

**T.C.**  
**AYDIN ADNAN MENDERES ÜNİVERSİTESİ**  
**SOSYAL BİLİMLER ENSTİTÜSÜ**  
**EKONOMİ VE FİNANS ANABİLİM DALI**  
**2020-YL-107**

**DİJİTAL DÖNÜŞÜMDE BLOKZİNCİR TEKNOLOJİSİ**  
**ve BITCOIN'İN EKONOMİYE ETKİSİ**

**HAZIRLAYAN**

**Özgür GÜVEN**

**TEZ DANIŞMANI**

**Dr. Öğr. Üyesi Şahin BULUT**

**AYDIN – 2020**

**T.C.**  
**AYDIN ADNAN MENDERES ÜNİVERSİTESİ**  
**SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE**  
**AYDIN**

Bu tezde sunulan tüm bilgi ve sonuçların, bilimsel yöntemlerle yürütülen gerçek deney ve gözlemler çerçevesinde tarafımdan elde edildiğini, çalışmada bana ait olmayan tüm veri, düşünce, sonuç ve bilgilere bilimsel etik kuralların gereği olarak eksiksiz şekilde uygun atıf yaptığımı ve kaynak göstererek belirttiğimi beyan ederim.

... / ... / 2020

Özgür GÜVEN

## ÖZET

### DİJİTAL DÖNÜŞÜMDE BLOKZİNCİR TEKNOLOJİSİ

#### ve BITCOIN'İN EKONOMİYE ETKİSİ

Özgür GÜVEN

Yüksek Lisans Tezi, Ekonomi ve Finans Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Şahin BULUT

2020, XIII + 84 sayfa

Teknolojinin hayatı kolaylaştıran etkisi finansal enstrümanlarda bitcoin ile kendini göstermiştir. Bitcoin, 2009 yılında ortaya çıkmasının ardından ödeme sistemlerinde devrim niteliğinde bir altyapı sunan kripto para türüdür. Bitcoinin temel teknolojisi olan blokzincir, güvenilir bir üçüncü tarafa ihtiyaç duymayan, merkezi olmayan bir sistem olarak tasarlanmış; geniş uygulama potansiyeli ile kamu ve iş dünyasında hızla kabul görmüştür. Bu teknolojik altyapı üzerinde geliştirilen kripto paralar ile birey ya da kurumlar nakit parayla yapılan her türlü harcamayı ve para transferini gerçekleştirmektedir.

Bu çalışmada, Ocak 2012 – Mart 2020 tarihleri arasında cumhuriyet altını, altın ons fiyatı, ham petrol fiyatı, amerikan doları ve euro para birimleri ile bitcoin arasındaki korelasyon ilişkisi incelenmiştir. Araştırma kapsamında tanımlayıcı istatistikler, Spearman korelasyon analizinden faydalanılarak yapılmıştır. Yapılan analizlerinin sonucuna göre piyasalarda yer edinmeye başladığı ilk dönem olan 2012'de bitcoinin diğer göstergelerle arasında istatistiksel olarak anlamlı bir ilişkisi saptanmamıştır ( $p>0.05$ ). Bitcoinin dolar karşılığının bir önceki yıla göre üç katından fazla arttığı 2017 yılı ise bitcoinin zirve yılı olup; euro ile arasında pozitif yönlü kuvvetli bir ilişki vardır ( $r=0.873$ ;  $p<0.001$ ). 2012-2020 döneminde istatistiksel olarak bitcoinin ham petrol fiyatı ile arasında negatif yönlü ve zayıf; cumhuriyet altını, altın ons fiyatı, dolar ve euro ile arasında ise kuvvetli bir ilişki vardır ve bu ilişki anlamlıdır. Yüksek hareketlilik, bitcoinin, istikrarlı bir ödeme aracından ziyade spekülasyon bir yatırım aracı olarak görülmesi olarak algılanabilir. Bitcoinin uzun dönemde en çok euro ile arasında kuvvetli bir ilişki olduğu saptanmıştır.

**ANAHTAR SÖZCÜKLER:** Bitcoin, Blokzincir, Blockchain, Fintech (Fintek).

## **ABSTRACT**

### **BLOCKCHAIN TECHNOLOGY in DIGITAL TRANSFORMATION**

#### **and BITCOIN'S EFFECT ON THE ECONOMY**

Özgür GÜVEN

Master Thesis Department of Economics and Finance

Thesis Supervisor: Dr. Şahin BULUT

2020, XIII + 84 pages

The life-effect of technology has manifested itself in financial instruments with bitcoin. Bitcoin is a type of cryptocurrency that offers a revolutionary structure in payment systems since its inception in 2009. Blockchain, bitcoin's core technology, is designed as a decentralized system that does not need a trusted third party; with its wide application potential, it has quickly gained acceptance in the public and business world. With the cryptocurrencies developed on this technological structure, individuals or institutions carry out all kinds of cash and money transfers.

In this study, the correlation relationship between Cumhuriyet Gold, gold ounce price, crude oil price, american dollar and euro currency and bitcoin between January 2012 and March 2020 was examined. The descriptive statistics of the research were made by using Spearman correlation analysis. In 2012, when it first started to take a place in the markets, a significant relationship between bitcoin and other indicators was not detected ( $p > 0.05$ ). The year 2017, when the dollar value of bitcoin increased three times than the previous year, was the peak year of bitcoin; there is a strong positive relationship with the euro ( $r = 0.873$ ;  $p < 0.001$ ). Negative and weak between bitcoin and crude oil price in the period of 2012-2020; there is a strong relationship between Cumhuriyet Gold, gold ounce price, dollar and euro, and this relationship is significant. High mobility can be perceived as seeing bitcoin as a speculative investment tool rather than a sample payment instrument. It has been determined that bitcoin has a strong relationship with the euro for the long term.

**KEYWORDS:** Bitcoin, Blockchain, Fintech.

## ÖNSÖZ

Bu çalışmaya başlamadan önce ilk literatür taraması yaptığım tarihlerde dünya genelinde yayınlanmış akademik çalışmaların sayısı ile bu satırları yazdığım şu anda mevcut olan akademik çalışma sayısı arasında dikkate değer bir fark bulunmaktadır. Bu durum, teknolojinin ve beraberinde getirdiği dijitalleşmenin, küresel bir popüleriteden ziyade kullanım alanlarının hızla arttığı köklü değişimleri göstermektedir.

Tez konusu belirlerken ilgi alanımı göz önünde bulundurarak, bana bilgi ve tecrübeleriyle yol gösteren tez danışmanım Dr. Öğr. Üyesi Şahin BULUT'a teşekkürlerimi sunarım.

Değerli varlıklarım oğullarım Onur ve Teoman'a enerjileri için teşekkür ederim.

Özgür GÜVEN

# İÇİNDEKİLER

KABUL VE ONAY SAYFASI.....	iii
BİLİMSEL ETİK BİLDİRİM SAYFASI.....	iv
ÖZET .....	v
ABSTRACT .....	vi
ÖNSÖZ.....	vii
ŞEKİLLER DİZİNİ .....	x
TABLolar DİZİNİ.....	xi
EKLER .....	xii
KISALTMALAR DİZİNİ .....	xiii
GİRİŞ.....	1
<b>1. BÖLÜM</b> .....	<b>3</b>
1. BLOKZİNCİR TEKNOLOJİSİ.....	3
1.1. Kriptoloji Kavramı.....	4
1.2. Blokzincir Çalışma Prensipleri .....	6
1.2.1. HASH Fonksiyonları.....	8
1.2.2. Eşler Arası Değer Değişim Sistemi .....	10
1.3. İşleyişteki Mekanizmalar .....	14
1.3.1. Emek Kanıtı (Proof of Work) .....	15
1.3.2. Hisse Kanıtı (Proof of Stake).....	15
1.3.3. PoW ve PoS Karşılaştırması .....	16
1.4. Sıfır Bilginin İspatı (Zero Knowledge Proof).....	18
1.5. Blokzincirin Sorun ve Sınırlamaları .....	20
1.6. Herkes Yağmura Şiir Yazdı.....	22
1.7. Blokzincir Teknolojisinin Kullanım Alanları .....	23
1.8. Dünyada Blokzincir Atılımları .....	26

1.8.1. Kullanıldığı Sektörler.....	27
1.8.2. Avrupa Birliği Blokzincir Gözlemevi.....	29
1.9. Türkiye’de Blokzincir Atılımları.....	31
1.9.1. Tübitak Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi.....	33
1.9.2. Blokzincir Çalıştayları.....	33
<b>2. BÖLÜM.....</b>	<b>36</b>
<b>2. KRİPTOPARALAR VE BITCOIN.....</b>	<b>36</b>
2.1. Bitcoinin Geçmişi.....	36
2.2. Bitcoin İşlem Süreci.....	39
2.3. Güncel Haliyle Piyasalarda Bitcoin.....	44
2.4. Kripto Paraların Piyasadaki Yeri.....	49
2.5. Libra.....	51
2.6. Literatür Taraması.....	53
2.6.1. Akademik Çalışmalar.....	53
2.6.2. Çalışmanın Literatürü.....	55
<b>3. BÖLÜM.....</b>	<b>58</b>
<b>3. UYGULAMA VE ANALİZ.....</b>	<b>58</b>
3.1. Uygulamanın Amacı.....	58
3.2. Uygulamanın Kapsamı, Veri Seti ve Model.....	58
3.3. Metodoloji ve Yöntem.....	59
3.4. Uygulama Bulguları.....	60
<b>4. SONUÇ.....</b>	<b>71</b>
<b>5. KAYNAKLAR.....</b>	<b>73</b>
<b>6. EKLER.....</b>	<b>81</b>
<b>ÖZGEÇMİŞ.....</b>	<b>84</b>

## ŞEKİLLER DİZİNİ

Şekil 1. Kriptoloji Bilimi Alt Dalları .....	1
Şekil 1.1. Blok Zincirleri .....	6
Şekil 1.2. Blok Başlığı.....	7
Şekil 1.3. Hashcash Başlığının Bir Örneği .....	9
Şekil 1.4. Blokzincir Topolojileri .....	12
Şekil 1.5. PoW ve PoS Karşılaştırması .....	17
Şekil 1.6. Sıfır Bilgi Kanıtı Algoritmasında Kanıtlar ve Gizli Veriler.....	19
Şekil 1.7. Küresel Bitcoin Ağındaki Tam Uçlar.....	28
Şekil 1.8. Uçların Ülkelere Göre Dağılımı .....	28
Şekil 1.9. BCTR İş Birlikçileri .....	31
Şekil 1.10. Takas İstanbul Blokzincir Projelerinde Kullanılan Teknolojiler .....	32
Şekil 2.1. Bitcoin Sembol ve Logoları .....	37
Şekil 2.2. Kâğıt Cüzdan Örneği.....	40
Şekil 2.3. Bitcoin Çalışma Mantığı .....	41
Şekil 2.4. Bitcoin İşlem Süreci .....	42
Şekil 2.5. Bitcoin'in Türk Lirası Karşılığı (Temmuz 2019).....	46
Şekil 2.6. Bitcoin'in Türk Lirası Karşılığı (Ekim 2019) .....	46
Şekil 2.7. Libra Birliği Üyeleri: Libra Ekosistemi .....	52
Şekil 3.1. 2012-2020 Yılları Arasında Yatırım Aracı Olarak Bitcoin ve Altın.....	70



## TABLÖLAR DİZİNİ

Tablo 1.1. ECB (European Central Bank) Para Matrisi .....	3
Tablo 1.2. Türk Alfabesi İçin Mod 29'a Göre Tamsayı Karşılıkları.....	4
Tablo 2.1. Aralık 2016 ve Haziran 2019 için Karşılaştırmalı Bitcoin Piyasa Değerleri .....	45
Tablo 2.2. Bitcoin'in Serbest Piyasadaki Karşılıkları (2 Temmuz 2019) .....	47
Tablo 2.3. Kripto Para ATM'lerinin Artışı (coinatmradar.com, Aralık 2019).....	49
Tablo 2.4. Piyasa Değerine (Haziran 2019) Göre En İyi 30 Kripto Para Birimi.....	50
Tablo 2.5. Bitcoin ve Blokzincir Alanındaki Akademik Çalışmalar.....	54
Tablo 2.6. YÖK Tez Merkezi: Bitcoin ve Blokzincir Alanındaki Akademik Çalışmalar...	55
Tablo 2.7. Dergi Park Akademik: Bitcoin ve Blokzincir Alanındaki Akademik Çalışmalar.....	55
Tablo 3.1. Korelasyon Tablosu: Ocak 2012 – Mart 2020 .....	61
Tablo 3.2. Korelasyon Tablosu: Ocak – Aralık 2012.....	62
Tablo 3.3. Korelasyon Tablosu: Ocak – Aralık 2013.....	63
Tablo 3.4. Korelasyon Tablosu: Ocak – Aralık 2014.....	64
Tablo 3.5. Korelasyon Tablosu: Ocak – Aralık 2015.....	65
Tablo 3.6. Korelasyon Tablosu: Ocak – Aralık 2016.....	66
Tablo 3.7. Korelasyon Tablosu: Ocak – Aralık 2017.....	67
Tablo 3.8. Korelasyon Tablosu: Ocak – Aralık 2018.....	68
Tablo 3.9. Korelasyon Tablosu: Ocak – Aralık 2019.....	69

## **EKLER**

Ek 1: BDDK Basın Açıklaması .....	81
Ek 2: I. Ulusal Blokzincir Çalıştayı.....	82
Ek 3: II. Ulusal Blokzincir Çalıştayı .....	83



## KISALTMALAR DİZİNİ

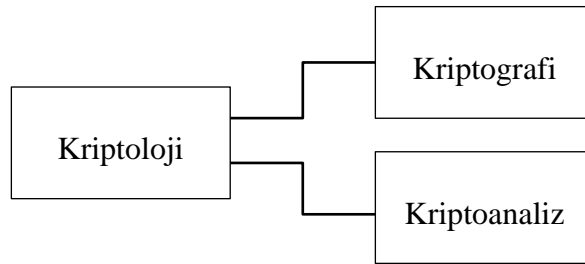
ASIC	: Application Specific Integrated Circuit
ATM	: Automatic Teller Machine (Otomatik Vezne Makinesi)
BCT	: Blockchain Technology (Blokzincir Teknolojisi)
BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
BTC	: Bitcoin (Kripto Para Birimi)
Coin	: Kendi Blokzincir platformu olan kripto paraların tümü
Fintech	: Financial Technology (“Finansal Teknoloji” sözcüklerinin birleşimi)
ICANN	: Internet Corporation of Assigned Names and Number (İnternet Tahsisli Sayılar ve İsimler Kurumu)
IIF	: The Institute of International Finance (Uluslararası Finans Enstitüsü)
KYC	: Know Your Customer (Müşterinizi Tanıyın: Bir müşterinin kimliğini doğrulayan ve iş ilişkisine yönelik olası yasadışı niyet riskleri ile uygunluğunu değerlendiren bir işlemdir)
P2P	: Peer to Peer (Eşten Eşe Bağlantı)
PoS	: Proof of State (Hisse Kanıtı)
PoW	: Proof of Work (Emek/İş Kanıtı)
SPK	: Sermaye Piyasası Kurumu
TCMB	: Türkiye Cumhuriyeti Merkez Bankası
W3C	: World Wide Web Consortium (Dünya Çapında Ağ Konsorsiyumu, Ekim 1994'ten itibaren uluslararası Dünya Çapında Ağ standartlarını belirleyen örgüttür)

## GİRİŞ

Türkçe’de kullandığımız “para” sözcüğü dilimize Farsça kökenli “pâre”den geçmiştir. Bir malın satışı veya hizmet alımı işlemlerinde harcanan zamanı ve değer kaybını azaltmak amaçlı olarak ilk para birimi sikke kullanılmaya başlanmıştır. Sikkelerin günlük hayatta aktif yer alması ile hem işlem fiyatları düşmüş hem de ekonomide devinim yükselmiştir. Dilimize Arapçadan geçen bir sözcük olan sikke, üzerindeki resim ve yazılarla devletin garantisini arkasına alarak ticarete yaygın bir ödeme aracı olmuştur. Madeni formda olmasının getirdiği saklanma ve taşınma problemi, beraberinde güvenlik problemini de getirdiği için zaman içinde günümüzdeki senede benzer kâğıtlar kullanılmaya başlanmıştır (Keş, 2015: 33-34).

Bir satın alma gücü olarak paranın kullanılmadığı dönemlerde insanlar takas yöntemine başvurmuştur. Para icat edilmeden önce, deniz kabuğundan kıymetli metallere kadar çeşitli mallar değişim aracı olarak kullanılmıştır. İlerleyen teknoloji ile günümüzde hem satın alma hem de serveti koruma amaçlı olarak para dijital bir şekle dönüşerek “kripto para birimi” halini almıştır.

Kriptoloji bir şifre bilimi olup verilerin gizliliğini ve değişmezliğini sağlamayı hedeflemektedir. Burada bahsedilen gizlilik, bir şifreleme işlemi söz konusu olduğunda ancak anahtar uzunluklarının artırılmasıyla çözülmektedir (Özyılmaz, 2014: 82). Kullanıcı kimliğinin doğrulanması olarak da bilinen bu yöntem sayesinde, bir kişinin başka birinin kimliğine bürünmesi engellenmiş olur. Burada devreye giren yardımcı faktörler ise elektronik sertifikalar ve elektronik imzalıdır.



Şekil 1. Kriptoloji Bilimi Alt Dalları (Özyılmaz, 2014: 2)

Kriptoloji olarak Türkçe’ye geçmiş *Cryptography* sözcüğünün kökeni Yunanca olup; gizli, saklı anlamına gelen *kryptos* sözcüğü ile yazmak anlamına gelen *graphein* sözcüğünün birleşiminden türetilmiştir. Kriptoanaliz sözcüğü ise elde edilen şifrelenmiş, diğer deyişle anlamlı olmayan bir yazımdan birtakım teknikler kullanarak gerçek yazıma ulaşma

yöntemidir. Kripto para mantığının temelinde yatan “kriptoloji” terimi, matematiğin hem şifre bilimi (kriptografi), hem de şifre analizini (kriptoanaliz) kapsayan dalıdır. Bir şifreleme işleminde hedef, iletinin istenmeyen kişiler tarafından okunmasını önlemektir (Özyılmaz, 2014: 2).

Bir ağ üzerinde yer alan veri formundaki dijital paraların güvenliği ve güvenilirliği önem kazanmıştır. İşte bu aşamada, kullanıcıya ait verilerin güvenle saklanması için algoritmalar geliştirilmeye başlanmıştır. Bugün geldiğimiz noktada “kriptoloji” amaca en uygun ulaşım olarak kabul edilir ve veriyi oluşturan haricindekilerin erişimini engellemektedir (Yılmaz, 2007: 137).

Çalışmanın ilk bölümünde kriptolojinin yapısı, verilerin şifrelenerek kaydedilmesini ve takip edilmesini sağlayan, güven, zaman ve maliyet gibi problemlere çözüm sunmak üzere tasarlanan Blokzincir teknolojisinin mimarisi, işleyişindeki mekanizmalar ve kullanım alanları incelenmiştir. Sonraki bölümde bitcoinin tarihçesi, tasarım özellikleri, diğer kripto paralardan farkı ve piyasadaki güncel hali değerlendirilmiştir. Son bölümde cumhuriyet altını, altın ons fiyatı, ham petrol fiyatı, amerikan doları ve euro para birimleri ile bitcoin arasındaki korelasyon ilişkisi incelenmiştir.

# 1. BÖLÜM

## 1. BLOKZİNCİR TEKNOLOJİSİ

Kripto para birimi, yapısında kriptolojiyi (şifreleme bilimi) kullanan para birimidir. Kripto para birimlerinin işleyişindeki mekanizmalar, çalışan algoritmalar, ağ sistemini ayakta tutan bilgisayar yazılımları ve donanımları bir bütün olarak ele alındığında matematik dalını ve bilişim teknolojileri dalını ilgilendirmektedir (Yılmaz, 2007: 138). Öte yandan para birimi özelliği göstermesi ve sistemin sürdürülebilirliğinin sağlanması açısından gerekli olan servis sağlayıcıları da içinde barındıran bir ekonomik sistem oluşturması nedeniyle iktisadi bilimler de ilgi alanına girmektedir (Gültekin Y. ve Bulut Y., 2016: 83).

Tablo 1.1. ECB (European Central Bank) Para Matrisi (Kaynak: Avrupa Merkez Bankası)

Yasal Statü	Para Formatı	
	Fiziksel	Dijital
Regülasyona tabi olmayan	- Farklı türlerdeki yerel para birimleri	- Sanal para birimi
Regülasyona tabi	- Banknot ve madeni paralar	- Elektronik para - Ticari bankalarda bulunan tasarruflar

Fiziksel yapıdaki banknot ve madeni paralar ile bankalarda tutulan tasarruflar ve elektronik paralar regülasyona tabidir. Sanal para birimi olarak da adlandırılan kriptoparalar ise merkezi denetimden bağımsızdır.

Şifreleme bilimi artık güncel hayatın pek çok alanında uygulanmaktadır. Kullanım alanlarına bankamatikler, rezervasyon sistemleri, e-posta iletileri, telefon bankacılığı ve normal bankacılık işlemleri, cep telefonları, uydu sistemleri, füze sistemleri, savaş uçakları, sağlık sistemleri, e-devlet uygulaması gibi birçok alan örnek verilebilir. Dijital dünyada bölgeler ve ülkeler arasındaki sınır ortadan kalkmış bulunmaktadır. Dijital dünyada sınırları elektronik olarak aşmak, gerçek dünyaya ait fiziki harita sınırlarını aşmaktan daha kolay olmaktadır. Bu noktada bilginin güvenliği için kriptografinin önemi öne çıkmaktadır; ülkelerin vatandaşlarına ve kurumlarına hızlı ve kolay erişim için elektronik ortamda aktardığı hizmetler güvenli yollarla sunulmalıdır (Ülker, 2013: 38).

Ağ teknolojisinin gelişimi ile birlikte dijital olarak depolanan bireysel veri miktarı

hızla artmaktadır. Depolama ve verilerin paylaşımı, yazılım uygulamalarının bulut teknolojisini kullanmasıyla bir kaynak bulmuşsa da ekonomik tasarruflar dâhilinde faydalanılan bulutta veri kaybı veya gizlilik sızıntısı gibi durumlar söz konusu olabilmektedir. Çözümü sağlamak için ihtiyaç duyulan verilerin bütünlüğü ve gizliliğidir. Bazı veri paylaşım uygulamalarında, sertifika yetkilerinde koruma sağlama gibi, genellikle birden fazla tarafça bakılması gerekmektedir. Bilgi güvenliği sorununun veri paylaşımı alanında nasıl çözüleceği konusu her zaman önem taşımıştır (Zheng, 2018: 557).

## 1.1. Kriptoloji Kavramı

İnsanlık tarihi boyunca bazı bilgilerin özel olması nedeniyle yanlış kişilerin eline geçmesi engellenmek istenmiştir. Bu çaba neticesinde ilkel sayılabilecek yöntemlerle şifrelemenin temelleri atılmıştır. Teknolojik gelişmelerin hız kesmediği günümüzde ise güvenliğin ve özellikle bilgi güvenliğinin taşıdığı önem büyüktür. Dijital dünyada kriptografik algoritmalarla yararlanarak özel veya gizli bilgilerin istenmeyen kişilerden korunması için yazılım uygulamaları geliştirilmiştir.

Şifrelemede, kullanılan anahtarın özelliğine ve çeşidine göre algoritmalar bulunmaktadır. Klasik kriptolojide yaygın olan Kaydırma Şifresi (The Shift Cipher) olup modüler aritmetiğe dayanmaktadır (Özyılmaz, 2014:16). Kaydırma şifresini kullanarak basit bir şifreleme yapmak için mod 29'daki Türk alfabesini baz alan bir örnek aşağıda yer almaktadır.

Tablo 1.2. Türk Alfabesi İçin Mod 29'a Göre Tamsayı Karşılıkları

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Kaydırma şifresi için alınacak değer ( $k$  olarak adlandırılır), bu durumda 0 ile 28 arasında bulunmalıdır.

Özyılmaz (2014: 17) çalışmasında yer alan örnekleme esas alınır;  $k = 8$  ve düz metin = “YAŞASIN TÜRKİYE” olacak şekilde yürütülen bir şifrelemede izlenen akış aşağıdaki gibidir:

Öncelikle düz metindeki her harf Tablo 1.2 kullanılarak tamsayılara çevrilir ve

Y A Ş A S I N T Ü R K İ Y E

27 0 22 0 21 10 16 23 25 20 13 11 27 5

elde edilir.

Ardından her bir rakama mod 29’a göre 8 eklenir;

6 8 1 8 0 18 24 1 3 28 21 19 5 13

elde edilir.

Elde edilen bu tamsayılar şifreli metni oluşturmak için Tablo 1.2 yardımıyla alfabetik karakterlere çevrilir ve

F Ğ B Ğ A Ö U B Ç Z S P E K

şifreli metin elde edilir.

F Ğ B Ğ A Ö U B Ç Z S P E K

şifreli metin tam sayılı rakamlara çevrilir.

6 8 1 8 0 18 24 1 3 28 21 19 5 13

Ardından mod 29’a göre sırayla her rakamdan 8 çıkarılınca

27 0 22 0 21 10 16 23 25 20 13 11 27 5

elde edilir.

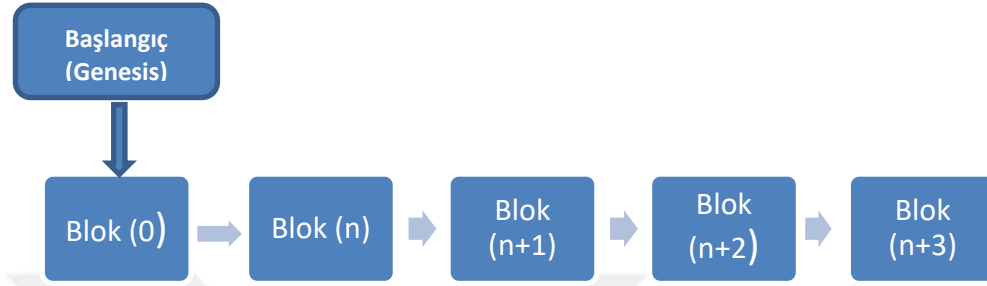
Tekrar Tablo 1.2 yardımıyla tam sayılar alfabetik karakterlere çevrilerek

“YAŞASIN TÜRKİYE” mesajı elde edilir.



## 1.2. Blokzincir Çalışma Prensibi

Adından da anlaşılacağı üzere, Blokzincir yaklaşımında verilerin saklandığı yapılar blok olarak adlandırılmaktadır ve bu blok yapıları bir zincir şeklinde (zaman açısından doğrusal bir dizi yapısında) düzenlenmektedir. Bu zincir kapsamındaki ilk blok yapısına “genesis” (başlangıç) blok denir.



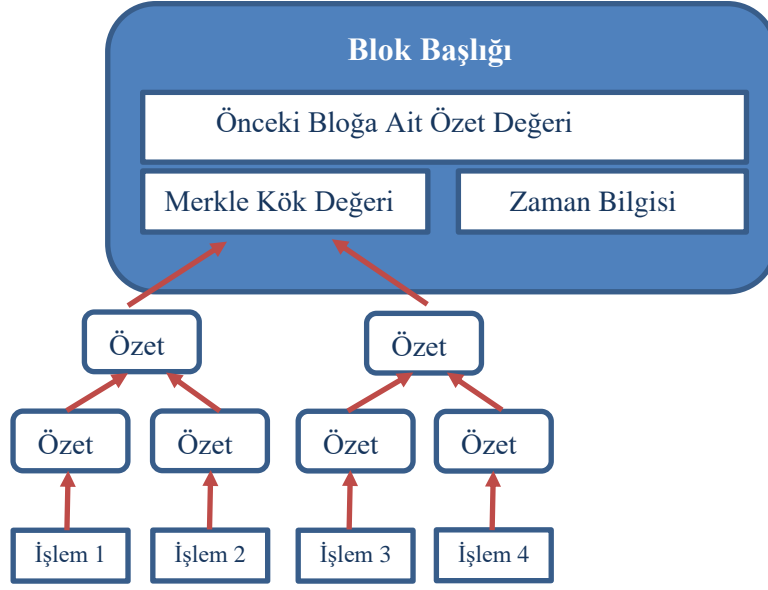
Şekil 1.1. Blok Zincirleri (<https://bctr.org/blockchain-nedir/> esinlenerek çizilmiştir, 01.07.2019)

Blok başlığı içindeki bilgilerin toplu bir şekilde, bir güvenli özetleme algoritmasından geçirilmesi ile o bloğa ait olan özetleme bilgisine (block hash) ulaşılmaktadır.

Her bir blok 1 MB uzunluğunda olup her birinde en az bir işlem tutulmaktadır. Bloğa ilişkin veriyi tutan üst bilgi ise 80 Byte boyutundadır. Bir blok içerisinde 350-500 civarında işlem verisi tutulmaktadır. Bir transfer işlemi gerçekleştirildiğinde en az 250 Byte boyutundadır (Çarkacıoğlu, 2016:43).

Blokzincirine yeni blokların eklenmesi işlemine “madencilik” adı verilir. Madencilik işlemi için çaba harcayan her bir üye de “madenci” olarak isimlendirilmektedir. Madenciler blokzincirinin kayıt altına alınması ve transfer işlemlerinin gerçekleştirilmesi için zorunlu uygulayıcıdır. Bitcoin için başlangıçtaki blok oluşturma ödülü 50 bitcoin olarak belirlenmiştir ve her 210.000 blokta ödül yarılanmaktadır. Bu da yaklaşık olarak 4 yıllık bir süreyi işaret etmektedir. Hesaplandığı takdirde yarılanmanın 2140 yılına kadar devam edeceği öngörülmektedir (Antonopoulos, 2014:2).

Transfer işlemlerinin tamamının ağda yer alan tüm taraflar aracılığıyla izlenmesi mümkündür. Madenciler tarafından onaylanan işlemler bir araya gelerek blokları oluşturmaktadır.



Şekil 1.2. Blok Başlığı (Wang, 2018: 96)

Şekil 1.2’de görüldüğü üzere her bir blok kendisinin önündeki bloğa ait özet verisini içermektedir. Mevcut bloğun kendi özet verisini oluşturması ile ardından gelecek blok için bu hazırlanan özetleme bilgisi kullanılmaktadır.

Eğer bir saldırgan bu yapıya müdahale etmek isterse, Blokzincir ağı içindeki hedef aldığı bloğun içeriğini değiştirebilmesi için hem hedef bloğu hem de bu bloğu takip eden diğer tüm blokları değiştirmesi gerekmektedir (Wang, 2018: 96). Süreklilik arz eden bir blok üretimi (kötü niyetli birisi değişim yaparken Blokzincire yeni blokların katılıyor olması) ve blok üretim algoritmasının mantığı gereği bu senaryo teorikte mümkün gibi görünse de pratik açıdan saldırıyı hayata geçirmesi normal koşullarda gerçekleşmeyecektir.

Bir transfer işlemlerinin gerçekleştirilmesi için tarafların kim olduğunun belli olması gerekmektedir. Ancak tarafların gizliliğinin sağlanabilmesi amacıyla kişisel bilgilerini vermek zorunluluğu bulunmamaktadır. Bu amaçla tarafları adresleyebilmek için elektronik hesap cüzdanları kullanılmaktadır. Bir cüzdan aslında açık ve gizli anahtara sahip bir adres verisinden oluşmaktadır. Cüzdan adresi SHA-256 özetleme algoritması ve açık anahtar kullanılarak oluşturulmaktadır. Adresler Base58 kodlama sistemini kullanmaktadır. Örnek bir cüzdan adresi “1ELiFNCg6v1wnc6cxTrY4m1MNDC5e5Vb1B” şeklinde olup bu adresin gizli anahtarı “5JNbVn7tXtkAp5rYagA9ZPaGDBCRueqycsyxTugpW” şeklinde olmaktadır. Cüzdanın sahibi, cüzdana ait gizli anahtarı bilen tek kişidir. Burada yasal bir ilişkilendirme ve hak sahipliği söz konusu olmamaktadır. Bu sebeple gizli anahtarın

gizliliğinin korunması en önemli noktalardan biri olarak öne çıkmaktadır. Bir elektronik cüzdan üzerinden harcama yapabilmek için işlemlerin gizli anahtar kullanılarak imzalanması gerektiğinden bu verinin gizli tutulması gerekmektedir. Bir cüzdana gönderim yapılabilmesi için sadece adresinin bilinmesi yeterli olmaktadır (Kırbaş, 2018: 79).

### 1.2.1. HASH Fonksiyonları

Bir karma işlevi, bir girdi olarak rastgele uzunluktaki verileri alan ve karma değeri adı verilen sabit uzunlukta bir bit dizgisi çıkaran bir algoritmadır.

Karma değer, aynı giriş verileri için her zaman aynıdır. Karma fonksiyonlar, hesaplamalarda, örneğin karma tabloları kullanarak hızlı bir şekilde veri kayıtlarını bulmak için kullanılmaktadır. Karma değerlerin boyutu genellikle olası giriş verilerinin boyutundan daha küçüktür. Bu nedenle birçok girdi veri noktası tek bir hash değerini paylaşmaktadır. İyi bir karma işlevi, giriş değerlerini orantısız olarak karma değerlere dağıtmalı, böylece her bir karma değeri, aynı sayıda olası giriş değerine bağlanmalıdır. Bu orantılılığı elde etmenin bir yolu, karma değerinin mümkün olduğunca rastgele “davranmasını” sağlamaktır. Karma değer rastgele olduğu gibi davranmasına rağmen, hala belirleyici olduğu unutulmamalıdır: Bir girdi verildiğinde, onun karma değeri her zaman aynı olmaktadır. Bitcoin, çalışma kanıtı (Proof of Work) gerçekleştirmek için şifreleme karma işlevlerini kullanmaktadır. Kriptografik karma fonksiyonları (bazen güvenli karma işlevleri olarak adlandırılır) düzenli hash işlevlerine göre ek gereksinimler getirmektedir (Franco, 2015: 96):

**Tek yönlü (Önleme) direnci:** Karma değeri göz önüne alındığında, giriş verilerini bulmak hesaplama açısından uygun olmamalıdır. Daha ileride açıklanacağı üzere, bu, iş kanıtının uygulanması için önemli bir özelliktir.

**Zayıf çarpışma direnci:** Bir girdi verildiğinde, aynı karma değere sahip başka bir girdi bulmak, hesaplama açısından mümkün değildir.

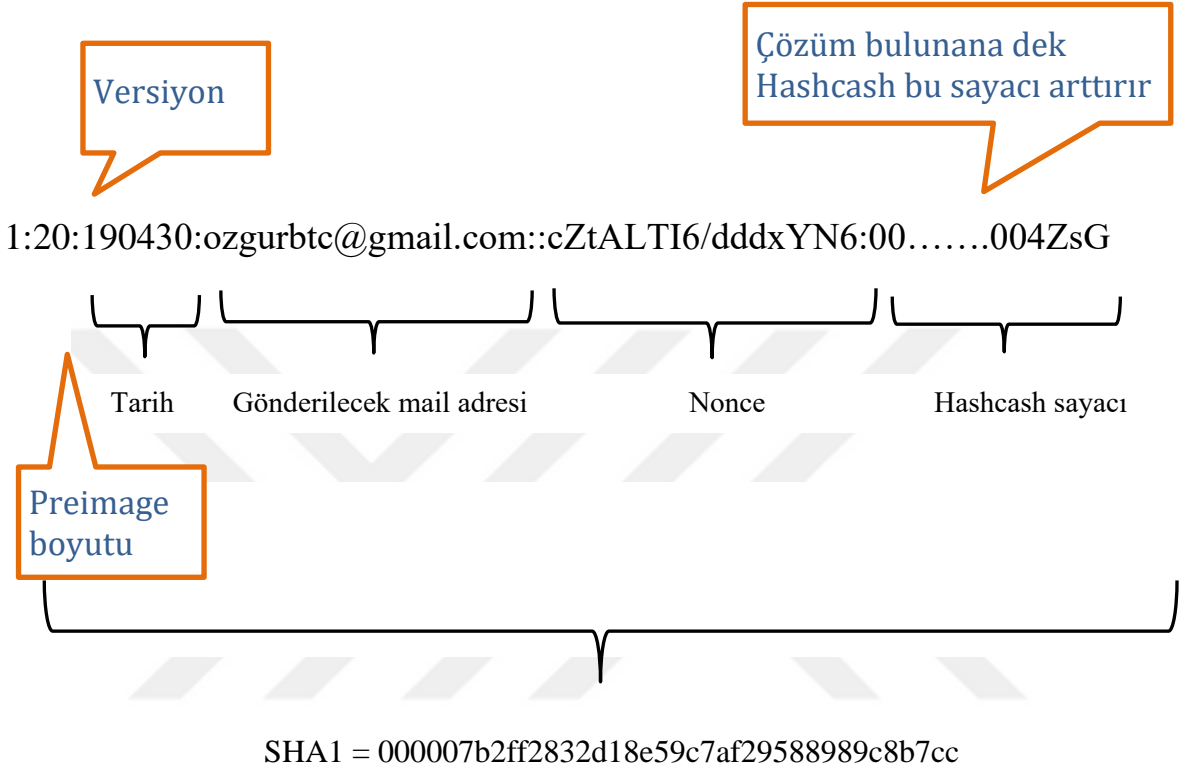
**Güçlü çarpışma direnci:** Aynı karma değeriyle sonuçlanan iki girdi veri noktasını bulmak sayısal olarak mümkün değildir.

Bitcoin, işin ispat fonksiyonu olarak  $SHA256^2$ 'yi kullanır.  $SHA256^2$ ,  $SHA256$  hashing fonksiyonunun iki kez uygulanmasıdır.  $SHA256^1$ , NSA (Ulusal Güvenlik Dairesi,

---

<sup>1</sup> SHA özetleme fonksiyonları, NSA tarafından tasarlanmış ve NIST tarafından Birleşik Devletler Federal Bilgi İşleme Standardı olarak yayınlanmış bir dizi kriptografik özetleme fonksiyonudur. SHA, Secure Hash

National Security Agency) tarafından tasarlanan ve NIST (Ulusal Standartlar ve Teknoloji Enstitüsü, National Institute of Standards and Technology) tarafından 2001'de yayınlanan karma işlem kümesinin (SHA-2) bir parçasıdır. SHA256, çıkışı 256 bit uzunluğundaki bu ailenin bir karma işlevidir (Franco, 2015: 96).



Şekil 1.3. Hashcash Başlığının Bir Örneği (Franco, 2015: 104 esinlenerek çizilmiştir)

Bir dijital zaman damgası, bir mektup üzerindeki bir posta damgası veya resmi bir kurumdan gelen bir lastik damga gibi fiziksel bir zaman damgasına benzemektedir. Dijital bir zaman damgası, belirli bir zamanda, dijital bir belgenin var olduğunu ispat etmektedir. İki taraf arasında bir sözleşmenin imzalandığını, bir web sitesindeki bir işlemin gerçekleştiğini veya bir dijital para birimindeki işlemlerin gerçekleştiğini belgelemek gibi birçok uygulamaya sahiptir. Dijital zaman damgasındaki bilgiler genellikle güvenliğin sağlanması için gereken veridir. Bir karma kullanmak çeşitli avantajlara sahiptir. İlk olarak, zaman damgalı olacak bilgiler, zaman damgasını korumak için kullanılan ortamdan özel ve ayrı tutulabilir. İkincisi, bir karma, genellikle, onu oluşturan bilgidен önemli ölçüde daha küçüktür ve bu da dolayısıyla depolama maliyetlerini düşürmektedir. Üçüncü olarak, dijital

---

Algorithm yani Güvenli Özetleme Algoritması anlamına gelmektedir. Bugün SHA-0, SHA-1, SHA-2 olmak üzere üç farklı yapıda özetleme algoritması mevcuttur. SHA256 daha güvenli bir algoritma ile daha güçlü şifreleri meydana getirmeye yardımcı olmuştur.

imzalar genellikle önceden belirlenmiş bir boyuttaki veriler üzerinde en iyi şekilde çalışmaktadır (Franco, 2015: 99).

Hashcash bir çalışma kanıtı (PoW) sistemidir ve madencilik algoritmasının bir parçası olarak bitcoinde kullanılmaktadır. Bir hashcash şunları içermektedir (Franco, 2015: 104):

- . Hashcash protokolünün sürümü, 1.
- . Preimage boyutu, 20 bit veya 5 ilk sıfır karakteri kapsamaktadır. Kısmi karma inversiyon için başlangıç sıfır bitlerinin sayısını göstermektedir.
- . E-postanın gönderildiği tarih, 190430 veya 30 Nisan 2019 olarak ifade edilmektedir. Hash jetonu yalnızca belirli bir süre için geçerli olmaktadır.
- . Alıcı e-posta adresi, ozgurbtc@gmail.com olarak örnekte kullanılmıştır.
- . Sadece bir e-posta için kullanılan bir nonce<sup>2</sup> örnekte cZtALTI6/dddxYN6 biçimindedir. Bu perdenin arkasındaki mantık, birçok e-postayı göndermek için kullanılan aynı hashcash başlığını önlemek amaçlıdır. Alıcı e-posta sunucusu, verileri bir önbellekte saklayabilir ve e-posta önbelleğinde bulunmayan bir e-posta geldiğinde, e-posta düşürülmektedir. Bu, bir botnet<sup>3</sup> ustasının, birden fazla e-postada aynı hashcash başlığını yeniden kullanmasını önlemektedir.
- . Sayaç örnekte 00... 004ZsG biçimindedir. Hashcash, bu sayacı, tüm başlığın karmasının ön koşul gereksinimiyle eşleşeceği bir değer bulana kadar arttırmaktadır.

### 1.2.2. Eşler Arası Değer Değişim Sistemi

Bitcoin, yeni iletişim biçimine adapte bir ödeme sistemine uygun hızlı, güvenli ve sınırsız bir paraya olan ihtiyaca cevap vermiştir (Antonopoulos 2014:1). Bununla birlikte, tam olarak uygulanabilir bir dijital paranın (veya hisse senetleri, tahviller veya lisanslar gibi herhangi bir dijital varlığın) ortaya çıkması iki temel teknik sorun sunmaktadır: Orijinallik onayı ve çifte harcama sorunu.

---

<sup>2</sup> Nonce, İngilizce Number only used once (Sadece bir kere kullanılan sayı), istenilen blok özetleme değerini üretmek amacıyla kullanılan ve değiştirilebilen sayı değeridir. Başka bir deyişle hash edilen bloğa eklenen ve yeniden hash edildiğinde zorluk seviyesi kısıtlamasının olduğu sayıdır. Nonce, madencilerin çözdüğü Blokzinciri sayısıdır.

<sup>3</sup> Botnet sözcüğü, "robot" ve "network" (ağ) sözcüklerinin birleşiminden türetilmiştir; siber suçluların ele geçirdiği ve internete bağlanabilen her türlü cihazlardır.

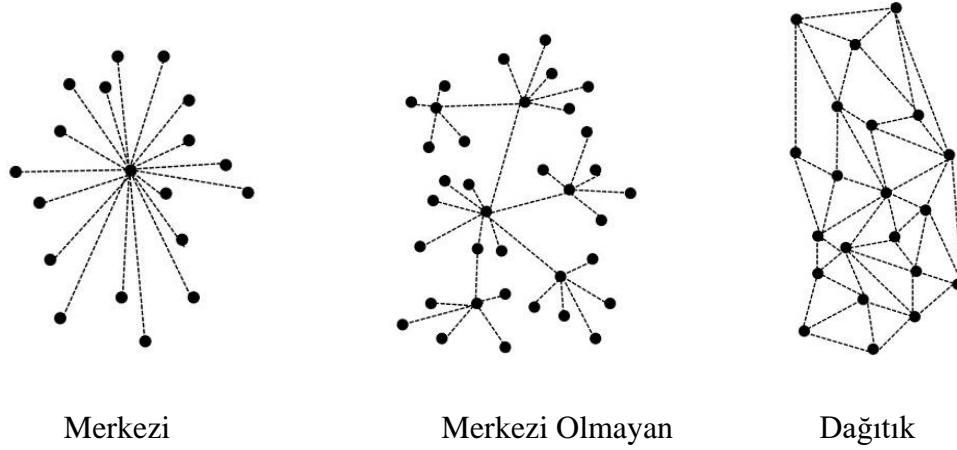
Fiziksel varlıklardan farklı olarak, dijital nakit veya diğer dijital varlıklar sadece bir bilgisayar (bit dizisi) şeklindedir ve diğer tüm dijital dosyalar gibi, kopyalanabilmektedir. Hesap sahibinin bakiyesinin defterini tutacak aracı yoksa (örneğin nakit veya menkul kıymetler hesap bakiyesi), biri kartı gönderebilmekte ve bir kopyasını saklayabilmektedir. Bu, çift harcama problemi olarak bilinmektedir ve bunu önlemek için, her bir harcamada merkezi bir deftere karşı çevrimiçi kontrol edilmesi gerekmektedir (Chaum, 1992: 98). Bu nedenle, dijital varlığın tüm işlemlerinin yetkili bir kaydına ihtiyaç duyulmaktadır.

Schollmeier (2001), katılımcıların işlem gücü veya depolama kapasitesi gibi kendi donanım kaynaklarının bir kısmını paylaştığı, dağıtılmış bir ağ mimarisi olarak eşler arası bir ağ tanımlamaktadır. Bu paylaşılan kaynaklar, ağ tarafından sunulan hizmet ve içeriği sağlamak için gerekmektedir (örneğin, iş birliği için kullanılan çalışma alanlarını paylaşmak, depolamak) ve aracı kuruluşlar devreye girmeden diğer meslektaşlar tarafından doğrudan erişilebilmektedir.

Nakamoto tarafından bu iki sorunun (orijinallik onayı ve çifte harcama sorunu) önüne geçmek için önerilen çözüm, açık veya özel anahtar şifreleme teknikleri sayesinde belirli bir fikir birliği mekanizmasıyla birlikte sürekli güncellenen ve kamuya açık bir muhasebe sistemine dayanmaktadır.

We propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions (İşlemlerin kronolojik sırasının hesaplamalı kanıtını oluşturmak için eşler arası dağıtılmış bir zaman damgası sunucusu kullanarak çift harcama sorununa bir çözüm öneriyoruz) (Nakamoto, 2009: 8).

Hofmann (2018) tarafından belirtildiği üzere, dijital para, geniş kabul görmeden önce halkın güvenini kazanmalı ve korumalıdır. Bu nedenle, sahtecilik her ne pahasına olursa olsun önlenmelidir. Dijital para birimi yalnızca değeri temsil eden bitler olduğu için, dijital para birimi işlemlerinin transit geçiş sırasında, makbuzda veya depolamada kurcalamayı önleyecek şekilde yapılması gerekmektedir. Mevcut bankacılık sisteminin aksine, örneğin, bitcoin işlemleri ağın birçok katılımcısı tarafından yayınlanmakta, kaydedilmekte ve saklanmaktadır. Herhangi bir merkezi tescilli sunucuda değil, mutabakat veya herhangi bir manuel müdahale olmadığından işlemlerin dakikalar içinde arka planda değerlendirilmesini sağlamaktadır (Hofmann, 2018: 36).



Şekil 1.4. Blokzincir Topolojileri (Swanson, 2015: 1'den esinlenerek çizilmiştir)

Blokzincir “zincir” olarak adlandırılrsa da, Blokzincir sadece bir “zincir” değildir. Her Blokzincirinin ağda kendi veri blokları mevcuttur. Bu veri blokları düğüm olarak kabul edilmektedir. Tüm düğümler, bazı ara bağlantı yöntemleri yoluyla doğrudan ya da dolaylı olarak bağlanmaktadır. Blokzincirler, düğümlerini kenarlarından birbirine bağlayan temel yapılar olarak farklı tipte ağlara sahiptir. Şekil 1.4'de gösterildiği üzere merkezi topoloji, merkezi olmayan topoloji ve dağıtık topoloji dahil olmak üzere Blokzincirleri için kullanılan üç tipik topoloji mevcuttur. Temel olarak topolojiler, Blokzincirlerine düğümleri organize etmeleri için destek sağlamaktadır (He, 2018: 142).

Oluşturulan bu yetkili kayıt, tüm işlemlerin mimari olarak dağıtılmış eşler arası bir ağ tarafından bloklar halinde kaydedildiği, paylaşılan bir veritabanı olan Blokzincirdir. “Zaman damgası sunucusu” ile verinin belirli bir zamanda var olması gerektiğini kanıtlanmış olmaktadır ve işlem bloklarına kronolojik bir düzen vermek için tüm işlemlerin ‘zaman damgalı’<sup>4</sup> olduğu anlamına gelmektedir. Her yeni blok daha sonra tüm işlem geçmişini pekiştirerek öncekine kriptografik olarak zincirlenmektedir. Tüm işlemlerin geçmişi paraların sahiplerini tanımlar ve kopyalanması imkânsız olan fiili benzersiz varlıklar (dijital belirteçler) oluşturmaktadır (Hofmann, 2018: 37). Bitcoin gibi kripto para birimleri söz konusu olduğunda, işlemi iptal etmek veya aynı parayı iki kez harcamak durumunda, kötü niyetli bir katılımcının tarihin bir bölümünü (yani işlemin kaydedildiği dijital bloklar zincirini) tekrar yapması teorik olarak imkansızdır (Nakamoto, 2009: 2).

İşleyişteki bu müdahaleyi önlemenin çözümüne, 1976'da W. Difé ve M. Hellman

<sup>4</sup> Zaman damgası, 1 Ocak 1970'ten itibaren geçen saniye sayısına dayanan 4 baytlık (32 bit) bir dosyadır. (Epoch Unit Timestamp) (Antonopoulos 2014, p. 188). Şu an bu satırlar yazılırken (11 Mart 2019, 23:34), mevcut zaman 1552336457 (<http://www.epochconverter.com/>).

tarafından önerilmiş olan ve Nakamoto'nun blokzincir tasarımına entegre ettiği bir konsept olan dijital imzalar ile ulaşılmıştır. Dijital bir imza, mesajı (yani işlemi) şifreli olarak imzalanmış bir belgeye dönüştürmektedir; böylece okuyan herkes, kimin gönderdiğinden emin olmaktadır. İmzalar, mesajları imzalamak için kullanılan bir gizli anahtar ve bunları doğrulamak için kullanılan bir ortak anahtar kullanmaktadır; böylece yalnızca özel anahtarla imzalanan mesajlar, halka açık olan aracılığıyla doğrulanabilmektedir. Bu işlem şifreleme kanıtı olarak bilinmektedir ve elektronik paralar dijital imzalar zinciri olarak tanımlanmaktadır (Chaum, 1992: 96). Bu nedenle, madeni paraların kilidini açmak için anahtarlara sahip olmak, nakit bulundurmaya eşdeğerdir ve özel anahtar kaybolursa, karşılık gelen dijital cüzdandaki tüm madeni paralar da kaybolmaktadır (Antonopoulos, 2014: 231).

Doğrulama sürecinin aynı anda en iyi şekilde hızı, verimliliği ve güvenliği garanti edebileceği tartışması çözümlenmemiş gibi gözüksede, PoW<sup>5</sup> en sık kullanılan işlem olarak görünmektedir (Antonopolous, 2014: 205). Gerçek blok büyüklüğü 1 MB ile sınırlıyken, teorik olarak saniyede maksimum 7 işlem yapılır; bu da ne yazık ki ana ekonomiye hizmet vermek için yeterli bulunmamaktadır (Hofmann, 2018: 42). Buna karşılık, Visa'nın ağı saniyede 50.000'den fazla işlem gerçekleştirebilmektedir (VisaNet, 2019).

Ayrıca, madencilik endüstrisi, çoğu ideolojik olarak şirketlere karşı olan ya da zayıf yasal sistemleri olan ülkelerde bulunan, büyük ölçüde bilinmeyen taraflardan (büyük madenciler) oluşmaktadır (Greenspan, 2015: 11). Örneğin, bitcoin ağı, karma hesaplama gücünün %51'ini potansiyel olarak kontrol edebilecek ve yeni oluşturulan bir blokta bulunan bilgileri yeniden yazabilecek 1Thash veya F2Pool (bitcoin.info) gibi büyük madencilerin bulunduğu bir havuzda yer almaktadır.

Bu nedenlerden dolayı, çeşitli finansal kurumlar, kendi özel ağlarına veya ortak sistemlere sahip olma fikrini yürütmüş, izinli defterler olarak adlandırılan güvenilir ve önceden seçilmiş onaylama düğümleri ile çalışmaya başlamışlardır. Uluslararası Finans Enstitüsü (IIF) (2015) tarafından yayımlanan makalede vurgulandığı üzere, bu kavram, bitcoin ve diğer birçok kripto para birimi veya alternatif hizmet sağlayıcıların tamamen merkezi olmayan tasarımıyla tümüyle örtüşmektedir.

Blokzincir alanındaki en önemli yeniliklerden biri Ethereum projesidir. İlkelerinin çekirdeği ilk olarak 2013 yılında, mucitlerinden biri olan V. Buterin tarafından yazılmış bir

---

<sup>5</sup> PoW: Proof of Work, "İş Kanıtı", Blokzincir teknolojisinin güvenilirliğinin temel taşlarından biridir.



makale ile önerilmiştir. Ethereum, Turing-complete programlama dili ile geliştirilmiş açık kaynaklı bir dijital para birimidir (Buterin, 2013).

Temel olarak, PoW gibi zorlu hesaplama teknikleriyle güvence altına alınan, tamamen halka açık ve kontrolsüz bir ağa sahip olmak yerine, bu çözümler erişim izinlerinin sıkı bir şekilde kontrol edildiği ve Blokzinciri durumunu değiştirme ya da okuma haklarının seçilen kullanıcılarla sınırlı olduğu bir sistem oluşturur. 2015 tarihli blog yazısında, Buterin iki adet izin verilen Blokzinciri uygulaması kategorisini belirlemiştir (Buterin, 2015):

(1) Konsorsiyum blokajı ve (2) Tamamen özel blokaj.

1. Konsorsiyum blokajları, konsensüs sürecinin önceden seçilmiş bir düğüm seti tarafından kontrol edildiği muhasebe sistemlerini ifade etmektedir. Örneğin, her biri bir düğüm işleten ve her biri bloğu geçerli kılmak için her bloğu imzalamak zorunda olan 15 finansal kurumdan oluşan bir konsorsiyum olarak düşünülebilir. Blokzinciri okuma hakkı katılımcılara açık veya sınırlı olmaktadır.

2. Tamamen özel blokajlarda, izinler bir kuruluştaki merkezi olarak kalmakta ve okuma izinleri herkese açık olmaktadır veya kapalı sayıda katılımcı ile sınırlı olmaktadır. Muhtemel uygulamalar tek bir şirket için veri tabanı yönetimi, denetim veya diğer iç kullanımları içermekte olup, bu nedenle kamuya açık bir okunabilirlik birçok durumda gerekli olmamaktadır. İzin verilen Blokzincirler, düğümleri bilindiği için zorunlu olmayan hesaplamalı blok oluşturma avantajına sahip olmaktadır (Greenspan, 2015). Bu, daha hızlı doğrulama işlemlerine ve artan ölçeklenebilirliğe izin vermektedir ve bu nedenle ana akım ekonominin işlem hacimlerine daha fazla adapte olmaktadır; düzenleyiciler ve yasa koyucular için daha elverişli olmaktadır (IIF, 2015).

### **1.3. İşleyişteki Mekanizmalar**

Blokzincir, saldırıların önlenmesini sağlamak için kimlik doğrulama, şifreleme ve verilerin bütünlüğünü doğrulama yetilerini kullanmaktadır. Bu nedenle, Blokzincir bulut ile bağlantılı platformlar ve yüksek ölçeklendirilebilir olay odaklı mimariler gerektiren işlemler de dahil olmak üzere güvenli veri alışverişini kolaylaştıracağına dair gerekli altyapıyı sağlamaktadır (Mylrea, 2017: 21).

### **1.3.1. Emek Kanıtı (Proof of Work)**

Emek/İş Kanıtı (PoW), esas olarak hesaplama kimliğini çözmek için gerekli olan hesaplama maliyetini, yeni eklenen bloğun güvencesi olarak kullanmakta ve ödül olarak gelir elde etmektedir. Satoshi Nakamoto, dağıtılmış düğümlerin hesaplamalı güç rekabeti ile verilerin tutarlılığını ve fikir birliğinin güvenliğini sağlamak için kullanılan bitcoin hakkındaki makalesinde PoW fikir birliği mekanizmasını önermektedir (Nakamoto, 2008: 3). Bitcoin sisteminde, tüm düğümler bir SHA256 matematik problemini kendi bilgisayar güçleri ile çözmek için rekabet etmektedir. Herhangi bir problemi hesaplamak için karmaşık olmasına rağmen doğrulanması kolay olmaktadır. Bu sorunu çözen, blok hesap haklarına sahip olmaktadır ve bitcoin otomatik olarak ödül olarak üretmektedir (Zheng, 2018: 560).

Gereksinimleri karşılayan blok başlığının karma değeri, genellikle birden çok baştaki sıfırdan oluşmaktadır. Hedef karma değeri ne kadar küçükse, blok başlığının karma değeri o kadar fazla olmakta ve uygun rastgele sayıyı bulmak ve yeni bloğu kazmak daha zor olmaktadır. Bu sayede bitcoin Blokzincir sisteminin güvenliği ve tahribatsız değişimi garanti altına alınmaktadır (Wang, 2018: 96).

PoW konsensüs mekanizması yüksek bilgi işlem gücüne sahiptir. Blok verilere yapılan herhangi bir saldırı veya kurcalama durumu söz konusu olduğunda, tüm blokların problemi yeniden hesaplanması gerekmektedir ve hesaplama hızı, sahte zincirin uzunluğunun ana zinciri geçmesini sağlamaktadır. Bu saldırının maliyeti, doğal olarak mevcut maliyeti çok aşmaktadır (Franco, 2015: 102).

### **1.3.2. Hisse Kanıtı (Proof of Stake)**

PoW yöntemleri, madencilerin işlemleri gerçekleştirmek için çok zor bir matematik denklemini çözmelerini gerektirmektedir. PoS sisteminde, madeni para sahipleri bankacı/madenci rolünü üstlenmekte ve bu paralar yeni basılmış madeni paralarla ödüllendirilmektedir (Kelly, 2015: 110).

Bir satıcının, bir ürün satışı yaparak 10.000 ETH aldığı örneği baz alındığında, bu parayı alması ve mülkünün ağda yayılması gerekmektedir. Mülkiyet yayını Blokzincirinde saklanmaktadır ve satıcı ETH'leri harcamayı seçtiğinde, geçerli bir işlemi doğrulamak için yine bu veri kullanılmaktadır. Uygulamada, satıcı paralarını cüzdanında

yedi gün tutabilir; böylece herkes bu paranın satıcıya ait olduğunu bilmektedir. Satıcının coin'lerdeki hissesiyle ilgili bilgiler ağ için değerlidir ve bu değer daha fazla coin ile ödüllendirilmektedir. Bu durumda, yedi gün sonra, satıcının hesabında net 11.000 ETH bulunmaktadır, bu fazladan 1.000 ETH hissesiyle bağlantılıdır. Bu örnekte, satıcı yedi gün içinde yüzde 10'luk bir faiz ödemesi almaktadır. Bunu garanti eden, bilgisayar kodu olan “merkez bankası”dır (Kelly, 2015: 110).

Bir hisse kanıtı sistemi protokolü, ağdaki bazı katılımcılara gönderilecek olan bir sonraki bloğu ödüllendirmektedir. Bu süreç genellikle katılımcıların fon payları ile orantılı olarak bir sonraki bloğu oluşturmak için “seçildiği” anlamında, rastgele ve adil yapılmaktadır (Franco, 2015: 235).

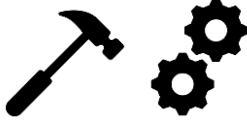
### **1.3.3. PoW ve PoS Karşılaştırması**

Blokzincir teknolojisi tabanlı kripto paralar iki tür veri madenciliği kullanmaktadır. Bunlar Proof-of-Work ve Proof-of-Stake olup kısaca PoW ve PoS olarak ifade edilmektedir.

PoW tipi madencilik türü incelendiğinde kazılan blok kadar coin kazanıldığı görülmektedir. Bazen bir kişi bazen ise bir grup tarafından gerekli algoritma çözülür, böylece Blokzincirindeki bir sonraki bloğun zincire eklenmesi sağlanır. Bu madencilik tipinde yatırımcılar veri bloklarını doğrulama aşamasında asıl çabayı sarf etmektedir. Gerçekleştirilen çözüm ile işlemlerin doğrulanması yapılmakta ve yeni coin'lerin üretilmesini sağlamaktadır. PoW tipi madencilikte blok doğrulanması yapılırken aktif rol oynamadığında ödül kazanılması söz konusu olmamaktadır (Kelly, 2018: 114).

PoW tipi madencilikte ödül, yeni bloğu çözen ilk kişiye verilmektedir. Bu durumda blok algoritmasını çözebilmek için yüksek işlemci gücü gereksinimi doğmaktadır. En yüksek işlemci gücüne sahip olan yatırımcıların ödülü kazanma şansı daha fazla olmaktadır. Madencilik çiftliklerinin ortaya çıkış sebebi bundan kaynaklanmaktadır (Kelly, 2018: 114). Çünkü sayısı milyonlarla ifade edilebilecek kadar yüksek kapasiteli işlemcilerin çalıştığı bu çiftlikler ile madencilik işlemi zamanla kurumsallaşmaya başlamıştır. Açıkça görülmektedir ki artık normal bir vatandaşın evinde bulunan masaüstü bilgisayar ile bitcoin madenciliği yapması imkânsız hale gelmiştir. Bu da bitcoinin ilk çıkış fikri olan bir merkeze bağlı olmama düşüncesini günden güne zedelemektedir (Antonopoulos, 2014: 27).

## Proof of Work



PoW, mining adı verilen yüksek işlemci gücü gerektiren masraflı madencilik türüdür.



Ödül, her blok problemini çözen ilk kişiye verilir.



Ağdaki madenciler, matematiksel problemi çözen ilk kişi olmak için yarışır.

## Proof of Stake



PoS, her yeni bloğun rastlantısal olmayan şekilde, kişinin bakiyesine göre belirlendiği sistemdir.



PoS sisteminde blok ödülü yoktur, madenciler işlem ücretleri ile ödüllendirilir.



PoS paralar binlerce kez daha az maliyetlidir.

Şekil 1.5. PoW ve PoS Karşılaştırması (Rosic, 2016 esinlenerek çizilmiştir)

Bireysel kullanıcılar şu günlerde PoW madenciliği için ASIC isimli çipleri satın alıp bu şekilde madencilik yapmaya devam etmektedir (Franco, 2015, 47).

ASIC kelimesinin açılımı Application Specific Integrated Circuit olup düşük bir enerji ile yüksek verimlilik sağlamaktadır. ASIC, görevler arasında hızlı geçişler yaparak algoritmadaki hesaplamalar için bir görev ara belleği kullanmaktadır. Bir ASIC çipi, belirli bir karma algoritmasına dayalı olarak dijital para birimine yönelik bir madencilik donanım parçasıdır (Koin Bülteni, 2019-b).

Ağdaki işlemleri doğrulamanın bir diğer türü PoS olup esas itibari ile bu yöntem aslında madencilik tanımına uymamaktadır. Çünkü kullanıcıların yeni bir para üretmeleri

için herhangi bir işlem yapmalarına gerek yoktur. Bu nedenle esas ifadesi *mining* değil *minting*'dir. Bunu *madencilik* değil *para basmak* olarak açıklamak daha doğru olacaktır (Franco, 2015: 234).

Kripto parayı tutmak için açılan elektronik cüzdan hesabı, PoS yönteminde ödül kazanıldığında da kullanılır. Kazanılacak olan ödül, elektronik cüzdanda bulunan coin miktarı ile doğru orantılıdır. Cüzdanda ne kadar çok para tutuluyor ise o kadar çok ödül kazanılmaktadır, başka bir ifade ile yeni para üretilmektedir. Elektronik cüzdanda bulunan coinlerin kalış süreleri ne kadar uzar ise o kadar kıdemli olmaktadır ve dolayısıyla bir işlem doğrulaması gerçekleştirildiğinde kazanılacak olan ödül miktarı da o seviyede yükselecektir (Franco, 2015: 234).

PoS sisteminde coinlerin her biri başlangıçta tespit edilmiş olan bir yıllık getiriye sahiptir. Bu noktada sabit bir getiri elde etmeyi garanti etmiş olan yatırımcılar bulunmaktadır. PoW'da ise bu şekilde sabit bir getiri mevcut değildir. Ağdaki düğüm sayılarının ve operasyon sayılarının artması ile madencilik çiftliklerinin sayıları da artmaktadır; bunun getirisi olarak da artık bireysel kullanıcıların gelir elde etme şansı düşmektedir.

İlk yöntem olan PoW'a göre PoS maliyetten tasarruf sağlamaktadır. Elektrik tüketim maliyeti neredeyse sıfırdır. Ayrıca ödül, cüzdan bakiyesi bazlı olduğu için yatırımcıları daha fazla yatırım yapmaya teşvik etmektedir.

PoS metodu ilk olarak 2012 yılında bazı alternatif kripto paralar tarafından kullanılmaya başlanmıştır. Popüler kripto para birimlerinden biri olan Ethereum PoW'dan PoS'a geçiş yapanlar arasındadır. Böylece hem blok üretiminin hem de doğrulanma süreçlerinin hızlanması ve enerji ihtiyacının da azalması amaçlanmaktadır (Ethereum, 2017). Peercoin, Ohm coin, MorningStar, OkCash gibi görece yeni coinlerin çoğu PoS metodunu kullanmaktadır.

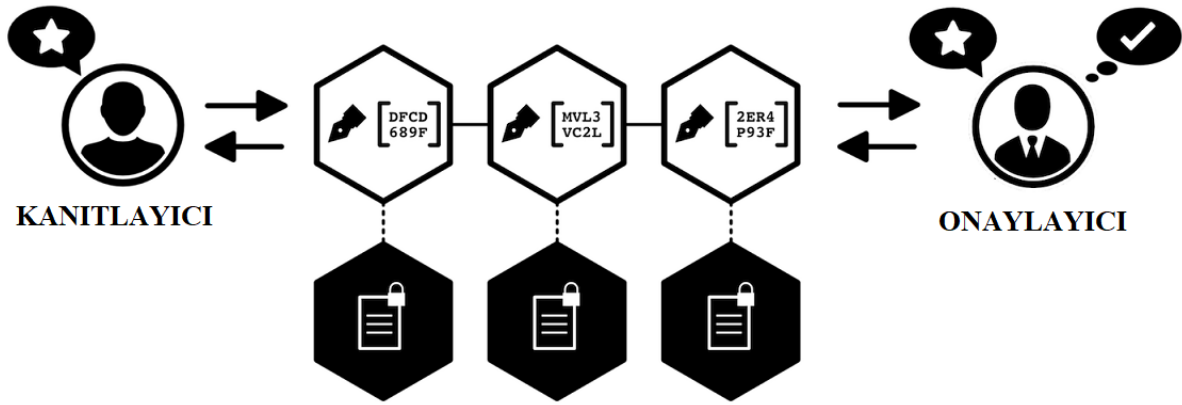
#### **1.4. Sıfır Bilginin İspatı (Zero Knowledge Proof)**

Zero Knowledge Proof (ZKP), bilgisayar bilimlerinde çokça adı geçen önemli bir konu olup Blokzincir teknolojisi ile ilgilenenler tarafından da bilinmektedir.

Sıfır bilgi ispatının genel konsepti, başkalarına A gerçeğinin bilindiğinin kanıtlanmak zorunda olunması durumudur. Ancak A ile ilgili hiçbir bilginin ispatta

gösterilmemesidir. Sıfır bilgi ispatının asıl sorunu verinin işleniyor olmasıdır. ZKP algoritmasında, bir kanıtlayıcı ve bir onaylayıcı mevcuttur. Kanıtlayıcı, mesaj alışverişinde bulunarak bir ifadeyi ispat etmek istemektedir. Genel olarak istenen özellikler, hiçbir kanıtlayıcının, kullanıcıyı yanlış bir ifade konusunda ikna edememesi ve kanıtlayanın, herhangi bir gerçek ifade hakkında onaylayıcıyı ikna etmesi için belirli bir stratejisinin bulunmamasıdır. Gizli işlemlere ve gizlilik sorunlarına cevap olarak, ZKP yüksek derecede gizli olmayı gerektirmektedir. Sıfır bilgi ispatı, Blokzinciri hesaplama işleminde veri miktarını ve hesaplama miktarını da optimize etmektedir (Wang, 2018: 96-97).

Sıfır bilgi kanıtı teknolojisini kullanan kripto para birimlerinin ortaya çıkması Blokzincir dünyasında güvenlik ve mahremiyet açısından önemli bir gelişme olarak görülmektedir. ZKP algoritması, özetle bilinen bir bilginin bir başkasına, bilgiyi ona vermeden ispat edilmesi olarak tanımlanmaktadır. ZKP algoritması, günümüzde özellikle iş süreçlerinin Blokzincir ağlarına aktarılması ve kurumların gizli bilgilerinin tam olarak korunması konusunda önemli bir yer tutmaktadır. Blokzincir ağına dahil olan tarafların işlem ayrıntılarının hiçbirini görmeden onlara onay vermesine imkan tanıdığı için ekstra bir güvenlik sağlamaktadır. Zerocash (ZCash), ZKP teknolojisini kullanan öncü kripto para birimleri arasında yer almaktadır (Ünsal, Kocaoğlu, 2018: 61).



Şekil 1.6. Sıfır Bilgi Kanıtı Algoritmasında Kanıtlar ve Gizli Veriler (Schor, 2018)

Şekil 1.6'yı açıklayan bir senaryoda bir tünel mevcuttur. Tünelin ortasında tünelin tamamını kapatan ve diğer tarafa geçişi izin vermeyen büyük bir kapı bulunmaktadır. X tünelin bir tarafında, Y ise diğer taraftadır. Y kapının arkasına geldiğinde karşı tarafa geçmesinin tek bir yolu vardır, o da elindeki şifreyle kapıyı açmaktır. Eğer Y şifreyi girip kapıyı açarsa, X onun geldiğini görür ve onun şifreyi bildiğini anlar. Bunun için Y'nin

girdiği şifrenin içeriğini X'in bilmesine gerek yoktur.

ZKP, son zamanlarda Blokzinciri uygulamalarında mahremiyeti ve güvenliği artırma potansiyelleri nedeniyle heyecan yaratmaktadır. Kriptograflar yıllardır sıfır bilgi içeren kanıtlarla çalışmakta olup kavramın kendisi yeni değildir; ancak teknoloji artık çevrimiçi gizlilik kavramını yeniden tanımlayacak durumdadır. Herhangi bir sıfır bilgi uygulamasıyla karşılanması gereken üç gereklilik vardır (Schor, 2018):

- Tamlik: Girdi doğruysa, sıfır bilgi kanıtı her zaman 'true' değerini döndürür.
- Sağlamlık: Girdi yanlışsa, 'true' değerini döndürmek için sıfır bilgi kanıtını kandırmak mümkün değildir.
- Gizlilik: Giriş başka hiçbir tarafça alınmaz.

### **1.5. Blokzincir'in Sorun ve Sınırlamaları**

Hangi teknolojik devrim olursa olsun, geçişler dönemlerinde daha önce öngörülmemeyen sorunlarla karşılaşmıştır. Günümüzde artık internetsiz bir şehir yaşamı düşünülemez; ancak internetin ilk yaygınlaşmaya başladığı dönemlerde bugün karşılaşılmakta olan güvenlik ve gizlilik ile ilgili problemler yaşadığımız boyutta öngörülmemiştir.

Bir kripto para tasarımı için altyapı oluşturan Blokzincir'in özelliklerinin bununla sınırlı kalmadığı fark edilmiştir. Bu teknolojik altyapı, dijital dünya için merkezi yapıya ihtiyaç duymayan, buna rağmen güvenilir olan ve ağdaki kullanıcıların tümü tarafından takip edilebilir bir formatta bulunmaktadır. Sistemin şeffaflığı, takip edilebilirliği, geriye dönük silme ve düzeltme yapılamaması gibi işlemler yüksek güvenlik özelliği olarak değerlendirilmektedir (Kırbaş, 2017:81).

Sistemde her kullanıcının kendi hesabı ve bu hesaba ait gizli anahtarı mevcuttur. Kullanıcının gizli anahtarını kaybetmesi durumunda sahipliğini ispatlayacak bir kanıtın bulunmaması, sisteme alışmakta karşılaşılabilecek sorunlardan biri olarak karşımıza çıkmaktadır. Doğal yapısı gereği anonim kullanımı ile yasa dışı işlemlerde çekici hale gelmesi, hem bireyleri hem kamu otoritelerini endişelendirmektedir. Kimlik bilgilerinin gizliliği, bir otoritenin denetim ve düzenlemesine tabi olmayışı, sistemi her türlü yasa dışı finansal transfer işlemine açık hale getirmektedir. Tek bir merkezden yönetimi bulunmadığı

için yapılan bir işleme veya transfere itiraz durumunda silme veya geri alma mümkün olmamaktadır. Her sistemin bir maliyeti vardır. Burada en büyük maliyet madencilik aşamasında görünmektedir. Elektrik sarfiyatının yüksekliği ve ilk kurulum masrafları olsa da, toplam maliyeti, pek çok merkez bankasının toplam maliyetinden az olmaktadır. (Çarkacıoğlu, 2016: 65-66). Enerji harcamalarını karşılaştırmayı sağlayan Power Compare platformu tarafından 2019 yılında yapılmış olan araştırma verilerine göre bitcoin madenciliği 159 ülkeden daha fazla enerji harcamaktadır (Powercompare, 2019).

Mevcut Blokzincir tabanlı tasarıma karşı en büyük eleştirilerden biri sistemdeki anonimlik talebidir. Önerilen anonimlik, siber suçu teşvik etmektedir. Ayrıca Blokzincir'i fonksiyonlarıyla yönetmek için uygun fiyatlandırma maliyetlerinin getirilmesi gerekmektedir (Romano ve Schmid, 2017: 28).

Araştırma ve geliştirme, başarı ve başarısızlık, deneme ve yanılma yoluyla Blokzincir'in mevcut sorunları ve sınırlamaları yaşanarak öğrenilmiştir. Teknoloji çok yeni olduğu için bazı Blokzincir sorunlarıyla karşılaşmış olup, aşağıdaki başlıklarda incelenmiştir (Atozmarkets, 2019):

Terminoloji karmaşası: Blokzincir teknolojisi tamamen yeni bir kelime hazinesi içermektedir.

Kriptografiyi daha yaygın hale getirmiştir, ancak son derece uzmanlaşmış endüstri jargon (Fikri, mesleki vb. ortaklık gösteren kişilerin kullandığı ortak ağız; genel olarak bu terim belli bir uğraş veya ilgiyi paylaşan kişilerin kullandığı dile karşılık gelir) doludur. İnternette ve paydaş forumlarda kapsamlı ve anlaşılması kolay sözlükler ve dizinler sağlama konusunda birçok oluşum mevcuttur.

Ağ boyutu: Blokzincir (tüm dağıtılmış sistemler gibi) kötü niyetli ataklara karşı kırılgan durmaktadır; ancak saldırılara cevap verilmesi ile güç kazanmaktadır.

Bu ihtiyaç, büyük bir kullanıcı ağı gerektirmektedir. Bir Blokzincir, geniş çapta dağılmış bir düğüm yapısına sahip sağlam bir ağ değilse, tüm avantajdan yararlanmak daha zor hale gelmektedir.

İşlem maliyetleri, ağ hızı: Blokzincir tabanlı popüler bitcoin, varlığının ilk birkaç yılında "ücretsiz" olarak lanse edildikten sonra bir miktar işlem maliyetine sahip olarak günümüzde işlem görmeye devam etmiştir.



2016 yılının sonundan itibaren, saniyede yalnızca yedi işlem gerçekleştirebilmekte ve her işlem yaklaşık 0.20 ABD doları tutarında ve yalnızca 80 bayt veri depolayabilmektedir. 2019 sonu itibariyle bir blok ücreti 0.79 ABD dolarına ve 10 dakikalık süreye yükselmiştir. İşlem maliyetlerindeki bu durumu bir Blokzinciri sorununu olarak görmek de mümkündür.

İnsan hatası: Teknoloji bir veritabanı olarak kullanılıyorsa, veri tabanına giren bilginin yüksek kalitede olması gerekmektedir. Bir Blokzincirinde depolanan verilerin doğal olarak ilk önce doğruluğunun bilinmesi uygundur.

“Çöp içeri, çöp dışarı”<sup>6</sup> ibaresi, tıpkı merkezi bir veritabanında olduğu gibi, bir Blokzincir kayıt sisteminde de geçerlidir.

Kaçınılmaz güvenlik açığı: bitcoin ve diğer Blokzincir uygulamalarında dikkate değer bir güvenlik açığı varsayılabilir. Ağa hizmet etmek için düğüm olarak çalışan bilgisayarların yarısından fazlası yalan söylüyorsa, yalan gerçek olarak kabul görmektedir. Buna “%51 atağı” da denilmektedir ve bitcoini başlattığında Satoshi Nakamoto tarafından bu husus vurgulanmıştır. Bununla birlikte, Blokzincirindeki blokları değiştirerek %51 atağının gerçekleştirmesi için ciddi büyüklükte kaynaklar gerekmektedir (Baliga, 2017: 6).

## 1.6. Herkes Yağmura Şiir Yazdı

Blokzincir teknolojisinin sunduğu fırsatlar sadece finans sektörü tarafından farkedilmemiş, bu dijital teknolojinin sunduğu olanaklardan işletmeler de faydalanmak üzere çalışmalar başlatmışlardır. Tıpkı bir tsunamiye benzer etki oluşmuş ve dördüncü sanayi devriminin (Endüstri 4.0 olarak da adlandırılır) odak noktasına ağır ağır yerleşmiştir (Tapscott, 2017: 35). Bu noktada Tapscott’a göre gerçek devrim sosyal medya, büyük veri, robotlar ya da yapay zeka alanında değil, kripto paranın alt yapısını oluşturan Blokzincir teknolojisindedir.

1990’lı yıllarda insanlar arası iletişimi sağlayan medyanın merkezileşmeye başlaması göze çarpmıştır. O yıllarda medya, tek elden ve güçlü olan tarafça kontrol edilebilen, diğer insanların pasif kaldığı ve sadece “tüketici” olduğu bir yapıda bulunmaktadır. İnternetin yaygınlaşması ve internet tabanlı yazılımların geliştirilmesi ile medyanın şekli ve işleyişi zaman içerisinde değişmeye başlamıştır. Toplum sahip olduğu tek

<sup>6</sup> Bilgisayar bilimlerinde “çöp içeri, çöp dışarı” (Garbage In Garbage Out: GIGO), hatalı veya saçma girdi verilerinin saçma çıktı veya “çöp” ürettiği kavramı tanımlar.

yönden çıkmış, aynı zamanda media, haber konusunda “üretici” rolünü de üstlenmeye başlamıştır. Tapscott’a göre o dönemde internet neyse, çağımızda da Blokzincir teknolojisi odur; kendi ifadesiyle gerçek devrimdir (Tapscott, 2017: 28).

Sosyal medya ortamında popüler olan “*Asıl marifet buluttaydı, fakat herkes yağmura şiir yazdı*” ifadesi bitcoin ve Blokzincir arasındaki ilişkiye çok uygun bir açıklama getirmektedir.

## **1.7. Blokzincir Teknolojisinin Kullanım Alanları**

İngiltere, Estonya, Singapur, Dubai, İsviçre ve Kıbrıs Blokzinciri alanında inovasyona öncülük eden ülkelerdendir. Güvenilir ve değiştirilemez verinin kaydının tutulmasına ihtiyaç duyan bir sektör olarak kamusal alanda, birçok ülke Blokzinciri uygulamalarının yatırımlarına destek vermeye başlamıştır (Ersin, Kocaoğlu, 2018: 59). Blokzinciri teknolojisini baz alan yenilikçi uygulamalara ilgi gösteren bir başka kamusal alan savunma sektörüdür. Amerikan Savunma Bakanlığı ve NATO’nun bitcoinin omurgası olan Blokzinciri teknolojisini kullanan ürünler ile ilgilendiği bilinmektedir. NATO lojistik ve tedarik gibi daha geleneksel sayılan uygulamaların altyapısında Blokzinciri teknolojisini kullanmayı hedeflerken, Amerikan Savunma Bakanlığı ise daha ziyade Blokzinciri üzerinde güvenilir bir mesajlaşma uygulamasına odaklanmaktadır (Kar, 2016).

Blokzincir’in devrim yaratabileceği bir diğer alan bilimdir. Bilimsel araştırmalara duyulan güven, bilimsel sonuçların güvenilirliği, özellikle tıp bilimleri gibi yaşamsal alanlarda önem taşımaktadır. Geçmişte sonuç değiştirme, veri temizleme ve seçicilik gibi veri manipülasyonlarıyla ilgili suistimaller nedeniyle elde edilen sonuçların yayınlanması bilimsel sonuçlarda güven eksikliğine neden olmuştur (Romano ve Schmid, 2017: 7).

Tıpkı internetin icat edilmesiyle teknolojinin yeni bir altyapıya kavuşması gibi Blokzincir de bir yenilik getirmiştir. Bir ağ üzerinden geniş kitlelere erişim olanağı sağlayan bu teknoloji de doğal olarak sektörler tarafından dikkat çekmektedir. İnternet üzerindeki her uygulamanın ve programın işleyişi için Blokzincir kullanılması gibi bir durum uygun olmayabilir. Çünkü öncelikle zayıf ve güçlü yönleri, fırsatları ve tehditleri incelenerek bir teknolojinin kullanılmasına karar verilmelidir (Türkmen ve Durbilmez, 2019: 34). Blokzincir’in kullanım alanları aşağıdaki gibi yedi başlıkta özetlenmiştir (ledracapital.com, 17.10.2018):

i) Finansal Araçlar, Kayıtlar ve Modeller: Para Birimi, Finansal Enstrümanlar (Özel ve Devlet Sermayeli Hisse Senetleri, Bonolar, Tahviller), Türev Araçlar (Future Sözleşmeleri, Opsiyonlar, Swaplar, Forwardlar vb.), Finansal Araçlara Bağlı Oy Hakları, Emtialar, Harcama ve Ticaret Kayıtları, Rehin İpotek/Kredi Kayıtları, Hizmet-Servis Kayıtları, Kitlese Fonlama, Mikro Finans ve Mikro Yardımlaşma.

ii) Kamusal Kayıtlar: Tapu ve Arsa-Arazi Kayıtları, Araç Kayıtları, İşletme Lisansları, İşletmelerin Faaliyet (Açılma-Kapanma) Kayıtları, Düzenleyici Kayıtlar, Mevzuatlar, Suç Kayıtları, Pasaportlar, Doğum ve Ölüm Belgeleri, Oy Kullanım Belgeleri, Oylama ve Oylama Kayıtları, Sağlık ve Güvenlik Denetimleri, İnşaat İzinleri, Silah Ruhsatları, Adli Tıp Kayıtları, Mahkeme Kayıtları, Oy Kanıtları, Kâr Amacı Gütmeyen Kayıtlar.

iii) Özel Kayıtlar: Sözleşmeler, Kontratlar, İmzalar, Vakıflar, Emanetler, Kişisel GPS Kayıtları.

iv) Diğer Yarı Kamusal Kayıtlar: Unvanlar-Dereceler, Sertifikalar, Öğrenme Çıktıları, Notlar, İnsan Kaynakları Kayıtları (Performans Çıktıları, Maaşlar vb.), Sağlık Kayıtları, Muhasebe Kayıtları, Ticari Kayıtlar ve Teslimat Kayıtları.

v) Fiziksel Varlık Kilitleri: Ev/Apartman Kilitleri, Tatil Evi/Otel Odası Kilitleri, Araba/Kiralık Araba Kilitleri, Güvenlik Kasası Kilitleri, Teslimatlar ve Bahis Kayıtları.

vi) Soyut Varlıklar: Rezervasyonlar, Patentler, Telif Hakları, Yazılım Lisansları, Oyun Lisansları, Müzik/Film/Kitap Lisansları, Domain (Alan) Adları, Dijital Kimlikler, Eser ve Yazarlık Kayıtları.

vii) Diğer: Dokümanlar (Fotoğraf, Video, Ses), Veri Kayıtları (Sıcaklık, Skor vb.) ve Sim Kartlar.

Blokszinciri teknolojisinin kamu sektöründe kullanılabileceği bazı alanlar şunlardır (Ünsal ve Kocaoğlu, 2018: 59):

- Oylama
- Doküman Yönetimi
- Enerji Dağıtım

- Akıllı Kontratlar
- Dijital Kimlik
- Dijital Pasaport
- Sosyal Güvenlik Sistemi
- Vergi Sistemi

Kamusal kayıtlar açısından kullanılabileceği alanlar Türkmen ve Durbilmez (2019: 34) tarafından şöyle listelenmiştir: Tapu ve arsa-arazi kayıtları, araç kayıtları, işletme lisansları, işletmelerin faaliyet (açılma-kapanma) kayıtları, düzenleyici kayıtlar, mevzuatlar, suç kayıtları, pasaportlar, doğum ve ölüm belgeleri, oy kullanım belgeleri, oylama ve oylama kayıtları, sağlık ve güvenlik denetimleri, inşaat izinleri, silah ruhsatları, adli tıp kayıtları, mahkeme kayıtları, oy kanıtları, kar amacı gütmeyen kayıtlar.

Blokzincir uygulamalarına ait alanlar sağlıktan ticarete, spordan siber güvenliğe, spordan resmî işlemlere dağılım göstermektedir (Murathan, Murathan, 2019: 72).

Sigortacılık açısından bakıldığında, maliyetli olan sigorta isteklerinin alınması, kaza ve olayların uzun süren inceleme süreçleri, sahte belgelerin önlenmesi, Blokzincir'in kullanılması ile daha şeffaf ve hızlı işleyen bir döneme çevrilmesi mümkündür.

Sağlık alanında, hasta bilgilerinin tek bir sistemde tutulması ile hastaneler, klinikler ve doktorlardan oluşan ağ tarafından hasta hakkında doğru stratejinin yürütülmesi ve sigorta süreçlerinin daha verimli ve hızlı işlenmesi anlamına gelmektedir. Kripto para birimlerinin, sağlık sektöründeki uluslararası ödeme sorununa bir çözüm getirerek, değişim aracı rolünü üstlenerek kritik bir rol oynaması mümkündür.

Spor alanında kullanımı ile oyuncular ve kulüpler arasında geleneksel sözleşmeler yerine daha kısa sürede ve bir aracı olmaksızın sözleşmeler imzalanmakta, spor salonları ve stadyumlarda maç olduğunda koltuk biletleri online satışa sunulmakta ve sorun çıkardığı için stadyuma girişi yasaklanan kişilerin kontrolünün yapılabilmesi sağlanmaktadır. Spor organizasyonlarının ve turnuvaların kaydının tek kaynaktan tutulmasının yanı sıra sektörde bulunan tüm spor araç gereçleri ile sporcu, antrenör ve tesis seçimlerinde güvenilir veri oluşturulması amacıyla bir uygulama geliştirilmesi mümkündür (Murathan, Murathan, 2019: 69-71).

Blokzincir'in sahip olduđu en byk potansiyel; delillerin farklı lkelerdeki mahkemeler tarafından tanınabilecek olması, belgelerin dođrulunun kısa srede onaylanması ve kresel bađlamda geerli Blokzincir altyapısına oturmuř ortak kimlik sistemlerinin geliřimi neticesinde; szleřmeler, mřterini tanı (KYC = Know Your Customer), onaylamalar, notlandırmalar, transferler gibi eřitli gncellemelerdir.

zellikle denetim ve gvenliđin tek elden sađlanması zor olduđu uygulama alanlarında, dađıtık yapıdaki ve gvenilir bir merkez kurmanın maliyetinin yksek olduđu durumlarda BC yaklařımı avantajlı hale gelmektedir (Kırbař, 2018: 80). Tarımda ve zirai uygulamalarda yetiřtirme, ilalama ve paketleme srelerinin takibinde ve onaylanmasında kullanılmaktadır. Alan adı ynetim sistemlerinde de BC teknolojisi kullanılarak alan adı sahipliđi ve taraflar arasında devir iřlemleri gerekleřtirmek mmkndr. Birden fazla tarafın iřbirliđini gerektiren yazılım geliřtirme sektrnde de taraflar arasında yapılacak iřlemlerin akıllı szleřme transferleri ve sıralı ve oklu onaylama sistemi ile otomatikleřtirilerek takip ve idare edilmesi de mmkndr (Kırbař, 2018: 81).

Gnlk yařama ait olan anlařmalar, grevler ve demeler Blokzinciri sisteminde tanımlanma, dođrulanma, depolanma ve paylařılma zelliđine sahip dijital kayıttır. Gnmzde imzaların paylařılması ve gvenliđi ile ilgili avukat gibi aracılara, bu teknolojinin yaygınlařmasının ardından gerek duyulması řphe tařımaktadır.

## **1.8. Dnyada Blokzincir Atılımları**

Blokzincir denilince ilk akla gelen kripto paralara karřı yasaklamalar ve yaptırımlar uygulayan, kullanımına karřı olumsuz olan lkeler in ve Rusya'dır. Trkiye'nin de aralarında bulunduđu birok lke kripto paralarla ilgili net bir bakıř aısı ortaya koymayarak tarafsız ođunluktadır. Blokzincir teknolojisine tarafsız yaklařmayı uygun gren tek lke Rusya olmuřtur; in, İngiltere, Avusturya, Fransa, Hindistan, Trkiye, Singapur, Japonya, Kanada gibi lkeler ise konuya olumlu yaklařarak arařtırma kurumları ile destek vermiř ve alıřma grupları oluřturmuřlardır. Blokzinciri dostu olarak n yapmıř kk bir ada lkesi olan Malta, kendisini "Blokzincir adası" olmaya da aday gstermektedir. lke, Blokzinciri teknolojisini yasal olarak destekleyeceđini resmi olarak belgelemiř ve bu giriřiminin sonucunda diđer lkelere gre bir adım ne ıkmıřtır. Malta hkmeti tarafından 4 Temmuz 2018'de dzenleyici erevenin onaylanması ile Blokzinciri ve benzeri yeni teknolojiler iin teřvik maddeleri, merkezi olmayan banka ve borsaların tercih edebileceđi ilk yer olarak grlmesi sađlanmıřtır. Byk lkelre kıyasla kk lkeler hızla deđiřen dnyaya

adaptasyonda belirgin bir avantaja sahiptir ve Estonya, Blokzincir uygulamalarına uyum sağlama konusunda mükemmel bir örnek oluşturmaktadır. Dubai hükümeti yapay zekâ ve ileri teknoloji konusunda gereken yatırımın yapılmasına öncelik tanımış olup yeni teknolojilerin benimsenmesi ve uygulanması amacıyla bir bakanlık kurmuştur. Fatura ödeme, lisans yenileme ve vize başvurularının kolay ve hızlı gerçekleştirilmesi için tamamen Blokzincir’de depolanan veriler ile kâğıtsız sisteme geçmeyi planlamaktadır. Dubai bu girişimi ile yıllık 1,5 milyar dolara kadar artırım sağlamayı amaçlamaktadır (Türkmen ve Durbilmez, 2019: 37-38).

Dünyanın dört bir yanındaki bankalar ve finansal kurumlar, Blokzincir teknolojisini günlük operasyonlara dâhil etmeye çalışmaktadır. Dünya Ekonomik Forumu, fon transferi sırasında Blokzincir’in tüketicilerin ve tedarikçilerin doğrudan bağlantı kurmalarını, üçüncü taraflara duyulan ihtiyacı ortadan kaldırılmasını sağladığını” belirtmektedir (Hutt, 2016).

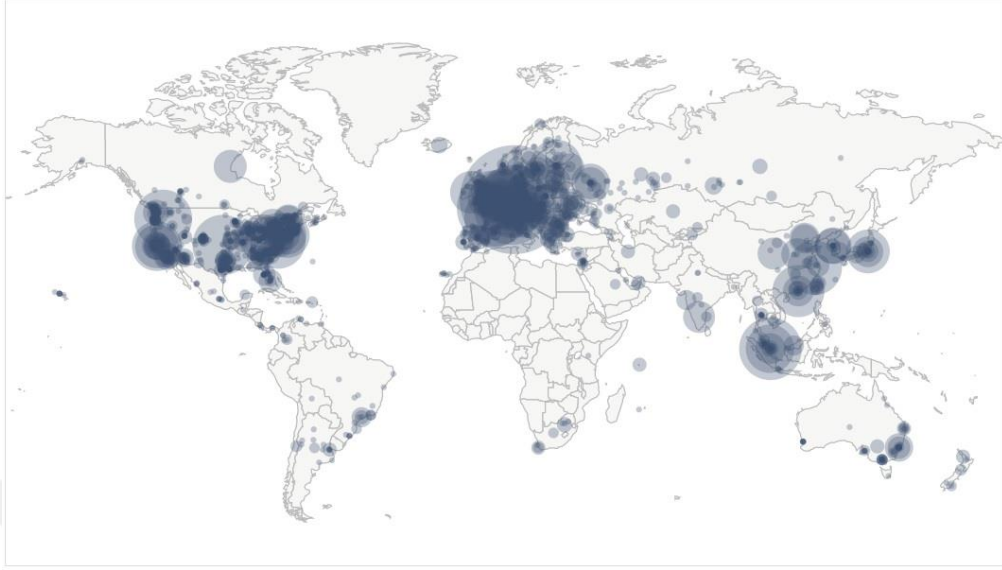
### **1.8.1. Kullanıldığı Sektörler**

Sağlık alanında hastaların medikal kayıtlarının tutulması, taraflar arasında güvenli bir şekilde transfer edilmesi, ilaç sahtekârlığının tespit edilmesi ve önlenmesi konularında bu teknolojiden faydalanmak mümkündür. Estonya hükümeti 2011 yılında Guardtime adlı bir proje başlatarak sağlık platformunu blokzincir teknolojisi üzerinde çalışır hale getirmiştir (Kırbaş, 2018: 81).

Dünya çapında içerdiği milyonlarca şarkı ve diğer içeriğe anında erişimi sağlayan bir dijital müzik, podcast ve video aktarma hizmeti veren Spotify 2017 yılında telif haklarını daha kolay denetleyebilmek için Blokzincir hizmeti sunan bir firmayı satın almıştır (McIntyre, 2017). Blokzincir teknolojisi, müzik endüstrisinin en sıcak konularından biridir. Çünkü CD satışlarından MP3 indirmelere geçiş yaptıktan sonra ve ardından içerikler yayımlandıkça, doğru kişilere telif ücreti ödemek için gereken trilyonlarca veri noktasını takip etmek zorlaşmaktadır.

Her bir elmasın sahiplik ve kaynağının takibi için bu altyapıyı kullanmayı tercih eden firmalar (Singapore Diamond Invest Exchange) olduğu gibi, değerli taşların alışverişi sırasında bir doğrulama sistemi oluşturmayı amaçlayan bir sistem geliştirmek için 2017 yılından itibaren Blokzincir altyapısını kullanmaktadır (Tian, 2017).

Finans sektörünün öncü kripto parası bitcoinin dünya üzerindeki Blokzincir ağındaki uçların dağılımı, sahip olduğu küresel ekonomik değeri göstermektedir:



Şekil 1.7. Küresel bitcoin Ağındaki Tam Uçlar (<https://bitnodes.earn.com>, 12.12.2019)

### KÜRESEL BITCOİN DÜĞÜMLERİNİN DAĞILIMI

**9399 DÜĞÜM**

*erişilebilir düğüm  
sayısına sahip ilk 10 ülke*

SIRALAMA	ÜLKE	DÜĞÜM
1	ABD	2463 (%26.20)
2	Almanya	1895 (%20.16)
3	Fransa	597 (%6.35)
4	Hollanda	495 (%5.27)
5	Birleşik Krallık	342 (%3.64)
6	Singapur	342 (%3.64)
7	Kanada	329 (%3.50)
8	Çin	292 (%3.11)
9	Rusya	213 (%2.27)
10	Diğer	192 (%2.04)

Şekil 1.8. Uçların Ükelere Göre Dağılımı (<https://bitnodes.earn.com>, 12.12.2019)

Amerika Birleşik Devletleri kökenli bir perakende şirketi<sup>7</sup> yiyeceklerin üretiminden

<sup>7</sup> Bu perakende şirketi WalMart olup, 2016 verilerine göre, mağazalar zincirinde büyük çoğunluğu Amerika'da olmak üzere 2,1 milyon insan çalışmaktadır ve dünya genelinde (27 ülkede) 10.000'den fazla mağazası

başlayıp işleyişi takip etmek için bir Blokzincir altyapısı kullanmaktadır.

Solar Change adlı bir güneş paneli firması, kullanımı artırmak için belli bir Megawatt elektrik üretimi karşılığı müşterilerine kendi adını verdiği coin olan SolarCoin adlı bir dijital para hediye etmektedir (Solarcoin, 2019). SolarCoin tıpkı bitcoin gibi çeşitli yerlerde kullanılabilir. SolarCoin'in vizyonu güneş enerjili bir gezegeni teşvik etmektir. SolarCoin, güneş enerjisi üreticilerini enerji referanslı bir para birimi ile ödüllendirerek küresel enerji geçişinin temellerini atmaya yardımcı olmaktadır.

UNICEF (Birleşmiş Milletler Çocuklara Yardım Fonu) 2019 Ekim ayında kripto para birimi fonu ile BTC ve ETH bağışlarını kabul etmeye başladığını duyurmuştur. Bu fonun ilk bağışçısı da Ethereum Vakfı olup 100 ETH (yaklaşık 18 bin dolar) bağışlamıştır. Bu gelişme, 1946 yılında kurulmuş olan UNICEF'in Blokzincir teknolojisini ilk keşfettiği an olmayıp, 2018 Aralık ayında 6 Blokzincir girişimine destek vermeye başlamıştır. Bu girişimler dâhilinde sağlık hizmetleri ve mali kaynakları yönetme sorunlarına çözüm aranmaktadır (UNICEF, 2019). Prescripto, reçeteleri güvence altına almaya ve izlemeye odaklanan; Surge, gençlerin yeni beceriler öğrenmesinde rol oynayan; Project Connect dünyadaki her okulu haritalamayı (internet bağlantı kalitesini değerlendirerek her toplum için bilgi ve fırsatlara erişimi) amaçlayan girişimleridir.

### **1.8.2. Avrupa Birliği Blokzincir Gözlemevi**

Göze çarpan en önemli özelliği merkezi olmayan bir doğrulama sistemi olan Blokzincir teknolojisi, bu yönüyle, dijital dönüşümün en net görüldüğü alanlardan biridir. Arsa, arazi, bina, apartman, iş yeri, konut, villa, fabrika ve benzeri taşınmazlar, araç ve değerli varlıkların kanıt ve kaydından doğum, evlilik ve ölüm belgelerinin kaydının tutulmasına, yerel ve genel seçimlerin gerçekleştirilmesi ve akıllı kontratların yönetilmesinden finansal dokümanların saklı tutulması, işlenmesi ve yönetilmesine kadar birçok değişik alanda bir dijital kayıt deposu olarak kullanımı mümkün olan bir teknolojidir. Dijital kimlik açısından bakılacak olursa Blokzincir teknolojisi ile benzersiz bir bireysel yapı sağlanmaktadır. Bu özelliği açısından bir *küresel açık hesap defteri* olarak da tanımlanabilir. Dijital kimlik yönüyle ortaya koyduğu bu yapı sayesinde güven ekonomisinin anahtarı konumunda yer almaktadır (Piscini, 2017).

---

bulunmaktadır. 2016 yılında 256 milyar dolar cirosu olduğu açıklanmıştır. Birçok ülkenin gayrisafi milli hasılası düşünülürse WalMart'ın şirketten öte bir devlet olarak nitelendirilmesi mümkündür.



Bu sebeple, Şubat 2018’de Avrupa Birliği Komisyonu Blokzincir teknolojilerinin araştırılması üzerine Blokzincir Observatory and Forum (Blokzincir Gözlemevi) isimli bir birim kurmuştur (ec.europa.eu, 2018-1). İki ayrı çalışma grubu burada aktiftir:

### 1. Blokzincir Politikası ve Çerçeve Koşullarında Çalışma Grubu

Bu grup, özellikle blokaj uygulamalarının daha geniş çaplı bir şekilde uygulanması için gerekli olan öngörülebilirliği ve yasal kesinliği teşvik etmek için gerekli olan politika, yasal ve düzenleyici koşulları oluşturmak için kesişen konulara bakmaktadır. Analiz, akıllı sözleşmelerden, kişisel verilerin korunmasından, tıkanıklıkların yasal olarak tanınmasından, belirteç ekonomisinden, özellikle de faydalı belirteçlerden oluşan konuları dikkate almaktadır. Çalışma grubu, birlikte çalışabilirlik, ölçeklenebilirlik ve sürdürülebilirlik, siber güvenlik ve enerji verimliliği gibi teknolojik ve ekosistem gelişmeleri ile ilgili konuları da tartışmaktadır.

### 2. Kullanım Durumları ve Geçiş Senaryoları Çalışma Grubu

Bu grup, özellikle kamu sektörü açısından (öncelikle sağlık hizmetleri, enerji veya çevresel raporlama dahil olmak üzere kimlik ve hükümet hizmetleri) ve geçiş senaryolarına (örneğin, eski sistem entegrasyonu) bakarak, gelecek vaat eden kullanım durumlarına odaklanmaktadır. Ayrıca Fintech ve mali hizmetler, tedarik zinciri, yaratıcı endüstriler veya kâr amacı gütmeyen sektördeki kullanım durumlarına da değinmektedir.

Blokzincir Observatory and Forum açılışına Avrupa Parlamentosu Milletvekili Jakob Von Weizsacker ve Dijital Ekonomi ve Toplum Avrupa Komisyonu üyesi Mariya Gabriel katılmıştır. Mariya Gabriel: *“Gelecekte, tüm kamu hizmetleri Blokzincir teknolojisini kullanacak. Blokzincir, Avrupa ve üye devletlerin bilgi sistemlerini yeniden düşünmeleri, kullanıcı güvenini ve kişisel verilerin korunmasını teşvik etmeleri, yeni iş fırsatları yaratmaları ve yeni liderlik alanları oluşturmak, vatandaşlara, kamu hizmetlerine ve şirketlere fayda sağlamak için bir fırsattır”* Avrupa Parlamentosu milletvekili Jakob Von Weizsacker: *“Potansiyeli görerek ve risklerle yüzleşerek bu oluşum ile bir uzmanlık yaratmayı umut ediyoruz.”* sözleriyle AB’nin dijitalleşme planını açıklamıştır (Euronews, 2018).

Blokzincir Ortaklık Bildirimi 22 AB üyesi ülke tarafından imzalanmış olup, 23 Mayıs 2018 tarihinde Yunanistan tarafından da imzalanmasıyla, ortaklıktaki ülke sayısı 23’e

çıkmiştir. Yapılan basın açıklamasında, Avrupa Komisyonu'nun Blokzincir ile ilgili projelerde 80 milyon €'dan fazla yatırım yaptığı ve 2020 yılına kadar Blokzincir'in geliştirilmesi için yaklaşık 300 milyon €'luk yatırım yapmayı hedeflediği belirtilmektedir (ec.europa.eu, 2018-2).

## 1.9. Türkiye'de Blokzincir Atılımları

Finans alanında Türkiye'deki ilk Blokzincir projesi Eylül 2018'de Borsa İstanbul (BİST) Bilişim Teknolojileri ekibi tarafından aktif edilmiştir. BİST resmi web sitesinde konuyla ilgili bir duyuru yayımlayarak, Müşterini Tanı = Know Your Customer (KYC) anlayışıyla tasarlanan bu projenin, yeni müşteri kayıtlarının tutulması ve verinin düzenlenmesi işlemlerinde Blokzincirin tercih edildiğini belirtmiştir (Borsaistanbul, 2018). Tercihin bu yönde yapılmasının ardındaki amaç, veri girişi problemlerinin önüne geçmek ve şeffaf, güvenilir, hızlı bir mimarinin oluşmasının sağlanmasıdır.

Blokzinciri okur yazarlığını yükseltmek ve konuyla ilgili olan, çalışma yapmak isteyen paydaşları tek bir noktada buluşturmak hedefiyle, Türkiye Bilişim Vakfı (TBV) liderliğinde ticari kaygılardan uzak bir çizgide ve bağımsız bir yapıda Blokzincir Türkiye Platformu (BCTR) 2018 yılında kurulmuştur (bctr.org, 2018). Blokzincir Türkiye Platformu'nun başlıca işbirlikçileri aşağıda gösterilmiştir:



Şekil 1.9. BCTR İş Birlikçileri (<https://bctr.org/is-birlikleri>, Erişim: 02.11.2019)

BCTR'nin misyonu, Türkiye'de sürdürülebilir Blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapma biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu olmaktır. Web sitesinde yayınlar, makaleler ve röportajlardan bir arşiv oluşturarak, çeşitli eğitimler ve etkinlikler düzenleyerek fayda sağlamaktadır.

BCTR Platformu iş birlikleri aracılığıyla üniversiteler, düşünce kuruluşları, bilim, sanayi ve teknoloji akademileri, diğer ülke ve birliklerin Blokzincir platform ve konsorsiyumları ile bir ekosistem ağı oluşturmayı hedeflemektedir. Takas İstanbul Blokzincir projelerinde kullanılan teknolojiler aşağıda gösterilmiştir:

	BiGA	DTS	Kitle Fonlaması	BES
Önyüz	ANGULARJS JBoss TRUFFLE	React	React	node Microsoft .NET
Geliştirme Dili	Java spring SOLIDITY Go	JavaScript Go	SOLIDITY	SOLIDITY
Blockchain Framework	HYPERLEDGER Quorum	Octa	ethereum	Quorum
Veritabanı	CouchDB docker PostgreSQL	PostgreSQL docker	docker	docker
AR-GE Odağı	Dijital Altın	Dijital Değer	Token ve ICO	Akıllı Kontrat Yönetimi
AR-GE Paydaşları	Fintech Şirketi - 1 ve TÜBİTAK	Fintech Şirketi - 2 ve TÜBİTAK	Fintech Şirketi - 3 ve TÜBİTAK	Fintech Şirketi - 4 ve TÜBİTAK

Şekil 1.10. Takas İstanbul Blokzincir Projelerinde Kullanılan Teknolojiler (Takasbank, 2018. “Blokzincir: Şehir Efsanesi mi Uygulaması Var mı?” Paneli, Türkiye Sermaye Piyasaları Kongresi, Kasım, İstanbul)

Marka adı BiGA (Bir Gram Altın) Dijital Altın olan AR-GE projesi Takas İstanbul’a ait olup hedeflenen başarı kriterleri kapsamında 2018 yılında başlanarak 2019’da tamamlanmıştır (Takasbank, 2019-1). BiGA, fiziksel dayanağı olan, regülasyona uyumlu, maksimum gizlilik ve güvenlik sağlayan blokzincir tabanlı altın transfer altyapı platformudur. BiGA projesi hakkında detaylı bir rapor hazırlanarak yayımlanmıştır (Takasbank, 2019-2).

Türkiye’nin Blokzincir teknolojisinde uluslararası ödüllü ilk şirketi<sup>8</sup> ile Türkiye’de fikri ve sınai mülkiyet hakları alanında sektör liderliğini koruyan bir firma arasında iş birliği protokolü 2018’in Nisan ayında imzalanmıştır. Yapılan işbirliği sayesinde artık proje ve eserlerin korunması için gereken yasal deliller, Türkiye ve dünyadaki mevzuatlarla uyumlu olarak elde edilmektedir. Türkiye’de 5070 sayılı kanuna uygun zaman damgası delili ve Avrupa Birliği’nde 910/2014 sayılı eIDAS yasasına uygun olup 28 AB ülkesinde geçerli yasal delillere sahip olmak mümkün kılınmıştır (www.destekpatent.com, 2019).

<sup>8</sup> Proofstack (eski adıyla Copyrobo).

### **1.9.1. TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi**

TÜBİTAK bünyesindeki Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM), ülkemizin ihtiyaçlarına yenilikçi ve milli çözümler üreten ulusal Ar-Ge merkezidir.

2010 yılında TÜBİTAK bünyesinde yer alan iki önemli enstitü - TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) ile daha önce TÜBİTAK Marmara Araştırma Merkezi'ne (MAM) bağlı olarak faaliyet gösteren Bilişim Teknolojileri Enstitüsü (BTE) - TÜBİTAK BİLGEM adı altında birleştirilmiştir.

Kamu ve özel kurum/kuruluşların ihtiyaçlarına istinaden, blokzincir teknolojilerinin altyapısı, kuruluşu, güvenlik ve mahremiyet analizi, iş modelleri, kitle fonlama yaklaşımları ve muhtelif teknik detayları üzerine Ar-Ge faaliyetlerini icra etmek üzere, BİLGEM UEKAE Matematiksel ve Hesaplamalı Bilimler Biriminin altında Blokzincir Araştırma Laboratuvarı (BCLabs) kurulmuştur.

### **1.9.2. Blokzincir Çalışmaları**

TÜBİTAK BİLGEM 1. Blokzincir Çalışmayı Ankara'da 2-3 Nisan 2018 tarihinde gerçekleştirilmiştir (TÜBİTAK, 2019-a). Kamu ve özel kurum/kuruluşların ihtiyaçlarına istinaden, blokzincir teknolojilerinin altyapısı, kuruluşu, güvenlik ve mahremiyet analizi, iş modelleri, kitle fonlama yaklaşımları ve muhtelif teknik detayları üzerine Ar-Ge faaliyetlerini icra etmek üzere, BİLGEM UEKAE altında Blokzincir Araştırma Laboratuvarı (BZLab) kurulmuştur (TÜBİTAK, 2019-b).

Blokzincir Araştırma Laboratuvarının ana görevleri şunlardır:

- Blokzincir ve dijital para konularında akademik açık literatürün takip edilmesi, katkı sunulması, pratik uygulamalarındaki teknolojik altyapıların incelenmesi ve analiz edilmesi
- Blokzincir ve dijital para teknolojilerinin güvenlik ve mahremiyet analizi
- İleri kriptografik yapıtaşlarının (Zero Knowledge Snark, Commitment, Dynamic Membership of Multi-party Signatures, Threshold Cryptography, Distributed Verification, Pairing-based Cryptography vb.) blokzincir teknolojisine tatbikatının araştırılması ve pratik uygulamalarda kavram analizlerinin yapılması Milli ve yerli blokzincir kuruluş kavram ispatı

- Ekonomik alanda ulusal çıkarlarımızı gözetmek adına risk analizlerinin çıkarılması
- Kitle fonlama (Crowdfunding, ICO) ve blokzincir tabanlı mikrofonlama / mikro ödeme sistemlerinin araştırılması
- Dijital paraların izlenebilirliği ve regülasyon altyapısı çalışması
- Eğitim/Danışmanlık
- Türkiye’de bilimsel düzeyde blokzincir çalıştayların yapılması
- İlgili kamu kurum/kuruluşlarına ve özel sektöre teknik destek sağlanması
- Blokzincir ve dijital para teknolojileriyle ilgili olarak akademik bitirme projeleri/yüksek lisans/doktora tezleri ile uluslararası literatüre katkı verilmesi

2. Ulusal Blokzincir Çalıştayında kamu kurum ve kuruluşları, özel sektör ve akademiye yaklaşık 800 katılımcı ve 21 davetli konuşmacı yer almış, 8 bildiri sunumu yapılmıştır (EK: 2). 246 kişiye bu kapsamda eğitim verilmiştir. Türkiye’de ilk defa bir workshopta blokzincir kodu yazdırılmıştır (TÜBİTAK, 2019-c).

Çalıştay BİLGEM tarafından 25-26 Eylül 2019 tarihlerinde İstanbul’da gerçekleştirilmiştir. Kamudan ve özel sektörden, profesyoneller, akademisyenler ve araştırmacıları blokzincir teknolojisindeki gelişmeleri değerlendirmek için bir araya getirmek hedeflenmiştir. “Blokzincirde Dijital Kimlik” ana temasıyla düzenlenen 2. Ulusal Blokzincir Çalıştayı bu kez blokzincir teknolojisinin vatandaşın hayatını nasıl değiştirebileceğini masaya yatırmıştır. “Kamu hizmetlerinden, belediye hizmetlerinden ya da özel kurumların sunduğu örgün hizmetlerden yararlanırken, vatandaşın veya tüzel kişilerin yaşadıkları süreçleri blokzincir teknolojisi ile hızlı ve güvenli hale getirmek mümkün müdür? Dijital dünyada vatandaşın mahremiyeti korunurken yönetime katılımı nasıl artırılır? gibi konular çalıştayın temasını oluşturmaktadır. Bunların yanı sıra devlet kontrollü paralar (stable coins), uzlaşma mekanizmaları (algorand, avalanche, elixir), pratik kullanım senaryoları (anket, ödüllendirme, ödeme) gibi sektörün gündeminde olan konularda uzmanlar davet edilmiştir (EK: 3).



Hakem kurulu tarafından deęerlendirilen ve 2. Ulusal Blokzincir alıřtayı'nda yer alan bildiri sunumlarına ve konferansın web sayfasına ulaşmak için yandaki karekod kullanılabilir. <https://easychair.org/cfp/BILGEM-BW2019>

BİLGEM, kamu ve özel kurum/kuruluşlar ile akademisyenlerle işbirliği yapmakta, güven merkezleri içeren yapılarıdaki güven merkezlerini dağıtarak daha verimli ve şeffaf yapıların kurulması için blokzincir tabanlı tasarım ve geliştirme çözümleri sunmaktadır.

Bu kapsamda, finansal hareketler, tedarik zincirleri, Nesnelerin İnterneti (IOT), risk yönetimi ve sağlık hizmetlerine kadar her türlü elektronik işlemi basitleştirmek ve güvence altına almak için ağlar kurulması üzerine çalışmaktadır. BİLGEM'in amacı, alanında en güçlü uzmanları bir araya getirerek işletmelerin blokzincir teknolojisini anlama ve kullanma becerilerini geliştirmek, bilimsel ve akademik çalışmalar yapmak, uygulamalı analizler gerçekleştirmek gibi aksiyonlarla ulusal çıkarları gözetmek ve teknolojik olarak katma değer sağlamaktır. Bununla beraber, Blokzincir alanındaki güvenlik ve gizlilik kavramlarının çalışılması, analizi gibi teknik çözümleri araştırmaktadır.

## 2. BÖLÜM

### 2. KRİPTOPARALAR VE BITCOIN

Kripto paralar, merkezi otoriteye ihtiyaç duymayan, dağıtık ve dijital bir para birimi olarak son yıllarda finans dünyasındaki popüler konuların başını çekmektedir. İlk ortaya çıktığı dönemlerde sanal paranın finansal özelliklerine duyulan ilgi, zaman içerisinde kripto paraya hayat veren Blokzinciri teknolojisine yönelmiştir. Uygulama alanlarını her geçen gün genişleten Blokzinciri teknolojisi konusunda akademik araştırmalar sınırlı sayıda olup henüz hızına yetişememiştir.

Kripto para birimlerinin ortaya çıkması ve paylaşım ekonomisinin gelişmesi, Blokzinciri kavramının bu yeni işletme paradigmasını beslemek için ideal bir teknoloji olduğunu göstermektedir. İşletmeler, kar maksimizasyonunu bir değer olarak görmektedir ve dijital para birimlerinde değer, kaynakların maksimize edilmesiyle elde edilmektedir. Yeni nesil liderler tarafından benimsenmesi gereken, yeni bir yol olarak Blokzincir dikkat çekmektedir (Kelly, 2015: 162).

Başta finans sektörü olmak üzere çeşitli sektörlerde kullanımına dair alt yapıyı oluşturmak adına IEEE ve ISO gibi kuruluşlar Blokzinciri teknolojisinin standardizasyonu alanında hazırlıklar yapmaktadır. Dünyanın önde gelen teknoloji yatırımcılarından Microsoft ve IBM, Blokzincir teknolojisini kullanmak isteyen firmalar için bulut tabanlı yapılar geliştirmiş ve firmaların kullanımına açmıştır. Tüm bu gelişmeler, bu yeni teknolojinin küresel formda rağbet gördüğünü, yaygınlaşmasının desteklendiğini, olumlu beklentilerin olduğunu ve bu yönde önemli yatırımlar yapıldığını göstermektedir. (Ünsal ve Kocaoğlu, 2018: 60).

#### 2.1. Bitcoinin Geçmişi

Kripto para birimleri arasında en popüler ve kullanımı en yaygın olan bitcoin (Sembolü ₿, kısaltması: BTC) olup, transferi ve güvencesi resmi veya özel bir kurum tarafından gerçekleştirilmemektedir (Sönmez, A., 2014, s.10). Merkez bankası veya devlet gibi merkezi bir otorite tarafından kontrol edilmediği gibi, geleneksel para birimlerinin altyapısından farklı olarak elektronik ortamda yönetilen bir para birimidir. Bitcoinin yarattığı ilk tetikleyici etki, işlemleri onaylama konusunda hiçbir güvenilir tarafa ihtiyaç duyulmamasından kaynaklanmaktadır. Bu özelliği ile kripto paraların, bilinen standart

paralarla karşılaştırıldığında en baskın özelliği P2P<sup>9</sup> teknolojisine dayanması ve tamamen dijital bir yapıya sahip olmasıdır. Bitcoinin piyasadaki kullanımı ve sirkülasyonunun artmasına bağlı olarak başta gelişmiş ülkeler olmak üzere artık ATM'leri (ATM<sup>10</sup>: Automatic Teller Machine) kurulmaktadır. Örneğin Japonya ve İrlanda'da ATM üzerinden işlem yapılabilmektedir. Dünyada ilk bitcoin ATM'si Kanada'da faaliyete geçmiş olup Türkiye'de ise sadece İstanbul'da hizmete sunulmuştur (Koin Bülteni, 2019-a).



Şekil 2.1. Bitcoin Sembol ve Logoları

Bitcoinin günlük hayata girmesiyle, güvenilir bir üçüncü taraf kullanılmadan, dijital varlıkların değerini ve sahipliğini aktarmak için bir çözüm olan “Blokzincir teknolojisi” (BCT) dikkat çekmeye başlamış ve tanınmıştır. En basit haliyle, Blokzinciri, belirli bir varlığın tüm işlemlerinin, kriptografik olarak zincirlenmiş veri bloklarında kaydedildiği, paylaşılan bir veritabanı olarak ifade edilmektedir. Sistem, ilgili taraf riskini ortadan kaldırmak için herhangi bir merkezi otorite veya herhangi bir güvenilir üçüncü taraf gerektirmemektedir. Bu teknolojideki daha fazla gelişme, ticari taraflar arasında sözleşmeye dayalı ilişkilerin güvenilir bir şekilde otomasyonunu mümkün kılan küçük programların (yani akıllı sözleşmelerin – smart contract) çalıştırılmasını sağlamıştır. İnternetin günlük hayata girmesiyle emsaller arasında bilgi alışverişine izin verilmiş olup, BCT ile değer değişimi mümkün kılınmıştır. Bu teknik devrimin sonucu olarak tüm endüstriler ve insan faaliyetleri için büyük fırsatlar yakalanmıştır. Öyle ki, örneğin, en büyük finansal hizmet şirketleri, daha hızlı ve daha güvenli bir sistem oluşturmak için BCT'yi bir mülkiyet ve işlem kaydı olarak kullanmayı planlamaktadır. Yapılan analizlere göre, bu yeni teknolojinin, bankaların 2022 yılına kadar sınır ötesi ödemelere, menkul kıymet alım satım işlemlerine ve mevzuata uygunluğa atfedilebilecek altyapı maliyetlerini yıllık 15-20 milyar dolar

<sup>9</sup> P2P (Peer to Peer - Eşten Eşe Bağlantı): Birbirine "eş" iki veya daha fazla istemci arasında haberleşmenin sağlanması, veri paylaşımı yapılmasını sağlamak amacıyla kullanılan bir ağ protokolüdür (<http://p2p.nedir.com/#ixzz3SzJACvQI>, Erişim: 07.03.2019).

<sup>10</sup> Dünyada ilk ATM cihazı İskoç kökenli Shepherd-Barron tarafından Barclays adlı banka için 1967 yılında Londra'da hizmete girmiş olup, Türkiye'de ilk kez 1982 yılında İşbankası tarafından Bankamatik adıyla duyurulmuştur.



azaltabilecektir (Santander InnoVenture, 2015). Şu anda, halihazırda 50'den fazla finansal kurum tarafından desteklenen ve bu alandaki en önde gelen iki şirket, New York merkezli bir Blokzincirleme teknolojisi olan R3 CEV ([www.r3cev.com](http://www.r3cev.com)) ve Ripple Labs (<https://ripple.com>) güvenli, hızlı ve neredeyse ücretsiz küresel finansal işlemler kurmayı hedeflemektedir. İş birliği ve finansman kesişiminde yer alan, özellikle lojistik ve tedarik zinciri yönetimi gibi alanlarda Blokzinciri uygulamalarından faydalanılması olası görülmektedir (Hofmann, 2018: 1).

Piyasaların anlık arz ve talep grafiği kripto paraların değerini belirlemektedir. Kripto paraların merkezi olmayan yapısal özelliği nedeniyle herhangi bir ülkenin ekonomik koşullarının piyasaya etkisi olmamaktadır; bu paraların tutulduğu dijital hesaplara el konulması veya hesapların dondurulması hiçbir şekilde mümkün değildir (Eğilmez, 2017).

Bitcoinin ilk bloğu olan *Genesis Bloğu* 3 Ocak 2009 tarihinde oluşturulmuş olup bu tarih tesadüf değildir (BTCTÜRK, 2019). 2008 yılında Yunanistan'da bir sabah halk bankadaki paralarını çekememiş, hiçbir resmi otorite veya banka da açılış tarihi verememiştir (BBC, 2015). 2008 yılında bu kriz sadece bu ülkede değildir, global bir kriz söz konusudur; tüm dünyada mevcut ekonomik ve politik sisteme karşı bir güvensizlik hakimdir. Bitcoin, dokuz sayfalık bir makale olarak 31 Ekim 2008'de Satoshi Nakamoto tarafından White Paper<sup>11</sup> olarak yayınlanarak dünyaya duyurulmuştur (BTCTÜRK, 2019). Hemen ardından Nakamoto'ya ait bitcoin cüzdanına 50 bitcoin transfer edilmesi ile Genesis bloğu üretilmiştir. Satoshi Nakamoto isminin gerçek kişi olup olmadığı bilinmemektedir (Eğilmez, 2013). Zaman içerisinde "Satoshi Nakamoto" olduğunu iddia eden bazı kişiler olmuş ancak gerçek kişinin kim olduğu veya gerçekte böyle bir kişinin varlığı henüz kanıtlanamamıştır. Bitcoin sistemini icat eden kişi 2011 yılının Nisan ayından sonra ortadan kaybolmuştur (Eğilmez, 2013). Buna rağmen oluşturmuş olduğu sistem matematik prensipleri ve şeffaflığı (Mancar, 2017) ile aktif olarak yürütülmeye devam etmektedir.

Nakamoto'nun açtığı yol, finansal sistem için bir iksir olma özelliği taşımaktadır. 2008 mali krizinden öğrenilen, tek bir başarısızlık noktasının tüm sistemi yok etme potansiyeline sahip olması durumudur. Nakamoto'nun mirası bu soruna bir çözüm bulmaktadır. Bitcoin ve Blokzincir kavramı, başarısızlık noktalarını azaltmanın ve finansal sistemi dağıtmanın zarif bir yolunu göstermektedir. Aktif kullanımı arttıkça bitcoinin

---

<sup>11</sup> White Paper: İlk Para Teklifi'nin (ICO) çözmek istediği bir problemin ana hatlarını, bu sorunun çözümünü, ürünlerinin ayrıntılı bir tanımını, mimarisini ve kullanıcılarla etkileşimini içeren bir belgedir.

sınırlarını keşfetmek mümkün olacaktır. Ancak, ademi merkezîyetçilik (decentralization) doğru yönde bir adım olarak görünmektedir. Victor Hugo'nun sözleriyle, “Vakti gelmiş bir fikri hiçbir şey durduramaz.” (Kelly, 2015: 47).

Satoshi Nakamoto'nun yapmış olduğu şey aslında *Bizanslı Generallerin Problemini* çözmektir ve onun zarif çözümü için bir “uzlaşma” gereklidir. *Bizanslı Generallerin Problemi* ilk olarak 1982 yılında bilgisayar bilimcileri Leslie Lamport, Robert Shostak ve Marshall Pease tarafından bir öneri olarak ortaya atılmıştır (Lamport, 1982: 382). Özünde, *Bizanslı Generallerinin Problemi*, güvenilemeyen bir iletişim ağı üzerinden ilişkisiz taraflar arasında güven kurmak sorunudur (Wang, W. 2018: 94). İnternet, ağa bağlanan herkese bilgiye erişim hakkı sağlamaktadır. Bu kendi içinde, insanlık tarihinde benzeri görülmemiş ve çok sayıda devrim başlatmıştır. İnsanlık tarihinde daha önce hiçbir zaman, kitle nüfusu, liderler ile aynı bilgilere erişememiştir. Ancak bilindiği üzere, herkes internete bilgi gönderebildiğinden, bu bilgi her zaman güvenilir bulunmamaktadır. Bitcoinden önce güvenilir bilgilerin, saygın medya kuruluşları ve devlet kurumları gibi üçüncü taraflarda merkezileştirilmesine ihtiyaç duyulmaktaydı. Elbette, bu üçüncü taraflar tek bir başarısızlık noktasını temsil etmekte olup, bazen görevlerini yerine getirmedikleri de görülmüştür. Aslında geçmişe bakıldığında, bu üçüncü tarafların bazıları zaman zaman kendi çıkarları için bilgileri manipüle etme güçlerini kullanmışlardır. *Bizanslı Generallerin Problemi* bilgisayar bilimcilerinin akıllarını 30 yıldan fazla bir süredir karıştırmış olup bitcoin'e kadar birçok kişi bu problemi düşünmüş, üzerinde çalışmış, lakin çözülememiştir (Kelly, 2015: 34). Bitcoin protokolü olarak adlandırılan Satoshi Nakamoto'nun çözümü, yalnızca internetin tüm kullanıcılarına bilgileri güvenli bir şekilde aktarmanın bir yolunu vermekle kalmamakta, aynı zamanda bilginin meşru olmasını da sağlamaktadır.

## 2.2. Bitcoin İşlem Süreci

1 BTC 8 basamağa kadar bölünebilmektedir. “Satoshi” (okunuşu: satoşi) olarak adlandırılan en küçük birimi ile 0,00000001 bitcoin'lik işlem yapılması mümkün kılınmıştır. Diğer bir ifade ile 100 milyon Satoshi 1 BTC etmektedir. Arkasında teknolojik bir altyapı olsa da piyasalardaki işleyişi açısından Euro ve Dolar gibi para birimlerinden bir farkı bulunmamaktadır; alışveriş yapılacak olan işyeri bitcoini kabul ediyor/tanıyor ise ürün veya hizmet alımı ve satımı yapılabilmektedir (Dilek, 2018: 14-16).

Kuramsal açıdan bakıldığında sistemin kullanımı karmaşık görünmemektedir. Bu durumda ilk olarak wallet olarak adlandırılan bir cüzdan programı üzerinde yeni bir hesap

tanımlanmalıdır. Cüzdan programı, kullanıcının bitcoinlerini tıpkı fiziki bir cüzdandaki gibi saklamakta ve dijital ortamda bu cüzdandaki paralar ile işlem yapılması olanağını sağlamaktadır. Standart bankacılık sistemindeki bir banka hesap cüzdanı gibi işlev gören bu dijital cüzdanlar, kimlik ve adres gibi hiçbir özel bilgiyi içermeyen, rakam ve harflerin bir araya gelmesiyle oluşturulmuş, metin formatında ifade edilen karışık bir dizedir. Hesabı olan herkes bitcoin satın alabilir ve transfer edebilir; bu işlemler belli bir bedel karşılığı olmadan birkaç dakika içinde ve çalışma saati kalıpları dışında olarak 7 gün 24 saat süresince gerçekleştirilebilir. Bitcoin Euro, Dolar, TL veya başka para birimlerine istenildiği zaman takas edilebilmektedir (Antonopoulos, 2014: 105).



Şekil 2.2. Kâğıt Cüzdan Örneği (Antonopoulos, 2014: 106)

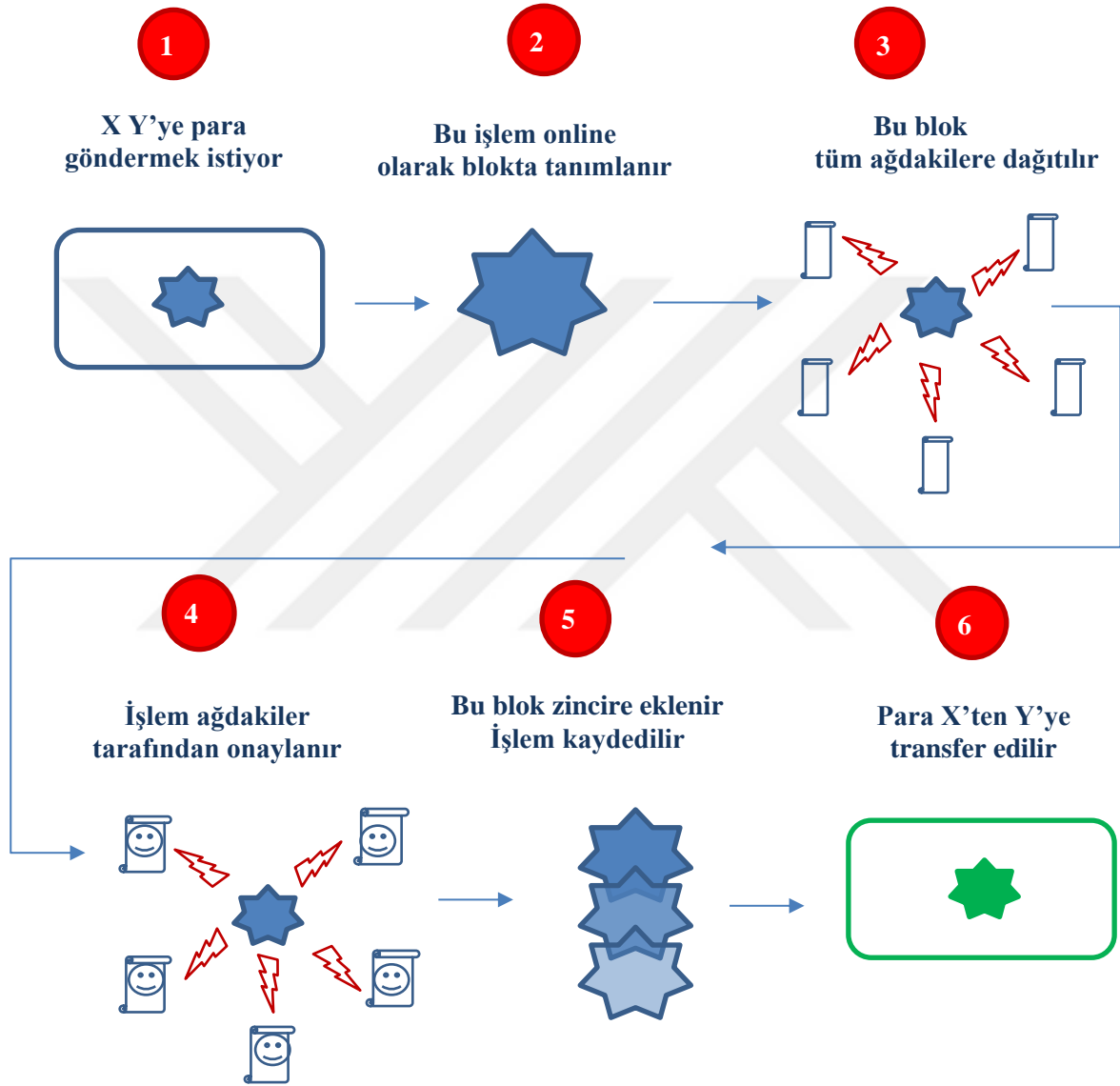
Hızlı ve küresel olduğu gibi şeffaf olması nedeniyle, şayet bir bitcoin cüzdan adresi biliniyorsa, bu hesaba ait bütün bitcoin işlemleri ağdaki dileyen herkes için görünür durumdadır (Çarkacıoğlu, 2016: 11-12; 16).

Geleneksel finans sektöründe çoğunlukla merkezi veya uçları birbirine tam bağlı dağıtık yapı kullanılmaktadır. Bankalar, VISA<sup>12</sup>, PayPal<sup>13</sup> ve aracı kurumlar gibi para transferi işlemlerinin gerçekleştirildiği bu sistemlerde merkezde yer alan sunucu bozulduğunda veya hacklendiğinde (ki bu riskler yüzden yüksek yedekleme maliyetleri mevcuttur) sistemin bütünü tehlikeye girmektedir. Diğer taraftan sunucuyu barındıran kuruluşa ait bir sistem güvenliği söz konusudur; ilgili kuruluşun iflas konumuna gelmesi veya aldatıcı işlemler yapması olasılığı da üstlenilmiş bir risk olmaktadır (Çarkacıoğlu, 2016: 12-13).

<sup>12</sup> Visa Inc., merkezi Foster, Kaliforniya, ABD'de bulunan bir Amerikan çok uluslu finansal hizmetler şirkettir. Dünya genelinde Visa markalı kredi kartları ve banka kartları aracılığıyla elektronik fon transferlerini kolaylaştırır (visa.com.tr, 02.07.2019).

<sup>13</sup> PayPal, internet üzerinde çalışan online bir ödeme sistemidir. Kredi kartı kullanarak internet üzerinden güvenli alışveriş yapılmasını ya da istenilen kişiye sadece bir e-posta adresi aracılığıyla para gönderilmesini sağlamaktadır. Haziran 2016 tarihinden itibaren Türkiye'deki faaliyetlerini durdurmuştur (www.paypal.com/tr/home, 02.07.2019).

Bitcoinin tasarlandığı altyapı olan Blokzincir ağı merkezi olmayan ve uçtan uca bağlı bir yapıdır. İçeriğinde bir sunucu yoktur, herhangi bir kontrol noktası içermemektedir. Geliştirildiği tabandaki bu yapısal özelliği nedeniyle BTC bir merkezden üretilmemekte, hiçbir otorite tarafından sisteme dışarıdan para arz edilememektedir (Gültekin Y. ve Bulut Y., 2016: 89).



Şekil 2.3. Bitcoin Çalışma Mantığı (Financial Times, 2015'ten esinlenerek çizilmiştir)

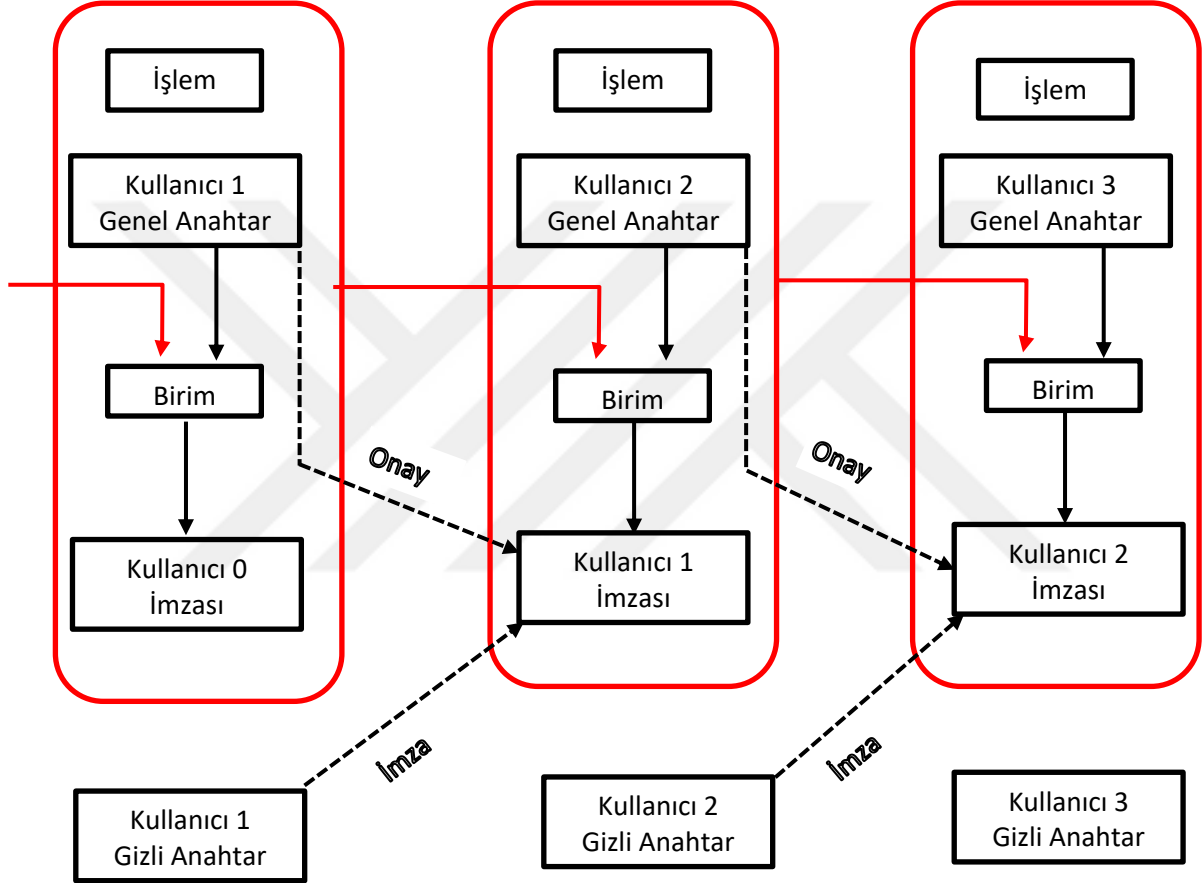
Bitcoin'le ilgili tüm işlem geçmişleri Blokzincir'de bulunmaktadır. Yeni bir işlem yapıldığında ise onaylanmış işlemler zincirinin sonuna eklenmektedir.

İşlemler, açık kaynak kodlu madenci yazılımını çalıştıran gönüllü bilgisayarın işlemci gücüyle yapılmaktadır. Çözüme ilk ulaşan madenciye ödül olarak bir miktar BTC

verilir. Algoritma gereği yaklaşık her dört yılda bir bu ödül oranı yarılanmaktadır. Sistemin doğru işlemesi durumunda 2140 yılına kadar bu yarılanmanın devam etmesi beklenmektedir (Antonopoulos, 2014: 2).

Algoritması gereği sistemde üretilecek olan maksimum bitcoin sayısı 21.000.000 ile sınırlanmış durumdadır (Dilek, 2018: 14).

Blokszincir'in işlem süreci Şekil 2.4'te verilmiştir.



Şekil 2.4. Bitcoin İşlem Süreci (Nakamoto, 2008: 2 esinlenerek çizilmiştir)

Bitcoin kullanıcılarına verilen isim “miner” (madenci), bu kullanıcıların onaylanmasını bekledikleri işlem süreçlerine verilen isim ise “mining”dir (Bitcoin Developer Guide, 2019). Bu süreç dâhilinde onaylanacak olan blok yapılar birikir ve oluşan karmaşıklığın çözülmesi konusunda madencilerin büyük işlemsel güç harcaması gerekmektedir. Bu aşamada blok yapısını ilk çözen kişi hem Blokszincir'in sonuna eklenir hem de ödül olarak blok başına tanımlanmış bitcoin kazanırlar.

Albert Einstein'in meşhur "Basit bir şekilde anlatamıyorsanız, konuyu tam olarak anlamamışsınız demektir." sözü baz alınarak bir bitcoin transfer işleminin basit şekilde açıklaması aşağıda yapılmıştır:

X isimli bir kişinin elinde 1 adet zeytin olduğu ve bu zeytini 1TL karşılığında Y isimli şahsa sattığı varsayalım. Y, fiziki olarak zeytini almış ve X de parasını almıştır. Artık X'in zeytini tekrar satmak gibi bir olanağı söz konusu değildir ve ticarete bunu kayıt altına alması gereken üçüncü bir kişiye ihtiyaç duyulmamaktadır.

Bu gerçekleşen ticaretin dijital versiyonuna bakılacak olursa, dijital formda yani bilgisayarda/internette bulunan bir zeytin çok güzel görünmekte ve sosyal platformlarda beğeni/like almaktadır; X isimli şahıs 1TL karşılığında bunu Y şahsına online satmıştır. Ancak fiziken mevcut olmasa dahi, aynı zamanda veya ertesi gün, aynı zeytini yine bir tuşa basarak Z ve T isimli şahıslara da satabilmektedir. Bunun önüne geçilmesi nasıl mümkündür? Borsaların işleyişi örnek teşkil etmektedir. Menkul kıymet, X'in bilgisayarında değil, merkezi bir takas bankta durmaktadır.

Dolayısıyla satış işlemi gerçekleştiğinde takas bank malı X'den çıkarıp Y'nin hesabına aktarmaktadır. Gerçekleşen satış işleminin tekrarlanma olanağı bulunmamaktadır, çünkü "merkezi" olarak gerçekleştirilmiştir. Bu merkezi senaryoda güvenilir birim bir devlet kurumu veya bir özel sektör şirketi olabilir. Bu gerçekleştirilen ticari işlemde araya üçüncü bir birimin girmesi maliyetin artması anlamına geldiği gibi, insan faktörünün devrede olması nedeniyle sahtekârlığa da yatkın olması söz konusu olabilir; istenirse zeytin eklenebilir.

Çizilen dijital senaryoda beklenen çözüm "herkesin" kayıt tutması ile sağlanabilmektedir. Herkese açık ve herkesin aynı anda güncellemesine uygun bir tablo (excel dosyası gibi -ledger-) mevcuttur. X şahsı elindeki zeytini 1TL'ye sattığında herkesin kayıtları güncellenecektir.

Daha sonra dijital ortamda zeytini tekrar satmaya kalktığında ise sistem artık X'in zeytinin sahibi olmadığını görecektir. Artık o zeytin, dijital ortamda olsa bile fiziki zeytin özelliklerini göstermektedir. Gerçekleşen ticari işlemde ise herhangi bir aracı birim yer almamaktadır. Bir para transferi işleminde bitcoin buradaki zeytin, bahsedilen "güncellenen kayıtlar zinciri" ise Blokzincir sistemidir.

Nakamoto'nun makalesinin yayınlanmasıyla başlayan sürecin “zaman çizelgesi” olarak aşağıda yer aldığı gibi basitçe ifade edilmesi mümkündür (Financial Times, 2015):

- 2008: “Bitcoin: Eşler Arası Elektronik Para Sistemi” adlı bir makale, Satoshi Nakamoto takma adı altında yayınlanmıştır.

- 2009: bitcoin açık kaynak kodlu bir zincirde çalışmaya başlamıştır.

- 2012: Para transferi için dijital para birimi ve Blokzinciri olan Ripple<sup>14</sup> piyasaya sürülmüştür.

- 2013: bitcoin fiyatı, 2011 yılında 0.31 \$ gibi düşük bir rekordan 1.242 \$ 'ya ulaşmıştır. ABD, bitcoin kullanan bir çevrimiçi pazar olan Silk Road'u kapatmıştır.

- 2014: Bankalar bitcoin ile kara para aklama riski konusunda uyarıda bulunmuştur. Dijital para borsası Mt Gox<sup>15</sup> çökmüştür, 480 milyon dolarlık müşteri mevduatının kayıp olduğu belirtilmiştir.

- 2015: Bankalar ve finansal kuruluşlar, kendi bünyelerinde izin verilen sistemlerde bitcoin ve Ripple kullanımı da dâhil olmak üzere Blokzincir teknolojisini test etmeye başlamıştır. Coinbase, ABD'de regülasyona tabi ilk borsa olarak 25 eyalette faaliyete geçmiştir.

- 2017: Japonya, bitcoini resmi ödeme yöntemi olarak kabul etmiştir. Çin, kripto para alım satım platformlarının kapatılacağını duyurmuştur. Chicago (CBOE) borsasında bitcoin vadeli işlemleri başlamıştır.

- 2018: Ocak ayında 16.800.000 BTC'in üretilmesiyle toplam bitcoinin %80'i üretilmiş durumdadır. Facebook, Google ve Twitter kripto para reklamlarını yasaklamıştır.

### **2.3. Güncel Haliyle Piyasalarda Bitcoin**

BTC ile ilk satın alma işleminin gerçekleştirilmesi 22 Mayıs 2010 yılını bulmuştur. Takma adı Laszlo Hanyecz olan bir kullanıcı online olarak Dominos'tan 2 adet pizza satın almış; karşılığında 10.000 BTC ödemiştir (Surda, 2014: 4). Tarihte ilk kez BTC'nin takas

---

<sup>14</sup> Akbank Ripple ile 2017'de anlaşarak Blokzincir alanında atılım yapan ilk Türk bankası olma özelliğini taşımaktadır: <https://www.akbank.com/tr-tr/Yatirimci-iliskileri/Sayfalar/Bizden-Haberler.aspx>

<sup>15</sup> 2014'ün başında, Japonya merkezli bir bitcoin borsası olan Mt Gox, dünyadaki tüm bitcoin işlemlerinin %70'inden fazlasını gerçekleştiren, dünyanın en büyük bitcoin borsasıdır.

aracı olarak kullanılması nedeniyle dünyanın birçok şehrinde 22 Mayıs tarihi “Laszlo'nun Pizza Günü” olarak kutlanmaktadır.

Tarihe bakıldığında binlerce yıldır para basımında altın ve gümüşün revaçta olduğu görülmektedir. Diğer elementler ile karşılaştırıldığında altın ve gümüşün erime noktası düşüktür, bu nedenle bozuk para, külçe ve takı haline dönüştürülmeleri daha kolay yapılmaktadır. Ancak gümüşün kararması sebebiyle altın daha çok tercih edilmiştir. Altın kalıcılığı, doğada nadir bulunuşu, kolay parçalara ayrılabilmesi gibi özellikleri göz önüne alındığında enflasyon ve ekonomik düzensizlikler için güvenli bir yatırım aracı olarak tercih edilmiştir. Çalkantılı bir piyasada, ana sermayeyi korumak ve kâr elde etmek üzere BTC kullanılabilir ve elle tutulur bir yatırım aracı olmadığı için foreks kontratlarına benzetilmektedir. Foreks piyasalarında işlemler 5/24 açıkken, bitcoin piyasalarında bu durum 7/24'tür. Günlük işlem hacmi açısından bakıldığında, foreks piyasası trilyonlarca amerikan doları, daha küçük ve yeni olan bitcoin piyasası ise 200 milyon amerikan doları gibi çok daha düşük düzeylerde seyretmektedir (Çarkacıoğlu, 2016: 20).

Tablo 2.1. Aralık 2016 ve Haziran 2019 için Karşılaştırmalı bitcoin Piyasa Değerleri

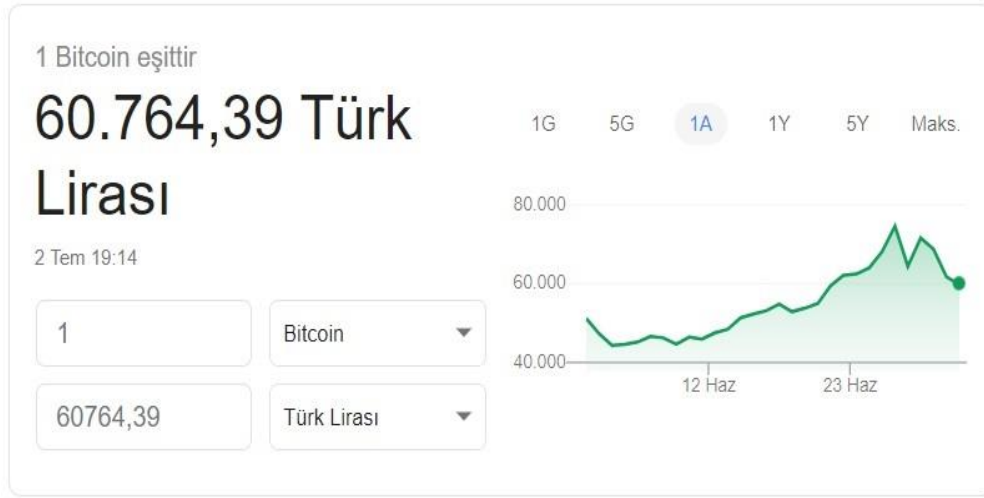
Değerler	2016 Aralık	2019 Haziran
<b>Piyasadaki Toplam BTC</b>	16.018.575 BTC	17.704.137 BTC
<b>1 BTC'nin Piyasa Fiyatı</b>	752 \$	10.800,75 \$
<b>Piyasa Değeri (Market Capitalization)</b>	12.069.035.148 \$	192.300.000.000 \$
<b>Günlük Ticaret Hacmi</b>	259.387 BTC	294.444,39 BTC
	195.432.628 \$	3.180.000.000 \$

Tablo 2.1'de 2016 yılı Aralık ayı değerleri (Çarkacıoğlu, 2016: 17) ile 2019 yılı Haziran ayı<sup>16</sup> değerleri kullanılarak piyasadaki yönelim incelenmiştir.

Bir kripto paranın gerçek hayatta kabul görüp kullanımda tercih edilmesi ancak ödeme aracı olarak kullanımının yaygınlaşması ile açıklanabilmektedir. Tablo 2.1'de verildiği üzere iki buçuk yıldaki ilerleme katsayısının ortalama 15 kat olduğu gözlenmiştir.

<sup>16</sup> Veriler <http://www.blockchain.info/charts> adresinden temin edilmiştir.





Şekil 2.5. Bitcoinin Türk Lirası Karşılığı (Temmuz 2019)

2 Temmuz 2019 tarihi itibariyle 1 BTC = 60.764,39 ₺'dir.

2019 yılı Eylül ayı sonlarında piyasalardaki bitcoin gerileme kaydetmeye başlamıştır:











Şekil 2.6. Bitcoinin Türk Lirası Karşılığı (Ekim 2019)

17 Ekim 2019 tarihi itibariyle 1 BTC = 47.076,59 ₺'dir. Eylül ayı sonlarında bitcoin hash rate'inin düşmesi sonucu sektörde ciddi bir dalgalanma olmuştur. Düşüşün nedenlerinden biri sürekli artan yüksek enerji maliyetleri olup, Çin hükümetinin indirimli elektrik kullanımını Eylül itibariyle kaldırmasıdır. Çarkacıoğlu'nun 2016 yılında yaptığı çalışmasında yazdığı üzere Çin'de elektriğin ucuz olması, pek çok madencinin Çin'de olmasına sebep olmaktadır. ABD'deki finans otoritelerinin de aynı tarihlerde yaptıkları kripto para karşıtı (Facebook'un Libra'sı ardından gelen yankılar) açıklamalar etkili olmuştur. Genel bir kural olarak, piyasada büyük miktarda bitcoin satıldığında, satış baskısı

arttığından bitcoinin fiyatını düşürmektedir.

Tablo 2.2. Bitcoinin Serbest Piyasadaki Karşılıkları (2 Temmuz 2019)

 DOLAR 10 889.0	 EURO 9 643.95	 POUND 8 642.20	 JAPON YENİ 1 174 651.57
 TÜRK LİRASI 60 764.39	 İSVİÇRE FRANGI 10 734.97	 SUUDİ ARABİSTAN RİYALİ 38 470.21	 AVUSTRALYA DOLARI 15 583.62

Bitcoinin kur değerleri bir kaç ülke için Tablo 2.2’te verilmiştir. Kur değerleri belli bir zaman dilimi içerisinde incelendiğinde inişler ve çıkışlar göze çarpmaktadır. Bu hareketliliğin sebebi diğer para birimlerindeki değer-kayıp durumları, teknolojik başarısızlık, ülkenin siyasal ve politik durumu, ülkenin kripto para birimlerine yönelik yasal düzenlemeler yapması veya bunlara benzer olağan piyasa hareketliliği olabilmektedir. Bitcoin hakkında medyada yayılan bir haber bu hareketliliği etkileyebileceği gibi maaş günü gibi insanların alım gücünün yüksek olduğu dönemler de etkindir (Cengiz, 2018: 95).

Tüm zamanların en yüksek BTC değeri 17 Aralık 2017 tarihinde 19.524,32\$ olarak tarihe geçmiştir (23.06.2019 itibariyle, kaynak: <https://www.Blokzincir.com/tr/prices>)

Kripto para piyasası hakimiyeti açısından 23.06.2019 tarihi itibariyle %58 BTC (1BTC = 10.800,75\$), %10 ETH (1ETH = 312,54\$) ve %6,2 XRP (1XRP = 0,48\$) ilk üç sırayı almaktadır. Aynı tarihte 1 BTC = 62.791,88₺ değerindedir (<https://coinmarketcap.com/tr/currencies/bitcoin-cash>).

Bitcoin borsaları (Bitcoin Market, Mt Gox gibi) 2010 yılında alım ve satım işlemleri için faaliyete geçmiştir. Oysa başlangıçta bitcoin sadece online gönüllüler ve hevesliler tarafından kullanılmaktadır. Günümüz finansal dünyasının parlayan yıldızları Amazon, PayPal, Tesla, Microsoft ve Dell gibi kuruluşlar bitcoini tanımakta ve ödeme aracı olarak kabul etmektedir (Dilek, 2018: 17). Bir pizza alımıyla başlayan yolculuğunun, zaman içerisinde iş dünyasında ödeme aracı olarak tercih edilmesi neticesinde, BTC borsaları piyasada yer almaya başlamıştır.

Küresel gelişmeler böyle devam ederken, Türkiye’nin finansal yaklaşımında ise BDDK (Bankacılık Düzenleme ve Denetleme Kurumu) ve SPK (Sermaye Piyasası Kurumu)

tarafından yapısı ve çalışma prensibi nedeniyle kripto paralar, kanun kapsamında “elektronik para” şeklinde kabul görmemektedir. TCMB (Türkiye Cumhuriyeti Merkez Bankası) tarafından finansal kararlılık ve süreklilik açısından faydasının incelenmesi amacıyla bitcoin yakından izlenmeye başlanmıştır. Bu amaçla, bahsi geçen bu kurumlar bir araya gelerek kripto paraların temelini oluşturan teknolojiyi ve bu teknolojinin dünyadaki uygulama alanlarını incelemek üzere Blokzincir Çalışma Grubu’nu oluşturduklarını duyurmuştur. TCMB resmî sitesinde 21 Kasım 2018 tarihinde yürürlüğe giren “100 Soruda Merkez Bankacılığı” dokümanında kripto para tanımına (TCMB, 2018: 64) yer vermiştir. Dokümanda, bir varlığın paranın temel fonksiyonlarını ne ölçüde yerine getirdiği kişiden kişiye ve zaman içerisinde değiştiğini belirtmiştir. Bu fonksiyonları yerine getirmesinin, bir varlığın yasal açıdan para olarak nitelendirileceği anlamına gelmediğini ifade etmiştir. Gelecekte bir gün, spekülasyondan uzak ve kararlı kripto paraların piyasada yer alması ve yaygınlığının yüksek olması olanak dışı olmamakla birlikte, günümüz koşulları altında kripto paraların para olarak kabul edilmesini uygun bulmamaktadır. Bu nedenle “kripto para” yerine “kripto varlık” terimi kullanımını önermektedir. Ülkemizde henüz kripto paranın işleyişine dair kanuni bir düzenleme yürürlükte değildir. Dönemin başbakan yardımcısı tarafından bitcoin finans tarihinin en büyük balonu olarak tanımlanmış, fiyatının birdenbire dibe vuracağı ve ardından yine birdenbire yükselişe geçebileceği gibi tutarsızlıklar göz önüne alındığında, en doğrusunun bitcoine mesafeli kalınması olduğu belirtilmiştir (Alptekin, 2017: 11).

Bitcoin hakkında yasal düzenlemeler hazırlayarak vergilendirilmesi konusunda, tüm dünyada olduğu gibi, Türkiye’de de tartışmalar yapılmaktadır. Bitcoinin merkezi olmayan yapısından dolayı sadece Türkiye’yi içeren bir vergilendirme sistemi bir kesime göre uygulamaya konulamaz; diğer bir kesime göre ise gerekli kanuni durum önce bir zeminde koşullandırılmalıdır ve ardından vergilendirilmesi sözkonusu olabilecektir. Kanada, Brezilya, Bulgaristan, Danimarka ve Finlandiya gibi ülkelerin bitcoin kullanımını yasal bir tabana oturtup ardından bunun vergilendirilmesi hususunda çalışmaları olmuştur. Singapur’a göre bitcoin tıpkı bir ürün gibi değerlendirilerek vergilendirilmiş, ülke içinde gerçekleştirilen bu alım satım işlemleri üzerinden katma değer vergisi tanımlanmıştır. Bir ülke ekonomisi açısından bitcoin bir tür gelir olduğundan şayet vergilendirilirse hükümetler buna karşı çıkmayacaklardır (Çarkacıoğlu, 2016: 56-59).

2017 yılının sonlarında dünya genelinde 61 ülke içerisinde toplam 1.963 adet ATM bitcoin hizmeti vermektedir ve 11.000’den fazla işletme bitcoini bir ödeme aracı olarak

işlemlerinde kullanmaktadır. Bitcoin dışında diğer bazı kriptoparalar ile de işlem yapılmasına olanak sağlayan bitcoin ATM'lerinin tümüne oranı %35 civarındadır. ABD bitcoin ATM'lerinin yaklaşık %60'ına ev sahipliği yapmaktadır. ABD'de 1.197, Kanada'da 316, İngiltere'de 104 ve Avusturya'da 94 ATM hizmet vermektedir. Avrupa ve Kuzey Amerika kıtalarında %96 gibi çok yüksek oranda bitcoin ATM'lerine yatırım yapılmışken Asya'da bu oran %2,4 civarında seyretmektedir (Dilek, 2018: 17-18).

Haziran 2019'da 4 olan Türkiye'deki coin ATM sayısı, Aralık 2019 tarihi itibarıyla 10 olup tümü İstanbul'da bulunmaktadır (Coinatmradar, 2019). ATM'lerin bazıları sadece alış işlemine açık olup, bazıları ise hem alış hem satışı izin vermektedir. ATM'lerde başta BTC olmak üzere BCH, ETH, LTC ve DASH işlem görmektedir.

Dilek (2018) verilerinin günümüz verileri ile karşılaştırması aşağıdaki tabloda yer almakta olup kripto paraların global gidişatı konusunda bu son iki yılın değerleri bir fikir vermektedir:































Tablo 2.3. Kripto Para ATM'lerinin Artışı (coinatmradar.com, Aralık 2019)

Tarih	Ülke Sayısı	ATM Sayısı	İşletme Sayısı	İlk 3 Ülke
Aralık 2017	61	1963	>11.000	ABD, Kanada, İngiltere
Aralık 2019	75	6217	148.884	ABD, Kanada, İngiltere

## 2.4. Kripto Paraların Piyasadaki Yeri

Gün geçtikçe daha çok ilgi çeken BC teknolojisinin en önemli kullanım alanı, kripto paralar ve özellikle bitcoin sayesinde "finans" olmuştur. 2019 yılı Nisan ayı itibarıyla dünya genelinde 2.140 tür kripto para çeşidi olduğu bilinmektedir. Kripto paraların güncel piyasa değeri 168.511.316.889 dolar olup 92.576.653.524 dolara yaklaşan piyasa değeri ile bitcoin bu değerlerin çok önemli bir kısmını oluşturmaktadır (<https://coinmarketcap.com/>, Nisan 2019). Bu haliyle BTC'nin piyasa hâkimiyeti %54,9'dur.

Tablo 2.4. Piyasa Değerine (Haziran 2019) Göre En İyi 30 Kripto Para Birimi  
Kaynak: <https://coinmarketcap.com>, 10.06.2019

Sıra No	Kripto Para Birimi	Piyasa Kapitalizasyonu	Güncel Değer	İşlem Hacmi (24 saat)	Değişim (24 saat)
1	 bitcoin	\$202.237.099.993	\$11.374,25	\$22.663.589.127	4,09%
2	 Ethereum	\$32.970.129.742	\$309,17	\$8.948.352.180	0,11%
3	 XRP	\$19.716.350.686	\$0,463188	\$1.796.917.168	0,40%
4	 bitcoin Cash	\$8.402.554.167	\$470,53	\$2.104.484.787	-0,10%
5	 Litecoin	\$8.281.753.396	\$132,74	\$4.067.025.568	-0,91%
6	 EOS	\$6.488.230.904	\$7,05	\$2.416.459.238	-1,29%
7	 Binance Coin	\$5.119.981.771	\$36,27	\$279.477.994	-2,18%
8	 bitcoin SV	\$4.201.846.498	\$235,33	\$465.253.238	0,66%
9	 Tether	\$3.528.355.475	\$0,997555	\$21.502.567.976	0,07%
10	 TRON	\$2.528.918.677	\$0,037925	\$971.563.915	-0,34%
11	 Cardano	\$2.455.973.535	\$0,094726	\$164.441.291	-1,66%
12	 Stellar	\$2.393.080.921	\$0,123274	\$477.355.398	-2,65%
13	 Monero	\$1.916.446.253	\$112,32	\$154.891.187	-4,13%
14	 UNUS SED LEO	\$1.898.018.557	\$1,90	\$7.246.385	0,87%
15	 Dash	\$1.560.312.937	\$175,63	\$312.531.034	-0,11%
16	 NEO	\$1.379.683.856	\$19,56	\$862.466.662	10,37%
17	 Cosmos	\$1.244.840.165	\$6,53	\$71.398.213	-0,84%
18	 IOTA	\$1.233.067.193	\$0,443624	\$25.678.719	-1,71%
19	 Ethereum Classic	\$1.010.183.357	\$9,06	\$725.721.538	-1,88%
20	 Ontology	\$855.064.842	\$1,73	\$240.866.890	10,22%
21	 NEM	\$813.683.232	\$0,090409	\$26.128.080	0,28%
22	 Chainlink	\$756.312.248	\$2,16	\$169.182.873	16,73%
23	 Maker	\$739.321.377	\$739,32	\$878.407	1,26%
24	 Tezos	\$716.273.384	\$1,09	\$7.556.092	-4,79%
25	 Zcash	\$714.286.734	\$104,53	\$344.521.264	-3,92%
26	 bitcoin Gold	\$545.377.986	\$31,14	\$17.753.705	2,65%
27	 Crypto.com Chain	\$531.149.785	\$0,072998	\$5.237.486	25,62%
28	 VeChain	\$508.615.422	\$0,009172	\$276.444.033	31,06%
29	 Qtum	\$501.802.651	\$5,24	\$518.977.014	25,53%
30	 Basic Attenti...	\$402.413.892	\$0,316573	\$38.842.704	-1,93%

Bankacılık sektöründe öncü uygulamalar, uluslararası ticaretin finansmanı ve uluslararası para transferi işlemlerinde geliştirilmektedir.

Türkiye’den bir bankanın da dahil olduğu Ripple, uluslararası para transferi çerçevesinde tercih edilen bir Blokzinciri çözümdür. Akbank, daha az maliyetle ve daha kısa sürede işlemlerin yapılmasını sağlayan Ripple platformu ile anlaşılan ilk Türk Bankası olmuştur. 2018 yılında teknolojik yeniliklerle müşterilerine çözüm yaratmak amacıyla Ripple iş birliği ve Blockchain altyapısı ile uluslararası para transferi gibi katma değeri yüksek, sektörde öncü projeler hayata geçirilmiştir (Akbank, 2019).

Türkiye’de basın yayın kuruluşlarında ve internette bitcoin hakkında çeşitli haberlerin çıkması üzerine BDDK 2013 yılında bitcoin Hakkında Basın Açıklaması (EK: 1) yapmıştır. BDDK’nın resmi sitesinde bitcoinin 6493 sayılı kanun kapsamındaki elektronik para olup olmadığına dair açıklama yapılmıştır (BDDK, 2019). Açıklamaya göre, herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen bitcoin, mevcut yapısı ve işleyişi itibarıyla kanun kapsamında elektronik para olarak değerlendirilmemekte, bu nedenle de kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir.

## **2.5. Libra**

Libra için 2019 yılı Haziran ayında yeni bir kripto paranın piyasaya sürülmesi konusunda hazırlıklar tamamlanmış olup, bir “white paper” (Libra, 2019-a) ile izahnameye dönüşerek yapısı resmîyet kazanmıştır.

Henüz sanal dünyada aktif olarak kullanıma açılmamış olan Libra’nın, günümüzde global en gelişmiş dijital kimlik sistemine sahip olan Facebook tarafından desteklenmiş olması, mevcut popüler kripto paralardan daha yaygın kullanım ağına sahip olacak izlenimi vermektedir (Coinmarketcap, 2019).



Şekil 2.7. Libra Birliği Üyeleri: Libra Ekosistemi (libra.org)

Şekil 2.7’de görüldüğü üzere Libra Birliği üyeleri, coğrafi olarak dağıtılmış çeşitli işletmelerden, kâr amacı gütmeyen ve çok taraflı kuruluşlardan ve akademik kurumlardan oluşacak biçimde organize olmuştur (Libra, 2019-b). Birlik üyeleri, çeşitli sektörlerdeki uzmanların katılımı ile finansal sektörle iş birliği yapmanın; sürdürülebilir, güvenli ve güvenilir yeni bir sistemin oluşmasında tek yol olduğuna inanarak bir araya gelmiştir. Hedefleri şu başlıklar altında toplanmaktadır:

1. Kişisel finansal varlıkların mobil cihazda güvence altına alınmanın basit ve rahat olması.
2. Parayı dünya çapında dolaştırmak, nerede yaşıyor olursa olsun, ne yapılırsa yapılsın, ne kadar kazanılırsa kazanılsın, bir kısa mesaj göndermek veya bir fotoğrafı paylaşmak kadar kolay ve uygun maliyetli olması.

Libra, tıpkı bitcoin ve Ethereum gibi, yazılım tabanı olarak Blokzincir üzerine inşa edilmiştir. Bitcoinde 7, Ethereum’da 15 olan saniyelik işlem kapasitesinin 1000 civarında olması beklenmektedir. Libra Birliği, İsviçre/Cenevre merkezli bağımsız, kâr amacı gütmeyen bir üyelik organizasyondur. Kripto para birimlerinin çoğunun aksine, Libra, tamamen gerçek varlık rezerviyle desteklenmektedir. Libra’nın içsel değerine güven oluşturmak üzere, yaratılan her bir Libra için Libra Rezervi’nde banka mevduatı ve kısa vadeli devlet tahvil sepeti tutulması planlanmaktadır. Libra altın yerine banka mevduatları ve istikrarlı, saygın merkez bankalarının para birimlerine endeksli, kısa vadeli devlet

tahvilleri gibi düşük volatiliteli varlıklardan oluşan bir sepet ile desteklenmektedir. Libra, tek bir para birimine “sabitlenmiş” değildir. İzahatnamesi yayınlanmış olan Libra henüz piyasaya sürülmemiş olup hedef çıkış tarihi 2020 yılının ilk yarısı olarak beklenmektedir. Kullanıcılar Libra işlemleri için Calibra dijital cüzdan hesabı açmak zorundadırlar (Calibra, 2019).

Libra'nın white paper yayınlamasının ardından yankılar devam etmiş ve Avrupa'da Fransa ve Almanya Facebook'un kripto parasını engelleyeceklerini bildirmişlerdir (Reuters, 2019). Yaptıkları ortak bildiri, “hiçbir ulusun, ulusların egemenliğine özgü bir parasal güç talep etmediğine” vurgu yapılmıştır.

2019 yılı Ekim ayında, PayPal Libra ekosisteminden çıkacağına dair açıklama yapmıştır (Feiner, 2019). Paypal, önceden birliğin 28 kurumsal destekçisinden biri olup, bazı ülkelerin gösterdiği tepkilerin sonuç bulması ile ayrıldığını duyurmuştur.

## **2.6. Literatür Taraması**

Kripto paralar her geçen yıl daha fazla ilgi görmekte ve buna bağlı olarak hakkındaki bilimsel yayınlar da artmaktadır. Dolaşımdaki standart para birimleri basılı bir şekilde fiziksel yapıdadır, kripto paralar ise sadece sanal ortamda (bir bilgisayar yazılımında kayıtlı) bulunmaktadır. Kripto paraların değeri, piyasada anlık oluşan arz ve talep durumuna göre şekillenmektedir. Bu paraların bulunduğu dijital hesaplara el konulması mümkün olmadığı gibi aynı zamanda hesaplar dondurulamamaktadır. Para arzı, iş kanıtı ve güçlü anonimlik gibi özellikleriyle birbirlerinden ayrılan altcoinlerin hiçbiri henüz bitcoin kadar yaygınlaşmamıştır (Cengiz, 2018: 90-94).

Türkiye'de her sektörün yenilikçi, araştırmacı ve uzman kişilerden oluşan bir ekibe olan ihtiyacı, Blokzincir'in daha iyi anlaşılması için gerekmektedir. Bununla birlikte kripto paraların popüler olmasıyla öne çıkan ve kripto para ile Blokzincirinin aynı şeymiş gibi algılanması nedeniyle Blokzincir'in itibarı düşmektedir, taşıdığı potansiyel yeterince anlaşılammaktadır (Türkmen ve Durbilmez, 2019: 42).

### **2.6.1. Akademik Çalışmalar**

Literatürde kripto paralara yönelik yapılan çalışmalar incelendiğinde araştırmaların bitcoin ve tasarımı üzerine yoğunlaştığı görülmektedir. Kripto para piyasasının yarısından



fazlasına hakim bir para birimi için bu olağan bir sonuç olarak karşılanabilir. BC ve BTC konusunda yapılan bilimsel çalışmalar incelenerek aşağıda sunulmuştur.

Ünsal ve Kocaoğlu (2018: 55) çalışmalarında popüler uluslararası akademik veri tabanlarında “Bitcoin” ve “Blokzincir” anahtar kelimelerini kullanarak bir tarama yapmışlardır. Mevcut yayınların çoğunlukla “Bitcoin” anahtar kelimesini içerdiği, “Blokchain” anahtar kelimesini içeren yayın sayısının ise azınlıkta olduğu gözlemlenmektedir (Tablo 2.5). Mart 2018 ve Nisan 2019 tarih aralığı baz alındığında, yaklaşık bir yıllık zaman dilimi içerisinde yayınlanmış akademik çalışmaların sayısında yükseliş olduğu açıktır.

Tablo 2.5. Bitcoin ve Blokzincir Alanındaki Akademik Çalışmalar

Veritabanı	Anahtar Kelimeye Göre Toplam Yayın/Sonuç Sayısı			
	Bitcoin		Blokzincir	
	Mart 2018	29.04.2019	Mart 2018	29.04.2019
Google Scholar	31.700	54.900	23.000	58.500
ScienceDirect	691	1.319	339	1.259
SpringerLink	1.386	2.906	991	3.248
JStor	180	463	52	227

Akademisyenler, çeşitli yazılım firmaları ve bağımsız yazılım geliştiriciler ülkemizde Blokzinciriyle ilgili çalışmalar yapmaktadır. Henüz gelişmekte olan bir teknoloji olarak uygulama alanları yaygınlaşmamış olup, süregelen araştırmalar daha çok teknik yapısının incelendiği ve kavramların açıklandığı çalışmalar olarak öne çıkmaktadır (Türkmen ve Durbilmez, 2019: 40).

Ülkemizdeki yayınlara bakıldığında yapılmış akademik çalışmaların fazla olmadığı söylenebilir. Yapılmış olan bu çalışmalar, dünya çapındaki yayınlarla uyumlu olarak, esas itibarıyla bitcoinin hukuki ve finansal statüsünü incelemektedir. Blokzincir teknolojisi, tıpkı benzer yeni teknolojilerin de karşılaştığı bir süreç olarak, sağlıklı bir yapıda gelişmek ve yaygınlaşmak için akademik yayınlarla desteklenmeye ihtiyaç duymaktadır.

Aralık 2019 itibarıyla Türkiye kaynakları incelendiğinde YÖK *Tez Merkezi* ve *DergiPark Akademik* üzerinde “Blokzincir” ve “Bitcoin” kelimeleri filtrelendiğinde aşağıdaki tablolarda yer alan sonuçlar gözlemlenmiştir.

Tablo 2.6. YÖK Tez Merkezi: Bitcoin ve Blokzincir Alanındaki Akademik Çalışmalar

Tür	Anahtar Kelimeye Göre Toplam Yayın/Sonuç Sayısı			
	Bitcoin		Blokzincir	
	Mart 2018	Aralık 2019	Mart 2018	Aralık 2019
Yüksek Lisans	7	26	9	46
Doktora	-	-	1	1

Tablo 2.7. Dergi Park Akademik: Bitcoin ve Blokzincir Alanındaki Akademik Çalışmalar

	Bitcoin	Blokzincir	
2019	34	32	66
2018	35	21	56
2017	5	-	5
2016	4	-	4
2013	1	-	1
	79	53	

### 2.6.2. Çalışmanın Literatürü

Antonopoulos (2014), çalışmasına teknik olmayan kullanıcılar, yatırımcılar ve şirket yöneticileri için bitcoini açıklamakla başlamış, daha sonra mühendisler ile yazılım ve sistem mimarları için bitcoin ve kriptografik para birimlerinin teknik temellerinin detaylarına girmiştir. Bitcoin yaşam döngüsünün ve güvenlik ilkelerinin ayrıntılarını vererek alternatif para birimlerini açıklamıştır.

Chaum (1992), çalışmasında meslektaşları ile birlikte CWI'de (Hollanda/Amsterdam'da finanse edilen Matematik ve Bilgisayar Bilimleri Merkezi) geliştirdikleri şifreleme tekniğinden bahsetmekte olup bu tekniğin güvenliğinin artması ve kayıt tutma maliyetlerinin düşürülmesinde etkin olduğundan bahsetmektedir. Dijital imzaların çalışma prensiplerini incelemiş, kullanıcıların iş yaptıkları her kuruluşa farklı ancak kesin olarak doğrulanabilir bir takma ad vermekte olduğundan bahsetmiştir. Dijital kimliklerin oluşturulması konusunda teknolojinin hızla ilerlediğine değinmiştir.

Çarkacıoğlu (2016), Sermaye Piyasası Kurulu için yapmış olduğu bitcoin araştırmasında paranın ilk nesne halinden sonraki elektronik kimliğine bürünmesine kadar geçen aşamayı anlatmıştır. Bitcoin madenciliği ve altında yatan teknik altyapı olan Blokzincir mimarisini incelemiş, kripto paraların yasal statüsüne değinmiştir. Kripto paraların dünya çapında yaygınlaşacağını öngörmüş ve Türkiye olarak bitcoin pazarında öne çıkmak için gerekli mevzuatın kısa sürede oluşturularak bir bitcoin borsasının kurulmasını önermiştir.

Dilek (2018), çalışmasına paranın dönüşümü ve dijitalleşme süreci ile başlamış, kripto paralar ve bitcoin madenciliği konusunda transferlerin yüksek maliyetlere ulaşan problemlerine değinmiştir. Kripto paraların alternatif para birimi olarak kullanılmasının tartışılmasıyla beraber, ulus devletin en önemli güçlerinden biri olan para basma tekeline bir meydan okuma olarak değerlendirmiştir.

Hofmann (2005), çalışmasında “İnternet +” isimli bir dönem tanımlayarak tüm endüstrilerin değişim geçirdiğinden bahsetmiştir. İnternet tedarik zinciri finansmanı da bu değişim sürecini hızlandırmaktadır. Hofmann’a göre Çin’de e-ticaret endüstrisinin büyük gelişimi nedeniyle, gittikçe daha fazla sayıda ticari işlem, çevrimdışıdan çevrimiçi durumuna geçmektedir. Farklı modellerin özelliklerini analiz ederek gelecekteki operasyonel mekanizma ve gelişme eğilimlerini özetlemiştir.

Kırbaş (2018), çalışmasında Blokzincir ile yapılan işlemlerde takip edilebilirlik, şeffaflık, geriye dönük düzeltme ve silme yapılamaması gibi özellikleri işlem güvenliğini artırıcı unsurlar olarak değerlendirmiştir. Kripto para birimi bitcoinin fikir olarak ortaya atıldığı 2008 yılından kendi çalışmasını yaptığı 2017 yılına kadar artan bu popülerliğinin altında yatan teknik detay olan Blokzinciri teknolojisini ele almış ve örnekler üzerinden geleneksel merkezi sistemlerden farklılıkları üzerinde durmuştur.

Murathan ve Murathan (2019), çalışmalarında spor sektöründe Blokzincir teknolojisinden nasıl yararlanılması gerektiğine değinmiştir. Spor organizasyonlarının kaydının tutulmasından piyasaya sahte ürün sürülememesine kadar geniş bir yelpazede bu teknolojinin kullanılmasının mümkün olduğu belirtilmiştir.

Mylrea (2017), çalışmasında Blokzincir tabanlı akıllı sözleşmeler sayesinde, üçüncü taraflarla etkileşime girme ihtiyacının ortadan kalkması, hem enerji akışlarının hem de finansal işlemlerin piyasa tarafından benimsenmesi ve para kazanılmasının

kolaylaştırmasını açıklamaktadır. Yazar, akıllı şebeke siber esnekliğini ve güvenli enerji uygulamalarını geliştirmek için Blokzincir ve akıllı sözleşmelerin uygulanmasını incelemiştir.

Nakamoto (2008), çalışmasında tamamıyla eşler arası elektronik para sürümünün mümkün olduğunu, çevrimiçi ödemelerin bir finans kuruluşundan geçmeden, doğrudan bir taraftan diğerine gönderilmesine olanak sağlayan dijital bir çözümün detaylarını vermektedir. Eşler arası dağıtılmış bir zaman damgası sunucusu kullanarak çift harcama sorununa bir çözüm önermiştir. Duyulan ihtiyaç nedeniyle gerçekleştirilen; herhangi bir istekli tarafın, güvenilir bir üçüncü tarafa ihtiyaç duymadan doğrudan birbirleriyle işlem yapmalarına olanak sağlayan, şifreleme kanıtına dayanan bir elektronik ödeme sisteminin teknik alt yapısı olan Blokzincir'i açıklamış ve dünyaya yeni bir teknoloji sunmuştur.

Özyılmaz (2014), çalışmasında şifreleme terminolojisi, klasik şifreleme teknikleri ve kriptografik algoritmalara yer vermiş olup şifrelemenin güvenilir bir iletişim için öncelikli koşul olduğunu vurgulamıştır.

Schollmeier (2001), çalışmasında eşler arası (peer-to-peer) ağ tanımını yaparak eşler arası ağ kavramına dayalı yeniden paylaşım ağları ve kaynak paylaşımı yapılarını açıklamıştır. Eşler arası ağ iletişiminin gerçek bir başarıya ulaşması için birçok sorunun çözülmesi gerektiğinden bahsetmiş, bunlardan birinin kesinlikle ağ içindeki trafik mühendisliği olduğunu belirtmiştir.

Wang (2018), çalışmasında mevcut Blokzinciri teknolojisinde karşılaşılan güvenilirlik ve güvenlik konularını ele almıştır. Sistem içerisinde veri kullanılabilirliği sorunları, sahte müşteri, sahtekârlık ve sıfır bilginin ispatı ile ilgili sorunları incelemektedir. Blokzinciri teknolojisinde ölçeklenebilirlik ve güvenlik açısından karşılaşılan sorunları tartışmaya açmıştır.

## 3. BÖLÜM

### 3. UYGULAMA VE ANALİZ

Çalışmanın bu bölümünde bitcoinin ekonomiyle arasındaki ilişkiyi ölçmek amaçlanmıştır. Mal ve hizmet alımından ziyade yatırım amaçlı kullanımı tercih edildiği için 2012-2020 dönemindeki hareketliliği incelenmiştir.

#### 3.1. Uygulamanın Amacı

Çalışmada bitcoinin ekonomik gösterge olarak cumhuriyet altını, altın ons fiyatı, ham petrol fiyatı, amerikan doları ve euro ile arasındaki istatistiksel ilişki incelenmiştir. Verilen bu değişkenler arasında olumlu ya da olumsuz bir doğrusal ilişkinin varlığını tespit etmek ve değerlendirmek amaçlanmıştır.

#### 3.2. Uygulamanın Kapsamı, Veri Seti ve Model

Çalışmada kullanılan veri setinin frekansı aylıktır. Dönem analizi için zaman aralığı Ocak 2012 ile Mart 2020 arası dönemi kapsamaktadır. Çalışmada kullanılan değişkenler aşağıda verilmiştir:

1. Bitcoin: Kripto para birimi olarak sektörün lideri bitcoin seçilmiştir.
2. Cumhuriyet altını: Darphane tarafından basılan bu altının, fiziki olarak saklanarak tasarrufta kullanımı Türkiye genelinde yaygın olduğu için tercih edilmiştir.
3. Altın ons fiyatı: Her koşulda satınalma gücünü koruyabilmesi, değer saklama aracı olarak tüm dünyada kabul edilmesi, siyasi ve ekonomik belirsizlik ortamında güvenilir olması nedeniyle altın stratejik önem taşımaktadır (Vural, 2003: i).
4. Ham petrol: Önemli bir hammadde oluşunun yanı sıra yatırım aracı olarak da piyasada bulunan petrol bu araştırmaya dahil edilmiştir.
5. Amerikan doları: Rezerv para olması, küresel çapta varlık fiyatlandırmasında tercih edilmesinden dolayı seçilmiştir.
6. Euro: Türkiye'nin coğrafi konumu itibarıyla yatırım amaçlı tercih edilmesinden dolayı seçilmiştir.

Verilerden cumhuriyet altını ve altın ons fiyatı TCMB (www.tcmb.gov.tr) Elektronik Veri Dağıtım Sistemi'nden (EVDS), ham petrol WTI vadeli işlem verileri www.investing.com veri tabanından ve bitcoin verileri www.statista.com adresli global veri platformundan temin edilmiştir.

Veri setlerinin her biri Ocak 2012-Mart 2020 yılları arasındaki aylara ait gözlemlerden oluşmaktadır; toplamda 99 adet gözlem içermektedir.

### 3.3. Metodoloji ve Yöntem

Korelasyon analizi, iki değişkene ait gözlem verilerinin birbirleriyle arasındaki değişim şeklini araştırmaktadır. Bu nedenle, serilerin gözlem değerlerinin akışı arasında benzerlik tespit edilirse, reelde ilişkisiz görünen bu seriler arasında güçlü bir korelasyon çıkması da mümkündür.

İki değişken arasındaki doğrusal ilişkinin derecesi korelasyon katsayısı ile ölçülmektedir. İki değişkenin birlikte değişme derecesini ölçmek amacıyla hesaplanan korelasyon katsayısına korelasyon katsayısı denilmekte ve “r” ile gösterilmektedir. Korelasyon katsayısı matematiksel olarak en küçük değer -1 ve en büyük değer +1 şeklinde olmaktadır. Eğer korelasyon katsayısı -1 ve +1'e eşit durumda ise, deterministik ilişki söz konusu olmaktadır ve iki değişken arasında mutlak kesinlikte bir ilişkiden söz edilmektedir. Korelasyon katsayısının pozitif değer alması, iki değişken arasında pozitif bir ilişki bulunduğunu ve iki değişkenin aynı yönde, birlikte artıp birlikte azaldığını ifade etmektedir. Korelasyon katsayısının negatif değer alması, iki değişken arasında negatif yönlü bir ilişki bulunduğunu ifade etmekte ve bu durumda değişkenlerden biri artarken diğerinin azalmakta olduğu anlaşılmaktadır. Korelasyon katsayısının sıfır çıkması durumu ise, söz konusu iki değişken arasında ilişki olmadığını değil, iki değişken arasında doğrusal bir ilişki bulunmadığını ifade etmektedir<sup>17</sup>. Korelasyon katsayısı r değerlendirilirken, şayet r değeri 0-0.49 arasında ise korelasyon zayıf, 0.5-0.74 arasında ise orta derecede, 0.75-1 arasında ise kuvvetli ilişki vardır olarak yorumlanmaktadır. Çeşitli korelasyon katsayıları istatistiksel hesaplamalarda kullanılmaktadır. Bunlardan bazıları; Spearman korelasyon katsayısı, Pearson korelasyon katsayısı, Canonical korelasyon katsayısı ve kısmi korelasyon katsayısı olarak ifade edilebilir. Çalışmada, kullanımı yaygın olan Spearman korelasyon katsayısı analizi tercih edilmiştir (Bulut, 2013: 145-146).

<sup>17</sup> Daha fazla bilgi için: Andersen, Bollerslev, Christoffersen ve Diebold (2007) Practical Volatility and Correlation Modeling for Financial Market Risk.

Değişkenlerin X ve Y olarak sembolize edilmesi durumunda, doğrudan gözlem değerleri kullanılarak aralarındaki korelasyon katsayısı aşağıdaki formül yardımıyla hesaplanmaktadır (Başer, 2012: 6).

$$r = \frac{\sum X_i Y_i - n\bar{X}\bar{Y}}{\sqrt{(\sum X_i^2 - n\bar{X}^2)(\sum Y_i^2 - n\bar{Y}^2)}}$$

Formülde yer alan;

$\bar{X}$  : X serisinin ortalamasını,

$\bar{Y}$  : Y serisinin ortalamasını ve

n : gözlem sayısını ifade etmektedir.

Bu çalışmada analiz için IBM SPSS Statistics 25 kullanılmıştır.

### 3.4. Uygulama Bulguları

Yapılan uygulamada, bitcoinin takas ve yatırım aracı olarak kendini göstermeye başladığı 2012 yılı baz alınmıştır. Ocak 2012 itibariyle 1 BTC=5,59 \$'dır.

2012 ve takip eden her yıla ait değişkenler arası korelasyonları içeren tablolar ardarda sıralanmış ve değerlendirilmiştir. Tablo 3.1'deki korelasyon tablosu, değişkenler arasındaki uzun dönem (2012-2020) ilişkiyi göstermektedir. Ocak 2012 – Mart 2020 dönemindeki istatistiksel ilişki değerlendirildiğinde aşağıdaki sonuçlara ulaşılmıştır.

Yapılan analizlerinin sonucuna göre piyasalarda yer edinmeye başladığı ilk dönem olan 2012'de bitcoinin diğer göstergelerle arasında istatistiksel olarak anlamlı bir ilişkisi saptanmamıştır ( $p>0.05$ ). Bitcoinin dolar karşılığının bir önceki yıla göre üç katından fazla arttığı 2017 yılı ise bitcoinin zirve yılı olup; euro ile arasında pozitif yönlü kuvvetli bir ilişki tespit edilmiştir ( $r=0.873$ ;  $p<0.001$ ).

Bitcoinin cumhuriyet altını, altın ons fiyatı, dolar ve euro ile arasında kuvvetli bir ilişki vardır ve bu ilişki anlamlıdır. Ancak ham petrol fiyatı ile negatif ve zayıf bir ilişkisi olduğu saptanmıştır.

Tablo 3.1. Korelasyon Tablosu: Ocak 2012 – Mart 2020

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	,784**	,787**	-,336**	,898**	,921**
	Anlamlılık (p)	.	,000	,000	,001	,000	,000
	Gözlem Sayısı	99	99	99	99	99	99
Cumhuriyet Altını	Korelasyon Katsayısı	,784**	1,000	,999**	-,519**	,904**	,896**
	Anlamlılık (p)	,000	.	,000	,000	,000	,000
	Gözlem Sayısı	99	99	99	99	99	99
Altın Ons	Korelasyon Katsayısı	,787**	,999**	1,000	-,526**	,909**	,900**
	Anlamlılık (p)	,000	,000	.	,000	,000	,000
	Gözlem Sayısı	99	99	99	99	99	99
Ham Petrol	Korelasyon Katsayısı	-,336**	-,519**	-,526**	1,000	-,555**	-,491**
	Anlamlılık (p)	,001	,000	,000	.	,000	,000
	Gözlem Sayısı	99	99	99	99	99	99
Amerikan Doları	Korelasyon Katsayısı	,898**	,904**	,909**	-,555**	1,000	,984**
	Anlamlılık (p)	,000	,000	,000	,000	.	,000
	Gözlem Sayısı	99	99	99	99	99	99
Euro	Korelasyon Katsayısı	,921**	,896**	,900**	-,491**	,984**	1,000
	Anlamlılık (p)	,000	,000	,000	,001	,000	.
	Gözlem Sayısı	99	99	99	99	99	99

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin cumhuriyet altını, altın ons fiyatı, dolar ve euro ile arasında istatistiksel olarak anlamlı, pozitif yönlü ve kuvvetli bir ilişki vardır (r değerleri sırasıyla 0,784; 0,787; 0,898 ve 0,921). Ancak ham petrol fiyatı ile negatif yönlü ve zayıf bir ilişkisi olduğu saptanmıştır (r= -0,336).



Tablo 3.2. Korelasyon Tablosu: Ocak – Aralık 2012

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	,375	,308	-,487	,047	-,380
	Anlamlılık (p)	.	,229	,330	,108	,884	,224
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	,375	1,000	,991**	,221	-,292	,360
	Anlamlılık (p)	,229	.	,000	,491	,358	,250
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	,308	,991**	1,000	,252	-,291	,365
	Anlamlılık (p)	,330	,000	.	,430	,359	,243
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	-,487	,221	,252	1,000	-,597*	,470
	Anlamlılık (p)	,108	,491	,430	.	,040	,123
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	,047	-,292	-,291	-,597*	1,000	-,064
	Anlamlılık (p)	,884	,358	,359	,040	.	,844
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	-,380	,360	,365	,470	-,064	1,000
	Anlamlılık (p)	,224	,250	,243	,123	,844	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin tablodaki ekonomik göstergelerle arasında istatistiksel olarak anlamlı bir ilişkisi saptanmamıştır ( $p>0.05$ ).

Tablo 3.3. Korelasyon Tablosu: Ocak – Aralık 2013

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	-,483	-,503	-,077	,762**	,637*
	Anlamlılık (p)	.	,112	,095	,812	,004	,026
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	-,483	1,000	,965**	-,133	-,678*	-,609*
	Anlamlılık (p)	,112	.	,000	,681	,015	,035
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	-,503	,965**	1,000	-,112	-,594*	-,511
	Anlamlılık (p)	,095	,000	.	,729	,042	,089
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	-,077	-,133	-,112	1,000	,315	,270
	Anlamlılık (p)	,812	,681	,729	.	,319	,397
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	,762**	-,678*	-,594*	,315	1,000	,928**
	Anlamlılık (p)	,004	,015	,042	,319	.	,000
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	,637*	-,609*	-,511	,270	,928**	1,000
	Anlamlılık (p)	,026	,035	,089	,397	,000	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin cumhuriyet altını ve altın ons fiyatı ile arasında negatif ve zayıf ( $r = -0,483$  ve  $-r = 0,503$ ), dolar ile pozitif ve güçlü ( $r = 0,762$ ) euro ile pozitif ve orta kuvvette ilişkisi ( $r = 0,637$ ) olduğu görülmektedir. Bunun yanında bitcoin ile ham petrol arasında istatistiksel olarak anlamlı bir ilişki yoktur ( $p > 0,05$ ).

Tablo 3.4. Korelasyon Tablosu: Ocak – Aralık 2014

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	,217	,187	,755**	-,677*	,623*
	Anlamlılık (p)	.	,499	,556	,005	,016	,031
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	,217	1,000	,956**	,308	,021	,783**
	Anlamlılık (p)	,499	.	,000	,331	,948	,003
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	,189	,956**	1,000	,172	,106	,734**
	Anlamlılık (p)	,556	,000	.	,594	,743	,007
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	,755**	,308	,172	1,000	-,723**	,673*
	Anlamlılık (p)	,005	,331	,594	.	,008	,017
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	-,677*	,021	,106	-,723**	1,000	-,284
	Anlamlılık (p)	,016	,948	,743	,008	.	,372
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	,623*	,783**	,734**	,673*	-,284	1,000
	Anlamlılık (p)	,031	,003	,007	,017	,372	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin ve dolar ile arasında negatif ve orta kuvvette ( $r = -0,677$ ), euro ile pozitif ve orta kuvvette ( $r = 0,623$ ), ham petrol fiyatı ile pozitif ve güçlü ( $r = 0,755$ ) cumhuriyet altını ve altın ons fiyatı ile pozitif ve zayıf ( $r = 0,217$  ve  $r = 0,189$ ) ilişkisi olduğu görülmektedir.

Tablo 3.5. Korelasyon Tablosu: Ocak – Aralık 2015

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	,126	-,021	-,608*	,480	,413
	Anlamlılık (p)	.	,696	,948	,036	,114	,183
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	,126	1,000	,974**	-,137	,807**	,830**
	Anlamlılık (p)	,696	.	,000	,672	,002	,001
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	-,021	,974**	1,000	-,028	,743**	,769**
	Anlamlılık (p)	,948	,000	.	,931	,006	,003
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	-,608*	-,137	-,028	1,000	-,620*	-,573
	Anlamlılık (p)	,036	,672	,931	.	,032	,051
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	,480	,807**	,743**	-,620*	1,000	,991**
	Anlamlılık (p)	,114	,002	,006	,032	.	,000
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	,413	,830**	,769**	-,573	,991**	1,000
	Anlamlılık (p)	,183	,001	,003	,051	,000	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin cumhuriyet altını, dolar ve euro ile arasında pozitif ve zayıf ( $r$  değerleri sırasıyla 0,126; 0,480 ve 0,413), ham petrol fiyatı ile negatif ve güçlü ( $r = -0,608$ ) ilişkisi olduğu görülmektedir. Ancak bitcoin ile altın ons fiyatı arasında istatistiksel olarak anlamlı bir ilişki yoktur ( $p > 0,05$ ).

Tablo 3.6. Korelasyon Tablosu: Ocak – Aralık 2016

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	,746**	,804**	,797**	,578*	,840**
	Anlamlılık (p)	.	,001	,002	,002	,049	,001
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	,846**	1,000	,986**	,685*	,655*	,882**
	Anlamlılık (p)	,001	.	,000	,014	,021	,000
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	,804**	,986**	1,000	,671*	,634*	,865**
	Anlamlılık (p)	,002	,000	.	,017	,027	,000
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	,797**	,685*	,671*	1,000	,0333	,738**
	Anlamlılık (p)	,002	,014	,017	.	,291	,006
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	,578*	,655*	,634*	,333	1,000	,805**
	Anlamlılık (p)	,049	,021	,027	,291	.	,002
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	,840**	,882**	,865**	,738**	,805**	1,000
	Anlamlılık (p)	,001	,000	,000	,006	,002	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin cumhuriyet altını, altın ons fiyatı, ham petrol fiyatı ve euro ile pozitif ve kuvvetli ( $r$  değerleri sırasıyla 0,846; 0,804; 0,797 ve 0,840) ilişkisi olduğu görülmektedir. Bununla beraber bitcoin ile dolar arasında pozitif yönlü orta kuvvette bir ilişki vardır ( $r=0,578$ ).

Tablo 3.7. Korelasyon Tablosu: Ocak – Aralık 2017

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	,545	,476	,301	,004	,873**
	Anlamlılık (p)	.	,067	,118	,342	,991	,000
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	,545	1,000	,972**	,664*	,446	,438
	Anlamlılık (p)	,067	.	,000	,018	,147	,154
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	,476	,972**	1,000	,741**	,540	,459
	Anlamlılık (p)	,118	,000	.	,006	,070	,133
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	,301	,664*	,741**	1,000	,786**	,509
	Anlamlılık (p)	,342	,018	,006	.	,002	,091
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	,004	,446	,540	,786**	1,000	,195
	Anlamlılık (p)	,991	,147	,070	,002	.	,544
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	,873**	,438	,459	,509	,195	1,000
	Anlamlılık (p)	,000	,154	,133	,091	,544	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin cumhuriyet altını, altın ons fiyatı, ham petrol fiyatı ve dolar ile arasında istatistiksel olarak anlamlı bir ilişki bulunmamaktadır ( $p>0,05$ ).

Euro ile arasında pozitif yönlü kuvvetli bir ilişki vardır ( $r=0.873$ ;  $p<0.001$ ).

Tablo 3.8. Korelasyon Tablosu: Ocak – Aralık 2018

Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	-,664*	-,664*	,112	-,690*	-,685*
	Anlamlılık (p)	.	,018	,018	,729	,013	,014
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	-,664*	1,000	1,000**	,329	,984**	,986**
	Anlamlılık (p)	,018	.	.	,297	,000	,000
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	-,664*	1,000**	1,000	,329	,984**	,986**
	Anlamlılık (p)	,018	.	.	,297	,000	,000
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	,112	,329	,329	1,000	,312	,308
	Anlamlılık (p)	,729	,297	,297	.	,324	,331
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	-,690*	,984**	,984**	,312	1,000	,998**
	Anlamlılık (p)	,013	,000	,000	,324	.	,000
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	-,685*	,986*	,986*	,308	,998**	1,000
	Anlamlılık (p)	,014	,000	,000	,331	,000	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin cumhuriyet altını, altın ons fiyatı, dolar ve euro ile arasında negatif ve güçlü (r değerleri sırasıyla -0,664; -0,664; -0,690 ve -0,685) ilişki varken ham petrol fiyatı ile anlamlı bir ilişki yoktur ( $p>0,05$ ).

Tablo 3.9. Korelasyon Tablosu: Ocak – Aralık 2019

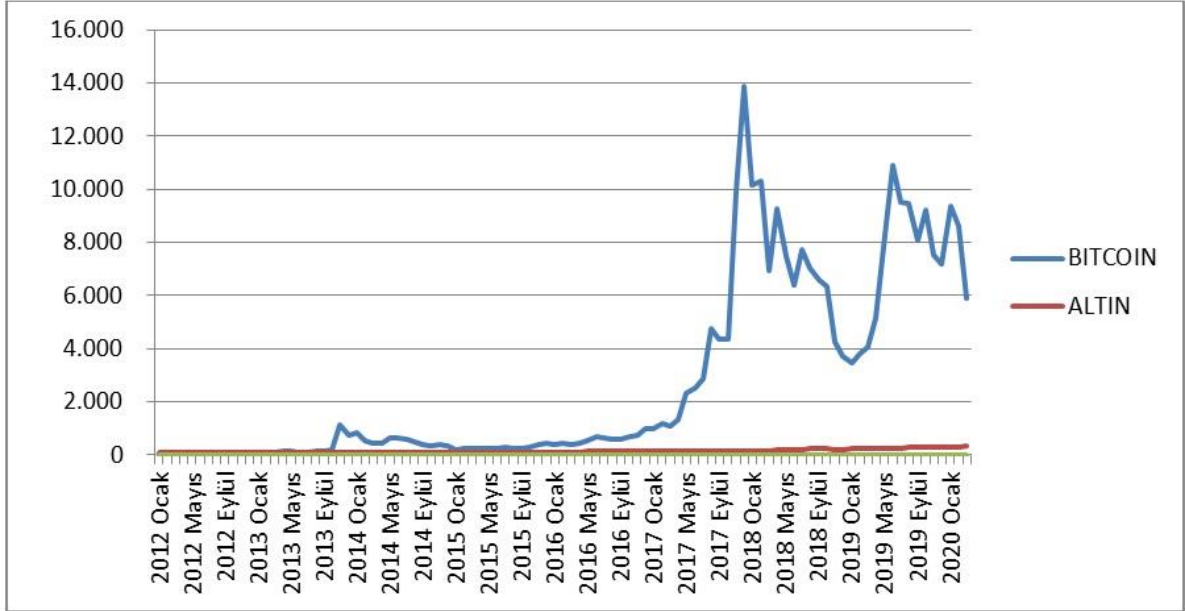
Değişken		Bitcoin	Cumhuriyet Altını	Altın Ons	Ham Petrol	Amerikan Doları	Euro
Bitcoin	Korelasyon Katsayısı	1,000	,552	,552	-,084	,483	,559
	Anlamlılık (p)	.	,63	,63	,795	,112	,059
	Gözlem Sayısı	12	12	12	12	12	12
Cumhuriyet Altını	Korelasyon Katsayısı	,552	1,000	1,000**	-,070	,580*	,448
	Anlamlılık (p)	,063	.	.	,829	,048	,145
	Gözlem Sayısı	12	12	12	12	12	12
Altın Ons	Korelasyon Katsayısı	,552	1,000**	1,000	-,070	,580*	,448
	Anlamlılık (p)	,063	.	.	,829	,048	,145
	Gözlem Sayısı	12	12	12	12	12	12
Ham Petrol	Korelasyon Katsayısı	-,084	-,070	-,070	1,000	,028	,126
	Anlamlılık (p)	,795	,829	,829	.	,931	,697
	Gözlem Sayısı	12	12	12	12	12	12
Amerikan Doları	Korelasyon Katsayısı	,483	,580*	,580*	,028	1,000	,965**
	Anlamlılık (p)	,112	,048	,048	,931	.	,000
	Gözlem Sayısı	12	12	12	12	12	12
Euro	Korelasyon Katsayısı	,559	,448	,448	,126	,965**	1,000
	Anlamlılık (p)	,059	,145	,145	,697	,000	.
	Gözlem Sayısı	12	12	12	12	12	12

\*\* Korelasyon 0,01 düzeyinde anlamlıdır

Bitcoinin cumhuriyet altını, altın ons fiyatı, dolar, euro ve ham petrol fiyatı ile istatistiksel olarak anlamlı ilişkisi görülmemiştir ( $p>0,05$ ).



Bitcoinin diğer ekonomik göstergelerle arasındaki korelasyon ilişkisi incelendiğinde hareketliliğin yüksek olduğu görülmektedir. Bu durum bitcoinin, istikrarlı bir ödeme aracından ziyade spekülatif bir yatırım aracı olarak görülmesi olarak algılanabilir.



Şekil 3.1. 2012-2020 Yılları Arasında Yatırım Aracı Olarak Bitcoin ve Altın

Şekil 3.1’de 2012-2020 döneminde bir yatırımcının BTC ve altın olarak tasarruf etmesi durumunu gösteren grafik yer almaktadır. Grafik incelendiğinde 2017 yılına kadar bitcoin kurunda fiyat seyrinin çok dalgalı olmadığı görülmektedir. Bitcoinin dolar karşılığının bir önceki yıla göre 3 katından fazla artmasıyla, 2017 yılı bitcoinin zirve yılı olarak kayda geçmiştir.

## 4. SONUÇ

Finans sektöründe işlemlerin gerçekleşmesi güven çerçevesinde sağlanmaktadır. Geleneksel yöntemlerde işlemler aracı kurumlar tarafından güvence altına alınmaktadır. 2008 yılında küresel bir kriz yaşanmış, mevcut ekonomik ve politik sisteme karşı bir güvensizlik ortama hakim olmuştur. Finansal kurumlara olan güvenin sarsıldığı bu kriz ortamında Nakamoto tarafından Blokzincir teknolojisi yayımlanmıştır.

Blokzincir teknolojisi ardında bıraktığı 10 yıla rağmen popülerliğini kaybetmeyerek; son yıllarda yenilikçi teknoloji uzmanlarından ve hükümetlerden artan bir ilgi görmektedir. Blokzincir ve merkezi olmayan platformların sosyal etkileşimleri büyük ölçüde yönetme ve geleneksel merkezi otoriteleri rahatsız etme yeteneğine sahip aşırı politik araçlar olarak değerlendirilmesi mümkündür. Günümüzde, Blokzincir güvenilir bir ağ sistemidir. Ancak, merkezileşmiş benzerlerinden daha yavaş olduğu bir gerçektir.

Türkiye’de, özellikle TÜBİTAK çatısı altında kurulan Blokzincir Araştırma Laboratuvarı (2018) bu alanda atılmış büyük bir adımdır. TC Merkez Bankası öncülüğünde Blokzinciri alanında çalışma grupları oluşturulmuştur. Kasım 2019 itibariyle Hazine ve Maliye Bakanlığı, Merkez Bankası ve Bankacılık Düzenleme ve Denetleme Kurumu’nun (BDDK) iş birliğini yürüteceği Ödeme Hizmetleri ve Elektronik Para Kuruluşları Birliği’ni kurulacağı duyurmuştur. Yayımlanan 2020 Yılı Cumhurbaşkanlığı Yıllık Programı’nda Merkez Bankası’nın Blokzincir tabanlı dijital parasının uygulamaya konulacağı bilgisi yer almıştır. Türkiye Bilişim Vakfı (TBV) liderliğinde ticari kaygılardan uzak bir çizgide ve bağımsız bir yapıda kurulan Blokzincir Türkiye Platformu da, Blokzincir teknolojisinin okur yazarlığının artırılması ve ilgili paydaşların ortak bir zeminde toplanması açısından önemli gelişmelerdir.

Blokzincir teknolojisinin kullanım alanı oldukça geniş olup sahip olduğu potansiyel keşfedilme aşamasındadır. Sağlamış olduğu avantajlar ile başta finans sektörü olmak üzere sosyal, siyasal, ticari ve askeri sektörlerin de mevcut iş süreçleri için çözüm içermektedir. Geleceğin teknolojisi olma potansiyeline sahip Blokzincir için bu kapsamdaki bilimsel araştırmaların desteklenmesi teşvik edilmelidir.

Bu çalışmada, kripto para türleri arasında popüler olan ve kripto para piyasasının %54,9’unu elinde tutan bitcoinin işleyiş süreci incelenmiştir. Önceki yıllarda yapılmış çalışmalardaki veriler ile güncel piyasa hacmi karşılaştırılmıştır. Bitcoin değerinin artan bir

trendde olduđu gözlenmiştir. Başta bitcoin olmak üzere kripto paraların yaşamın bir çok alanında kullanılmaya başlanması ile yeni kavramların ve işleyişlerin günlük hayata girdiği izlenmiştir.

Çalışmada, Ocak 2012 – Mart 2020 tarihleri arasında cumhuriyet altını, altın ons fiyatı, ham petrol fiyatı, amerikan doları ve euro para birimleri ile bitcoin arasındaki istatistiksel ilişkisi araştırılmıştır. Araştırma kapsamında analizlerde IBM SPSS Statistics 25 programından faydalanılmış, Spearman korelasyon katsayısı analizi kullanılmıştır. Yapılan analizlerinin sonucuna göre piyasalarda yer edinmeye başladığı ilk dönem olan 2012’de bitcoinin diğer göstergelerle arasında istatistiksel olarak anlamlı bir ilişkisi saptanmamıştır ( $p>0.05$ ). Bitcoinin dolar karşılığının bir önceki yıla göre üç katından fazla arttığı 2017 yılı ise bitcoinin zirve yılı olup; euro ile arasında pozitif yönlü kuvvetli bir ilişki tespit edilmiştir ( $r=0.873$ ;  $p<0.001$ ).

2012-2020 döneminde istatistiksel olarak bitcoinin ham petrol fiyatı ile arasında negatif yönlü ve zayıf; cumhuriyet altını, altın ons fiyatı, dolar ve euro ile arasında ise kuvvetli bir ilişki var olduğu ve bu ilişkinin anlamlı olduğu saptanmıştır. Yüksek hareketlilik, bitcoinin, istikrarlı bir ödeme aracından ziyade spekülasyon bir yatırım aracı olarak görülmesi olarak algılanabilir. Bitcoinin uzun dönemde en çok euro ile arasında kuvvetli bir ilişki olduğu saptanmıştır.

Türkiye’de bitcoin alımsatım işlemleri gerçekleşmesine rağmen, bir çok dünya ülkesinde olduğu gibi ilgili otoriteler tarafından uzaktan izlenmektedir. Henüz bir bitcoin borsası ülkemizde kurulmamıştır. Bitcoin kullanımını destekleyen düzenlemelerin olası riskler değerlendirilerek hayata geçirilmesiyle bu pazardan pay alınması ve gelir elde edilmesi mümkün görülmektedir.

## 5. KAYNAKLAR

- Akbank (2019). 10 Nisan 2019 tarihinde <https://www.akbank.com/tr-tr/Yatirimci-iliskileri/Sayfalar/Kisaca-Akbank.aspx> adresinden alınmıştır.
- Alptekin, E. (2017). Blokzincir ve Kripto Paralar, Dünya Ekonomisini Dönüştürüyor. *İzmir Ticaret Odası, AR&GE Bülten 2017 Kasım Aralık - Ekonomi* 19 Nisan 2019 tarihinde [http://izto.org.tr/demo\\_betanix/uploads/cms/yonetim.ieu.edu.tr/6417\\_1514355987.PDF](http://izto.org.tr/demo_betanix/uploads/cms/yonetim.ieu.edu.tr/6417_1514355987.PDF) adresinden alınmıştır.
- Andersen, T.G., Bollerslev, T., Christoffersen, P. and Diebold, F. X. (2007). Practical Volatility and Correlation Modeling for Financial Market Risk, The Risks of Financial Institutions. University of Chicago Press, 513-548.
- Antonopoulos, M. A. (2014). *Mastering Bitcoin - Unlocking Digital Currencies*. O'Reilly Media.
- Atozmarkets (2019). What are Blockchain's Issues and Limitations? 12 Kasım 2019 tarihinde <https://atozmarkets.com/news/what-are-Blockchains-issues-limitations> adresinden alınmıştır.
- Atzori, M. (2015). Tecnologia Blokzincir E Governance Decentralizzata: Lo Stato È Ancora Necessario? (Blockchain technology and decentralized governance: Is the state still necessary?) <https://ssrn.com/abstract=2731132> veya <https://doi.org/10.2139/ssrn.2731132>.
- Baliga, A. (2017). *Understanding Blockchain Consensus Models*, Persistent Systems Ltd., 6.
- Başer, F. (2012). Ankara Üniversitesi Açık Ders Malzemeleri. 10 Mart 2020 tarihinde [https://acikders.ankara.edu.tr/pluginfile.php/102241/mod\\_resource/content/0/%C4%B0statistik%20Ders%20Notu%2012.pdf](https://acikders.ankara.edu.tr/pluginfile.php/102241/mod_resource/content/0/%C4%B0statistik%20Ders%20Notu%2012.pdf) adresinden alınmıştır.
- BBC (2015). 10 Mayıs 2019 tarihinde [https://www.bbc.com/turkce/ekonomi/2015/06/150628\\_yunanistan\\_banka\\_kapali](https://www.bbc.com/turkce/ekonomi/2015/06/150628_yunanistan_banka_kapali) adresinden alınmıştır.
- bctr.org (2018). Blokzincir Türkiye Platformu. 20 Kasım 2019 tarihinde <https://bctr.org> adresinden alınmıştır.
- BDDK (2019). Ödeme Sistemleri ve Elektronik Para Kuruluşları. 12 Aralık 2019 tarihinde <https://www.bddk.org.tr/Sss-Kategori/Odeme-Sistemleri-ve-Elektronik-Para->

Kuruluslari/3 adresinden alınmıştır.

Bitcoin Developer Guide (2019). Mining. 7 Mart 2019 tarihinde <https://bitcoin.org/en/developer-guide#mining> adresinden alınmıştır.

Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa. 20 Kasım 2019 tarihinde <https://powercompare.co.uk/bitcoin> adresinden alınmıştır.

Borsa İstanbul (2018). Türkiye'nin İlk Finansal Blokzincir Projesi Borsa İstanbul Bilişim Teknolojileri Ekibi Tarafından Hayata Geçirildi. 10 Ekim 2019 tarihinde <https://www.borsaistanbul.com/duyurular/2018/09/05/turkiye-nin-ilk-finansal-blokzincir-projesi-borsa-istanbul-bilisim-teknolojileri-ekibi-tarafindan-hayata-gecirildi> adresinden alınmıştır.

BTCTÜRK (2019). 10 Yılda Bitcoin. 10 Mayıs 2019 tarihinde <https://www.btcturk.com/yardim/10-yilda-bitcoin> adresinden alınmıştır.

Bulut, Ş. (2013). *Türkiye'de Seçilmiş Makroekonomik Değişkenler ile İstanbul Menkul Kıymetler Borsası (İMKB) Arasındaki İlişki*. Doktora Tezi. Adnan Menderes Üniversitesi, Sosyal Bilimler Enstitüsü, Aydın.

Buterin, V. (2013). A Next Generation Smart Contract And Decentralized Application Platform. <https://ethereumbuilders.gitbooks.io/guide/content/en/whitepaper.html>

Buterin, V. (2015). On Public and Private Blockchains. 21 Mart 2019 tarihinde <https://blog.ethereum.org/2015/08/07/on-public-and-private-Blockchains> adresinden alınmıştır.

Calibra (2019). A connected wallet for a connected World. 9 Ekim 2019 tarihinde <https://www.calibra.com> adresinden alınmıştır.

Cengiz, K. (2018). En Popüler Kripto Para Birimi: BITCOIN. *Bandırma Onyedi Eylül Üniversitesi, Sosyal Bilimler Araştırmaları Elektronik Dergisi*, 2018; 1(2), 87-100.

Chaum, D. (1992). Achieving Electronic Privacy. *Scientific American*, 267 (2): 96–101.

Coinatmradar (2019). Bitcoin ATMs in Turkey. 6 Aralık 2019 tarihinde <https://coinatmradar.com/country/218/bitcoin-atm-turkey> adresinden alınmıştır.

Coinmarketcap (2019). About Facebook Libra. 6 Ekim 2019 tarihinde <https://coinmarketcap.com/tr/currencies/facebook-libra> adresinden alınmıştır.

- Çarkacıoğlu, A. (2016). Kripto-Para Bitcoin. Sermaye Piyasası Kurulu Araştırma Raporu, Ankara.
- Dilek, Ş. (2018). Blokzincir Teknolojisi ve Bitcoin. *Analiz*, Şubat 2018, Sayı: 231, Ankara, SETA Yayınları.
- Ec.europa.eu (2018-1). EU Blockchain Observatory and Forum - Call for Contributors. 25 Mart 2019 tarihinde <https://ec.europa.eu/digital-single-market/en/news/eu-blockchain-observatory-and-forum-call-contributors> adresinden alınmıştır.
- Ec.europa.eu (2018-2). European countries join Blockchain Partnership. 26 Nisan 2019 tarihinde <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership> adresinden alınmıştır.
- Eğilmez, M. (2013). Kendime Yazılar: Bitcoin. 10 Nisan 2019 tarihinde <http://www.mahfiegilmez.com/2013/11/bitcoin.html> adresinden alınmıştır.
- Eğilmez, M. (2017). Kendime Yazılar: Kripto Paralar, Bitcoin ve Blokzincir. 19 Nisan 2019 tarihinde <http://www.mahfiegilmez.com/2017/11/kripto-paralar-bitcoin-ve-blokzincir.html> adresinden alınmıştır.
- Ethereum (2017). White Paper, 20 Haziran 2019 tarihinde <https://whitepaper.io/coin/ethereum> adresinden alınmıştır.
- Euronews (2018). AB Blokzinciri kullanmak için harekete geçti. 25 Mart 2019 tarihinde <http://tr.euronews.com/2018/02/01/ab-blok-zinciri-kullanmak-icin-harekete-gecti> adresinden alınmıştır.
- Feiner, L., Rooney, K. (2019). PayPal withdraws from Facebook's libra cryptocurrency. 9 Ekim 2019 tarihinde <https://www.cnbc.com/2019/10/04/paypal-withdraws-from-facebooks-libra-cryptocurrency.html> adresinden alınmıştır.
- Financial Times (01.11.2015). Technology: Banks seek the key to Blockchain. 16 Ekim 2019 tarihinde <https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64> adresinden alınmıştır.
- Franco, P. (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*, John Wiley & Sons, Incorporated.
- Greenspan, G. (2015). Ending The Bitcoin Versus Blockchain Debate. <http://www.multichain.com/blog/2015/07/bitcoin-vs-Blockchain-debate/>

- Gültekin, Y. ve Bulut, Y. (2016). Bitcoin Ekonomisi: Bitcoin Eko-Sisteminden Doğan Yeni Sektörler ve Analizi. *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 3 (3), 82-92.
- He, Y. (2018). A Novel Cross-Chain Mechanism for Blockchains. Qiu, M. (Ed.). *Smart Blockchain*. Springer, 139-148.
- Hofmann, E. (2005). Supply Chain finance: Some Conceptual Insights. In: Lasch R, Janker CG (2005) *Logistik Management - Innovative Logistikkonzepte*. Deutscher Universitätsverlag, Wiesbaden, 203-214.
- Hofmann, E., Strewe, U. M., Bosia, N. (2018). *Supply Chain Finance and Blockchain Technology*. Springer.
- Hutt, R. (2016). All you need to know about Blockchain, explained simply, WEFORUM. 2 Mart 2019 tarihinde <https://www.weforum.org/agenda/2016/06/Blockchain-explained-simply> adresinden alınmıştır.
- 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-usmilitary>
- Kelly, B. (2014). *The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World*. John Wiley & Sons.
- Keş, Y. ve Turgut, B. F. (2015). Kültür ve Sanatın Yansıması Para Tasarımı "Osmanlı Son Dönem Kaimeleri ve Cumhuriyet'in İlk Emisyonları". *Medeniyet Sanat, İstanbul Medeniyet Üniversitesi Sanat ve Tasarım Fakültesi Dergisi*, Cilt: 1, Sayı: 2, 31-47.
- Kırbaş, İ. (2018). Blokzinciri Teknolojisi ve Yakın Gelecekteki Uygulama Alanları. *Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 9 (1), 75-82
- Koin Bülteni (2019-a). Türkiye'nin Tek Bitcoin ATM'si, İstanbul'da Açıldı. 7 Mart 2019 tarihinde <https://koinbulteni.com/turkiyenin-ilk-bitcoin-atmsi-istanbulda-acildi-33985.html> adresinden alınmıştır.
- Koin Bülteni (2019-b). ASIC Nedir? 7 Mart 2019 tarihinde <https://koinbulteni.com/asic-nedir> adresinden alınmıştır.
- Lamport, L., Shostak, R., Pease, M. (1982). The Byzantine Generals Problem, *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, July 1982, 382-401.

- <https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf> adresinden alınmıştır.
- Libra (2019-a). Libra White Paper. 8 Ekim 2019 tarihinde <https://libra.org/en-US/white-paper> adresinden alınmıştır.
- Libra (2019-b). Partner with Libra. 8 Ekim 2019 tarihinde <https://libra.org/en-US/partners> adresinden alınmıştır.
- Mancar, B. (2017). Bitcoin Hakkında Bilmeniz Gereken 9 Önemli Bilgi. 19 Nisan 2019 tarihinde <http://www.webmasto.com/Bitcoin-hakkinda-bilmeniz-gereken-9-onemli-bilgi> adresinden alınmıştır.
- McIntyre, H. (2017). Spotify Has Acquired Blockchain Startup Mediachain, 2 Mayıs 2019 tarihinde <https://www.forbes.com/sites/hughmcintyre/2017/04/27/spotify-has-acquired-Blockchain-startup-mediachain/#69eb516769ee> adresinden alınmıştır.
- Murathan T., Murathan F., (2019). Spor Sektöründe Blokzinciri Uygulamaları. *Gaziantep Üniversitesi Spor Bilimleri Dergisi*, Mart 2019, Cilt: 4, Sayı: 1.
- Mylrea, M., Gourisetti, S. (2017) Blockchain For Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security. *2017 Resilience Week (RWS)*, Wilmington, USA, 18-23.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 7 Mart 2019 tarihinde <http://www.bitcoin.org/bitcoin.pdf> adresinden alınmıştır.
- Özyılmaz, Ç. (2014). *Kriptolojiye Giriş*. Yüksek Lisans Tezi. Karabük Üniversitesi, Fen Bilimleri Enstitüsü, Karabük.
- Piscini, E., Hyman, G., Henry, W. (2017). *Blockchain: Trust Economy*, Deloitte U. Press (Feb. 7, 2017), <https://dupress.deloitte.com/dup-us-en/focus/tech-trends/2017/Blockchain-trust-economy.html>.
- Powercompare (2019). 20 Kasım 2019 tarihinde <https://powercompare.co.uk/bitcoin> adresinden alınmıştır.
- Reuters (2019). France and Germany agree to block Facebook's Libra. 9 Ekim 2019 tarihinde <https://www.reuters.com/article/us-facebook-cryptocurrency-france-german/france-and-germany-agree-to-block-facebooks-libra-idUSKCN1VY1XU> adresinden alınmıştır.
- Romano, D. ve Schmid, G. (2017). Beyond Bitcoin: A Critical Look at Blockchain-Based



- Systems. *Cryptography*, 1 (2), 15; <https://doi.org/10.3390/cryptography1020015>, 1-31.
- Rosic, A. (2016). Proof of Work vs Proof of Stake: Basic Mining Guide. 12 Mart 2019 tarihinde <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake> adresinden alınmıştır.
- Santander InnoVenture (2015). Fintech 2.0 Paper - Rebooting The financial Sector. 7 Ocak 2019 tarihinde <http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf> adresinden alınmıştır.
- Schollmeier, R. (2001). A Definition of Peer-To-Peer Networking For The Classification of Peer-To-Peer Architectures And Applications. [https://www.researchgate.net/publication/3940901\\_A\\_Definition\\_of\\_Peer-to-Peer\\_Networking\\_for\\_the\\_Classification\\_of\\_Peer-to-Peer\\_Architectures\\_and\\_Applications](https://www.researchgate.net/publication/3940901_A_Definition_of_Peer-to-Peer_Networking_for_the_Classification_of_Peer-to-Peer_Architectures_and_Applications)
- Schor, L. (2018). On Zero-Knowledge Proofs in Blockchains. 1 Ekim 2019 tarihinde <https://medium.com/@schor/on-zero-knowledge-proofs-in-Blockchains-14c48cfd1dd1?> adresinden alınmıştır.
- SolarCoin (2019). 2 Mart 2019 tarihinde <https://solarcoin.org> adresinden alınmıştır.
- Sönmez, A. (2014). Sanal Para Bitcoin. *The Turkish Online Journal of Design, Art and Communication - TOJDAC*, July, Volume 4, Issue 3, 1-14.
- Surda, P. (2014). The Origin, Classification And Utility of Bitcoin. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2436823](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436823)
- Swanson, T. (2015). *Consensus as A Service: A Brief Report of Permissioned, Distributed Ledger Systems*. <https://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>
- Takasbank (2019-1). Takas İstanbul, Takasbank'tan Blokzincir Tabanlı Yeni Nesil Transfer Sistemi. 12 Aralık 2019 tarihinde <https://www.takasbank.com.tr/tr/duyurular/duyuru-detay/takasbank-tan-blokzincir-tabanli-yeni-nesil-transfer-sistemi> adresinden alınmıştır.
- Takasbank (2019-2). BİGA Projesi. 20 Kasım 2019 tarihinde <https://biga.takasbank.com.tr> adresinden alınmıştır.

- Tapscott, D., Tapscott, A. (2017). Realizing the Potential of Blockchain. White Paper, World Economic Forum. [http://www3.weforum.org/docs/WEF\\_Realizing\\_Potential\\_Blockchain.pdf](http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf)
- TCMB (2018: 64). 100 Soruda Merkez Bankacılığı. 12 Mart 2019 tarihinde <https://www.tcmb.gov.tr/wps/wcm/connect/2d9f2c1d-18eb-4124-8fd9-a4ea189a24ad/100+Soruda+TCMB+web.pdf?MOD=AJPERES&CVID=&CACHE=NONE&CONTENTCACHE=NONE> adresinden alınmıştır.
- Tian, C. (2017). Singapore Exchange to Trial Blockchain Verification for Diamond Trading. 2 Mart 2019 tarihinde <https://www.coindesk.com/singapore-exchange-trial-blockchain-verification-diamond-trading> adresinden alınmıştır.
- TÜBİTAK (2019-a). 1. Ulusal Blokzincir Çalıştayı. 12 Mart 2019 tarihinde [http://blokzincir.bilgem.tubitak.gov.tr/document/Calistay\\_bildirileri.pdf](http://blokzincir.bilgem.tubitak.gov.tr/document/Calistay_bildirileri.pdf) adresinden alınmıştır.
- TÜBİTAK (2019-b). BİLGEM’de Blokzincir. 12 Mart 2019 tarihinde <https://Blokzincir.bilgem.tubitak.gov.tr/bz-calistay/bzlab.html> adresinden alınmıştır.
- TÜBİTAK (2019-c). 2. Ulusal Blokzincir Çalıştayı. 2 Nisan 2019 tarihinde [https://Blokzincir.bilgem.tubitak.gov.tr/bz-calistay/files/Blokzincir\\_Tanitim\\_Brosuru.pdf](https://Blokzincir.bilgem.tubitak.gov.tr/bz-calistay/files/Blokzincir_Tanitim_Brosuru.pdf) adresinden alınmıştır.
- Türkmen, S. Y. ve Durbilmez, S. E. (2019). Blokzincir Teknolojisi ve Türkiye Finans Sektöründeki Durumu, *Finans Ekonomi ve Sosyal Araştırmalar Dergisi*, 2019 (3), 30-45.
- UNICEF (2019). Blockchain, Exploring Blockchain applications to accelerate impact 12 Ekim 2019 tarihinde <https://www.unicef.org/innovation/Blockchain> adresinden alınmıştır.
- Ülker, Ü. (2013). Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti. *Bilişim Teknolojileri Dergisi*, Cilt: 6, Sayı: 2, 31-39.
- Ünsal, E., Kocaoğlu, Ö. (2018). Blokzinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri. *Avrupa Bilim ve Teknoloji Dergisi*, Sayı: 13, 54-64.
- VisaNet (2019). 20 Nisan 2019 tarihinde <https://www.visa.com.tr/visa/visanet.html> adresinden alınmıştır.

- Vural, M. G. (2003). *Altın Piyasası ve Altın Fiyatlarını Etkileyen Faktörler*. Uzmanlık Yeterlilik Tezi. Türkiye Cumhuriyeti Merkez Bankası, Ankara.
- Wang, W. (2018). A Vision for Trust, Security and Privacy of Blockchain. Qiu, M. (Ed.). *Smart Blockchain*. Springer, 93-98.
- www.destekpatent.com (2019). 12 Mart 2019 tarihinde <https://www.destekpatent.com/haber-detay/destek-patent-proofstackden-mevzuatlara-uyumlu-delil-uretimi-icin-is-birligi> adresinden alınmıştır.
- Yılmaz, Y. (2007). Kriptoloji Uygulamalarında Hukuki Boyut. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Cilt: 13, Sayı: 1-2.
- Zheng, B., Zhu, L., Shen, M. (2018). Scalable And Privacy-Preserving Data Sharing Based On Blockchain. *J. Comput. Sci. Technol.* 33 (3), 557-567

## 6. EKLER

### EK 1: BDDK Basın Açıklaması



### BASIN AÇIKLAMASI

Sayı : 2013 / 32

25 Kasım 2013

### BASIN AÇIKLAMASI

Son dönemde bazı basın yayın kuruluşlarında ve internette "Bitcoin" hakkında çeşitli haberlerin çıktığı görülmektedir.

Bilindiği üzere, 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" (Kanun) 27.06.2013 tarih ve 28690 sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir. Kanunun Geçici 1 inci maddesine göre bu Kanunda öngörülen yönetmelikler Kanunun yayımı tarihinden itibaren bir yıl içinde hazırlanarak yürürlüğe konulacaktır. Kanunun Geçici 2 nci maddesine göre ise Kanunun yürürlüğe girdiği tarih itibari ile ödeme hizmetleri sunan ya da elektronik para ihraç eden ve bu Kanun kapsamında ihdas edilen ödeme veya elektronik para kuruluşu kategorisine dahil edilebilecek olan kuruluşlar Kurumumuzca çıkarılacak ilgili yönetmeliklerin yayımı tarihinden başlayarak bir yıl içinde Kurumumuza başvurarak gerekli izinleri almak ve uygulamalarını bu düzenlemelerde yer alan hükümlere uygun hale getirmek zorundadır.

Herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen Bitcoin, mevcut yapısı ve işleyişi itibarıyla Kanun kapsamında elektronik para olarak değerlendirilmemekte, bu nedenle de söz konusu Kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir.

Diğer taraftan, Bitcoin ve benzeri sanal paralar ile gerçekleştirilen işlemlerde tarafların kimliklerinin bilinmemesi, söz konusu sanal paraların yasadışı faaliyetlerde kullanılması için uygun bir ortam yaratmaktadır. Ayrıca Bitcoin, piyasa değerinin aşırı oynak olabilmesi, dijital cüzdanların çalınabilmesi, kaybolabilmesi veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi gibi risklerin yanı sıra yapılan işlemlerin geri döndürülemez olmasından dolayı operasyonel hatalardan ya da kötü niyetli satıcıların suistimalinden kaynaklı risklere de açıktır.

Herhangi bir mağduriyet yaşanmaması adına, yukarıda belirtilen hususların duyurulmasında ve bu çerçevede Bitcoin ve benzeri sanal paraların barındırdığı muhtemel risklerin kamuoyuna hatırlatılmasında fayda mülhaza edilmektedir.

Kamuoyuna saygıyla duyurulur.



T.C. Bilim, Sanayi ve Teknoloji Bakanlığı



TUBITAK BİLGEM

# 1. Ulusal BLOKZİNCİR ÇALIŞTAYI

2-3 Nisan 2018 ANKARA JW Marriott Hotel

ANA SPONSOR



TÜRKİYE CUMHURİYET MERKEZ BANKASI

Misafir Konuşmacılar >

**Peter Gaži**  
Research Fellow, co-author of the Ouroboros Praos protocol - the next version of the Cardano system  
IOHK research  
iohk.io

**Malcolm Lerider**  
Senior R&D Manager  
NEO Smart Economy  
neo.org

Konular >

- Bitcoin ve Diğer Kripto Paralar
- Merkezi Olmayan Sistemlerde Bizans Hata Toleransı
- Blokzincir Teknolojisinin Gerçek Hayattaki Muhtemel Uygulamaları
- Blokzincir Ekosistemi: Finans, Enerji, Tedarik Zinciri, Depolama, Hesaplama, Haberleşme
- Kripto Paraların Güvenlik ve Mahremiyeti
- Akıllı Kontratlar
- Kitle fonlama, ICOlar
- Blokzincir Teknolojisinin Devlet Kurumlarına Uyarlanması
- Sahtecilik ve finansal kriz önleme yöntemleri
- Kripto paralarda ekonomi ve oyun teorisi analizleri
- Emegin İspatı (PoW), Hissenin İspatı (PoS)
- Kullanılabilirlik ve Son Kullanıcı Senaryoları
- Kripto Paraların Adaptasyon ve Uyum Süreci
- Regülasyonlar ve Yasal Düzenlemeler
- Merkezi Olmayan Yapılara Hukuki, Etik ve Sosyal Bir Yaklaşım

Özet Çağrısı >

Son Başvuru Tarihi	11 Mart 2018
Sonuçların Açıklanması	19 Mart 2018









Detaylı Bilgi > ve Başvuru

[blokzincir.bilgem.tubitak.gov.tr](http://blokzincir.bilgem.tubitak.gov.tr)



## EK 3: II. Ulusal Blokzincir Çalıştayı


# 2. Ulusal BLOKZİNCİR ÇALIŞTAYI

25-26 Eylül 2019  
 İstanbul  
Lutfi Kırdar  
ICEC

Kamu ve özel sektörden profesyoneller, akademisyenler ve araştırmacılar blokzincir teknolojisindeki gelişmeleri değerlendirmek için bir araya geliyor.



ANA SPONSOR ?  
ALTIN SPONSOR ?  
GÜMÜŞ SPONSOR ?



# ÖZGEÇMİŞ

## Kişisel Bilgiler

Adı Soyadı: Özgür GÜVEN

Doğum Yeri ve Tarihi: İstanbul / 21.01.1977

## Eğitim Durumu

Önlisans Öğrenimi: Selçuk Üniversitesi / Teknik Bilimler MYO / Bilgisayar Programcılığı, Bölüm Birincisi

Lisans Öğrenimi: Anadolu Üniversitesi / İktisat Fakültesi / Kamu Yönetimi

Lisansüstü Öğrenimi: Aydın Adnan Menderes Üniversitesi / Sosyal Bilimler Enstitüsü / Ekonomi ve Finans ABD / Yüksek Lisans

Bildiği Yabancı Diller: İngilizce

## İş Deneyimi

Yazılım Geliştirici: (1997-Devam) Aydın Adnan Menderes Üniversitesi

Öğretim Elemanı: (2018-2019) Aydın Adnan Menderes Üniversitesi, Tıp Fakültesi, “Biyoteknoloji”

(2019-2020) Aydın Adnan Menderes Üniversitesi, Tıp Fakültesi, “Tıp ve Teknoloji”

## İletişim

e-posta Adresi: oguven@adu.edu.tr

Tarih: 02.07.2020