapay zekâ* içinde 141-170. B. Yalçınkaya, M. A. Ünal, B. Yılmaz ve F. Özdemirci (Ed.). Ankara Üniversitesi Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi. https://doi.org/10.33461/uybisbbd.598989

Demirkan, G. (2021). Blokzincir teknolojisi ve teknolojik determinizim çerçevesinde toplumsal değişime etkileri. [Yayınlanmamış Yüksek Lisans Tezi]. İstanbul Medipol Üniversitesi.

Emniyet Genel Müdürlüğü (2022). *Sosyal medya dolandırıcılığı*. Erişim adresi: https://www.egm.gov.tr/sosyal-medya-dolandiriciligi Erişim tarihi: 10.05.2022.

Fernandez, P. (2021). Non-fungible tokens and libraries. *Library Hi Tech News. 38*(4), 7-9. https://doi.org/10.1108/LHTN-08-2021-0048

Freedom of Information Act (2000). UK Public General Acts, c.36. Erişim adresi: http://www.legislation.gov.uk/ukpga/2000/36/ contents

Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2022). Resmi Gazete Tarih: 26 Nisan 2022, Sayı: 31821. Erişim adresi: https://www.mevzuat.gov.tr/MevzuatMetin/21.5.5529.pdf

Green, A., Bell, M., Sheridan, J., Collomosse, J., Bui, T., Brown, A., Fawcett, J., Thereaux, O., Tennison, J. (2018). Using blockchain to engender trust in public digital archives. IPRES 15th International Conference on Digital Preservation, 2018, September 21, Boston USA. https://doi.org/10.17605/OSF.IO/KEFJ8

Güler, C. ve Furat, F. (2022). Belge yönetimi ve arşiv uygulamalarının bilgi güvenliği ilkelerine katkısı: Kavramsal bir değerlendirme. *Türk Kütüphaneciliği*, *36*(1), 74-89. https://doi.org/10.24146/tk.1012325

Güven, V. ve Şahinöz E. (2018). *Blokzincir, kripto paralar, bitcoin: Satoshi dünyayı değiştiriyor*. Kronik Kitap.

Hoy, B. M. (2017). An introduction to the blockchain and its implications for libraries and medicine. *Medical Reference Services Quarterly*, *36*(3), 273-279. https://doi.org/10.1080/02763869.2017.1332261

Hyperledger (2023a). Erişim adresi: https://www.hyperledger.org/ Erişim tarihi: 04.07.2023.

Hyperledger (2023b). *Case studies.* Erişim adresi: https://www.hyperledger.org/learn/case-studies Erişim tarihi: 04.07.2023.

Hughes, E. (1993). *A cypherpunk's manifesto* [Blog yazısı]. Erişim adresi: https://www.activism.net/cypherpunk/manifesto.html

International Organization of Standardization (ISO) (2016). Information and Documentation - Records Management (ISO 15489-1: 2016). Switzerland.

İngiliz Ulusal Arşivleri (2023a). *Holding history: What is 'The National Archives'?.* Erişim adresi: https://www.nationalarchives.gov.uk/education/resources/holding-history/ Erişim tarihi: 30.06.2023.

İngiliz Ulusal Arşivleri (2023b). *What we hold.* Erişim adersi: https://www.nationalarchives.gov.uk/about/our-role/what-we-do/ Erişim tarihi: 30.06.2023.

Kıral, B. (2020). Nitel bir veri analiz yöntemi olarak doküman analizi. *Sosyal Bilimler Enstitüsü Dergisi*, *8*(15), 170-189. https://doi.org/10.33437/ksusbd.915548

Kim, B. (2020). Moving forward with digital disruption: What big data, IoT, synthetic biology, AI, blockchain, and platform businesses mean to libraries. *Library Technology Reports*, 56 (2), 1-37. American Library Association (ALA). Erişim adresi: https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1126&context=lib_ts_pubs Erişim tarihi: 30.06.2023.

Kuloğlu, E. ve Öncel, M. (2015). Yeşil finans uygulaması ve Türkiye'de uygulanabilirliği. *Gazi Üniversitesi Sosyal Bilimler Dergisi*, *2*(2), 2-19. https://doi.org/10.18069/fusbed.92578

LaFountain, C. (2021). Non-fungible tokens, libraries, and publishers. *Online Searcher: Information Discovery, Technology, Strategies*, *45(*4), 22-27. Erişim adresi: https://www.infotoday.com/OnlineSearcher/Articles/Features/NonFungible-Tokens-Libraries-and-Publishers-147856.shtml Erişim tarihi: 05.07.2023.

Lemieux, V. L. (2016). Blockchain for recordkeeping help or hype. The University of British Columbia: Technical Report No.1. Montreal: Social Sciences and Humanities Research Council of Canada. https://doi.org/10.13140/RG.2.2.28447.56488

Lemieux, V. L. (2017a). Evaluating the use of blockchain in land transactions: An archival science perspective. *European Property Law Journal*, *6*(3), 392-440. https://doi.org/10.1515/eplj-2017-0019

Lemieux, V. L. (2017b). Blockchain and distributed ledgers as trusted recordkeeping systems an archival theoretic evaluation framework. Future Technologies Conference, 29-30 November 2017, Kanada: Vancouver, 1-11. Erişim adresi: https://www.researchgate.net/publication/317433591 Erişim tarihi: 28.06.2023.

Lemieux, V. L., Lacombe, C., Flores, D. (2018). Real estate transaction recording in the blockchain in Brazil. (RCPLAC-01)-Case Study 1 Document Control Version History Version Date by Version Notes. https://doi.org/10.13140/RG.2.2.10569.85606

Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journal*, *20*(2), 182-198. https://doi.org/10.1108/09565691011064322

Metin, S. (2021). *Bilgi yönetimi ve blokzinciri teknolojisi*. Gazi Kitabevi.

National Archives and Records Administration (NARA) (2019). *Blockchain white paper*. Erişim adresi: https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Erişim adresi:

https://doi.org/10.2139/ssrn.3977007

National Institute of Standards and Technology (NIST) (2018). Blockchain technology overview. [Prepared by D. Yaga, P. Mell, N. Roby, K. Scarfone]. US Department of Commerce: NISTIR 8202. https://doi.org/10.6028/NIST.IR.8202

Nebulas (2018). *Nebulas technical whitepaper*. Erişim adresi: https://www.nebulas.io/docs/NebulasTechnicalWhitepaper.pdf Erişim tarihi: 02.05.2022.

NTV Haber (2019). *Sosyal medyadaki linke tıkladı, 49 bin TL dolandırıldı*. Erişim adresi: https://www.ntv.com.tr/turkiye/linke-tikladi-49-bin-tl-dolandirildi,CVDFLjUdD0-ATnsiloez8Q Erişim tarihi: 10.05.2022.

OECD (2023). *ICT access and usage by households and individuals*. Erişim adresi: https://stats.oecd.org/Index.aspx?DataSetCode=ICT_BUS# Erişim tarihi: 25.06.2023.

Onbirinci Kalkınma Planı 2019-2023 (2019). *T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı*. Erişim adresi: https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf Erişim tarihi: 25.06.2023.

Özdemirci, F. (2009). Arşivcilik ve arşivlerin geleceği: e-Dönüşüm sürecinde e-belge Yönetimi ve e-arşivler. 45. Kütüphane Haftası VEKAM Türkiye'de Arşivler ve Arşivcilik Uygulamaları, 2-3 Nisan 2009, Ankara, Bildiriler (Yay. Hazl. ve Editör: B. Z. Önen, M. Türkyılmaz, T. Berkes). Vehbi Koç ve Ankara Araştırmaları Merkezi. Erişim adresi: http://fahrettinozdemirci.com.tr/wp-content/uploads/2018/09/vekam.pdf Erişim tarihi: 20.06.2023.

Özdemirci, F. (2019). Milli e-arşiv bilgi sistemi ağı ve veri merkezi yapılanma önerisi: yenilikçi Teknolojiler-yeni nesil arşivciler-yapay zekâ ve ötesi. *Bilgi Yönetimi Dergisi*, *2*(2), 169-176. https://doi.org/10.33721/by.570634

Presearch (2018). *Presearch PRE technical whitepaper*. Erişim adresi: https://whitepaper.io/coin/presearch Erişim tarihi: 03.05.2022.

Raghavan, R. (2019, Aralık 28). *Blockchain-based search engines: All you need to know*. Erişim adresi: https://www.technology.org/2019/12/28/blockchain-based-search-engines-all-you-need-to-know/ Erişim tarihi: 24.05.2022.

Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik (2020). Resmi Gazete Tarih: 10 Haziran 2022, Sayı: 31151. Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/21.5.2646.pdf

Rezaee, E., Saghiri, A. M., Forestiero, A. (2021). A survey on blockchain-based search engines. *Applied Sciences*, *11*(15). https://doi.org/10.3390/app11157063

World Wide Web Consortium (W3C) (2013). *PROV-Overview: An overview of the PROV family of documents. W3C Working Group Note, 2013, Nisan 30.* Erişim adresi: https://www.w3.org/TR/prov-overview/ Erişim tarihi: 09.07.2023.

San Jose State University (SJSU) (2017). *Blockchains for the information profession: A project of SJSU iSchool*. Erişim adresi: https://ischoolblogs.sjsu.edu/blockchains/ Erişim tarihi: 01.05.2022.

San Jose State University (SJSU) (2022). *SJSU scholar works*. Erişim adresi: https://scholarworks.sjsu.edu/ Erişim tarihi: 13.05.2022.

SeekStorm Search API (2022). Erişim adresi: https://seekstorm.com/ Erişim tarihi: 13.05.2022.

Sert, T. (2020). *Blokzincirin çıkış felsefesi ne?* [Blog yazısı]. Erişim adresi: https://medium.com/turansert/blokzincirin-çıkış-felsefesi-ne-8185da57f46d

Sharma, T. K. (2020, Haziran 29). *A brief introduction to hybrid pow+pos consensus mechanism. Blockchain-Council.org*. Erişim adresi: https://www.blockchain-council.org/blockchain/a-brief-introduction-to-hybrid-powpos-consensus-mechanism/#:~:text=Hybrid%20PoW%2FPoS%20consensus%20mechanisms,weaknesses%20of%20e

ach%20consensus%20mechanism Erişim tarihi: 20.08.2023.

Stuart, H. ve Stornetta, W.S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3(*2), 99-111. https://doi.org/10.1007/bf00196791

Stuart, H. ve Stornetta, W.S. (1999). Secure names for bit-strings. CCS '97: Proceedings of the 4th ACM Conference on Computer and Communications Security, 1997, Nisan, 28-35. https://doi.org/10.1145/266420.266430

The Arweave Project (2023, Mart 2). Arweave is an evolutionary protocol. Medium.com. https://arweave.medium.com/arweave-is-an-evolutionary-protocol-e072f5e69eaa Erişim tarihi: 04.07.2023.

The European Union's Decentralised Citizen Owned Data Ecosystem (DECODE) (2017). *European Union's Horizon 2020 Programme.* Erişim adresi: https://decodeproject.eu/index.html Erişim tarihi: 20.01.2022.

Top storage coins by market cap (2023). *Gecko Labs*. Erişim adresi: https://www.coingecko.com/tr/categories/storage. Erişim tarihi: 31.08.2023.

Turkcell (2022). 5G teknolojisi. Erişim adresi: https://www.turkcell.com.tr/5g. Erişim tarihi: 25.06.2023.

TÜBİTAK BİLGEM UEKAE Blokzincir Araştırma Laboratuvarı (2018). *Blokzincir*. Erişim adresi: https://blokzincir.tubitak.gov.tr/blok-zincir.html

Türk Standardları Enstitüsü (TSE) (2015). Elektronik Belge ve Arşiv Yönetim Sistemi Standardı (TS 13298). Ankara.

Türk Standardları Enstitüsü (TSE) (2022). Bilgi Güvenliği Yönetim Sistemleri (TS ISO/IEC 27001). Ankara.

Türkiye Ekonomi Bankası (2022). *Dolandırıcılık yöntemleri.* Erişim adresi: https://www.teb.com.tr/guvenlik/dolandiricilik-yontemleri/ Erişim tarihi: 10.05.2022.

Usta, A. ve Doğantekin, S. (2018). *Blockchain 101 v2. Bankalararası Kart Merkezi. Güncellenmiş Versiyon*. Erişim adresi: https://bkm.com.tr/blockchain-101/ Erişim tarihi: 30.06.2023.

Ünal, G. ve Uluyol, Ç. (2020). Blok zinciri teknolojisi. *Bilişim Teknolojileri Dergisi*, *13*(2), 167-175. https://doi.org/10.17671/gazibtd.516990

YacY (2022). *YacY Search Engine Software*. Erişim adresi: https://yacy.net/ Erişim tarihi: 13.05.2022.

Yapıcı S., Oral, N., Yumuşak, R., Eren, T. (2021). Blokzincir teknolojisi ile merkezi ve dağıtık veritabanının karşılaştırılması. *Endüstri Mühendisliği Dergisi*, *32*(3), 457-472.

YCharts (2023). *Bitcoin blockchain size*. Erişim adresi: https://ycharts.com/indicators/bitcoin_blockchain_size Erişim tarihi: 31.08.2023.

Zhang, L. (2019). Blockchain: The new technology and ıts applications for libraries. *Journal of Electronic Resources Librarianship*, *31*(4), 278-280. https://doi.org/10.1080/1941126x.2019.1670488

Zikratov I., Kuzmin, A., Akimenko, V., Niculichev, V., Yalansky, L. (2017). Ensuring data integrity using blockchain technology. 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, Russia. *Proceedings of the XXth Conference of Open Innovations Association FRUCT*, *776*(20), 534-539. https://doi.org/10.23919/FRUCT.2017.8071359