

# Blok Zinciri Teknolojisi

## Literatür Makalesi/Review Article

 Gökhan ÜNAL<sup>1\*</sup>,  Çelebi ULUYOL<sup>2</sup>

<sup>1</sup>Yazılım uzmanı, İstanbul, Türkiye

<sup>2</sup>Bilgisayar ve Öğretim Teknolojileri Eğitimi, Gazi Üniversitesi, Ankara, Türkiye

[fatihgokhanunal@gmail.com](mailto:fatihgokhanunal@gmail.com), [celebi@gazi.edu.tr](mailto:celebi@gazi.edu.tr)

(Geliş/Received:23.01.2019; Kabul/Accepted:24.04.2020)

DOI: 10.17671/gazibtd.516990

**Özet**— Günümüzde sosyal medya, bankacılık uygulamaları ve gelişmekte olan diğer teknolojiler cihazların büyük miktarda veri üretmesine neden olmaktadır. Bu verilerin kontrol, yönetim, bakım süreçleri ve güvenli bir şekilde paylaşılması gün geçtikçe daha da önem kazanmaktadır. Finans sektörünün liderliğinde veri depolama ve veri yönetim arayışlarına her geçen gün yeni bir bakış açısı veya teknoloji eklenmektedir. Bunun son ve en popüler örneklerinden biri Blok zinciri (Blockchain) teknolojisidir. Kripto para birimi Bitcoin’le en popüler zamanına ulaşan Blok zinciri teknolojisinin sadece bir sanal para birimi teknolojisi olmadığı açıktır. Bu araştırma Blok zinciri teknolojisini derinlemesine ele almakta, çeşitleri, mimarisi, çalışma prensibi, kullanım alanlarını inceleyerek bu teknolojiyi çeşitli kriterler açısından geleneksel veritabanı yönetim sistemleri ile karşılaştırmaktadır. Araştırma sonuçları merkezi yapıyı sonlandıran ve güvenliği ön planda tutan bu teknolojiye hızlı bir şekilde adapte olunması gerektiğini ortaya koymaktadır.

**Anahtar Kelimeler**— Blok zinciri, veritabanı, güvenlik, veritabanı güvenliği

## Blockchain Technology

**Abstract**— Social media, banking applications, and other emerging technologies cause devices to produce large amounts of data. Moreover, the control, management, maintenance and security of data becomes vital. A new perspective/technology is being added to the search for data storage and data management under the leadership of the finance sector. In this sense, Blockchain technology is often mentioned. It is clear that Blockchain technology, which reaches its most popular time with Bitcoin, is not just a virtual currency technology. This research examines the Blockchain technology in depth, examines its types, architecture, working principle, usage areas and compares this technology with traditional database management systems for various variables. The results of the research show that the technology should be adapted quickly to the central structure and to keep the security in the forefront.

**Keywords**— blockchain, database, security, database security

### 1. GİRİŞ (INTRODUCTION)

21. yüzyılın en değerli hazinesi bilgidir. Bilgiye dönüşümde veriler toplanmakta, gruplandırılmakta, sıralanarak özetlenmekte, elle ya da bilgisayarla işlenip enformasyona dönüştürülerek anlam kazanmaktadır. Günümüzde her alanda veri toplanmakta, bu verilerin güvenli bir şekilde depolanması ve kolayca yönetilebilmesi ihtiyacı doğmaktadır. Bu amaçla ortaya çıkan veritabanı yönetim yaklaşımları her geçen gün gelişmekte ve değişmektedir.

Dosyalar halinde saklama yöntemiyle başlanan veri depolama günümüzde büyük sistemlerin kullanıldığı bir ortama dönüşmüştür. Gelişen teknoloji ve farklılaşan ihtiyaçlarla birlikte veritabanı teknolojilerinde de ciddi bir değişim söz konusudur. Sosyal medya başta olmak üzere milyonlarca veri üreten alanların oluşmasıyla yeni veritabanı yaklaşımlarına ihtiyaç duyulmaktadır [1]. Bu yaklaşımların gelişiminde performans, güvenlik ve denetim başlıkları önemli yer tutmaktadır. Geleneksel veritabanı yönetim sistemlerinin avantaj ve dezavantajları şu ana kadar birçok araştırmayla ortaya konmuştur. Özellikle üçüncü kişilerin erişimine karşı verinin korunması, devlet ve özel sektör başta olmak üzere veri

depolayan ve yöneten herkesin önceliği durumuna gelmektedir. Kötü niyetli kişilerin saldırı yöntemleri her geçen gün değişmekte ve güvenli olarak bilinen sistemlerin açıkları ortaya çıkmaktadır [2].

Son yıllarda popülerliğini artıran kripto para birimi Bitcoin [3] ile birlikte bu para biriminin altyapısını oluşturan Blok zinciri sistemi veri yönetimi alanında teknoloji sektöründe yerini almaya başlamıştır. Bu sistem güvenli ve tutarlı bir veritabanı sistemi iddiasıyla başta finans sektörü olmak üzere birçok alanda yaygınlaşmaya başlamıştır. Bu durum geleneksel veritabanı yaklaşımları ile Blok zinciri sisteminin karşılaştırılarak başta güvenlik olmak üzere avantaj ve dezavantajlarının değerlendirilmesi ve ortaya konmasını zorunlu kılmaktadır. Blok zinciri sisteminin getirdiği yenilik ve avantajlar veritabanı konusunda yeni bir yaklaşım arayışında olan veri sahipleri için de önem arz etmektedir. Son dönemde ciddi kullanıcı sayısına ulaşan [4] ve giderek yaygınlaşan bu sistemin ne kadar uyumlu ve güvenli olduğu konusunda araştırmalar devam etmektedir.

Bu araştırmanın amacı son dönemde adından sıkça söz ettiren Blok zinciri hakkında detaylı bir inceleme sunmaktır. Bu amaçla Blok zinciri çeşitlerine değinilecek, mimarisi ve çalışma prensipleri anlatılacak, kullanım alanlarına örnekler verilecek, Blok zinciri platformları örneklendirilecek ve çeşitli kriterler açısından geleneksel veritabanı yönetim sistemleri ile karşılaştırması yapılacaktır. Bu çalışma ile Blok zinciri sistemini kullanmak ve değerlendirmek isteyen kişilere yol göstermek, araştırmacılara temel bir kaynak oluşturmak ve mevcut sorulara cevap aramak açısından geleceğe ilişkin yön çizmek hedeflenmiştir.

## 2. BLOK ZİNCİRİ (BLOCKCHAIN)

Blok zinciri 2008 yılında ortaya atılmış, 2009 yılında ise Bitcoin sanal para birimi ile birlikte tanınmaya başlamıştır. Bu teknoloji dağıtılmış bir kayıt defteri olarak tanımlanmaktadır. Daha kapsamlı bir ifadeyle Blok zinciri, dağıtık, paylaşılan, şifrelenmiş, geri dönüşü olmayan ve bozulmayan bir bilgi deposudur [4]. Blok zinciri, ağ yardımı ile sistemi kullanan kullanıcılar arasındaki işlemlerin tümünü doğrularak saklayan bir sistemdir. Bu yüzden bütünlüğüne güvenilir bloklar ve bu blokları oluşturan sorgulanabilir işlemlerden oluşan bir veritabanı olarak tanımlanmaktadır.

Blok zinciri sisteminde işlemler bloklar halinde tutulur ve bu bloklar birbirine bağlanarak zincir oluşturulur. Belli kurallar çerçevesinde oluşturulan bloklar sisteme yazılmaktadır. Daha sonra blok tüm dağıtık kayıt defterlerine yayılır ve eklenir. Yeni blok oluşturmada bir önceki bloğa ait özet alınır ve ikinci blok üretilerek zincire ekleme yapılmaktadır. Bu yapı tüm blokları birbirine bağlayan ve bir önceki bloğun özeti ile beraber olacak biçimde devam eden bir yapı ile sürdürülür. Bir işlem gerçekleştiğinde mevcut ağ üzerinden yayımlanır ve şifreleme algoritmaları ile bu işlem doğrulanarak blok oluşturulur. Sisteme dahil olan her düğüm, sistemdeki

herhangi iki kişi tarafından yapılan bu işlemi onaylayarak kaydını tutar. Bu sayede blok doğrulanır, sonrasında bu bilgi asla değiştirilemez veya silinemez. Her blok birbirine zincirlenerek eklenmeye devam eder. Böylece başka biri onları hiçbir zaman değiştiremez.

Sistemde bulunan her bir kullanıcı bir düğümü ifade eder. Sisteme katılan her düğüm, kendi başına bir blok zinciri kopyasına yani kayıt defterine bir başka deyişle veritabanına sahiptir. Bu defter bir uçtan uca protokolü kullanılarak diğer düğümlerle senkronize edilir. Bu sayede aracı ortadan kaldırılmakta ve merkezi bir otorite zorunluluğu da gerekmemektedir. [4]. Bir düğüm başarısız olur veya işlevini durdurursa, kalan düğümler arızalı yerin yokluğunda tüm işlem ayrıntılarını muhafaza eder. Bu şekilde sistem gerçek zamanlı bilgi sağlamakta ve işlemlerin hata ya da başarısızlık oranlarını azaltmaktadır [5].

Birden fazla tarafın bulunduğu Blok zinciri sisteminde, sisteme eklenmesi istenen herhangi bir işlemin doğrulanabilmesi için genel kabul görmüş kurallara uygunluğunun kontrol edilmesi gerekmektedir. Bu kontrol sürecine ve sonunda işlemin geçerli olduğu konusunda fikir birliğine varılmasına “mutabakat” adı verilmektedir. Mutabakattaki kontrol işlemi sistem içerisinde gerçekleştirilebileceği gibi güvenli dış bir unsur tarafından da yapılabilir. Eğer mutabakat sistem içerisinde sağlanırsa kayıt defterine sahip her düğümün bu işlemin geçerliliği için fikir birliği oluşması gerekmektedir. Mutabakat sağlandığında işlem doğrulanmış olur ve artık işlem kayıt defterine eklenir. Bu yaklaşıma da “mutabakat yapısı” adı verilmektedir.

Blok zinciri sistemi temel bazı kriterlere [6] sahip olup bu standartlar üzerine kurulur. Bu özellikler aşağıda kısaca açıklanmıştır.

**Dağıtık:** Blok zincirinin en temel özelliği verilerin tek bir yerde tutulmaması, dağıtılabilir şekilde kaydedilmesi, depolanması ve güncellenmesidir.

**Şeffaf:** Blok zinciri sistemi ile verilerin kaydı her düğüme şeffaf olup veriler geriye dönük olarak doğrulanabilir. Bu nedenle blok zinciri güvenilir kabul edilmektedir.

**Bağımsız:** Mutabakat yapısı sayesinde blok zincir sistemindeki her düğüm verileri güvenli bir şekilde aktarabilir, merkezi bir sisteme ihtiyaç duyulmamaktadır.

**Değiştirilemez:** Blok zincirine eklenen kayıt hiçbir şekilde güncellenemez, silinemez ve kayıt kalıcı olarak saklanır [7]. Kaydın değiştirilebilmesi çeşitli saldırı tipleri dışında mümkün değildir.

**Kimlik gizliliği:** Blok zinciri sisteminde düğümler kimlik belirtmeden veri aktarımı gerçekleştirebilir. Bu işlem için kişinin blok zinciri adresinin bilinmesi yeterlidir.

## 2.1 Blok Zinciri Çeşitleri (Types of Blockchain)

Blok zinciri izin mekanizmasına göre üç çeşitten oluşmaktadır: Açık, özel ve konsorsiyum blok zinciri.

### 2.1.1 Açık blok zinciri (Public Blockchain)

Açık blok zinciri ağında herkes ağa katılabilir. Bu sistem tamamen bağımsız ve merkezi otorite gerektirmeyen blok zinciri sistemi olarak kabul edilmektedir. Akıllı sözleşmeleri kullanmayı sağlayan ve geliştiricilerin dağıtılmış uygulamaları yayınlamasına olanak tanıyan platform ve programlama dili sağlayan Ethereum ve Bitcoin bu yapıya örnek olarak gösterilebilir [8,9].

### 2.1.2 Özel blok zinciri (Private Blockchain)

Özel blok zinciri sisteminde sadece izin verilen kullanıcılar ağa katılabilir. Ağ içindeki mutabakata dahil olmak herkese açık ya da izin gerektiren bir biçimde tanımlanabilir [6]. Özel blok zinciri sisteminde izinli olup sisteme yerleşenler mutabakat yapısına izinsiz giriyorsa bu sistemlere kısmen izin gerektiren sistem adı verilmektedir. Bu ağlarda merkezi bir otoritenin ihtiyaca dayalı olarak kuralları değiştirmek ve işlemleri geri almak gibi yetkileri bulunmaktadır. Özel sistemlerin kurulması, maliyetlerin düşürülmesi ve verimliliklerin artması için kullanılmaktadır. Bu sisteme örnek olarak Eris Industries isimli blok zincir teknolojisini kullanarak paylaşılan yazılım veritabanı sağlayıcısı ve Multichain isimli finansal işlemler için açık kaynaklı dağıtılmış bir veritabanı sağlayıcısı verilebilir [8].

### 2.1.3 Konsorsiyum blok zinciri (Consortium Blockchain)

Konsorsiyum blok zinciri ağları açık ve özel blok zinciri ağlarının karışımı olarak kabul edilmektedir. Yetki sahibi olan kişi veya kurum tarafından düğümün önceden seçebildiği bir sistemdir. Bu blok zincirindeki veriler açık ya da özel olabilir. Konsorsiyum bir blok zincirinde okuma ve yazma kabiliyeti belirli sayıda düğüme genişletilebilir. Bu durum, bir araya gelerek birbiriyle iş birliği yaparak farklı modeller geliştirmeye çalışan kurum veya kuruluşlar tarafından kullanılabilir. IBM firmasının Hyperledger projesi bu zincir türünün en büyük örneğidir [8].

## 2.2 Blok Zinciri Mimarisi ve Çalışma Prensipleri (Architecture and Working Principles of Blockchain)

Blok zinciri işlemleri bloklar içinde saklanmakta ve bloklar ile zincir oluşturmaktadır. Bu bloklar ile zincir belirli özelliklere sahip olup belirli kurallar ile bir araya gelmektedir. Aşağıda bununla ilgili temel kavramlar açıklanmıştır.

### 2.2.1 Blok (Block)

Blok zinciri sisteminde verilerin saklanması blok olarak isimlendirilir. Bloklar zincir biçiminde sıralanır. Bu zincir yapısı içerisinde yer alan ilk blok başlangıç bloğu olarak isimlendirilir. Her blok başlık ve gözde kısımlarından

oluşur [10]. Blok başlığında meydana gelen bir değişiklik başlık özetlerinde uyumsuzluğa neden olur ki bu da blok zincirinin en önemli güvenlik unsurudur [11]. Bloktaki işlem sayısı işlemlerin boyutuna ve işlemlerdeki blok sayısına göre değişmektedir. Her blokta öncesinde bulunan blokla ilgili özetleme bilgisi tutulmakta olup [12], bir blokta yaklaşık olarak 350 ile 500 arasında işlem bilgisi yer almaktadır [13].

### 2.2.2 Dijital imza (Digital signature)

Her kullanıcının sahip olduğu özel anahtar (private key) ve açık anahtar (public key) olmak üzere iki farklı anahtar mevcuttur. İşlemleri imzalamak için özel anahtar kullanılmaktadır. Dijital imzalanmış tüm işlemler ağ içerisinde herkes tarafından ulaşılabilecek biçimde açık anahtarlar kullanılarak erişilmektedir. Dijital imza imzalama ve doğrulama olmak üzere iki aşamadan oluşmaktadır. Örnek vermek gerekirse, bir imza atmak isteyen Ahmet'in işlemi için işlemden oluşturulmuş özet bir değer üretilir. Sonrasında bu özet değer, özel anahtar kullanılarak şifrelenir ve şifrelenmiş özet bilgisi Hasan'a ulaştırılır. Hasan, şifrelenmiş özet Ahmet'in gönderdiği açık anahtarla çözer ve mesajın özetini oluşturur. Kontrol işlemi ise Ahmet'in mesajından türetilen özet değeri arasındaki karşılaştırma yoluyla alınan işlem ile sağlanır.

### 2.2.3 Mutabakat mekanizması (Consensus mechanism)

Blok zinciri ağındaki verinin tüm kayıt defterlerinde senkronize biçimde bulunması gerekir. Bu durumun oluşması için ağ genelinde mutabakat sağlanması gerekir. Blok zinciri sisteminde blokların güvenilir olduğu bilgisini sağlamak için Kriptografik Özetleme (Cryptographic Hashing) ve zaman bilgisi kullanılmaktadır. Blok başlığındaki bilginin özetleme ile işlenmesi özetleme bilgisini (block hash) ortaya çıkarır. Bu özetin içerisinde bir önceki bloğun özet bilgisi yer almaktadır. Bu sayede zincirin sürekliliği doğrulanmaktadır [6]. Blok zinciri platformları bu konuda farklı yaklaşımlar sergilemektedir. Bu yaklaşımlardan en çok kullanılan iki algoritma aşağıdaki gibidir [10]:

**İş kanıtı (Proof of Work-POW):** Bu algoritma blok zinciri ağına yeni bir blok eklenmesi için çözülmesi zor ama çözümün doğruluk kontrolünün kolay olduğu bir bulmacanın çözülmesi şeklinde çalışmaktadır. Bu sistemde önemli olan blokla ilgili özetlemenin belli bir kurala uygun olmasıdır. Bu uyum belirlenen bir aralık içerisinde bulunma ya da belli bir dizi ile başlama gibi kısıtlara uygun olmakla sağlanmaktadır. Bitcoin yapısında yaklaşık on dakikada bir iş kanıtına uygun blok oluşturulmaktadır. Bitcoin için iş kanıtı oluşturma işlemi madencilik (mining) olarak adlandırılmaktadır [6].

**Hisse kanıtı (Proof of Stake-POS):** İş kanıtı yöntemi çok fazla elektrik enerjisi gerektirerek bilgi işlem gücünün harcanmasına neden olmaktadır. Bu algoritma, blok zincirindeki blok üretim ve doğrulama işlemi ile bloğu üreten düğümün zincirdeki sahip olduğu payı

ilişkilendirmektedir. Bu sistemde kripto paralar en başında tüm sisteme yatırımlara göre dağıtılır. Bu paralardan pay miktarı hesaplanır ve düğümler bu miktar üzerinde sistemde öncelik hakkı kazanır. Bir sonraki bloğun üretiminde ise rastlantısal fonksiyon kullanılmaktadır. Bu sayede payı yüksek olan düğümün seçilme şansı yükselir. Eğer bu düğüm uygun bir blok üretmezse sıradaki düğüme bu hak verilir. Bir başka yaklaşımda ise belirlenen pay çözülecek olan bulmacanın zorluğunda etkili olur [6].

#### 2.2.4 Çatallaşma işlemi (Fork)

Çatallaşma, herhangi bir kaynak kodu ele alıp uyarlama yapıp farklı ve yeni bir çalışma ortaya koyma işlemidir. Bu duruma açık kaynak kodlu projelerde çok sık rastlanmaktadır. Blok zinciri yazılımının yeni sürümü yayınlandığında, uzlaşma kuralındaki yeni yazılım düğümlere dağıtılır. Blok zinciri yapısı dağıtık olduğundan ve merkezi kontrollü olmadığından eğer değişiklik isteği büyük bir grup tarafından kabul görürse bu andan itibaren yeni kurallar belirlenerek yeni çatallaşma duyurusu yapılır [14]. Böyle bir durumda dört olay oluşmaktadır:

- Yeni düğümler, eski düğümler tarafından gönderilen blok işlemine katılırlar.
- Yeni düğümler, eski düğümler tarafından gönderilen blok işlemine katılamaz.
- Eski düğümler, yeni düğümler tarafından gönderilen blok işlemine katılırlar.
- Eski düğümler, yeni düğümler tarafından gönderilen blok işlemine katılamazlar.

Blok zinciri ağındaki düğümler her zaman kuralları kabul etmeyebilir. Bu dört farklı durumda fikir birliği oluşmamasından dolayı çatal problemi olur. Dört farklı olaya göre çatal problemleri Sert çatallaşma (Hard Fork) ve Yumuşak çatallaşma (Soft Fork) olmak üzere iki gruba ayrılmaktadır [15].

Sert çatallaşma: Blok zinciri sistemi üzerinde yapılan değişiklik önceki bloklarla uyumlu olmadığında sert çatallaşma meydana gelmektedir. Sert çatallaşma olurken ağdaki düğümlerin yeni yazılımı aynı anda yükseltmesi gerekir [15,16].

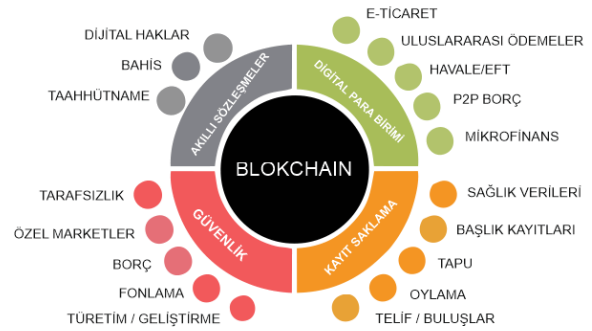
Yumuşak çatallaşma: Blok zinciri sistemi üzerinde yapılan değişiklik önceki bloklarla uyumluysa yumuşak çatallaşma meydana gelmektedir. Yeni yazılıma sahip düğümlerin bilgi işleme gücü eski düğümlerden daha güçlü olduğundan, eski düğümler tarafından doğrulanmaya çalışılan blok yeni düğümler tarafından onaylanmayacaktır. Eski ve yeni düğümler aynı zincir üzerinde çalışmaya devam eder. Yumuşak çatallaşma olurken ağdaki düğümlerin yeni yazılımı aynı anda yükseltmesi gerekmez, kademeli olarak yükseltmesine izin verilir [15,16].

#### 2.2.5 Akıllı sözleşmeler (Smart contracts)

Akıllı sözleşme kullanıcıların iletişimini daha güvenli bir biçimde yürütebilmek amacıyla 1994 yılında ortaya çıkmış bir kavramdır. Fikrin en önemli örneği Bitcoin’de kısmen bulunmakla birlikte, kod yazarak sözleşme yazmayı insanlara gösteren ve 2014 yılında ortaya çıkan Ethereum’dur [17]. Akıllı sözleşme her bir tarafın kabul ettiği kuralları içerir ve bu şartlar sağlandığında çeşitli işlemler yapılır. Akıllı sözleşmeleri kabul eden tarafların imzasının ardından bu sözleşmeler kriptografi kullanılarak Blok zincirine yüklenir [18]. Akıllı sözleşme içerisinde yer alan tüm kodların açık, net ve herkes tarafından rahatlıkla anlaşılabilir durumda olması gerekmektedir.

#### 2.3 Blok Zinciri Kullanım Alanları (Usage Areas of Blockchain)

Blok zinciri finans sektörü ile birlikte yayılsa da birçok alanda kullanılmaktadır. Bitcoin ile tanınan teknoloji daha sonra birbirinden farklı sektörlerde kullanılmaya başlanmıştır.



Şekil 1. Blok zinciri kullanılan alanlar, <https://smartyim.pro/> adresinden uyarlanmıştır (Usage areas of Blockchain)

##### 2.3.1 Gayrimenkul endüstrisi (Real estate industry)

Blok zinciri teknolojisi tapu ve arazi mülkiyeti kayıtları ve ilgili paydaşlar ile acentelerin mülkiyet kayıtlarına gerçek zamanlı erişimi için kullanılmaktadır. Bu sayede mülkiyet anlaşmazlıkları ve araçların mülkiyet sahibinin erişimini gerektiren belge gereksinimi önemli ölçüde azalmaktadır. Özel sektörde kira anlaşmaları yine bu sistem ile yapılabilmektedir. Kişi ve kurumlar bu sayede maliyet ve zamandan tasarruf sağlamaktadır [4].

##### 2.3.2 Sağlık sektörü (Health area)

Sağlık sektöründe en büyük sıkıntılar sahte ilaçlar ve uyuşturucu bazı ilaçların denetimsiz satılması problemleridir. İlaç, üretiminden itibaren hastaya ulaşana kadar doğrulanması ve denetlenmesi gerekmektedir. Blok zinciri teknolojisi ile bu işlem sistemli hale getirilmiş ve kolaylaştırılmıştır. Fabrikadan ilaç paketlerinin kimliği doğrulanmış ve her ara teslim noktasında zaman damgalı hale getirilmiştir. İlacın dağıtım hattı boyunca kimliği doğrulanır ve bu ilacın izlenmesini sağlar [4].

### 2.3.3 Devlet kurumları (Government agencies)

Devlet kurumları kamuya açık kayıtları depolayan dağıtık bir veri tabanına anlık ve eşzamanlı olarak erişmekten büyük ölçüde yararlanabilir. Birden fazla acentenin gerçek zamanlı olarak kimliği paylaşması, erişmesi ve doğrulamasını sağlamak için pasaport veya sürücü ehliyeti Blok zincirine yerleştirilebilir. Birçok banka ve finans kuruluşu şu anda Blok zincirinde kurumsal ve kişisel finansal işlemler düzenlemeye yönelik çalışmaktadır. Finansal işlemlerde her işlem ilgili vergi dairelerine görünür olduğu için, defterin varlıkların devrini takip etmesi nedeniyle otomatik olarak vergilendirilebilir. Bu, dosyalama ve vergilerin denetimi açısından yükü azaltır ve süreçte çeşitli araçlara olan ihtiyacı azaltır [4].

### 2.3.4 Pırlanta sektörü (Diamond industry)

Elmas sanayi en büyük doğal kaynak endüstrilerinden biri olup özellikle Afrika ülkelerinde ihracatın önemli bir bölümünü oluşturmaktadır. Sektörün en büyük problemi kaçakçılıktır. Taşlar küçük, gizlenmesi ve taşınması kolaydır. Suçlular için işlemlerin gizli tutulması önemli bir faktördür. Elmas ve pırlantalar büyük bir ölçekte kara para aklama ve terörizmin finanse edilmesinde kullanılıyor. Bu gibi sıkıntılardan kurtulmak için Everledger şirketinin Blok zinciri yazılımı kullanılmaktadır. Şirket, sigorta şirketlerinden talep sahiplerine ve kolluk kuvvetlerine kadar, elmasın üretim ve pazarlama aşamasında dokunduğu her kesime elmas tanımlama ve işlem doğrulaması için değiştirilemez bir kayıt defteri tedarik etmektedir. Everledger her taş işlem yaparken eşlik edecek benzersiz bir parmak izi oluşturarak her elmas için bir "dijital pasaport" atar [8].

### 2.3.5 Dijital içerik ve telif (Digital content and Copyright)

Sanatçılara ve yazarlara blok zincir yardımıyla eserlerini koruma şansı tanınabilmektedir. Üretilen eserin orijinalliğini ispatlamak için benzersiz bir kimlik belgesi ve dijital kimlik doğrulama sertifika üretilir ve tüm sistemlere aynı anda işlenir. Bu sertifika sayesinde eserin nasıl, hangi tarihte, hangi otorite tarafından korunduğu kayıt altına alınabilir [19].

### 2.3.6 Seçimler (Elections)

Blok zinciri teknolojisinin en büyük avantajlarından birisi olan verilerin değiştirilemediğini doğrulama özelliği seçim konusunda hükümetlerin ilgisini çekmektedir. Oyların şifrelenerek defterlere dağıtılması sayesinde hem şeffaflık hem de güvenlik sağlanacaktır. Belirli yetkili kişilerin oylarının sayıldığını ve kimin için oy verdiklerini onaylaması sağlanabilir. Sistem bu sayede, hükümete de para tasarrufu sağlamaktadır. İnternet üzerinden tüm vatandaşlara sunulan açık veri seçim verilerine anlık olarak özgürce erişilebilir.

### 2.4 Blok Zinciri Platformları (Blockchain Platforms)

Blok zinciri açık kaynak bir projedir. Bu projenin dışında finans başta olmak üzere birçok sektörde proje ve uygulamalar ortaya çıkmıştır. Bunların en popüler ve yaygın olanlarından bazıları aşağıda incelenmektedir.

#### 2.4.1 Bitcoin (Bitcoin)

Bitcoin merkezi bulunmayan dijital bir para birimidir. 2009 yılında ortaya çıkmıştır. Bitcoin, Blok zinciri sistemi üzerine kuruldu ve bu şekilde geliştirmeye başlandı. Düğümler her bir işlemi kendi sistemlerinde (defterlerinde) depolamaktadır. Defterde yapılan her eşleştirme hareketinin geçmişi kaydedilir ve bloklar "madencilik" adı verilen bir süreçle eklenir. Merkezi bir denetim gerektirmez ve her yerde herkes tarafından erişilebilen açık ödeme sistemidir [19].

#### 2.4.2 Ethereum (Ethereum)

Ethereum, merkezi olmayan uygulamaları oluşturmak, çalıştırmak ve kullanmak için kullanılabilen açık bir Blok zinciri platformudur. Böyle bir platformun tasarlanma sebebi güvenli olması, hızlı geliştirme süresi ve uygun etkileşim sunması olarak sıralanabilir. Ethereum, geliştiricilerin Ethereum sisteminde çeşitli programlama dillerinde çalışan uygulamalar oluşturmasına izin veren bir "Turing complete" programlama dili kullanmaktadır [20]. Ethereum'daki tüm işlemler, Ether adlı bir kripto para kullanılarak akıllı sözleşme hesaplamalarının yapıldığı Ethereum Sanal Makinesi "EVM" vasıtasıyla yürütülmektedir. EVM'in her düğümü zincir boyunca mutabakat sağlamak için tüm hesaplamaları yürütür.

#### 2.4.3 Ripple (Ripple)

Ripple, 2012'de oluşturulan bir ödeme ağı (RippleNet) hem de şifreleme (Ripple XRP) projelerinin birleşimidir. RippleNet, bankaları ve diğer büyük kurumları birbirine bağlayarak ağ üzerinden para ve diğer varlıkları aktarmasını sağlar. Tüm işlemler merkezi olmayan XRP Deedger'a kaydedilir. Ripple XRP, tüm ödemelerin ödeme ağına kullanılan ve uluslararası ödemelerde ilişkili zamanı ve parayı düşüren para birimidir. Sistemdeki her bir işlemin işleme süresi maksimum dört saniyedir. Ethereum, Bitcoin ve geleneksel sistemlere göre çok hızlıdır [21].

### 2.5 Blok Zinciri ve Geleneksel Veritabanı Yönetim Sistemlerinin Karşılaştırılması (The Comparison of Blockchain and Traditional Database Management Systems)

Bu araştırma kapsamında Blok zinciri ile geleneksel veritabanı sistemleri çeşitli değişkenler bakımından karşılaştırılmıştır. Bu karşılaştırma Tablo 1'de görülmektedir.

Tablo 1. Blok zinciri ve geleneksel veritabanı yönetim sistemleri karşılaştırması  
(The comparison of Blockchain and traditional database management systems)

	Blok zinciri	İlişkisel Veritabanı	Dağıtık Veritabanı
Merkeziyet		√	√
Dağıtık mimari	√		√
Gizlilik	√	√	√
Güvenlik	√	√	√
Dayanıklılık	√	√	√
Doğrulama	√	√	√
Performans	√	√	√
CRUD		√	√
Sorgulama		√	√

Tablo 1’de görüldüğü üzere Blok zinciri ile geleneksel veritabanı sistemleri birçok kriterde farklılık göstermektedir. Bu farklılıklar aşağıda kısaca açıklanmaktadır. Kıyaslama çalışmaları yapan farklı çalışmalar da mevcuttur [22,23].

### 2.5.1 Mutabakat sistemi ve dağıtık yapı (Consensus system and distributed structure)

Geleneksel veritabanlarında istemci-sunucu ağ mimarisi kullanılır. İstemci ya da kullanıcı sunucuya erişim depolanmış verileri değiştirebilir. Erişim denetimi belli kurallar çerçevesinde belirlenmiş kimlik bilgilerinin doğrulanması ile sağlanır. Bu otoritenin, veri tabanının idaresinden sorumlu olması nedeniyle, otoritenin güvenliği tehlikeye girerse veriler değiştirilebilir hatta silinebilir [24]. Böyle bir yapılandırmanın sebebi güvenliğin garanti altına alınması ve şebekenin kurcalanmasının zorlaştırılmasıdır [25]. Verilerin birçok düğümde yani makinada bulunması ve senkronize olarak depolanması sayesinde herhangi bir makinanın zarar görmesi halinde kalan düğümler aynı şekilde işlevine devam edecektir. Yine bu sayede verilerin herhangi bir şekilde değiştirilmesi veya manipüle edilmesi mümkün olmayacaktır. Sistem içerisinde yer alan bilgisayar sayısının artmasıyla bu durum daha fazla güçlenecektir [26].

Dağıtık veri tabanı sistemi olan NoSQL ile Blok zinciri arasındaki en büyük fark; NoSQL gibi veri tabanı sistemlerinde tüm makinelere güvenilir ve verilerin bütünlüğüne saldırmaya çalışmamalarını beklenmez. Çünkü tüm makinalar kontrol altındadır. Merkezi bir yönetim tarafından yönetilmektedir. Blok zincirinde ise hiçbir makineye güvenilmez, böyle bir duruma ihtiyaç duyulmaz. Ağa bağlı bilgisayarların %51’inden fazlasının dürtüst ve veri bütünlüğüne saldırmayacağı kabul edilmektedir.

### 2.5.2 Gizlilik (Privacy)

Geleneksel veri tabanı sistemlerinde depolanmış veriler belirli kişilerin yetkisi ile okunabilir veya yeni veri eklenebilir. Sisteme erişim sağlayan yetkili kişilerin genelde tüm verileri açık şekilde görebileceği anlamına

gelmektedir. Geleneksel sistemde genelde bilgiler erişim kısıtlama ile korunmaktadır. Bunun dışında şifre benzeri çok gizli olması gereken bilgiler ise kapalı veya şifreli depolanabilmektedir. Yetkisiz kişilerin saldırı dışında verilere erişimi mümkün değildir. Bu saldırı sisteme olduğu gibi yetkili kişilerin yani insanların açıkları ile de olabilir.

Blok zinciri sisteminde, verilerin okunma talebi kabul edebilecek veya reddedecek olan merkezi yetkili makamlardan geçmemektedir. Geleneksel bir veri tabanı okuma ve yazma kontrollüdür, Açık Blok zinciri yapısı yazma ve okuma işlemlerinde kontrol yapısına sahip değil ancak Özel Blok zinciri sisteminde ağa girebilecek kişinin kontrolü ve yazma izni sadece izin verilen düğümlere verilmektedir [26]. Bitcoin sistemi en fazla şeffaflığa sahip sistemlerden biridir. Kullanıcı kimliği dışında tüm transaction (işlem) bilgisine isteyen herkes ulaşabilmektedir. Bu durum şeffaflık arayan sistemlerde avantaj olsa da bankacılık gibi kişisel mahremiyet içeren sistemlerinde büyük bir sıkıntı oluşturabilir. Bazı Blok zinciri sistemlerinde bu durumu aşmak için işlemler daha öncesinde şifreleme algoritmaları (SHA-256) ile şifrelenerek gönderilmektedir (Bauerle, tarih yok). Blok zinciri yapısı her ne kadar daha gizli bir yapıya sahip olsa da şifreleme işlemleri yüksek işlem gücü ve zaman gerektirmektedir. Bu yüzden geleneksel veri tabanları bir adım daha öne çıkmaktadır.

Bir başka Blok zinciri özelliği ise “Anonimlik” tir. Blok zinciri ağında işlem gerçekleştiren düğümler gizli bir kimliğe sahiptir. Bu durum işlemi gerçekleştiren kişilerin gizli kalmasını ve daha rahat hareket etmesini sağlamaktadır. Geleneksel yapılarda ise her kullanıcı belirli bir kimliğe sahiptir. Bu fark hem avantaj hem dezavantaj yaratmaktadır.

### 2.5.3 Güvenlik (Security)

Geleneksel veri tabanı sistemlerinde verinin güvenliği için çok sayıda sistemsel önlem alınmaktadır. Yüksek güvenlik maliyetleri nedeniyle bu önlemlerden kaçınılması gibi riskler bulunmaktadır. Bunun dışında mevcut sistemlerin en büyük sorunlarından birisi DDoS saldırı ile sistemin işlevsiz bırakılması veya verilere müdahale edilmesi ve değiştirilmesidir.

Blok zinciri uygulamaları arasında güvenlik anlayışı değişiklik göstermektedir. Ancak temel olarak birkaç özellik barınmaktadır. Dağıtık yapısı sayesinde DDoS saldırısına karşı sistem esnekliği bulunmaktadır. Hizmet dışı kalan düğüm olsa dahi kalan düğüm veri kaybı olmadan işleme devam edebilmektedir. Kullanılan özetleme şifreleri sayesinde sistem dışı kalan düğümde veriler değiştirilse dahi mutabakata katılamayacak ve diğer düğümler tarafından doğrulanmayacaktır. Bunun yanında çoğu sistemde kullanıcılar işlemleri gerçekleştirmesi veya akıllı sözleşmelerin çalışması için şebekeye küçük bir işlem ücreti ödemeleri öder. Bu ücretler Blok zincirinin

bakım maliyetlerini karşılaması yanında kötü niyetli kişilere karşı da koruma sağlar [4].

#### 2.5.4 Dayanıklılık (Durability)

Geleneksel veri tabanlarının veriyi çoğaltma ve koruma için birçok teknik yapıya sahiptir. Bu durum, geleneksel veri tabanlarının pahalı altyapı ve felaket kurtarma senaryo zorunluluğunu dezavantaja çevirmektedir. Birincil veri tabanı, farklı bir fiziksel konumdaki bir yedekleme sistemine işlemleri aktarır ve yakından izlenen üst düzey bir donanım üzerinde çalışır. Birincil veri tabanı başarısız olursa (ör. Elektrik kesintisi veya felaket gibi bir donanım hatası nedeniyle), otomatik olarak yedek veri tabanı devreye girer ve yeni birincil olur. Bu pahalı bir altyapı ve güçlü sistemler gerektirmektedir.

Blok zinciri ağı herhangi bir yapılandırılmaya gerek duymadan sadece düğümleri bir araya getirerek ve otomatik olarak kendilerini senkronize tutar. Bir düğümün herhangi bir ağa eklenmesi ya da ağdan kaldırılması için herhangi bir hazırlık gerekmemektedir. Bu düğümler, birbirine sıkıca bağlı olacak, karşılıklı iş birliği temelinde işlemler paylaşacak ve mutabakat sağlayarak bir blok zinciri oluşturacaktır. İşlemleri üreten son kullanıcılar, bu düğümlerin bir kısmıyla iletişim bağlantısının kesilmesi halinde kalan düğümlerle sorun yaşamadan işlemlere devam ederler. Eğer bir veya birkaç düğüm belirli bir günde tamamen başarısız olursa, kimse bu durumdan etkilenmez çünkü hala dolaşmaya yetecek kadar kopya vardır. Bu durum düşük maliyetle yüksek dayanıklılık elde edilmesini sağlamaktadır [26].

#### 2.5.5 Performans (Performance)

Blok zincirleri şu an ki yapısıyla geleneksel veri tabanlarından daha yavaş işlem gerçekleştirme gücüne sahiptir. Blok zinciri kayıt sistemleri olarak kullanılabilir ancak, Visa ve PayPal gibi ile bugün gördüğümüz dijital işlem teknolojilerine kıyasla oldukça yavaştır [27]. Blok zinciri yazılımlarının yeni ve optimize olmaması şu an için süreleri daha kısa yapmak için dezavantaj durumundadır. İşlemleri gerçekleştirirken bir Blok zinciri normal bir veri tabanı ile aynı şeyleri yapmak zorunda, bunun dışında 3 ek işlem daha gerçekleştirilmektedir:

**İmza doğrulama:** Her blok zinciri işlemi, imzalanıp bu imzanın doğrulanması gerekmektedir. Bu hesaplama karmaşıktır ve zaman almaktadır. Buna karşılık, merkezi veri tabanlarında, bir kez bir bağlantı kurulduktan sonra, üzerinde gelen her isteği tek tek doğrulamaya gerek yoktur

**Mutabakat mekanizması:** Bir Blok zinciri ağına, ağdaki düğümlerin fikir birliğine ulaşmasını sağlamak için çaba sarf edilmektedir. Bu mutabakat belirli bir zaman almaktadır. Geleneksel veri tabanlarının aynı zamanda çakışan ve iptal edilen işlemlerle uğraşması gerektiği doğru olsa da, işlemlerin tek bir yerde kuyruğa alınarak işlendiği yerlerde bu ihtimal azalmaktadır.

**Düğüm sayısı:** Geleneksel veri tabanlarında işlemleri bir kez (veya iki kez) işlerken, bir Blok zincirinde ağdaki her düğüm tarafından bağımsız olarak işlenmeleri gerekir. Böylelikle aynı sonucu elde edebilmek için çok daha fazla iş yapıldığını söylemek mümkündür [26].

#### 2.5.6 Denetleme ve doğrulama (Auditing and verification)

Çoğu geleneksel veri tabanı, belirli bir anda güncel olan bilgileri tutar. Çok eskiye ait veriler silinir. Blok zinciri veri tabanları ise kurulduğu andan itibaren tüm işlemleri saklar. Blok zinciri teknolojisi kendine ait geçmişe sahip veri tabanları oluşturabilir. Bu durum her katılan düğüm için geçerlidir. Blok zinciri ağına girdiğine geçmişe ait tüm veri kümesini kaydetmek zorundadır. Çünkü her yeni işlem bir önceki bloğa eklenecektir [27].

Veriler eklendiğinde ve zincir zamanla büyüdükçe, daha eski veriler kilitli kalır ve etkin bir şekilde kurcalanmaya karşı korunur. Sistem doğrulanabilir ve güvenilir denetime açıktır ve katı uyumu kurallarıyla yükümlü olan kuruluşlar için son derece yararlı olabilir [25]. Bu durum geleneksel veri tabanlarına göre hem avantaj hem de dezavantajdır. Çünkü bu veriler eklendikçe mevcut veri tabanı şişecek ve büyüyecektir. Devasa boyutlara ulaştığında çeşitli zorluklar çıkarması muhtemeldir. Aynı zamanda yeni eklenecek düğümlerin devasa boyuttaki veri tabanı kopyasını elde etmesi de zorlaşacaktır.

#### 2.5.7 CRUD işlemleri (CRUD processes)

Veritabanında Create (Oluşturma), Read (Okuma), Update (Güncelleme) ve Delete (Silme) olmak üzere dört işlemin yapıldığı görülmektedir. Bu işlemler veri tabanı yönetim sistemi yazılımı ile kolayca gerçekleştirilebilir. Blok zinciri veri tabanında ise, kullanıcı sadece veri ekleyebilir. Eklenecek verilerin ardından önceki verilerde herhangi bir değişim, bozulma ya da silinme olmaz [24]. Bu durum verilerin değiştirilmediğinden ve silinmediğinden emin olmak için oldukça avantajlıdır. Ancak yine bu durum veri tabanının şişmesi ve devasa boyutlu veri kümeleriyle uğraşmak zorunda kalmamıza neden olmaktadır. Yapılacak olan projenin ihtiyaçlarına göre bu durum değerlendirilmelidir.

#### 2.5.8 Sorgulama işlemleri (Query processes)

Geleneksel veritabanı sistemlerinde mevcut veriler birçok farklı kombinasyonla elde edilebilmektedir. Bu sayede raporlama hizmetleri gerçekleştirilir ve büyük firmaların veri analizi yapımında kullanılır. Günümüzde Büyük veri (Big Data) alanında yapılan çalışmalar için veri sorgulama önemli bir alan teşkil etmektedir. Sosyal medyanın büyük şirketleri olan Facebook ve Twitter gibi şirketler milyonlarca veriyi dağıttık veri tabanları kullanarak depolamaktadır. Daha sonra bu verileri Veri madenciliği (Data mining) alanında kullanılmaktadır. Bu yüzden SQL gibi sorgulama dillerinin kullanılması geleneksel veri tabanı sistemlerinde büyük bir avantajdır.

Blok zinciri sisteminde sorgulama dili bulunmamaktadır. Yalnızca işlem numarası (transaction id) ile sorgulanmak istenen işlem yapılmakta, raporlama gibi istekler karşılanmamaktadır. Son dönemde Blok zinciri yetenekleri kazandırılmış veritabanı sistemleri üzerinde çalışmalar yapılmaktadır. BigchainDB isimli açık kaynak yazılım dağıtılmış bir veritabanının üzerine Blok zinciri özellikleri eklenerek ortaya çıkarılmış büyük bir veri çözümüdür. NoSQL'in sahip olduğu sorgu dilini içerir ve finansal sistemlerin gereksinimlerini karşılaması için gereken saniyede 1 milyon işlem yazma performansı hedeflemektedir. Klasik blok zinciri performansı bu veritabanı türü ile aynı olmayıp, yalnızca saniyede birkaç işlem gerçekleştirerek onayları on dakikaya kadar sürebilmektedir [28].

### 3. SONUÇ VE ÖNERİLER (CONCLUSION AND RECOMMENDATIONS)

Blok zinciri teknolojisi avantaj ve dezavantajları değerlendirildiğinde çok hızlı şekilde geleneksel sistemlerin yerini alması mümkün gözükmemektedir. Dayanıklılık, güvenlik ve veri aktarım kriterlerinde oldukça başarılı sonuçlar elde edilmektedir. Bu kriterler ileride daha da büyük avantaj elde etmek için kullanılabilir. Performans, doğrulama ve sorgulama kriterleri ise şu an için büyük bir dezavantaj olarak göze çarpmaktadır.

Finans sektörü açısından düşünüldüğünde performans büyük bir olumsuzluktur. Mevcut sistemlerde saniyede iki bine yakın işlem yapılmaktadır [29]. Bitcoin'de bu çok çok düşük rakamlardadır. Bu yüzden bu eksikliğin giderilmeden mevcut sistemlerle yarışmak kolay olmayacaktır. İşlemlerin geriye yönelik doğrulanması ise büyük veri ile işlemler yapılmasına yol açmaktadır. Bu durum da performansa etki etmektedir.

Gizlilik ve dağıtık yapı her iki yaklaşım için benzer avantajlar sağlamaktadır. Ancak merkezi otorite konusu tamamen göreceli olarak değerlendirilebilir. Kimi zaman avantaj kimi zaman büyük bir zorluk ortaya çıkarabilir. Günümüzde büyük verilerin ve raporların işlenmesi çok kritik konudur. Şu an için Blok zinciri bu konuda yolun başındadır. O yüzden bu alanda da geleneksel veritabanı sistemleri öne çıkmaktadır.

Blok zinciri teknolojisi son dönemde popülerliğini artırmış güncel bir teknolojidir. Çok çeşitli alanlarda büyük bir dönüşüm potansiyeline sahiptir. Diğer yeni teknolojilerde olduğu gibi Blok zincir teknolojisinde de yeni projelerle denemeler yapılmaktadır. Yapılan her yeni projede açıklar kapanarak sistem geliştirilmektedir. Hızla gelişen teknolojinin doğru şekilde büyümesi ve yaygınlaşması, yenilik ve gelişimini ihlal etmeden, sistemin yönetim, güvenlik ve esnekliğini sağlamak için doğru denge üzerinde durmak gerekecektir. Blok zincirinde başarının en önemli sebeplerinden birisi etkili yönetimdir. Sistemin gizlilik ve siber güvenlik risklerine karşı dayanıklılığını artırmaktadır.

Finanstan gayrimenkule, sağlıktan kuyumculuk sektörüne kadar birçok alanda Blok zinciri teknolojisi için proje yatırımları başlamış durumdadır [23,30,31]. Öncelikle StartUp şirketlerinin ilgi alanında bulunan Blok zinciri teknolojisi artık büyük şirketler tarafından da incelenmektedir. Akıllı sözleşmelerin işlem güvenliğini artırma ve manipülasyon riskini azaltma için potansiyel olarak çekici hale gelmesine rağmen, teknolojinin uygulanmasını yasal düzenleme eksikleri zorlaştırmaktadır. Bu durumun aşılabilmesi bu teknolojinin tutarlı bir gelişim gösterebilmesi ve özellikle kripto para sektöründe kötüye kullanımının önüne geçilebilmesi için hem teknolojik hem ticari hem de yasal standartların belirlenmesi ve geliştirilmesi gerekmektedir.

Blok zinciri teknolojileri geliştiricilerine göre şu anda dünyada bu teknolojiyle ilgili yeniliklere odaklanan binin üzerinde şirket (Blockchains startups) bulunmaktadır. Bu teknolojiye bilgi birikimi ve tecrübenin istikrarlı bir ekosistem oluşturması için yeterli sayıda müşteri, girişimci ve geliştiriciye ihtiyacı bulunmaktadır. Bunun için yeterince yaygın olup olmayacağı şu an için bilinmemekle birlikte özellikle kripto para birimi Bitcoin sayesinde popülerliği artmaya devam etmektedir.

Veri paylaşımı için hızlı ve güvenilir sistem arayışı bilişim teknolojileri altyapı ve veritabanı yöneticilerinin de en büyük sıkıntularından biridir. Bu yöneticiler için Blok zinciri ilk çözümlerden biri olarak ortaya çıkmaktadır. Yetmiş eleman açığı ise şu an için Blok zinciri teknolojisine geçişi yavaşlatmaktadır.

Blok zinciri getirdiği yeniliklerin yanında yeni alanlar da açmaktadır. Farklı Blok zinciri türleri ortaya çıktıkça kullanıcılar hangi Blok zincirinin gereksinimlerini karşılayıp karşılamadığını bilmek istemektedirler. Dolayısıyla Blok zinciri test mekanizması farklı sistemleri test etmek için de gerekmektedir. Bu sistem üzerinde veri analizi konusunda büyük bir sektör boşluğu bulunmaktadır. Blok zinciri teknolojisindeki son gelişmeler yapay zeka uygulamaları için yeni fırsatlar yaratmaktadır. Yapay zeka teknolojileri birçok Blok zinciri zorluğunun çözülmesine yardımcı olacağı öngörülmektedir. Blok zinciri teknolojisinin vadedtiği güvenli ve etkin veri aktarımı geleneksel sistemlerle zorlu bir yarışa gireceğinin göstergesidir. Mevcut sisteme sahip şirketlerin bu alanda Ar-Ge çalışmalarını hızlandırdıkları bilinmektedir. Mevcut sistemlerin yanında Blok zincirine yatırım yapmak dışında açacağı yeni alanlara da yatırımlar yapılması büyük önem kazanmaktadır. Bu alanlarda yapılan yatırımlar arttıkça Blok zinciri teknolojisinin daha hızlı gelişmesi ve yaygınlaşması mümkündür.

### KAYNAKLAR (REFERENCES)

- [1] E. Önder, *Yönetim Bilişim Sistemleri Kapsamında Web Tabanlı İlişkisel Veritabanı Yönetim Sistemleri ve Bir Uygulama*, Yüksek Lisans Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, 2005.



- [2] Y. Vural, Ş. Sağıroğlu, “Veritabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri”, *Politeknik Dergisi*, 13(2), 71-81, 2010.
- [3] İnternet: S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system (Technical Report). [www.bitcoin.org](http://www.bitcoin.org), 15.02.2020.
- [4] İnternet: H. Kakavand, N. Kost De Sevres, B. Chilton, The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies, <https://ssrn.com/abstract=2849251>, 03.01.2019.
- [5] G. R. Nair, S. Sebastian, “Blockchain Technology Centralised Ledger to Distributed Ledger”, *International Research Journal of Engineering and Technology (IRJET)*, 4(3), 2823-2827, 2017.
- [6] I. C. Lin, T. C. Liao, “A Survey of Blockchain Security Issues and Challenges”, *IJ Network Security*, 19(5), 653-659, 2017.
- [7] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain”, **2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)**, 577–578, 2015.
- [8] İnternet: T. Wan, H. Max, Bitcoin: Fact. Fiction. Future, <https://www2.deloitte.com/insights/us/en/topics/emerging-technologies/bitcoin-fact-fiction-future.html>, 04.01.2019.
- [9] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, R. Brooks, “A brief survey of Cryptocurrency systems”, **2016 14th Annual Conference on Privacy, Security and Trust (PST)**, 745–752, 2016.
- [10] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, “Blockchain Challenges and Opportunities: A Survey”, *International Journal of Electric and Hybrid Vehicles*, 14(4), 1–23, 2017.
- [11] S. Singh, N. Singh, “Blockchain: Future of financial and cyber security”, **2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)**, 463–467, 2016.
- [12] İnternet: P. Kovary, F. Zhou, M. Adoul, Blockchain - Technical Details, [http://www.doc.ic.ac.uk/~ma7614/topics\\_website/tech.html](http://www.doc.ic.ac.uk/~ma7614/topics_website/tech.html), 07.01.2019.
- [13] A. Çarkacıoğlu, **Kripto-para Bitcoin**, Sermaye Piyasa-sı Kurulu Araştırma Dairesi, 2016.
- [14] İnternet: Qtum, What is a blockchain fork?, <https://blog.qtum.org/what-is-a-blockchain-fork-16cef86c0ad8>, 23.12.2019.
- [15] İnternet: B. Yazıcı, Soft Fork ve Hard Fork Nedir? Temel Farkları Nelerdir?, <http://www.burcinyazici.com/soft-fork-ve-hard-fork-nedir-farklari-3599.html/>, 20.12.2018.
- [16] İnternet: F. İstanbul, F. H. Fork, Mecburi Çatallaşma nedir?, <http://fintechistanbul.org/> 2016/07/30/hard-fork-sert-catal-nedir/, 10.12.2019.
- [17] İnternet: Y. Chu, J. Ream, D. Schatsky, Getting smart about smart contracts, <https://www2.deloitte.com/tr/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html>, 10.12.2019.
- [18] İnternet: S. Doğanekin. (Çok) Akıllı Sözleşmeler, <https://medium.com/@sdogantekin/%C3%A7ok-ak%C4%B1ll%C4%B1-s%C3%B6zle%C5%9Fmeler-80a3a9938fa6>, 01.12.2019.
- [19] M. Crosby, P. Nachiappan, S. Verma, V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin”, *Applied Innovation Review*, 2, 6-19, 2016.
- [20] İnternet: M. Pilkington. Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, <https://ssrn.com/abstract=2662660>, 15.12.2018.
- [21] İnternet: M. Rutnik, What is Ripple? - a short guide, <https://www.androidauthority.com/what-is-ripple-819806/>, 02.12.2018.
- [22] N. Bozic, G. Pujolle, S. Secci, “A tutorial on blockchain and applications to secure network control-planes”, **2016 3rd Smart Cloud Networks Systems (SCNS)**, 1–8, 2016.
- [23] İ. Kırbaş, “Blokzinciri teknolojisi ve yakın gelecekteki uygulama alanları”, *Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 9(1), 75-82, 2019.
- [24] İnternet: S. Ray, Blockchains versus Traditional Databases, <https://hackernoon.com/blockchains-versus-traditional-databases-c1a728159f79>, 14.12.2019.
- [25] İnternet: K. Finlow-Bates. Blockchain Meets Database: Replace or Combine?, <https://dzone.com/articles/blockchain-vs-database-replace-or-enhance>, 12.12.2019.
- [26] İnternet: G. Greenspan. Blockchains vs centralized databases, <https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/>, 03.12.2019.
- [27] İnternet: N. Bauerle. What is the Difference Between a Blockchain and a Database? <https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database/>, 04.12.2019.
- [28] G. Peters, G. Vishnia, “Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges”, *SSRN Electronic Journal*, 8, 1-20, 2016.
- [29] İnternet: S. Kalla, Gavin Andresen Tests Bitcoin Block Size Increase. <https://bravenewcoin.com/news/gavin-andresen-tests-bitcoin-block-size-increase/>, 04.12.2019.
- [30] F. Tian, “An agri-food supply chain traceability system for China based on RFID blockchain technology”, **2016 13th International Conference on Service Systems and Service Management (ICSSSM)**, 1–6, 2016.
- [31] M. Mettler, “Blockchain technology in healthcare: The revolution starts here”, **2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)**, 1–3, 2016.