Avrupa Bilim ve Teknoloji Dergisi
Sayı 13, S. 54-64, Ağustos 2018
© Telif hakkı EJOSAT'a aittir
Derleme Makale

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 13, pp. 54-64, August 2018
Copyright © 2018 EJOSAT
Review Article

Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri

Ersin ÜNSAL[1*], Ömer KOCAOĞLU[2]
[1]Fibabanka Ar-Ge Merkezi, Şişli, İstanbul, ersin.unsal@fibabanka.com.tr
[2]Fibabanka Ar-Ge Merkezi, Şişli, İstanbul

(İlk Geliş Tarihi 15 Mayıs 2018 ve Kabul Tarihi 1 Ağustos 2018)

(DOI: 10.31590/ejosat.423676)

Öz

Bitcoin, merkezi otoriteye ihtiyaç duymayan, dağıtık ve dijital bir para birimi olarak, son yıllarda finans dünyasındaki popüler konuların başında gelmektedir. İlk dönemde Bitcoin'in finansal özelliklerine duyulan ilgi, zaman içerisinde Bitcoin'e hayat veren blok zinciri teknolojisine doğru kaymaya başlamıştır. Hemen her gün yeni bir uygulama alanını duymaya başladığımız blok zinciri teknolojisi alanındaki akademik araştırmalar sınırlı sayıdadır. Ülkemizde de gerek uygulama gerekse akademik anlamda yeterli sayıda çalışma olmadığını söyleyebiliriz. Bu inceleme, blok zinciri teknolojisini sistematik olarak gözden geçirerek, kullanım alanlarını, açık noktalarını ve gelecek beklentilerini tartışmaktadır.

Anahtar Kelimeler: Bitcoin, blok zinciri, dağıtık uzlaşı, kripto para, dijital para

Blockchain Technology: Use Cases, Open Issues and Future Expectations

Abstract

In recent years, as being a distributed and digital currency, and not being in need of a centralized authority, Bitcoin has become the foremost among the most popular subjects of the financial world. The initial interest in Bitcoin's financial features change course into blockchain technology, which essentially vitalizes the Bitcoin. While we have started to hear about the new implementations of blockchain technology almost every day, worldwide academic research is still limited. Unfortunately, implementation efforts and academic studies on blockchain in our country is also scarce. This paper systematically investigates the blockchain technology to discuss its usage areas, open issues, and future expectations.

Keywords: Bitcoin, blokchain, distributed consensus, cyrptocurrency, digital money

1. GİRİŞ (INTRODUCTION)

Önümüzdeki dönemde başta finans dünyası olmak üzere birçok alanda büyük yenilikler ve dönüşümler yaratması beklenen blok zinciri kavramı, 31 Ekim 2008 yılında yayınlanan Bitcoin makalesiyle ortaya çıkmıştır (Nakamoto, 2008). Makalenin yazarı olarak görünen Satoshi Nakamoto, 2009 yılında ilk Bitcoin yazılımını geliştirerek Bitcoin sisteminin kurulmasını sağlamıştır. Nakamoto, 2010 yılı ortalarına kadar Bitcoin ekosisteminin gelişmesini desteklemiş ve ardından projeden desteğini çekerek ortadan kaybolmuştur (Wikipedia, 2018a). Kaybolmuştur çünkü Satoshi Nakamoto gerçek bir isim değildi ve 2018 yılı itibariyle 150 milyar dolar boyutunda bir değer yaratan bu fikrin arkasında kim ve kimlerin olduğu uzun süre merak konusu olmuştur ve olmaya da devam etmektedir (Wikipedia, 2018a)(Blockchain Luxembourg S.A., 2018). New York Times, The Economist ve Wired gibi birçok ünlü haber dergisinde Bitcoin'in bu gizemli öyküsü çeşitli defalar yayınlanmış ve Bitcoin'in arkasındaki kişi veya kişilerin kimler olduğuna dair çeşitli tahminler yapılmıştır. Bu makalenin yazıldığı tarihte bu konuda en önemli iddia, Satoshi Nakamoto'nun gerçekte Craig Steven Right isimli bilişim alanında lisans ve doktora derecelerine sahip eski bir akademisyen olduğu yönündedir (Wikipedia, 2018b).

Gizemli ve efsanevi bir hikâyeyle ortaya çıkan Bitcoin, öncelikle finansal özellikleri ve oluşturduğu ekonomik değer ile ilgi çekmiş ve gerçekten de günümüz itibariye 150 milyar dolar boyutunda bir değer oluşturarak önemli bir başarı sağlamıştır. Bu gelişmelere paralel olarak, Bitcoin'in temel yapıtaşı olan blok zinciri teknolojisi de ilgi çekmeye başlamış ve başta finans sektörü olmak üzere birçok farklı alanda yeni ürün ve hizmetler oluşturmak için kullanılabileceği gözlemlemiştir. Günümüzde, öncelikle merkez bankaları olmak üzere çeşitli devlet kurumları, birçok büyük banka ve teknoloji şirketi blok zinciri teknolojisine yatırım yapmakta ve bu amaçla çeşitli işbirlikleri oluşturmaktadır. Bu gelişmeler ve blok zinciri teknolojisinin kullanım alanları makalenin ilerleyen bölümlerinde detaylı şekilde tartışılacaktır.

Bitcoin ve blok zinciri konusu akademik olarak değerlendirildiğinde ise bu alandaki akademik yayınların oldukça sınırlı olduğu gözlemlenmektedir. Sınırlı sayıdaki akademik yayınların büyük kısmının ise blok zinciri teknolojisinden ziyade, Bitcoin ve benzeri kripto paraların ekonomik olarak incelendiği finans ve ekonomi odaklı yayınlar olduğu gözlemlenmektedir. Farklı uluslararası akademik veri tabanlarında "*Bitcoin"* ve "*blockchain"* anahtar kelimeleriyle yapılan taramalar, yayınların büyük kısmının "*Bitcoin"* anahtar kelimesini içerdiğini, "*blokchain"* anahtar kelimesini içeren yayınların azınlıkta olduğunu göstermektedir (Tablo 1).

Tablo 1. Bitcoin ve Blok Zinciri Alanındaki Akademik Çalışmalar
(Academic Reseach on Bitcoin and Blockchain)

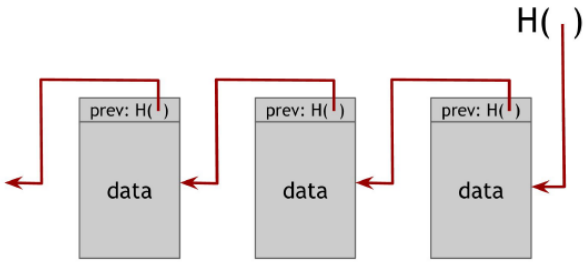
	Anahtar Kelimeye Göre Toplam Yayın/Sonuç Sayısı	
Veritabanı	***Bitcoin***	***Blockchain***
Google Scholar	31.700	23.000
ScienceDirect	691	339
JStor	180	52
SpringerLink	1.386	991

Ülkemizdeki yayınlar incelendiğindeyse bu alanda yapılan akademik çalışmaların oldukça az olduğu gözlemlenmektedir. Mart 2018 itibariyle Türkiye kaynaklarını incelemek amacıyla, YÖK Tez Veritabanı ve Tübitak Ulakbim Veritabanı üzerinde "*Bitcoin*", "*blockchain*" ve "*blok zinciri*" anahtar kelimeleriyle yapılan taramalarda yedi adet yüksek lisans tezi (Kılınç, 2014) (Çay, 2016) (Tüfek, 2017) (Yakupoğlu, 2016) (Göksaran, 2017) (Balçısoy, 2017) (Karaköse, 2017) ile bir adet doktora tezi (Bayram, 2017) ve toplam 9 adet makale olduğu gözlemlenmiştir (Sönmez, 2014) (Ateş, 2014) (Bozdoğanoğlu, 2014) (Yüksel ve Armağan, 2015) (Koçoğlu ve ark. 2016) (Taşdöken, 2016) (Önal, 2016) (Kızıltepe ve Öz, 2016), (Plassaras, 2017). Bu çalışmaların önemli bir kısmı da, dünya yazınındaki yayınlarla paralel bir şekilde, ağırlıklı olarak Bitcoin'in hukuki ve ekonomik durumuna odaklanmaktadır. Her yeni teknolojide olduğu gibi, blok zinciri teknolojisinin sağlıklı şekilde gelişebilmesi ve yaygınlaşabilmesi de ancak akademik alanda yapılacak çalışmalarla desteklenmesiyle mümkündür. Bu nedenle, blok zinciri teknolojisini sistematik olarak inceleyen, araştırma alanlarını, açık konuları ve kullanım alanlarını tartışan akademik çalışmalara ihtiyaç duyulduğu gözlemlenmektedir.

2. BLOK ZİNCİRİ TEKNOLOJİSİ ve KRİPTO PARA KAVRAMI (BLOCKCHAIN TECHNOLOGY AND CRYPTOCURRENCY

2.1. Blok Zinciri Veri Yapısı (Blockchain Data Structure)

Blok zinciri, en basit tanımıyla, bir bağlı liste (linked list) yapısının özelleşmiş halidir. Standart tek bağlı liste yapısında, listenin her elemanı, kendinden sonra gelen elemanı bir işaretçi yordamıyla işaret eder. Bu şekilde listenin başlangıç elemanından kuyruk elemanına kadar bütün elemanlar birbirlerine bağlanmış şekildedirler (Cormen ve ark. 2009). Blok zinciri yapısında ise her eleman (blok), sadece sonraki bloğu işaret etmez, aynı zamanda o bloğun özet (hash) değerini de saklar. Diğer bir ifadeyle blok zinciri, özet-işaretçilerle oluşturulmuş özel bir bağlı liste yapısıdır (Şekil 1) (Narayanan ve ark., 2016).



Şekil 1. Blok Zinciri Veri Yapısı
(Blockchain Data Structure)

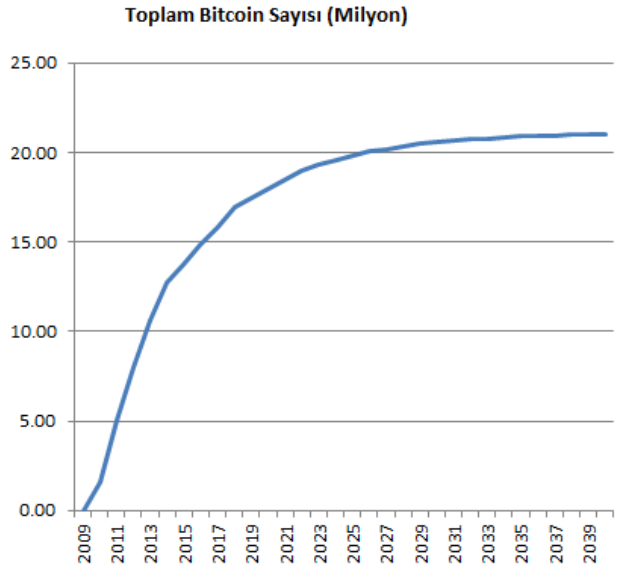
Blok zincirinin, klasik bağlı listeye göre özet-işaretçi yapısıyla elde ettiği en önemli farklılığı, listedeki herhangi bir bloğun değiştirilmek istenmesi durumunda ortaya çıkar. Özet-işaretçi yapısı, bu tür bir değişikliğe izin vermez, daha doğrusu bu tür bir değişiklik yapıldığı kolaylıkla anlaşılır. Çünkü yeni eklenen bloğun özet değeri, bu yeni bloğu işaret eden özet-işaretçisinin işaret ettiği değerden farklı olacaktır. Bu özellik blok zincirinin güvenli bir yapı olmasını sağlayan önemli etmenlerin başında gelmektedir. Bitcoin ile yapılan finansal işlemler, açık muhasebe defteri ismi verilen ve blok zinciri mantığıyla inşa edilen bir yapıda saklanmaktadır.

2.2. Dağıtık Uzlaşı ve Teşvik Sistemi (Distributed Consensus and Incentive Scheme)

Merkezi olmayan, eşten eşe çalışan (peer to peer) ve Bitcoin'de olduğu gibi finansal hareketleri yöneten bir sistemin güvenliğini sağlamak ve kötü amaçlı eşlerden koruyabilmek oldukça önemlidir. Bitcoin'de eşler arasında yapılan finansal işlemler, yine eşler tarafından tüm sisteme yayımlanır. Bu bilgiler daha sonra açık muhasebe defterine kaydedilir. Bu şekilde, tüm finansal hareketler açık muhasebe defterine kaydedilmiş ve merkezi bir otorite olmaksızın finansal bir işleyiş kurulmuş olur. Burada en önemli nokta, açık muhasebe defterine kaydedilen işlemlerin doğru işlemler olması, kötü niyetli eşler tarafından üretilen sahte veya hatalı işlemler olmamasıdır. Aksi halde, sistem finansal hırsızlık olaylarına açık hale gelir. Blok zinciri dünyasında bu güvenlik mekanizmasının adı dağıtık uzlaşı sistemidir. Dağıtık uzlaşı sisteminde, her seferinde rasgele

bir eş, kendisinde bulunan güncel işlemleri tüm eşlere yayımlar. Diğer tüm eşler, kendilerine gelen işlemleri değerlendirir ve doğru ise kabul ederek kendilerinin üreteceği yeni işlem bloklarına eklerler.

Bitcoin, blok zincirine doğru işlemleri yayan eşleri blok ödülü ve işlem ücretleri ile ödüllendirir. Bu finansal teşvik yardımıyla dağıtık uzlaşı sisteminin, doğru işlemleri paylaşan güvenilir eşleri destekleyerek daha güvenli hale gelmesi hedeflenmiştir. İşlem ücretleri opsiyoneldir ancak blok ödülleri belli periyotlarla yarılanarak devam etmektedir. Şubat 2018 itibariyle blok ödülü 12.5 Bitcoin'dir. Blok ödülü belirli periyotlarla (her 210.000 blokta bir – yaklaşık 4 yıllık süre) yarılanarak ve azalarak devam etmektedir. 2016 başında 25 Bitcoin olan blok ödülü, Ağustos 2016 itibariyle 12.5 Bitcoin'e düşmüştür. Diğer bir taraftan da teşvik mekanizması, sisteme yeni bir Bitcoin eklemenin tek yoludur. Teşvik mekanizması algoritmasına göre, sistemde toplam 21 Milyon Bitcoin olabilecektir. Belirli bir süre sonra blok ödülü teşviki geçersiz hale gelecektir. Böyle bir durumda, şu an opsiyonel olan ve genelde sıfır olarak belirlenen işlem ücretleri teşvikinin, blok ücretleri teşvikini ikame edecek şekilde kullanılacağı değerlendirilmektedir (Şekil 2) (Narayanan ve ark., 2016).



Şekil 2. Dolaşımdaki Toplam Bitcoin Sayısı
(Total Bitcoins in Circulation)

2.3. Dijital İmzalar, Güvenlik ve Gizlilik (Digital Signatures, Security and Privacy)

Dijital imza, gerçek hayattaki imzalarla sağlanan güvenliğin dijital ortamda da sağlanabilmesi için yapılandırılmış bir güvenlik aracıdır. Gerçek imzada olduğu gibi, bir kişiye ait olan dijital imza sadece o kişi tarafından kullanılabilir, başka birisi tarafından kullanılamaz. Yine gerçek hayatta olduğu gibi, bir dijital dokümana iliştirilmiş dijital imza, o dijital dokümanın imza sahibi tarafından onaylandığının göstergesidir.

Bitcoin dünyasında yapılan en temel finansal işlem, bir kişinin diğeriyle para değiş tokuşu yapmasıdır. Gerçek dünyada yapılan işlemde güvenlik önlemleri, fiziksel paranın güvenli şekilde imal edilmesine ve kolay şekilde taklit edilememesine odaklanmıştır. Dijital para dünyasında ise güvenlik, işlemlerin dijital imzalarla doğrulanmasıyla mümkün olmaktadır. Yani A kişisi B kişisine para transferi yaparken, işlemi kendi dijital imzasıyla imzalayarak güvenli hale getirir.

Dijital imzalama işlemi, yapılan işlemlerin güvenliğini sağlarken; ayrıca işlem sahiplerinin de gizliliğini sağlamaktadır. Çünkü Bitcoin dünyasında, gerçek kişiler sadece kendilerinin bildiği ve doğrulayabildiği dijital imzalarla işlem yapabilirler. Ayrıca her gerçek kişi birden fazla dijital imza yaratabilir ve bu dijital imzaları kullanarak kendisine ait finansal işlemlerini istediği şekilde yönetebilir. Bitcoin ile yapılan tüm işlemler açık muhasebe defterine kaydedilir ve adından da anlaşılacağı üzere bu deftere isteyen herkes erişebilir. Ancak işlemlerde gerçek kişi bilgileri veya bundan türetilen bir bilgi yerine, dijital imzalar yer aldığı için finansal hareketlerin gerçekte kimler tarafından yapıldığı bilinmez.

2.4. Bitcoin Madenciliği (Bitcoin Mining)

Dağıtık uzlaşı sisteminde teşvik mekanizması, blok zincirine yeni bir blok ekleyebilen bir eşin ödüllendirilmesi şeklindedir. Teşviği hangi eşin alabileceği konusu ise oldukça önemli bir problemdir. Bitcoin dünyasında, yeni Bitcoin'ler sadece teşvik sistemiyle üretilerek sisteme dâhil edilebilmektedir. Dolayısıyla teşvik edilecek eşlerin seçimi, rastlantısal şekilde olabilmeli ve sistemde hiçbir eş ya da eş grubu tekel olarak davranamamalıdır. Bitcoin, bu problemin çözümünü emek ispatı (proof of work - PoW) adı verdiğimiz bir mekanizmayla sağlamaktadır. Eşlerin, sisteme yeni blok ekleyebilmeleri, çözümü için yüksek işlemci gücüne ihtiyaç duyacak karmaşık bir özet-bulmacanın çözülmesiyle mümkün olmaktadır.

Yüksek işlemci gücüne dayalı bir problemin çözümü, teşvik kazanmak isteyen kimselerin güçlü özelliklerdeki çok sayıda bilgisayarı Bitcoin sistemine dâhil etmelerini sağlamıştır. Ancak sürekli yeni eşlerin katılarak, sistemi büyüttüğü bir dağıtık sistemde, belirli eş veya eşlerin tekel olabilmeleri çok kolay olmamaktadır. Diğer taraftan donanım ve elektrik giderleri, teşvik sistemi tarafından sunulan teşvik getirilerinden az olduğu için Bitcoin madenciliği adını verdiğimiz bir yöntem oluşmuştur. Kimi zaman fabrika büyüklüğündeki binaların içine kurdukları bilgisayar ağlarıyla Bitcoin sistemine dâhil olan kişi ya da kişiler, teşvik sisteminden faydalanarak önemli kazançlar sağlamaktadırlar. Sisteme katılan eşlerin sayısının artması da Bitcoin sisteminin güvenilirliğini artıran önemli bir faktör olmaktadır (Price, 2015).

Emek ispatı hali hazırda en popüler blok zinciri platformlarında kullanılan blok üretim ve doğrulama mekanizması olmakla birlikte, yüksek enerji tüketimine neden olmakta ve özel donanım gereksinimleri ortaya çıkarabilmektedir. Bu durum ise çeşitli eleştirilere neden olmakta ve alternatif çözümler önerilmektedir. Alternatif bir yöntem olarak öne çıkan hisse ispatı (proof of stake – PoS), bloğu üreten eşin ilgili blok zinciri ağı üzerinde sahip olduğu pay ile orantılı olarak geçerlilik onay yetkisi vermektedir. Bu yöntemde, yüksek pay sahibi eşlere sürekli bir avantaj sağlanmasının önüne geçmek için akış içerisindeki hesaplamalarda kullanılmak üzere yaş (age) kavramı da geliştirilmiştir. Bu sayede, herhangi bir blok üretimi için kullanılan pay kapsamındaki kripto paraların yaş değerleri sıfırlanır ve ancak belirli bir süre sonra tekrar yaş değeri kazanmaya başlarlar. Diğer bir popüler blok zinciri platformu olan Ethereum, emek ispatı yerine hisse ispatı yöntemine geçmeyi planlamaktadır. Bu sayede blok üretimi ve doğrulanma

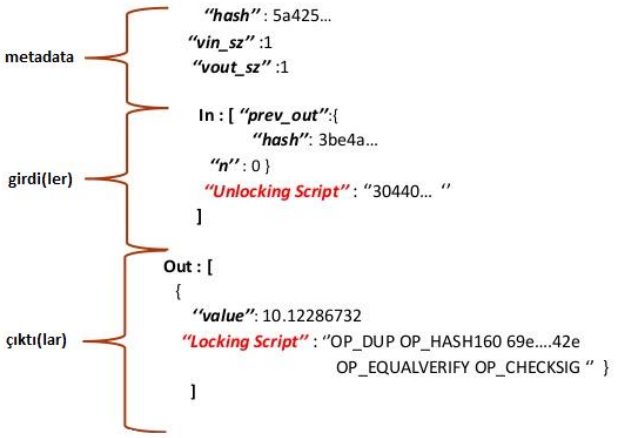
süreçlerinin hızlanması ve enerji ihtiyacının azalması hedeflenmektedir (Usta ve Doğantekin, 2017).

2.5. Bitcoin İşlemleri (Bitcoin Transactions)

Bitcoin'de yapılan finansal işlemlerde, temel olarak girdiler ve çıktılar vardır. Bu durum alışık olduğumuz hesap yönetiminden biraz daha farklıdır. Örneğin banka hesabınızda bir bakiyeniz vardır; hesabınıza gelen paralar bakiyenizi arttırırken, hesaptan çıkan paralar da bakiyenizi azaltır. Bir para harcaması yapacağınız zaman, eğer harcamak istediğiniz tutar bakiyenizden büyükse işlemi yapamazsınız. Diğer bir ifadeyle sürekli olarak bakiyenin kontrol edilmesi ve doğruluğunun sağlanması ihtiyacı vardır.

Bitcoin işlemleri ise bir bakiye yönetimi gibi çalışmaz, her işlem kendi içinde girdi ve çıktılarını belirtir. Örneğin A kişisi, B kişisine 5 Bitcoin transfer etmek istediğinde, transfer etmek istediği 5 Bitcoin'in kendisine hangi finansal işlemler sonucu transfer edildiğini yeni işleme girdi olarak sunar.

Şekil 3.'de görülebileceği gibi, Bitcoin işlemlerinde metadata, girdi ve çıktı olarak isimlendirilen 3 bölüm vardır. Metadata bölümünde, işlemin tekil numarası, girdi sayısı ve çıktı sayısı gibi işleme ait temel veriler yer almaktadır. Girdi bölümünde, güncel işlemde kullanılmak istenen ve önceki işlemlerle elde edilen Bitcoin'leri işaret eden işaretçi ve indeksler yer almaktadır. Çıktı bölümünde ise, girdide işaret edilen Bitcoin'lerin işlem sonunda hangi dijital adreslere transfer edileceği belirtilmektedir. İşlem yapısında yer alan betik (script) alanları ise, Bitcoin Betik diliyle yazılmış betikleri ifade eder. Bitcoin betikleri, başta akıllı kontratlar olmak üzere farklı uygulamaların geliştirilmesine de imkân sağlamaktadır (Narayanan ve ark., 2016).



Şekil 3. Bitcoin İşlem Yapısı
(Bitcoin Transaction Structure)

2.6. Bitcoin Cüzdanları (Bitcoin Wallets)

Blok zinciri üzerinde Bitcoin'leri transfer edebilmek, kişilerin kendilerine ait dijital imzaları yardımıyla mümkün olmaktadır. Dolayısıyla Bitcoin'lere erişebilmek ve kullanabilmek için, Bitcoin sahiplerinin dijital imzaları oluştururken kullandıkları anahtarları yönetmesi gerekmektedir. Anahtar yönetimiyse bilişim güvenliği alanında başlı başına önemli bir konudur. Zira anahtarların başkaları tarafından ele geçirilmesi önemli riskler içerir. Bitcoin dünyasında, anahtarlarının başkaları tarafından ele geçirilmesi finansal kayıplarla sonuçlanabilecek bir durumdur. Bitcoin özelinde, anahtar yönetimiyle ilgili diğer bir konu da bir kişinin istediği kadar farklı anahtarlar yaratarak, istediği kadar fazla dijital kimlik ile Bitcoin alışverişi yapabilmesidir. Birden fazla dijital kimliğin, diğer bir ifadeyle anahtarların, yönetiminin de etkin şekilde yapılabilmesi Bitcoin cüzdanları adı verilen yazılımlarla mümkün olabilmektedir.

Bitcoin cüzdanları, basit arayüzler sunarak, dijital anahtarlarınızı ve bu sayede Bitcoin'lerinizi yönetmenizi sağlayan yazılımlardır. İnternette ücretsiz olarak birçok Bitcoin cüzdanı yazılımına erişilebilir. Bu alanda yenilikçi bir çözüm de sadece Bitcoin'leri değil, paralelinde birçok farklı kripto parayı yönetmeyi sağlayan özelliği ile öne çıkan Exodus (http://www.exodus.io) isimli cüzdandır. Bunun yanısıra Electrum (https://electrum.org), Jaxx (https://jaxx.io/) ve Mycelium (https://wallet.mycelium.com/) gibi cüzdanlar da popüler cüzdan yazılımlarıdır.

Bitcoin cüzdanları, her ne kadar Bitcoin'leri yönetebilmek için kolay bir arayüz sunsalar da, cüzdanların üzerinde koştuğu mobil cihazlar veya bilgisayarlardaki herhangi bir güvenlik açığı veya sürekli çevrimiçi erişilebilir olan Bitcoin cüzdanı yazılımının kendisinden kaynaklı bir güvenlik zafiyeti, özellikle büyük meblağlarda Bitcoin içeren dijital kimliklerin çaldırılmasına neden olabilir. Bu nedenle sıcak ve soğuk cüzdan kavramları geliştirilmiştir. Sıcak cüzdanlar günlük hayatta ihtiyaç duyulabilecek miktarda Bitcoin'i üzerinde taşımayı hedefleyen ve sürekli çevrimiçi olarak mobil cihazlar ve bilgisayarlar üzerinde çalışan cüzdanları ifade eder. Soğuk cüzdanlar ise daha güvenli olması amacıyla, sürekli çevrimiçi olmayan ve sadece gerektiğinde sıcak cüzdanlarla para transferi yapmak için çevrimiçi olan cüzdanları tarif eder. Trezor (https://trezor.io/) ve Ledger (https://www.ledgerwallet.com/) günümüzde yaygın olarak donanım tabanlı soğuk cüzdanlardır. Soğuk ve sıcak cüzdanlar arasındaki para transferinin yönetimini kolaylaştırmak amacıyla ayrıca hiyerarşik cüzdan yapıları geliştirilmiştir (Narayanan ve ark., 2016).

2.7. Açık, Özel ve Hibrid Blok Zincirleri (Public, Private and Hybrid Blockchain)

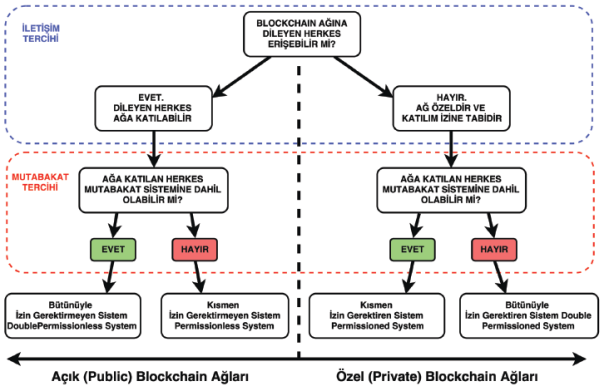
Blok zinciri teknolojisi, herkesin erişebileceği açık yapısı ve dağıtık uzlaşı özelliği ile öne çıkmış olsa da ilerleyen zamanda farklı ihtiyaçları karşılayabilmek amacıyla kısmi-merkezi (partially-decentralized) ve özel (private) blok zinciri yapıları geliştirilmiştir.

Kısmi-merkezi bok zinciri yapılarında, diğer bir adıyla konsorsiyum blok zincirleri, dağıtık uzlaşı yöntemi yerine sadece önceden belirlenmiş sınırlı sayıda eşin, uzlaşı sistemini yönettiği yapılardır. Bu tür yapılarda blok zinciri verisi herkese açık olabileceği gibi verilerin erişilebilirliğinin de çeşitli şekillerde kısıtlandığı karma blok zinciri yapıları oluşturulabilir.

Özel blok zincirlerinde ise, blok zincirine yazma (yeni bir işlem ekleme) yetkisi sadece özel bir gruba/organizasyona aittir. Verileri okuma hakkı ise herkese açık olabileceği gibi çeşitli şekillerde kısıtlanabilir.

Blok zinciri yapılarını sınıflandırmak amacıyla kullanılan yöntemlerden birisi de iletişim tercihine ve mutabakat tercihine

göre sınıflandırma yapmaktır. Açık blok zincirlerinde dileyen herkes ağa katılabileceği gibi aynı zamanda mutabakat sistemine de dâhil olabilmektedir (Şekil 4) (Usta ve Doğantekin, 2017).



Şekil 4. Açık ve Özel Blok Zinciri Yapıları
(Public and Private Blockchains)

2.9 Blok Zinciri Platformları (Blockchain Platforms)

Blok zinciri, Bitcoin ile popüler olmuş ve yaygınlaşmış bir teknoloji olmakla birlikte, günümüzdeki blok zinciri projeleri geliştirmek için kullanılabilecek farklı blok zinciri platformları ortaya çıkmıştır. Bu platformlar, açık kaynaklı olup olmamaları, fiyatlandırma yapısı, destekledikleri programları dilleri ve destekleri blok zinciri yapılarına (açık, hibrid, özel) göre farklılaşmaktadır. Ethereum ve Hyperledger, bu alanda en yaygın kullanılan, en bilindik alternatiflerdir. Bunların yanısıra Ripple, Tendermint ve Corda gibi farklı blokchain platformları da vardır (Usta ve Doğantekin, 2017). Ayrıca yakın zamanda Microsoft Azure üzerinde blok zinciri platformunu bir servis olarak (Blockchain as a service) sunmaya başlamıştır. Öncelikli olarak IBM ve ardından da Microsoft, blok zinciri teknolojisine önemli oranda yatırım yapan teknoloji devleridir.

Blok zinciri teknolojisinin farklılaşabildiği ilginç noktalardan birisi de değiştirilememe özelliğiyle ilgilidir. Blok zinciri teknolojisinin özet-işaretçi yapılarıyla elde ettiği değiştirilememe özelliği, pratik hayatta çeşitli nedenlerle hatalı olarak eklenen blok zinciri verilerinin silinmesine izin vermemektedir. Danışmanlık firması Accenture, blok zincirinin değiştirilebilir olmasının gerçek dünyanın ihtiyaçlarına daha uygun olabileceğinden hareketle değiştirilebilir blok zinciri yapısını tarifleyen bir patent başvurusunda bulunmuştur (Accenture, 2016).

3. BLOK ZİNCİRİ TEKNOLOJİSİNİN KULLANIM ALANLARI (USES CASES FOR BLOCKCHAIN TECHNOLOGY)

Blok zinciri teknolojisinin en önemli kullanım alanı, kripto para kavramı ve Bitcoin olmuştur. Günümüzde Bitcoin dışında, binden fazla kripto para çeşidi olduğu bilinmektedir (Wikipedia, 2018c). Kripto paraların toplam piyasa değeri 380 milyar dolar civarındadır ve 150 milyar dolara yaklaşan piyasa değeri ile Bitcoin bu değerin çok önemli bir kısmını oluşturmaktadır (CoinMarketCap, 2018).

Kripto paralar dışında blok zinciri teknolojisinin özellikle güven sorunu yaşanan ve bu sorunu aşmak için aracı kişi ve kurumların (intermediaries) yer aldığı birçok iş alanında kullanılabileceği öngörülmektedir. Blok zinciri teknolojisini kullanan birçok kavram kanıtlama ve prototip ürün çalışmaları yapılmasına rağmen gerçek hayatta kullanılan uygulamalar henüz hayata geçmemiştir. Dolayısıyla blok zinciri teknoloji kullanan iş fikirleri oldukça ilgi çekmesine rağmen, bu fikirlerin hayata geçmesi için yatırım bütçelerine ve zamana ihtiyaç vardır. ICO (Initial Coin Offering), blok zinciri temelli yeni iş fikilerinin fon bulmak için kullanmaya başladığı oldukça yenilikçi bir fon toplama mekanizmasıdır (CoinMarketCap, 2018). 2013 yılında kullanılmaya başlayan bu yöntemin ilk başarılı örneklerinden birisi, döneminin en büyük ICO'su olarak yaklaşık 18 milyon USD fon toplayan Ethereum projesidir.

Günümüzde blok zinciri projelerin en önemli fonlama aracı haline gelen ICO'lar, yasal statüleri hakkındaki çeşitli tartışmalara rağmen, çok ciddi miktarlarda fon toplayabilmektedirler. 2017 yılında 211 adet ICO yapılmış ve yaklaşık olarak 4 milyar USD fon toplanmıştır. 2018 yılının sadece ilk 2 ayında yapılan ICO'lar ise 1 milyar USD boyutunda fon toplamayı başarmıştır (Özgün Law, 2017).

Henüz neredeyse bir fikir aşamasındayken fon toplama sürecine başlayan ICO'ların bu boyutlarda fon toplayabilmesi oldukça önemli bir başarıdır. ICO'ların başarısı, iş fikriyle ilintili olduğu kadar, proje ve danışman ekibinin niteliği ve tecrübesinden, girişimin şeffaflığına kadar birçok farklı parametreden etkilenebilmektedir (CoinSchedule Limited, 2018), (Mougayar, 2016).

Tablo 2. 2017 Yılı En Büyük ICO'lar
(Top Ten ICOs of 2017)

Sıralama	Proje Adı	Toplanan Tutarı
1.	Hdac	258.000.000 $
2.	Filecoin	257.000.000 $
3.	EOS Stage 1	185.000.000 $
4.	Paragon	183.157.275 $
5.	Bancor	153.000.000 $
6.	Status	90.000.000 $
7.	Bankex	70.600.000 $
8.	Tenx	64.000.000 $
9.	Nebulas	60.000.000 $
10.	MobileGO	53.069.235 $

3.1. Finans Endüstrisi (Finance Industry)

Birçok banka ve finansal kurum, blok zinciri teknolojisinin kripto para dışındaki olası kullanım alanlarını araştırmakta ve yenilikçi çözümlere yatırım yapmaktadır. Bu araştırmalar sonucunda çeşitli kaynaklarda yayınlanan olası bazı finansal kullanım alanları şunlardır (Deloitte, 2015), (Cognizant, 2016), (Everis Next, 2016), (Evans, 2015):

- Ödeme İşlemleri
- Para Transferleri
- Alış/Satış Platformları
- Takas Yönetimi
- Yetkilendirme, Doğrulama
- Dijital Kimlik Yönetimi

- Doküman Yönetimi
- İslami Bankacılık Uygulamaları

Bankacılık alanında örnek uygulamaların öncelikle uluslararası para transferi ve yine uluslararası ticaretin finansmanı alanında öne çıktığı gözlemlenmektedir. Ülkemizde bir bankanın da dahil olduğu Ripple, uluslararası para transferi alanında öne çıkan bir blok zinciri çözümüdür. Uluslararası ticaretin finansmanı konusunda ise çeşitli bankaların bir araya gelip konsorsiyumlar oluşturduğu duyurulmaktadır.

3.2. Kamu Sektörü (Public Sector)

Blok zinciri teknolojisinin kamusal anlamda da yenilikçi kullanım alanları vardır ve öncül uygulamalar ortaya çıkmaya başlamıştır. Blok zinciri teknolojisinin kamu sektöründe kullanılabileceği bazı alanlar şunlardır (Cognizant, 2016):

- Oylama
- Doküman Yönetimi
- Enerji Dağıtımı
- Akıllı Kontratlar
- Dijital Kimlik
- Dijital Pasaport
- Sosyal Güvenlik Sistemi
- Vergi Sistemi

Çeşitli ülkelerde, kamusal alanda blok zinciri yatırımlarının yapılmaya başlandığı bilinmektedir. Dubai, İsviçre, İngiltere, Estonya, Singapur ve Kıbrıs blok zinciri alanındaki inovasyona öncülük eden ülkelerdendir.

Blok zinciri teknolojisi temelli yenilikçi ürünlere ilgi gösteren diğer bir kamusal alan da savunma alanıdır. Yakın zamanda gerek NATO'nun gerekse Amerikan Savunma Bakanlığının blok zinciri teknolojisiyle ilgilenmeye başladığı bilinmektedir. Amerikan Savunma Bakanlığı daha çok blok zinciri tabanlı güvenli bir mesajlaşma uygulamasına odaklanırken, NATO lojistik ve tedarik gibi daha geleneksel uygulamaların altyapısında blok zinciri teknolojisini kullanmayı hedeflemektedir (Kar, 2016).

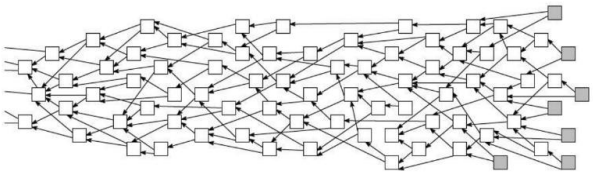
3.3. Akıllı Kontratlar (Smart Contracts)

Blok zinciri teknolojisinin, sektörlerden bağımsız olarak ya da diğer bir ifadeyle birçok farklı sektörü etkileyebilecek en önemli kullanım alanlarından birisi akıllı kontratlardır. Blok zinciri teknolojisi, farklı paydaşlar arasında dijital sözleşmelerin blok zinciri üzerinde tanımlanmasını sağlamaktadır. Bitcoin Betik diliyle tanımlanabilen akıllı kontrat yapısı sayesinde, kontrat içeriğinde belirtilen gerekli mantıksal koşulların sağlanması durumunda, amaçlanan işlemin hayata geçmesi sağlanmaktadır. 2014 yılından duyurulan Ethereum ise Blok Zinciri 2.0 olarak adlandırılan alt yapısıyla, akıllı sözleşmeler için en çok tercih edilen blok zinciri çözümü olmuştur. Merkezi bir otoriteye gerek duymaksızın, farklı paydaşlar arasında dijital sözleşmelerin tanımlanabilmesi ve sözleşme koşullarının takip edilerek sonucuna göre hedeflenen aksiyonların otomatik olarak hayata geçirilebilmesi, blok zinciri teknolojisinin en çok heyecan yaratan uygulama alanları arasındadır.

3.4. Nesnelerin İnterneti, Paylaşım Ekonomisi ve Finansal Dönüşüm (Internet of Things, Shared Economy and Financial Transformation)

Blok zinciri teknolojisinin mevcut ürün ve hizmetlerin iyileştirilmesi alanında kullanımı konusunda ar-ge çalışmaları yapılmaya devam etmektedir. Diğer bir taraftan, blok zinciri teknolojisinin etkilerinin mevcut ürün ve hizmetleri iyileştirmenin çok daha ötesinde olacağını savunan ve buna yönelik düşünceler geliştirilen kişi ve kurumlar da vardır. Blok zinciri teknolojisinin sağladığı merkezi otoriteye gerek duymayan dağıtık para kavramını, günümüzde öne çıkmaya başlayan nesnelerin interneti ve paylaşım ekonomisi gibi gelişmelerle birlikte değerlendirerek daha büyük etkiler yaratabileceği ifade edilmektedir (Tapscott ve Tapscott, 2016), (Short, 2016), (Ramsey, 2016), (Huckle ve ark., 2016).

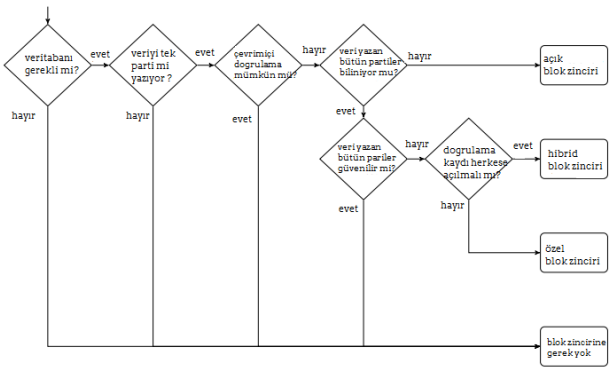
Nesnelerin interneti konusunda en çok öne çıkan çözümlerinden bir tanesi IOTA isimli projedir. IOTA, komisyon ücretleri olmadan, dağıtık ve ölçeklenebilir bir altyapı sunmakta ve nesnelerin açık muhasebe defteri (ledger of things) olarak adlandırmaktadır. IOTA ile ilgili diğer bir özellik, altyapı olarak blok zinciri teknolojisi değil, Tangle isimli bir teknoloji kullanmaktadır. Tangle, madenciler, bloklar ve zincir gibi kavramlar yerine, DAG isimli bir altyapı kullanmaktadır. Bu yapıda, ağın her bileşeninin, yeni bir işlem yapabilmek için daha önce yapılmış iki işlemi onaylaması gerekmektedir (Şekil 5) (Popov, 2017).



Şekil 5. Tangle ve İşlem Akışı
(Tangle and Transaction Flow)

3.5. Blok Zincirine Gerçekten İhtiyaç Var mı? (Internet of Things, Shared Economy and Financial Transformation)

Blok zinciri teknolojisini kullanarak çeşitli iş çözümleri geliştirmeye başlayan yüzlerce girişim olduğu gibi diğer taraftan da çeşitli büyük bankalar ve firmalar tarafından oluşturulmuş konsorsiyumlar da blok zinciri alanında çözümler geliştirmeyi hedeflemektedir. Bu gelişmelere biraz daha mesafeli duran ve blok zinciri teknolojisi etrafında oluşan yüksek beklentilerini sorgulayan ve blok zinciri teknolojisinin net faydalarının görülebileceği projelere odaklanılmasını öneren görüşler de vardır. Bu amaçla bir projede blok zinciri teknolojisini gerçekten kullanmak gerekli mi, gerekliyse hangi tip blok zinciri yapısını kurgulamak gerekli gibi sorulara yanıt verirken kullanmak üzere akış şemaları ortaya çıkmaya başlamıştır (Şekil 6) (Bauerle, 2018), (Wüst ve Gervais, 2017).

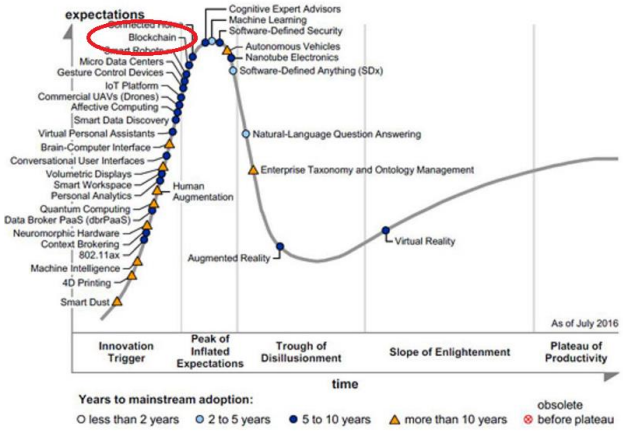


Şekil 6. Açık ve Özel Blok Zinciri Yapıları Ne Zaman Kullanılmalı?
(When To Use Public and Private Blockchains)

4. BLOK ZİNCİRİ TEKNOLOJİSİNİN GELECEĞİ VE AÇIK KONULAR (FUTURE OF BLOCKCHAIN TEHCNOLOGY AND OPEN ISSUES)

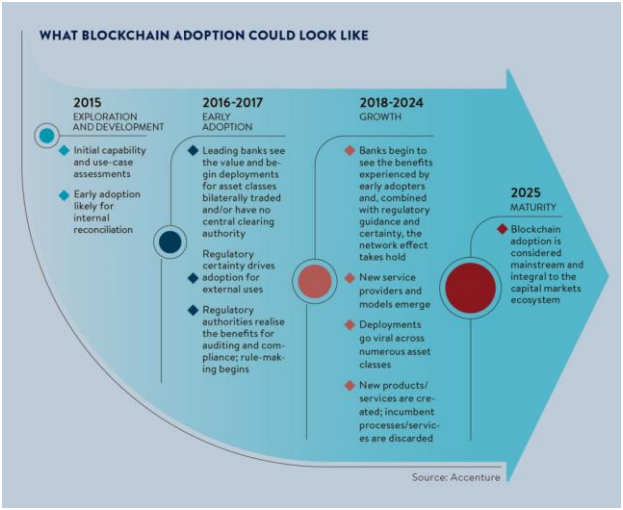
4.1. Blok Zinciri Teknolojisinin Geleceği (Future of Blockchain Technology)

Yeni ve gelişmekte olan teknolojilerin gelişimini takip edebilmek ve gelecek öngörüleri yapabilmek için başvurulan araçların başında önemli danışmanlık firmalarının yayınladığı araştırma raporları gelmektedir. Gartner firması tarafından geliştirilen Hype Cycle metodolojisi, yeni teknolojileri takip etmekte kullanılan en önemli araçlar arasındadır. Blok zinciri teknolojisi, ilk kez 2016 yılında Gartner Hype Cycle çalışmasına dâhil edilmiştir. Gartner'ın bu çalışmasına göre blok zinciri teknolojisi, henüz inovasyonu tetikleyici bölgededir. Gartner'a göre, blok zinciri teknolojisi 5-10 yıllık bir zaman zarfı içinde olgunlaşacak ve yaygın olarak kullanılmaya başlayacaktır (Şekil 7).



Şekil 7. Gartner Hype Cycle 2016
(Gartner Hype Cycle 2016)

Teknoloji alanındaki gelişmeleri yakın takip eden önemli diğer bir danışmanlık firması Accenture'a göre ise blok zinciri teknolojisinin yetenekleri ve potansiyeli 2015 yılında keşfedilmeye başlanmıştır. 2016 yılı ile birlikte lider bankalar, blok zinciri teknolojisine yatırım yapmaya ve teknolojiyi test etmeye başlamışlardır. Accenture firması, 2018-2024 yılları arasında blok zinciri teknolojisinin yaygınlaşacağını ve 2025 yılı itibariyle olgunlaşarak finans sektörü başta olmak üzere birçok sektör için önemli bir teknolojik platform haline geleceğini öngörmektedir (Şekil 8).



Şekil 8. Blok Zinciri Adaptasyonu - Accenture
(Blockchain Adaption - Accenture)

Diğer önemli bir danışmanlık firması Deloitte ise, tahminleme çalışmalarının bir adım ötesine geçerek, Blok Zinciri Laboratuvarı kurmuş ve ihtiyaç duyan firmalara blok zinciri alanında eğitim, strateji, danışmanlık ve çözüm sunmaya başlamıştır (Deloitte, 2018).

Danışmanlık şirketlerinin raporlarının yanı sıra, yeni bir teknolojinin gelişimini destekleyen en önemli konulardan biri de standardizasyon çalışmalarıdır. Blok zinciri teknolojisi için standardizasyon konusunda da önemli gelişmeler yaşanmaya başlamıştır. Teknoloji alanındaki standartlar konusunda öncülük eden iki önemli kuruluşun (IEEE ve ISO) blok zinciri konusunda standartlar geliştirmeye hazırlandıklarına dair çeşitli haberler yayınlanmıştır (Rozenfeld, 2016), (Cohen, 2016).

Gerek danışmanlık şirketlerinin blok zinciri hakkındaki olumlu beklentileri, gerekse IEEE ve ISO gibi kuruluşların blok zinciri teknolojisinin standardizasyonu alanındaki hazırlıkları; blok zinciri teknolojisinin çok yakın bir süre içinde başta finans sektörü olmak üzere birçok farklı sektörde yoğun şekilde kullanılmaya başlanacağının habercisi olarak yorumlanabilir. Bu beklentilerle uyumlu şekilde, Microsoft ve IBM firmaları, blok zinciri teknolojini kullanmak isteyen firmalar için, bulut tabanlı blok zinciri altyapıları geliştirmiş ve firmaların kullanımına açmışlardır. Tüm bu gelişmeler, dünya çapındaki önemli kuruluşların blok zinciri teknolojine önem verdiklerini, yaygınlaşmasını desteklediklerini, bu teknolojinin geleceğine dair olumlu beklentileri olduğunu ve bu yönde önemli yatırımlar yaptıklarını göstermektedir.

4.2. Açık Konular (Open Issues)

4.2.1. Güvenlik (Security)

Her ne kadar blok zinciri teknolojisi bir güvenlik makinası ("Trust Machine") olarak adlandırılsa da özellikle Bitcoin takas merkezlerinde yaşanan önemli hırsızlık olayları toplumun bu teknolojiye duyduğu güveni sarsmaktadır. Amerika Yurt

Güvenlik Bölümü tarafından desteklenen bir çalışma, Bitcoin'in ortaya çıkışından bu yana yapılan tüm takas işlemlerinin önemli bir kısmının hacklendiğini ifade etmektedir ve bu çok yüksek bir orandır. Yine farklı araştırmalarda da benzer şekilde güvenlik zafiyetleri ve hırsızlık olayları raporlanmaktadır (Young, 2016).

Yaşanan bu hırsızlık olaylarının özünde, Bitcoin takas merkezlerinin çoklu-imza (multi-signature) güvenlik teknolojisine gereken hassasiyeti göstermemeleri ve soğuk cüzdanlar yerine sıcak cüzdanlarla entegrasyona ağırlık vermeleri olduğu gözlemlenmektedir. Ortaya çıkışından bu yana Bitcoin dünyasında yaşanan önemli hırsızlık olayları ve miktarları Tablo 2.'de özetlenmiştir (Newbium, 2016). Bunlara ek olarak, özellikle 2017 yılında başta ICO ve Tether odaklı farklı hırsızlık (hack) olayları da ortaya çıkmıştır (Duggan, 2017).

Tablo 3. Büyük Bitcoin Hırsızlıkları
(Biggest Bitcoin Hacks)

Olay Adı	Kurum/Ürün Tipi	Hırsızlık Tutarı	Tarih (Ay/Yıl)
Mt.Gotx	Takas Merkezi	500.000.000 $	01/2014
Bitfinex	Takas Merkezi	70.000.000 $	08/2016
Linode	Web Hosting	27.000.000 $	03/2012
Bitstamp	Takas Merkezi	11.000.000 $	01/2015
Bitstamp	Takas Merkezi	11.000.000 $	01/2016
Bter	Takas Merkezi	4.000.000 $	02/2015
Picostocks	Takas Merkezi	3.500.000 $	11/2013
Inputs.io	Cüzdan	2.400.000 $	11/2013
Mintpal	Takas Merkezi	2.100.000 $	12/2014
Kipcoin	Takas Merkezi	1.700.000 $	02/2015

Blok zinciri dünyasında güvenlik ve mahremiyet açısından önemli bir gelişme Sıfır Bilgi Kanıtı (Zero Proof Knowledge) teknolojisini kullanan kripto para birimlerinin ortaya çıkmasıdır. Sıfır Bilgi Kanıtı algoritması, özetle bildiğiniz bilgiyi bir başkasına, bilgiyi ona vermeden ispat etmek olarak tanımlanabilir. Sıfır Bilgi Kanıtı algoritması, erişilebilir blok zinciri verileri üzerinden işlem ve grafik analizi gibi yöntemlerle çeşitli çıkarımlar yapmanın önüne geçmede ve blok zinciri işlemlerinin mahremiyeti artırmada etkili bir algoritmadır. Zerocash (ZCash), Sıfır Bilgi Kanıtı teknolojisini kullanan öncü kripto para birimleri arasındadır (Sasson ve ark., 2014).

4.2.2. Değişiklik Yönetimi (Change Management)

Bitcoin, dağıtık uzlaşı prensipleri ışığında eşten-eşe çalışan bir teknik mimariye sahiptir. Sistemin güvenli ve dağıtık bir şekilde çalışabilmesi için bütün eşlerde aynı özellik ve algoritmaları çalıştıran açık kaynaklı yazılımlar çalışmalıdır. Çeşitli nedenlerle bu yazılımın özellikleri, parametreleri veya kullandığı algoritmalarda değişiklikler veya geliştirmeler yapılması gerekebilmektedir. Bu durumlarda yapılan değişikliklerin bazen yumuşak (soft-fork) bazen sert (hard-fork) şekilde yapılabilir: Diğer bir ifadeyle yapılan değişiklik daha önce geçerli olan bir bloğu/işlemi geçersiz hale getirebilir (soft-fork) veya daha önce geçersiz olan bir bloğu/işlemi geçerli hale getirebilir (hard-fork).

Dağıtık uzlaşı prensipleriyle çalışan bir sistemde bu tür değişikliklerin yapılması; seçilen yöntem ve tercih edilen zamanlama açısından dağıtık sistemin eşleri arasında anlaşmazlıklara ve krizlere neden olabilmektedir (Wirdum, 2016). Bu krizler sisteme olan güveni azaltabilmekte ve blok zinciri teknolojisine olan desteğin de azalmasına neden olabilmektedir.

4.2.3. Regülasyonlar (Regulations)

Bitcoin ve blok zinciri teknolojisinin gelişimi açısından önemli diğer bir konu ise yasallık ve regülasyonlar konusudur. Her ne kadar blok zinciri üzerindeki tüm işlemler kamuya açık olsa da, başta Bitcoin olmak üzere kripto paraların kara para aklama ve terör finansmanı için kullanılabileceğine dair çekinceler mevcuttur. Kamu otoriteleri ve merkez bankaları tarafından da henüz yeterli desteği alamayan ve hatta bazı ülkelerde yasaklanan Bitcoin, bu nedenle olumsuz bir imaja sahiptir. Her ne kadar, blok zinciri teknolojisinden ziyade özel olarak kripto para kavramıyla ilişkili bir konu olsa da; bu durum da blok zinciri teknolojisinin geleceği açısından önemli risklerden birisidir (Acheson, 2018).

Blok zinciri teknolojisinin en önemli özelliklerinden birisi, yapılan işlemleri değiştirilemez şekilde zincire eklemesidir. Blok zinciri teknolojisinin güvenlik anlamında en önemli yapı taşlarından olan bu özellik, diğer taraftan hatalı yapılan işlemleri veya hırsızlık gibi olaylar sonucu ortaya çıkan işlemleri temizleyebilmek açısından ise bir dezavantaj olarak yorumlanabilir. İşlemlerin değiştirilememe özelliğinin, finans dünyasındaki bazı düzenleme ve yasalar ile çelişebileceği ve blok zinciri teknolojisinin yaygınlaşması açısından zorluklar ortaya çıkarabileceği ifade edilmektedir (Lumb, 2016).

4.2.3. Performans ve Ölçeklenebilirlik (Performance and Scalibility)

Bitcoin, her ne kadar gittikçe artan bir kullanım oranına sahip olsa da, dünyadaki tüm finansal işlemlerin hacmi düşünüldüğünde henüz düşük diyebileceğimiz seviyelerde finansal hacime ve sınırlı işlem sayılarına sahip bir para birimidir. Bitcoin'in hızlı yaygınlaşmasının devam etmesi durumunda ise blok zinciri teknolojisinin mevcut haliyle artan ölçekteki ihtiyaçları karşılayabilecek bir teknik altyapı olup olmadığı önemli bir sorudur. Ölçeğin artması böylesine büyük dağıtık bir sistem üzerinde koşan algoritmaları saniyede binlerle ifade edebilecek işlem seviyeleri ile karşı karşıya bırakacaktır. Blok zinciri teknolojilerinin performansı ve ölçeklenebilirliği alanı akademisyenler tarafından öncelikli olarak araştırılmaya başlayan konular arasındadır (Croman ve ark. 2016), (Decker, 2015), (Sasson ve ark., 2014). Pratik hayatta da blok zincirini iyileştirmeye yönelik örnekler ortaya çıkmaya başlamıştır. Örneğin 2014'de duyurulan Etherum, gerek blok eklenme süresinin Bitcoin'e göre çok daha kısa olması gerekse kullandığı betik dilinin daha karmaşık işlemleri yerine getirilebilecek şekilde esnek ve gelişkin olması gibi özelliklerle, son dönemde en çok öne çıkan blok zinciri yapılarının başında gelmektedir.

Performans ve ölçeklenebilirlik konusunda önemli gelişmelerden bir tanesi, 1 Ağustos 2017 yılında yapılan ve blok boyutunun arttırıldığı bir hard-fork sonrası Bitcoin Cash (BCC) isimli yeni bir kripto para biriminin ortaya çıkmasıdır. BCC temel olarak işlemleri hızlandırmak, işlem ücretleri düşürmek ve dünya çapında bir ödeme altyapısı sunabilmek hedefiyle hayata geçirilmiş bir kripto para birimidir (Bitcoin.com, 2017).

Son dönemde ödeme işlemlerin hızlandırılması ve sistemin ölçeklendirilmesi anlamında yeni bir gelişme de Lightning Network (Şimşek Ağ) isimli bir teknolojidir. Bu teknoloji hızlı ve ucuz işlem ücretleriyle işlem yapmak isteyen eşlerin, kendi aralarında ve blok zincirine ağına bağımlı ödeme kanalları açmaları ve işlemlerini bu ödeme kanalları üzerinde yapmaları esasına dayanır. Ödeme kanalları üzerinde işlem güvenliğini sağlamak için çoklu imzalama ve iki yönü ödeme yapılabilmesi gibi mekanizmalar da tasarlanmıştır. Blok zinciri ağına iş yükü yaratmadan tamamlanabilen bu işlemler, çeşitli durumlarda blok zincirine yansıtılarak tüm sistemdeki işlemlerin tutarlı olması sağlanır (Lightning Network, 2018).

5. TARTIŞMA (DISCUSSION)

Bitcoin ve kripto para kavramları, son dönemde ekonomi ve finans dünyası için en ilgi çekici konuların arasında yer almaktadır. Bitcoin'e hayat veren ve açık muhasebe sistemi kavramını hayatımıza sokan blok zinciri teknolojisi ise, gerek dağıtık mimarisi gerekse güvenlik özellikleriyle büyük mühendislik firmaları ve danışmanlık şirketlerinin ilgi odağı olmuştur. Blok zinciri teknolojisinin uygulama alanları sadece bankacılık sektörüyle sınırlı kalmamış, çeşitli kamusal uygulamalardan güvenlik uygulamalarına kadar birçok alana yayılmıştır. On yıl gibi kısa bir sürede birçok ürün ve hizmetin altyapısını oluşturması beklenen blok zinciri teknolojisi, mühendislik anlamında önemli gelişmelerin yaşanacağı, büyük dönüşümlerin gözlemleneceği bir alan olarak öne çıkmaktadır.

Tüm teknolojik alanlarda olduğu gibi, blok zinciri teknolojisi alanındaki gelişmeler de akademik çalışmalarla desteklenerek daha ileri seviyelere ulaşabilecektir. Dünyanın önde gelen üniversitelerinde bu alanda derslerin açılmaya başlandığını ve araştırma laboratuvarlarının kurulduğunu gözlemlemek mümkündür.

Uluslararası gelişmelere baktığımızda gerek mühendislik uygulamaları gerekse akademik çalışmalar anlamında, blok zinciri teknolojisi alanında önemli gelişmeler gözlemlenmektedir. Ülkemizde ise sınırlı sayıda olmakla birlikte olumlu gelişmeler yaşandığını söyleyebiliriz. Özellikle 2017 yılı itibariyle çeşitli üniversitelerimizde gerçekleştirilen blok zinciri odaklı çalıştaylar ve yine TÜBİTAK bünyesinde kurulan Blokzincir Araştırma Laboratuvarı (Tübitak, 2018) bu alandaki önemli gelişmelerdir. Ayrıca TC Merkez Bankası öncülüğünde blok zinciri alanında çalışma gruplarının oluşturulması ve blok zinciri alanında yapılan bazı konferanslara kamu kurumlarından çeşitli yetkililerin katılması da blok zinciri teknolojisinin regülasyon boyutuyla ilgili önemli gelişmelerdir. Yine ülkemizde, blok zinciri teknolojisini kullanarak yeni iş çözümleri üretmeye çalışan çeşitli teknolojik girişimlerin (kimlic.io ve Colendi vs.) de olduğu bilinmektedir.

Blok zinciri teknolojisi, yapay zekâ ve nesnelerin interneti teknolojileri gibi çok büyük değişimlere yol açabilecek teknolojiler arasında gösterilmektedir. Henüz olgunlaşma dönemindeki bu teknolojinin ülkemizde de yakın olarak takip edilmesi oldukça önemli bir gelişmedir. Ülkemizde blok zinciri teknolojisi alanında yapılan gerek akademik gerek uygulama gerekse regülatif çalışmaların sonuç odaklı olarak yürütülmesi, hızlı ve kaliteli şekilde çıktılar üretebilmesi hedeflenmelidir. Bu alandaki çalışmaların teşvik edilerek yaygınlaştırılması, dünyada yaşanan önemli bir teknolojik dönüşüm sürecinde ülkemizin hak ettiği yeri almasını sağlayacaktır.

KAYNAKLAR (REFERENCES)

Nakamoto, S. 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf .

Wikipedia, 2018a, Satoshi Nakamoto, Wikimedia Foundation, https://en.wikipedia.org/wiki/Satoshi_Nakamoto .

Blockchain Luxembourg S.A., 2018, Blockchain Market Capitalization, https://blockchain.info/charts/market-cap .

Wikipedia, 2018b, Craig Steven Wright, Wikimedia Foundation, https://en.wikipedia.org/wiki/Craig_Steven_Wright .

Kılınç, H. 2014, Fair and secure multi-two party computation and multi party fair exchange, Koç Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Çay, Ş. 2016, Elektronik ödeme sistemlerinin finansal piyasalara etkisi, Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Tüfek, B. Ü. 2017, Elektronik ödeme araçları ve geleceğin yaklaşımı kripto para, Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Yakupoğlu, C. 2016, A comparative study of bitcoin and alternative cryptocurrencies, Yıldırım Beyazıt Üniversitesi, Fen Bilimler Ensitüsü, Yüksek Lisans Tezi, Ankara.

Göksaran, E. C. 2017, An analysis of neoliberal sociality in the particular case of bitcoin, Orta Doğu Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Balçısoy, E. 2017, Yüksek performanslı bitcoin madenciliği için SHA256 özet algoritmasının eniyilenmesi, TOBB Ekonomi ve Teknoloji Üniversitesi, Fen Bilimleri Ensitütüsü, Yüksek Lisans Tezi, .Ankara.

Karaköse, İ. S. 2017, Elektronik ödemelerde blok zinciri ve sistematiği ve uygulamaları, Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Kayseri.

Bayram, O. 2017, Dış ticarette yeni ödeme şekli banka ödeme yükümlülüğü BPO-etkinlik analizi, İstanbul Ticaret Üniversitesi, Dış Ticaret Enstitüsü, Doktora Tezi, İstanbul.

Sönmez, A. 2014, Sanal Para Bitcoin, The Turkish Online Journal of Design, Art and Communication, 4(3), 1-14.

Ateş, L. 2014, Bitcoin: Sanal Para ve Vergileme, Vergi Sorunları Dergisi, 37(308), 131-141.

Bozdoğanoğlu, B. 2014, Sanal Para Birimi Bitcoin'in Kayıtdışı Ekonomi ile Karapara Faaliyetlerine Etkisi ve Vergilendirilmesi, Legal Mali Hukuk Dergisi, 10(111), 3-18.

Yüksel, B., Armağan, E. 2015 Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 74(2), 173-220.

Koçoğlu, Ş., Çevik, Y. E., Tanrıöven, C. 2016, Bitcoin Piyasalarının Etkinliği, Likitidesi ve Oynaklığı, Journal of Business Research Turk-Türk İşletme Araştırmaları Dergisi, 8(2), 77-97.

Taşdöken, S. 2016, Dijital Para Bitcoin'in KDV'si, Vergi Dünyaları Dergisi, 0(417), 118-121.

Önal, A. 2016, Banka Vasıtalı Ödeme Araçlarını Dışlayan Bir Sistem Olarak Kripto Sanal Para Bitcoin ve Hukuki Niteliği, Banka ve Finans Hukuku Dergisi, 5(17), 165-195.

Kızıltepe, F., Öz, H. 2016, Bitcoin Nedir / Ne Değildir, *Vergi Sorunları Dergisi*, 39(331), 90-95.

Plassaras, A. N., 2017, Dijital Para Birimlerini Düzenleme: Bitcoin'in IMF ile Birlikte Değerlendirilmesi, (Çev: Gökçen, H. B.), Vergi Dünyası, 0(428), 120-137.

Cormen, T. H., Leiserson, J. E., Rivest, R. L., Stein, C. 2009, Introduction to Algorithms**,** 3rd Edition, MIT Press, A.B.D.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. 2016 Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University, New Jersey.

Price, R. 2015, The 21 Companies That Control Bitcoin, Business Insider UK, http://uk.businessinsider.com/bitcoin-pools-miners-ranked-2015-7

Usta, A., Doğantekin, S. 2017, Blockchain 101, MediaCat Kitapları, İstanbul.

Accenture, 2016, Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems, https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm .

Wikipedia, 2018c, List of Cryptocurrencies, Wikimedia Foundation, https://en.wikipedia.org/wiki/List_of_cryptocurrencies .

CoinMarketCap, 2018, All Cryptocurrencies https://coinmarketcap.com/all/views/all .

Özgün Law, 2017, ICO (Initial Coin Offering) Nedir? http://www.ozgunlaw.com/tr-TR/HDetay/ico--initial-coin-offering-nedir--255.html .

CoinSchedule Limited, 2018, Cryptocurrency ICO Stats 2018, http://www.coinschedule.com/stats.html .

Mougayar, W. 2016, 4 Criteria For Evaluating Blockchain ICOs, CoinDesk, https://www.coindesk.com/evaluate-blockchain-initial-cryptocurrency-offering/ .

Deloitte, 2015, Blockchain Distrupting the Financial Services Industry https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_Cons_Blockchain_1015.pdf .

Cognizant, 2016, Blockchain in Banking : A Measured Approach, https://www.cognizant.com/whitepapers/Blockchain-in-Banking-A-Measured-Approach-codex1809.pdf .

Everis Next, 2016, 17 Blockchain Disruptive Use Cases, https://everisnext.com/2016/05/31/17-blockchain-disruptive-use-cases/ .

Evans, C. W. 2015, Bitcoin in Islamic Banking and Finance, *Journal of Islamic Banking and Finance*, 3(1), 1-11.

Kar, I. 2016, GENERAL BLOCKCHAIN, The latest customers for the technology behind bitcoin are NATO and the US military, Quartz, http://qz.com/681580/the-latest-customers-for-the-technology-behind-bitcoin-are-nato-and-the-us-military/ .

Tapscott, D., Tapscott, A. 2016, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World, Portfolio/Penguin, A.B.D.

Short, T. 2016, Blockchain: The Comprehensive Guide to Mastering the Hidden Economy, Amazon CreateSpace Independent Publishing Platform, A.B.D.

Ramsey, S. 2016, **Blockchain: Quick Start Guide to Understanding Blockchain, the Biggest Revolution in Financial Technology and Beyond Since The Internet**, Amazon Digital Services, A.B.D., 2016.

Huckle, S, Bhattacharya, R, White, M, Beloff, N. 2016, Internet of Things, Blockchain and Shared Economy Applications, *Procedia Computer Science*, 98(2016), 461-466.

Popov S. 2017, The Tangle, http://iotatoken.com/IOTA_Whitepaper.pdf .

Bauerle, N. 2018, Why Use a Blockchain?, CoinDesk, https://www.coindesk.com/information/why-use-a-blockchain/.

Wüst, K., Gervais, A. 2017, Do you need a blockchain?, IACR Cryptology Print Paper Archieve, 375.

Deloitte, 2018, Deloitte Blockchain Lab, https://www2.deloitte.com/ie/en/pages/technology/topics/blockchain-lab.html

Rozenfeld, M. 2016, Getting Linked to the Blockchain, http://theinstitute.ieee.org/technology-topics/computing/getting-linked-to-the-blockchain .

Cohen, B. 2016, ISO May Propose Certified Standards for Blockchains and Distributed Ledgers, Bitcoin Magazine, https://bitcoinmagazine.com/articles/iso-may-propose-certified-standards-for-blockchains-and-distributed-ledgers-1464189647 .

Young, J. 2016, Why 1/3 of all bitcoin exchanges since 2009 were hacked, Coinfox, http://www.coinfox.info/news/6323-why-1-3-of-all-bitcoin-exchanges-since-2009-were-hacked .

Newbium, 2016, The 10 Biggest Bitcoin Hacks In History, https://coins.newbium.com/post/655-the-10-biggest-bitcoin-hacks-in-history .

Duggan, W. 2017, 12 Biggest Cryptocurrency Hacks In History, Benzinga, https://www.benzinga.com/fintech/17/11/10824764/12-biggest-cryptocurrency-hacks-in-history.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M. 2014, Zerocash: Decentralized Anonymous Payments from Bitcoin, *IEEE Symposium on Security and Privacy*, San Jose, CA, USA

Wirdum, A. V. 2016, Ethereum's DAO Forking Crisis: The Bitcoin Perspective, Bitcoin Magazine, https://bitcoinmagazine.com/articles/ethereum-s-dao-forking-crisis-the-bitcoin-perspective-1467404395 .

Acheson, N. 2018, Is Bitcoin Legal?, Coindesk, http://www.coindesk.com/information/is-bitcoin-legal/ .

Lumb, R. 2016, Downside of Bitcoin: A Ledger That Can't Be Corrected, The New York Times, http://mobile.nytimes.com/2016/09/10/business/dealbook/downside-of-virtual-currencies-a-ledger-that-cant-be-corrected.html .

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G,. Song, D., Wattenhofer, R. 2016, On scaling decentralized blockchains, Financial Cryptography and Data Security 2016, https://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf .

Decker, C., Wattenhofer, R. 2015, A fast and scalable payment network with bitcoin duplex micropayment channels, *Stabilization, Safety, and Security of Distributed Systems*, 9212, 3-18.

Bitcoin.com, 2017, What Is Bitcoin Cash? https://www.bitcoin.com/info/what-is-bitcoin-cash .

Lightning Network, 2018, Lightning Network: Scalable, Instant Bitcoin/Blockchain Transactions https://lightning.network/.

Tübitak, 2018, Blokzincir Araştırma Laboratuarı, Tübitak BİLGEM, http://blokzincir.bilgem.tubitak.gov.tr/ .