# Blokzinciri Teknolojisi Nedir ? Ne Değildir ?: Alanyazın İncelemesi

*Araştırma Makalesi/Research Article*

Mustafa TANRIVERDİ[1]*, Mevlüt UYSAL[1], Mutlu Tahsin ÜSTÜNDAĞ[2]

[1]Bilgi İşlem Daire Başkanlığı, Gazi Üniversitesi, Ankara, Türkiye
[2]Bilgisayar ve Öğretim Teknolojileri Eğitimi, Gazi Üniversitesi, Ankara, Türkiye
mustafatanriverdi@gazi.edu.tr, mevlutuysal@gazi.edu.tr, mutlutahsin@gazi.edu.tr
(Geliş/Received:30.03.2019; Kabul/Accepted:18.06.2019)
DOI: 10.17671/gazibtd.547122

***Özet***— Günümüzde iş yapış şekillerimiz ve alışkanlıklarımızı değiştiren bilgi ve iletişim teknolojileri hızını kesmeden rolünü devam ettirmektedir. Bu hızlı değişime ülkeler, politika belirleyiciler, araştırmacılar ve bunlardan ciddi şekilde etkilenen iş dünyasının ayak uydurması ve katkı sağlayacak teknolojilerin iş süreçlerine dahil edilmesi önemlidir. Bu noktada dijital paralarla adını konuşur olduğumuz blokzinciri (blockchain) kavramı ortaya çıkış şekli ve hızı 20.yy sonlarında ortaya çıkan internet kavramına benzemektedir. Blokzinciri teknolojisi mevcut veri tabanı mantığından farklı olarak merkezi otoritedeki yetkilerin zincirdeki her bir düğüme dağıtılarak yetki ve sorumluluk paylaşımını sağlamaktadır. Blokzinciri kavramının insanların algıladığı gibi sadece dijital paralarla ilgili olmadığı, dağıtık yapısı, veri güvenliği ve şeffaflık gibi özelliklerinin yanında barındırdığı uzlaşma protokolleri, güvenlik yapıları ve akıllı sözleşmeler gibi teknolojiler ile birlikte kullanımının anlaşılması önemlidir. Alanyazın incelendiğinde araştırmacıların bile blokzinciri teknolojisini ve yapısını doğru anlamadığı, ihtiyaçlara yanlış model ve çözümler üretme çabasında oldukları görülmektedir. Bu teknolojinin yenilik etkisinin avantajını kullanarak yapılan araştırmaların, blokzinciri yapısının doğru kullanımı ve entegrasyonuna gerekli özeni verip rekabetçi iş dünyasına katkı sağlaması gerektiğini de unutmamak gerekir. Bu nedenle bu araştırmanın amacı kapsamlı bir alanyazın taraması ile teknolojiyi doğru tanıtmak, ulusal alanyazında yer alan eksikliği gidermek ve farklı alanlardan iyi uygulamaları tanıtarak araştırmacılara konu üzerinde düşünmelerine yardımcı olmaktır.

***Anahtar Kelimeler***— blokzinciri, alanyazın taraması, akıllı sözleşmeler, uzlaşma protokolleri

# What is Blockchain Technology? What isn't?: Literature Review

***Abstract***— Information and communication technologies that change our ways of doing business and our habits today continue its role without interrupting the pace. It is important that countries, policymakers, researchers and the technologies that are heavily influenced by the business world to adapt these rapid changes and to include technologies that will contribute in business processes. At this point, the concept of blockchain, in which we speak the digital coins, resembles the concept of internet that emerged in the late 20th century. Blockchain technology differs from the existing database logic and distributes the powers of the central authority to each node in the chain and provides the authority and responsibility sharing. It is important to understand the concept of blokchain not only related to digital money, but also with its properties like distributed structure, data security and transparency in combination with technologies such as consensus protocols, security structures and smart contracts. When the literature is examined, it is seen that even the researchers do not understand the technology and structure of the blokchain and try to produce the wrong models and solutions to the needs. It should not be forgotten that research using the advantage of the innovation effect of this technology should give due attention to the proper use and integration of the blockchain structure and contribute to the competitive business world. Therefore, the aim of this study is to introduce the technology correctly through a comprehensive literature review, to eliminate the deficiency in the national literature and to help researchers to think about the subject by introducing good practices from different fields.

***Keywords***— blockchain, literature review, smart contracts, consensus protocols

## 1. GİRİŞ (INTRODUCTION)

Blokzinciri teknolojisi son zamanlarda ulusal ve uluslararası basın, çeşitli uluslararası kuruluşlar, özel sektör ve kamu kurumları tarafından büyük ilgi görmekle birlikte bazı araştırmacılar tarafından potansiyel olarak Internet'ten daha güçlü bir teknoloji olarak ifade edilmektedir [1]. Allied Market Research tarafından yayınlanan raporda blokzinciri piyasasının 2016 yılında 228 milyon $ olduğu ve 2023 yılına kadar 5.4 milyar $ seviyelerine ulaşabileceği belirtilmiştir [2]. Akademik açıdan bakıldığında çok kısa zaman önce alanyazında blokzinciri konulu bir çalışmaya rastlamak çok zor iken şuan bu konuyla ilgili birçok çalışmanın bulunduğu ve sayılarının giderek arttığı görülmektedir [3].

Blokzinciri sayesinde insanlar artık ürün veya hizmet transferi işlemlerinde güvenlik ve doğrulamayı sağlaması için üçüncü taraf bir aracıya ihtiyaç duymamaktadır. Blokzinciri ile oluşturulan "güven protokolü" güvenilir, şeffaf ve hesap verebilir bir ortam sunmaktadır. Blokzinciri, kullanıcılar için merkezi olmayan dağıtık veri yapıları sayesinde güvenliğin temeli oluşturmaktadır [4]. İnternetin dünya çapında iletişimi çok kolay hale getirmesi sonucu dünya giderek birbiri ile bağlantılı bir toplum haline gelmiş ve akıllı telefonlar, nesnelerin interneti (internet of things), akıllı sözleşmeler gibi teknolojiler hızla yaygınlaşmaya başlamıştır. Bu teknolojilerin dahil olacağı gelecekte blokzinciri insanların, uygulamaların ve nesnelerin arasındaki ağın gücünü arttırmak için önemli bir araç olacaktır.

Kriptografik olarak güvenli blok verileri üzerine ilk çalışma Haber ve Stornetta tarafından yapılmıştır [5]. Blokzinciri kelimesi ilk kez gerçek kimliği henüz bilinmeyen Satoshi Nakamoto isimli bir yazarın "Bitcoin: A Peer-to-Peer Electronic Cash System" adlı makalesinde kullanılmıştır [6]. Bitcoin, blokzinciri üzerinde geliştirilen merkez bankaları ve hükümetlerden bağımsız alternatif ödeme aracı olarak tasarlanan eşler arası elektronik para sistemidir. Blokzinciri teknolojisinin son zamanlarda çok popüler hale gelmesinin ana nedenlerinden biri, değeri ortaya çıktığı günden bu yana yaklaşık 60 000 kat artan Bitcoin'dir. Bunun aynı zamanda blokzinciri üzerinde negatif bir etkisi olmuştur, çünkü Bitcoin ve blokzinciri kavramları birbiri ile çok sık karıştırılmakta ve yapılan birçok çalışma sayısız türü ve teknik özellikleri olmasına rağmen Blokzinciri kavramı yerine sadece Bitcoin blokzincirine odaklanmaktadır [7].

Alanyazında sayısı hızla artan blokzinciri konulu çalışmalar incelendiğinde çok gerçekçi olmayan öneriler ve beklentilere rastlamak mümkündür [7]. Bu araştırmanın amacı kapsamlı bir alanyazın taraması ile blokzinciri teknolojisini doğru tanıtmak, ulusal alanyazında yer alan eksikliği gidermek ve farklı alanlardan iyi uygulamaları tanıtarak araştırmacılara konu üzerinde düşünmelerine yardımcı olmaktır.

## 2. BLOKZİNCİRİ TANIMI VE ÖZELLİKLERİ (BLOCKCHAIN DEFINITION AND PROPERTIES)

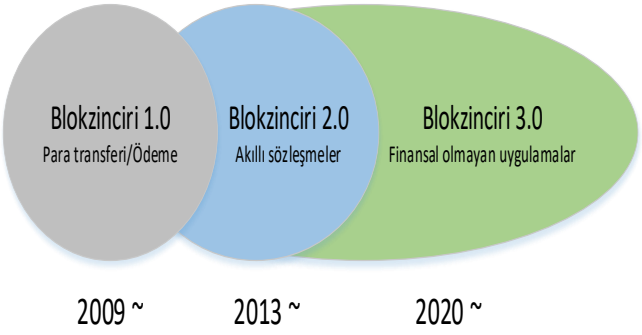
Nakamoto' ya göre blokzinciri, yapılan her işlem bilgisinin ağdaki katılımcılar tarafından kaydedildiği ve paylaşıldığı dağıtılmış bir veri yapısıdır [6]. Beck' e göre ise blokzinciri, ağdaki çok sayıda düğüm tarafından güvenli ve tutarlı işlemlerin yapılmasını sağlayan bir veritabanıdır [8]. Zheng vd. blokzincirini, onaylanan tüm işlemlerin blok listeleri halinde depolandığı ve yeni bloklar eklendikçe büyüyen bir veri defteri olarak tanımlamıştır [9]. Reyna vd. göre blokzinciri, işlemlerin güvenirliğinin ağdaki paydaşlar tarafından doğrulandığı dağıtılmış, şeffaf, değiştirilemez ve güvenli bir veri yapısıdır [10]. Glaser blokzincirini, kullanıcıları arasında paylaşılan ve bir aracı veya merkezi otoriteye ihtiyaç duymadan değerli varlıkların kayıtlarının kamuya açık ve takma isimlerle kaydedildiği bir veritabanı olarak tanımlamıştır [11]. Tama vd. tarafından blokzinciri, amacı veri bütünlüğü sağlamak olan dağıtılmış bir yazılım sisteminin bir parçası olarak ifade edilmiştir. [12]. Bazı araştırmacılar blokzincirin ayrıntılı bölümlerini ihmal ederek sadece veri bütünlüğüne odaklanmaktadır. Örneğin Halpin vd. blokzinciri sadece kriptografik olarak doğrulanabilir bir veri listesi olarak tanımlamaktadır [13]. Teknik açıdan bakıldığında blokzinciri, dağıtık bir veritabanı, merkezi olmayan mutabakat mekanizması ve kriptografik algoritmaların birleşimi olarak tanımlanması doğru olacaktır. Blokzinciri üzerinde yapılan işlem verileri kriptografik olarak birbirine bağlı ve potansiyel olarak sonsuz olan veri blokları dizisinde saklanır. Bu blokların oluşması, yapılan işlemlerin doğruluğunun ve geçerliliğinin merkezi olmayan zaman damgalı algoritmalar aracılığıyla katılımcı düğümler tarafından oylanması sonucu sağlanır [14]. Zhao vd. blokzincirin en önemli özelliği olarak, insanların takibi ve kontrolü yerine ağa dayalı hesaplamalar yoluyla güvenilir ve şeffaf işlemlerin desteklenmesini göstermiştir [15]. Bu özelliği ile blokzinciri "etkileşimler için işletim sistemi" olarak düşünülebilir [16]. Lewis' e göre blokzinciri ve geleneksel veritabanları arasındaki ana fark olarak, blokzincirinin yeni kayıt ekleme, bilgilerin doğrulanması ve dağıtılması gibi işlemleri için P2P ağı üzerinde mutabakat kurallarına dayalı çözümler sunan gelişmiştirilmiş bir veritabanı olması gösterilmiştir [17]. Blokzincirinin avantajlarını ve dezavantajlarını genel olarak aşağıdaki gibi sıralayabiliriz [18].

Blokzincirinin avantajları;

- Verilerin bir kopyası tüm paydaşlar tarafından kaydedilir, herkes bu verilere erişebilir ve yapılan işlemleri görebilir. Verilerin bu şekilde saklanması sayesinde veri kaybı ve veri tahribatı önlenir.
- Dijital imza ve doğrulamalar sayesinde aracılara ihtiyaç duymadan paydaşlarını birbirine güvenmesini sağlanır.
- Herkes hem kendi işleminin durumunu hem de blokzincirindeki tüm işlemlerin ayrıntılarını görebilir, bu şekilde şeffaflık sağlanmış olur.
- Blokzinciri üzerindeki veriler değiştirilemez veya silinemez.
- Merkezi bir otorite olmadan çalışabilir, bu dağıtık yapısı sayesinde kontrol edilemez, iptal edilemez veya kapatılamaz.
- Akıllı sözleşmeler sayesinde belirli faaliyetler otomatikleştirilebilir.

Blokzincirin dezavantajları;

- Uzlaşma protokolü olarak proof of work (işin ispatı) kullanılan blokzincirlerinde çok fazla enerji tüketilmekte ve çok pahalı bilgisayar sistemleri çalıştırılmaktadır.
- Blokzincirindeki tüm veriler her bir düğümde ayrı ayrı saklanmaktadır ve her bir işlem sonrası bu düğümlerdeki verilerin tutarlılığı sağlanmaktadır. Örneğin zincire bir blok eklemek Bitcoin zincirinde 10-60 dakika Ethereum zincirinde ise 15 saniye zaman almaktadır. Bu nedenle geleneksel veritabanları ile performans bakımından kıyaslandığında yetersiz kalmaktadır.
- Ağdaki her bir düğümün tüm verilerin bir kopyasını saklayabilmesi ve içeriğine erişebilmesi, kullanıcıların mahremiyetine zarar verebilir.
- Akıllı sözleşmeler bir kez oluşturulduktan sonra değiştirilemez ve blokzincirinde herkesin erişimine açık halde saklanır. Bu da akıllı sözleşmeleri kötü niyetli saldırılara karşı savunmasız bırakabilir.




Şekil 1. Blokzincirin Gelişimi [19]
(Evolution of blockchain)

Günümüzde blokzincirinin gelişimi Şekil 1' deki gibi üç evre halinde tanımlanabilir [15], [20]–[22];

**Blokzinciri 1.0:** Dijital para evresi olarak da adlandırılan Blokzinciri 1.0, para transferi ve dijital ödeme gibi uygulamaları bulunan kripto paraları ifade etmektedir. Kripto paralarda madencilik, şifreleme ve blok yapısı gibi blokzinciri teknolojileri kullanılmaktadır. İlk kripto para olan Bitcoin uygulama olarak kuramın önüne geçmiştir [23]. Bitcoin, para transferi ve elektronik alışverişler için geleneksel yöntemlerle kıyaslandığında çok küçük miktarlarda işlem ücreti gerektirmektedir. Bitcoin hesapları takma isimli olması sayesinde kredi kartlarına oranla daha fazla gizlilik sağlamaktadır. Geleneksel para birimleri, mali düzenlemeler ve para basma gibi işlemler için bir merkez bankasına bağlıdırlar bunun aksine, Bitcoin ve diğer dijital para birimleri ise sabit para arzını garantilemek için kriptografiyi kullanmaktadır. Bu sayede dijital paralar enflasyona karşı korunmaktadır [24].

**Blokzinciri 2.0:** Dijital ekonomi olarak da ifade edilen Blokzinciri 2.0, basit ödemeler ve para transferi işlemlerin ötesinde çok çeşitli ekonomik ve finansal uygulamaları kapsamaktadır. Bu tür uygulamalar arasında, krediler ve ipotekler gibi geleneksel bankacılık araçları, hisse senetleri, tahviller, vadeli işlemler ve sözleşme gibi araçlar yer almaktadır [22]. Bu tür kurallara bağlı karmaşık işlemler için akıllı sözleşmeler (smart contracts) kullanılmaktadır. Akıllı sözleşmeler blokzinciri ağı üzerinde bulunan belirli kurallara sahip bilgisayar programları olarak ifade edilebilir. Akıllı sözleşmeler, kullanımı son zamanlarda hızla yaygınlaşan bir blokzinciri teknolojisidir.

**Blokzinciri 3.0:** Dijital toplum olarak da adlandırılan Blokzinciri 3.0, para, sözleşme, finansal uygulamalar dışında bilim, sanat, sağlık, eğitim, iletişim, yönetim ve denetim alanlarını da kapsamaktadır [22]. Blokzinciri teknolojisinin gelecek vadeden en önemli uygulamalarından biri, akıllı yönetim, akıllı ulaşım, akıllı yaşam, doğal kaynakların akıllı kullanımı ve akıllı ekonomi gibi kavramların tümünü içeren akıllı kentlerdir [25]. Nesnelerin interneti (internet of things) kapsamında makinelerin haberleşmesi (machine to machine) alanlarında blokzinciri teknolojisinden faydalanmak mümkündür [26]. Dijital kimlik, bankacılık, siber güvenlik ve elektronik tıbbi kayıt sistemlerinde de blokzinciri teknolojilerinin kullanılması Blokzinciri 3.0 kapsamında değerlendirilebilir [27], [28].

### *2.1. Blokzinciri Sistemlerinin Sınıflandırması (Classification of Blockchain Systems)*

Mevcut blokzinciri sistemleri Genel Blokzinciri, Özel Blokzinciri ve Konsorsiyum Blokzinciri olmak üzere üç kategoride sınıflandırılmıştır [29], [30].

*Genel (Public) Blokzinciri:* Genel Blokzinciri, çeşitli kurumlara bağlı ya da bağımsız kişilerin katılımına, kayıt eklemesine ve madencilik yapmasına imkân veren açık bir platform sunmaktadır. Bu tür blokzincirlerinde herhangi

bir kısıtlama yoktur ve bu yüzden izinsiz blokzinciri olarak da adlandırılır. Genel Blokzincirleri tamamen açık ve şeffaftır ve herhangi bir özel doğrulayıcı düğüm barındırmamaktadır. Blokzincirinde isteyen herkesin tüm zincir verilerini indirip madenciliğe başlayabilmesi, zincirin birçok aktif kopyasının olmasını sağlamaktadır. Bu da blokzincirin güvenliğini ve tutarlılığını arttırmaktadır. Bu şekilde herhangi bir kontrol mekanizması olmayan dağıtık yapılarda mevcut ağdaki veri boyutunun büyümesinden dolayı zincirde bir değişiklik yapılması sırasında uzlaşma protokollerine çok iş düşmektedir.

*Özel (Private) Blokzinciri:* Bir ya da birkaç organizasyondaki kişiler arasında paylaşım ve veri alışverişini sağlayan, bir kişi ya da grup tarafından yönetilen blokzinciri yapılarına Özel Blokzinciri denmektedir. Özel bir izni olmayan kişilerin zincire katılamadıkları için izinli blokzinciri olarak da adlandırılabilir. Ağa bir düğümün katılımı ve erişimi, ağı yöneten grup tarafından belirlenen kurallara göre yapılmaktadır. Bu da blokzincirinin merkezi olmayan ve şeffaf yapısına uygunluğu azaltmaktadır.

*Konsorsiyum (Consortium) Blokzinciri:* Konsorsiyum Blokzinciri, blok doğrulama ve uzlaşma işlemlerinde tek bir organizasyonun yerine önceden belirlenmiş bir grup düğümün karar verici olarak yer aldığı kısmen özel ve izinli bir blokzinciri olarak tanımlanabilir. Kimlerin ağa katılabileceğine ve kimlerin madencilik yapabileceğine bu düğümler karar vermektedir. Blok doğrulaması için, bir bloğun sadece yetkili düğümler tarafından imzalanmışsa geçerli sayıldığı çoklu bir imza şeması kullanılır. Ağın herkese açık olması ya da sınırlı olmasına ve ağdaki herkesin veri okuma ve yazma işlemlerine sahip olma durumlarına bir konsorsiyum tarafından karar verilir.

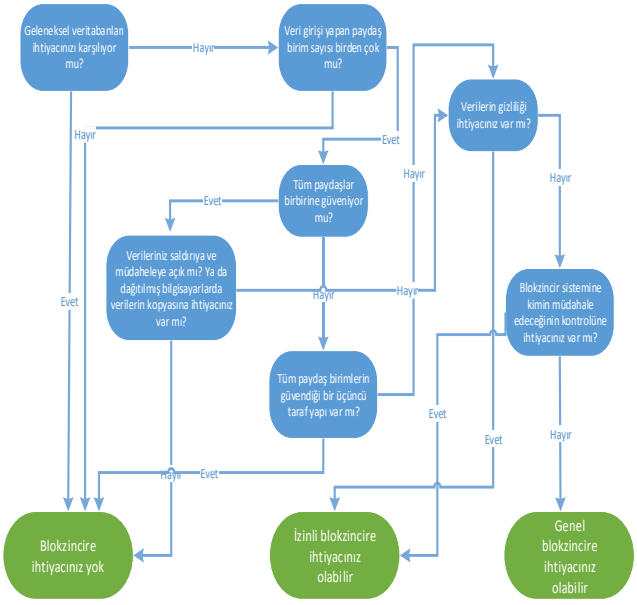
Tablo 1. Genel, Özel ve Konsorsiyum Blokzincirlerinin karşılaştırılması [9]
(Comparison of Public, Private and Consortium Blockchains)

| | Genel Blokzincir | Konsorsiyum Blokzincir | Özel Blokzincir |
|---|---|---|---|
| Uzlaşma sağlayıcılar | Bütün madenciler | Seçilmiş düğümler | Bir organizasyon |
| Okuma izinleri | Açık | Açık veya izinli olabilir | Açık veya izinli olabilir |
| Verimlilik | Düşük | Yüksek | Yüksek |
| Merkeziyetçilik | Hayır | Kısmen | Evet |
| Uzlaşma işlemlerine katılım | İzinsiz | İzinli | İzinli |

Tablo1'de Genel, Özel ve Konsorsiyum blokzincirlerinin uzlaşma sağlayıcılar, katılımcıların veri okuma izinleri, verimlilik, merkeziyetçilik ve uzlaşma işlemlerine katılım durumlarına göre karşılaştırılmasına yer verilmiştir.

### *2.2. Hangi Blokzincire İhtiyacını var (Which Blockchain Do You Need?)*

Blokzinciri teknolojisi son yıllarda çok popüler bir çalışma alanı haline gelmiştir. Blokzincirinin gelişim süreci hala devam etmekte ve farklı durumlar için farklı çözümler sunmaktadır. Şekil 2'de Peck tarafından blokzinciri teknolojisine ihtiyaç olup olmadığı, ihtiyaç varsa ne tür bir blokzinciri sistemine ihtiyaç duyulduğunu belirlemek için sunulan modelin karar ağacı grafiği görülmektedir [31].




Şekil 2. Blokzinciri ihtiyacının belirlenmesi [31]
(Determining the need for blockchain)

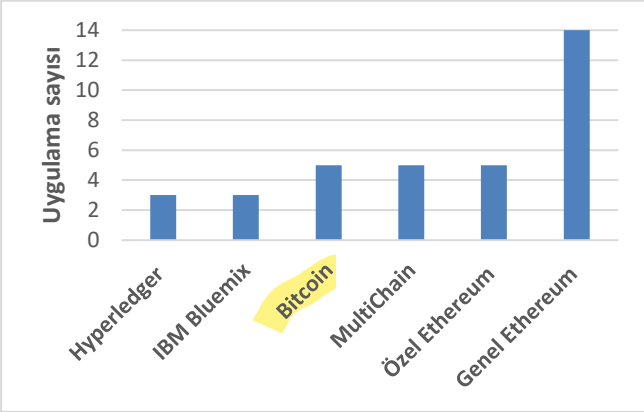
Geliştirilecek bir uygulamada veri depolanması gerekmiyorsa, o uygulamada blokzinciri kullanılmaz. Veri depolama ihtiyacı varsa ve veri girişi sadece bir birim tarafından yapılacaksa o uygulamada da blokzinciri kullanılması uygun değildir. Birden fazla birim için veri girişi gerektiren uygulamalarda geleneksel veritabanları ihtiyaçları karşılayabiliyorsa bu uygulamalarda blokzinciri kullanılmasına gerek yoktur. Bu durumlar dışında uygulamalar için Şekil 2' deki yönlendirmeler sayesinde ihtiyaç duyulan blokzinciri özellikleri tespit edilebilir.

### *2.3. Literatürde Kullanılan Blokzinciri Sistemleri (Blockchain Systems Used in Literature)*

Literatürde çok sayıda blokzinciri konulu çalışmaya rastlanmaktadır. Bunlardan bir kısmı bir mimari veya bir çözüm önermektedir. Bir kısım yayında ise mevcut blokzinciri sistemlerinden faydalanılarak gerçek uygulamalar hayata geçirilmiştir. Abadi vd. 2018 yılında yaptıkları bir çalışmada alanyazında en çok kullanılan blokzinciri sistemleri Şekil 3'teki gibi listelemiştir [32].

Abadi'nin çalışmasına göre araştırmacılar tarafından en çok kullanılan blokzinciri sistemi genel Ethereum

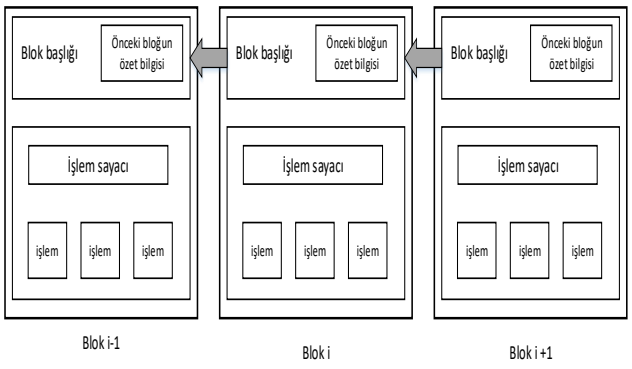
olmuştur. Araştırmacılar bu çalışmalarda ayrı bir blokzinciri ağı kurup yönetmeden hâlihazırda halka açık olarak çalışan genel Ethereum sistemini kullanmıştır. Bunun dışında çalışmaları için özel Ethereum blokzinciri oluşturan araştırmacılar da bulunmaktadır. Ethereum dışında MultiChain, IBM Bluemix, Hyperledger ve Bitcoin sistemleri de kullanılmıştır.




Şekil 3. Literatürde kullanılan blokzinciri sistemleri [32]
(*Blockchain systems used in literature*)

## 3. BLOKZİNCİRİ MİMARİSİ (ARCHITECTURE OF BLOCKCHAIN)

Blokzinciri, defteri kebir gibi gerçekleşen tüm işlemlerin kayıtlarının tutulduğu sıralı bloklardan oluşmaktadır [33]. Şekil 4' te blokzinciri yapısının bir örneği gösterilmektedir. Bir blok sadece bir ana bloğa sahiptir ve her bloğun üst bilgisinde önceki bloğun özet bilgisi yer almaktadır. Blokzincirinin ilk bloğu, bir ana bloğu olmayan genesis blok olarak adlandırılır.

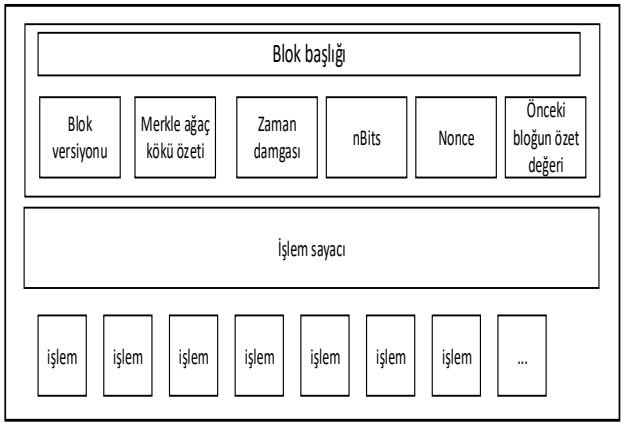



Şekil 4. Blokzinciri yapısı
(Architecture of blockchain)

### *3.1. Blok (Block)*

Bir blok Şekil 5'te gösterildiği gibi bir başlık ve bir gövdeden oluşmaktadır. Blok başlığında bulunan bilgiler şu şekildedir [9];

- Blok versiyonu, hangi blok doğrulama kurallarının uygulanacağını belirler.
- Merkle ağaç kökü özeti, bloktaki tüm işlem kayıtlarının özet değerini tutmaktadır.
- Zaman damgası, 1 Ocak 1970 tarihinden beri evrensel zamanda saniye olarak geçerli zaman bilgisini tutmaktadır.
- Nbit, geçerli bir blok özet değeri için eşik değer bilgisi içermektedir.
- Nonce, genellikle 0 ile başlayan her bir hesaplama için artan 4 byte boyutunda bir alandır.
- Önceki blok özet değeri alanında zincirde bir önceki bloğa karşılık gelen 256 bit boyutunda bir özet değer tutulmaktadır.




Şekil 5. Blok yapısı
(Architecture of block)

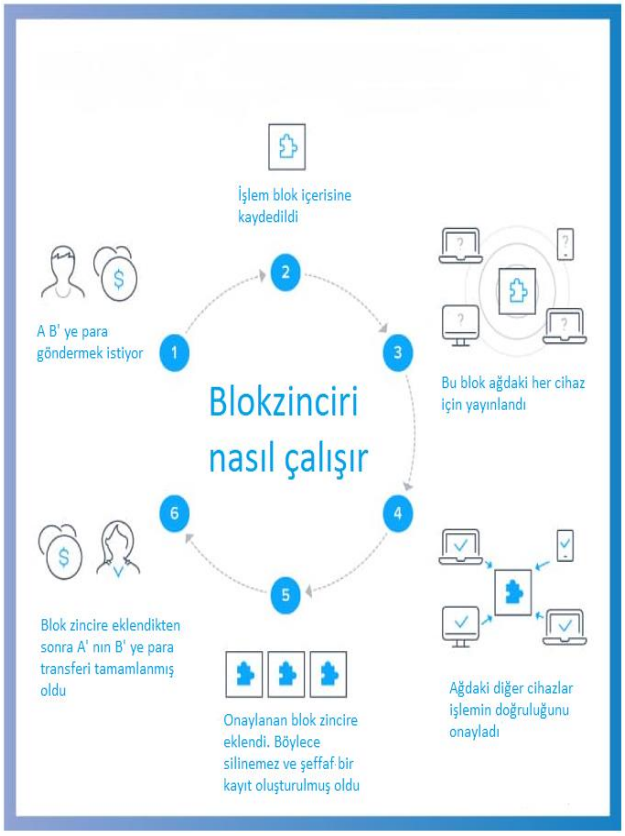
Blok gövdesi, gerçekleşen işlem kayıtlarından ve bir işlem sayacından oluşmaktadır. Bir bloğun içerebileceği maksimum işlem sayısı, blok büyüklüğüne ve her bir işlemin büyüklüğüne bağlı olarak değişebilmektedir. Blokzincirinde işlemlerin doğrulanmasını onaylamak için asimetrik bir şifreleme mekanizmasına dayalı dijital imza kullanılmaktadır.

### *3.2. Dijital İmza (Digital Signature)*

Dijital imza, blokzinciri üzerinde tutulan verilerin güvenliğini ve bütünlüğünü sağlamanın temel yöntemlerinden biridir. Dijital imzalar asimetrik kriptografiyi kullanır ve şifrelenen bilgi herkese açık bir anahtar kullanılarak paylaşılabilir. Blokzincirinde her kullanıcının bir genel (public) bir de özel (private) anahtarı bulunmaktadır. Gizli tutulan özel anahtar işlemleri imzalamak için kullanılmaktadır. Dijital olarak imzalanan işlemler tüm blokzinciri ağında yayınlanır. Bir dijital imza, imzalama ve doğrulama olmak üzere iki aşamadan oluşmaktadır. Örneğin A kullanıcısı B kullanıcısına dijital imzalı bir mesaj göndermek istemektedir. İmzalama aşamasında, A kullanıcısı verilerini özel anahtarı ile şifreler ve B kullanıcısına şifrelenmiş mesajı ve orijinal verileri gönderir. Doğrulama aşamasında B kullanıcısı, eline geçen mesajı A kullanıcısının genel anahtarı ile doğrular. Böylelikle, B kullanıcısı verilerin tahrif edilip edilmediğini kolayca kontrol edebilir.

### *3.3. Blokzinciri Nasıl Çalışır (How Blockchain Works)*

Blokzincirinde içerisinde veri bulunduran her işlemin zincire eklenmesi sonucu zincirin boyutu giderek artmaktadır. İşlemlerin boyutu belirli bir büyüklüğe eriştikten sonra yeni bir blok oluşturulmakta ve bir önceki blok ile ilişkilendirilerek zincire eklenmektedir.




Şekil 6. Blokzincirin çalışması [34]
(Working schema of blockchain)

Bir işlem kaydının doğrulanması ve zincire eklenmesi süreci şekil 6'daki gibi gerçekleşmektedir. Şekilde blokzincirin nasıl çalıştığının daha iyi anlaşılması için örnek bir senaryo oluşturulmuştur. Örneğin A kişisi B kişisine bir miktar sanal para ya da dijital bir karşılığı olan başka bir varlık göndermek istemektedir. Sanal paralar bir adres tarafından tanımlanan dijital bir cüzdanda saklanmaktadır. A kişisi aktarım işlemi için aktarmak istediği sanal para miktarını ve B kişisine ait dijital cüzdanın adresini belirler ve bu bilgiler A kişisinin cüzdanına ait gizli anahtar ile şifrelenir. Böylece bu işlemin A kişisi tarafından oluşturulduğu anlaşılır ve ağdaki başka biri tarafından değiştirilmesi engellenmiş olur. Şifrelenen işlem daha sonra yayınlanmak üzere ağa gönderilir. Diğer ağ düğümleri dijital imzayı analiz ederek bu işlemin A kişisine ait olup olmadığını kontrol ederler. Daha sonra A kişisinin cüzdanındaki bakiyenin B kişisine göndermek istediği tutarı karşılayıp karşılayamayacağı bilgisi, karşılıyorsa da A kişisinin aynı zaman aralığında başka kişilere de para transferi yapıp yapmadığı yani olası bir çift harcama durumunun tespit edilmesi gerekmektedir. Bu kontroller dışında karşılaşılan uyuşmazlıkların çözülmesi ve güvenlik ihlallerine karşı bir korumanın oluşturulması da gerekmektedir. Blokzincirinin tutarlılığı ve güvenliği için bahsedilen bu kontrollerin ve korumanın sağlanması çok önemlidir. Blokzincirinde merkezi bir yapı bulunmadığı için ağdaki düğümler tarafından uyulması gereken kurallar belirlenmeli ve bir uzlaşma mekanizması oluşturulmalıdır [18], [30]. Ağdaki düğümlerin uzlaşması sonrasında ilgili işlem yeni bir bloğa eklenir, yeni blok belirli bir boyuta ulaştıktan sonra önceki bloklar ile bağlantılı olarak zincire eklenir. Yeni bloğun zincire eklenmesi ve yayınlanması sonrasında, işlemde yer alan tutar B kişisinin cüzdanına eklenecek ve A kişisinin cüzdanından düşülecektir. Yapılan bu işlemin kaydı şeffaf olarak izlenebilecek ve ağdaki tüm düğümlerde kayıtlı olacağından dolayı değiştirilmesi veya silinmesi mümkün olmayacaktır.

## 4. UZLAŞMA PROTOKOLLERİ (CONSENSUS PROTOCOLS)

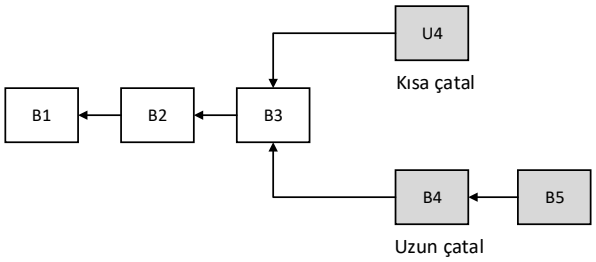
Blokzincirinin dağıtık yapısı gereği zincirdeki verilerin tümümün bir kopyası ağda bulunan her düğümde ayrı ayrı saklanmaktadır. Genel blokzinciri herkese açık olduğu için ağda güvenilmez düğümlere rastlanabilmektedir. Bu durumlarda düğümler arasında bir uzlaşmanın nasıl sağlanacağı, Bizans Generalleri (Byzantine Generals) problemine benzer bir sorun olarak karşımıza çıkmaktadır [35]. Bizans Generalleri probleminde, Bizans ordusunun bir kısmını komuta eden bir grup general düşman şehrini çevrelemiştir. Bazı generaller saldırmayı tercih ederken, diğer generaller geri çekilmenin daha doğru olacağını savunmaktadır. Bu durumda generallerin sadece bir kısmı şehre saldırırsa saldırı başarısız olacaktır. Bu sorunun üstesinden gelmek için tüm generallerin saldırmak veya geri çekilmek için bir anlaşmaya varmaları gerekmektedir.

Düğümler blokzinciri üzerinde veri eklemeye ve yayınlamaya başladıklarında, uyuşmazlıkların çözülmesi ve güvenlik ihlallerine karşı korumanın sağlanması için tüm düğümlerin ortak bir veri güncelleme protokolü üzerinde anlaşmaları sağlanmalı ve salt çoğunluğun onayı olmadan zincire yeni bir kayıt eklenmesi engellenmelidir. Bu gibi durumlarda blokzincirin tutarlılığının ve güvenliğinin sağlanması için uzlaşma protokolleri geliştirilmiştir. Nakatomo ilk uzlaşma protokolü olarak karmaşık kriptografik bulmacaların madenciler tarafından çözülmesine dayalı Proof of Work protokolünü sunmuştur [6]. Daha sonra araştırmacılar tarafından Proof of Work protokolünün zayıf yönlerinden hareketle Proof of Stake, Proof of Burn, Proof of Elapsed-time ve Proof of Capacity gibi protokoller sunulmuştur. Aşağıda bazı uzlaşma protokolleri hakkında bilgi verilmiştir [9].

### *4.1. İşin İspatı (Proof of Work)*

İşin ispatı (PoW), Bitcoin ağında kullanılan uzlaşma protokolüdür ve madencilik (mining) olarak adlandırılır

[6]. PoW protokolünde daha önceden belirlenmiş özelliklere sahip bir özet (hash) değerine ulaşmak için madenciler karmaşık hesaplamalar yapmaktadır. Belirlenen özet değerine ilk ulaşan madenci zincire yeni bir bloğu eklemeye hak kazanır. İlgili blok hesaplanan özet değeri ile diğer düğümlere yayınlandıktan ve tüm düğümlerden özet değerin doğruluk onayı alındıktan sonra blok zincire eklenir. Daha sonra tüm madencilerin yeni bloğu zincirlerine eklemesiyle zincirin bütünlüğü sağlanmış olur. Bu işlem sonunda bloğu yayınlayan madenci ödüllendirilir.




Şekil 7. Blokzincirin çatallanması
(Blockchain bifurcation)

Dağıtık ağ ortamında birden fazla madencinin belirlenen özet değerine aynı anda ulaşması ve aynı anda yayınlaması durumunda blokzincirinde Şekil 7'deki gibi çatallar oluşabilir. Ancak iki rakip çatalın aynı anda sonraki bloğu üretmesi olası değildir. Çatallanma olduktan sonra iki taraftaki madenciler de çalışmaya devam etmektedir. Çatalların birinde yeni bir blok yayınlanınca kısa çataldaki madenciler uzun çatala geçerek burada çalışmaya başlarlar. Örnek olarak Şekil 1'de U4 ve B4 olarak ayrılan iki çatal görülmektedir. B4 deki çatala yeni bir blok olarak B5 eklendikten sonra U4 çatalında bulunan madenciler B çatalına geçerek B6 bloğu için çalışmaya devam edecektir.

Madenciler PoW protokolünde çok sayıda bilgisayar gücü gerektiren işlemler yapmak zorunda kalmaktadır. Bu da çok fazla enerji ve bilgisayar gücü gerektirmekte ve zaman kaybına neden olmaktadır. Bu kayıpları azaltmak için içerisinde bazı ek uygulamaları içeren yeni PoW protokolleri geliştirilmiştir. Bunlara örnek olarak matematiksel hesaplamalar için kullanılabilecek özel asal sayı zincirleri üzerine çalışan Primecoin verilebilir [36].

### *4.2. Değerin İspatı (Proof of Stake)*

Değerin ispatı (PoS), PoW protokolüne alternatif enerji tasarrufu sağlayan bir uzlaşma protokolüdür. PoS protokolündeki madenciler bir para miktarının (değerin) sahipliğini kanıtlamak zorundadır. Bu protokolde daha fazla varlık sahibi kişilerin doğrulama işlemlerinde kullanılma olasılığı daha yüksektir. Bu şekilde hesap bakiyesine dayalı tercih çok adil olmamaktadır çünkü tek zengin kişinin ağda baskın olabilmesi mümkündür. PoS protokolünde iyileştirmeler için bir sonraki bloğun yayınlanmasına ilişkin farklı çözümler önerilmektedir. Örnek olarak Blackcoin ile sonraki madenci randomizasyon algoritması ile belirlenmekte ve kombinasyondaki en düşük özet değeri ve varlık miktarını kullanan bir fonksiyon sunulmaktadır [37]. Başka bir örnek olarak Peercoin, varlıkların oluşturulma zamanını dikkate alan bir seçim sunmaktadır [38]. Peercon' de daha eski ve daha büyük varlık kümelerinin sonraki bloğu oluşturmaları daha olasıdır.

PoW protokolü ile karşılaştırıldığında PoS protokolü büyük oranda enerji tasarrufu sağlamaktadır. Ama madencilik maliyeti neredeyse sıfır olduğu için ağa yapılacak saldırılara karşı daha savunmasız olabilmektedir. Birçok blokzinciri uygulaması başlangıçta PoW'u benimsemekte ve daha sonra PoS'a kademeli olarak dönüşüm sağlamaktadır. Örneğin, Bitcoin' den sonra dünyanın en büyük sanal parası olan Etherum bir çeşit PoW olan Ethash'tan [39] bir PoS türü protokol olan Casper'e [40] geçmeyi planlamaktadır.

### *4.3. PBFT (Practical Byzantine Fault Tolerance)*

PBFT, Bizans Generalleri problemine benzer sorunlar için çözüm sunan bir protokoldür. Hyperledger Fabric uygulaması, uzlaşma protokolü olarak PBFT protokolünü kullanarak, yeni bir bloğun eklenmesi aşamasında 1/3 oranında kötü niyetli Bizans Generalleri tarzı saldırılarının üstesinden gelmektedir [41]. Bu protokolde her bir değişiklik işlem öncesi, işlem ve işlem onayı olarak üç aşamaya ayrılır. Bir düğümün bir değişiklik yapabilmesi için ilgili değişiklik için her aşamada diğer düğümlerin 2/3' ünden daha fazla onay alabilmesi gerekmektedir. PBFT benzer olarak, Stellar Consensus Protokolü (SCP) de Bizans Generalleri gibi problemlere çözüm sunan bir protokoldür [42]. PBFT'de, her düğümün diğer düğümleri sorgulaması gerekirken SCP, katılımcı düğümlere hangi düğümlere inanılması gerektiğine dair öneri ve seçme hakkı verir.

### *4.4. DPOS (Delegated proof of stake)*

PoS protokolünde demokrasi uygulanırken, DPOS protokolünde ise temsili demokrasinin uygulanmaktadır. Ağdaki düğümler blok oluşturma ve doğrulama işlemleri için delegeler seçer ve blok doğrulama ve onaylama işlemleri az sayıda seçilmiş delege sayesinde çok hızlı yapılabilir. Bu arada, blok boyutu ve blok aralıkları gibi ağ parametreleri delegeler tarafından düzenlenebilir. Bitshares uygulaması, uzlaşma protokolü olarak DPOS kullanmaktadır [43].

### *4.5. Ripple*

Ripple, büyük bir ağda bulunan güvenilir alt ağların uzlaşmasına dayalı bir protokoldür [44]. Ağdaki düğümler,

uzlaşma süreçlerine katılımcı olan sunucu düğümler ve sadece varlık transferi yapan istemci düğümler olarak ikiye ayrılmaktadır. Zincirde bir işlemin onaylanması sırasında uzlaşmaya katılımcı düğümlerin uzlaşma oranlarına bakılır, bu oran % 80 ve üzerinde bir değere ulaşabilmişse işlem onaylanır ve tüm ağ için yayınlanır.

Tablo 2. Uzlaşma Protokollerinin Karşılaştırılması [9], [45]
(Comparison of Consensus Protocols)

| Kriter | PoW | PoS | PBFT | DPOS | Ripple |
|---|---|---|---|---|---|
| Ağa düğüm eklenmesi | Açık | Açık | İzin gerekir | Açık | Açık |
| Enerji tasarrufu | Hayır | Kısmen | Evet | Kısmen | Evet |
| İşlem kabulü için onay oranı | >25% bilgis ayar gücü | >51% değer | >66% onay | >51% doğrulama | >80% onay |
| Örnek uygulama | Bitcoi n[6] | Peercoin [38] | Hyperledg erFabric[4 1] | Bitshares[ 43] | Ripple[4 4] |

Tablo 2'de uzlaşma protokolleri ağa yeni bir düğüm eklenmesi, enerji tasarrufu, bir işlemin kabulü için gerekli onay oranı ve örnek uygulama kriterlerine göre karşılaştırılmıştır [45]. PBFT protokolünde ağa yeni bir düğüm eklenmesi aşamasında ilgili düğümün bilgilerinin tanımlanması gerekmektedir. Diğer uzlaşma protokollerinde herhangi bir kısıtlama olmadan ağa yeni bir düğüm eklenebilmektedir. Enerji tasarrufu bakımından bir karşılaştırma yapılırsa, PoW protokolünde madenciler karmaşık bilgisayar hesaplamalarını çözmek için çok fazla elektrik ve bilgisayar gücü harcamaktadır. PoS ve DPOS protokollerinde madencilerin yaptıkları işlemler, çok daha az enerji ile tamamlanabilmektedir. PBFT ve Ripple protokollerinde madencilik yapılmamaktadır dolayısıyla diğer protokollerle karşılaştırıldığında büyük oranda enerji tasarrufu sağlanmaktadır. PoW protokollerinde ağın kontrol edilmesi için genellikle 51% oranında özet değeri çözümü gerekmektedir. Ama bencil madencilik stratejileri ile bu değer 25% oranlarına inebilmektedir. PBFT protokolünde bir düğümün kabul edilmesi için diğer düğümlerden 2/3 oranından onay alması gerekmektedir. Ripple protokolünde ise bu oran 80%'dir. Bu uzlaşma protokollerini kullanan uygulamalar için birer örnek vermek gerekirse, PoW için Bitcoin, PoS için Peercoin, PBFT için Hyperledger Fabric, DPOS için Bitshares, Ripple protokolü için ise Ripple uygulaması gösterilebilir.

İyi bir uzlaşma protokolü verimli, kullanışlı ve güvenli olmalıdır. Son zamanlarda, blokzincirindeki uzlaşma protokollerini geliştirmek için bir dizi çalışma yapılmıştır. Bu çalışmalardan biri olan PeerCensus blok oluşturma ve onaylama işlemlerinin birbirinden ayırarak uzlaşma işlemlerini önemli ölçüde hızlandırmayı hedeflemiştir [45]. Yüksek blok üretim oranları Bitcoin gibi PoW kullanılan uygulamaların güvenliğini riske atabilmektedir. Kraft, bir bloğun sabit bir hızda üretilmesini sağlamak için GHOST adlı zincir seçim kuralını önermiştir [46]. GHOST, en uzun zincir dalı yerine, dalların yüklerini dikkate alarak madenciler için daha verimli seçimler yapılmasını sağlayabilmektedir. Chepurnoy vd. ise madenciler için önceki blokların tüm verisi yerine sadece blok başlıklarının saklanmasına ilişkin bir çözüm sunmuştur [47].

## 5. AKILLI SÖZLEŞMELER (SMART CONTACTS)

Akıllı sözleşme, ilk kez 1993 yılında Nick Szabo tarafından "bir sözleşmenin şartlarını yerine getiren bilgisayarla işletilen bir işlem protokolü" olarak tanımlamıştır. Blokzinciri teknolojisi ortaya çıkmadan önce bu teknolojik olarak imkânsızdı. Blokzincirin akıllı sözleşmeleri desteklemek için ideal bir teknoloji olduğu ortaya çıkmıştır. Buna ek olarak akıllı sözleşmeler de blokzincirin gelişimine ve yaygınlaşmasına katkıda bulunmuştur. Akıllı sözleşmeler, blokzinciri 2.0 olarak bilinen ikinci nesil blokzincirin oluşmasını sağlamıştır. Akıllı sözleşmeler, güvenilir bir ortamda merkezi denetim olmadan klasik sözleşmelerin yerini alabileceğini vadetmektedir [10]. Akıllı sözleşmeler, bir dizi olayın yürütülmesi için uzlaşma protokollerini kullanan blokzinciri sistemleri üzerinde çalışan bir programın parçalarıdır. Akıllı sözleşmelerin özelliklerinden bazıları şunlardır [48]:

- Akıllı sözleşmeler, blokzinciri platformunda çalışan makine tarafından okunabilen yazılım kodu parçalarıdır.
- Akıllı sözleşmeler, olay odaklı programlardır.
- Akıllı sözleşmeler, oluşturulduktan sonra izlenmeye gerek duymadan otomatik olarak çalışır.
- Akıllı sözleşmeler, merkezi otoriteden bağımsız, dağıtılmış yapıdadır.

Bir akıllı sözleşme adres, fonksiyonlar ve belirlenen durumlardan oluşur [49]. Akıllı sözleşme için benzersiz bir adres tanımlanır ve blokzinciri üzerinde bu adres ile saklanır. Önceden belirlenen durumların oluşması sonucu ilgili fonksiyonlar tetiklenir ve sözleşmenin gerekleri otomatik olarak yerine getirilir. Burada akıllı sözleşmenin değiştirilemezliği, tutarlılığı ve şeffaflığı blokzinciri tarafından sağlanmaktadır. Bitcoin blokzinciri basit bir betik dili (scripting language) sunmaktadır ve bu durumun akıllı sözleşmeler için yetersiz olduğu ortaya çıkmıştır [10]. Bu da akıllı sözleşmelerin entegrasyonuna imkân veren yeni blokzinciri uygulamalarının ortaya çıkmasına yol açmıştır. Günümüzde akıllı sözleşmelerin geliştirilmesine imkân veren en önemli blokzinciri uygulaması Ethereum' dur [29]. Ethereum üzerindeki akıllı sözleşmeler yığın tabanlı (stack-based) Ethereum sanal makine kodu (Ethereum virtual machine code) ile geliştirilmektedir. Ethereum ve diğer blokzinciri sistemleri

üzerinde akıllı sözleşmeler geliştirmek için genellikle ileri seviye bir dil olan Solidity kullanılmaktadır [50].

Akıllı sözleşmeler banka, noter ve benzeri üçüncü tarafları aradan çıkarmaktadır, dolayısıyla maliyet, hız ve güvenlik bakımından önemli avantajlar sağlamaktadır. Akıllı sözleşmelerde bütün işlemler bilgisayar sistemleri tarafından elektronik olarak yürütülmektedir. Bu durum iletişim sorunları, yazılım hataları (bugs), virüs, ağ saldırıları gibi durumlarda sistemin tamamen ya da kısmen çalışmaz hale gelmesine neden olabilir. Akıllı sözleşmelerin müşteriler ve katılımcılar tarafından yaygın olarak kullanılabilmesi için güvenliğinin ve doğru çalışacağının garanti edilmesi çok önemlidir. Gelecek yıllarda bu alanda yapılacak çalışmaların faydalı olacağı düşünülmektedir [51]. Ayrıca geleneksel sözleşmelerde ölçülebilir olmayan hükümler ve koşullar yer alabilmektedir. Bu kapsamda geleneksel sözleşmelerin bilgisayar sistemleri tarafından temsil edilebilmesi ve çalıştırılabilmesi için akıllı sözleşmelere göre modellenmesi gerekmektedir. Ek olarak kullanıcılar için akıllı sözleşmelerin oluşturulması, incelenmesi ve anlaşılması için araçlara (uygulamalara) ihtiyaç duyulmaktadır [52].

Akıllı sözleşmelerin kullanımı durumunda faydalı olabileceği alanlardan bazıları şunlardır;

**Tedarik Zinciri Uygulamaları:** Taşımacılık ve gıda gibi farklı alanlarda tedarik zinciri uygulamaları kullanılmaktadır. Blokzinciri sistemleri bu tür uygulamaların daha şeffaf, daha güvenilir ve merkezi otoriteden daha bağımsız hale getirmektedir. Bu uygulamalarda akıllı sözleşmelerin kullanılması durumunda şeffaflık ve güvenliğin yanında bir otomatizasyon da sağlanabilmesi mümkün olacaktır.

**Nesnelerin İnterneti (İnternet of Things, IoT):** Nesnelerin interneti gelecek vadeden araştırma alanlarından biridir. IoT cihazları daha az bellek ve işlem gücüne sahip cihazlardır ve sayıları çok hızlı artmaktadır. Blokzinciri tabanlı akıllı ev, akıllı şehir ve akıllı taşımacılık gibi araştırma konularında çalışmalar yapılmaktadır. Bu alanda akıllı sözleşmelerin kullanımı durumunda IoT teknolojileri daha etkili, daha özerk ve daha otomatik çalışır hale gelebilecektir.

**Sağlık Uygulamaları:** Yakın zamanda, geliştirilen cihazlar ve yardımcı teknolojiler sayesinde insanlar evlerinden sağlık durumlarını izleyebilmektedir. Blokzinciri teknolojisi, hasta mahremiyeti ve bilgilerin dağıtık yapıda saklanması alanlarında faydalı olmaktadır. Bu sistemleri daha güvenilir ve otomatik hale getirmek için Akıllı sözleşmelerden faydalanılabilir. Toplanan sağlık verileri sonuçlarına veya ortaya çıkan durumlara göre yapılması gereken işlemlerin otomatik olarak tetiklenmesi sağlanabilir.

**Sigorta Uygulamaları:** Geleneksel sigorta çözümlerinde belirsizlikler ve uzun sonuç alma süreleri bulunmaktadır. Süreçlerdeki belirsizlikleri ortadan kaldırarak akıllı sözleşmelerin entegrasyonu sağlanırsa üçüncü bir taraf müdahalesi olmadan çok hızlı ve şeffaf sonuçlar elde edilebilir.

**Finans Uygulamaları:** Akıllı sözleşmeler yapısı gereği çek, kredi, kiralama gibi birçok finansal alanda kullanılabilir.

**Gayrimenkul Uygulamaları:** Geleneksel gayrimenkul sistemleri zaman alıcı ve riskli süreçler içermektedir. Ayrıca yasal zorunluluklar gereği kâğıt israfı ve ıslak imza gibi zorunluluklar da bulunmaktadır. Akıllı sözleşmeler sayesinde üçüncü taraf bir kurum aracılığına ihtiyaç duymadan alım satım yapılabilir ve yapılan işlemler şeffaf olarak dijital defterlerde saklanabilir.

**Telif Hakkı Uygulamaları:** Telif hakkı içeren ürünler farklı oranlarda ödeme şartları gerektirebilmektedir. Bu tür uygulamalarda akıllı sözleşmelerin kullanılması faydalı olabilir.

## 6. ZORLUKLAR VE SON GELİŞMELER (CHALLENGES AND RECENT ADVANCES)

Blokzinciri teknolojisinin sahip olduğu büyük potansiyele rağmen yaygın kullanımını sınırlayan bazı zorluklar da bulunmaktadır. Karşılaşılan zorluklardan bazıları ve bu durumlara karşı önerilen çözümler aşağıda açıklanmıştır.

### *6.1. Ölçeklenebilirlik (Scalability)*

Günden güne artan işlem sayılarından dolayı blokzinciri sistemlerinin boyutu periyodik olarak artmaktadır. Blokzinciri ağında bulunan her düğüm doğrulama ve uzlaşma işlemleri için tüm blokzinciri verisini saklamak zorundadır. Bu da blokzincirin giderek hantal bir hale gelmesine neden olmaktadır [9]. Blok kapasitesi ve blok yayınlama hızı gibi sınırlılıklar nedeniyle zincirde belirli bir sürede onaylanan işlem sayısı sınırlı olmaktadır. Örneğin Bitcoin blokzincirinde saniyede yaklaşık 7 işlem onaylanabilmektedir [53]. Diğer ödeme sistemleriyle karşılaştırıldığında Bitcoin çok yavaş kalmaktadır. Örneğin VISA ağı (VisaNet) saniyede 65.000 işlem gerçekleştirebilme kapasitesine sahiptir [54]. Blokzincirin blok yapısından kaynaklanan sınırlılıkların dışında, madencilerin yüksek gelir elde edebilmek için büyük miktardaki para transferine öncelik vermesi ve küçük miktardaki işlemleri göz ardı etmeleri nedeniyle de işlem sürelerinde gecikmeler yaşanabilmektedir.

Ağdaki bir düğümün tüm blokzinciri verisini saklaması ve devamlı güncel tutması sistemin çalışmasını zorlaştırmaktadır. Bruce, bu duruma çözüm olarak eski işlem kayıtlarının dikkate alınmadığı bir sistem tasarlamıştır [55]. Bu sistemde hesap ağacı adlı bir veritabanı oluşturulmakta ve bakiyesi boş olmayan tüm hesap verileri burada saklanmaktadır. VerSum uygulamasında [56] ise bilgisayar gücü düşük olan düğümlerin de büyük hesaplamalar içeren ve büyük kazanç sağlayan işlemlere katılmasına olanak sağlanmıştır.

Eyal vd. tarafından Bitcoin' in yeni jenerasyonu olan Bitcoin-NG tasarlanmıştır [57]. Bitcoin-NG' de blokzinciri bloğu, yapılan işlem detaylarının kaydedilmesi ve lider seçim işlemleri olarak ikiye ayrılmaktadır. Bitcoin-NG aynı zamanda blok oluşturma zamanını da bölümlere ayırarak blok oluşturma işlemini hızlandırmaktadır.

### *6.2. Mahremiyet (Privacy)*

Blokzincirinde kullanıcılar gerçek kimliklerini kullanmadan kendilerine ait genel ve özel anahtarlar ile işlem yapabilmekte ve kullanıcı mahremiyeti önemli oranda korunabilmektedir. Aynı zamanda blokzincirinde yapılan bir işlemin şeffaflığı esas olduğu için gönderen, alıcı, zaman ve transfer edilen değer gibi veriler herkesin görebileceği şekilde yayınlanmaktadır. Bu da kullanıcıların yaptıkları tüm işlem kayıtlarının, kimlerle alışveriş yaptıklarının ve bakiye bilgilerinin elde edilmesine olanak vermektedir. Paylaşılan bu verilerin üçüncü taraflar tarafından analiz edilmesi sonucu kullanıcıların gerçek kimliklerine erişim de mümkün olabilmektedir [58]. Blokzincirinde karşılaşılabilecek bu tür mahremiyet ihlallerine karşı anonimliği geliştirmek için bazı çalışmalar yapılmıştır. Bu çalışmalar iki kategoride incelenebilir;

*Karıştırma:* Blokzincirinde kullanıcı adresleri gerçek kimliklerinden bağımsızdır. Ama birçok kullanıcı tüm işlemlerini aynı adres üzerinden yapmaktadır, bu da kullanıcının gerçek kimliğine erişim imkânı vermektedir. Karıştırma hizmeti verilerin çoklu gönderen adreslerden toplanarak çoklu alıcı adreslere iletilmesini sağlamaktadır. Örneğin A kişisi B kişisine bir miktar para göndermek istediğinde direkt olarak B kişisinin cüzdanına para gönderdiğinde A ile B kişisinin alışveriş ilişkisi ortaya çıkabilir. Bunun yerine A kişisi parayı güvenilir bir üçüncü taraf olarak C kişisine, C kişisi de g1, g2, g3 .. gibi gönderim adreslerinden a1, a2, a3 .. gibi alıcı adreslere göndererek daha sonra paranın B kişisine ulaşmasını sağlayabilir. Bu şekilde yapılan para transferinde A kişisi ile B kişisi arasındaki ilişkiyi ortaya çıkarmak çok zorlaşmaktadır. Ancak bu tür para transferlerinde aracı olarak kullanılan üçüncü taraf kişilere güvenmek zorunda kalınmaktadır. Bu kişilerin kötü niyetli olması durumunda para transferi gerçekleşmeyebilir ya da kullanıcı bilgileri başkaları tarafından elde edilebilir.

Mixcoin uygulamasında [59], karıştırma yöntemi ile para gönderimi işlemlerinde transfer edilen para miktarı, transfer tarihi, alıcı ve gönderici kişilerin bilgileri şifrelenerek, kullanıcı bilgilerinin ve transfer edilen para miktarının üçüncü taraflar tarafından elde edilmesi engellenebilmektedir. Coinjoin uygulaması [60] hırsızlığı önlemek için merkezi bir karıştırma sunucusu tarafından alıcı adreslerin karıştırılmasını sağlamaktadır. CoinShuffle uygulaması [61] ise hem şifreleme hem de adres karıştırma yöntemlerini kullanmaktadır.

*Anonimleştirme:* Zerocoin uygulaması [62], kullanıcı mahremiyetinin sağlanması için madencilik ve dijital imza ile doğrulama yerine, tek taraflı bir şifreyle doğrulama işlemi yapmayı sağlayan sıfır bilgi kanıtı (zero-knowledge proof) yöntemi kullanmaktadır. Bu şekilde transfer işlemi ile kişinin arasındaki ilişki gizlenmiş olmaktadır. Zerocash uygulamasında [63] gelişmiş bir zero-knowledge proof yöntemi olan olan zk-SNARKs kullanılmıştır. Bu sayede transfer edilen para miktarı da gizlenebilmektedir.

### *6.3. Blok Atma Saldırısı (Selfish Mining)*

Blokzinciri, birlikte hareket eden kötü niyetli madencilerin saldırılarına karşı savunmasızdır. Eyal ve Sirer, ağın küçük bir bölümüne ait bilgisayar gücünün kötü niyetli saldırılarında bile blokzincirin savunmasız kalabileceğini bildirmiştir [64]. Blok atma saldırısında kötü niyetli madenciler oluşturdukları blokları yayınlamadan bekletirler ve gerekli şartlar oluştuktan sonra kendi bloklarını kullanarak özel zincir dallarını yayınlarlar. Sonuç olarak zincirde Şekil 7'deki gibi bir çatallanma meydana gelir. Özel zincir dalı asıl zincirden uzun olduğunda bütün madenciler yanılarak bu sahte dal için madencilik yaparak zamanlarını ve güçlerini boşa harcamış olmaktadır. Kötü niyetli madenciler ise bu süreçte hem rakipleri yanıltarak onların zamanlarını ve gücünü boşa harcamasına neden olmakta hem de kendi dalları üzerinden haksız kazanç elde edebilmektedir. Blok atma saldırılarına karşı Heilmann dürüst madenciler için istedikleri zincir dalını seçme fırsatı vermiştir [65]. Bu şekilde dürüst madenciler zaman damgası gibi kriterlere göre doğru dallara ait blokları seçebilmektedir. Blok atma saldırılarına karşı başka bir çözüm de ZeroBlock uygulaması [66] tarafından sağlanmıştır. Bu uygulamada her blok belirli bir maksimum zaman içerisinde kabul edilmeli ve yayınlanmalıdır. Bu sayede kötü niyetli madencilerin hazır blokları bekletmesi engellenmiş olup, hak ettiklerinden fazla ödül almasının önüne geçilmektedir.

## 7. BLOKZİNCİRİ TEKNOLOJİSİNİN UYGULAMA ALANLARI VE ÖRNEKLERİ (APPLICATION AREAS OF BLOCKCHAIN AND EXAMPLES)

Blokzincirin 2016 ve 2017 yıllarında geniş kitleler tarafından tanınmaya başlanması sayesinde blokzinciri konulu araştırmaların ve uygulamaların sayısında önemli bir artış görülmüştür. Bu adaptasyon sürecinin çok hızlı olmasından dolayı pek çok gerçekçi olmayan öneriler ve beklentiler ortaya çıkmıştır. Hatta blokzinciri konusuyla ilgilenen yatırımcıları kandırmak amacıyla yapılan sahtekârlıklara da rastlanmıştır [7]. Bu nedenle blokzinciri teknolojisinin olası uygulama alanlarının anlaşılması önem taşımaktadır.

Hileman ve Rauchs' a göre gelecekte blokzinciri uygulama alanlarının 30%' unun finans ve bankacılık, 13%' nün kamu 12%' sinin sigortacılık ve 8%' inin sağlık sektörlerinde olacağı tahmin edilmiştir [67]. Bazı araştırmacılar ise blokzinciri teknolojisinin hala çok yeni bir çalışma alanı olarak kabul etmiş, her sektörün bu teknolojiden yüksek beklentileri olduğunu belirtmiş ve blokzinciri uygulamalarının adaptasyonu bağlamında bu sektörlerin özelliklerinin incelenmesi gerektiğini ifade etmiştir [68], [69]. Aşağıda farklı sektörlerde yapılmış önemli blokzinciri uygulamaları hakkında bilgi verilmektedir.

### *7.1. Finans* (Finance)

Blokzinciri, sanal para olarak adlandırılan uygulamalar sayesinde finans sektöründe yaygın olarak kullanılmaktadır. Bunlara örnek olarak Bitcoin [6], Ethereum [29] ve Ripple [44] gibi uygulamalar gösterilebilir. Sanal para uygulamaları dışında birçok alanda blokzinciri uygulamalarına rastlamak mümkündür. Blokzinciri sistemleri ve akıllı sözleşmelerin yapıları gereği noterlik hizmetlerinde kullanılması çok faydalı olabilir. Noterlik hizmetleri için mevcut blokzinciri sistemleri ihtiyaca göre özelleştirilip kullanılabilir, ya da bitcoin notary [70] ve stampd [71] gibi hazır çözümlerden faydalanılabilir. Sigortacılık alanında önemli bir uygulama olarak müşteri bilgilerini blokzinciri üzerinde saklanmasına ve paylaşılmasına olanak veren B3i uygulaması Avrupa' da hizmet veren beş büyük sigorta firması tarafından oluşturulmuştur [72]. Blokzincirinin kullanım alanlarından biri de bağış sistemleridir. Nor vd. tasarladığı sadaka sistemi ile bağış yapan ve ihtiyaç sahibinin birbirini tanımadan şeffaf ve güvenli bir şekilde bağış süreçlerinin yönetilmesi hedeflemiştir [73]. Ayrıca bağış sistemleri için CAF (Charities Aid Foundation) gibi blokzinciri tabanlı hazır bağış uygulamaları da bulunmaktadır [74].

### *7.2. Kamu Hizmetleri (Public Services)*

Blokzinciri sistemlerinin en fazla uygulandığı alanlardan biri de kamu hizmetleri alanıdır. Birçok devlet çeşitli alanlarda blokzinciri teknolojisine yatırım yapmaktadır. 2018 OECD raporuna göre dünya genelinde 2017 yılında 26 farklı ülke tarafından 117 blokzinciri hizmeti girişimi ve uygulaması yapılmışken, 2018 yılında 45 ülke tarafından 202 girişim ve uygulama hayata geçirilmiştir [75]. Kamu hizmetlerinde kullanılan blokzinciri uygulamalarından bazıları şunlardır;

*BenBen:* Gana' da tüm tapu kayıtlarının Ethereum sistemi üzerinde tutulmasını sağlayan bir projedir. Bu projede tüm tapu parselleri ve arazi sahipleri blokzinciri üzerinde tutulmakta ve diğer paydaş kurumlar ile paylaşılmaktadır. BenBen sayesinde Gana'da gayrimenkul alım satım süreleri 75% oranında kısalmış ve hukuki anlaşmazlıkların sayısı ciddi oranda azalmıştır [76].

*E-estonia:* Blokzinciri teknolojilerine en fazla yatırım yapan ülkelerden biri de Estonya'dır. Estonya' da gerekli yasal düzenlemeler yapılmış olup dijital kimlik, dijital sağlık, dijital vergilendirme gibi hizmetlerin blokzinciri üzerinde tutulması ve paydaş kurumlar tarafından paylaşılmasına olanak veren sistem hayata geçirilmiştir [77].

*Project Ubin:* Singapur Para Yönetimi Kurumu ülkedeki bankalar arası para transferlerini incelemiş ve yapılan transferlerin verimsiz ve yavaş olduğunu tespit etmiştir. Bunun üzerine Singapur Para Yönetimi Kurumu ve bankalar arası ortak bir kurul tarafından birlikte yapılan bir çalışma sonucu bankalar arası Singapur Doları transferlerini blokzinciri üzerinden yapılmasını sağlayan bir sistem geliştirilmiştir. Geliştirilen sistem şuan inceleme ve test aşamasında olup kaynak kodları GitHub üzerinde paylaşılmıştır [78].

*The Voatz:* Eylül 2018' de Amerika Birleşik devletlerinin Virginia eyaletinde ülke dışında bulunan vatandaşların bulundukları ülkelerde senato seçimlerinde oy kullanabilmesi için blokzinciri tabanlı Voatz adlı uygulama kullanılmıştır [79].

*Vehicle Wallet:* Danimarka'da her araç için üretim, tamirat, kiralama, mülkiyet değişikliği, hurdaya çıkma gibi bilgilerin blokzinciri üzerindeki dijital cüzdanlarda saklanmasına olanak veren bir projedir. Bu proje sayesinde alım satım süreçlerindeki riskler azaltılmıştır. Aynı zamanda Danimarka Vergi Kurumlarının araç cüzdanlarına erişimi sayesinde vergi tahsilatlarının etkili bir şekilde yapılmasına olanak sağlanmıştır [80].

### *7.3. Sağlık (Health)*

Blokzinciri, sağlık alanındaki uygulamaların birlikte çalışabilirlik sorunlarının üstesinden gelme konusunda büyük bir potansiyele sahiptir [81]. Blokzinciri, sağlık kurumları ve ilaç araştırmacıları gibi paydaşların elektronik sağlık verilerini güvenli bir şekilde paylaşmalarını sağlayan bir standart olarak kullanılabilir. Sağlık verilerinin paylaşılması tıbbı hizmetlerin kalitesinin artmasına ve hekimler için öneriler geliştirilmesine olanak sağlayabilir [82]. Bu kapsamda Yue vd. geliştirdikleri uygulama ile mobil cihazlar aracılığıyla hasta verilerine kolayca paylaşılması ve analiz edilmesini hedeflemiştir [83]. Sunulan uygulama, hasta mahremiyetini tehlikeye atmadan verilerin analiz edilmesini ve verilerin doktorlar, hastalar ve diğer çalışanlar dahil kimse tarafından değiştirilmesine olanak vermeden blokzinciri yapısında saklanmasını sağlamaktadır. Azaria vd. hasta verilerinin blokzinciri üzerinde yönetilmesi için MedRec adlı bir sistem tasarlamıştır [27]. Bu sistem ile tüm blokzinciri verisi ağdaki tüm düğümlere dağıtılmakta ve yeni bir kayıt eklemek ya da kayıtları izlemek gibi işlemler yetki kontrolleri çerçevesinde yönetilmektedir. Ayrıca farklı düğümlerde tutulan hasta verileri kullanıldığı akıllı sözleşmelerde kullanılmıştır. Mettler tarafından yapılan bir araştırmada hastaların mahremiyeti korunarak verilerine diğer sağlık kurumları tarafından da erişilmesine olanak tanınmıştır [81]. Böylece hastaların geçmişteki tüm tedavileri şeffaflaştırılarak hekimlerin erişimine açılmıştır. Ek olarak hasta verilerinin saklanması, yönetilmesi ve paylaşılması konularının araştırıldığı MedVault [84] ve BitHealth [85] gibi çalışmalar yapılmıştır.

### *7.4. Tedarik Zinciri (Supply Chain)*

Nesnelerin interneti kavramı ile elektronik cihazlar ve insanlar arasında bir bağlantı kurmak mümkün olmuştur. Nesnelerin interneti ve blokzinciri teknolojilerinin uygulama alanlarından biri de tedarik zinciri sistemleridir. Blokzinciri ile gıda işleme, ulaşım ve lojistik gibi alanlarda üçüncü taraflar olmadan sistemlerin otomatikleşmesi, şeffaflığı ve güvenliği sağlanabilecektir [48]. Tian vd. yaptıkları çalışmada gıda kalitesi ve güvenliğini takip edebilmek için blokzinciri ve RFID teknolojilerinden faydalanılabileceğini belirtmiştir [86]. Araştırmacılar bu çalışmada gıda ürünlerini hasat ortamından market raflarına kadar RFID teknolojisi sayesinde takip edilebileceğini ve tüm bu taşıma verilerinin blokzinciri üzerinde tutularak veri güvenliğinin sağlanabileceğini ifade etmiştir. Bu çalışmaya göre blokzinciri sayesinde üretici, taşımacı, perakende satıcısı ve müşterilere gıda ürünlerinin kalite ve güvenliklerine ilişkin sorgulamalar yapabilme imkânı verilecektir. Tedarik zincirinde ürünlerin izlenilebilirliği üzerine başka bir çalışma da Lu ve Xu tarafından yapmıştır [87].

### *7.5. Eğitim (Education)*

İngiltere' de bulunan Open University tarafından yayınlanan "Innovating Pedagogy 2016" adlı raporda eğitim alanında blokzinciri kullanımının 4 yıldan uzun bir süre içerisinde yaygınlaşacağı belirtilmiştir [88]. Raporda blokzinciri üzerinde eğitim içeriklerinin, ders kredilerinin ve sertifika bilgilerinin dağıtık yapıda saklanabileceği ve paylaşılabileceği ifade edilmiştir. Avrupa Komisyonu 2017 yılında "Blockchain in Education" adlı bir rapor yayınlamıştır [89]. Bu raporda blokzinciri teknolojisinin sertifikasyon, hayat boyu öğrenme, harç ücreti ödemeleri ve öğrencilere burs ödemeleri gibi alanlarda kullanım senaryoları önerilmiştir. Bu alanda yapılmış çalışmalara örnek olarak Turkanavic vd. tarafından geliştirilen EduCTX uygulaması gösterilebilir [90]. Bu uygulama sayesinde yükseköğretim öğrencilerinin tamamladıkları ders kredileri blokzinciri üzerinde ağdaki tüm kurumlar tarafından saklanmaktadır. Bu sayede öğrenciler farklı kurumlarda tamamladıkları ders kredilerini blokzincirindeki hesaplarında görebilmektedir. Ayrıca katılımcı tüm yükseköğretim kurumları başvuru, belge doğrulama gibi işlemleri blokzinciri üzerinden yönetebilmektedir. Karataş tarafından yapılan çalışmada Moodle uygulaması üzerinde çalışan sertifika modülünün blokzinciri ile entegrasyonu sağlanmış ve dijital sertifikalar blokzinciri üzerinde saklanabilmiştir [91].

## SONUÇ (CONCLUSION)

Blokzinciri, şeffaflığı ve merkezi otoriteyi ortadan kaldıran dağıtık yapısı sayesinde bilgi teknolojilerinde yeni bir dönemin başlangıcı olarak ifade edilebilir. Basın, sosyal medya, uluslararası kuruluşlar özel sektör ve kamu kurumları blokzinciri konusuna büyük ilgi göstermektedir ve alanyazın incelendiğinde son birkaç yılda blokzinciri konulu çalışmaların sayısının hızla arttığı görülmektedir. Akademik çalışmalar ve piyasadaki uygulamaları arttıkça blokzinciri teknolojisinin bazı sınırlılıkları da ortaya çıkmıştır. Yeni bir teknoloji olan blokzincirin yaygın kullanımı durumunda karşılaşılan performans ve güvenlik sorunlarına karşın geliştirilen çözümler bu teknolojinin olgunlaşmasına öncülük etmektedir. Çalışmada blokzinciri teknolojisinin özellikleri, genel yapısı, çalışma prensibi, uzlaşma protokolleri, akıllı sözleşmeler ve uygulama alanları hakkında ayrıntılı bilgi verilmiştir. Blokzinciri mevcut yapısı, çalışma şekli, uygulama alanları ve vadettiği fırsatlar bakımından daha fazla araştırma potansiyeline sahip görülmektedir.

Blokzinciri teknolojisi iş dünyasının iş yapış şekillerini değiştirebileceği, ülkeler bağlamında sınırların kalkmasına ve ortak dili konuşma noktasında destek olacağı anlaşılmaktadır. Örnek olarak bankacılıkta bir ülkeden başka bir ülkeye para aktarmada (swift) ücret ödeme ve zorluğu varken dijital paralarla saniyeler içinde küçük masraflar ile aktarımının sağlanması gerçekleşmektedir. Blokzinciri gibi merkeziyetçi yapıları ortadan kaldıran

şeffaf ve hesap verebilir teknolojilerin ortaya çıkması ve gelişimi sonrasında iş dünyasının bu değişime ayak uydurması, ülkelerin bunlara göre kendini, yönetimlerini, kanunlarını yeniden düzenlemesi gerektiği anlaşılmaktadır. Bu kapsamda eğitim müfredatlarında blokzinciri gibi yeni teknolojilere yer verilmesi, çağın yeterliklerine sahip insan kaynağının yetişmesi, bu teknolojilerin uygulama sahasının gelişmesine ve daha doğru anlaşılmasına katkı sağlayacaktır. Bu alanda yetişmiş insan gücü kurum/kuruluşların küresel ekonomide daha rekabetçi hale gelerek daha fazla katkıda bulunma imkânına sahip olacaktır.

## KAYNAKLAR (REFERENCES)


[1] K. Sultan, U. Ruhi, R. Lakhani, "Conceptualizing Blockchains: Characteristics and Applications", **11th IADIS International Conference on Information Systems**, 49–57, 2018.

[2] Internet: Blockchain Distributed Ledger Market Size by Type, End-User, Allied Market Research Report 2017, https://www.alliedmarketresearch .com/blockchain-distributed-ledger-market, 15.10.2018.

[3] R. Anascavage, N. Davis, "Blockchain Technology: A Literature Review", 2018.

[4] D. Tapscott, A. Tapscott, "how the technology behind bitcoin is changing money, business and the world", *Blockchain revolution*.

[5] S. Haber, W. S. Stornetta, "How to time-stamp a digital document" *Journal of Cryptology*, 3(2), 99–111, 1991.

[6] Internet: S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System,http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986, 08.10.2018.

[7] K. Zile, R. Strazdiņa, "Blockchain Use Cases and Their Feasibility", *Applied Computer System*, 23(1), 12–20, 2018.

[8] R. Beck, "Beyond Bitcoin: The Rise of Blockchain World", *Computer*, 51(2), 54–58, 2018.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", **Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017**, 557–564, 2017

[10] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, "On blockchain and its integration with IoT Challenges and opportunities", *Future Generation Computer Sysems.*, 88, 173–190, 2018.

[11] F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis", *HICSS*, 2017.

[12] B. A. Tama, B. J. Kweka, Y. Park, K.-H. Rhee, "A critical review of blockchain and its current applications", **2017 International Conference on Electrical Engineering and Computer Science (ICECOS)**, 109–113, 2017.

[13] H. Halpin, M. Piekarska, "Introduction to Security and Privacy on the Blockchain", **2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)**, 1–3, 2017.

[14] F. Hawlitschek, B. Notheisen, T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy", *Electronic Commerce Research Application*, 29, 50–63, 2018.

[15] J. L. Zhao, S. Fan, J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue", *Finance Innovation*, 2(1), 28, 2016.

[16] I. Nath, "Data Exchange Platform to Fight Insurance Fraud on Blockchain", **2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)**, 821–825, 2016.

[17] Internet: A. Lewis, So, You Want to Use a Blockchain for That ?, https://www.coindesk. com/want-use-blockchain/, 09.10.2018.

[18] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaria, "To Blockchain or Not to Blockchain: That Is the Question", *IT Professional*, 20(2), 62–74, 2018.

[19] J. C. Cheng, N. Y. Lee, C. Chi, Y. H. Chen, "Blockchain and smart contract for digital certificate", **Proceedings of 4th IEEE International Conference on Applied System Innovation**, 1046–1051, 2018.

[20] M. Swan, **Blockchain: Blueprint for a New Economy**, 2015.

[21] D. Efanov, P. Roschin, "The all-pervasiveness of the blockchain technology", *Procedia Computer Science*, 123, 116–121, 2018.

[22] K. Burgess, "The Promise of Bitcoin and the Blockchain", *Consumers Research Primary*, 2015.

[23] S. Narayanan, A., Bonneau, J., Felten, E., Miller, A. Goldfede, **Cryptocurrency Technologies: A Comprehensive Introduction**, 2016.

[24] T. Moore, "The promise and perils of digital currencies", *International Journal of Critical Infrastructure Protection*, 6(3–4), 147–149, 2013.

[25] J. Sun, J. Yan, K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities", *Finance. Innovation*, 2(1), 2016.

[26] J. J. Sikorski, J. Haughton, M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market", *Applied Energy*, 195, 234–246, 2017.

[27] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", **2016 2nd International Conference on Open and Big Data (OBD)**, 25–30, 2016.

[28] Y. Cai, D. Zhu, "Fraud detections for online businesses: A perspective from blockchain technology", *Finance Innovation*, 2(1), 20, 2016.

[29] Internet: V. Buterin, On Public and Private Blockchains, Ethereum Blog Crypto renaissance salon, 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, 20.10.2018.

[30] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, G. Das, "Everything You Wanted to Know about the Blockchain: Its Promise, Components, Processes, and Problems", *IEEE Consumer Electronics Magazine*, 7(4), 6–14, 2018.

[31] M. E. Peck, "Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem", *IEEE Spectrum*, 24(10), 38–60, 2017.

[32] F. A. Abadi, J. Ellul, G. Azzopardi, "The Blockchain of Things, Beyond Bitcoin : A Systematic Review The Blockchain of Things, Beyond Bitcoin : A Systematic Review", 2018.

[33] D. Lee Kuo Chuen, **Handbook of digital currency : bitcoin, innovation, financial instruments, and big data**, Elsevier, 2015.

[34] Internet: Crypto-Investing - A Simple Guide for Beginners - CryptoDigest, https://cryptodigestne ws.com/crypto-investing-a-simple-guide-for-beginners-5608154c33dc, 07.12.2018.

[35] L. Lamport, R. Shostak, M. Pease, "The Byzantine Generals Problem", *ACM Transaction on Programing Language and Systems*, 4(3), 382–401, 1982.

[36] Internet: S. King, Primecoin: Cryptocurrency with prime number proof-of-work, http://primecoin.io/bin/ primecoin-paper.pdf, 28.10.2018.

[37] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2" *Self-published*, 2014.

[38] Internet: Ppcoin: Peer-to-peer crypto-currency with proof- of-stake, https://www.researchgate. net/publication/265116876_PPCoin_Peer-to-Peer_Crypto-Currency_with_Proof-of-Stake, 16.10.2018.

[39] D. G. Wood, "Ethereum: a Secure Decentralised Generalised Transaction Ledger", 2014.

[40] Internet: V. Zamfir, Introducing Casper 'the Friendly Ghost 2015, https://blog.ethereum.org/ 2015/08/01/introducing-casper-friendly-ghost/, 16.10.2018.

[41] Internet: N.N., Hyperledger Project, Linux Foundation, 2016. https://www.hyperledger.org/, 16.10.2018.

[42] J. Kim, "Stellar Consensus Protocol", 1–15.

[43] Internet: BitShares 2.0 - Industrial-grade decentralized (DPoS) eco-system on blockchain, https://bitshares.org/, 16.10.2018.

[44] Internet: Ripple, https://ripple.com, 16.10.2018.

[45] C. Decker, J. Seidel, R. Wattenhofer, "Bitcoin Meets Strong Consistency", 2014.

[46] D. Kraft, "Difficulty control for blockchain-based consensus systems", *Peer-to-Peer Network and Application*, 9(2), 397–413, 2016.

[47] A. Chepurnoy, M. Larangeira, A. Ojiganov, "A Prunable Blockchain Consensus Protocol Based on Non-Interactive Proofs of Past States Retrievability", 2016.

[48] B. K. Mohanta, S. S. Panda, D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology", **2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)**, 1-4, 2018.

[49] A. Bahga, V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things", 2016.

[50] Internet: Solidity - Solidity 0.5.1 documentation, https://solidity.readthedocs. io/en/develop/, 26.10.2018.

[51] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, "Making Smart Contracts Smarter", **Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16**, 254–269, 2016.

[52] C. K. Frantz, M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts", **Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems**, 210–215, 2016.

[53] M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication", Springer, Cham, 2016, 112–125, 2016.

[54] Internet: VISA Fact Sheet, https://usa.visa.com/dam/VCOM/download/corporate/media/visa net-technology/aboutvisafactsheet. pdff, 26.10.2018.

[55] Internet: The Mini-Blockchain Scheme - J.D. Bruce - BitPaper, http://bitpaper.info/paper/ 5659313586569216, 28.10.2018.

[56] M. Csail, M. F. Kaashoek, N. Zeldovich, "VerSum: Verifiable Computations over Large Public Logs Jelle van den Hooff", 2014.

[57] I. Eyal, A. E. Gencer, E. G. Sirer, R. Van Renesse, "Bitcoin-NG: a scalable blockchain protocol", **Proc. 13th Usenix Conference Networked System Desesign and Implementation**, 45–59, 2016.

[58] S. Meiklejohn ve diğerleri, "A fistful of bitcoins", **Proceedings of the 2013 conference on Internet measurement conference - IMC '13**, 127–140, 2013.

[59] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, E. W. Felten, "Mixcoin: Anonymity for Bitcoin with Accountable Mixes", Springer, Berlin, Heidelberg, 486–504, 2014.

[60] Internet: CoinJoin: Combining Bitcoin Transactions to Obfuscate Trails Bitcoin Magazine, https://bitcoinmagazine.com/articles/ coinjoin-combining-bitcoin-transactions-to-obfuscate-trails-and-increase-privacy-1465235087/, 28.10.2018.

[61] T. Ruffing, P. Moreno-Sanchez, A. Kate, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin", Springer, Cham, 345–364, 2014.

[62] I. Miers, C. Garman, M. Green, A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin", **2013 IEEE Symposium on Security and Privacy**, 397–411, 2013.

[63] E. Ben Sasson ve diğerleri, "Zerocash: Decentralized Anonymous Payments from Bitcoin", **2014 IEEE Symposium on Security and Privacy**, 459–474, 2014.

[64] I. Eyal, E. G. Sirer, "Majority is not enough", *Communications of the ACM*, 6(7), 95–102, 2018.

[65] E. Heilman, "One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner (Poster Abstract)", 161–162, 2014.

[66] S. Solat, M. Potop-Butucaru, "ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin", 2016.

[67] G. Hileman, M. Rauchs, "Global Blockchain Benchmarking Study", 2017.

[68] H. Wang, K. Chen, D. Xu, "A maturity model for blockchain adoption", *Finance Innovation*, 2(1), 12, 2016.

[69] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, "Where Is Current Research on Blockchain Technology? A Systematic Review", *PLoS One*, 11(10), 2016.

[70] Internet: Bitcoin.com Notary, https://notary.bitcoin.com/, 03.12.2018.

[71] Internet: A Document Blockchain Stamping Notary App | stampd.io, https://stampd.io/, 03.12.2018.

[72] Internet: European Insurance Firms Launch New Blockchain Consortium - CoinDesk, https://www.coindesk.com/europe-insurance-blockchain-consortium, 03.12.2018.

[73] R. M. Nor, H. Rahman, T. Rahman, A. Abdullah, "Blockchain Sadaqa Mechanism For Disaster Aid Crowd Funding", 2017.

[74] İnternet: Charities Aid Foundation (CAF) | We Make Giving Count, https://www.cafonline.org/, 03.12.2018.

[75] OECD, "Blockchain and its Use in the Public Sector", 2018.

[76] Internet: BenBen - Digital Land Transaction Services in Ghana, http://www.benben.com.gh/, 03.12.2018.

[77] Internet: e-Estonia - We have built a digital society and so can you, https://e-estonia.com/, 03.12.2018.

[78] Internet: Project Ubin, http://www.mas.gov.sg/ Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx, 03.12.2018.

[79] Internet: West Virginians abroad in 29 countries have voted by mobile device, in the biggest blockchain-based voting test ever - The Washington Post, https://www.washingtonpost .com/technology/2018/11/06/west-virginians-countries-have-voted-by-mobile-device-biggest-blockchain-based-voting-test-ever/?noredirect=on&utm_term=.01948326432f, 03.12.2018.

[80] Internet: Blockchain technology could add transparency to buying and selling a car, https://www.nets.eu/perspectives/Pages/Blockchain-technology-could-add-transparency-to-buying-and-selling-a-car.aspx, 03.12.2018.

[81] 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.

[82] L. A. Linn, M. B. Koo, "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research", 2018.

[83] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control", *Journal of Medical Systems*, 40(10), 218, 2016.

[84] D. Blough, G. Tech, "MedVault: Ensuring Security and Privacy for Electronic Medical Records (Secure Patient-Centric Health Information Sharing)", 2013.

[85] Internet: BitHealth | Devpost, https://devpost.com/ software/bithealth, 03.12.2018.

[86] Feng 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.

[87] Q. Lu, X. Xu, "Adaptable Blockchain-Based Systems: A Case Study for Product Traceability", *IEEE Software*, 34(6), 21–27, 2017.

[88] M. Sharples ve diğerleri, "Innovating Pedagogy 2016 Exploring new forms of teaching, learning and assessment, to guide educators and policy makers", 2016.

[89] A. F. Camilleri, "Blockchain in Education", 2017.

[90] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, A. Kamisalic, "EduCTX: A Blockchain-Based Higher Education Credit Platform", *IEEE Access*, 6, 5112–5127, 2018.

[91] E. Karataş, "Moodle Öğrenme Yönetim Sistemi için Ethereum Blok Zinciri Tabanlı Belge Doğrulama Akıllı Sözleşmesinin Geliştirilmesi", *Bilişim Teknolojileri Dergisi*, 11(4), 399–406, 2018.