T.C.

RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İKTİSAT ANA BİLİM DALI

SANAL PARA VE FİNANS PİYASALARI: TÜRKİYE ÜZERİNE BİR UYGULAMA

(Yüksek Lisans Tezi)

Yusuf ÇOLAK

Prof. Dr. Ali Rıza SANDALCILAR

Danışman

RİZE

2019

KABUL VE ONAY

Recep Tayyip Erdoğan Üniversitesi, Sosyal Bilimler Enstitüsü, İktisat Ana Bilim Dalında, Yusuf ÇOLAK tarafından hazırlanan *Sanal Para ve Finans Piyasaları: Türkiye Üzerine Bir Uygulama* başlıklı bu çalışma, 02.12.2019 tarihinde yapılan savunma sınavı sonucunda oy birliği/~~oy çokluğuyla~~ başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Başkan: Prof. Dr. Ali Rıza SANDALCILAR Kabul/~~Red~~

Üye: Doç. Dr. Cemalettin KALAYCI Kabul/~~Red~~

Üye: Dr. Öğr. Üyesi Ali ALTINER Kabul/~~Red~~

18 / 12 / 2019

Doç. Dr. Ahmet YANIK

Enstitü Müdürü

ETİK BEYAN

Bu tezdeki bütün bilgileri etik davranış ve akademik kurallar çerçevesinde elde ettiğimi ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yaptığımı bildiririm. İfade ettiklerimin aksi ortaya çıktığında ise her türlü yasal sonucu kabul ettiğimi beyan ederim. 02/12/2019

Yusuf ÇOLAK

ÖN SÖZ

Çalışma boyunca bana yol gösteren, bilgi ve görüşlerini benimle paylaşarak desteğini esirgemeyen değerli hocam Prof. Dr. Ali Rıza SANDALCILAR'a teşekkürlerimi sunmayı bir borç bilirim. Çalışmanın analiz kısmının her aşamasında yardımlarına başvurduğum Dr. Öğr. Üyesi Mustafa ÇAYIR'a ve Dr. Öğr. Üyesi Ali ALTINER hocalarıma da teşekkürlerimi sunarım. Ayrıca çalışma boyunca yaşanan tüm engelleri benimle göğüsleyen, beni karşılaştığım zorluklarda motive eden, iki evladı için gün içindeki koşuşturmasının yanında bana hayat refikalığı görevinden de taviz vermeyen, her zaman desteğini yanımda hissettiğim kıymetli eşim Ayşenur ÇOLAK'a da sonsuz teşekkürlerimi sunarım.

Yusuf ÇOLAK
RİZE 2019

İÇİNDEKİLER

İKİNCİ BÖLÜM

2.KRİPTOLOJİ, BLOKZİNCİR (BLOCKCHAIN) TEKNOLOJİSİ VE SANAL (KRİPTO) PARALAR

Recep Tayyip Erdoğan Üniversitesi Sosyal Bilimler Enstitüsü
Ana Bilim Dalı: İktisat
Tez Türü: Yüksek Lisans Tezi
Danışman: Prof. Dr. Ali Rıza SANDALCILAR
Hazırlayan: Yusuf ÇOLAK
Yıl: 2019
Sayfa Sayısı: 118

ÖZET

SANAL PARA VE FİNANS PİYASALARI: TÜRKİYE ÜZERİNE BİR UYGULAMA

Para, günümüze kadar ki yolculuğunda farklı şekillerde varlığını devam ettirmiş ve bir takım değişikliklere uğramıştır. Her bir değişiklik ticari, sosyal ve teknolojik gelişmelerden etkilenmiştir.

Sanal para birimleri de bu değişimin son temsilcisi olma özelliğini taşımaktadır. Sanal paralar, kriptolojik işlemlerle oluşturulan, eşler arasında (Peer to Peer) çevrimiçi ödeme gönderilmesini mümkün kılan ve merkezi herhangi bir finansal kurumun kontrolünde olmayan dijital para birimi olarak tanımlanmaktadır.

Çalışmada Türkiye'deki seçili bir takım finansal değişkenlerle (USD, EURO, POUND, SDR, BİST 100, Cumhuriyet Altını, M1 ve M2 para arzları) sanal para birimi Bitcoin (BTC) arasındaki ilişki incelenmiştir. Bu kapsamda 2013-2019 dönemine ait aylık veriler kullanılmıştır. Analizler sonucunda değişkenlerin birinci farklarının durağan olduğu tespit edilmiş, diğer taraftan Bitcoin ile diğer finansal değişkenler arasında uzun dönemli bir eşbütünleşmenin varlığı belirlenmiştir. Değişkenler arasında nedenselliğin araştırıldığı Granger Nedensellik testi ile de Bitcoin'in bağımlı değişken olduğu denklemde SDR ve USD 'den BTC'ye doğru %5 anlamlılık düzeyinde, Euro ve BIST 100 değişkeninden BTC'ye doğru ise %10 anlamlılık seviyesinde bir nedenselliğin olduğu görülmüştür.

Anahtar Kelimeler: Sanal Para, Kriptoloji, Bitcoin, Eşbütünleşme Nedensellik

Recep Tayyip Erdoğan University Institude of Social Science
Department: Economics
Type of Thesis: Master
Adviser: Prof. Dr. Ali Rıza SANDALCILAR
Author: Yusuf ÇOLAK
Year: 2019
Pages: 118

ABSTRACT
CRYPTOCURRENCY AND FINANCIAL MARKETS: AN APPLICATION ON TURKEY

Money has survived in different ways in its journey to the present and has undergone a number of changes. Each change has been affected by commercial, social and technological developments.

Virtual currencies are also the last representative of this change. Virtual money is defined as a digital currency created by cryptological transactions, which enables online payments between peers (Peer to Peer) and is not under the control of any central financial institution.

In the study, selected by a number of financial variables in Turkey (USD, EURO, POUND, SDR, BİST 100, Republic gold, money supply M1 and M2) have examined the relationship between virtual currency Bitcoin. In this context, monthly data for 2013-2019 period were used. As a result of the analyzes, the first differences of the variables were found to be stationary, while the existence of a long-term cointegration between Bitcoin and other financial variables was determined. The Granger Causality test, which investigates causality between variables, showed that there is a 5% significance level from SDR and USD to BTC and a 10% significance level from Euro and BIST 100 to BTC in the equation where Bitcoin is a dependent variable.

Key Words: Virtual Money, Cryptology, Bitcoin, Cointegration, Causality

KISALTMALAR

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
ADF	:	Augmented Dickey-Fuller Testi
AES	:	Advanced Encryption Standard
AMLD	:	Avrupa Komisyonu Kara Para Aklanmasını Önleme Direktifi
APİ	:	Açık Piyasa İşlemleri
ATM	:	Otomatik Para ödeme Makinesi
BDDK	:	Bankacılık Düzenleme ve Denetleme Kurumu
BIST	:	Borsa İstanbul
BM	:	Birleşmiş Milletler
BOJ	:	Japonya Merkez Bankası
BTC	:	Bitcoin
CAC	:	Çin Siber İdaresi
CBOE	:	Chicago Opsiyon Borsası
CC	:	Dolaşımdaki Paralar
CFTC	:	ABD Emtia Vadeli İşlemler Ticaret Komisyonu
CIRC	:	Çin Sigorta Düzenleme Kurumu
CME	:	Chicago Ticaret Borsası
CNY	:	Çin Ulusal Para Birimi (Yuan)
DD	:	Vadeli Mevduatlar
DES	:	Veri Şifreleme Standardı
DLT	:	Dağıtık Defter Teknolojisi
ECB	:	Avrupa Merkez Bankası
ECC	:	Eliptik Eğri Kriptografi

ECCB	:	Doğu Karayipler Merkez Bankası
EFT	:	Elektronik Fon Transferi
EMKT	:	Elektronik Menkul Kıymet Transferi
EVDS	:	Elektronik Veri Dağıtım Sistemi
FBI	:	Amerika Federal Bürosu
FINCEN	:	Finansal Suçları Engelleme Ağı
FIPS	:	Federal Bilgi İşleme Standardı
GBP	:	Birleşik Krallık Ulusal para Birimi (Pound)
GSYH	:	Gayri Safi Yurtiçi Hasıla
ICO	:	İlk Coin Arzı
IMF	:	Uluslararası Para Fonu
LTC	:	Lithereum
Mb	:	Mega Bayt
M.Ö	:	Milattan Önce
M.S	:	Milattan Sonra
NIST	:	ABD Ulusal Teknoloji ve Standartları Enstitüsü
NSA	:	ABD Ulusal Güvenlik Ajansı
PBOC	:	Çin Merkez Bankası
RBI	:	Hindistan merkez Bankası
SEC	:	ABD Menkul Kıymetler ve Borsa Komisyonu
SHA	:	Güvenli Özet Algoritması
SDR	:	Özel Çekme Hakları (IMF Rezerv Birimi)
SWIFT	:	Dünya Çapında Bankalar Arası Finansal Telekomünikasyon Birliği
TCMB	:	Türkiye Cumhuriyet Merkez Bankası
TD	:	Vadesiz Mevduatlar
TÜBİTAK	:	Türkiye Bilimsel ve Teknik Araştırma Kurumu
yy.		Yüz Yıl

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GİRİŞ

Her yenilik veya dönüşüm beraberinde şüphe ve korku getirir. İnsanlık tarihi boyunca elde edilen başarılar, insanlığın yaşamına sunulan kolaylıklar ve alışılagelmemiş uygulamalar her zaman güler yüzle karşılanmamıştır. Her seferinde eski düzenin itibarlıları veya otoriteleri, bu yeni gelişmelere karşı çıkan ilk cephenin içerisinde yerlerini almışlardır. Çünkü sahip oldukları avantajlı konumları ve çıkarları açısından hayata geçen yeniliğin kendilerine neler getireceğinin veya götüreceğinin hakkında emin olamazlar. Tıpkı 15.yy'da Floransalı Medici ailesinin bankacılığın ilk adımlarını attığı dönemde, para transferlerini kolaylaştıran mekanizmaları sayesinde kişiler arası ticaretin daha ötesinde uluslararası ödemelerin dahi kolaylıkla yapılabileceğini anlatmaları, diğer bir ifadeyle bu konuda güven elde etmeleri, o dönemde adeta para kasalığı görevini üstlenen kilise mensuplarının ve şehir baronlarının tepkisini çektiği gibi.

Teknolojik gelişmeler hayatın olağan akışı içerisinde yaşama yön veren birer akarsu yataklarıdır. Hiçbir kuvvetin, coşkun bir akarsuyu durdurabilmiş olması vaki değildir. Ancak büyük setlerle bir süreliğine engellenebilirler. Bu konuda en yalın ifade Fransız yazar Victor Hugo'ya aittir; *"Hiçbir ordu vakti gelmiş bir fikir kadar güçlü değildir"*.

Paranın söz konusu olduğu değişimler daha sancılıdır ve nispeten daha uzun süreye yayılır. Çünkü hayatın idamesi ve insan ilişkilerinin temelinde paranın yeri ve önemi oldukça büyüktür. Çalışmanın konusunu oluşturan sanal para olgusu da tam olarak bu klasik dönemden geçmektedir. Taşıdığı özellikler ve getirdiği yenilikler daha önce para hakkında bilinenlere ve uygulamalara aykırı izler taşımaktadır.

2008 yılı sonbaharında ABD orijinli küresel finans krizinin yaşandığı dönemde, Satoshi Nakamoto isimli bir kişi tarafından oluşturan bir e-posta da, paranın, merkezi olmayan, herhangi bir devlet ya da otoritenin tekelinden bağımsız, aracıların olmadığı, kriptografik işlemlerle ortaya çıkarılan ve sanal

ortamda aktarımı yapılan yeni bir türünün oluşturulabileceği fikri, birkaç bilgisayar mühendisinin yer aldığı forumlarda tartışılmaya başlanmış, 2009 yılının ilk ayında ise 30.000 satırlık kaynak kodunun sisteme girilmesi ile söz konusu fikir, Bitcoin ismini alarak hayata geçirilmiş oldu. Bu yeni teknoloji ile beraber bankalar, kamu otoriteleri ve aracı kurumlar öncelikle Bitcoin hakkında olumsuz beyanatlarda bulunarak, söz konusu sanal para biriminin para olarak kullanımının imkânsız olduğunu, kimsenin bu paraya güven duymayacağını, paranın klasik özelliklerini taşımadığını ve genel bir kabul görme işlevinden uzak kalacağını ileri sürmüşlerdir. Ancak unuttukları önemli birkaç nokta vardı. 2008 finans kriziyle bireylerin finansal piyasalara ve para otoritelerine güvenleri sarsılmış, para aktarımları için aracı kurumlara ödedikleri havale komisyonları giderek artmış ve teknolojinin getirdiği yüksek işlem hızından mahrum kalmışlardı. İşte sanal para birimleri insanlığa tam da bu yenilikleri vadetmekteydi. Diğer taraftan 1990'lı yıllarda hiç kimse bir gün orta yaşın üstündeki kişilerin bile birer sosyal medya kullanıcısı olabileceklerini düşünemezdi. Teknolojinin yayılması ve kullanım kolaylığı gibi etmenler sanal paraların genel olarak kabul görmesini de kolaylaştırmaktaydı.

Sanal para birimlerinin yalnızca parasal yönleri dikkat çekici değildir. Sanal paraların oluşturulduğu teknolojinin, yani Blokzincir kapsamında Dağıtık Defter Teknolojisi (DLT) ve akıllı kontratlar sayesinde etkilenecek alan sayısı her geçen gün artmaktadır. Bu nedenle çalışmada Sanal Para Birimlerinin alt yapısını oluşturan söz konusu teknolojik gelişmelerin anlaşılması da ayrıca bir ihtiyaç haline gelmiştir.

Çalışmanın amacını sanal para birimlerinin ilki olma özelliğini taşıyan Bitcoin (BTC) ve seçili bir takım finansal büyüklükler arasında bir nedensellik ve eşbütünleşme ilişkisinin var olup olmadığının tespit edilmesi ile sanal para birimlerinin genel olarak ekonomiye etkilerinin araştırılması oluşturmaktadır. Bu amaç doğrultusunda; ilk bölümde paranın tanımı, özellikleri ve işlevlerinden bahsedildikten sonra ikinci bölümde sanal paraların nasıl oluşturulduğu kriptoloji, Blokzincir ve Dağıtık Defter Teknolojilerinin incelenmesi ile ortaya konmaya çalışılmıştır. Blokzincir teknolojisinin kullanıldığı alanlar ve dağıtık defter yapısının özellikleri de yine bu bölümde yer almaktadır. Üçüncü bölümde ise

konu ile ilgili olarak akademik literatür taraması ile kripto (sanal) paralar hakkında yapılmış çalışmalardan örnekler verilip, analiz bölümünde de sanal para birimlerinin ilk ve en büyük hacime sahip örneği Bitcoin ile seçili bir takım finansal değişkenler arasında nedensellik ve eşbütünleşmenin varlığı test edilmiştir. Çalışma, sonuç ve değerlendirme bölümü ile sonlandırılmıştır.

BİRİNCİ BÖLÜM

1. PARA TEORİSİ VE PARANIN TARİHİ GELİŞİMİ

1.1. Paranın Tanımı ve Özellikleri

Para, ortaya çıktığı ilk günden bu yana mübadele aracı olma asli fonksiyonu üzerinden tarif edilmeye çalışılmıştır. Paranın doğuşu da bu fonksiyonu sebebiyle olmuş, takas ekonomisinin getirdiği güçlükler para ile aşılmıştır (Hiç, 1975). Paranın olmadığı ekonomilerde yaşanan ve karşılıklı mal değişimini esas alan takas işlemleri, işlem, taşıma ve değer saklama maliyetlerini beraberinde getirmiştir. Takasta kullanılacak malların değişim yerine intikali ve saklanması, karşılıklı ihtiyaçların birbiriyle çakışması gereği ve her bir malın diğer mallar karşısındaki sabit olmayan değeri söz konusu maliyetlerin nedenleridir (Handa, 2000). Paranın değer ölçü birimi olması takas ekonomisinde değişim değerlerinin her bir farklı mal için hesaplanması ve akılda kalması sorununu ortaya çıkarmıştır.

Ekonomilerde n tane malın varlığı söz konusu ise bu ekonomide $\frac{n(n-1)}{2}$ kombinasyon değeri kadar değişim değeri vardır (Paya, 2007). Hiç şüphesiz paranın varlığı, her bir malın değerinin belli bir para miktarı olması nedeniyle takas ekonomilerine nispeten kıymet ölçümünün çok daha kolay ve akılda kalıcı olmasını sağlamaktadır. O halde anlatılanlardan yola çıkarak ekonomi literatüründe de ortak görüş haline gelmiş para tanımı şu şekilde yapılabilir;

Para, ticarete konu tüm mal ve hizmetlerin satın alınmasında satıcıya ödenen ya da borçların geri ödenmesinde kullanılan genel kabul görmüş her şeydir (Mishkin, 2015).

Para olarak isimlendirilen bir değişim aracının sahip olması gereken asgari şartlar vardır (Paya, 2007). Bu şartlar değinildiği gibi asgari olup zamanla paranın

bu özelliklerine işlev ve şekil bakımından eklemeler yapılmaktadır. Çalışmanın ilerdeki bölümlerinde söz konusu diğer özelliklere de yer verilecektir.

Para olarak kullanılan bir değişim aracının sahip olması gereken asgari özellikler Tablo 1'de belirtilmiştir (Öçal, 1990).

Tablo 1
Paranın özellikler

Homojen olması	Paranın meydana getirildiği madenin her yerinin aynı değerde olduğunu,
Bölünebilir olması	Ticarette yer alan tüm mal ve hizmetlerin değerini karşılayabilecek küçük değerleri de temsil edebilirliğini,
Bozulmama ve Taşınabilir olması	Paranın değişim yerine naklinin kolay ve fiziki olarak uzun süre kullanılabilir olduğunu,
Taklit edilememesi	Paranın sahte ödemelere karşı belirli bir takım özelliklere sahip olduğunu,
Genel kabul görmüş olması	Herkes tarafından görünümü, değeri ve itibarı kabul edilmiş olmasını göstermektedir.

1.2 Paranın İşlevleri

Paranın işlevleri bir taraftan paranın kullanım amaçlarını oluştururken diğer taraftan da merkez bankaları aracılığıyla kamu otoritesinin ekonomideki parasal büyüklüğe, buradan hareketle de ekonomik düzenlemelere de müdahale edilmesini kolaylaştırmaktadır. Paranın işlevleri Tablo 2'de gösterilmiştir.

Tablo 2
Paranın İşlevleri

Değişim (Mübadele) Aracı Olması	Paranın Her türlü alış veriş işleminde taraflarca tereddüt edilmeden mübadele aracı olarak kabul edilmesidir.
Hesap (Değer) Birimi Olması	Tüm mal ve hizmetlerin değerlerinin bir parasal değerle ifade edilmesidir.
Değer Saklama Aracı Olması	Paranın gelecekte ihtiyaç halinde kullanılabilmesi amacıyla saklanabilir olmasıdır.
İktisat Politikası Aracı Olması	Kamu otoritesinin piyasadaki para miktarı ile ekonomik büyüklüklere etki edilebilmesidir.

1.3. Tarihi Süreç İçerisinde Para Sistemleri

1.3.1. Mal Para Sistemi

Tarih boyunca para olarak kullanılan eşyalarda farklılıklar gözlemlenmiştir. Tütün, hayvan derileri, büyük taşlar, deniz kabukları, boncuklar ve işlenmiş madenler bunlardan bir kaçı olarak sıralanabilir (Hiç, 1975). Bu gibi paralar, ekonomi literatüründe mal para olarak tanımlanmakta, sistemin adı da mal para sistemi olarak anılmaktadır. Mal para sisteminde kullanılan eşyaların taşınma zorluğu ve kısa sürede fiziki bozulmaya uğramaları, mal paraların kullanılmasında yaşanan güçlükler olarak sıralanabilir. Bu sebeplerle mal paraların kullanımının yerini fiziken bozulmaya ve yıpranmaya dayanıklı, taşınması daha kolay para türleri almıştır.

1.3.2. Metal Para Sistemi

M.Ö 7. yüzyılda Batı Anadolu'da yaşayan Lidyalılar ilk kez ülke içinde alış verişte ve diğer ülkelerle yapılan dış ticaretlerinde devletin ölçü ve miktarını

tayin ettiği resmi bir anlam taşıyan madeni parayı kullanmışlardır (Cesur, 2014). Bu gelişme ile beraber madeni paranın kullanımı hızla artmış, büyüklüğü, miktarı ve meydana geldiği maden itibariyle çeşitli şekillerde ve boyutlarda olmak üzere geniş bir coğrafyanın vazgeçilmez değişim aracı olarak ticaret hayatında kullanılmaya başlanmıştır. Metal para sistemi olarak adlandırılan bu dönemde metal paranın en önemli örnekleri altın ve gümüş olmuştur. Söz konusu madenlerin kendiliğinden bir değere sahip olmaları kullanım amaçlarının ana sebebini oluşturmuştur (Sekmen, 2012). Devletler madeni paranın içerdiği miktar ve saflık derecelerini belirleyerek, paranın üzerine özel işaret ve resimler işleyerek herkes tarafından tanınabilir olmasını ve alış verişlerde paranın güvenirlilik şüphesinin giderilmesini sağlamışlardır. Örneğin Makedonya Kralı Büyük İskender'in resminin olduğu ve arka yüzünde mührünün yer aldığı altın paralar (M.Ö 356) kullanılmıştır (Şıklar, 2004). Mal para sisteminde eski çağlarda kullanılan eşyaların yerini madenlerin (altın ve gümüşün) almasının en önemli sebepleri; değişim aracı olarak kullanılan eşyaların taşınmasında, saklanmasında ve söz konusu eşyaların çok küçük değer birimlerine bölünmesindeki güçlükler sıralanabilir.

Altınla birlikte gümüşün kullanıldığı madeni para sistemi çift maden sistemi (bimetalizm) olarak bilinmektedir (Parasız, 2011). Sistemde yer alan altın ve gümüş paralar devlet tarafından resmi para birimi olarak tanımlanmış, yine devlet tarafından iki metal para arasında bir dönüşüm oranı belirlenerek alış verişlerde kullanılması sağlanmıştır. Önceleri altın ve gümüş arasında belirlenen 1/10 dönüşüm oranı, gümüş rezervlerindeki artışa bağlı olarak 1/15 oranına kadar düşmüştür (Ergin, 1983). Sistemdeki madenlerin piyasa fiyatları ile devlet tarafından belirlenen değerleri arasındaki fark arttıkça da içeriğinde daha az değerli maden bulunduran para, daha fazla değerli maden içeren paraya göre kullanımda daha çok tercih edilmeye başlamıştır. Ekonomi literatürüne Gresham Yasası olarak giren bu durum "kötü para iyi parayı piyasadan kovar" olarak da açıklanmaktadır (Erdem, 2016).

Çift maden sisteminin kullanıldığı dönemlerde para basma yetkisini elinde bulunduran otorite tarafından altın ve gümüşün ayarlarında yapılan değişikliklerle gelir elde edilmeye çalışılmış, aynı miktar metal parayla daha fazla ödeme

yapılması sağlanmıştır. Buna tağşiş adı verilmektedir (Özbilen , 2016). Tağşişle para arzının, para olarak kullanılan madenin üretiminden daha fazla olması sağlanarak, toplam talebin artırılması yoluna gidilmiştir. Bu duruma Osmanlı Devletinde kullanılan altın paranın ayarındaki değişiklik örnek olarak gösterilebilir. Fatih Sultan Mehmet dönemindeki altın ayarı 0,993 iken altın ayarı tağşişe uğrayarak II. Mahmut döneminde 0,582'ye kadar düşürülmüştür (Ergin, 1983). Diğer taraftan para basma yetkisi, bu yetkiyi elinde bulunduran otorite için bir gelir kaynağı oluşturmaktadır. Geçmişten günümüze bu tekeli elinde bulunduran devlet ya da siyasi güç, paranın üzerinde yazılı olan değer ile paranın maliyet değeri arasındaki farkı, vergi yahut başkaca bir araç kullanmadan adeta parayı kullanan piyasa aktörlerinden faizsiz bir borç alır gibi toplamış, devlet harcamalarını bu yolla finanse etmiştir (Aslan, 2009). Senyoraj geliri olarak bilinen bu durum, para basma monopolü karşılığında devletin elde ettiği gelir olarakta ifade edilebilir.

1.3.3. Altın Para Sistemi

Altın sikkelerinin taşınma, aşınma ve çok küçük birimlere bölünememesi sorunu karşısında, sarraflar tarafından kendilerine emanet edilen ve karşılığında altın sikke sahiplerine üzerlerinde altın miktarının yazılı olduğu kâğıtlar verilmeye başlanmıştır (Aren, 2007). Banknot adı verilen bu kâğıtlar tamamen üzerlerinde yazılan altın değerini temsil eden ve iç piyasada kullanılabilen paralar haline gelmiştir. Ancak ülkeler dış ödemelerinde altın kullanmaya devam etmişlerdir. Altın para sistemi olarak adlandırılan bu uygulamada tedavüldeki toplam banknot değeri kadar altın rezervi olduğu gerçeğinden hareket edilmektedir. Sistemde kendilerine altın emanet edilen ve karşılığında altın sahiplerine banknot veren sarraflar, bu altınların sahipleri tarafından sürekli talep edilmediğini, belli bir süre söz konusu altınların kendilerinde kaldığını fark ettiler (Şıklar, 2004). Bu durum sarrafların ellerindeki altın miktarından daha fazla değerde banknotu piyasaya sürmelerine neden olmuştur. Para sistemlerinin en önemli dayanağı olan güvenirlilik vasfı bu yolla sarsılmaya başlamıştır. Devletler, ülkede para sisteminin bozulmaması adına kasalardaki altın miktarlarının belirli bir miktar fazlası için yasal banknot tedavülüne izin vermiştir (Aslan, 2009). Örneğin

kendisinde bir birim altın rezervi bulunan sarraf yahut banka benzeri kurumlar, ancak üç birim kâğıt para piyasaya sürebilirlerdi. Bu anlatılanlar bir diğer taraftan bankacılığın ilk gelişim evresini oluşturmaktadır.

Birinci Dünya savaşına kadar sorunsuz devam eden bu süreç, savaş öncesi ve sonrasında ülkelerin borçlarını ödeme ve harcamalarını gerçekleştirebilmeleri için paraya ihtiyaç duymaları sebebiyle rezervlerinde bulunan altın stokundan yasal miktarlardan daha fazla kâğıt para basmalarına, piyasadaki karşılıksız para miktarı da fiyatlar genel seviyesinin artmasına (enflasyona) neden olmuştur (Paya, 2007). Bu olumsuzluğa rağmen savaş sonrasında da devletlerin altın karşılığı olan kâğıt para sistemine devam etmeye çalıştığı görülmektedir.

1.3.4. Altın Kambiyo Sistemi

1929 yılında başlayan ABD orijinli ekonomik bunalım sürecinde ülkeler, krizden çıkma yolu olarak; iç üretimi ve talebi artırma, iş gücü geçişkenliğini sınırlandırma, gümrük tarifelerini artırma ve yerel para birimlerinin diğer ülke para birimleri karşısında değerini düşürerek (devalüasyon) ihracatı artırma politikalarını izlemişlerdir (Öztürk, 2011). Söz konusu durum bu politikayı güden ülke için bir takım avantajlar oluştursa da özellikle gelişmekte olan ülkelerin negatif yönde etkilenmesine neden olmuştur. "Komşuyu zarara uğratma" politikası adı verilen bu davranış, küresel ekonomi için içinden çıkılamaz bir durum haline gelmişti (Jefrey & Lake, 2003). Para birimleri arasında konvertibilite dengesizlikleri ortaya çıkmış, dış ticarette ödemelerin gerçekleştirilmesi zorlaşmıştır. II. Dünya savaşı sonrasında bu duruma çözüm yolu olarak Altın Kambiyo sistemi önerilmiştir. Sistem, altının direkt kullanılması yerine altına çevrilebilen bir yabancı para (kambiyo) kullanılmasını içermektedir (Aren, 2007). Çalışmalar sonucunda ABD'nin New Hampshire eyaletinin Bretton Woods kasabasında 1944 yılının Temmuz ayında Birleşmiş Milletler (BM) para ve finans konferansında uluslararası para antlaşması imzalanmıştır. 44 ülkeden 730 delegenin katıldığı anlaşmaya göre katılan ülke paraları için sabit bir kur esası benimsenmiş ve anlaşmaya katılan her ülkenin parasının değerinin, ABD doları esas alınarak saptanması kabul edilmiştir (IMF, 2019). Altın kambiyo

sistemi ile dünya altın stokunun birden fazla ülkeye ait para birimi için karşılık görevi üstlenmesi sağlanmıştır.

Bretton Woods anlaşmasının genel çerçevesi şu şekilde belirlenmiştir (Folkerts & Garber, 2004);

- Anlaşma tarafı olan ülkelerin yerel para birimlerinin değeri, dolara göre saptanmıştır. Dolar ise altın ile dönüştürülebilir tek para birimidir.
- 1 ons altın = 35 dolar ya da 1 dolar 0,88867 gr. altın olarak belirlenmiştir. ABD dolarının diğer para birimlerine ya da altına bu kur üzerinden çevrilmesi kabul edilmiştir.
- Ancak ülkeler, beklenmedik ve çözülmesi imkânsız görünen durumlarda yerel para birimlerinin ABD doları karşısındaki değerini en çok % 10 oranında devalüasyona tabi tutabilirler. Söz konusu düzenleme % 10'u aşacaksa, IMF'den izin alınması şartı getirilmiştir.

Altın kambiyo sistemi ya da diğer adıyla Bretton Woods anlaşması gereği altının dönüştürülebilir tek para birimi olan ABD dolarının, dış ödemeler dengesi fazlasının yaşandığı dönemlerde değerinin artmasına neden olmuştur. Ancak 1950'li yıllarda ABD, soğuk savaş dönemi ve Kore Savaşı sebebiyle askeri harcamalarının ve dış yardımlarının artması sonucu dış ödemeler açığı ile karşı karşıya kalmıştır. Bu nedenle doların küresel ekonomilerde altın karşısında talep edilebilirliği azalmış, ABD'nin sahip olduğu altın stokunun oldukça üstünde bir dolar emisyonu gerçekleştirdiği anlaşıldığından dolara karşı güvenirlilik sarsılmıştır (Seyidoğlu, 2017). Başta Avrupa ülkeleri olmak üzere anlaşmaya taraf ülkeler teker teker altın kambiyo sistemini terk etmiştir. ABD dolarının 1971 yılı itibariyle altın karşısında yaklaşık %9'luk bir devalüasyon yaşaması da ABD'nin de söz konusu sistemi devam ettiremeyeceğini anlamasını sağlamıştır.

Altın para sisteminin ekonomiye sağladığı avantajlar ve dezavantajlar şöyle sıralanabilir (Aren, 2007);

Avantajları;

- Altın para sisteminde tüm ülke para birimlerinin değeri bir kambiyo ya bağlı olması hasebiyle altın nev'inden belirlenebildiğinden dış ticaret ödemelerinde kolaylıkla kurların belirlenmesi sağlanmaktadır.

- İhracatın artması ile ülkede altın stokunun artmakta, artan altın miktarıyla yurt içi fiyatların artması ve böylelikle ithalatın artması sağlanmaktadır. Bu haliyle altın kambiyo sistemi dış ödemeler dengesinin kurulmasında otomatik bir düzenleyici rolü oynamaktadır.
- Para emisyonu, sahip olunan altın miktarıyla belirlendiğinden devletlerin gereğinden fazla para arzında bulunması ve dolayısıyla enflasyonun oluşması önlenebilmektedir.

Dezavantajları;

- Dünya ekonomik faaliyetlerinin artış hızına bağlı olarak ödemelerin altın olarak yapılması gerekliliği, altın rezervlerinin kıtlığı nedeniyle olanaksız bir hale gelmiştir. Ticari ve finansal ödemeleri sorunsuz bir şekilde yerine getirebilmek için bu miktarda bir altın emisyonunu gerçekleştirebilecek altın rezervi ve altın üretim hızı hayatın doğal akışına aykırıdır.
- Paranın özelliklerinden bahsedilirken mutlaka değerli bir madenden yapılması gerekliliği vurgulanmamıştır. Altın gibi değerli bir madenin çıkarılması, işlenmesi ve para olarak basılması oldukça pahalı olmaktadır. Bu işlemleri gerçekleştirilirken kullanılan kaynaklar -emek, zaman- israf edilmektedir. Bu kaynaklar ülke ekonomileri için daha verimli alanlarda kullanılabilmektedir. Özellikle kalkınmakta olan ülkeler için gereksinimlerini karşılayacak kadar para basmaları için elzem altın miktarını ithal etmek oldukça maliyetli ve ekonomileri için olumsuz etkilere sahiptir.

1.3.5. Kâğıt Para Sistemi

Mevcut durumda ülkeler, yerel para birimlerinin emisyonunu ne altın kambiyo sistemine ne de paranın herhangi bir ölçüte bağlandığı bir yapıyla gerçekleştirirler. Siyasal iktidarlar, -şekil ve miktar olarak kendilerinin belirlediği-istedikleri kadar kâğıt paranın arzını gerçekleştirmeye muktedirlerdir (Aren, 1992). Bu yetki ya da güç, sınırsız gibi gözükse de emisyondaki gereksiz fazlalık söz konusu ülke için yüksek enflasyon demektir. Paranın değer bakımından kayba uğraması anlamına da gelen enflasyon olgusu, bir bakıma o paraya duyulan

güveni de temsil etmektedir. Bu bakımdan ülkeler için tedavüldeki yerel paralar o ülkenin güvenirliliğini ya da diğer bir ifadeyle itibarını göstermektedir (Paya, 2007). Mevcut ekonomilerde yerel para birimi olarak kullanılan ve altın karşılığında basılmayan ancak devletin itibarını gösterdiğinden piyasada güvenle kullanılan kâğıt paralar itibari para adıyla anılmaktadır. Paranın kâğıt para halinde; daha az maliyetle ve arzının serbestçe yapılıyor olması ülkelerin ekonomi otoriteleri adına oldukça işlevsel bir para politikası aracı olmasını sağlamaktadır (Hubbard, 2002). Bu yolla da gelir, üretim, istihdam ve dış ödemeler dengesi gibi ekonomik değişkenlere etki etmek kolaylaşmaktadır.

1.3.6. Kaydi Para Sistemi

Para piyasalarının sağlıklı bir şekilde işlemesi, para politikası araçlarının kullanılması ve para arzının belirlenmesinde bankaların yeri ve önemi büyüktür. Bankalar, ekonomilerde atıl durumdaki fon fazlasını fon talep edenlere aktaran, topladıkları mevduatlarla kredi veren, diğer bir ifadeyle paradan para kazanan finans kurumlarıdır (Karan, 2011). Bankalar da para emisyon erkini elinde bulunduran devlet otoriteleri gibi para arzını etkileyen önemli bir kurumdur. Bu işlevini yerine getirirken uhdesinde bulundurduğu vadesiz mevduat hesaplarının belirli bir kısmını önceden belirlenmiş bir oran ölçüsünde ayırmakta, kalan tutarı ise -kendisine yatırılan mevduat miktarının üstünde bir miktarda- kredi vererek para yaratmaktadır. Somut varlığından çok bankaların kayıtlarında oluşturulduğundan banka parası veya kaydi para (Mankiw, 2017) olarak adlandırılan bu para sistemi parasal tabanı etkileyen önemli bir etmendir.

1.3.7. Elektronik Para Sistemi

Bilişim teknolojilerinin ve altyapısının günümüz dünyasında hızla gelişmesi ve büyümesi, ticaret şekillerinde, para sistemlerinin yapısında ve paranın aktarım usullerinde önemli değişikliklere neden olmaktadır. Özellikle bilginin sistemli bir şekilde işlenmesi, saklanması, düzenlenmesi, iletilmesi ve istenildiğinde yeniden değerlendirilmesini kolaylaştıran bilgisayarlar, elektronik ortamda ödemelerin gerçekleştirilmesini ve ticaretin yaygınlaşmasını

sağlamaktadır (Aslan, 2009). Elektronik bir ortamda yine elektronik bir araca yükleme yapılarak kullanılabilen elektronik paralar kart tabanlı veya internet tabanlı olabilmektedir. Bu bağlamda gelişen teknolojik gelişmelerin paralelinde elektronik paralar, banka şubeleri kullanılmaksızın para çekimi, borç ödemeleri ve birçok bankacılık işlemlerinin gerçekleştirilmesini sağlayan ATM (Automatic Teller Machine)'ler, hızlı ve güvenli bir şekilde fon transferini mümkün kılan EFT (Electronic Funds Transfer) sistemleri paranın şekil ve mübadelesinde yaşanan önemli değişikliklere örnek verilebilir.

Kullanımı her geçen gün artan elektronik para sisteminin, işlem maliyetlerini düşürmesi, kayıt dışı ekonomiyi küçültmesi, ülke ekonomilerinin birbiriyle entegrasyonunu pekiştirmesi ve işlem hacmini artırması sebebiyle ekonomik büyümeye katkı sağlaması olumlu yanları olarak sıralanabilir. Sistemin bilişim altyapısından gelebilecek saldırılarla mağduriyetlerin yaşanması, merkez bankasının para kontrolünde yaşayabileceği sıkıntılar, vergi kaçırma ve kara para aklanması gibi işlemlerin takibinin zorlaşması sistemin olumsuzlukları olarak bahsedilebilir (Takan, 2001).

Çalışmanın konusunu oluşturan ve sonraki bölümde incelenecek olan sanal para olgusu da yukarıda bahsedilen teknolojik değişim ve dönüşümün devamı niteliğindeki son örneklerden biridir.

1.4. Para Arzı Tanımları

Bir ülke ekonomisinde para yerine geçen tüm araçların toplam miktarına tedavüldeki para miktarı adı verilmektedir (Cechetti & Scohenholtz, 2011). Ancak söz konusu para miktarının hangi bileşenlerden oluşacağı farklı ekonomik görüşler arasında tartışma konusu olmuştur. Özellikle para politikalarının etkinliği için piyasalardaki paranın miktarının belirlenmesi ve izlenmesi para otoriteleri için önem arz etmektedir (Mishkin, 2015).

Ekonomilerde dolaşımdaki para miktarı teorik olarak yasal tedavül zorunluluğu olan paralar ve para yerine geçen kıymetler olarak iki ana gruba ayırılarak incelenmektedir (Aren, 2007). Yasal paralar, devletler tarafından piyasaya sürümü yapılan, her türlü ödeme işleminde kabulü zorunlu ve gücünü yasalardan alan paraları, para yerine geçen kıymetleri ise değişim aracı olarak

kullanılan ancak yasal paralara nispeten likiditesi düşük vadeli ve vadesiz mevduat hesapları, hazine bonoları ve devlet tahvillerini temsil etmektedir. Yasal para hüviyetinde bulunan paraların, para yerine geçen kıymetlerden daha likit olması, para arzının değişik tanımları yapılırken dikkate alınmaktadır. Bu nedenle temel para arzı tanımlarının öncelikle paranın ilk ve en önemli özelliği olan değişim aracı olma vasfından hareketle oluşturulması gerekliliği göz önünde bulundurulmaktadır (Özbilen , 2016). Buradan yola çıkılarak merkez bankası para arzı tanımları Tablo 3'de gösterilmiştir (TCMB, 2018).

Tablo 3
Para Arzı Tanımları

M1 Kâğıt Para + Madeni Para + Vadesiz Mevduatlar + Vadesiz Mevduatlar
M2 M1 + Vadeli Mevduatlar
M3 M2 + Repo + Para Piyasası fonları + İhraç Edilen Menkul Kıymetler

1.5. Merkez Bankası ve Para Politikası Araçları

Merkez bankaları için finans literatüründe ortak bir tanımlama yapılamasa da genel görüş açısından merkez bankalarının devlet adına para basan, para ve döviz politikalarını belirleyen ve yönlendiren kurumlar oldukları ifade edilebilir (Erdem, 2016). Dünyada merkez bankacılığının ilk örneği İngiltere'de 17.yy sonlarında görülse de bugünkü anlamıyla merkez bankası işlevinde faaliyet göstermeleri 19. yy 'a rastlamaktadır. Merkez bankalarının gelişimi, madeni paradan kâğıt paraya geçişi müteakiben bankaların para yaratma vasfının ortaya çıkması ile yaşanmıştır (Öztürk, 2011).

Türkiye'de merkez bankacılığı adına ilk adım, Osmanlı Devletinden miras alınan ve İngiliz-Fransız ortak sermayesiyle 1863 yılında kurulmuş Osmanlı Bankası'dır. Bu banka Türkiye Cumhuriyetinin kurulması akabinde de görevine devam etmiş, milli bir merkez bankasının kurulması gerekliliği yönündeki

çalışmalar sonucunda 1931 yılında Türkiye Cumhuriyet Merkez Bankası kurulmuştur. Kuruluş döneminden bu yana ortaklık yapısı farklılıklar gösterse de hâlihazırda anonim şirket statüsünde %55 devlet hazinesi, %25 Türkiye de faaliyette bulunan milli bankalar, %0,02 milli bankalar dışında kalan diğer bankalar, %19,8'i Türk uyruklu gerçek ve tüzel kişiler sermaye ortaklığı ile faaliyetlerini sürdürmektedir (TCMB, 2018).

1.5.1. Merkez Bankasının İşlevleri

Merkez bankalarının geçmişten bu yana kuruluş amaçları her ne kadar para basma ve para arzının kontrolü olsa da ekonomik araçların, teknolojinin ve finansal entegrasyonların gelişmesiyle görev ve yetkilerinde de çağın gerektirdiği ölçüde değişimler olmaktadır.

Günümüz merkez bankalarının temel işlevleri Türkiye Cumhuriyet Merkez Bankası örnek alınarak Tablo 4'de belirtilmiştir (TCMB, 2018).

Tablo 4
Merkez Bankasının İşlevleri

Banknot Basma	Bir ülke için egemenlik ve bağımsızlık sembolü olan para emisyonunu gerçekleştirmesidir.
Para Politikası Uygulama ve Fiyat İstikrarını Sağlama	Merkez bankalarının temel görevi olan fiyat istikrarının sağlanması amacıyla para politikası araçlarını kullanmasıdır.
Finansal Sistemin İstikrarını Sağlama	Merkez bankalarının finansal sistemin merkezinde olması ve bu mekanizmanın çalışmasını sağlama görevini üstlenmesidir.
Ödeme Sistemlerinin Denetimi	Merkez Bankalarının kanunlardan aldığı yetkiyle para ve menkul kıymetlerin güvenli ve hızlı bir şekilde transfer edilebilmesi için ödeme ve menkul kıymet transferi ve mutabakat sistemleri kurma, kurulmuş ve kurulacak sistemlerin kesintisiz işlemesini ve denetimini sağlayacak düzenlemeleri yapma görevidir.
Döviz Kuru Politikası Uygulama	Kamu otoritesinin ekonomik ve finansal hedeflerinden sapma görüldüğü durumlarda merkez bankası tarafından döviz kurunu değiştirmeye yönelik doğrudan müdahalelerde bulunarak fiyat ve finansal istikrara tehdit oluşturabilecek durumların engellenmeye çalışılmasıdır.
Rezerv Yönetimi	Ülkenin altın ve döviz rezervlerini saklamak ve yönetmektir.

1.5.2 Para Politikası Araçları

Merkez bankasının hükümetle birlikte, belirlenen makroekonomik hedefler için uyguladığı para politikaları, ekonomideki sorunların nedenleri ve finansal gelişmelere bağlı olarak çeşitlilik göstermektedir. Merkez bankalarının para politikalarını uygularken kullandığı araçların kapsamı Tablo 5'te sunulmuştur.

Tablo 5
Para Politikası Araçları, Uygulama Alanları ve Amaçları

Politika	Uygulama	Amaç
Açık Piyasa İşlemleri	Merkez Bankasının piyasalar aracılığı ile devlet tahvili, hazine bonosu ve özel sektöre ait tahvil veya senetlerin alım satımını gerçekleştirdiği işlemlerin tümüne verilen addır.	Alım satım işlemleri ile para arzını kontrol etmek, piyasalardaki likiditeye etki etmek.
Reeskont Oranları	Bankaların piyasalardan iskonto ederek aldıkları senetlerin yeniden iskonto karşılığında fon talepleri nedeniyle yeniden iskonto ederek (reeskont) merkez bankasına vermesidir.	Piyasalardaki likidite miktarını ve fonlama faiz oranlarını düzenlemek.
Zorunlu Karşılıklar	Bankalar tarafından toplanan fonların (mevduatların) belirlenen yasal miktar kadarının Merkez Bankası uhdesinde tutulması zorunluluğudur.	Bankaların kaydi para yaratma olanaklarını etkileyerek piyasadaki para miktarını düzenlemek.
Kredi Tavanı Belirlenmesi	Bankaların kullandırdıkları kredilerin üst limitinin belirlenmesidir.	Kredi tavanı uygulamasıyla bankaların kullandırabilecekleri kredi miktarını, böylelikle de piyasadaki nakit miktarını kontrol edilebilmek.
Merkez Bankasının Moral Takviyesi (Moral Suasion)	Merkez Bankasının gerçekleştirdiği veya yapmayı planladığı politikaların, Merkez Bankası tarafından basın açıklamaları yapılarak ya da telkin yoluyla bankalar ve diğer finansal aracıların beklentilerini etkilemeye çalışılmasıdır.	Moral takviyenin uygulanması, bankaların aktif-pasif pozisyonlarını etkilemekte, bankalar bu yolla, kredilerine belirli üst limitler getirmekte, faiz oranlarını yükseltmektedir. Böylelikle fonlama faizlerine ve fon miktarlarına etki edilebilmektedir.

Not: Bu tablo, TCMB'nin web sitesinde bulunan bilgiler kullanılarak yazar tarafından oluşturulmuştur.

İKİNCİ BÖLÜM

2.KRİPTOLOJİ, BLOKZİNCİR (BLOCKCHAİN) TEKNOLOJİSİ VE SANAL (KRİPTO) PARALAR

2.1. Kriptolojinin Tanımı ve Kriptolojinin Tarihi

Kriptoloji, kelime anlamı olarak Latince gizli, bilinmeyen anlamına gelen "cyripto" ve çalışma/bilim anlamına gelen "logi" kelimelerinden oluşmakta, "cryptology" ise bilinmeyen üzerine yapılan çalışma disiplinini ifade etmektedir (Dooley, 2013). Literatürdeki bir diğer anlamıyla kriptoloji, gizlilik, bütünlük, kimlik denetimi, inkâr edememe gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünü olarak da tanımlanmaktadır (Yerlikaya & Buluş, 2006).

İnsanların günlük yaşamlarında çevreleriyle iletişimlerinde, devletlerin ve kurumların birbirleri arasında gerçekleştirdikleri enformasyon akışında ihtiyaç duydukları iki önemli faktör vardır; gizlilik ve doğruluk. Başkalarının görmesini istemediğimiz bilgilerin özellikle teknolojinin her geçen gün geliştiği günümüzde güvenliğini korumak daha da güçleşmektedir. Bu problemin yalnızca yaşadığımız zamana ait olmayan, tarihsel süreç içerisinde süre gelen bir gereksinim olduğu görülmektedir. Eski Mısır kalıntılarında bulunan ve M.Ö 4000 yıllarında yazılmış olduğu tahmin edilen bir biyografinin içerisine serpilmiş gizli anlamlar taşıyan semboller ve resimler, yazarının farkında olmadan bir bilim dalına öncülük ettiğinin habercisidir (Babaoğlu, 2018).

Mısırda bulunan söz konusu hiyerografilerden yaklaşık 3000 yıl sonra Roma İmparatoru Julius Caesar da, ordu komutanlarına gönderdiği mektuplarında gizlilik konusuna önem vermiş ve metin içerisindeki yazıları, her harfin yerine alfabedeki yerlerine göre kendisinden sonra gelen üçüncü harfle değiştirip şifreleyerek yazmıştır (Çeşmeci, 2009). Caesar şifresi olarak anılan algoritma aşağıdaki gibi formüle edilebilir;

S=M+3 (mod26) burada; S açık metin harfini M gizli metin harfini göstermektedir.

Bu teknik o dönemde metinleri anlaşılabilir hale getirebilecek basit analizlerin dahi bilinmemesi nedeniyle uzun zaman boyunca başarıyla kullanılmıştır. Diğer taraftan Araplar M.S 6.yy' dan başlayarak "cifr" ya da "cifir" olarak adlandırdıkları, Arap harflerinin her birine verilen bir sayısal değerle birlikte dilin kendi yapısal özelliklerinden kaynaklanan bir takım harflerin yan yana gelememesi kuralı işletilerek gizli haberleşme teknikleri kullanmışlardır. Şifre anlamına gelen Fransızca "chiffre" ve İngilizce "cipher" sözcükleri de "cifir" kelimesinin söz konusu dillerdeki karşılığı olmuştur (Babaoğlu, 2018). Kriptoloji tarihinin önemli basamaklarından biri de Alberti 'nin kodlamayı ve şifrelemeyi birleştirerek bir başka önemli başarıya daha imza atmasıdır: Şifreli Kod. Alberti 'nin keşfi olan disklerde harflerle birlikte bulunan dört rakam kodlama amacıyla kullanılıyordu (Lois, 1989).

Julius Caesar'dan 1586 yılında Blaise de Vigenere (1523-1596)'in ilk kez açık metin ve şifreli metinlerin anahtarlanarak şifrelenmesinden bahsettiği kitabına kadar kriptoloji biliminde önemli bir gelişmenin yaşanmadığı ileri sürülebilir.

Vigenere'nin şifreleme algoritması, çoklu alfabetik yer değiştirme yöntemi olarak da bilinen ve periyodik olarak belirli bir anahtar değerinde yer değiştirme uygulanan algoritmadır. Algoritmada K anahtarı bir dizi harf olarak belirlenir. Bu durumda K = k1, k2,.... kn olarak gösterilen ifadede kullanılan k; değeri i=l,2,...,n olmak üzere, alfabede yapılması gereken i'nci ötelemeyi gösterdiğinde, şifreleme sonucu elde edilen harf, f(a) = a + ki (mod n) (n = 26) biçiminde gösterilir (Yerlikaya & Buluş, 2006).

Bütün bu çabaların ortak nedeni, bir bilginin belirli bir yöntemle karmaşık hale getirilip istenmeyen taraflarca anlaşılmamasını sağlamak ve yine bilgiye dışarıdan herhangi bir müdahalenin engellenmesidir. İşte kriptoloji biliminin de amaç ve yöntemi tam da bu ifadede karşılığını bulmaktadır.

Kriptoloji, kullanılmaya başladığı ilk dönemlerden itibaren günümüze kadar teknolojik, siyasi ve askeri olaylarında etkisiyle önemli gelişmeler göstermiştir. 1623'de Sir Francis Bacon tarafından 5-bit ikili kodlama ve karakter

tipi değişikliğine dayanan stenografinin bulunması yeni bir çağın başlangıcının ilk adımlarıdır. 1920'li yılların başlarında Amerika Birleşik Devletlerinde (ABD) Federal Araştırma Bürosu (FBI) içki kaçakçılarının haberleşmelerin tespiti ve çözümlenmesi üzerine özel bir büro kurarak kriptografik metinleri deşifre etmeye çalışmıştır. Arthur Scherbius tarafından icat edilen ve II. Dünya savaşının seyrini önemli bir süre Almanlar lehine çeviren şifreleme makinesi Enigma, Alan Turing ve ekibi tarafından yine kripto analiz yöntemleri sayesinde çözülmüş, savaşın sonucu bu gelişmeyle önemli şekilde etkilenmiştir (Sarıtaş, 2015).

20. Yy'in ortalarında kriptoloji alanındaki diğer önemli gelişmeler, kronolojik sırasıyla; Horst Feistel, Data Encryption Standard'ın (DES) temelini oluşturan Lucifer algoritmasını geliştirmesi ve bu algoritmanın ABD tarafından Federal Information Processing Standard 46 (FIPS 46) standardı olarak açıklanması, Martin Hellman ve Whitfield Diffie'nin açık anahtar sistemini anlattıkları makaleyi yayınlamaları, ardından Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman, Rivest Shamir-Adleman (RSA) algoritmasını bulmaları, 1985'de Neal Koblitz ve Victor S.Miller'ın Eliptik Eğri Kriptografi (ECC) sistemlerini tarif ettikleri makalelerini yayınlamaları, ABD Ulusal Teknoloji ve Standartları Enstitüsü (NIST)'nün 1985 yılında Secure Hash Algorithm (SHA-1) özet algoritmasını, 2001'de ise Belçikalı Joan Daemen ve Vincent Rijmen'e ait Rijndael algoritmasını Advanced Encryption Standard (AES) adıyla standart haline getirilmesi olarak sıralanabilir (Bayar, 2012).

Kriptoloji, şifreleme bilimi kriptografi ve bu şifrelerin kırılarak anlamlı metinlere dönüştürülmesini sağlamak amacını güden kripto analiz bölümlerinden oluşmaktadır.

Kriptolojinin alt dalı olan kriptografi, diğer adıyla şifreleme işlemleri, günümüzde kullanılan bilgi güvenliği sistemlerinin (bilgisayar ve haberleşme araçları) sağlıklı işleyişinde önemli ve yaygın bir metot olarak kullanılmaktadır (Moldovyan, 2006).

2.2. Kriptolojinin Amaçları

Her türlü iletişim kanalının istenmeyen kişiler tarafından birçok müdahaleye açık olabileceği herkesin malumudur. Bir mektubun alıcısına

ulaşıncaya kadar içeriğinin öğrenilemediğine veya değiştirilemediğine emin olunamayabilinir. Dijital ortamlarda iletilen herhangi bir e-postanın kimden geldiği, içeriğinin değiştirilip değiştirilmediği ve doğru alıcıya ulaşıp ulaşamadığının tespiti ve güvenliği, söz konusu e- postanın iletildiği ortamın özellikleri göz önüne alındığında, ortamda bulunan bilgisayar kullanıcılarının sayısı kadar şüphenin doğmasına neden olur ki, bu durum çok büyük bir olasılığı barındırır. Dolayısıyla bilginin gizliliğini ve güvenliğini sağlamak için kullanılacak şifreleme, çoğu zaman hayati öneme sahiptir. Kriptografik yöntemlere geçmeden önce bu yöntemlerin hangi amaçlar doğrultusunda çalıştığını bilmek gereklidir. Kriptolojik yöntemlerin ilgilendiği tehdit unsurları olarak da değerlendirilebilecek bu amaçlara Tablo 6'da yer verilmiştir (Akleylek, Yıldırım, & Tok, 2011).

Tablo 6
Kriptolojinin Amaçları

Gizlilik	İletilen bir bilginin alıcıya varmadan önce istenmeyen kişilerce öğrenilmesini veya bu bilginin içeriğine müdahale edilmesini engellemeyi amaçlamaktır.
Bütünlük	Saklanan bir bilginin içeriğinin değiştirilmeden, alıcıya ulaşan iletinin ulaştırılmak istenen bilgiyle aynı olduğunun tespiti ve sağlamasının yapılabilir olmasını amaçlamaktır.
Reddedilemezlik	Bilginin, onu oluşturan kişi tarafından reddedilememesini yani kendisi tarafından gönderildiğini inkâr edememesini amaçlamaktır.
Kimlik Belirleme	Bilginin veya iletinin göndericisinin ve alıcısının kimliklerinin karşılıklı olarak doğrulanabilir olmasını, başka birinin gönderen veya alıcının kimliğine bürünememesini sağlamayı amaçlamaktır.

2.3. Kriptoloji Yöntemleri

Yukarıda kriptolojinin tarihi gelişiminin anlatıldığı kısımda da yer verildiği gibi kriptolojinin uygulanmaya başlandığı ilk dönemlerden günümüze kadar gerçekleşen teknolojik gelişmelerle birlikte kriptolojik yöntemlerde de önemli değişiklikler yaşanmıştır. Bu nedenle kriptolojik gelişmeleri iki ana gruba ayırarak incelemek mümkündür (Stalling, 1998).

- Klasik Şifreleme Yöntemleri,
- Modern Şifreleme Yöntemleri'dir.

2.3.1. Klasik Şifreleme Yöntemleri

Tarihi kronolojik süreçte kriptoloji biliminin ilk örneklerinden başlayarak 20. yy'in ilk yarısına kadar ki dönem içeresinde kullanılan şifreleme yöntemleri bu grup altında yer almaktadır. Bunlar;

- Julius Caesar 'ın şifreleme yöntemi
- Zodyak'ın şifreleme yöntemi
- Blaise de Vigenere çoklu alfabetik yer değiştirme yöntemi
-Joseph Mauborgne ve Gilbert Vernam tek kullanımlık sistem (One-Time Pad, OTP) yöntemi
-II. Dünya savaşında Almanların kullandığı Enigma şifreleme yöntemidir (Cormen & Leiserson, 2009).

Söz konusu klasik şifreleme yöntemlerinde karşılaşılan ve modern şifreleme yöntemlerinin doğmasını sağlayan dezavantajlı durumları ise şu şekilde sıralanabilir (Koblitz, 2006);

- Klasik yöntemlerin modern teknolojik gelişmelerin arkasında kalmıştır.
- Klasik şifreleme yöntemlerinin her birinin kripto analizleri yapıldığından geçersiz hale gelmişlerdir.
- Klasik şifreleme de kullanılan anahtarlar, bilginin ulaşması istenen her alıcıda bulunması gerektiğinden bu sistem önemli ölçüde açık anahtar dağıtım problemine sahiptir.
- Klasik sistemler yalnızca askeri işlemlerde kullanılabilen dar bir kullanım alanına sahip olmuşlardır (Koblitz, 2006).

2.3.2. Modern Şifreleme Yöntemleri

Hiç kuşku yok ki son teknolojik gelişmelerin kullanıldığı modern şifreleme yöntemleri, yukarıda açıklanan klasik şifreleme yöntemlerinin dezavantajlarını ortadan kaldırmış ve daha başarılı kriptolojik sonuçlar meydana getirmiştir. Bu gelişmeler aşağıdaki maddelerde açıklanmaya çalışılmıştır (Ryabko & Fionov, 2005);

- Modern şifreleme yöntemleri kriptoloji biliminin standart bir yapıya kavuşmasını sağlamıştır. Bu standart temeller şifreleme yönteminin kendinden sonraki teknolojik gelişmelere bağlı olarak daha üstün hale getirilmelerini kolaylaşmıştır.
- Açık Anahtar (Public Key) 'ın keşfi ile şifrelenen bilgilerin kripto analizleri önemli ölçüde zorlaşmıştır.
- Güvenlik tanımlamalarının biçimlendirilmesi sağlanmıştır.

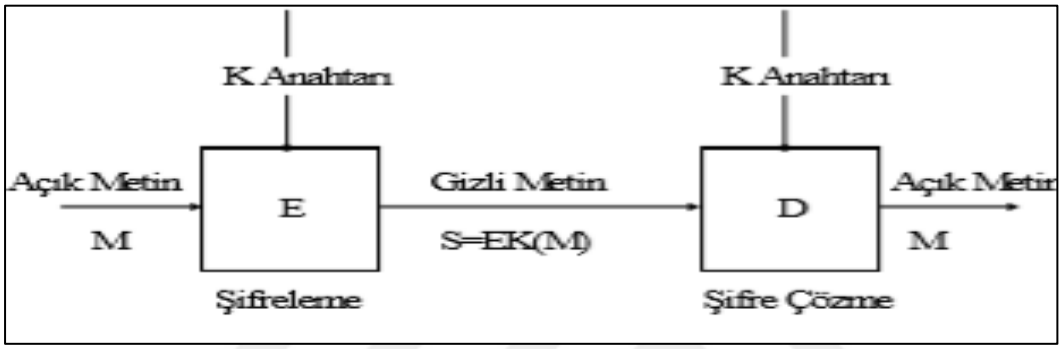
Modern şifreleme yöntemleri günümüz teknolojik temellerinde üç gruba ayırılmaktadır.

2.3.2.1. Simetrik (Gizli Anahtarlı) Şifreleme Sistemi

Simetrik şifreleme yöntemlerinde şifreleme ve deşifrelemede gizli anahtar tek 'dir. Bu aynı anahtar gönderici ve alıcı tarafından ortak kullanılır. Blok ve akan şifreler simetrik şifreleme grubuna girmektedir. Simetrik şifreleme sistemlerinde kullanılan anahtarlar kişiler arasında gizli tutulduğu için bu şifreleme tekniğine gizli anahtarlı şifreleme sistemi de denir (Schneier, 1996). Bu sistemde önemli olan şifrelemenin yapılacağı ve şifrenin çözüleceği anahtarın tüm kişiler arasında ortak bir anahtar olmasıdır. Ayrıca bu anahtarın istenmeyen kişilerin eline geçmesini engellemek gerekmektedir. Kullanılan şifrenin karmaşıklığı ve güvenli bir şekilde saklanması elbette istenen gizliliği sağlayacaktır. Ancak bilginin ulaştırılmak istenen kişi sayısının fazla olduğu durumda bunu gerçekleştirmek oldukça güç olabilmektedir. Çünkü ortamda bulunan her alıcının söz konusu bilgiye haiz olması istenmeyebilir, herhangi iki kişi arasındaki özel bilgiler anahtar sahibi herkes tarafından bilinecektir. Her bir birey arasında ikili gizli anahtarların oluşturulabileceği varsayıldığında ise anahtar

sayısı topluluğun sayısına "n" denilirse; $\frac{n(n-1)}{2}$ sayısı kadar farklı anahtar sayısına ulaşılır ki bu sayıda farklı anahtarın işleri zorlaştıracağı, bu kişilerden herhangi birinin şifrenin güvenliğini sağlayamaması tüm kişileri etkileyecektir.

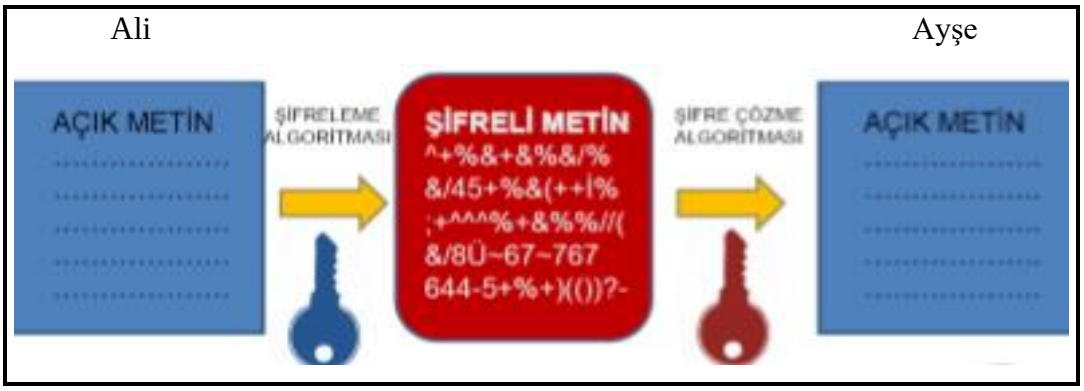
Simetrik şifreleme sisteminin çalışma prensibi şekil 6'da sunulmuştur. Bura da M açık metni, E ve D harfleri sırasıyla kriptolama ve kripto çözme algoritmalarını, K ise ortak kullanılan gizli anahtarı temsil ettiğinde, gizli metin $S = E_K(M)$ formülüyle gösterilebilir (Yerlikaya & Buluş, 2006) .



Şekil 1 Simetrik Anahtar'da Şifreleme

2.3.2.2. Asimetrik (Açık Anahtarlı) Şifreleme Sistemi

Asimetrik şifreleme algoritmalarında şifreleme safhasında gizli bir anahtar kullanılırken, deşifre için herkes tarafından kullanılabilen bir açık anahtar bulunur. Diğer bir ifadeyle açık anahtarlı sistem, şifreleme ve şifre çözme işlemleri için farklı anahtarların kullanıldığı sistemdir. Gizli anahtar sisteminde yer alan anahtarın alıcıya iletilmesi sorununa karşın bu sistem tarafından getirilen çözüm sayesinde bu problem çözülmüş oldu. Şöyle ki; alıcının özel (Private Key) ve açık (Public Key) anahtar çifti algoritmalarını oluşturarak açık anahtarı göndericiye iletmesi ve aldığı iletiyi kendinde bulunan özel anahtarla kripto analizini yaparak açık metin haline getirmesi ile gerçekleştirilmektedir (Oppliger, 2005). Gönderici ve alıcı arasındaki açık anahtar farklı kişilerde bulunsa bile özel anahtarın güvenliği korunduğu müddetçe alıcı dışında hiç kimse iletinin içeriğine haiz olamamaktadır.



Kaynak; (Akleylek, Yıldırım, & Tok, 2011)

Şekil 2 Açık Anahtar Şifreleme Sistemi

Şekil 4'te Ali'nin Ayşe'ye göndermek istediği açık metin, Ali tarafından Ayşe'nin herkesçe bilinen açık anahtarıyla şifrelenerek Ayşe'ye gönderilir ve yalnızca Ayşe'de bulunan gizli anahtarla deşifre edilerek tekrar açık metin haline dönüştürülür.

2.3.2.3. Hash Algoritmaları

Hash algoritmalarındaki özgünlük, şifrelenmiş verilerin belirli bir standart büyüklük içinde yer almalarıdır. Bir sonraki başlık altında ayrıntılı şekilde açıklanacak olan blokzincir teknolojisinin güvenlik altyapısını oluşturan Hash algoritmalarının blok yapıları, bu belirli standart yapıyı ifade etmektedir. Hash algoritmaları, simetrik ve asimetrik şifreleme algoritmalarına nazaran kimlik denetimi açısından daha büyük bir öneme sahiptir.

Hash kelime anlamı olarak "doğrulamak/özel iz ya da parmak izi" anlamlarına gelmektedir (Balcısoy, 2017). Diğer şifreleme yöntemleri gibi bir bilgiyi istenmeyen kişilerin müdahalesinden korumak asıl amaç olmakla birlikte bir bilginin, belgenin ya da verinin özgünlüğünü ispatlamak için de kullanılır. SHA (Secure Hash Algorithm), herhangi türde bir verinin (belge, resim vb.) hangi uzunlukta olursa olsun sabit uzunlukta çıktı haline getirebilen bir algoritmadır (Dadda & Machetti, 2004). Bununla birlikte söz konusu belgede gerçekleştirilecek en küçük bir değişiklik farklı bir Hash değerine neden olacağından özet belge Hash'i ile bizdeki Hash algoritması karşılaştırıldığında verinin özgünlüğü ispatlanmış olacaktır.

Hash fonksiyonları tek yönlü olduklarından Hash'lenmiş bir verinin geriye yönelik olarak çözümlenmesi ve değişiminin yapılması olanaksızdır. Değiştirmek için söz konusu fonksiyona müdahalede bulunmak tamamen farklı bir Hash değerinin oluşmasına ve yapılan en küçük bir müdahalenin dahi sistemde fark edilmesine neden olacaktır (Grembowski & Lien , 2002). Bununla birlikte farklı girdilerle aynı Hash değeri üretilemeyeceğinden random sayılarla şifreleme tekniklerine göre daha güvenli bir şifreleme kullanılmış olur. Özetle bir Hash fonksiyonun ayırt edici özellikleri aşağıdaki gibi sıralanabilir;

- Hash fonksiyonu diğer şifreleme tekniklerinde kullanılan sayısal şifrelere göre kolayca oluşturulur;
- Hash şifresinin çözümlenmesi, yani başlangıçtaki verilerin Hash değerine göre yeniden oluşturulması imkânsızdır;
- Farklı girdi verileri için aynı Hash değeri üretmek mümkün değildir.

Sanal para birimlerinde kullanılan ve yukarıda özellikleri verilen SHA'lar (Secure Hash Algorithm) Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı (NSA) tarafından sayısal imza standardı olarak kullanılmaları için tasarlanmıştır. İlk olarak SHA0 1993 yılında oluşturulduktan sonra yaşanan güvenlik açıkları sebebiyle sırasıyla SHA1 ve SHA2 olmak üzere diğer sürümleri kullanılmaya devam etmiştir. Blokzincir teknolojisinin altyapısında kullanılan ve SHA2'nin altında çalışan dört farklı fonksiyondan biri olan SHA256 her bir girdiyi 256 bitlik uzunlukta çıktı haline getirdiğinden bu ismi almıştır (Cormen & Leiserson, 2009).

2.4. Blokzincir (Blockchain) Teknolojisi

Bu bölümde, sanal (kripto) paraların ortaya çıkması ile birlikte bilinirliği ve kullanımı artan, sanal paraların teknolojik alt yapısını oluşturan, gelecekte hayatın birçok alanında sıklıkla karşılaşılabilecek blokzincir (blokzincir) teknolojisi anlatılmaya çalışılacaktır.

Blokzincir teknolojisi için -önemli bir teknolojik gelişme olmasına karşın- yeni olarak adlandırılabilecek geçmişi nedeniyle akademik yazın literatüründe araştırmacılar tarafından ortak bir tanım kullanılamasa da bu yeniliğin öncüsü Satoshi Nakamoto'nun açıklamaları ile blokzincir 'in ne olduğuna dair bilgi edinilebilir.

Blokzincir teknolojisi, 2008 yılında kimliği tam olarak bilinmeyen bir kişi olan –belki de takma bir isim kullanan- Satoshi Nakamoto'nun yayınladığı makale de kelime olarak geçmese de "birbirlerine zincirlenmiş diziler halindeki veri blokları" (Nakamoto, 2008) olarak tanımlanmış ve ilk sanal para örneği Bitcoin ile somut hale gelmiştir. Sonraki dönemlerde söz konusu teknolojinin yapısında yer alan "blok ve zincir" kelimelerinin birleştirilmesiyle blokzincir adını almıştır. Satoshi 'nin yayınladığı ve Dünya da çığır açan gelişmelere neden olan makalenin içeriği, blokzincir ve bu teknolojinin nasıl oluşturulacağı ve neler başarılabileceği çalışmamızın ileriki safhalarında anlatılacaktır. Elbette blokzincir teknolojisi yalnızca sanal para birimlerinin hayata geçirilmesinde kullanılmamaktadır. Ancak çalışmamızın konusunu oluşturduğu için, blokzincir teknolojisi sanal para sistemindeki teknik alt yapı ve çalışma sistemi temelinde ele alınacaktır.

2.4.1. Dağıtık Defter Teknolojisi (Distributed Ledger Technology)

Günlük yaşamda insanlar, kurumlar ve devletlerarasında gerçekleştirilen birçok veri akışının kayıt altında tutulması ve güvenliğinin sağlanması önemli bir durumdur. Küçük işletmelerden, aylık harcamalarını not alan bir öğrenciye kadar herkes güvenliği, doğruluğu ve gerektiğinde ibraz edilebilmesi için bilginin kayıt altında bulunmasını isteyebilir.

Örneğin bir arkadaş grubunun aralarında para alış verişi yaptıklarını ve ödemelerini kayıt altında tuttuklarını varsayalım. Ali, Metin, Hasan ve Ayşe her işlemin ardından kendilerine gelen ve yaptıkları ödemeleri bir deftere yazmaktadırlar. Bu şekilde her birinde ayrı ayrı dört defterin bulunması gerekmektedir. Yılın sonunda yapmış oldukları işlemleri karşılaştırarak işlemlerin gerçekleştiğinin doğruluğunu ibraz etmeye çalışmaktadırlar. Ancak bu durumda önemli bir sorun ortaya çıkacaktır. Her birinin defterinde yer alan bilgiler gerçeği tam olarak yansıtmakta mıdır? Karşılıklı ödeme işlemleri birbirini tutmakta mıdır? Ayrıca bu bilgilerin kaybolması, bozulması, silinmesi veya saldırıya uğraması olanak dışında mıdır?

İşlemlerin gerçekleştiğini kayıt altına alan, gruptaki herkes tarafından güvenilirliği kabul edilmiş merkezi bir otoritenin bulunması halinde bu sorunlardan bahsedilemeyecektir. Ancak aksi durumda işlemler birbirlerini

tanıyan kişiler arasında dahi güvensizliğe neden olacaktır. Söz konusu işlemlerdeki güvenirlilik sorunu gruptaki herkes tarafından kullanılabilen, yapılan her değişikliğin, yazan kişinin kimliği ile birlikte yer aldığı, daha önceki yazılan bilgilerin ise kimse tarafından değiştirilemediği ortak tek bir defter de tutulması ile halledilebilecektir. İşte dağıtılmış hesap defteri teknolojisi (DLT) adı verilen bu yapı yukarıda yer verdiğimiz güvenlik ve doğruluk sorunlarını ortadan kaldıran, kriptografik şifreleme işlemleri ile her bir işlemin kayıt altına alındığı, herkes tarafından görülebilen, değiştirilemeyen ve ortak kullanılabilen bir kayıt sistemidir (Natarajan, Krause, & Gradstein, 2017).

Blokzincir teknolojisinin altında yatan yenilik ve özgünlük de dağıtılmış hesap defterleri sisteminin bir uygulaması olmasıdır. Blokzincir teknolojisiyle herhangi bir sistemde birbirini tanımayan kişiler arasında her türlü belge, bilgi ve değer aktarımı, birbirlerine güven duymaksızın ve merkezi bir otoritenin bulunmadığı söz konusu dağıtık yapıyla mümkün olmaktadır (Tapscott, 2016). Buradan yola çıkarak sistem ağlarındaki kişiler arasında dağıtılmış hesap defteri teknolojisi (DLT) sisteminin blokzincir teknolojisi alt yapısıyla işleyişini sırasıyla şöyle açıklanabilir;

- Blokzincir tabanlı DLT sistemleri, yalnızca yeni eklenen verilerden oluşan blok zinciri şeklindedir. Veri tabanına yapılan eklemeler sistemdeki üyelerden biri tarafından başlatılır.
- Eklenen yeni veri sistemdeki üyelerle paylaşılır, söz konusu veri şifrelenmiş olduğundan ağ dışına çıkmaz.
- Sistem içerisinde bulunan tüm üyeler, oluşturulan yeni veri bloğunun geçerli olduğuna daha önceden tanımlanmış algoritmik doğrulama metoduna (konsensüs mekanizması) uygun şekilde karar verir (Nakamura & Matsutani, 2017). Bu doğrulama sonunda veri bloğu diğer üyeler tarafından kendi defterlerine de kaydedilmiş olur. Bu mekanizma ile defterde gerçekleşen her değişimin bir kopyası ağda bulunan herkeste bulunur.

2.4.1.1. DLT’nin Avantajları

Dağıtılmış hesap defterleri, geleneksel merkezi defterlere ve diğer ortak defterlere göre potansiyel olarak çeşitli avantajlara sahiptir. DLT'nin en önemli potansiyel avantajları aşağıda listelenmiştir ancak, herhangi bir blok zincirin sahip olabileceği çok çeşitli tasarım ve özelliklerden dolayı karşılaşılabilecek her türlü DLT için bu özellikleri genellemek mümkün olamayacaktır (Berentsen & Schär, 2018).

Âdemi merkeziyetçilik ve Aracının Bulunmaması; DLT, iki taraf arasında doğrudan dijital değer (belge, resim, sanal para vb.) aktarımı sağlar ve merkezi olmayan kayıt tutma; defteri kontrol eden aracı ya da merkezi otorite ihtiyacını ortadan kaldırır. Bu da daha düşük maliyetlerle işlemleri gerçekleştirmeye, daha iyi ölçeklendirilebilirliğe ve piyasada daha hızlı hareket etmeye neden olmaktadır.

Şeffaflık ve Kolay Denetlenebilirlik; Tüm ağ üyelerinde dağıtılmış hesap defterinin şifrelenmiş tam bir kopyası bulunduğundan değişiklikler ancak fikir birliği sağlandığında ve gerçek zamanlı olarak tüm ağa yayılırsa yapılabilir. Bu özellik, merkezi bir otorite eksikliği veya merkezi bir otoritenin sınırlı katılımıyla birleştiğinde, sahtekârlığı azaltma ve uzlaşma maliyetlerini ortadan kaldırma potansiyeline sahiptir.

Otomasyon ve Programlanabilirlik; DLT önceden kararlaştırılmış bir program çerçevesinde işlemlerin gerçekleştirilmesini mümkün kılar. Diğer bir ifadeyle mutabık kalınan programın otomatik olarak yürütülmesini sağlar. Buna “akıllı sözleşmeler” denir. Örneğin, bir gönderimin ulaştığı anda ödemesinin yapılması ya da sözleşmenin yerine getirilmesi durumunda kendilerine ödeme yapılacaklar ve yine ödemesi işin tesliminde gerçekleşecek faturalar gibi. Akıllı sözleşmeler geleneksel merkezi muhasebe sistemlerinde de yapılabilir, ancak merkezi muhasebe sistemlerinin tasarımından kaynaklanan nedenlerle, ödemeler ve fatura kesimleri söz konusu işlemlerin ancak ilgili tarafların merkezi sistemde kaydedilmiş olan temel işlemi kabul etmesinin ve mutabık kalınmasının ardından yapılabilir (Zyskind , Nathan, & Pentland, 2015). Buna karşılık, DLT’de, taraflar tanım gereği, işlemin tamamlandığı anda, her ikisinde de işlemin gerçekleştiğine dair kayıt oluşur.

Ölçülebilirlik ve Doğrulanabilirlik; DLT, herhangi bir dijital veya fiziksel varlığın işlemlerinde değişmez ve doğrulanabilir bir denetim izi sağlar. İşlemlerin doğruluğu ve yerindeliği basit ve güvenli bir şekilde kontrol edilebilir.

Hız ve Verimin Artırılması; DLT, işlemlerdeki gereksiz süreçleri veya aracıları ortadan kaldırılarak işlemlerin daha hızlı ve verimli bir şekilde gerçekleştirilmesini sağlar (Zyskind , Nathan, & Pentland, 2015).

Maliyet indirimleri; DLT, uzlaşma ihtiyacının ortadan kalkması nedeniyle belirgin bir maliyet azaltma potansiyeli sunar. Çünkü DLT tabanlı sistemler tanım gereği "paylaşılan gerçeği" içerir ve dolayısıyla "gerçeğin" bir versiyonunu, bir diğerinin muadili ile uzlaştırmaya gerek yoktur. Bazı çalışmalarda yer alan tahminlere göre, dağıtılmış defter teknolojisi, yalnız finansal piyasalarda yılda 15 milyar dolar tasarruf sağlayabilmektedir (Filipova, 2015).

Gelişmiş Siber Güvenlik Dayanıklılığı. DLT, geleneksel merkezi veri tabanlarından daha esnek bir sistem sağlama ve tek bir saldırı noktasını ortadan kaldıran dağıtılmış doğası nedeniyle farklı siber saldırı türlerine karşı daha iyi koruma sağlama potansiyeline sahiptir (Berentsen & Schär, 2018).

2.4.1.2. DLT'nin Karşılaştığı Zorluklar

Olgunluk Eksikliği; Henüz gelişme aşamasında olan DLT için, özellikle büyük hacimli işlemler, standart donanım ve yazılım uygulamalarının kullanım kolaylığının test edilmemiş olması ve aynı zamanda yetenekli profesyonellerin bol miktarda bulunmaması nedeniyle DLT'nin sağlamlığı ve dayanıklılığı konusunda ciddi endişeler bulunmaktadır. Ancak, IBM ve Microsoft gibi büyük geleneksel bilgi teknolojileri piyasasının güçlü aktörleri yanı sıra Visa ve Master Card gibi finans sektörü oyuncuları da DLT konusunda çalışmalarını hızlandırmaktadır (Narayanan, Bonneau, Felten, & Miller, 2016).

Ölçeklenebilirlik ve İşlem Hızı; DLT sistemlerinin daha büyük ölçekte ve daha hızlı bir şekilde işlem gerçekleştirebileceği kapasite artırımlarına ihtiyaç vardır. Her geçen gün artan işlem stoku karşısında ölçek kapasitesi ve işlem hızı kısa vadede güçlükler ortaya çıkarmaktadır.

Müşterek Çalışma ve Sisteme Entegrasyon; Farklı DLT sistemlerinin diğerleriyle birlikte çalışabilmesi için halihazırdaki defterler ve mevcut sistemlerin birbirlerine entegre edilip, ölçeklendirilebilmeleri, finansal sistemde tanıtılmaları gerekmektedir. Bunu gerçekleştirebilmek için de önemli masraflar gerekecektir.

Siber güvenlik, Hiçbir yazılım teknik güvenlik açıklarına karşı tamamen korunmuş değildir. İstatistikler, her 1000 kod satırı için yaklaşık 15-50 hata olduğunu göstermektedir. Sanal para birimlerinin blokzincir alt yapılarına yapılan saldırılar akıllı sözleşmelerdeki herhangi bir zayıflığın istenmeyen etkiler yaratmak için kullanılabileceğini göstermiştir (Narayanan, Bonneau, Felten, & Miller, 2016).

Merkezi Yönetim; Merkezi bir altyapının ve merkezi bir varlığın bulunmaması, etkin yönetişimin sağlanması konusunda endişelere yol açmaktadır. Finansal sektör düzenleyicileri, tarihsel olarak merkezi altyapı ve diğer düzenlenmiş kuruluşlar üzerinde etkili yönetişim düzenlemelerine alışık olduğundan bu durum sistemin kabul edilebilirliğini zorlaştırmaktadır.

Düzenleyici Mevzuat ve Standart Eksikliği; Genç bir teknoloji olduğundan DLT için Dünya çapında yasal ve standart düzenleyici hükümler bulunmamaktadır. Bu husus ortak bir politika için belirsizlik yaratmaktadır.

Gizlilik; DLT ağlarında belirli durumlarda, katılımcının kimliği işlem modellerine veya diğer belirteçlere dayanarak çıkarılabilir. Bu nedenle de ağdaki kişilerin işlem gerçekleştiren kişi ve firmaların kimliğine ulaşabilir. Özellikle finans sektörünün müşteri sırrı kapsamında bu duruma temkinli yaklaştığı görülmektedir.

2.4.2. Blokzincir Teknolojisi Uygulama Alanları

Sanal para birimlerinin ilki olan Bitcoin'le popüler olan DLT ve blokzincir teknolojileri yalnızca kripto paraların oluşturulmasında değil, birçok farklı sektör ve alanda da kullanılmaya başlamıştır (TÜBİTAK, 2019). Blokzincir 'in kullanım alanları, söz konusu teknolojinin gelişim sürecinde kat ettiği aşamalarla değişiklik gösterdiği söylenebilir. Bu gelişim trendi Tablo 7 'de gösterilmektedir;

Tablo 7
Blokzincir Teknolojisinin Kullanım Alanları

Süreç	Kullanım Alanı
Blok Zinciri 1.0	Sanal para oluşturma, dijital kimlik, para transferleri, havale, küresel ve dijital ödemelerde.
Blok Zinciri 2.0	Akıllı sözleşmelerin hayata geçirilmesiyle birlikte birincil ve ikincil piyasalarda hisse senedi ve tahvil alım satımları, vadeli opsiyonlar, telif kayıt sistemleri, tapu kayıtları, noterlik uygulamaları, müşteri tanıma (Know Your Customer –KYC), krediler ve ipotek belgelerinde.
Blok Zinciri 3.0	Önceki sürümlerindeki kullanım alanları dışında bağış toplama, oy kullanma, tedarik zincirleri yönetimi, lojistik yönetimi, kamu ve sağlık kayıtları, nesnelerin interneti.

Kaynak: www.blokzincir.bilgem.tubitak.gov.tr E.T:05.08.2019

Blokzincir teknolojisinin kullanıldığı alanlar ve sektörler bu teknolojinin bilinirliği, güvenirliliği, kamu otoritelerinin yasal düzenlemeleri hayata geçirmesi ile artacağı düşünülmekte, insanoğlunun hayal gücünün ve karşılaştığı sorunların çeşitliliği bu teknolojinin kullanım sahasını daha genişleteceği beklenmektedir.

2.4.3. Blokzincirlerde Kayıt Sistemi

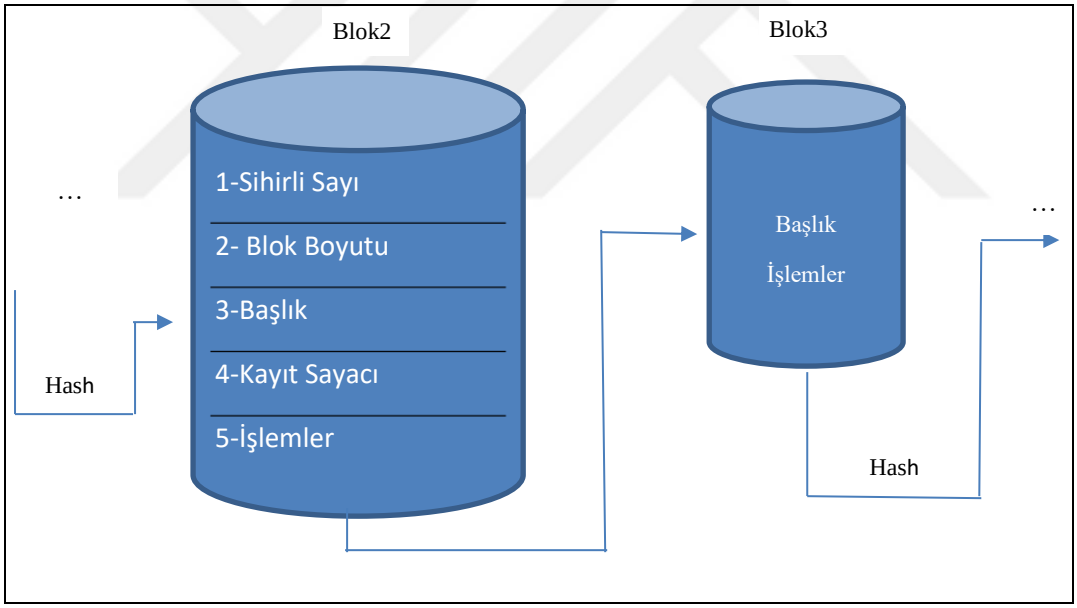
Blokzincir teknolojisinin kullanıldığı sistemlerde gerçekleştirilen her işlem belli ölçekteki bloklara kaydedilir. Her bir blok kapasitesi dolduğunda eldeki verilerle Hash'i oluşturulur ve üzerine yeni bir blok eklenir. Yeni eklenen blokun ilk girdisi bir önceki blokun Hash değeridir. Bu şekil döngüsüyle birbirlerine eklenen bloklar blokzincir yapısını oluşturur (Houben & Snyers, 2018). Her bir blok bir önceki blokun Hash'i ile birbirine bağlandığından bloklardan birinde yapılacak en küçük bir değişiklik o bloğun Hash değerini değiştirecektir. Böylece bir sonraki blokun da değişen Hash değeri diğer bloklarda da aynı etkiyi yapacak,

ağda bulunan üyelerdeki gerçek blokzincirinin orijinalliğinin bozulduğu üyeler ve sistem tarafından fark edilecektir.

Blokzincirlerdeki ilk bloğa "genesis bloku" adı verilir. Bu bloğa bir önceki bloğun Hash değeri boş olduğundan zinciri oluşturan kişi tarafından bir değer atanır. Bu değerde genellikle 256 tane 0'dan oluşur. Zinciri oluşturan bloklardan öncekine "ebeveyn-parent- blok" adı verilir. Kendisinden sonraki ise "yavru-child- bloktur" (Franco, 2015). Her blokun bir ebeveyn bloğu varken, ebeveyn bloğun birden fazla yavru bloğu olabilir. Bu konu çatallanma-forking konusunda ayrıntılandırılıcaktır

2.4.3.1. Blok Yapısı (Şekli) ve İçeriği

Blokzincirde işlemlerin yer aldığı ya da diğer bir ifadeyle kaydedildiği blokların yapısı Şekil 3 'te gösterilmiştir (Güven & Şahinöz, 2018).



Şekil 3 Blokzincir Blok Yapısı

Blokzincirdeki her bir blok'ta beş kısım bulunmaktadır (Cormen & Leiserson, 2009). Bloktaki kısımlar ve boyutları Tablo 7'de incelenmiştir.

Tablo 8
Blok Yapısı

Alan Adı	Boyutu	Açıklama
Sihirli Sayı	4 Byte	"Aşağıdaki bir bloktur" anlamındadır. Bu kısım daima 0xD9B4BEF9 olarak gösterilir. Veri tabanında okunurken, devamındaki bilgilerin bir bloğu oluşturduğunu ifade eder.
Blok Boyutu	4 Byte	Bir bloğun büyüklüğünü gösterir. Bloğun sonuna kadar kapladığı alanı ifade eder.
Blok Başlığı	80 Byte	Sürüm, önceki blok Hash'i, zaman damgası, zorluk hedefi ve Nonce bölümlerinden oluşur.
Kayıt Sayacı	1-9 Byte	Kaç adet kayıt (işlem) olduğunu gösterir
Kayıtlar (İşlemler)	Değişmektedir	Kaydedilen işlemleri gösterir.

2.4.3.2. Blok Başlığı ve Kısımları

Şekil 7'de yer alan ve blok başlığı olarak adlandırılan bölüm bir blok için önemli görevleri ifa eden altı kısımdan oluşmaktadır. Her bir kısmın adı ve ne ifade ettiği ayrıntılı ve başlıklar halinde açıklanacak olup aşağıdaki Tablo 9'da isimleri ve kapladıkları alan, özet olarak gösterilmiştir.

Tablo 9
Blok Başlığı

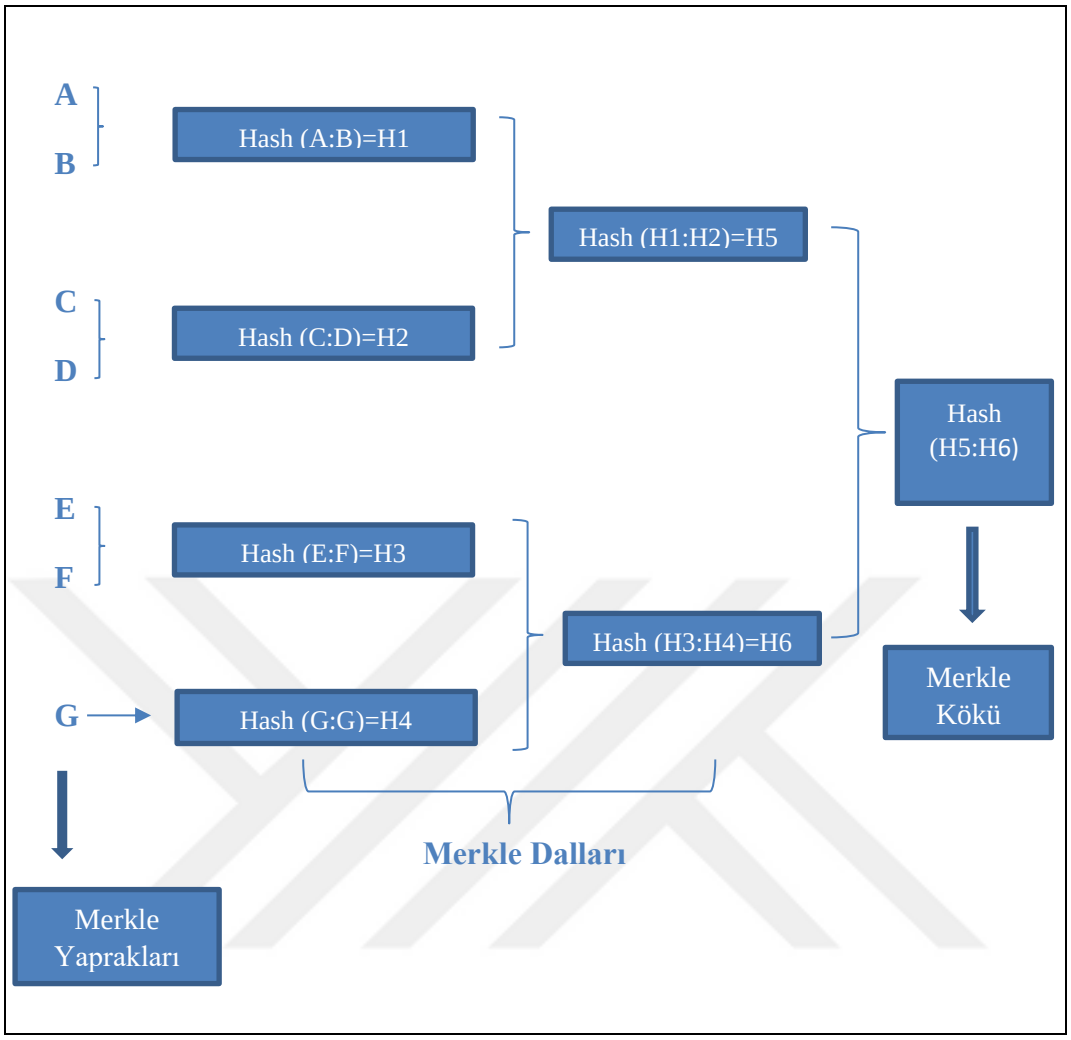
Alan Adı	Boyut
Sürüm (Versiyon)	4 Byte
Önceki Blok Hash'i	32 Byte
Merkle Kökü	32 Byte
Zaman Damgası	4 Byte
Zorluk Hedefi	4 Byte
Nonce	4 Byte

Kaynak: (İnci & Alpen, 2018)

Sürüm; Zincirin blok yapısındaki kuralların yer aldığı alandır ve bloğun yapısı, uzunluğu, neleri içereceği, kısımların sıralaması gibi bilgiler bulunur. Bu kurallar ağdaki herkesin genel uzlaşısı ile belirlenir. Yine bu kısımda yer alan kuralların blokzincirinin en başından mı yoksa işlemin gerçekleştirileceği bloktan mı başlayacağı teyit edilir.

Önceki Blok'un Hash'i; Birbirlerine zincirlenmiş blokları bağlayan unsur Hash algoritmalarıdır. Önceki bloğun Hash değeri sonraki blok yapısının başlık kısmındaki yapının içeriklerinden biridir. Zincirlerin değiştirilmez olmasının sebebi bu algoritmalardır.

Merkle Kökü; Bloktaki her iki işlem bir grup oluşturur ve grubun Hash'i birlikte alınır. Hesaplanan her bir çift grubun Hash değerleri de yine ikişerli olarak alınıp en son kalan iki grubun bir çift olacak şekilde alınan Hash değeri ile Merkle kökü hesaplanmış olmaktadır (İnci & Alpen, 2018). Merkle ağacı ve Merkle kökü kavramları Şekil 4'de gösterilmiştir.



Kaynak: (Güven & Şahinöz, 2018)

Şekil 4 Merkle Ağacı ve Kökü

Merkle ağacı blokzincir yapısında önemli bir yere sahiptir. Zira sistemde bulunan ve ikişerli gruplar halinde Hash değerleri alınan işlemlerde gerçekleşecek herhangi bir değişiklik Merkle kökünü değiştirecektir. Bu durum da bloğun başlık kısmının değişmesine neden olacak sonuç olarak da bir sonraki bloğun Hash değerinin değişmesiyle blok yapısı anlamsız olacaktır (Franco, 2015). Bir başka önemli nokta ise Merkle ağacı yöntemiyle, -kriptoloji sistemlerinin anlatıldığı bölümde de değinildiği gibi- Hash algoritmalarıyla bir veride özgünlüğün yani herhangi bir müdahale ya da değişikliğe uğrayıp uğramadığının izi sürülebilmektedir. Diğer bir ifadeyle Merkle ağacı silsilesinde, işlemlerin temeline inmeden gruplanmış daha sonraki Merkle dallarının Hash kontrolü yapılarak

doğruluk teyidinin kolaylıkla yapılabilirliği nedeniyle blokzincir sisteminde önemli ve de kolay bir kontrol mekanizması olarak görev yapmaktadır.

Zaman Damgası; Blokzincirdeki her bir bloğun üretim tarihini göstermektedir. Gösterilen tarih, orijin olarak 1 Ocak 1970 tarihini almaktadır. Bloklarda zaman damgası için ayrılan 4 Byte 'lık bir alan 32 bit büyüklüğü ifade etmektedir. Birinci Byte 'ın sayının işaretini gösterdiği bilindiğinden geriye kalan 2^{31}-1=2.147483.647 saniye yazılabilecek en uzun zaman dilimidir. Bu da başlangıç tarihinin 1 Ocak 1970 olarak alındığında 2038 yılına kadar işlemlerin zaman damgasının yapılabileceğini göstermektedir. Bu duruma bilgisayar dünyasında Y2038 problemi adı verilmektedir. Her ne kadar bir problem olarak addedilse de bu durum teknolojik altyapının geliştirilmesiyle ortadan kaldırılabilir. Nitekim 2000 yılının ilk gününde yaşanılacağı düşünülen sorunla eş değer olan bu durum aynı şekilde giderilmiştir (Narayanan, Bonneau, Felten, & Miller, 2016).

Zorluk Derecesi; Blokzincirde yer alan her bir blok üretiminin süreceği zamanı ve doğrulama için çözülmesi gereken matematiksel problemlerin zorluk derecesini ifade etmektedir. Zorluk derecesi, sistemdeki işlemci gücüne bağlıdır. İşlemci gücü arttıkça zorluk artar, azaldıkça zorluk azalır.

Nonce; Bilgisayar literatüründe tek kullanımlık alan olarak tanımlanan bu bölümde 4 Byte büyüklüğünde bir alan da sayılar bulunmaktadır ve bu sayılar, bloğun Hash değerinin değiştirilmemesini sağlayabilmek için sürekli değiştirilen, yeni bir Hash 'in hesaplanarak kurala uygun Hash bulunana kadar değiştirildiği yerdir.

2.5. Sanal (Kripto) Para Dünyası

2.5.1. Sanal Para Birimlerinin Doğuşu

Kriptografik işlemler kullanılarak merkezi olmayan dijital para oluşturma fikri 1980'li yıllardan günümüze uzanan, kimi zaman farklı uygulamalarla hayatımıza giren önemli bir kavram olmuştur. Daha çok elektronik para olarak adlandırılabilecek bu uygulamalar, merkezi bir otoritenin bulunmaması halinde başarılı olunamayacağı ya da sistemin çifte ödeme gibi sorunlarla karşı karşıya

kalabileceği, kısaca söz konusu dijital/elektronik paraların teknik alt yapılarına güven duyulmadığı için hayata geçirilememiştir. 1998 yılında Wei Dai'nin B-Money ve 2005 yılında Hal Finey'in iş ispatına dayanan ve merkezi olmayan dijital para uygulama fikirleri bu başarısız denemelere örnek olarak gösterilebilir (Dai, 1998). Ancak 2008 yılının Eylül ayına gelindiğinde Satoshi Nakamoto isimli (ya da takma adlı) bir kişinin internet ortamında yayınladığı makalede; güvenilir bir merkezi otorite olmadan, kriptografi ile oluşturulan, iş ispatına dayalı, birbirlerini tanımayan iki kişi arasında gerçekleştirilebilecek bir elektronik ödeme sisteminin var olabileceğinden bahsedilmiştir (Nakamoto, 2008). Yapılacak matematiksel hesaplamalarla her bir ödeme işlemi, zaman damgalı, geri döndürülemez ve değiştirilemez bir şekilde gerçekleştirilebilecektir.

Satoshi, daha önceki dijital para fikirlerinin aksine yalnızca teorik olarak fikrini açıklamakla kalmamış, "Bitcoin" adını verdiği bu yeni paranın hayata geçirilmesini sağlamış ve sistemin nasıl çalışacağının ana prensiplerini açıklayarak sitemin devamının ağdaki "düğüm" adını verdiği katılımcılar tarafından sağlanacağını belirtmiştir.

Satoshi Nakamoto fikri alt yapısını oluşturduğu bu yeni sistemi internet ortamında kriptografi ile ilgilenen bir kaç bilgisayar mühendisinin yer aldığı grup ile paylaşmıştır. 2009 yılının ilk ayında ise Satoshi tarafından 30 bin satırlık kaynak kodun sisteme girilmesi ile Bitcoin efsanesinin ilk somut adımı atılmıştır.

Sanal para birimlerinin ilk örneği olan Bitcoin'in ortaya çıkmasındaki etkenler araştırıldığında, bu fikrin ortaya atıldığı zaman ve şartlar da göz önünde bulundurulmalıdır. Şöyle ki; Bitcoin'in teknik altyapısının anlatıldığı makalenin "bitcoin.org" adlı internet sitesine konulduğu dönemde Dünya finansal piyasaları ABD orjinli, bugüne kadarki yaşanılan en büyük ekonomik krizle karşı karşıya kalmıştır. Mortgage krizi adı verilen bu kriz, ABD 'de önemli yatırım bankalarının iflas ettiği, binlerce kişinin işsiz kaldığı ve milyarlarca dolar zararın açıklandığı, sosyal hayatın önemli ölçüde etkilendiği, finans piyasalarının kalbi olan Wall Street'in insanlar tarafından işgale uğradığı bir zamanda cereyan etmekteydi (Franco, 2015). Tam da bu durumda artık insanların ülke ekonomilerine yön veren karar alıcılara güvenlerinin azaldığı bir zamanda,

merkezi bir otoritenin ve karar alıcılarının bulunmadığı bir sistem önerisinin, çoğu kişi tarafından kabul edilmesinin önemli sebeplerinden birini oluşturmuştur.

Bitcoin, blokzincir teknolojisinin kullanılarak ortaya çıkarılan ilk sanal para birimidir. Elbette Bitcoin'den sonra "Altcoin" adı verilen farklı sanal para birimleri ve az da olsa yine farklı teknolojileri de hayata geçirilmiştir ancak hepsinin ilham kaynağının Bitcoin olması nedeniyle bu çalışma da sanal para yaratma teknolojisi, Bitcoin örneği ile anlatılmaya çalışılacaktır.

Çalışmanın bu bölümünde sanal para birimlerinin hayata geçirilmesini sağlayan temel teknik altyapının nasıl çalıştığını Satoshi Nakamoto'nun sanal para birimleri ile ilgili ilk kaynağı oluşturan makalesindeki bölümlerde yer alan konuların detaylandırılması yolu ile anlatılacaktır.

2.5.2. Madencilik

Sanal para birimlerinin üretilmesi aşamasına "madencilik" adı verilir. Madencilik faaliyeti ile sistemin devamlılığını sağlayan, sanal paranın yapısını oluşturan blokların üretilmesi ve işlemlerin onaylanmasını gerçekleştiren kişilere ise madenci denmektedir (Narayanan, Bonneau, Felten, & Miller, 2016). Madenciler, işlem havuzunda bekleyen işlemlerden, her biri 1 MB büyüklüğünü aşmayacak şekilde blok oluşturmaya çalışmaktadırlar. Bunun sonucunda madenciler sistem tarafından Bitcoin'le ödüllendirilmektedir. Merkle Kökü'nün anlatıldığı bölümde de yer verilen gruplandırılmış ve Hash değerleri hesaplanmış blokların uygun özet değerleri, zor matematiksel problemlerin işlem yeteneği ve hızı yüksek bilgisayarla çözümlenmesi ile blok yapıları oluşturulup zincire eklenir (Narayanan, Bonneau, Felten, & Miller, 2016). Madencilerin sistem tarafından ödüllendirilmesinin içeriği ise hem blok oluşturarak hem de blok içindeki işlemleri yerine getirilerek elde edilen komisyonlar, kısaca Bitcoin'lerdir.

Blok oluşturma ve zincire ekleme olarak özetlenebilecek madencilik faaliyetlerinin tıpkı değerli madenlerin çıkarılması için sarf edilen çaba, madenciler arasındaki rekabet ve maden miktarının sınırlı olması gibi özellikleriyle bu isimle anılmasını sağlamıştır (Nakamura & Matsutani, 2017). Sanal Para birimlerinin toplam arzları da madenler gibi sınırlı tutulmuştur. Örneğin Bitcoin 'in toplam arz miktarı 21 Milyon adettir.

Bitcoin ’de blokların oluşturulması ve işlemlerin onaylanması yolu ile elde edilecek ödül miktarları belirli kurallar dâhilindedir. Bitcoin‘in piyasaya çıktığı 2009 yılı itibariyle madenciler oluşturdukları blok başına 50 BTC (Bitcoin) kazanırlarken kurala göre bu miktar her 210.000 blokta yarılanarak önce 25 BTC’ye sonrada 12,5 BTC ‘ye düşmüştür. Bundan sonraki ilk yarılanma dönemi ise takriben 2020 yılı Mayıs ayına tekabül etmektedir. Sistemdeki toplam 21 Milyon olan Bitcoin miktarı ve 10 dakikalık blok oluşturma süresi göz önünde bulundurulduğunda tüm Bitcoin’lerin 2140 yılında tamamen üretileceği hesaplanmaktadır (Güven & Şahinöz, 2018).

Sistemdeki madencilerin tek görevi blok oluşturmakla sınırlı değildir. Her madenci blok oluşturmanın yanı sıra işlemlerin onaylanması, işlemlerin doğrulanması ve dağıtık yapının sürekliliğini sağlama görevlerini de yerine getirir.

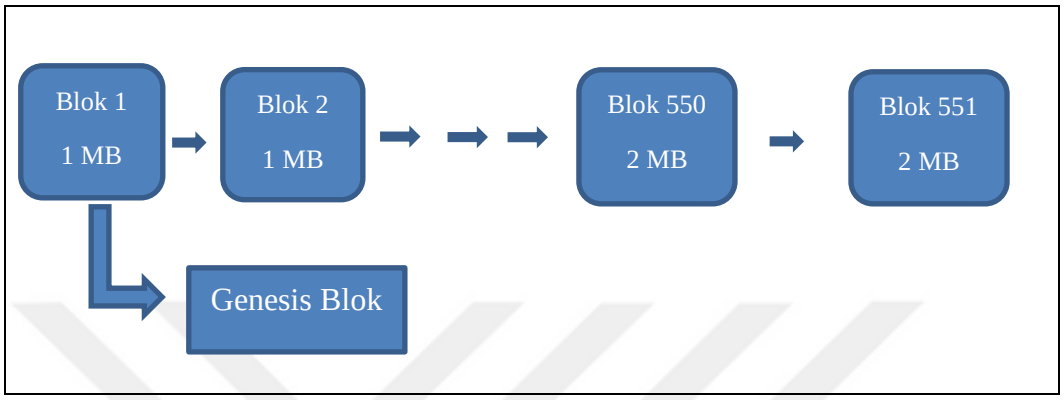
Madencilik faaliyetleri, ilk Bitcoin’lerin üretimi sırasında kullanıcılar tarafından evdeki bilgisayarlara ilgili programın yüklenmesiyle gerçekleştirilirken artık madenciler arasındaki rekabetin artması ile işlem hızının yüksek olduğu daha gelişmiş işlemcilere sahip bilgisayarlarla yapılabilmekte, diğer bir ifadeyle madencilik faaliyetleri git gide zorlaşmakta ve profesyonelleşmektedir. Bunun yanı sıra madenciler faaliyetlerini yerine getirirken yüksek elektrik sarfiyatı ve işlemlerin gerçekleştirildiği bilgisayarların soğutulması maliyetlerine de katlanmaktadırlar (İnci & Alpen, 2018). Öyle ki sanal para madenciliği yapan bir grup şirket, merkezlerini daha az elektrik maliyeti olan yerlere ya da soğutma işlemlerini daha ucuz ve kolay yapabilecekleri soğuk ve yüksek bölgelere taşımaktadırlar (IMF, 2019).

2.5.3. Çatallanma

Blokzincirde gerçekleştirilen her kayıt ağda bulunan üyelerin mutabakatı ile yoluna devam etmektedir. Söz konusu mutabakat bir tür kurallar dizinidir. Her bir kural ağda bulunanlarca kabul edilmiştir. Ancak bu kurallar esnetilemez ya da değiştirilemez değildir. Sistemdeki bir üyenin işlemlerin daha kolay ya da verimli yürütülmesi adına ortaya koyacağı yeni bir teklif ağdaki üyelerce kabul ya da reddedilebilir. Diğer taraftan ağ yapısında çok sayıda üyenin bulunduğu göz önüne alındığında her teklifin oy birliği ile kabul ya da reddedilmesi çoğu zaman

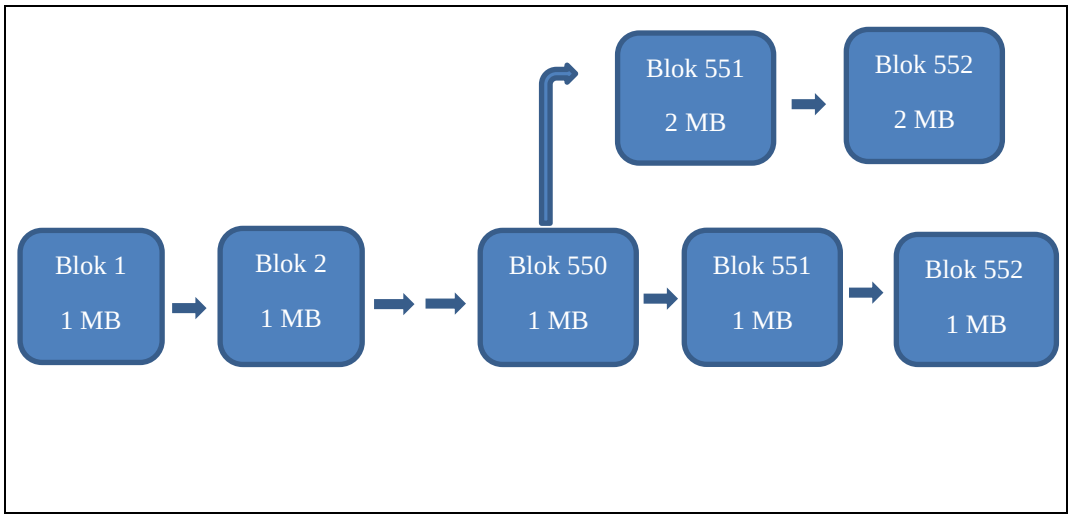
mümkün olmayabilir (Dadda & Machetti, 2004). Bu durumda üç farklı senaryo ile karşı karşıya kalınır.

Birinci senaryo söz konusu teklifin üyelerin tamamınca kabul edilerek yeni kurallarla blokzincirin devam etmesi anlamında olup Şekil 5'te gösterilmiştir (Güven & Şahinöz, 2018).



Şekil 5 Gönüllü Çatallanma

İkincisi yine tüm üyelerce reddedilip eski kurallar çerçevesinde işlemlerin yürütülmesidir. Üçüncüsü ise bir kısım üyelerin reddededip bir kısmının ise yeni teklife sıcak bakmasıdır ki önemli bir sayısal ayrımın-örneğin sistemdeki üyelerin %20-25 gibi bir kısmı- söz konusu olduğu durumda fikir birliğine varılamaması ile eski zincirin yanında yeni kuralla blok yapısı oluşturulan bir blokzincir daha meydana gelecektir. Bu durum Şekil 6'da gösterilmiştir. (Franco, 2015). Buna çatallanma (forking) adı verilir. İkinci senaryoda bahsedilen durum "gönüllü" (soft) çatallanmadır. Ancak eski blokzincirinin yanında yeni bir blokzincirinin oluşarak ikisinin birden çalışmaya devam etmesi durumunda "mecburi" (hard) çatallanma adını almaktadır (Dadda & Machetti, 2004)



Kaynak: (Güven & Şahinöz, 2018)

Şekil 6 Mecburi Çatallanma

Sanal (kripto) para dünyasında çatallanmaların yaşanması ile yeni kurallar ve yeni blokzincir yapılarıyla yeni sanal para sistemleri ortaya çıkmıştır. Örnek verilecek olunursa sanal para piyasasında hacimsel olarak ilk 10 büyük kripto para biriminden biri olan Lithereum (LTC), Bitcoin de kullanılan SHA256 algoritmasını "Scrypt" ismini verdiği farklı bir algoritmayla değiştirerek maksimum coin miktarını 4 katına çıkarmış ve blok çözme süresini 10 dakikadan 2.5 dakikaya indirmiştir. Bir diğer örnek ise yine bir sanal para birimi olan Bitcoin Cash'in Bitcoin sanal para biriminin mecburi çatallanması ile ortaya çıkması gösterilebilir (Nakamura & Matsutani, 2017).

2.5.4. İş İspatı ve Pay İspatı

İş ispatı ve pay ispatı algoritmaları, ağda bulunan madencilerin gerçekleştirilen işlemler üzerindeki mutabakatı sağlayan çeşitli algoritma türlerinden yalnızca iki tanesidir (Farell, 2015). Bu mutabakat algoritmalarının amacı blokzincirdeki tek düzeyliğin (tek zincirin) devamı için blok üretimlerinin sabit aralıklarla oluşturulmasını sağlamaktır.

İş ispatı algoritmaları blokların tamamlanmasını sağlayan madencilere gerçekleştirdikleri işin büyüklüğüne göre Bitcoin verilmesini amaçlamaktadır. Madenciler, blok yapısında bulunan Nonce kısmındaki değerleri değiştirerek (deneme-yanılma yöntemiyle) blok yapısına en uygun Hash özetini zorlu

matematiksel problemlerin çözümlenmesi ile bulurlar (Vlasov, 2017). Bu işlemlerin yapıldığı bilgisayarların saniyenin onda birinde on binlerce işlem yaptığını düşünürsek zorlu problemlerin çözümlenerek her blokun on dakikada oluşturulmasının nasıl mümkün olduğu anlaşılmış olacaktır.

Özet (Hash) değerlerin hesaplanmasında karşılaşılan matematiksel problemlere örnek verilecek olursa; öncelikle SHA algoritmalarının herhangi bir girdiyi 256 bitlik özetler haline getirdiğini hatırlayalım. Özet kodunun ilk bitin 'in tahmin edilebilme olasılığı %50 olacaktır (Sıfır ya da 1). Özet değerinin ilk 30 basamağının 0 olması kuralı konulduğunda ise problemin çözülebilme olasılığı üstel olarak artacak ve 2^{30} olacaktır. Bu problemin çözümü gelişmiş bilgisayar programları ile sadece bir saniye almaktadır. Ancak söz konusu özet değeri problemini "ilk 10 basamağın daha 0 olduğu" şeklinde düzenlersek işlemin zorluğu 2^{10} kat daha artacak yani 1024 saniye de çözülebilecektir. Ki bu süre de 17 dakikaya tekabül etmektedir (Farell, 2015). Buradan yola çıkılacak olursa blok oluşturma süresi azaldıkça özet değerinin hesaplandığı matematiksel problemlerin zorluğu da doğru orantılı bir şekilde artacak, diğer taraftan sistem tarafından ödüllendirilen madencilerin kazandıkları Bitcoin sayısı da artacaktır.

Pay ispatında ise madenciler hesaplama ve blok oluşturma konusunda birbiriyle yarışmaz. Madenciler sistem içerisinde sahip oldukları pay büyüklüğünde blok oluşturma görevi kendilerine verilir, diğer bir ifadeyle görevi alma ihtimali artar. Pay ispatı yönteminde blokların üretiminden ödül kazanılmaz ancak blok içindeki işlemlerin onaylanması ile komisyonlar elde edilir. Bu nedenle pay ispatı yönteminde madencilere "oluşturucu (forger)" adı verilir (Böhme, Christin, Edelman, & Moore, 2015).

2.5.5. Sanal Paralarda Cüzdan Kavramı

Sanal para cüzdanları sahip olduğumuz fiziksel cüzdanlara benzetilebilir. Sahip olunan sanal paraların saklandığı ve muhafaza edildiği yerlere de cüzdan (wallet) ismi verilmektedir.

Her ne kadar sanal paraları bilgisayarlar vasıtasıyla internet ortamında satın alınsa da bu paraları bilgisayarlara indirip orada saklamak mümkün olamamaktadır. Sanal paralar diğer tüm işlemlerin gerçekleştirildiği ve

onaylandığı gibi sistemdeki tüm ağ üyelerinde bulunan dağıtılmış hesap defterlerinde yine blokzincir dâhilinde tutulur. Şifreli bir adresle ilişkilendirilmiş özel anahtar, paranın bu adrese alınmasını ve yine bu adresten gönderilmesini sağlayan dijital bir imza gibi kullanılır (Ali, Barrdear, & Southgate, 2014). Sanal para alım-satımı yapmak isteyen kullanıcı söz konusu şifreli adresini bir banka hesabıyla ilintili şekilde oluşturur. Bu şifreli adres harflerin ve sayıların birlikte kullanıldığı ve genellikle 25 ile 35 arası karakterden oluşan bir adrestir. Sanal para sistemlerindeki kullanıcıların adresleri ağdaki üyeler tarafından görülse de bu adresler kullanıcıların kimliklerini yansıtmadığı için adres sahibi kullanıcıların kim oldukları bilinemez. Sanal cüzdanlar internet ağı dâhilinde ise sıcak dışında ise soğuk cüzdan adını almaktadır (Berentsen & Schär, 2018).

Sanal para transferlerini gerçekleştirirken dikkat edilmesi gereken en önemli husus önceki bölümlerde anlatılan açık anahtar (Public Key) ve gizli anahtar (Private Key) çiftinin üretilmesi ve özellikle özel anahtarın içeriğinin güvenli bir şekilde saklanmasıdır. Sanal para sisteminde transfer işlemlerinde, eşlerden biri parayı aktarmak istediği kişinin açık anahtarını öğrenip, blok içerisine o kişinin açık anahtarını kodlayarak kilitler. Sanal para artık başka birine aittir. Bu para daha sonra başka bir eşe gönderilmek istendiğinde sahip olan kişi tarafından özel anahtarıyla açılır alıcının açık anahtarı girilerek kilitlenir ve süreç bu şekilde devam eder (Swan & De Filippi, 2017).

Sanal cüzdanlarda sahip olunan gizli anahtarın güvenliğini sağlamak, başkaları tarafından öğrenilmesini engellemek oldukça mühimdir. Çünkü özel anahtarın kaybedilmesi, unutulması veya çalınması durumunda sahip olunan sanal paraların güvenliği tehlikeye girecektir. Bankacılık sisteminde hesap numaralarının unutulması ya da hatalı işlemlerin düzeltilmesi bankanın söz konusu işlemleri inceleyerek geriye dönük işlemleri gerçekleştirmesiyle düzeltilebilir. Ancak sanal para sistemlerinin temelini oluşturan üçüncü bir kişi ya da merkezin kontrolünde olmama, eşler arasında gerçekleşen transfer nedeniyle bu düzeltmeleri yapabilecek bir merkez bulunmamaktadır (Zyskind , Nathan, & Pentland, 2015). Bu nedenle karşılaşılabilecek herhangi bir olumsuz durumda sanal paraların kaybedilmesiyle karşılaşılabilir.

Sanal para transferinde göndericinin transfer adımları şu şekilde özetlenebilir;

a) Gönderici sahip olduğu sanal paranın bulunduğu blok yapısına işlem referansını, ödeme yapılacak kişinin açık anahtarlı adresini ve ödenecek tutarı kodlayarak bir mesaj oluşturur,

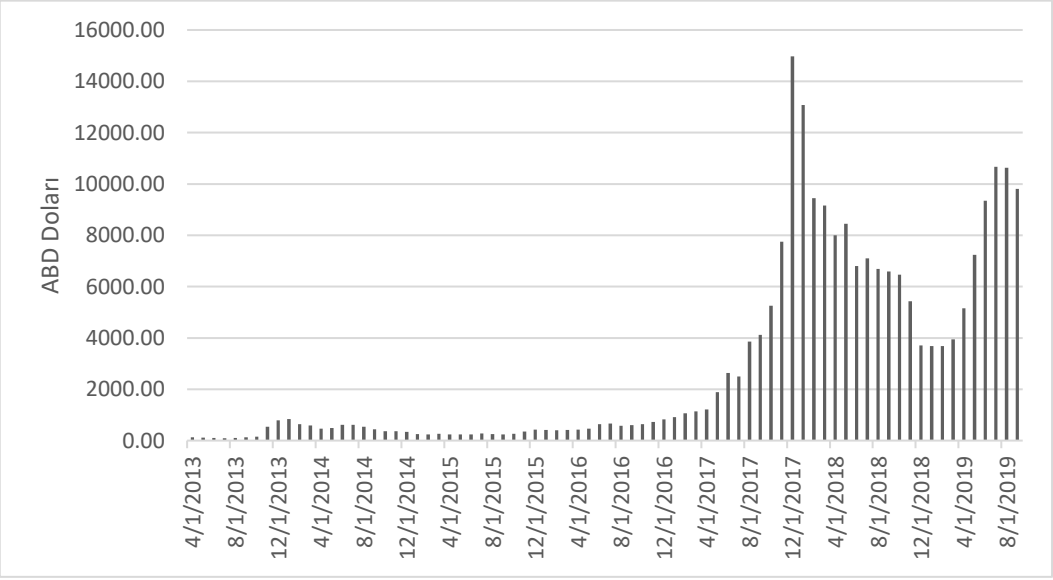
b) Bu işlemin ardından kendi özel anahtarıyla işlem bloğunu kilitleyerek dijital imzasını atar, bu şekilde tüm ağdaki üyeler işlemden haberdar olur,

c) Madenciler tarafından göndericinin yeni işlemi, işlem havuzundan alınarak yeni blok haline getirilir, işlemler ağdaki üyelerin doğrulama ve oy birliği teyitlerinden geçer, işlem blokzincirin sonuna yeni bir blok halinde eklenir.

2.5.6. Sanal Paraların Finansal Piyasalardaki Performansı

Sanal para birimlerinin ilk örneği olan Bitcoin 'in 2009 yılı başından itibaren sanal ortamda üretilmeye başlanması ve oluşturulan ilk sanal paraların ihracıyla Bitcoin ekosistemi şekillenmeye başlamıştır. Bitcoin'lere olan talebin 2013 yılı sonu itibariyle artış göstermesinin altında yatan sebepler irdelendiğinde söz konusu yılda yaşanan Avrupa borç krizi, Bitcoin kullanımının yasal yönden sakıncalı olmadığının altı çizildiği FINCEN (The Financial Crimes Enforcement Network- Finansal Suçları Engelleme Ağı) raporu ve Çin'de Bitcoin talebinin artması gösterilebilir (Bustillos, 2013).

Tablo 10
Bitcoin'in ABD Doları Cinsinden Piyasa Değeri

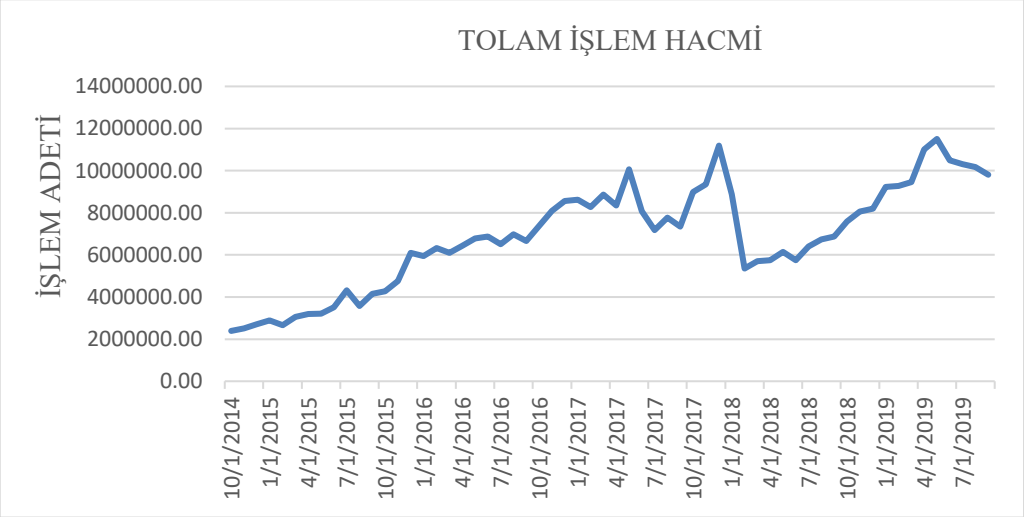


Kaynak: www.coinmarketcap.com/data/marketprices E.T:08.09.2019

Bitcoin‘in her geçen gün tanınırlığının artmasında, ABD’nin önemli finans kurumlarından Chicago Ticaret Borsasının (CME) ve Chicago Board Options Exchange (CBOE) ‘in Bitcoin için vadeli işlemlere başlaması, akabinde yatırımcıların yükselen ilgisiyle karşılaşılmasının önemli bir payı bulunmaktadır (Iansiti & Lakhani, 2017). Bunun yanı sıra birtakım ülke ekonomilerinin sanal paralarla ilgili yasal düzenlemeleri hayata geçirmeleri sonucunda 2017 yılının sonlarına doğru Bitcoin en yüksek değerine ulaşmıştır.

Bitcoin ‘in 2018 yılının başlarında işlem hacmindeki yaşanan düşüşün ana sebebini ise Bitcoin‘in işlem hacminin yaklaşık %90’ını oluşturan Çin ulusal para birimi (CNY) ile yapılıyor olması ve buradan hareketle 2017 yılında Çin Merkez Bankası tarafından ülkenin en büyük üç sanal para borsasına yapılan sıkı denetimler sonucu yatırımcıların sanal para ihracında kullandıkları borç olan marjin (teminat)’in alımına yasak getirilmesi oluşturmaktadır (Parker, 2017).

Tablo 11
Bitcoin’ in Toplam İşlem Hacmi

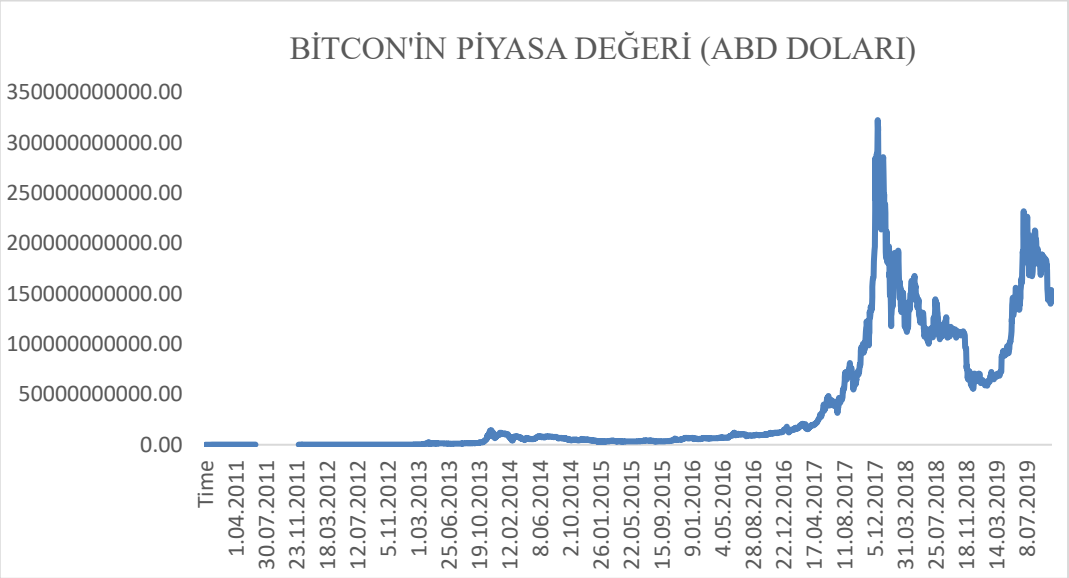


Kaynak: www.coinmarketcap.com/data/transactions E.T:08.09.2019

Bitcoin, sanal para piyasasının en büyük işlem hacmine ve piyasa büyüklüğüne sahip para birimi olması yanında kullandığı teknolojik alt yapıyla da kendinden sonra ortaya çıkan sanal para birimlerine öncülük etmiştir. Sanal para piyasasında Bitcoin’le beraber toplam 1997 adet sana para birimi işlem görmektedir (www.coinmarketcap.com/data/history E.T:08.09.2019).

Bitcoin’ in dolar cinsinden piyasa büyüklüğü Tablo 12 de ve Bitcoin’le beraber en büyük beş sanal para biriminin piyasa büyüklüğünün karşılaştırıldığı Tablo 13 aşağıda yer almaktadır.

Tablo 12
Bitcoin'in Piyasa Büyüklüğü (Bin ABD Doları)



Kaynak: www.coinmarketcap.com/data/bitcoin E.T:08.09.2019

Tablo 13
En Büyük Beş Sanal Para Biriminin Piyasa Büyüklüğü (ABD Doları)

Sanal (Kripto) Para Birimi	Bitcoin	Ethereum	Ripple	Tether	Bitcoin Cash	Diğer Tüm Kripto paralar
Piyasa Değeri	152.18 Milyar	20.2 Milyar	12.1 Milyar	4.1 Milyar	3.9 Milyar	39.15 Milyar
Piyasa Büyüklüğü	% 65.8	%8.63	%5.24	%1.79	%1.77	%16.90

Kaynak: www.coin-turk.com/sanalparalar/piyasabuyuklugu E.T:08.09.2019

Sanal para piyasasının toplam değeri 2019 yılı Eylül ayı itibariyle yaklaşık 232 Milyar ABD dolarına ulaşmıştır. Piyasa büyüklüğünün % 65'ini Bitcoin, %8,63'ünü Ethereum, %5,24'ünü Ripple, % 1,79'unu Tether, % 1,77'sini ise önceki bölümlerde de değinilen Bitcoin'in zorunlu çatallaşması ile oluşan altcoini Bitcoin Cash oluşturmaktadır. Geriye kalan tüm sanal para birimleri ise % 16,90'ini teşkil etmektedir.

Bitcoin 'in toplam piyasa arzı 21 Milyon adet ile sınırlandırılmıştır. 2019 yılı Eylül ayı sonu itibariyle piyasada ihraç edilen toplam Bitcoin sayısı 17

Milyon 997 Bin 437 adettir. Daha önceki bölümlerde de anlatıldığı gibi oluşturulan birim zamandaki blok sayısı ve her 210 Bin Blok'ta madencilerin elde edeceği ödül miktarının yarılanması bir arada düşünüldüğünde Bitcoin 'in 21 Milyonluk toplam arz miktarına yaklaşık olarak 2140 yılında ulaşılacağı tahmin edilmektedir.

Sınırlı arz miktarına sahip olan Bitcoin'e her geçen gün talebin artacağı düşünülürse değerinin gün geçtikçe artacağı ve enflasyon sorunu yaşamayacağı ileri sürülebilir. Bitcoin 'in ilerde fiyatının milyon dolarlara ulaşması durumunda da bu yüksek fiyatlı değişim aracı ile gerçekleştirilecek daha küçük tutarlı alış verişlerde sorun olmayacaktır. Çünkü 1 Bitcoin, 100 Milyona kadar bölünebilmektedir. Her bir Bitcoin'in yüz milyonda birine "Satoshi" adı verilmektedir (Tapscott, 2016). Bir milyon dolar değerine ulaşacağı düşünüldüğünde bir Satoshi'nin değeri 1 sent olur ki finansal piyasalarda en küçük para birimine karşılık gelecektir.

Sanal para birimleri, oluşturuldukları protokoller gereği yalnızca madencilik faaliyetleri ile elde edilmemekte, internet ortamında da alınıp satıldıkları ve alış verişlerde kullanılabildikleri için kısa zamanda birer yatırım aracına dönüşmüşlerdir.

Kripto paraların finansal piyasalarda bir değişim aracı haline gelmesi ve yatırım aracı olarak kullanılması sanal para borsalarının kurulması ile hayata geçmiştir. Kripto para borsaları, anlık olarak farklı para birimleri arasında sanal para alım-satımının yapıldığı, kısaca sanal para edinilmesinin madencilik faaliyetleri dışında da mümkün olabileceğini gösteren alternatif bir yatırım olanağı oluşturmuşlardır. Dünyada en büyük sanal para borsaları ve büyüklükleri Tablo 14' te gösterilmiştir.

Tablo 14
En Büyük Sanal Para Borsaları ve Hacimleri (Milyar ABD Doları)

Borsa Adı	Hacim (Günlük)	Hacim (Aylık)	Kuruluş	
BitMEX	1.890.520.531	70.583.721.706	NİSAN	2014
FCoin	1.294.284.691	40.841.877.576	MAYIS	2018
CoinEx	1.044.046.683	24.967.424.648	ARALIK	2017
P2PB2B	991.263.169	19.416.739.855	OCAK	2018
Binance	946.056.418	28.566.788.587	TEMMUZ	2017
Fatbtc	898.244.148	26.518.601.872	MAYIS	2014
CoinBene	877.144.247	25.053.011.829	EYLÜL	2017
LATOKEN	869.769.083	25.539.504.157	TEMMUZ	2017
MXC	853.205.421	26.860.345.602	NİSAN	2018
LBANK	826.686.096	23.965.033.683	EKİM	2017

Kaynak: www.coinmarketcap.com E.T:08.09.2019

2.5.7. Sanal Paranın Özellikleri ve İşlevleri Açısından İncelenmesi

Bitcoin öncülüğünde finansal piyasaları etkilemeyi başaran sanal para birimleri için en önemli tartışma konusu, sanal paraların konvansiyonel para birimlerinin yerine geçip geçemeyeceği, diğer bir ifadeyle bir para birimi olarak kabul edilip edilmeyeceğidir. Çalışmanın ilk bölümünde yer verilen paranın özellikleri ve işlevleri çerçevesinde sanal paraların para birimi olarak kabul edilebilir olup olmadığı bu kısımda irdelenecektir.

2.5.7.1. Paranın Özellikleri Açısından

Sanal para birimlerinin, paranın evrensel olarak kabul edilen özellikleri bakımından para vasfına sahip olduğu iddia edilebilir. Bitcoin örneğinde de olduğu gibi sanal para birimleri için homojen olmama ve bozulma gibi olumsuz özelliklerden sanal paraların doğası gereği bahsedebilmek mümkün değildir. Diğer taraftan sanal paraların elektronik ortamda efektif aktarım mekanizması sayesinde kolay taşınabilir oldukları ileri sürülebilir. Ayrıca sanal para birimleri küçük değerlere bölünebilir, mal ve hizmetlerin alım satımında kolaylıkla kullanılabilmektedirler. Örneğin Bitcoin'in 100.000 basamağa kadar bölünebilmesi bu özelliği taşıdığını ispat etmektedir.

Para olarak kullanılan metalarda aranan diğer özellikler ise taklit edilemezlik ve genel kabul görmedir. Çalışmanın ikinci bölümünde sanal para birimlerinin teknolojik altyapısı incelendiğinde de bahsedildiği gibi sanal para birimlerinin oluşturulma, aktarılma ve kullanılma safhalarında oldukça güvenli bir teknolojik alt yapıya sahip olduğu açıktır. İş ispatı protokolüyle işlemlerin tekrar edilemez olması ve çifte ödeme sorunun giderilmesi ile güvenli bir ödeme aracı olduğu anlaşılmaktadır. Günümüzde Bitcoin özelinde gerçekleştirilen işlem hacminin 10 Milyon âdete ulaşması ve bu sayının her geçen gün artış eğilimi göstermesi de sanal paraların işlem aracı olarak git gide daha fazla kabul gördüğünün göstergesi olmaktadır.

2.5.7.2. Paranın İşlevleri Açısından

Ekonomistler arasında Bitcoin ve diğer sanal para birimlerinin iyi birer değişim aracı oldukları ancak değer saklama işlevi yönünden riskler içerdiği ortak bir kanı haline gelmiştir. Bu kısımda kripto para birimlerinin paranın üç işlevini ne kadar iyi yerine getirdiği incelenecektir. Diğer kısımda ise volatilite, deflasyon ve düzenleme konuları ele alınacaktır. Bu bölümdeki ve diğer kısımdaki argümanların çoğunun, Bitcoin dışındaki herhangi bir kripto para biriminde de geçerli olduğu unutulmamalıdır.

2.5.7.2.1. Hesap (Değer) Birimi Olması

Sanal para birimleri henüz iyi birer hesap (değer) birimi olarak kabul edilmemektedir. Diğer taraftan söz konusu para birimleri birçok ürün ve hizmetle takas edilebiliyor olsalar da, bunların bir kısmı doğrudan sanal para birimi– örneğin Bitcoin- cinsinden fiyatlarını almaktadır. Bitcoin yüksek fiyat istikrarsızlığına sahip olduğundan tam olarak hesap değer birimi haline gelmesi bu durumu ile mümkün gözükmemektedir (Gültekin, 2017). Bitcoin fiyatının daha istikrarlı kalması durumunda ise piyasa aktörlerince Bitcoin cinsinden fiyatların oluşması söz konusu olabilecektir. Ekonomistler tarafından konu ile ilgili ileri sürülen en önemli argüman; yeni teknolojilerin geliştirilmesi ile sanal para

birimlerinin paranın genel kabul görmüş üç işlevine farklı işlevleri ekleyeceğidir (Dourado & Brito, 2014). Bu görüşe göre, Bitcoin'in, paranın diğer işlevlerini başarabilmesi durumunda günümüzde hesap birimi rolünü üstlenebilmesinin pek de önemli bir husus olmadığıdır.

2.5.7.2.2. Değişim Aracı Olması

Ekonomi literatüründe Bitcoin'in geleneksel para birimlerinin yerini alabilmesinin ve bir değişim aracı olabilmesinin genel kabul görme özelliğinin yeterince büyük bir kitle tarafından benimsenmesine bağlı olduğu ifade edilmektedir. Ancak sanal para birimlerinin hala küçük bir kullanıcı tabanına sahip olduğu ve evrensel bir değişim ortamı olması için kritik büyüklükte bir kitle tarafından elde edilmesi gerektiği konusunun altı çizilmektedir. Kritik kütle, yeni kullanıcılara sağladığı faydaların, yeni teknolojiyi benimseme maliyetini aştığı noktadır. Dijital para birimi gibi bazı teknolojilerde, yeni bir kullanıcının elde ettiği yarar, teknolojiyi çoktan benimsemiş olan diğer kullanıcı sayısı ile birlikte artmaktadır. Böylece tüm kullanıcılara sağladığı toplam fayda, kullanıcı sayısı ile doğru orantılı şekilde artmaktadır. Bu ağ etkisi olarak tanımlanmaktadır (Varian, 2013). Bir teknoloji kritik kütleye ulaştığında ve onu geçtiğinde, olumlu geri bildirim devreye girmekte ve teknolojinin benimsenmesi patlayıcı hale gelmektedir.

Bitcoin'in bir değişim aracı olarak yaygın şekilde benimsenmesi için kritik kütleye henüz ulaşılamadığı işlem hacmi büyüklüğü ve piyasa değeri bakımından incelendiğinde görülmektedir. Ancak sanal para birimleri hakkında olumlu düşünceye sahip ekonomistler tarafından Bitcoin 'in büyümesinin doğal olarak birkaç döngüden geçtiği iddia edilmektedir. Son döngünün, 2013 yılı sonunda teknolojik gelişmelere adapte olabilmeyi başarmış yeni nesil için kritik kütle noktasını geçtiği ve ardından doğal bir konsolidasyon dönemi geldiği öne sürülmektedir. Girişimcilerin ve düzenli kullanıcıların sanal paralardan istifadesini sağlayacak gelişmiş bir teknolojik altyapının oluşturulduğu ve böylece bir sonraki büyüme dalgası için temel atıldığı kanaati taşınmaktadır (Vlasov, 2017).

Sanal para birimleri ile gerçekleştirilen işlemler kredi kartı ile yapılan alış verişlere nazaran çok daha hızlı ve güvenli bir şekilde gerçekleşmektedir. Madenciler tarafından alınan onaylama işlemlerinin getirdiği maliyetler hâlihazırda kredi kartı komisyon ücretlerinden düşüktür. Buraya kadar ifade edilen hususlar sanal paraların değişim aracı olarak kullanılmasının olumlu yanları olarak sıralanabilir.

Bitcoin ve diğer sanal para birimlerinin oluşturulması adına merkezi bir otoriteye ve bu paraların korunması için banka yahut başkaca bir kurumun varlığına ayrıca para transferi için de elektronik para transferini gerçekleştirecek bir merkeze ihtiyaç duyulmadığından saklama ve transfer maliyetleri minimuma inmektedir (Gültekin & Bulut, 2016).

Konunun diğer tarafında ise sanal para üreticileri yani madencilerin sanal para üretimindeki performansları ve madenciliğin sürdürülebilirliği hakkındaki endişeler yatmaktadır. Madenciler tarafından faaliyetleri karşılığında elde ettikleri ödül ve komisyon gelirlerinin rekabet ve yarılanma sürelerinin sonunda kazanacakları Bitcoin miktarının yarı yarıya azalması, sanal paraların geleceği hakkındaki endişeleri artırmaktadır. Madencilik endüstrisi içi yatırımların pahalılığı ve madencilere ödenen komisyonların kredi kartı komisyon oranlarına yakınlaşması sanal paraların cazibesine gölge düşürebilecektir.

Girişimcilerin elde ettikleri sanal paralarının sanal ortamlardaki saldırılara karşı korunması gerekliliği ve geri dönülemez hatalı ödemeler de sanal para birimlerinin değişim aracı olarak kullanılması yönündeki eleştirilerden biridir. Özel anahtarların güvenli bir şekilde korunması zorunluluğu, son dönemlerde sık karşılaşılan sanal cüzdanlara ve sanal para borsalarına karşı yapılan siber saldırılar bu eleştirilerin haklılığını ortaya koymaktadır. Satıcıların kredi kartı ödemelerinde müşterilerin satın alınan malları iade talebi etmesi halinde söz konusu tutarları geri ödemesi birkaç gün sürse de sanal paralarla yapılan ödemelerde hatalı bir durumun ortaya çıkması sonucu ödemenin geri iadesi imkânsız olduğundan tüketicinin bu konuda çaresiz olması bir diğer olumsuz duruma örnek gösterilebilir.

2.5.7.2.3. Değer Saklama Aracı Olması

Sanal para birimlerinin değer saklama aracı olarak görülmesinin önündeki en büyük engel olarak bu para birimlerinin değerlerinde görülen aşırı oynaklık ve fiyat istikrarsızlığı gösterilmektedir. Finansal piyasalardaki genel kanı; sanal para birimlerinin değer saklama aracı olmaktan çok riskli bir yatırım aracı olduklarıdır.

Piyasadaki toplam Bitcoin sayısı ile işlem yapılan Bitcoin miktarı karşılaştırıldığında yastık altı olarak tabir edilen miktarın piyasalarda işlem gören miktardan oldukça fazla olduğu anlaşılmaktadır (Franco, 2015). Bu durumda spekülasyon amaçlı sanal para talebinin yüksek olduğu düşüncesini uyandırmakta ve elde tutulan yüksek miktardaki sanal paralar ile değişim aracı olarak kullanımının önünde engel teşkil etmektedir.

Ancak unutulmamalıdır ki eğer bir değer atfedilmesiydi Bitcoin ve diğer sanal para birimleri talep edilmezdi. Değeri olduğu düşünülen bir metanın da değişim aracı ve değer saklama aracı olarak kullanılmasının normal bir davranış olduğu muhakkaktır. Sanal Paraların değer saklama aracı olma özelliklerinin diğer varlıklarla karşılaştırılması Tablo 15’ te yer almaktadır.

Tablo 15
Değer Saklama Araçlarının Özelliklerinin Karşılaştırılması

Banka Enstrümanları	Nakit/Madeni	Bitcoin
Faiz ödemesi vardır.	Faiz ödemesi yoktur.	Faiz ödemesi yoktur ancak değer artışı olabilir.
Karşı taraf riski barındırır.	Erişimi ve kullanımı kolaydır.	Anonimdir Yüksek fiyat oynaklığı vardır. Yasal statüsü yoktur.
Vergi kesintisi ve haczedilmeye konudur.	Hırsızlık ve kaybedilme riski vardır.	Hırsızlık ve kaybedilme riski vardır.
Kur riski taşır.	Kur riski taşır.	Kur riski taşır.
Transfer ücretleri yüksektir. Transfer süreleri birkaç günlük zaman dilimi içinde gerçekleşebilmektedir.	Transfer ücretleri yüksektir. Transfer süresi 1 ila 3 gün arasındadır.	Yüksek miktardaki transferler dahi daha kolay, ucuz ve birkaç dakika sürebilecek kadar hızlıdır.

Kaynak: (IMF, 2019)

2.5.7.2.4. Para Politikası Aracı Olarak Sanal Paraların Değerlendirilmesi

a) Finansal piyasalara girişte sermaye yetersizliği ve yüksek maliyetler yatırımcılar için önemli engeller teşkil etmektedir. Sanal paraların ise bu engelleri azalttığı ve küçük yatırımcıların da (ödeme işlemcileri, borsalar veya havale sağlayıcıları vb.) piyasalarda var olmasını sağladığı savunulmaktadır. Bu durum elbette piyasalarda rekabeti artırarak, kar marjlarının düşmesine neden olmakta ve bankalar gibi diğer finansal kuruluşların teknolojik alt yapılarına daha fazla yatırım yapmalarını gerektirmektedir (Böhme, Christin, Edelman, & Moore, 2015).

b) Mevcut finansal kurumlar için bir başka risk ise piyasalardaki tasarruf sahiplerinin varlıklarının önemli bir kısmını sanal para birimleri cinsinden

saklamayı tercih etmeleri durumunda bankaların mevduatlardan elde etikleri faiz getirileri ve devletin vergilerden elde ettiği gelirlerin azalmasına neden olabilecektir.

c) Tartışma konusu olan diğer bir husus da bankalar tarafından uygulanan ve bankacılığın en önemli işlevlerden biri olan kısmi rezerv bankacılığının sanal paralar ile yapılmasının mümkün olup olamayacağıdır. Sanal para sahiplerinin sahip oldukları paraların az bir kısmının bankalar tarafından tutulup büyük bir kısmının ise kredi olarak fon talep edenlere borç olarak verilmesine, kısaca kısmi rezerv bankacılığına itiraz edip etmeyecekleri bilinmemektedir (Tapscott, 2016). Olumsuz bir durum karşısında bankalar kısmi rezerv bankacılığı ile elde ettikleri parasal büyüme ve kar tutarlarından mahrum kalabileceklerdir.

Buraya kadar anlatılan gelişmeler para politikalarının efektif bir şekilde uygulanmasının sağlayıcılarından olan ve finansal piyasaların önemli bir aktörü durumundaki bankaların ve finansal kurumların sanal paraların kullanımının yaygınlaşması durumunda parasal arz da ve karlılıklarında gerçekleşebilecek etkileridir.

d) Para politikası araçları birinci bölümde de anlatıldığı gibi merkez bankaları tarafından kullanılmakta ve para arzının kontrolünü sağlamaktadır. Sanal para birimlerinin kullanıldığı bir ortamda merkez bankası gibi son kredi merciinin bulunmaması, merkez bankalarının açık piyasa işlemleri, kredi tavanı belirleme ve zorunlu karşılıklar gibi kamu gücünün belirlediği para politikası hedeflerine ulaşabilmek için uygulayacağı enstrümanları etkisiz bırakacaktır.

e) Diğer taraftan paranın miktar teorisi göz önüne alındığında hem paranın dolaşım hızının hem de bir ekonominin reel çıktısının sabit olması halinde, para arzındaki bir artışın, fiyat düzeyinde bir artış yaratacağı görülmektedir. Bu teorinin ekonomi çevrelerinin çoğunluğu tarafından uzun vadede geçerli olduğu kabul edilmektedir. Sanal para birimlerinin piyasalarda kullanımının arttığı ve fiyat paranın nispeten azaldığı düşünüldüğünde denklemdeki paranın değişim hızı (V)'nin artacağı ve denklem gereği enflasyona neden olacağı, bu durum karşısında para otoritelerinin sıkılaştırıcı para politikalarını uygulamaya zorlayacağı düşünülmektedir (Franco, 2015).

f) Sanal paraların para politikaları adına olumlu etkileri üzerinde düşünüldüğünde ise tıpkı altın standardı gibi para arzının sahip olunan sanal para ile ilişkilendirilmesinin ülke ekonomilerinin cari açıklarının azaltılması ve enflasyonist etkilerden kurtulması yolunu açabileceği vurgulanmaktadır. Ayrıca ülke para biriminin yanında merkez bankası tarafından çıkarılan ve denetimi yapılan sanal para birimleri ile genel olarak ekonominin direncinin artırılabileceği, kargaşa veya mevcut finansal yapıların işlevsiz kaldığı durumlarda faydalı olabilecek alternatif bir ödeme sisteminin yaratılabileceği savunulmaktadır (Houben & Snyers, 2018).

2.6. Sanal Paraların Olası Ekonomik Etkileri

Çalışmanın içeriğini oluşturan sanal para birimleri ve Blokzincir teknolojisinin yakın gelecekte hâlihazırda kurulu sistemlerin değişim veya dönüşümlerine etki edebilecek önemli bir gelişme olduğu görülmektedir. Bu dönüşüm, alış verişlerde kullanılabilecek bir para olarak hayata geçen sanal paranın yalnızca değişim aracı olma özelliğini şu anki haliyle bile aştığı, konvansiyonel paraların etki ettiği ekonomik ve sosyal hayatın birçok değeri ile de yakından ilgili olduğu anlaşılmaktadır. Çalışmanın bu bölümünde söz konusu etkiler, ana hatlarıyla önemli ekonomik başlıklar altında, beklenen olumlu ve olumsuz etkileri ile incelenmiştir.

2.6.1. Bankacılık Sektörüne Etkileri

Para olgusuyla hayatımızla bütünleşmiş en önemli kurumlardan biri hiç şüphesiz bankalardır. Fon fazlası olan bireyler ile fon talep edenler arasında bir köprü durumundaki bankalar bu işlevlerini güven esasına bağlı olarak yerine getirirler. Bankalar, fon transferlerinde taraflar arasında gerçekleşen işlemlerin doğru, ispatlanabilir ve güvenli bir şekilde yapılabilmesi adına merkezi ya da diğer bir ifadeyle güvenilir üçüncü taraf görevini üstlenmektedirler (Ball, 2012). Ancak Blokzincir teknolojisinin anlatıldığı bölümde de altı çizildiği gibi sanal para teknolojisi ile güvenilir bir üçüncü taraf ya da merkezi bir otoriteye ihtiyaç

duyulmadan gerçekleşen işlemler sayesinde önemli ölçüde etkilenebilecek kurumların başında bankacılık sektörü gelmektedir.

Bankalar para transferlerini SWIFT ve EFT adı verilen sistemlerle gerçekleştirirler. Bu sistemlerde yapılan işlemler, fon sahipleri açısından yüksek maliyetli ve zaman alan işlemlerdir. SWİFT işlemleri uluslararası transferlerin gerçekleştirildiği sistemler olup, komisyon ücretleri transfer edilen miktara göre değişmekte, süre olarak da en az 3 gün almaktadır. Ayrıca bu sistemlerde ödeme miktarı belli bir tutardan az olması durumunda işlem maliyeti transfer edilmek istenen tutarı dahi aşmaktadır. Ancak fon transferleri sanal para ödeme ve transfer işlemlerinde daha ekonomik ve hızlı şekilde (birkaç saniyede) yerine getirilebilmekte, diğer taraftan sanal paralarla oldukça küçük meblağlarda da para transferleri çok düşük maliyetlerle yapılabilmektedir. Örneğin Ripple sanal para birimi ile milyarlarca doların transferi 0.05 $ karşılığında ve 3 saniyede Dünya'da ki her hangi bir noktaya yapılabilmektedir (Gültekin, 2017).

Diğer taraftan bankalar, müşteri bilgileri, işlemlerin gizliliği ve güvenliği için her yıl yüksek miktarda bilişim altyapısı yatırımlarını gerçekleştirmek zorunda kalmakta, bunu yaparken de istihdam ettikleri personel ve siber alt yapıları için oldukça yüksek maliyetlere katlanmaktadırlar. Söz konusu durumlar bankacılık sisteminin sanal para teknolojisi ile etkilenebilecek zayıf yönleri olarak sıralanabilir. Bankacılık sektörünün blokzincir tabanlı teknolojilerin kullanıldığı sistemlere entegre olması ile bu dezavantajlı durumu aşması kendileri adına daha akılcı olabileceği söylenebilir.

2.6.2. Enerji Tüketimine Etkileri

Sanal paralar, yüksek elektrik enerjisi kullanan bilgisayarlar tarafından gerçekleştirilen işlemler sonucunda oluşturulmaktadır. Sanal para transfer işlemlerinin gerçekleşebilmesi için de yine sistemde bu görevi yerine getiren madenciler tarafından işlem gücü yüksek bilgisayarlarla zamana karşı yarışılmaktadır. Her geçen gün teknolojinin gelişmesi ile beraber sabit blok üretim süresinin (10 dakika) varlığı nedeniyle rekabet halindeki madenciler tarafından yüksek işlem güçlü ancak enerji tüketimi de aynı derecede yüksek bilgisayarlar kullanılmaktadır. Bu bilgisayarlar enerji sarfiyatını artırmakta, diğer yandan

işlemlerin gerçekleştirildiği bilgisayarların soğutulması için ek enerji tüketimine de neden olunmaktadır.

Bitcoin sisteminin bir yılda tükettiği elektrik miktarı ortalama 53.16 TW/H'dir. Bu tüketim yaklaşık olarak Romanya'nın bir yılda tükettiği elektrik enerjisine eşittir. Yine Bitcoin üretilen tüm sistemin bir yılda tükettiği elektrik miktarı Dünya genelinde tüketilen elektriğin yaklaşık %0,24'üdür. Tüm madencilerin tükettiği elektrik enerjisinin maliyeti yaklaşık 2,6 Milyar ABD Dolarıdır. Eğer Bitcoin sistemi bir ülke olsaydı, Dünya'da elektrik tüketimi sıralamasındaki 48. ülke konumunda olacaktı (De Vries, 2019).

Sanal para sistemlerinde yüksek elektrik tüketiminin varlığı bir gerçek olmakla birlikte, banknot basma, sahte banknot üretiminin engellenmesi adına yapılan çalışmalar, kalpazanlık suçunun önlenmesine yönelik yatırımlar ve bankacılık sisteminin güvenliğinin sağlanması için gerçekleştirilen siber alt yapı çalışmalarındaki enerji sarfiyatı ve maliyetler, yalnızca VISA ve MASTERCARD sistemlerinin yıllık söz konusu maliyetleri göz önüne alındığında (8,4 Milyar ABD Doları) yukarıda yer verilen elektrik tüketim maliyetlerine nazaran oldukça yüksektir (Ali, Barrdear, & Southgate, 2014). Bitcoin üretimi sırasındaki çevreye verilen zararın da bir gerçek olduğu (karbon emisyonu miktarı) muhakkaktır. Ancak bankacılık sektörünün çevreye etkisi ile karşılaştırabilecek bir veri bulunmadığından bu konuda yorum yapabilmek güçtür.

Enerji tüketiminin yüksek maliyetleri, tüm sanal para birimleri için geçerli değildir. Söz konusu maliyetler, POW (Proof of Work) sistemi ile rekabetin ve hızın oldukça önemli bir yere sahip olduğu sistemler yerine Ethereum sanal para biriminin teknik alt yapısını oluşturan ve önceki bölümlerde açıklanan POS (Proof of Stake) sistemi kullanılarak enerji sarfiyatının % 90 oranında azaltılabileceği ve enerji maliyetlerinde tasarruf sağlanabileceği de göz önünde bulundurulmalıdır (Dourado & Brito, 2014).

2.6.3. İstihdama Etkisi

Sanal para birimleri, madenci adı verilen kişiler tarafından gerçekleştirilen işlemlerle devamlılığını sağlamaktadır. Bu kişiler işlemlerin bloklar haline getirilip ana zincire eklenmesi görevini yerine getirmeleri karşılığında belirli bir

komisyon ücreti ile kullandıkları bilgisayarlar yardımıyla zor matematiksel şifrelerin çözümlenmesi sonucunda sistem tarafından kendilerine ödül olarak verilen sanal paralarla gelir etmektedirler.

Madencilik faaliyetleri, sistemin yüklenebileceği teknolojik kapasiteye sahip bilgisayarlarla yapılabilmektedir. Gelişmiş teknolojik özellikleri ve yüksek işlem hızına sahip bilgisayarların ortaya çıkması ile de Dünya genelinde madencilik faaliyetlerini gerçekleştiren kişi sayısı hızla artmaktadır. Ancak sanal para birimleri, akıllı kontratlar ve blokzincir teknolojisinin gelecekte kullanımlarının artması ve bu sistemlerin yaygınlaşması ile bankacılık sektörü başta olmak üzere, finans, lojistik, hukuk, perakende ve tapu sicili gibi birçok sektördeki çalışanların atıl durumda kalabileceği, diğer bir ifade ile bu sektörlerde işsizliğin artabileceği düşünülmektedir (Filipova, 2015). Sanal para birimlerinin işleyişinde yer alan madenci sayısının işini kaybedebilecek kişi sayısı karşısında oldukça kısıtlı bir sayıda kalacağı tahmin edilmektedir. Teknolojinin kullanıldığı her sektörde karşılaşılan işsizlik olgusu ile sanal para sistemleri ve teknolojik alt yapılarının yaygınlaşmasıyla da tekrar karşı karşıya kalınabileceği düşünülmektedir.

Diğer taraftan sanal para birimlerinin kullanımının artmasıyla önceki bölümlerde de yer verilen para ve maliye politikalarının etkisinin azalacağı, kamu otoritesinin istihdam ve büyümeye yönelik politikalarını gerçekleştirebilecek araçlarının etkisiz kalmasına, başta senyoraj ve vergi gelirleri olmak üzere merkezi bütçenin gelirlerini oluşturan kalemlerden mahrum kalacağı da göz önünde bulundurulması gereken hususlardır.

2.6.4. Dış Ticarete Etkileri

Blokzincir ve dağıtık defter teknolojilerinin kullanıldığı bir diğer yeni gelişme de akıllı kontratlar (smart contrat)'dır. Bu kontratlar, iki taraf arasında gerçekleşen ve tarafları bir yükümlülük altına sokan durumlarda yine tarafların yükümlülüklerini yerine getirmesi akabinde karşılıklı olarak sonuç doğuran sözleşmelerdir (Franco, 2015). Bu sözleşmelerin işleyişi kısaca anlatılacak olursa; taraflar arasında kontratın şartları belirlenip kontrat bedeli, ödeme zamanı ve diğer şartlar Blokzincirde bir blok haline getirilir. Söz konusu kontrat içeriğinde

taraflarca yerine getirilmesi gereken şartlar ifa edildiğinde kontrat işleme girer ve kontrat bedeli de transfer edilir.

Dış ticarette mal ve hizmetlerin karşılığının satıcıya iletilmesinde, alınan malın veya hizmetin istenen şekil, cins ve özelliklere sahip olmasında güven unsurunun önemi oldukça büyüktür. Bu durumda bu güven problemi yine üçüncü bir tarafça sağlanmakta, mal veya hizmetin intikali ile bedelinin ödenmesi bu üçüncü taraflarca garanti altına alınmaktadır. Güncel hayatta söz konusu mal bedelinin ve çeşitli gümrük ve dış ticaret vesaikinin iletimi ve güvenliği bankalar aracılığıyla akreditif gibi işlemlerle yerine getirilmektedir (Hubbard, 2002). Ancak akıllı kontratların kullanılması ile üçüncü bir taraf olmaksızın dış ticarette; kontratlarda yer alacak şartlar doğrultusunda mal veya hizmetin ve ilgili vesaikin teslimiyle karşı tarafa ödeme yapılacağı ve taraflarca konulmuş diğer şartların yerine getirilmesi ile sözleşmenin geçerli olacağı belirtildiğinden güvenli, hızlı ve daha düşük maliyetleri içeren bir dış ticaretin ortaya çıkabileceği düşünülmektedir. Nitekim bu alanda akıllı kontratların üretilmesi ile ilgili faaliyetlerini sürdüren IBM, Fluent ve Blockverify gibi şirketler, sektörde akıllı kontratların kullanımının yaygınlaşmasında önemli rol oynamaktadır (Güven & Şahinöz, 2018).

2.7. Sanal Para İle İlgili Devlet ve Kurum Değerlendirmeleri

Her geçen gün hızla büyüyen kripto para birimi piyasasının dikkat çekici özelliklerinden birisi, söz konusu para birimlerinin temel aldıkları teknoloji ve kullanım amaçları açısından benzerlikleri taşısalar da farklı coğrafyalarda ve o coğrafyalara ait yasal mevzuat sistemlerinde tanımlanmaları için kullanılan terimlerin farklılıklar göstermesidir. Yaygın olarak "kripto para birimleri" olarak ifade edilmelerine karşın sanal para çeşitlerinin ülkeler tarafından kripto para birimi ifadesini referans alarak kullandıkları terimlerden bazıları şunlardır (Ray, 2018);

- Dijital Para Birimi → Arjantin, Tayland ve Avustralya
- Sanal Emtia → Kanada, Çin ve Tayvan
- Kripto-Token → Almanya
- Ödeme Belirteci → İsviçre

- Siber Para Birimi → İtalya
- Elektronik Para Birimi → Kolombiya ve Lübnan
- Sanal Varlık → Honduras ve Meksika
- Sanal Para Birimleri → Türkiye

Sanal para birimleri ile ilgili kamu otoritelerinin en yaygın reflekslerinin başında bu para birimlerinin ihraç edildiği piyasalara yatırım yapmanın riskleri hakkında ülke vatandaşlarının bilgilendirilmesi gelmektedir. Çoğunlukla merkez bankaları tarafından verilen bu tür uyarıların kapsamında, vatandaşları devlet güvencesi ile emisyonu yapılan konvansiyonel para birimleri ile herhangi bir yasal güvence altında olmayan sanal para birimleri arasındaki farkların gösterilmesi ve sanal para birimlerinin yüksek fiyat oynaklıkları ile bu tür işlemlerin gerçekleştirildiği organizasyonların (borsa vb.) çoğunun yasal düzenlemelere konu olmadığıdır. Ayrıca, sanal para birimlerine yatırım yapan vatandaşların karşılaşabilecekleri her türlü riskin kendilerine ait olduğu ve zarar durumunda yasal bir güvence verilemeyeceği anlatılmaya çalışılmaktadır.

Diğer taraftan çeşitli ülke yargı organları tarafından sanal para birimlerinin para aklama ve terörizm gibi yasadışı faaliyetler için yarattığı fırsatlara dikkat çekilmekte, kamuoyunun sadece uyarılması ile de kalınmamakta para aklama, terörle mücadele ve sanal para birimi piyasalarını da içerecek şekilde organize suçlar konusunda mevcut yasalarını genişletmektedirler. Söz konusu para birimleriyle yapılan işlemlerin yasal şartları yerine getirebilen bankalar ve diğer legal finans kurumları tarafından gerçekleştirilmesini talep etmekte bu tedbirlerden birini oluşturmaktadır. Buna örnek olarak Avustralya ve Kanada'nın 2017 yılında para aklama ve terörle mücadele finansman yasaları çerçevesinde illegal faaliyetleri kolaylaştıran sanal para birimi işlemleri ve bu işlemlerin gerçekleştirildiği kurumları daha titiz bir şekilde denetim altında tutabilmek amacıyla yeni yasalar çıkarmıştır (Loc, 2017).

Bir diğer önemli bir hususta sanal paralardan elde edilen gelirlerin hangi vergi grubu altında inceleneceği ve yasal olarak vergi takibinin ve tahsilatının nasıl gerçekleştirileceğidir. Bu konuda sanal paraların işlem gördüğü ülkelerde ortak bir görüş bulunmamaktadır. Ancak yasal olarak izin verilen işlemler için ülkeler arasında az da olsa farklı vergilendirme türleri görülmektedir.

Sanal para birimlerinin hangi vergi başlığı konusu olduğu hususunda farklı yaklaşımlar, Tablo 16' da yer alan aşağıdaki ülkeler nezdinde örneklendirilmiştir.

Tablo 16
Sanal Para Birimlerinin Vergilendirilmesi

ÜLKE		VERGİLENDİRME
İsrail	→	Menkul değer olarak vergilendirme
Bulgaristan	→	Finansal Varlık olarak vergilendirme
İsviçre	→	Döviz varlığı olarak vergilendirme
Arjantin & İspanya	→	Gelir Vergisi Olarak
Danimarka	→	Gelir Vergisi Olarak (Zararlar Vergiden Düşülebilir)
Türkiye	→	Herhangi Bir Düzenleme Bulunmamaktadır.

Kaynak: www.loc.gov/law/help/cryptocurrency/world E.T:20.08.2019

Bir takım ülkeler ise daha da ileri giderek sanal para birimlerinin yatırım ve değişim aracı olarak kullanılmasına kısıtlamalar getirmiştir. Bu ülkelere örnek olarak Cezayir, Bolivya, Fas, Nepal, Pakistan ve Vietnam verilebilir (IMF, 2019).

Ancak her ülke farklı nedenlerle de olsa, blok zinciri teknolojisinin ve sanal para birimlerinin gelişimini bir tehdit olarak görmemektedir. Tam aksine sanal paraların arkasındaki teknolojide önemli bir potansiyel görmekte ve bu sektörde öne çıkan teknoloji şirketlerinin yatırımlarını çekme amacıyla sanal para birimi dostu yasal düzenlemeleri hayata geçirmektedirler. Bu grupta yer alan ülkeler İspanya, Belarus, Cayman Adaları ve Lüksemburg olarak sıralanabilir (Varian, 2013).

Sanal para teknolojisinde daha önde ve avantajlı olmak isteyen, kendi sanal para birimleri sistemlerini geliştirmeye çalışan ülkeler de bulunmaktadır. Bunlara Marshall Adaları, Venezuela, Doğu Karayipler Merkez Bankası (ECCB) üye ülkeleri ve Litvanya'dır (www.coinmarketcap.com E.T:19.08.2019). Ayrıca, halka kripto para birimleri cinsinden yatırımların tuzakları hakkında uyarılarda bulunmakla beraber bazı ülkeler de kripto para birimi piyasasının büyüklüğünün bu noktada yasal düzenlemeyi veya bir yasaklamayı gerektirecek kadar olmadığını düşünen ülke yönetimleri de vardır; Belçika, Güney Afrika ve Birleşik Krallık (Berentsen & Schär, 2018).

Sayıları az da olsa kimi ülkelerde sanal para birimlerinin değişim aracı olarak kabul edildiği de görülmektedir. İsviçre'nin Zug Kantonunun tümünde ve Ticino kantonu içindeki bazı illerde kripto para birimleri devlet kurumları tarafından bile bir ödeme aracı olarak kabul edilmektedir. Ayrıca Man Adası ve Meksika kripto para birimlerinin ulusal para birimlerinin yanı sıra bir ödeme aracı olarak kullanılmasına da izin vermektedir. Dünyanın dört bir yanındaki devlet tahvillerini satarak çeşitli projeleri finanse eden hükümetler gibi, Antigua ve Barbuda hükümetleri, hükümet destekli ICO'lar (İnitial Coin Offering-İlk Coin Arzı) aracılığıyla projelerin ve yardım kuruluşlarının finanse edilmesine izin vermektedir (Dourado & Brito, 2014).

Yukarıda genel olarak ülkelerin sanal para birimi ve türevlerine karşı gerçekleşen farklı resmi mevzuat tarzları sıralanmış olup aşağıdaki kısımda da Dünya'nın önemli finansal piyasalarına ev sahipliği yapan ülkelerin spesifik olarak sanal para birimlerine olan yaklaşımları incelenecektir. Son olarak ta Türkiye de sanal para birimleri hakkındaki yasal düzenleme ve değerlendirmeler Bankacılık Düzenleme ve Denetleme Kurumunun yayınladığı bildiri ışığında aktarılacaktır.

2.7.1. ABD

ABD'nin sanal para birimlerinin ortaya çıkması akabinde ilk tepkisi temkinli hareket etmek olmuştur. Yaklaşık bir yıllık bir değerlendirme sürecinin ardından ABD Hazine Müsteşarlığının 2013 yılı sonunda yayınladığı raporda (FINCEN-The Financial Crimes Enforcement Network- Finansal Suçları Engelleme Ağı- Raporu) sanal para birimlerinin ilki olan Bitcoin konvertibl bir sanal para birimi olarak tanınmıştır. Vergilendirme kapsamında sanal para üreticilerinin gelir vergisine tabi olacağı, alım satım işlemlerinin faturalanmasının gerektiği bildirilmiş (2014) ve ABD'nin New York eyaletinde aracı kurumlar için bu kapsamda ilk ve tek olan BitLisans şartı konmuştur (Sackheim & Howell, 2018). Bu lisans ile Bitcoin'lerin takas platformlarının uyması gereken kurallar ayrıntılı bir şekilde sıralanarak kara para aklama gibi suç teşkil eden hususlarda sorumluluğun bulunduğu vurgulanmıştır.

Federal düzeyde, ABD Menkul Kıymetler ve Borsa Komisyonu (SEC), menkul kıymetler veya yatırım sözleşmeleri olarak teklif edilmeleri veya alınıp satılmaları veya toplu bir yatırım fonu aracılığıyla teklif edilmeleri durumunda sanal para ve ICO işlemlerini düzenlemekle yetkili kurumdur. SEC, Haziran 2018'de Winklevoss Bitcoin Trust'ın proje olarak arz edilmesini onaylamamış, Bitcoin pazarlarının manipülasyona açık olduğunu, hileli ve manipülatif eylemlerle yatırımcıların ve kamu yararının sekteye uğrayabileceğini ileri sürmüştür (Sackheim & Howell, 2018).

ABD'de yine federal bazda türev piyasalarının düzenleyicisi olan ABD Emtia Vadeli İşlemler Ticaret Komisyonu (CFTC), sanal para birimlerinin kendi yetki alanına giren mallar olduğunu bildirmiştir. CFTC, ABD'de sanal para türev işlemleri üzerinde yargı yetkisine sahiptir ve CFTC'nin düzenlenmiş türev borsaları ile ilgili kurallarına uymadığını ileri sürdüğü sanal para türevlerinin alım satım işlemlerine karşı yasal yaptırım davaları açmıştır (Schroeder, 2016).

2.7.2. Çin

Çin devlet kurumlarının - Çin Siber İdaresi (CAC), Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT), Sanayi ve Ticaret Devlet İdaresi (SAIC), Çin Bankacılığı Düzenleme Komisyonu (CBRC), Çin Menkul Kıymetler Düzenleme Komisyonu (CSRC) ve Çin Sigorta Düzenleme Komisyonu (CIRC),- 3 Aralık 2013 tarihinde kamuoyu önünde sanal paralar hakkında bir bilgilendirme toplantısı düzenlemiştir. Bu toplantıda Bitcoin ve diğer sanal para birimlerinin üretilmesini ve kullanılmasını yasaklayan, ayrıca sanal paraların taşıdığı riskleri konu alan bir açıklama da bulunulmuştur. Açıklamada spesifik olarak ilk sanal para Bitcoin, "doğası gereği" resmi para birimleri ile eşit yasal statüye sahip olmayan ve piyasada para birimi olarak dolaşımının yasak olduğunun altı çizildiği "özel bir sanal meta" olarak tanımlamıştır (Xiaochuan, 2018). Çin'deki ödeme aracılarının sanal paralar ile işlem yapmaları yasaklanmıştır. Ayrıca 2014 yılından itibaren Çin Merkez Bankası ve diğer kamu bankaları Bitcoin takas platformlarına hizmet sağlamayı bırakmışlardır. Buna karşın Çin'in merkez bankası olan Çin Halk Bankası (PBOC), bir dijital para enstitüsü kurarak Çin'in kendi sanal parasının üretimi için çalışmalara başlamıştır (Yujian, 2017).

Sanal para birimlerinin işlemlerinin gerçekleştirildiği sanal borsalara ait verilerde, Çin ulusal para birimi Yuan (CNY)'ın sanal para işlemlerinde en çok kullanılan para birimi olduğu görülmektedir (Üzer, 2017).

2.7.3. Hindistan

Hindistan Rezerv Bankası (RBI) 2017 yılı başında sanal paraların taşıdığı riskler nedeniyle vatandaşlarını uyarmıştır. RBI, sanal para mübadelesi veya ICO anlaşmalarını düzenlemek ve denetlemek adına herhangi bir işletmeye veya kuruma lisans veya yetki vermediğini deklare etmiştir. Ancak hükümet yetkilileri sanal para birimlerinin alt yapısını oluşturan blokzincir teknolojisinin veya dağıtılmış defter teknolojisinin, finansal katılım ve finansal sistemin verimliliğini artırmada potansiyel yararları olabileceğini belirtmiştir (Ray, 2018). Hindistan hükümeti tarafından RBI'den gerekli çalışmaları gerçekleştirip dijital bir para çıkarmanın uygunluğunu ve talep edilirliğini araştırması istenmiştir. Nisan 2017'de oluşturulan komite 7 Ağustos 2017 tarihinde raporunu hükümete sunmuştur ancak raporun ayrıntıları kamuoyuyla paylaşılmamıştır (Reserve Bank of India, 2017).

29 Aralık 2017 tarihinde, Hindistan Maliye Bakanlığı, RBI'nın yerel bir sanal para üretimi çalışmalarına başladığını ancak halihazırdaki sanal para birimlerinin güvenilir olmadığını ifade ederek Bitcoin gibi kripto para birimleri cinsinden alım satım işlemlerinin spekülatif değer değişimlerine sahip olduğu bu yüzden önemli riskler barındırdığı açıklanmıştır. 2018'in başında ise Bitcoin ve diğer kripto para birimlerinin Hindistan'da yasal statülerinin olmadığını ve para yerine kullanılamayacaklarını belirtmiştir (Vishwanathan, 2018).

2.7.4. Rusya

Rusya hükümeti, Maliye Bakanlığı tarafından hazırlanan dijital finansal varlıklar hakkındaki yasa tasarısını 20 Ocak 2018'de parlamentonun alt kanadı Duma'ya sunmuş ve söz konusu tasarı 20 Mart 2018 de kabul edilerek yürürlüğe girmiştir (Petukhova, 2018). Tasarı da madencilik terimi, sanal para birimlerinin oluşturulmasına yönelik faaliyetler olarak tanımlanmaktadır.

Madencilik faaliyetlerinin hükümet tarafından belirlenen enerji tüketim sınırlarını arka arkaya üç ay boyunca aşması durumunda vergilendirmeye tabi girişimci bir faaliyet olarak kabul edileceği belirtilmiştir. ICO teklifleri için de ancak merkez bankası tarafından belirlenecek hususi durumlar dışında yalnızca nitelikli yatırımcıların katılmasına izin verilecektir (Zamakhina, 2018).

Sanal paralar mali belgelerde mülk olarak sınıflandırılması öngörülmüştür. Yasa da sanal para birimlerinin ruble veya başka bir döviz cinsi ile değişimine izin verilmezken, yapılacak alış verişlerde yalnızca lisanslı aracılar kullanılarak sanal para birimleri ile ödeme yapılabileceği ve işlemlere ait faturaların akıllı sözleşmeler olarak tanımlanması gerektiği yer almaktadır. Ayrıca Telekom ve Kitle İletişim Bakanlığı, dijital finansal varlıklar hakkındaki mevzuatında madencilik faaliyetinde bulunanların vergi mükellefi olmaları ve enerji tüketimi için alınan şartları uygulamaları koşuluyla madencilerin faaliyetlerini teşvik etmek amacıyla iki yıllık bir süre boyunca vergiden muaf tutulmalarını sağlamaktadır. Diğer taraftan sanal para birimi sahiplerinin haklarını korumak için medeni kanun 'da yapılan değişiklikle bu paralara sahip olan kişilerin vefat etmeleri durumunda dijital varlıklarını miras olarak bırakabilmesi sağlanmıştır (Gayva, 2018).

2.7.5. Avrupa Birliği

5 Temmuz 2016'da Avrupa Komisyonu, dördüncü kara para aklanmasını önleme direktifini (AMLD) değiştirmek için bir yasama teklifi sunmuştur. Bu teklifte AMLD kapsamında sanal cüzdanların korunması, sanal para birimlerinin takasının yapıldığı platformların düzenlenmesi ve yakından izlenmesi, ortaya çıkacak suiistimallerin önlenmesi ve raporlanması için politika ve prosedürlerin en kısa zamanda gerçekleştirilmesi gerektiği belirtilmiştir (ECB, 2018). Düzenleme teklifinde, sanal para birimleri, “bir merkez bankası veya kamu otoritesi tarafından oluşturulmamış ya da herhangi bir yerel para birimine bağlı olmayan ancak gerçek veya tüzel kişiler tarafından kabul edilen dijital özellikli temsili bir para” olarak tanımlanmıştır. Sanal para birimlerinin ödeme aracı olarak elektronik ortamda devredilebileceği ve depolanabileceği ayrıca sanal para alım satımının tüm AB üye ülkelerinde KDV'den muaf tutulacağı belirtilmiştir. 29 Ocak 2018'de Avrupa Parlamentosu ve Avrupa Konseyi’nin kurumlar arası

müzakerelerinde kararlaştırılan söz konusu metin komitede onaylanmıştır. Avrupa Parlamentosu söz konusu teklif 19 Nisan 2018'de yapılan genel kurulda kabul etmiştir. Güncellenen yeni AMLD direktifi, Avrupa Birliği Resmi Gazetesinde yayınlanmasından üç gün sonra yürürlüğe girmiştir (ECB, 2018).

Ayrıca, 8 Mart 2018'de, Avrupa Komisyonu, Blockchain, yapay zekâ ve bulut hizmetleri gibi finansal hizmetlerdeki teknolojiye dayalı yeniliklerin sunduğu fırsatlardan nasıl yararlanılacağına dair bir eylem planı sunmuştur. Bu eylem planında, dijital varlıkların taşıdığı risklerin ve fırsatların araştırılması, ekonominin tüm sektörlerini içine alacak bir dağıtık defter teknolojisi (DLT) konusunda kapsamlı bir strateji belirlenmesi amacıyla Avrupa Birliği Blokzincir Gözlemevi ve Forumu hayata geçirilmiştir (ECB, 2018).

Avrupa Merkez Bankası (ECB) Başkanı Mario Draghi, Bitcoin ve diğer dijital para birimlerinin yüksek volatilite ve spekülatif değer değişimleri nedeniyle "çok riskli varlıklar" olduğu konusunda Avrupa Birliği vatandaşlarını uyarmakla kalmamış dijital para birimlerinin belirli bir denetleme yapısı dahilinde bulunmadığı, sigorta ve emeklilik yatırımları için uygun olmadığını belirtmiştir (Draghi, 2016). Bunlara ek olarak, Aralık 2016'da Avrupa Merkez Bankası (ECB) ve Japonya Merkez Bankası (BOJ), finansal pazar altyapıları için dağıtık defter teknolojisinin olası kullanımına yönelik "Stella" adlı ortak bir araştırma projesi başlatmıştır.

2.7.6. Türkiye

Sanal para birimlerinin ülkeler nezdinde yasal tanımlarının yapılabilmesi, bu değerlerin mahiyetlerinin belirlenmesi, hukuki yaptırımlarının nevi ve nasıl vergilendirilecekleri açısından oldukça önemli bir husustur. Sanal para birimlerinin Türkiye' deki yasal statüsünün belirlenebilmesi için ödeme ve menkul kıymet mutabakat sistemlerinde mi yoksa elektronik para kuruluşları ve ödeme kuruluşları başlığı altında mı değerlendirileceği tartışma konusudur. Çünkü bir ödeme sistemi olarak kabul edilmesi durumunda Türkiye Cumhuriyet Merkez Bankası'nın kontrolü altına, e-para olarak değerlendirilmesi durumunda ise Bankacılık Düzenleme ve Denetleme Kurumunun görev alanına girmiş olacaktır (TCMB, 2018).

Transfer edilebilen bir menkul değerin e-para olarak kabul görülebilmesi için bir ülke para birimi cinsinden ölçülebilir ya da o ülke parasına endeksli olması gerekir. Türkiye Cumhuriyet Merkez Bankası'nın yayınlamış olduğu 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun'da e-para, ihraç edenin yükümlülüğü olarak ve fon karşılığı ihraç edilmek zorundadır. Sanal paralar için bu durum geçerli olmadığı için e-para olarak adlandırmamız mümkün değilse de yapısal olarak e-para ya yakın olmaları nedeniyle konu hakkındaki ilk ve tek resmi açıklama 25 Kasım 2013 tarihinde BDDK tarafından yapılmıştır (Üzer, 2017). BDDK açıklamasında elektronik para olarak değerlendirilemeyeceği için "kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir" denilen sanal para birimlerinin sakıncaları hakkında önemli uyarılarda bulunulmaktadır (BDDK, 2013). Bu uyarının nedenleri olarak da sanal para birimi işlemlerinde tarafların kimliklerinin belli olmaması, yüksek ve spekülatif değer değişikliklerine sahip olmaları, sanal paraların saklandığı dijital cüzdanların, kaybolma, çalınma veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi gibi risklerin bulunması ve gerçekleştirilen işlemlerin geri döndürülemez olmasından dolayı operasyonel hatalara ya da suiistimallere açık olması gösterilmiştir.

BDDK tarafından yapılan bu resmi basın bildirisi dışında ülkemizde sanal para birimleri hakkında herhangi bir mevzuat ya da kanunun bulunmaması nedeniyle sanal para piyasalarının güvenli bir yapıda bulunmadığı, ciddi bir yasal boşluğun var olduğu ileri sürülebilir.

ÜÇÜNCÜ BÖLÜM

3.TÜRKİYE'DE SANAL PARA DEĞERİNİN BELİRLEYİCİLERİ: BİTCOİN ÜZERİNE BİR UYGULAMA

3.1 Literatür Taraması

Bu bölümde çalışmanın içeriğini oluşturan Kriptoloji, Blokzincir teknolojisi ve sanal paralar hakkında ulusal ve uluslararası yazınlardan oluşan literatür taraması yapılmıştır. Söz konusu çalışmalar incelenirken öncelikle sanal para birimlerinin teknolojik alt yapısını oluşturan kriptoloji ve Blokzincir teknolojisi ile ilgili çalışmalar hakkında bilgi verilip akabinde sanal paralar hakkında yapılan çalışmalar incelenmiştir.

3.1.1 Kriptoloji ve Blokzincir İle İlgili Çalışmalar

İkinci bölümde de ifade edildiği gibi sanal paralar, kriptografik işlemlerle oluşturulan elektronik ortamda para olarak kullanılan ve eşler arası iş ispatına dayanan bir transfer protokolüdür. Çalışmada sanal para sistemlerini anlatmadan önce kriptolojinin nasıl ortaya çıktığı ve bu bilim dalının uygulamaları hakkında bilgi verilmişti. Literatür bölümünün bu kısmında geçmişte yapılan kriptoloji ve Blokzincirle ilgili çalışmalar yer almaktadır.

Akleylek ve Yıldırım (2011) çalışmalarında, kriptoloji biliminin tarihi, elektronik imzalar, açık anahtar altyapısı, kriptografik algoritmaların farklı alanlardaki uygulamaları hakkında bilgi vermiş, kriptolojinin her geçen gün geliştiği ve ülkemizde konu hakkında verilecek eğitimlerin önemli olduğunu vurgulamıştır.

Yerlikaya ve Buluş (2006) kriptolojik algoritmaların geçmişten günümüze kadar geçirdiği evreler, modern kriptografik algoritmalar özellikleri ve kullanıldıkları alanlar hakkında bilgi vermiştir.

Coşkun ve Ülker (2013) ise çalışmalarında bilgi güvenliğinin ulusal güvenlik açısından önemini vurgulayarak çağımızda siber sistemlerin konvansiyonel silahlardan daha fazla etkili olduğunu ve ulusal bilgi güvenliğini tesis edecek bir algoritmanın geliştirilmesinin gerekliliğini ele almıştır.

Obaid, Sabonchi ve Akay (2016) yaptıkları çalışmada klasik algoritmalar alanında incelenen Cesar, Vigenere, Vernam, Hill, Playfair algoritmalarının yapısal karakterlerini inceleyerek bu algoritmaların düz metin ve Base64 tabanlı görüntülerde etkinliklerini karşılaştırmışlardır. Düz metin ya da görüntüler şifreli hale getirilip sisteme girdi olarak verildiğinde ortaya çıkan algoritmaların şifreleme zamanı, şifre çözme zamanı, hafıza ve işlem hızı ile avantaj ve dezavantajlarını göstermişlerdir.

Kiani ve Taş (2018) Blokzincir yapısına, madencilik faaliyetlerine, P2P mimarisine ve uzlaşma protokollerine karşı gerçekleştirilebilecek siber saldırıları inceledikleri çalışmalarında nasıl bir savunma stratejisinin kurgulanması gerektiği üzerinde durmuş, gelecekte Post Kuantum Kriptografi 'sinin olası etkilerinden bahsetmişlerdir.

Ünsal ve Kocaoğlu (2018) Blokzincir yapısının içeriği, işleyişi ve kullanım alanlarına dair bilgiler vererek söz konusu teknolojinin alt yapısal açıklarının neler olduğunu ve kısa vadede Türkiye ve Dünya ölçeğinde ne gibi değişikliklere zemin hazırlayabileceği üzerinde durmuşlardır.

Özdoğan ve Kargın (2018) çalışmalarında Blokzincir teknolojisinin muhasebe ve finans sektörlerindeki potansiyel kullanım alanları ile kripto para birimleri, akıllı sözleşmeler ve ödeme altyapılarının muhasebesel kayıt ve denetimi konularında değerlendirmelerde bulunmuş, diğer taraftan blokzincir teknolojisinin muhasebe ve finans alanlarındaki avantaj ve dezavantajları hakkında bilgiler verilerek gelecekteki olası etkilerini ifade etmişlerdir.

Durğay ve Karaarslan (2018) ise Blokzincir teknolojisinin e-devlet uygulamalarında gün geçtikçe etkin bir teknolojik uygulama haline geldiğinden bahisle, blokzincir teknolojisi ile e-devlet'in birlikte uygulanabildiği hususları örnekler halinde sunarak e-devlet uygulamasında blokzincir uygulamalarının olası etkilerine değinmişlerdir.

Dülger (2018) yaptığı çalışmada Blokzincir teknolojisinin bir takım hukuksal alanlarda kullanılabilirliğini tartışarak akıllı sözleşmeler, ticari faaliyetlerin hukuksal alanlarda blokzincir teknolojisi ile ilişkileri, noterlik işlemleri, oy kullanma ve blokzincir teknolojisinin kullanılarak gerçekleştirilen hukuka aykırı eylemlerin mahiyetini değerlendirmiştir.

Natarajan (2017), Dağıtılmış defter teknolojisinin (DLT) tanımını, gelişimini ve DLT'nin kullanıldığı alanlar ile gelecekte potansiyel kullanım alanlarının etkinliğini incelediği çalışmasında dijital paralar ile DLT'ler arasındaki ilişki, avantajlar, karşılaşılabilecek riskler ve finansal piyasalarda yaratacağı etkileri ifade etmeye çalışmıştır.

Avunduk ve Aşan (2018), Blokzincirle gerçekleştirilen sanal para yaratma süreçlerini detaylı bir şekilde incelemiş, söz konusu teknolojinin günümüzdeki kullanım alanları ile yakın gelecekteki olası etkilerini olumlu ve olumsuz yaklaşımlar çerçevesinde irdelemiştir.

Balcısoy (2017) ise sanal para sistemlerinin oluşturulmasında kullanılan SHA256 algoritmasının optimizasyonu ile bu algoritmanın daha hızlı, kullanılan kaynaklar ve harcanan güç bakımından iyileştirilebilir olabileceğine yönelik uygulamalı araştırmasında Xilinx Virtex-7 FPGA kartında gerçekleştirdiği metotlarla SHA256 'nın performansının %7 artırılabildiğini, kullanılan enerjide tasarruf sağlanabildiğini ve özet fonksiyonu oluşturma süresinin 1,8611 SHA256 işlem süresine düşebildiğini göstermiştir.

Zyskind ve Nathan (2015) çalışmalarında, kullanıcıların sahip oldukları verilerini aktarmaları ve kontrol etmelerini sağlayan merkezi olmayan yeni bir kişisel veri yönetim sistemi hakkında bilgi vermektedir. Bu uygulama da yeni bir blokzincir teknolojisi kullanılarak, üçüncü bir tarafa güven gerektirmeyen otomatik bir erişim kontrol yöneticisinin sanal olarak var olduğu bir protokol uygulaması ile Bitcoin teknolojisinden farklı olarak, sistemdeki işlemlerin finansal olmadığı, daha çok veri saklama, sorgulama ve paylaşma gibi talimatların yer aldığı bir blokzincir uygulaması hakkında bilgi vermektedir.

3.1.2 Sanal Paralar İle İlgili Çalışmalar

Aslan (2019), Bitcoin gibi elektronik ödeme yöntemlerinin Borsa İstanbul ve New York Borsası'nda işlem gören hisse senetleri üzerindeki etkisini araştırdığı çalışmasında BİST hisse senetleri getirileri üzerinde etkisi tek değişkenli GARCH analizi ile beraber nedensellik testleri Cheung Ng ve Hafner Herwartz varyans nedensellik testlerini kullanmıştır. Ardından Dinamik Koşullu Korelasyon Modeli analizi ile volatilite modellemesini karşılıklı olarak değerlendirmiştir. Analiz sonuçlarına göre Bitcoin ve BİST hisse senedi gelirleri arasında karşılıklı nedensellik bulamamış ancak New York Borsası verileri ile ikinci gecikmede anlamlı etkileşme olduğunu belirlemiştir. Diğer taraftan New York Borsasının ise verileri ile Bitcoin borsasını etkilediği sonucuna ulaşmıştır.

Çelikhan (2019), Abramova ve Böhme tarafından geliştirilen anketi sosyal medya kullanıcıları üzerinde uyguladığı çalışmasındaki sonuçlara göre, Bitcoin kullanımı algısının kullanım kabulüne olumlu ve kullanımı artırıcı bir etkisi olduğu görülmüş, Bitcoin 'in taşıdığı itibar riskinin ise sanal para kullanımını azaltıcı bir etkiye sahip olduğu belirlenmiştir.

Teker (2019), Yatırımcıların sanal paralara olan yaklaşımlarının incelediği çalışmasında yüz yüze görüşme tekniği ile bir yatırımcının sanal para algısının ölçmeyi hedeflemiş, sanal paraların henüz istenen güven seviyesinde olmadığı, yasal düzenlemelerin hayata geçirilmemesi nedeniyle özellikle ülkemizde sanal para işlem hacminin Dünya ortalamasının altında kaldığı sonucuna ulaşmıştır.

Laçin (2019) çalışmasında, döviz piyasalarında işlem gören en büyük hacme sahip döviz paritelerinin, Bitcoin fiyatına etkisini incelemiş, 2014 ile 2018 yılları arasındaki döviz verilerini kullanarak yaptığı zaman serisi analizinde yalnızca Yuan/Dolar paritesinden Bitcoin/Dolar paritesine doğru pozitif bir nedenselliğin olduğunu, ancak diğer paritelerle Bitcoin fiyatı arasında herhangi bir nedensellik ilişkisinin bulunmadığını tespit etmiştir.

Ketenci (2005) Teknolojik gelişmeler sonrasında günlük hayatta her geçen gün artan farklı ödeme sistemlerinin nakit para kullanımına yönelik etkilerini araştırdığı çalışmasında anket yöntemi kullanarak, bireylerin yeni ödeme sistemleri hakkındaki algısı ve güvenlerini ölçmüş, nakit para olgusunun

yeni gelişmeler karşısında kullanım arzusunun anlamlı bir değişikliğe uğramadığı sonucunu elde etmiştir.

Gültekin (2017) Sanal para birimlerinin piyasada işlem gördükleri tarihten bu yana piyasa büyüklükleri, değerleri ve oluşturuldukları algoritmalar üzerinden alt gruplara ayrıldığı çalışmasında söz konusu grupların aralarında istatistiksel açıdan volatiliteleri arasında anlamlı bir fark olup olmadığını incelemiştir. Sonuç olarak da işlem görmeye başladıkları tarih bakımından alt gruplara ayrılanlar arasında anlamlı bir fark olduğunu görmüştür. Korelasyon testleri sonucunda ise piyasada bulunma süresi ve sahip oldukları birim değerlerle volatiliteleri arasında ters korelasyon olduğunu belirlemiştir.

Polat (2018), sosyal medya ile yatırım kararları arasında bir nedensellik ilişkisinin olup olmadığını Bitcoin örneği ile araştırdığı çalışmasında, Twitter üzerinden metin madenciliği ile yapılan yorumları süzerek sentiment analizi ile yorumların olumlu ya da olumsuz olma durumunu incelemiştir. Bu analiz sonucu elde edilen sayısal değerler ile Bitcoin fiyatları arasındaki ilişkinin varlığı Granger Nedensellik analizine tabi tutularak yalnızca Bitcoin' in fiyat artışından Twitter yorumlarına doğru pozitif bir nedensellik ilişkisinin varlığı ortaya konmuştur.

Narayanan, Bonneau vd. (2016) yaptıkları çalışmalarında sanal paraların, oluşturulma süreci, teknolojik alt yapısı, ekonomik, sosyal etkileri ve âdem-i merkeziyetçi yapısıyla devletlerin otoritesini sarsıcı bir yenilik olduğunu belirtmiş ve sanal paraları madencilikten kullanım alanlarına kadar geniş bir yelpazede incelemiştir. Diğer taraftan gelecekte önemli bir ödeme sistemi haline geleceği iddia edilen sanal paraların ve Blokzincir teknolojisinin yalnızca olumsuz taraflarıyla ele alınmasının doğru olmadığı belirtilmiştir.

Franco (2015) Sanal paraların kriptografik, bilişim ve ekonomik olarak tüm yönlerini ortaya koymaya çalıştığı çalışması ile sanal para oluşturma, piyasada aktarım mekanizmaları, Blokzincir teknolojisinin önemi ve ekonomik etkileri hakkında temel bilgiler sunarak sanal para yazınında ilk kaynaklardan birini oluşturmuştur.

Doğan (2018) Kripto para kavramına ve sistemine bilgi teknolojileri ve ekonomik bakış açısı dışında din ve hukuk perspektifinden bakmaya çalıştığı

makalesinde sanal paraların İslam ekonomisinin ve hukukunun temel prensiplerinden olan bilinmezlik (garar) hali ve devlet güvencesi altında bulunmaması durumlarını taşıdığından, hâlihazırdaki görüntüsüyle İslami kurallara uygun olmadığını belirtmektedir. Ancak söz konusu teknolojinin tümüyle reddedilmemesi gerektiğini, İslam hukukuna ve ekonomik anlayışına uygun şekilde devlet tarafından fiyatı herhangi bir varlığa endekslenmiş sanal para oluşturma fikrinin de düşünülmesi gerektiğini ifade etmektedir.

Kızıltaş (2019) çalışmasında anket yöntemini kullanarak, turizm müşterilerinin sanal paralarla ödeme yapmaya niyetli olup olmadıklarını, ödemelere duydukları güven ve turizm şirketlerinin sanal paralarla ilgili algı düzeylerini ölçmeye çalışmıştır. Ayrıca ekonometrik analizler sonucu müşterilerce satın alınması düşünülen turizm ürünlerinden elde edecekleri fayda ile kullanabilecekleri sanal paraların işlevsellikleri arasında anlamlı ve pozitif yönlü bir ilişki bulunduğunu belirtmektedir.

Vlasov (2017) ise çalışmasında elektronik paranın gelişimindeki aşamaları analiz etmekte, paranın değeri, özellikleri ve kökeninin evrimsel teorisi ile Avusturya ekonomi okulu tarafından geliştirilen para ve kredi teorisi görüşünü karşılaştırmakta, sanal para birimlerinin ise para evrimi sürecinde bir sonraki aşama olarak görüldüğü, maddi dünyadaki nesnelerle hiçbir şekilde bağlantısı olmadığı için gerçekten elektronik para olarak kabul edilmeleri gerektiğini belirtmektedir.

Satoshi (2008) makalesinde; tamamen eşten-eşe çalışan bir elektronik para sisteminden bahsetmektedir. Bu sistemle merkezi herhangi bir finansal kurumun kontrolünden geçmeden, eşler arasında (P2P) çevrimiçi ödeme gönderilmesinin mümkün kılınacağını, oluşturulacak dijital imzalar sayesinde mükerrer harcamaların önüne geçilebileceğini ifade etmektedir. Ağda bulunan ve düğüm adı verdiği katılımcılardan, gerçekleştirecekleri işlemleri sürekli uzayan ve özet fonksiyonu tabanlı bir iş-kanıtı zincirine ekleyerek zaman damgasıyla işaretlemeleri gerektiğini, böylece iş-ispatını tekrar üretmeden değiştirilemez bir kayıt oluşturacaklarını anlatmaktadır.

3.2 Ekonometrik Analiz

3.2.1 Çalışmanın Konusu ve Veri Seti

Çalışmanın bu bölümünde ekonometrik uygulamalar yardımıyla 2013 yılında sanal para borsalarında işlem görmeye başlayan ve bu alanda ilk olma özelliğini taşıyan sanal para birimi Bitcoin (BTC) ile seçili bir takım finansal büyüklükler arasında bir eşbütünleşme ve nedensellik ilişkisinin var olup olmadığı araştırılacaktır.

Çalışmanın veri setini, Türkiye Cumhuriyet Merkez Bankası Elektronik Veri Dağıtım Sistemi (EVDS)'den alınan ve 2013 Ocak ayı ile 2019 yılı Ocak ayı arasındaki aylık bazda Dolar (USD), Euro (EUR), İngiliz Poundu (GBP), Cumhuriyet altını (CUMHALT), IMF hesap birimi (SDR)[1], Borsa İstanbul ay sonu kapanış değerleri (BIST 100), TCMB para arzı büyüklükleri olan M1 ve M2'nin Türk Lirası cinsinden değerleri ile nedensellik ilişkisinin araştırılacağı Bitcoin (BTC)'in, bir sanal para borsası olan Coin Market Cap isimli web sitesinden alınan 2013 Ocak ayı ile 2019 Ocak ayı arasındaki her ayın son gününün kapanış değerleri oluşturmaktadır.

Ekonometrik analiz de kullanılan değerlerin seçilmelerinin nedenleri sıralanacak olursa;

- Sanal para birimlerinin ödeme aracı ve hesap birimi olma özelliğinin karşılaştırılması amacıyla; Dolar, Euro, Pound ve SDR,

- Diğer taraftan yatırım aracı olarak ve bir değer saklama aracı olarak kullanılabilirliğinin karşılaştırılması amacıyla sırasıyla BİST 100 ve Cumhuriyet Altını,

[1] "SDR (Özel Çekme Hakları), IMF'nin üye ülkelerin mevcut resmi rezervlerine katkıda bulunmak amacıyla 1969 yılında oluşturduğu uluslararası bir rezerv varlığı olup üye ülkelere IMF kotalarıyla orantılı olarak tahsis edilmektedir. SDR aynı zamanda IMF ve bazı uluslararası kuruluşlar tarafından hesap birimi olarak kullanılmaktadır. SDR'nin değeri, Euro, Japon Yeni, İngiliz Sterlini, Çin Yuanı ve Amerikan Doları para birimlerinden oluşan bir sepet esas alınarak belirlenmektedir" (IMF, 2019).

- Son olarak para politikası aracı olma özelliğinin karşılaştırılması amacına yönelik olarak merkez bankasının M1 ve M2 para büyüklükleri uygulamaya veri olarak seçilmiştir.

Yukarıdaki nedenlerle seçilmiş finansal büyüklüklerle yapılan ilk çalışma olması çalışmamızın özgünlüğünü oluşturmaktadır.

Bitcoin ’in 2013 yılının Ocak ayı itibariyle sanal borsalarda işlem görmeye başlaması nedeniyle Bitcoin ile beraber tüm veri seti bileşenlerinin de 2013 yılı Ocak ayından başlamak üzere 2019 yılının aynı ayına kadar olan aylık Türk Lirası cinsinden değerleri veri kapsamına alınmıştır. Analizde veri bileşenlerinin 6 yıllık zaman dilimi kapsamındaki 73 aylık verileri ile analiz yapılmıştır. Ekonometrik analiz çalışması E-views 11 programı ile gerçekleştirilmiştir.

3.2.2 Çalışmanın Yöntemi

Veri seti bileşenlerinin aralarında eşbütünleşmenin var olup olmadığının belirlenmesinden önce zaman serilerinin durağanlıklarının bilinmesi gerekmektedir. Serilerin aynı dereceden durağan olmaması durumunda aralarında rasyonel olarak aynı zaman diliminde beraber hareket ettiklerine, diğer bir ifadeyle eşbütünleşik olduklarına dair sağlıklı bir yorum yapılamamaktadır. Bu nedenle çalışmamızda ilk olarak serilerin durağan olup olmadıkları Genişletilmiş Dickey-Fuller (ADF) ve Phillips-Peron (PP) birim-kök testleri ile belirlenmeye çalışılacak, zaman serilerinin aynı dereceden durağan oldukları anlaşıldığı takdirde Engel-Granger eşbütünleşme testi ile de uzun dönemde eşbütünleşik olup olmadıkları incelenecektir. Eşbütünleşme testi sonrasında Granger nedensellik testi ile Bitcoin ve diğer finansal değişkenler arasında bir nedensellik ilişkisinin varlığı araştırılacaktır.

3.2.2.1 Durağanlık (Birim-Kök) Testi

Belirli bir zaman aralığında alınan zaman serisi verilerinin süreç içerisinde sürekli bir artış ya da azalış göstermemesi yani yatay zaman çizgisi boyunca dağılması durumu, serilerin durağan olduğu şeklinde tanımlanmaktadır.

Diğer bir ifade ile serilerin sabit ortalama ve sabit varyansa sahip, seriye ait iki değer arasındaki farkın da zamana değil, yalnızca iki zaman değeri arasındaki farka bağlı olması şeklinde de tanımlanabilir (Sandalcılar, 2012). Kısaca serinin durağan olabilmesi için zaman serisinin ortalaması, varyansı ve kovaryansı zaman boyunca sabit kalmalıdır.

Zaman serilerinin durağan olmamaları durumu, serilerin trend içermelerine, çoğunlukla yüksek bir R^2 değerine sahip olsalar da sahte regresyonun ortaya çıkmasına sebep olmaktadır (Dickey & Fuller, 1979). Aşağıdaki Tablo 17' de yer alan varsayımlardan herhangi birinin bulunmaması halinde bir zaman serisinin durağan olmadığı ileri sürülebilir.

Tablo 17
Durağanlık Şartları

Durağanlık Şartı	Değişken	Açıklama
$E(Y_t) = \mu$	Ortalama	Serideki tüm zamanlar için
$Var(Y_t) = E(Y_t-\mu)^2=\sigma^2$	Varyans	Serideki tüm zamanlar için
$Cov(Y_t, Yt_{+k})= \gamma_k$ sabit	Kovaryans	(Serideki tüm zamanlar için ve tüm $k\neq0$ için)

Kaynak: (Yalta, 2011)

Zaman serilerinde birim kök (durağanlık) testi hipotezleri aşağıdaki gibi kurulmaktadır (Gujarati, 1999);

Sabitsiz ve Trendsiz Model $Y_t = Y_{t-1} + U_t$ $U_t(0, \sigma^2)$ hata terimi

Sabitli ve Trendsiz Model $Yt = a + pY_{t-1} + U_t$

Sabitli ve Trendli model $Yt = a + \beta t + pY_{t-1} + U_t$

Sürecinde birim kökün varlığı araştırıldığında hipotez şu şekilde oluşturulmaktadır.

$H_0 : p \geq 1$ (Seri durağan değildir) $H_1 : p<1$ (Seri durağandır)

$p = 1$ ise Y_t 'nin birim kökü bulunmaktadır, rassal yürüyüş serisidir ve durağan değildir (Dickey & Fuller, 1979).

Serinin durağanlığını test eden istatistiğe "t" istatistiği adı verilmektedir. İstatistiğin eşik değerleri Dickey–Fuller tarafından belirlenmiştir. Eğer hesaplanan-t değeri, 0.01, 0.05 ve 0.10 kritik-t değerlerinden daha negatifse H_0 reddedilir ve serinin durağan olduğuna karar verilir (Yücel & Ata, 2003).

Birim-kök testi uygulaması öncesinde analize tabi tutulan değerlerin doğal logaritmaları alınmıştır. Ardından aynı derecede durağan olup olmadıkları düzeylerinde (0) ve 1. derecede farkları (I) alınarak Genişletilmiş Dickey-Fuller (ADF) ve Phillips-Peron testleri ile sınanmıştır. Durağanlık testi sonuçları Tablo 18 ve 19' da yer almaktadır.

Tablo 18
ADF Birim-Kök Testi Sonuçları

Birim-Kök Testi Sonuçları	Augmented Dickey-Fuller Birim-Kök Testi Sonuçları					
	Sabitli		Sabitli ve Trendli		Sabitli	Sabitli ve Trendli
Değişkenler	Düzey Değerleri	Olasılık Değerleri	Düzey Değerleri	Olasılık Değerleri	1.Fark Değerleri	1.Fark Değerleri
LBTC	-2.470	0.127	-2.658	0.256	-8.042*	-8.169*
					(0.0045)	(0.0015)
LBİST-100	-1.447	0.554	-2.515	0.320	-7.823*	-7.779*
					(0.0042)	(0.0043)
LCumhalt.	1.346	0.998	-2.470	0.341	-6.927*	-6.917*
					(0.0016)	(0.0079)
LEuro	0.399	0.981	-1.260	0.889	-7.163*	-7.210*
					(0.0023)	(0.0052)
LM1	-1.210	0.665	-3.873	0.182	-9.294*	-9.252*
					(0.0002)	(0.0004)
LM2	-0.415	0.900	-3.213	0.090	-8.356*	-8.300*
					(0.0019)	(0.0021)
LPound	-0.331	0.914	-1.718	0.732	-6.694*	-6.656*
					(0.0082)	(0.0031)
LSDR	0.306	0.977	-1.778	0.704	-7.079*	-7.103*
					(0.0015)	(0.0008)
LUSD	0.066	0.960	-3.424	0.056	-6.547*	-6.542*
					(0.0014)	(0.0007)

*Katsayıların %1 düzeyinde anlamlı olduklarını, parantez içindeki değerler ise %1 düzeyindeki olasılık değerlerini göstermektedir.

Tablo 19
Phillips Perron Birim-Kök Testi Sonuçları

Birim-Kök Testi Sonuçları	Phillips Perron Birim-Kök Testi Sonuçları					
	Sabitli		Sabitli ve Trendli		Sabitli	Sabitli ve Trendli
Değişkenler	Düzey Değerleri	Olasılık Değerleri	Düzey Değerleri	Olasılık Değerleri	1.Fark Değerleri	1.Fark Değerleri
LBTC	-2.429	0.137	-2.804	0.200	-8.037*	-8.167*
					(0.0013)	(0.0017)
LBİST-100	-1.425	0.565	-2.498	0.328	-7.784*	-7.739*
					(0.0009)	(0.0003)
LCumhalt.	2.305	1.000	-2.415	0.368	-6.798*	-14.290*
					(0.0019)	(0.0021)
LEuro	0.393	0.981	-1.609	0.779	-5.931*	-6.272*
					(0.0001)	(0.0004)
LM1	-1.233	0.655	-3.919	0.706	-9.252*	-9.300*
					(0.0006)	(0.0012)
LM2	-0.362	0.909	-3.327	0.700	-8.972*	-8.856*
					(0.0011)	(0.0031)
LPound	-0.329	0.914	-1.967	0.608	-5.584*	-5.522*
					(0.0027)	(0.0005)
LSDR	0.273	0.975	-2.157	0.505	-5.822*	-6.014*
					(0.0008)	(0.0016)
LUSD	-0.098	0.945	-2.542	0.307	-5.337*	-5.291*
					(0.0028)	(0.0007)

*Katsayıların %1 düzeyinde anlamlı olduklarını, parantez içindeki değerler ise %1 düzeyindeki olasılık değerlerini göstermektedir.

Tablo 18 ve 19'da görüldüğü gibi BTC ve diğer finansal değişkenler için yapılan ADF ve PP birim-kök testlerine göre, değişkenlerin düzeyde durağan olmadıkları ancak birinci derece farkları I(1) alındığında durağan hale geldikleri, diğer bir ifadeyle H_0 hipotezinin reddedilerek H_1 hipotezinin kabul edildiği belirlenmiştir. Birim-kök testlerinden elde edilen sonuçlar, veri seti bileşenleri arasında eşbütünleşme ilişkisinin araştırılmasında ekonometrik açıdan herhangi bir sakınca olmadığını göstermektedir.

3.2.2.3 Engle-Granger Eşbütünleşme Testi

Zaman serilerinin eşbütünleşik olup olmadıkları Engle-Granger (1987) tarafından geliştirilen yöntemle incelenmiştir. Bu testte serilerin birlikte dâhil edildiği denklemde ortaya çıkan kalıntıların düzey değerinde durağan olması durumuna bakılmaktadır. Denklemde serilere ait kalıntıların düzey değerleri ADF birim kök testine tabi tutularak düzey değerlerinin I(0) kritik değerlerden büyük olduğu Tablo 20'de görülmüş olup, bu durumda H_0 hipotezi reddedilerek seriler arasında eşbütünleşme olduğuna karar verilmiştir.

Tablo 20
Engle-Granger Eşbütünleşme Testi Sonuçları

İncelenen Model	ADF Test İstatistiği	ADF Kritik Değerler			Karar
		%1	%5	%10	
BTC-BİST-100	-8.168	-4.092	-3.474	-3.164	H_O Red
BTC-CUMHALT	-8.102	-2.597	-1.945	-1.613	H_O Red
BTC-EURO	-8.230	-3.525	-2.902	-2.588	H_O Red
BTC-M1	-8.332	-2.597	-1.756	-1.515	H_O Red
BTC-M2	-8.586	-2.247	-2.586	-1.856	H_O Red
BTC-POUND	-8.178	-3.478	-1.754	-1.618	H_O Red
BTC-SDR	-8.231	-3.474	-2.578	-3.154	H_O Red
BTC-USD	-8.181	-3.425	-2.900	-2.545	H_O Red

Engle-Granger eşbütünleşme testi ile seriler arasında eşbütünleşme vektörünün varlığı tespit edildiğinden hata düzeltme modeli (ECM)'nin tahmin edilmesine geçilmiştir. ECM değişkenler arasında uzun dönemli bir ilişkinin varlığının tespiti durumunda uygulanmaktadır. Bu modelle uzun dönemdeki ilişkide gerçekleşen sapmalar belirlenmektedir (Doğan & Can, 2016).

Eşbütünleşme testinin uygulanabilmesi için gerekli ön şart serilerin durağan olmasıdır. Çalışmada kullanılan zaman serileri düzeylerinde durağan olmayıp, birinci farkları alındığında yani (I)'de durağan olduklarından farkları alınan serilerin uzun dönem bilgilerinde kayıplar oluşmaktadır. Bu nedenle hata düzeltme terimleri kullanılarak bu kayıplardan kaynaklanan dengesizlikler ortadan kaldırılmaya çalışılmaktadır (İçellioğlu & Öztürk, 2018).

Hata düzeltme modeli (ECM)'nde aralarında uzun dönemde eşbütünleşmenin olduğu serilerde meydana gelecek bir sapmanın zamanla giderilip giderilmediğinin ortaya konması amaçlanmaktadır. Buradan hareketle

serilerin dengeden uzaklaştıktan sonra ortalamaya nasıl ve hangi sürede yaklaştıkları araştırılmaktadır (Tarı, 2012).

Hata düzeltme modellerinde durağan değişkenlerle kurulan tahmin modellerinde hata terimlerinin bir gecikmeli hali alınarak modele dâhil edilmektedir. Diğer taraftan hata terimlerinin dâhil edildiği modelde, modelin anlamlı olabilmesi için değişkenlerin olasılık değerlerinin %1, %5 ve %10 anlamlılık değerlerinde ve hata terimlerinin katsayılarının ise 0 ile -1 arasında olması gerekmektedir. Bunun yanında R^2 değerinin yüksek, F istatistik değerininde düşük olması gerekmektedir. ECM sonuçları Tablo 21'de yer almaktadır.

Tablo 21
Hata Düzeltme Modeli (ECM) Sonuçları

Bağımlı Değişken	Bağımsız Değişken	Katsayı	t istatistik değeri	Olasılık Değeri	R^2 Değeri	F istatistik değeri	Hata Teriminin Katsayısı
dBTC	dBIST_100	-0.0011	0.554	0.956	0.0001	0.9947	0.006
dBTC	dCumhalt.	0.1712	0.165	0.869	0.0908	0.0374	-0.143
dBTC	dEuro	2.9215	3.435	0.001	0.8570	0.0208	-0.165
dBTC	dM1	1.4563	1.194	0.236	0.1114	0.0169	-0.152
dBTC	dM2	3.2376	1.595	0.115	0.1118	0.0167	-0.146
dBTC	dPound	1.5715	1.492	0.140	0.0996	0.0267	-0.146
dBTC	dSDR	1.1496	1.041	0.301	0.1004	0.0259	-0.148
dBTC	dUSD	1.0922	1.038	0.302	0.1110	0.0172	-0.149

Tablo 21'de yer alan sonuçlar yukarıda yer verilen kısıtlar çerçevesinde incelendiğinde; hata düzeltme modelinin uygulandığı değişkenler arasındaki uzun dönemli ilişki denklemlerinde, yalnızca BTC ile Euro arasında uzun dönemli ilişkideki bozulmanın hata teriminin katsayısına bakılarak (-0.16) gelecek dönemde %16'sının düzeldiği sonucu anlamlı olarak tespit edilebilmektedir. Ancak BTC ile diğer değişkenler arasındaki uzun dönemli ilişkideki dengenin hangi sürede düzelebileceğine dair anlamlı bir yorum yapabilmek için Tablo 20 de yer alan bilgiler ışığında anlamlı ve yeterli bir sonuç elde edilememiştir.

3.2.2.3 Granger Nedensellik Testi

Ekonomik olguların gerçekleşmesi sürecinde bir değişkenin zaman içerisinde başka bir ekonomik değişkene bağımlılığı söz konusu olabilmektedir.

Ancak iki değişken arasında tespit edilen bağımlılık, bu değişkenler arasında mutlaka bir sebep-sonuç ilişkisinin var olduğu anlamına gelmemektedir (Granger, 1969). Ayrıca nedensellik testi ile geleceğin tahmini değil nedenselliğin varlığı test edilmektedir.

İki ekonomik değer olan X ve Y arasında zamana bağlı bir gecikmeli ilişkinin varlığı ve kısa dönemli nedenselliğin yönünün (sebep ve sonuç ilişkisinin) istatistikî olarak belirlenmesi amacıyla gerçekleştirilen ilk çalışma C.W.J Granger tarafından yapılmıştır. Granger nedensellik testinin dayandığı temel argüman, zaman serisi verileridir.

Analiz çalışmasının bu bölümünde veri setindeki değişkenler arasında herhangi bir nedenselliğin olup olmadığına, var olması halinde nedenselliğin hangi değişkenler arasında olduğuna ve yönüne (hangi değişkenin bir diğerine istatistiksel olarak neden olduğuna) karar verebilmek için uygun aralık ve gecikme uzunlukları VAR modeli yardımıyla kurularak Granger nedensellik testi uygulanmıştır. VAR modeli aşağıdaki gibi tanımlanabilir (Granger, 1969).

$$X_t = c_x + \sum_{j=1}^{n} \alpha_{x,j} X_{t-j} + \sum_{j=1}^{n} \beta_{x,j} Y_{t-j} + \varepsilon_{x,t}$$

$$Y_t = c_y + \sum_{j=1}^{n} \alpha_{y,j} X_{t-j} + \sum_{j=1}^{n} \beta_{y,j} Y_{t-j} + \varepsilon_{y,t}$$

Nedensellik analizinin yapılabilmesi amacıyla gecikme uzunluklarının değerleri Akaike ve Schwarz Bilgi Kriterleri yardımıyla elde edilmiş ve en uygun gecikme uzunluğu belirlenmiştir. Tablo 22'de Granger nedensellik testi sonuçlarına yer verilmiştir.

Tablo 22
Granger Nedensellik Testi Sonuçları

Değişkenler		Granger Nedensellik Test Sonuçları		
Bağımlı Değişken	Bağımsız Değişken	Chi-sq	Gecikme	Olasılık
BTC	BIST100	8.265278(*)	4	0.0823
	CUMHALT.	6.289526	4	0.1785
	EURO	7.234516	4	0.1240
	M1	2.022674	4	0.7316
	M2	2.469183	4	0.6502
	POUND	7.977205(*)	4	0.0924
	SDR	9.642332(**)	4	0.0469
	USD	10.81564(**)	4	0.0287
BIST100	BTC	3.576864	4	0.4663
CUMHALT.		1.035045	4	0.9044
EURO		2.058039	4	0.7251
M1		5.661523	4	0.2259
M2		3.552600	4	0.4699
POUND		2.784965	4	0.5944
SDR		1.389212	4	0.8461
USD		1.587325	4	0.8111

Ki Kare test istatistik değerlerinin yanında yer alan ***, ** ve * ifadeleri, sırasıyla % 1, 5 ve 10 istatistiki önem seviyesinde anlamlılıkları temsil etmektedir.

Tablo 22 ‘de ki sonuçlara göre BTC ‘nin bağımlı değişken olduğu denklemde SDR ve USD ‘den BTC’ye doğru %5 anlamlılık düzeyinde, Euro ve BIST 100 değişkeninden BTC’ye doğru ise %10 anlamlılık seviyesinde bir nedenselliğin olduğu tespit edilmiştir. BTC ‘nin bağımsız olduğu denklemde ise finansal değişkenlerle BTC arasında herhangi bir kısa dönemli nedensellik ilişkisinin bulunmadığı görülmektedir.

SONUÇ VE ÖNERİLER

Çalışmada ampirik olarak; veri setini oluşturan finansal değişkenler (USD, EURO, Pound, SDR, Cumhuriyet Altını, BIST 100 endeksi ve M1/M2 para arzı büyüklükleri) ile sanal para birimi örneği Bitcoin arasındaki nedensellik ve eşbütünleşme testinden önce ADF ve Phillips-Peron Birim Kök testleri uygulanarak serilerin durağanlıkları incelenmiştir. Birim kök testleri sonuçlarına göre zaman serilerinin birinci farklarında durağan oldukları belirlenmiştir. Daha sonra finansal verilerle Bitcoin arasında uzun dönemli bir ilişkinin varlığının tespiti için Engle-Granger eşbütünleşme analizi yapılmıştır. Bu analizlerin sonuçları incelendiğinde BTC ile diğer değişkenler arasında uzun dönemli bir ilişkinin var olduğu görülmüştür.

Zaman serileri üzerinde değişkenler arasında bir nedensellik ilişkisinin var olup olmadığı da Granger Nedensellik testi ile sınanmıştır. Test sonuçlarına göre BTC'nin bağımlı değişken olduğu denklemde SDR ve USD'den BTC'ye doğru %5 anlamlılık düzeyinde, Euro ve BIST 100 değişkeninden BTC'ye doğru ise %10 anlamlılık seviyesinde bir nedenselliğin olduğu, BTC 'nin bağımsız olduğu denklemde ise finansal değişkenlerle BTC arasında herhangi bir kısa dönemli nedensellik ilişkisinin bulunmadığı görülmüştür.

Bu durumun ortaya çıkmasındaki nedenler irdelendiğinde sanal para birimi Bitcoin' in hacimsel, bilinirlilik ve güvenirlilik bağlamlarında Fiyat para örnekleri USD, EURO ve POUND'u anlamlı düzeyde etkileyebilecek düzeyde olmadığı, değer saklama aracı olarak da Cumhuriyet Altını ve hisse senedi değerleri ölçüsünde bulunmadığı ve para arzı büyüklükleri ile karşılaştırılabilecek bir para politikası aracı olmadığı sıralanabilir. Nitekim söz konusu görüş ve sonuçlar literatürdeki İçellioğlu & Öztürk (2017), Laçin (2019) ve Atik (2015) tarafından yapılan çalışmalarla benzerlik göstermektedir.

Sanal para birimleri, parasal özelliklerinin yanında hayata kattığı teknolojik yenilikleri ile de incelenmeye ve üzerinde durulmaya değer niteliklere sahiplerdir. Ancak sanal para birimlerine getirilen eleştirileri de ayrıştırmak

gerekmektedir. Finansal bir araç olma özelliği ile gereken güveni kazanamamış olsa da blokzincir teknolojisi ile farklı alanlarda karşımıza çıkması muhtemel bir gelişmenin anlaşılması, uygulanması ve uluslararası camia da fark yaratabilecek atılımların gerçekleştirilmesi için, oldukça yeni sayılabilecek söz konusu bu teknolojiyi şimdiden karamsar eleştirilerin odağı haline getirmek gerçekçi bir yaklaşım olmayacaktır.

Bitcoin özelinde tüm sanal para birimlerinin binlerce yıldır süregelen paranın genel geçer özelliklerini tam anlamıyla karşılamıyor olmalarında garipsenecek bir tarafın bulunmadığı anlaşılmalıdır. Çünkü Bitcoin'i ve diğer sanal para birimlerinin ortaya çıkaran ana neden, paranın bu özelliklerinin artık insanların değişen beklentilerine cevap veremiyor olmasıdır. Merkezi olmayan, daha güvenli, şeffaf, hızlı ve ucuz bir para aktarım mekanizması vadeden bu sistemle parasal işlemlerin daha kolay ve güvenli bir şekilde yapılıyor olması her geçen gün sanal paralarla yapılan işlem sayısını artırmaktadır.

Diğer taraftan sanal para teknolojisinin paranın işlevlerini yerine getirebilmesi ve kendisine duyulan güvenin artması adına kamu otoriteleri tarafından güçlü bir desteğin varlığı beklenmese de illegal bir sistem görünümüne büründürülmemesi, yapısal ve hukuki düzenlemelerin en kısa zamanda hayata geçirilmesinin gerektiği açıktır. Öyle ki ülkemiz de sanal para birimleri ile ilgili yalnızca 2013 yılındaki BDDK tarafından yapılan bildiri dışında yasal bir düzenleme ya da kuralların var olmaması hem hukuksal bir boşluğun oluşmasına hem de bu yeni teknolojinin kullanılmasındaki küresel yarışta geri kalınmasına neden olabilecektir. Diğer taraftan gerçekleştirilecek düzenlemelerle bankacılık ve finansal kurumların sistem dışına itilmesi engellenebilecek, aynı zamanda devlet, finansal varlıklar üzerinden elde ettiği vergi gelirlerinden mahrum kalmamış olacaktır.

Sanal para birimleri, oluşturuldukları Blokzincir tabanlı teknolojiyle bankacılık, lojistik, eğitim, sağlık, tapu ve noterlik alanları başta olmak üzere birçok alanda önemli etkileri de beraberinde getirmektedirler. Bu etkiler işlemlerin daha hızlı, güvenli ve daha az maliyetle yapılmasını sağladıkları gibi istihdam, enerji kullanımı ve çevreye verdikleri zararlarla da olumsuz yönde etkide bulunabilirler. Bahsi geçen sektörlerde blokzincir teknolojisinin

kullanımının artırılması ve yapılacak inovasyon çalışmalarıyla söz konusu alanlarda sahip olunan konum ve gelirlerin korunmasını sağlayabilir aksi takdirde sosyal yaşamdaki önemlerini ve işleyişlerini kaybetme noktasına gelebilirler. Türkiye de TÜBİTAK bünyesinde kurulan blokzincir araştırma laboratuvarı ve konu ile ilgili gerçekleştirilen çalıştaylar gelecek açısından umut vadeden gelişmeler olarak sıralanabilir.

İlerdeki dönemlerde konu ile ilgili yapılacak ekonometrik çalışmalarda zaman serilerinin uzunluğunun artması, sanal paraların bilinirliğinin, kullanımlarının ve hukuksal düzenlemelerinin gerçekleştirilmiş olması ile veri setine eklenebilecek yeni finansal değişkenlerle elde edilecek sonuçların farklılık gösterebileceği düşünülmektedir.

KAYNAKÇA

Akdiş, M. (2001). *Para Teorisi ve Politikası.* İstanbul: Beta Yayınları.

Akleylek, S., Yıldırım, H. M., & Tok, Z. Y. (2011). Kriptoloji ve Uygulama Alanları; Açık Anahtar Altyapısı ve Kayıtlı Elektronik Postalar. *Popüler Bilim Dergisi*(168), 1-27.

Aktan, C. C. (2010). Monetarizm ve Rasyonel Beklentiler Teorisi. *Ekonomi Bilimleri Dergisi, 2*(1), 168-187.

Aktan, C. C., Utkulu, U., & Togay, S. (1998). *Nasıl Bir Para Sistemi.* İstanbul: İMKB Yayınları.

Ali, R., Barrdear, J., & Southgate, J. (2014). The Economics Of Digital Currencies. *Bank of England Quarterly Bulletin, 54*(3), 276-286.

Aren, S. (1992). *İstihdam, Para ve İktisadi Politika.* Ankara: Savaş Yayınları.

Aren, S. (2007). *100 Soruda Para ve Para Politikası.* Ankara: İmge Kitapevi.

Aslan, H. (2009). *Para Teorisi ve Politikası.* Bursa: Alfa Aktüel Yayıncılık.

Babaoğlu, A. (2018). Kriptolojinin Geçmişi. *Bilim ve Teknik Dergisi*(500. sayı), 20-68.

Balcısoy, E. (2017). *Yüksek Performanslı Bitcoin Madenciliği İçin SHA 256 Özet Algoritmasının En İyilenmesi (Yüksek Lisans Tezi) https://tez.yok.gov.tr/UlusalTez Merkezi adresinden edinilmiştir.* Ankara.

Ball, L. (2012). *Money, Banking And Financial Markets.* London: Worth Publisher.

Bayar, E. (2012). Modern Kriptosistemlerle Şifrelemenin Modellenmesi ile Veri Güvenliğinin Sağlanması (Yüksek Lisans tezi). https://tez.yok.gov.tr/UlusalTezMerkezi adresinden edinilmiştir. .

BDDK. (2013). *BDDK Basın Açıklaması.* Ankara: BDDK.

Berentsen, A., & Schär, F. (2018). *A Short Introduction to the World of Cryptocurrencies.* Washington: Federal Reserve Bank Publishing.

Bocutoğlu, E., & Ekinci, A. (2009). Genel Teori, Küresel Krizler ve Yeniden Maliye Politikası. *Maliye Dergisi*(156), 58-80.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives, 29*(2), 2013-238.

Bustillos, M. (2013, 4 1). *New Yorker Ekonomi Bülteni.* The Bitcoin Boom: https://www.newyorker.com/tech/annals-of-technology/the-bitcoin-boom adresinden alındı

Cechetti, G., & Scohenholtz, K. (2011). *Money, Finance And Financial Markets.* California: McGraw&Hill Irvin Publishing.

Cesur, F. (2014). *Paraya Dair.* İstanbul: Paradigma Akademi Yayınları.

Coinmarketcap Cryptocurrency Market. (2019, 08 26). www.coinmarketcap.com adresinden alındı

Cormen, T., & Leiserson, J. (2009). *Introduction to Algorithms.* Boston: MIT Publishing.

Çeşmeci, Ü. (2009). Kriptoloji Tarihi. *Uluslar arası Kriptoloji Araştırma Enstitüsü, 1*(1), 12-54.

Dadda, L., & Machetti, M. (2004). *The Design of a High Speed ASIC Unit for the Hash Function SHA-256.* Paris: Design, Automation and Test in Europe Conference and Exhibition.

Dai, W. (1998). *B-Money*. http://www.weidai.com/bmoney.txt adresinden alındı

Dickey, D., & Fuller, W. (1979). Distribution Of The Estimators For Autoregressive Time Series With A Unit Root. *Journal Of American Statistical Association, 74*(366), 427-461.

Doğan, B., & Can, M. (2016). Küreselleşmenin Büyümeye Etkisi: Güney Kore Örnekleminde Eşbütünleşme Analizi. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 6*(2), 197-220.

Dooley, J. (2013). *A Brief History Of Cryptology And Cryptographic Algorithms.* İllinois: Springer Publishing.

Dourado, E., & Brito, J. (2014). Cyrptocurrency. *The New Palgrave Dictionary Of Economics*, 12-23.

Draghi, M. (2016). *The ECB Annual Report For 2016.* Strazburg: European Union Press.

ECB. (2018). *The Prevention of The Use of The Financial System for The Purposes of Money Laundering or Terrorist Financing and Amending Directive.* Strasbourg: European Union Parliament.

Erdem, E. (2016). *Para Banka ve Finansal Sistem.* Ankara: Detay Yayıncılık.

Ergin, F. (1983). *Para ve Faiz Teorileri.* İstanbul: Beta Yayınları.

Farell, R. (2015). An Analysis of the Cryptocurrency Industry. *Penn Libraries, University Of Pensylvania, 4*(5), 1-23. 08 20, 2019 tarihinde http://repository.upenn.edu/wharton_research_scholars/130 adresinden alındı

Filipova, N. (2015). Blokchain – An Opportunity For Developing New Bussiness Models. *Tsenov Academy of Economics* , 75-92.

Folkerts, D., & Garber, P. (2004). The Revived Bretton Woods System. *İnternational Journal Of Finance And Economics, 9*(4), 1-82.

Franco, P. (2015). *Understanding Bitcoin; Cryptography, Engineering and Economics.* Cornwall, UK: Wiley Publishing.

Gayva, Y. (2018). *Cryptocurrency Transactions Will Be Taxed in Russia.* Moskow: https://rg.ru.

Granger, C. (1969). Investigating Causal Relations By Economic Models And Cross Spectral Models. *Econometrica*(37), 424-438.

Grembowski, T., & Lien , R. (2002). *Comparative analysis of the hardware implementations of hash functions SHA-1 and SHA-512.* Sao Paolo: International Conference on Information Security Press.

Gujarati, D. N. (1999). *Econometric Models, Techniques and Applications.* London: Prentice Hall Publishing.

Gültekin, Y. (2017). *Kripto Para Birimleri Ve Yatırım Arcı Olarak Kullanımları: Tarihsel Volatilitileri Bağlamında Bir Değerlendirme (Yüksek Lisans Tezi) https://tez.yok.gov.tr/UlusalTez Merkezi adresinden edinilmiştir.* Samsun.

Günal , M. (2001). *Merkez Bankasının Değişen Rolü ve Para Politikası Uygulamaları.* İstanbul: İMKB Yayınları.

Güven, V., & Şahinöz, E. (2018). *Blokzincir, Kripto Paralar ve Bitcoin.* İstanbul: Kronik Kitap Yayınları.

Handa, J. (2000). *Monetary Economics.* London: Routledge Publishing.

Hiç, M. (1975). *Para Teorisi.* İstanbul: İstanbul Üniversitesi.

Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain.* Antwerp: Policy Department for Economic, Scientific and Quality of Life Policies European Parliament.

Hubbard, G. (2002). *Money, The Financial System And Economy.* Boston: Addison Wesley Publishing.

Iansiti, M., & Lakhani, K. (2017). The Truth About Blockchain. *Harvard Business Reveiw, 95*(1), 118-127.

İçellioğlu, Ş. C., & Öztürk, M. E. (2018). Bitcoin ile Seçili Döviz Kurları Arasındaki İlişkinin Araştırılması: 2013-2017 Dönemi için Johansen Testi ve Granger Nedensellik Testi. *Maliye ve Finans Yazıları,* 51-70.

IMF. (2019). İnternational Monetary Found: 10.08.2019 tarihinde www.imf.org/Data/Reports adresinden alındı

IMF. (2019). *Özel Çekme Hakları (SDR).* Washington: Uluslararası Para Fonu Dış İlişkiler Bölümü. https://www.imf.org/external/np/exr/facts/tur/sdrt.pdf adresinden alındı

İncekara, A., & Akalın, G. (2012). *Keynes'in Genel Teorisi Üzerine.* İstanbul: Kalkedon Yayınları.

İnci, S., & Alpen, İ. (2018). *Bitcoin Devrimi, Değişen Dünya Ekonomisinde Kripto Para Sistemi, Blokzincir ve Altcoinler.* Ankara: Elma Yayınevi.

Jefrey, F., & Lake, D. (2003). *British And American Hegemony Compared.* London: Taylor&Francis e-Library Publishing.

Johansen, S. (1988). Statistical Analysis Of Cointegration Vectors. *Journal Of Economic Dynamics And Control, 12*(3), 231-254.

Karan, M. B. (2011). *Yatırım Analizi ve Portföy Yönetimi.* Ankara: Gazi Kitapevi.

Koblitz, N. (2006). *A Course İn Number Theory And Cyrptography.* New York: Springer Verley Publishing.

Laidler, D. (1983). *Para Talebi Kuramlar ve Kanıtlar (Çev: Haluk Gürsel).* İstanbul: Türkiye İş Bankası Yayınları.

Loc. (2017). Regulation of Cryptocurrency Around the World: 25.08.2019 tarihinde http://www.loc.gov/law/help/cryptocurrency/world-survey.php#compsum adresinden alınmıştır. adresinden alındı

Lois, K. (1989). *Cyptology; Machines, History & Methods.* London: Artech House Publishing.

Mankiw, G. (2017). *Essantial Of Economics.* New York: Cengage Publishing.

Mishkin, F. (2015). *Money, Banking And Financial Markets.* London: Pearson Education Publishing.

Moldovyan, N. (2006). *İnnovative Cyrptography.* Boston: Course Technology Publishing.

Mucuk, M. (2008). *Bütçe ve Cari işlemler Dengesi Arasındaki İlişki: Türkiye Örneği (1989-2004).* Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü. https://tez.yok.gov.tr/UlusalTezMerkezi adresinden alındı

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* www.bitcoin.org adresinden alındı

Nakamura , K., & Matsutani, H. (2017). *An Based Hardware Caching for Blockchain.* Bochum: FPGA Publishing.

Narayanan, A., Bonneau, J., Felten, E., & Miller, A. (2016). *Bitcoin and Cryptocurrency Technologies.* Princeton: Princeton University Press.

Natarajan, H., Krause, S., & Gradstein, H. (2017). *Distributed Ledger Technology (DLT) and Blockchain.* Washington: International Bank for Reconstruction and Development .

Oppliger, R. (2005). *Contemporary Cyrptology.* Norwood: Artech House Publishing.

Öçal, T. (1990). *Para Teorisi.* Ankara: Gazi Üniversitesi İİBF Yayınları.

Özbilen , Ş. (2016). *Maliye Politikası.* Bursa: Ezgi Kitapevi.

Öztürk, N. (2011). *Para Banka Kredi.* Bursa: Ekim Yayınevi.

Parasız, İ. (2011). *Merkez Bankacılığı ve Para Politikası.* Bursa: Ezgi Kitapevi.

Parker, L. (2017). *Brave New Coin.* 19.08.2019 tarihinde https://bravenewcoin.com/insights/bitcoin-spam-attack-stressed-network adresinden alınmıştır. adresinden alındı

Paya, M. (2007). *Para Teorisi ve Politikası.* İstanbul: Filiz Kitapevi.

Petukhova, L. (2018). *Passion for Bitcoin: How Cryptocurrencies and ICO Will Be Regulated in Russia.* Moskow: 20.08.2019 tarihinde https://www.rbc.ru adresinden alınmıştır.

Ray, S. (2018). *Goverment Plans to Bring in Law to Regulate Cryptocurrency Trade.* Delhi: https://www.hindustantimes.com.

Reserve Bank of India. (2017). 22.08.2019 tarihinde https://www.rbi.org.in adresinden alınmıştır. adresinden alındı

Ritter, L., & Silber, W. (2019). *Principles Of Money, Banking & Financial Markets.* London: Pearson Publishing.

Ryabko, B., & Fionov, A. (2005). *Basics Of Contemporary For IT Practitioners.* New Jersey: World Scientific Publishing.

Sackheim , M., & Howell, N. (2018). *The Virtual Currency Regulation Review.* London: Law Business Research Press.

Sandalcılar, A. R. (2012). Türkiye'de Kağıt Tüketimi ile Ekonomik Büyüme Arasındakiİlişki: Eşbütünleşme ve Nedensellik Analizi. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi, 13*(1-15).

Sarıtaş, H. (2015). Dijital İmza Uygulamasının Eliptik Şifrelem Yöntemi Kullanılarak Gerçekleştirilmesi (Yüksek Lisans Tezi) Marmara Üniversitesi Fen Bilimleri Enstitüsü https://tez.yok.gov.tr/UlusalTezMerkezi adresinden edinilmiştir.

Schneier, B. (1996). *Applied Cyrptography* . New York: John Wiley & Sons Inc. Publishing.

Schroeder, J. (2016). *Bitcoin And Commercial Code.* Miami: Miami Business Review Press.

Sekmen, F. (2012). *Para Teorisi, Kavram-Kuram ve Modeller.* Ankara: Seçkin Yayınevi.

Seyidoğlu, H. (2017). *Uluslararası İktisat.* İstanbul: Güzem Can Yayınları.

Smith, A. (2006). *Ulusların Zenginliği.* İstanbul: Palme Yayınları.

Stalling, W. (1998). *Cyrptograpy And Network Security: Principles And Practice.* New York: Printice Hall Publishing.

Swan, M., & De Filippi, P. (2017). Toward A Philosophy Of Blockchain. *Metaphilosophy Dergisi, 48*(3), 603-619.

Şıklar, İ. (2004). *Para Teorisi ve Politikası.* Eskişehir: Anadolu Üniversitesi Yayınları.

Takan, M. (2001). *Bankacılık.* Ankara: Nobel Yayınları.

Tapscott, D. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World.* Massachusetts: Portfolio & Penguin Publishing.

Tarı, R. (2012). *Ekonometri.* Kocaeli: Umuttepe Yayınları.

TCMB. (2018). www.tcmb.org.tr (E.T:22.08.2019) adresinden alındı

TCMB. (2018). *100 Soruda Merkez Bankacılığı.* Ankara: Türkiye Cumhuriyet Merkez Bankası Yayınları.

TÜBİTAK.(2019). TÜBİTAK Web Sitesi: https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html adresinden alındı

Üzer, B. (2017). *Sanal Para Birimleri (Uzmanlık Yeterlik Tezi).* Ankara: Türkiye Cumhuriyet Merkez Bankası Yayınları.

Varian, H. (2013). Business Standard: 22.08.2019 tarihinde https://www.business-standard.com/article/finance/not-particularly-optimistic-about-bitcoin-s-future-hal-varian-113121601025_1.html adresinden alınmıştır. adresinden alındı

Vishwanathan, V. (2018). *Bitcoin Regulations in India.* Delhi: 23.08.2019 tarihinde http://www.livemint.com adresinden alınmıştır.

Vlasov, A. (2017). The Evolution of E-Money. *European Research Studies, 20*(1), 215-224.

Xiaochuan, Z. (2018). *Future Regulation on Virtual Currency Will Be Dynamic, Imprudent Products Shall Be Stopped for Now.* Pekin: 24.08.2019 tarihinde https://perma.cc adresinden alınmıştır.

Yalta, Y. (2011). *Para Teorisi ve Politikası Ders Notları.* İstanbul, Türkiye: Türkiye Bilimler Akademisi Yayınları.

Yerlikaya, T., & Buluş, E. (2006). *Kripto Algoritmalarının Gelişimi ve Önemi.* Denizli: TMMOB Yayınları.

Yujian, W. (2017). *Bitcoin Exchanges Ordered to Formulate Non-Risk Clearance Plan and Shut Down by End of September.* Pekin, China: 24.08.2019 tarihinde http://finance.caixin.com adresinden alınmıştır.

Yücel, F., & Ata, Y. (2003). Eş-Bütünleşme ve Nedensellik Testleri Altında İkiz Açıklar Hipotezi: Türkiye Uygulaması. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Dergisi, 12*(2), 1-13.

Zamakhina, T. (2018). *Money in the Web, A Bill on Digital Economy.* Moskow: 10.08.2019 tarihinde https://rg.ru. adresinden alınmıştır.

Zyskind , G., Nathan, O., & Pentland, A. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data.* Boston: IEEE CS Security and Privacy Workshops.

EKLER

Ek-1: USD, EUR. POUND, SDR, BIST 100, Cumhuriyet Altını Verileri

Tarih	USD	EUR	POUND	SDR	BIST 100	CUMH. ALTINI
2013-01	1,76	2,34	2,82	2,72	78783	641
2013-02	1,77	2,37	2,74	2,71	79334	628
2013-03	1,81	2,34	2,72	2,72	85899	625
2013-04	1,80	2,34	2,74	2,70	86046	592
2013-05	1,82	2,37	2,78	2,73	85990	574
2013-06	1,89	2,50	2,93	2,87	76295	552
2013-07	1,93	2,52	2,93	2,90	73377	556
2013-08	1,95	2,60	3,02	2,97	66394	585
2013-09	2,02	2,69	3,19	3,07	74487	585
2013-10	1,99	2,71	3,20	3,07	77620	570
2013-11	2,02	2,73	3,25	3,10	75748	566
2013-12	2,06	2,82	3,36	3,17	67802	557
2014-01	2,22	3,02	3,65	3,41	61858	595
2014-02	2,21	3,02	3,65	3,41	62553	611
2014-03	2,22	3,07	3,68	3,44	69736	631
2014-04	2,13	2,94	3,55	3,30	73872	599
2014-05	2,09	2,87	3,52	3,24	79290	582
2014-06	2,12	2,88	3,57	3,26	78489	588
2014-07	2,12	2,88	3,62	3,27	82157	594
2014-08	2,16	2,88	3,60	3,30	80313	600
2014-09	2,20	2,85	3,59	3,31	74938	587
2014-10	2,26	2,86	3,63	3,36	80580	588
2014-11	2,23	2,79	3,52	3,28	86169	574

Ek-1: (Devam) USD, EUR. POUND, SDR, BIST 100, Cumhuriyet Altını Verileri

2014-12	2,29	2,82	3,57	3,34	85721	590
2015-01	2,33	2,72	3,53	3,32	88946	622
2015-02	2,46	2,79	3,75	3,47	84148	644
2015-03	2,58	2,80	3,87	3,59	80846	654
2015-04	2,65	2,85	3,94	3,66	83947	678
2015-05	2,65	2,96	4,09	3,72	82981	673
2015-06	2,70	3,03	4,19	3,80	82250	677
2015-07	2,69	2,97	4,19	3,77	79910	657
2015-08	2,85	3,17	4,43	3,99	75210	687
2015-09	3,00	3,37	4,61	4,23	74205	719
2015-10	2,93	3,30	4,48	4,13	79409	719
2015-11	2,87	3,09	4,36	3,97	75233	668
2015-12	2,92	3,17	4,37	4,05	71727	677
2016-01	3,01	3,27	4,33	4,16	73481	704
2016-02	2,94	3,26	4,21	4,10	75814	755
2016-03	2,89	3,21	4,10	4,03	83268	767
2016-04	2,83	3,21	4,05	4,00	85328	752
2016-05	2,93	3,31	4,24	4,14	77803	791
2016-06	2,92	3,28	4,15	4,11	76817	794
2016-07	2,96	3,27	3,89	4,11	75406	836
2016-08	2,96	3,32	3,88	4,15	75968	847
2016-09	2,96	3,32	3,88	4,14	76488	842
2016-10	3,07	3,39	3,79	4,24	78536	842
2016-11	3,27	3,53	4,05	4,47	73995	877
2016-12	3,49	3,68	4,35	4,71	78139	875
2017-01	3,73	3,97	4,59	5,05	86296	957
2017-02	3,67	3,91	4,58	4,98	87478	975

Ek-1: (Devam) USD, EUR. POUND, SDR, BIST 100, Cumhuriyet Altını Verileri

2017-03	3,67	3,92	4,51	4,97	88947	975
2017-04	3,65	3,91	4,60	4,98	94655	998
2017-05	3,56	3,93	4,60	4,90	97542	962
2017-06	3,52	3,95	4,49	4,87	100440	959
2017-07	3,56	4,09	4,61	4,97	107531	953
2017-08	3,51	4,14	4,55	4,96	110010	969
2017-09	3,47	4,14	4,61	4,93	102908	980
2017-10	3,66	4,31	4,83	5,17	110143	1008
2017-11	3,88	4,55	5,12	5,47	103984	1067
2017-12	3,85	4,55	5,15	5,45	115333	1092
2018-01	3,77	4,59	5,19	5,42	119529	1115
2018-02	3,78	4,67	5,28	5,49	118951	1119
2018-03	3,88	4,79	5,41	5,64	114930	1141
2018-04	4,05	4,98	5,71	5,89	104283	1197
2018-05	4,41	5,22	5,94	6,29	100652	1281
2018-06	4,63	5,41	6,14	6,55	96520	1304
2018-07	4,75	5,55	6,24	6,68	96952	1306
2018-08	5,73	6,61	7,36	8,00	92723	1600
2018-09	6,37	7,42	8,29	8,92	99957	1674
2018-10	5,86	6,74	7,63	8,16	90201	1600
2018-11	5,37	6,11	6,92	7,45	95416	1478
2018-12	5,31	6,04	6,72	7,36	91270	1502
2019-01	5,37	6,13	6,90	7,49	104074	1562

Ek-2: M1 ve M2 Para Arzı Verileri

TARİH	M1 PARA ARZI	M2 PARA ARZI
2013-01	171648657	752407697
2013-02	171772600	751406806
2013-03	180944802	763376770
2013-04	179794721	773290765
2013-05	189925706	796167440
2013-06	201967585	807738125
2013-07	201287044	827649680
2013-08	210389829	852131839
2013-09	215113622	866492140
2013-10	213373183	869698340
2013-11	213243288	880339157
2013-12	225330535	910052031
2014-01	222778962	926478417
2014-02	221554826	930660071
2014-03	229538298	938075201
2014-04	225530537	934676019
2014-05	224382058	927561878
2014-06	238150238	953050237
2014-07	247677613	966305479
2014-08	241878967	968718703
2014-09	249785641	993410265
2014-10	247424552	985863566
2014-11	245494451	986974398
2014-12	251991723	1018546164
2015-01	251419161	1018089918
2015-02	256672749	1043797489
2015-03	261935572	1071698355

Ek-2 (Devam): M1 ve M2 Para Arzı Verileri

TARİH	M1 PARA ARZI	M2 PARA ARZI
2015-04	273990507	1100339648
2015-05	280246416	1109564558
2015-06	285907662	1129259516
2015-07	294157799	1151798945
2015-08	302536632	1177719805
2015-09	322378630	1219086712
2015-10	308090197	1189979858
2015-11	307160179	1189513751
2015-12	312005973	1195810095
2016-01	307780794	1205697764
2016-02	312767158	1215825528
2016-03	315704986	1231396884
2016-04	322480264	1232969976
2016-05	325211114	1256921835
2016-06	336562968	1272179301
2016-07	344856750	1287193949
2016-08	343756071	1288385902
2016-09	347747515	1304717378
2016-10	348794511	1327264814
2016-11	359751417	1374548287
2016-12	382351496	1406729188
2017-01	376732225	1434455756
2017-02	377212027	1401615999
2017-03	401173247	1441642897
2017-04	419127390	1468654894
2017-05	411475365	1488589565
2017-06	421573145	1505781397

Ek-2 (Devam): M1 ve M2 Para Arzı Verileri

TARİH	M1 PARA ARZI	M2 PARA ARZI
2017-07	419416200	1516361660
2017-08	433232693	1529488711
2017-09	434181238	1552264904
2017-10	429971761	1596047991
2017-11	437243382	1630658300
2017-12	449631796	1624675300
2018-01	428232624	1618277191
2018-02	433707515	1633681565
2018-03	451598421	1678936210
2018-04	463125545	1722685642
2018-05	496403641	1825422259
2018-06	513743217	1805825105
2018-07	509634432	1857436969
2018-08	588216432	2081025550
2018-09	559184535	2031956192
2018-10	523005315	1984481667
2018-11	488062659	1891085360
2018-12	512524057	1940589523
2019-01	505911428	1957327987

Ek-3: Sanal Para Borsasından Alınan Bitcoin (BTC) Verileri

TARİH	BTC	TARİH	BTC
2013-01	20,40	2016-02	1.419,73
2013-02	33,40	2016-03	1.295,34
2013-03	93,00	2016-04	1.385,19
2013-04	139,20	2016-05	1.728,61
2013-05	128,80	2016-06	2.105,26
2013-06	97,50	2016-07	2.298,85
2013-07	106,20	2016-08	1.737,97
2013-08	141,00	2016-09	1.734,95
2013-09	258,66	2016-10	2.211,36
2013-10	273,15	2016-11	2.666,67
2013-11	2.054,68	2016-12	4.694,84
2013-12	1.678,65	2017-01	3.703,70
2014-01	1.873,64	2017-02	4.500,18
2014-02	1.760,50	2017-03	6.288,15
2014-03	1.349,00	2017-04	6.039,94
2014-04	833,26	2017-05	12.390,96
2014-05	1.092,49	2017-06	8.724,65
2014-06	1.459,05	2017-07	9.334,66
2014-07	1.531,55	2017-08	16.859,67
2014-08	1.380,26	2017-09	15.938,82
2014-09	1.290,08	2017-10	23.635,09
2014-10	975,04	2017-11	45.396,58
2014-11	757,58	2017-12	52.007,59
2014-12	768,22	2018-01	37.322,66
2015-01	744,73	2018-02	37.376,37
2015-02	749,96	2018-03	27.075,10
2015-03	797,09	2018-04	36.127,37

Ek-3 (Devam): Sanal Para Borsasından Alınan Bitcoin (BTC) Verileri

TARİH	BTC	TARİH	BTC
2015-04	682,85	2018-05	34.820,10
2015-05	789,89	2018-06	28.747,01
2015-06	719,85	2018-07	37.898,36
2015-07	787,70	2018-08	44.217,36
2015-08	673,00	2018-09	40.085,62
2015-09	719,42	2018-10	34.321,30
2015-10	960,61	2018-11	20.600,00
2015-11	1.140,46	2018-12	20.377,67
2015-12	1.293,36	2019-01	18.738,07
2016-01	1.210,76		

ÖZ GEÇMİŞ

Adı, Soyadı	Yusuf ÇOLAK			
Doğum Yeri ve Yılı	Erzurum, 15.03.1984			
Medeni Durumu	Evli			
Bildiği Yabancı Diller ve Düzeyi	İngilizce (iyi)			
Öğrenim durumu	Başlama - Bitirme Yılı		Kurum Adı	
Lisans	2002	2003	İstanbul Ticaret Üniversitesi	
	2005	2012	İstanbul Üniversitesi	
Yüksek lisans	2017	2019	Recep Tayyip Erdoğan Üniversitesi	
Doktora	-	-	-	
Çalıştığı Kurumlar			Başlama-Ayrılma Yılı	
1. Artvin Çoruh Üniversitesi			2016	Devam
2. Asya Katılım Bankası A.Ş			2012	2015
3. Armodel Dekorasyon İnşaat Ltd. Şti			2009	2011
Katıldığı Proje ve Toplantılar	"2008 Küresel Finansal Krizinin Kırılgan Sekizli Ülkeleri Üzerindeki Etkileri", (Yükseköğretim Kurumları tarafından destekli bilimsel araştırma projesi) 29.04.2016 - 28.12.2017 (ULUSAL) "KOBİ'lerde Katılım Bankacılığı Algısı Artvin İli Örneği" Uluslararası Artvin Sempozyumu (Özet Bildiri/Sözlü Sunum) Yusuf Çolak, Barış Aydemir (2018)			
Yayınlar	"Kırılgan 8'lide Makroekonomik Değişkenler ile Kredi Notları Arasındaki İlişki" Ali Rıza Sandalcılar, Ali Altıner, Yusuf Çolak (2019) Uluslararası İktisadi ve İdari İncelemeler Dergisi (23), 257-276 "Türkiye'nin Makroekonomik Değişkenleri ile Kredi Notları Arasındaki Nedensellik İlişkisi: Moody's Örneği." Yusuf Çolak (2017). Uluslararası Ekonomi, İşletme ve Politika dergisi, 1(1), 61-74			
İletişim (eposta)	yusufcolak@artvin.edu.tr			