

**T.C.**  
**HASAN KALYONCU ÜNİVERSİTESİ**  
**SOSYAL BİLİMLER ENSTİTÜSÜ**  
**İKTİSAT ANA BİLİM DALI**  
**İKTİSAT TEZLİ YÜKSEK LİSANS PROGRAMI**

**YATIRIMCILARIN SANAL PARALARA OLAN YAKLAŞIMLARI**  
**BİTCOİN ÖRNEĞİ**

**YÜKSEK LİSANS TEZİ**

**HAZIRLAYAN**  
**ERDAL TEKER**

**GAZİANTEP-2019**

**T.C.**  
**HASAN KALYONCU ÜNİVERSİTESİ**  
**SOSYAL BİLİMLER ENSTİTÜSÜ**  
**İKTİSAT ANA BİLİM DALI**  
**İKTİSAT TEZLİ YÜKSEK LİSANS PROGRAMI**

**YATIRIMCILARIN SANAL PARALARA OLAN YAKLAŞIMLARI**  
**BİTCOİN ÖRNEĞİ**

**YÜKSEK LİSANS TEZİ**

**HAZIRLAYAN**  
**ERDAL TEKER**

**TEZ DANIŞMANI**  
**DR. ÖĞR. ÜYESİ M.LAMİHA ÖZTÜRK**

**GAZİANTEP-2019**



SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE  
YÜKSEK LİSANS KABUL VE ONAY FORMU

İktisat Anabilim Dalı İktisat Tezli Yüksek Lisans Programı öğrencisi **Erdal TEKER** tarafından hazırlanan “**Yatırımcıların Sanal Paralara Olan Yaklaşımları: Bitcoin Örneği**” başlıklı tez, **16/01/2019** tarihinde yapılan savunma sınavı sonucu **başarılı** bulunarak jürimiz tarafından **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Görevi

Unvanı, Adı ve Soyadı

İmzası:

Kurumu/Üniversitesi

**Tez Danışmanı**

Dr. Öğr. Üyesi Lamiha ÖZTÜRK

Hasan Kalyoncu Üniversitesi

**Jüri Başkanı**

Prof. Dr. Zehra Vildan SERİN

Hasan Kalyoncu Üniversitesi

**Jüri Üyesi**

Dr. Öğr. Üyesi Gülferah BOZKAYA

Kahramanmaraş Sütçü İmam Üniversitesi

**Bu tez Enstitü Yönetim Kurulunca belirlenen yukarıdaki jüri üyeleri tarafından uygun görülmüş ve Enstitü Yönetim Kurulu kararı ile onaylanmıştır.**

Prof. Dr. Mazlum ÇELİK  
Enstitü Müdürü

## TEZ ETİK VE BİLDİRİM SAYFASI

Yüksek lisans tezi olarak sunduğum “Yatırımcıların Sanal Paralara Olan Yaklaşımları: Bitcoin Örneği.” başlıklı çalışmanın tarafımda, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bunlara atıf yapılarak yararlanmış olduğumu belirtir ve onurumla doğrularım.16/01/2019

ERDAL TEKER



## ÖNSÖZ

Yüksek Lisans tezimde kaynak olarak kullandığım her türlü çalışmada emeği geçen tüm profesyonellere, çalışmamda konu seçiminde, yürütülmesinde, sonuçlandırılmasında ve sonuçlarının değerlendirilmesinde yardımcı olan tüm Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü bölümü hocalarına ve danışmanım Sayın Dr. Öğr. Üyesi M. Lamiha ÖZTÜRK hocama, yapılan çalışmalarda her türlü yardımı yapan ve tecrübesini paylaşan arkadaşlarıma teşekkür ederim.



## ÖZET

Bu çalışma en popüler kripto para birimi olan Bitcoin'nin alım satımının nasıl yapıldığını, avantajlarını ve dezavantajlarının neler olduğunu, Türkiye' de artış gösteren işlem hacminin altında yatan nedenlerin yanında blok-zincir sistemi üzerinde durmayı amaçlamaktadır.

Çalışma sonucunda, Bitcoinin ortaya çıktığı andan günümüze çok mesafe kaydettiği, mevcut zaman zarfında güvenli sonucuna ulaşılsa da gelişimini devam ettiren bir ivme içerisinde olduğu henüz dünya genelinde tam anlamı ile ekonomi yönetimleri tarafından kabul edilmediği, gerçek paranın yerini alamadığı görülmekte olup yüz yüze değişimlerde gerçek paranın sağladığı pratik işlem kabiliyetini taşımadığı görülmüştür. Bitcoin'in anonim yapısı hukuki statüsünün oluşturulmaması ve dünya genelinde tümüyle kabullenilmemiş olması takibinin zor olması gibi nedenlerden dolayı yasa dışı faaliyetlerde ve illegal yollarda kullanıldığı tahmin edilmektedir. Bunun yanında yatırımcıların sanal paralara olan yaklaşımları bir mülakat çerçevesinde incelenmiştir.

**Anahtar kelimeler:** Bitcoin, Blok-Zincir, Kripto-para

## ABSTRACT

This study is the most popular crypto-currency, how to do Bitcoin's trading, it is what their advantages and disadvantages, in Turkey, aims to focus on block-chain system alongside the underlying causes of the volume of transactions showed an increase.

At the end of the study, it is seen that Bitcoin has made a great distance to the present and that although it has reached a safe conclusion in the current time, it is still in an acceleration that continues its development. It is seen that it does not have practical processing capability. It is estimated that Bitcoin has been used in illegal activities and illegal roads due to the fact that the legal status of the Bitcoin is not established and the fact that it is difficult to follow up as it is not fully accepted in the world. In addition, investors' approaches to virtual money were examined in an interview.

**Keywords:** Bitcoin, Block-chain, Crypto-money

## İÇİNDEKİLER

Sayfa No.

ÖNSÖZ.....	i
ÖZET.....	ii
ABSTRACT.....	iii
İÇİNDEKİLER.....	iv
TABLolar LİSTESİ.....	vii
ŞEKİLLER LİSTESİ.....	viii
KISALTMALAR LİSTESİ.....	ix

### BİRİNCİ BÖLÜM

GİRİŞ.....	1
1.1. Araştırmanın Konusu ve Önemi.....	2
1.2. Araştırmanın Problemi.....	2
1.3. Araştırmanın Yöntemi.....	3
1.4. Sanal Para Üzerine Yapılan Akademik Araştırmalar.....	4
1.4.1. Yurt İçinde Yapılan Akademik Araştırmalar.....	4
1.4.2. Yurt Dışında Yapılan Akademik Araştırmalar.....	5

### İKİNCİ BÖLÜM

<b>SANAL PARA VE UYGULAMA ORTAMLARI</b> .....	<b>6</b>
2.1. Sanal Para Tanımı.....	6
2.2. Sanal Paranın Gelişimini Etkileyen Faktörler.....	7
2.3. Sanal Para Modellerinin Genel Özellikleri.....	8
2.4. Sanal Para ve Diğer Ödeme Sistemlerinin Karşılaştırılması.....	9
2.4.1. Bağımsızlık.....	10
2.4.2. Sistem Güvenliği.....	10
2.4.3. Kişisel Hakların Korunması.....	10
2.4.4. İşlem Maliyetleri.....	11
2.4.5. Transfer Edilebilirlik.....	11
2.4.6. Bölünebilirlik.....	11
2.4.7. Ödemelerin İspat Edilebilirliği.....	12
2.5. Sanal Paraya Dayalı Ödeme Sistemleri.....	12
2.6. Elektronik Ödeme Sistemleri.....	13



2.6.1. Kredi Kartı .....	13
2.6.2. Elektronik Fon Transferi (EFT).....	14
2.6.3. Elektronik Çek .....	14
2.6.4. Akıllı Kart .....	15
2.6.5. Elektronik Para .....	15
2.6.5.1. E-Cash .....	16
2.6.5.2. CyberCash .....	16
2.6.5.3. Netcash .....	17
2.6.5.4. Mondex .....	18

## **ÜÇÜNCÜ BÖLÜM**

<b>BİTCOİN'E GENEL BAKIŞ .....</b>	<b>19</b>
3.1. Bitcoin'in Tarihçesi .....	20
3.1.1. Dünyada Bitcoin'in Tarihsel Süreci .....	20
3.1.2. Türkiye'de Bitcoin'in Tarihsel Süreci .....	21
3.2. Bitcoin İle Geleneksel Para Sistemi Arasındaki Farklılıklar.....	24
3.3. Bitcoin Kullanmanın Avantajları ve Dikkat Edilmesi Gereken Noktalar .....	25
3.4. Btc İle Alakalı Mali ve Teknik Eleştiriler .....	28
3.5. Bitcoin'in Çalışma Mekanizmasının Özellikleri .....	30

## **DÖRDÜNCÜ BÖLÜM**

<b>BİTCOİN VE DİĞER PARA BİRİMLERİ ÇALIŞMA MEKANİZMASI VE TEKNOLOJİK ALTYAPISI .....</b>	<b>31</b>
4.1. Teknolojik Arka Plan .....	31
4.1.1. Kriptolojik Özet Fonksiyonu (Hash Function) .....	31
4.1.2. Sanal İmza .....	32
4.1.3. Bitcoin Adresi .....	33
4.1.4. İş Kanıtı (Proof of Work) .....	34
4.2. Bitcoin Transferi .....	36
4.3. Bitcoin'in Çalışma Sistemi.....	37
4.4. Bitcoin Cüzdanı .....	40
4.5. Bitcoin İşlemleri .....	40
4.5.1. İşlem Masrafı ve İşlemin Onaylanması .....	42
4.5.2. Çifte Harcama .....	44

4.6.	Blok-Zincir (Blockcham) .....	46
4.7.	Bitcoin Üretimi ( Bitcoin Madenciliği) .....	48
4.8.	Bitcom Ağı .....	50
	4.8.1. Tam Uç (Full Node) .....	51
	4.8.2. Hafif Uç (Lightweight Node) .....	52
4.9.	Altcoinler .....	52

## **BEŞİNCİ BÖLÜM**

	<b>BİTCOİN VE GENEL KARAKTERİSTİK ÖZELLİKLERİ.....</b>	<b>54</b>
5.1.	Bitcoin Alımı .....	54
	5.1.1. BTC Piyasaları.....	54
	5.1.2. Birebir Ticaret Yoluyla Bitcoin Alım ve Satımı .....	55
	5.1.3. Bitcoin ATM'leri Yoluyla Bitcoin Alım ve Satımı. ....	57
	5.1.4. Diğer Alım Satım Yöntemleri. ....	57
	5.1.5. Bitcoin Piyasası ve Para Arzı. ....	58
5.2.	Bitcoin'nin Yasal Statüsü ve Btc' ninKara Para Aklama İlişkisi.....	60
5.3.	Bitcoin' in Avantajları ve Dezavantajları .....	64

## **ALTINCI BÖLÜM**

	<b>SONUÇ .....</b>	<b>66</b>
	<b>KAYNAKÇA .....</b>	<b>68</b>
	<b>EKLER.....</b>	<b>73</b>
Ek	1. Bitcoin Hakkında Yapılan Görüşme .....	73

## TABLULAR LİSTESİ

	Sayfa No.
<b>Tablo 1:</b> Para, Nakit Para, Çek, Banka Kartının Özellikleri .....	9
<b>Tablo 2:</b> Basitleştirilmiş Bir Bitcoin Uygulama Örneği.....	41
<b>Tablo 3:</b> Bitcoin Alış & Satış Komisyonları .....	59



## ŞEKİLLER LİSTESİ

Sayfa No.

Şekil 1: Sanal Mevduat Birimlerinin Sınıflandırılması .....	12
Şekil 2: Bitcoin'in Logosu .....	19
Şekil 3:Fiziki Bitcoin Örnekleri.....	20
Şekil 4: BDDK' nın Bitcoin İle İlgili Basın Açıklaması .....	23
Şekil 5: Sha-256 Özet Fonksiyonu Örneği .....	31
Şekil 6: (A) İmzalama (B) İmza Doğrulama .....	32
Şekil 7:Uygulamada Kullanılan Bir Bitcoin Adresinin Örnek Bir QR Kodu.....	34
Şekil 8:İş Kanıtı .....	35
Şekil 9: Bitcoin Sisteminde Gerçekleşen İşlemlerin Genel Görünümü.....	36
Şekil 10: Bitcoin'in İşleyiş Mekanizması .....	38
Şekil 11:Çay İçen Bir Tüketicinin Bitcoin İle Ödeme İşlemi.....	42
Şekil 12:Basitleştirilmiş Blok-Zincir Veri Yapısı .....	46
Şekil 13: Blok-Zincir'deki Çatallaşma Örnekleri (A) Nadiren (B) Çok Nadiren Görülen Durumlar .....	47
Şekil 14: Bitcoin Üretimi ( Bitcoin Madenciliği) .....	48
Şekil 15: Bitcoin Madencileri Ne Türü Çalışırlar.....	49
Şekil 16: Bir Bitcoin Sahibinin, Başka Birine Sistem Üstünden Bitcoin transfer etmesi .....	50
Şekil 17: 18 Mayıs 2018 İtibarıyla Dünya Üzerindeki Bitcoin Ağındaki Tam Uçlar .....	51
Şekil 18:Bitcoin Ödemesi Kabul Eden Bir İşletme .....	56
Şekil 19: Bir Bitcoin ATM' si .....	57
Şekil 20:Bitcoin 2018 Yılı Fiyat Grafiği .....	59

## KISALTMALAR LİSTESİ

<b>age.</b>	:	Adı geçen eser
<b>A.B.D</b>	:	Amerika Birleşik Devletleri
<b>USD</b>	:	Amerika Birleşik Devletleri Doları
<b>ATM</b>	:	Automated Teller Machine (Otomatik Vezne Makinesi)
<b>BTC</b>	:	Bitcoin
<b>bk.</b>	:	Bakınız
<b>bs.</b>	:	Baskı, basım
<b>C.</b>	:	Cilt
<b>DİE</b>	:	Devlet İstatistik Enstitüsü
<b>DTÖ</b>	:	Dünya Ticaret Örgütü
<b>EFT</b>	:	Elektronik Fon Transferi
<b>E-para:</b>	:	Elektronik para
<b>EU</b>	:	European Union
<b>IMF</b>	:	International Monetary Fund
<b>KHK</b>	:	Kanun Hükmünde Kararname
<b>LTC</b>	:	Litecoin
<b>mad.</b>	:	Madde
<b>HKÜ</b>	:	Hasan Kalyoncu Üniversitesi
<b>Nu.</b>	:	Numara
<b>s.</b>	:	Sayfa
<b>TL</b>	:	Türk Lirası
<b>vb.</b>	:	Ve Benzeri
<b>BTC</b>	:	Bitcoin
<b>yy</b>	:	Yüzyıl

# BİRİNCİ BÖLÜM

## GİRİŞ

Ekonomi en net manası ile bölgesel yâda ulusal çapta üreticiler, dağıtıcılar ve mal ve hizmetleri tüketen kişilerden meydana gelen bir bütüncül ağ olarak ifade edilebilir. (Sutherlandve Canwell, 2009:52). 2013 yılında Türkiye’de günlük ortalama işlem sayısı 15.000 iken 2017 yılının Nisan ayında günlük ortalama işlem sayısı 500.000’ e yaklaşmıştır. Hızlı bir şekilde artan işlem sayısı ve 2018 yılının Ocak ayından bu yana sanal para olarak kabul edilen Bitcoin birincil piyasaları etkilemeye başlamıştır.

İşlem sayısındaki artış, piyasalara etkisi ve artan popülüratesi sebebi ile bitcoin sanal para çalışmamıza konu olmuştur.

Hızla gelişen sanal paraların geleceği üzerinde durmanın tartışılmaz bir gerçek olacağı kabul edilmektedir.

Bu çalışmanın amacı Bitcoin sanal para birimi tercih edilme nedenlerini araştırmayı hedeflemektedir. Bu bağlamda Türkiye’ de sosyal medya aracılığı ile çok geniş kitlelere ulaşan ve arabuluculuk yapan Semih Başaran ile birebir görüşme gerçekleştirilmiştir. Söz konusu görüşme çerçevesinde bitcoin sanal para kullanımının avantajları, dezavantajları ve Türkiye’ de artan popülüratesi sorgulanmıştır.

Çalışmanın birinci bölümünde sanal para uygulamaları, sanal paranın tanımı, sanal paraların gelişimini etkileyen faktörler ve sanal para uygulamalarının genel özellikleri ele alınmıştır.

Çalışmanın ikinci bölümünde bitcoine genel bakış, bitcoin uygulamaları, bitcoin’in tanımı, teknolojik arka planı, avantajları, dezavantajları ele alınmıştır.

Üçüncü bölümde bitcoin ve diğer para birimlerinin çalışma mekanizmalarına değinilmiştir.

Dördüncü bölümde sanal paranın teknolojik alt yapıları hakkında bilgilere yer verilmiştir.

Beşinci bölümde bitcoin ve genel karakteristik özelliklerine değinilmiştir

Son bölümde sonuç, tartışma, geleceğe yönelik öneriler, kaynakça ve ekler yer almaktadır.

## **1.1. Araştırmanın Konusu ve Önemi**

Araştırmamızın konusu 2009 yılından bu yana Bitcoin gibi sanal para birimlerinin kısa bir zaman zarfı içerisinde sosyal ve yazılı medyanın ilgi odağı olması konvansiyonel para birimlerinin yanı sıra sanal paranın bir değişim aracı olarak kullanılmasıdır. Dünya üzerinde hızla gelişen sanal para sistemi, 2013 yılında Türkiye’ de de duyulmaya ve yayılmaya başlanmıştır.

Ülkemizde 2013 yılında sanal paraların borsası oluşmasıyla beraber bitcoin ve bitcoin gibi sanal para çeşitlerinin alım satım işlemleri de başlamıştır. Aynı yıl içerisinde BDDK’nın 2013/32 sayı ve 25.11.2013 tarihli basın duyurusu ile sistem hakkında ülke vatandaşlarının her türlü iş ve işlemlerinde dikkatli olmalarının gerekliliğine ilişkin basın açıklaması yapılması gereği hissedilmiş olup konunun önemine dikkat çekilmiştir.

2013 yılında faaliyete geçen sanal para Türk borsaları 2018 yılına kadar hacimlerini genişleterek büyük bir taraftar kitlesine ulaştığı gözlemlenmiştir. Bu bağlamda bu çalışmanın konusu ve önemi tüketiciler ve alım satım yapan kişilerin neden sanal paralara yöneldiklerini? Yasal düzenlemesi henüz netleşmemişken bitcoin gibi kripto paraların yaygınlaşmasının ve popülüratesinin nedenlerinin araştırılması hedeflenmiştir.

Türkiye’de sosyal medya grupları (Telegram,Facebook, Twitter) aracılığıyla çok geniş kitlelere ulaşan aynı zamanda söz konusu sanal para işlemlerine aracılık eden Semih Başaran ile bire bir görüşme gerçekleştirilmiştir.

Dünya çapında popüler araştırma konularından olan elektronik ödeme araçları vesistemleri ile bu alanda yaşanan gelişmelerin gelecek için de aynı düzeyde önemli olacağı düşünülmektedir. Günümüzde mekândan bağımsız olarak dünyanın bir ucundan diğer ucuna tek bir hamlede fon transferleri yapılabilmektedir.

Kripto para teknolojisini hem finansal açıdan hemde temelinde barındırdığı altyapı dolayısıyla teknik açıdan inceleme imkânı bulunmaktadır. Bu çalışma kapsamında teknik açıdan da temel düzeyde bilgilendirme yapılmış olup, Türkçe literatür için temel teknik bilgi ve finansal araştırma kaynağın tek bir noktada toplanması düşünülmüştür.

## **1.2. Araştırmanın Problemi**

Yatırımcıların sanal paralara olan yaklaşımlarının altında yatan olguların bitcoin örneği üzerinden araştırılması ve 2009 yılında ortaya çıkan ‘bitcoin’ sanal para sisteminin

gelişimi geleceği hakkında bilgi kaynağı oluşturmaktır. Bu çalışmamızda söz konusu sanal para sisteminin kısa bir zaman diliminde insanlar arasında bu kadar hızlı yayıldığı sorusunun cevaplandırılmaya çalışılmıştır.

Geçmişte olduğu gibi günümüzde de finansal piyasalarda taraflar arasında gerçekleşen mal veya hizmet alım satımı için ödemelere ihtiyaç duyulmaktadır. Takas ile başlayan ticaret hayatı paranın icadı ile temel bir düzene kavuşmuştur. Ödeme araçları, ticaretin temelini oluşturmaktadır. İnsanlık tarihiyle beraber başlayan ticari hayat, günümüze kadar çok farklı şekillerde yapılmıştır. Teknolojinin gelişmesine paralel olarak ödeme araçları, elektronik ödeme araçlarına geçiş eğilimi göstermiştir. Günümüzde ödeme araçlarından bir türü de sanal para sistemleridir (Ateş, 2016: 358).

Bitcoin, her yerde herkese hızlıca ödeme olanağı sağlayan, merkezi olmayan dijital kriptoparadır. Bitcoin'ler satın alınabilir, bir başkası ile değiştirilebilir ve bir başkasına satılabilir. 2140' ta toplam 21 milyon adet Bitcoin (Btc) imal edilmişolacağı tahmin edilmektedir. Sanal para altyapılarından yararlanılarak türeyen çok fazla alt coin bulunmaktadır. Dijital para ticaretine aracılık eden toplam market hacmi 2017 yılı içerisinde 370 Milyar USD' nin üstünde gerçekleşmiştir. Söz konusu sanal paranın fiziki karşılığının olmaması ve oturmuş bir düzenin değişmesinin zorlukları nedeniyle sisteme mesafeli olanların sayısı çok fazladır. Dünyada pek çok ülke Bitcoin'e karşı pozitif bir bakış açısına sahipken; aynı zamanda yurttaşlarını fiyat hareketliliğinin ani değişimlerine, herhangi bir varlığa endeksli olmayışı ve herhangi bir merkezi otoriteye dayanmaması sebebiyle oluşabilecek riskler konusunda ikaz etmektedir.

### **1.3. Araştırmanın Yöntemi**

Bu çalışmada, insanların sanal paralara olan yaklaşımlarının yanı sıra sanal paraların tercih edilmesi hakkında bir anket düzenlenmiştir. Söz konusu anket bitcoin örneği üzerinde incelenecektir. Çalışmamız nicel ve nitel olarak analiz edilmiştir. Anket çalışmamızda on bir soruya yer verilmiştir. Anket çalışmamız 11.11.2018 tarihinde birebir görüşme şeklinde gerçekleştirilmiştir. Anket sorularının güvenilirliği ve anlaşılabilirliğini test etmek üzere ilk önce bir pilot çalışma ile iyileştirilmiştir. Anketimize 2017 yılından bu yana sosyal medya grup kitlelere ulaşan Semih Başaran katılmıştır. Elde edilen verilerin SPSS programı ile analiz edilmiştir. Soruların güvenilirliğini test etmek üzere t-testi ve scheldule testi uygulanmıştır.



## 1.4. Sanal Para ve Bitcoin Üzerine Yapılan Akademik Araştırmalar

Sanal para ve bitcoin üzerine bu zamana kadar gerçekleştirilmiş akademik çalışmalar yurt içinde yapılmış akademik çalışmalar ve yurt dışında yapılmış akademik çalışmalar şeklinde sınıflandırılmasında fayda bulunmaktadır

### 1.4.1. Yurt İçinde Yapılan Akademik Araştırmalar

**Çarkacıoğlu (2016)**, “Kripto-Para Bitcoin” isimli çalışmasında kripto para ve bitcoini incelemiştir. Çalışmasının sonucunda; Bitcoin Güvenlidir. Binlerce yıldır alışlagelmiş altın ile asırlardır kullanılan banknotlar ile kıyaslandığında sanal kripto-para olan Bitcoin’ni çok yeni olduğu görülmektedir. Kazandığı teknoloji geleceğe yönelik ümit verici ve geliştirilebilir konuları ihtiva etmektedir. Bitcoin ile birlikte birçok altcoinler türetilmiş olup ama bu altcoinlerin başarı performansları Bitcoin'e bağlıdır.

**Tüfek (2017)**, elektronik ödeme araçları ve geleceğin yaklaşımı kripto para isimli çalışmasında Ödeme araçlarının değişiminin devam edeceği ve bu değişimin finansal piyasalar ile kullanıcı alışkanlıklarına önemli derecede etki edeceği açıktır. Elektronik ortama taşınan ödemelerin güvenliğinin ve kesintisiz olmasının gelecekte çok daha önem arz edeceği düşünülmektedir.

**Bozkurt Yüksel (2014)**, “Elektronik Para, Sanal Para, Bitcoin ve Linden Doları’na Hukuki Bir Bakış” isimli çalışmasında elektronik paranın üstünlükleri ve olumsuz yönleri ile alakalı tavsiyeler dünya genelindeki ve ülkemizdeki tatbik edilme biçimleri nazarında tetkik edilmiştir. Çalışmanın sonucunda yasa yapıcının, sanal para birimleri kulvarındaki teknolojik ilerlemeler ve araştırmalara yabancı olmaması, vergi kaçakçılığı, hilekârlık, para aklama vb. gibi cürümlerin teknolojiden yararlanılarak ifa edilmesine olanak tanınmaması, tüketicinin korunmasının sağlanması yönünden büyük önem arz etmektedir. Burada üzerinde durulması icap eden konu da çok etkiliyasal düzenlemelerin oluşturularak ilerlemenin önünde set olmamak ve yenilikleri desteklemek ve bununla birlikte bu alanı açık kapı bırakmayacak biçimde düzenlemesinin de yapılmasıdır.

**Yakupoğlu (2016)**, çalışmasında veri tabanı sistemlerinde devrim niteliğinde olan blokzincir yapısının ve bu yapıya ait mesaj sisteminin detaylarını vermiştir. Teknik olarak çok karmaşık algoritma ve yöntemler barındıran kripto para sistemlerinin bu karmaşık işlemler sayesinde güvenli bir sistematik çerçevesinde çalıştığı görülmüştür.

**Bilir ve Çay (2016)**, Ticaretin gelişimi ile birlikte insanlar çeşitli ödeme araçları kullanmaya başlamıştır. Günümüzde elektronik ödeme yöntemlerinin yaygın bir kullanım alanı bulunmaktadır. Elektronik ödeme yöntemlerinin yaygınlaşması bir takım artı ve eksilerini de beraberinde getirmektedir. Transferlerin dijital olarak gerçekleştirilebilmesi; işlem masraflarının minimize edilmesi ve transferlerin seri şekilde yapılması gibi nedenlerde etkinlik sağlamıştır. Öte yandan dijital para, btc ve türevlerinin merkezi otoritelerin, devletlerin egemenlik sınırları hakkındaki tereddütleri de bir tartışma konusu haline getirmiştir. Tüm bu bilgiler ışığında dijital para ve türevlerinin finans sektörü üstündeki önem derecesini biraz daha artırmaktadır.

#### **1.4.2. Yurt Dışında Yapılan Akademik Araştırmalar**

**Raiborn ve Sivitanides (2015)**, değişik ülkeler ile ilgili yapılan çalışmada, bazı ülkelerin Bitcoin'in para tanımına uymadığı ve ödeme aracı olarak kullanılmayacağı görüşlerini değerlendirmiştir. Yapılan değerlendirme sonucunda bu tür negatif görüşlerin bile Bitcoin ekosisteminin genişlemesinin önüne geçememiş olduğu belirtilmiştir.

**Andreas (2014)**, Bitcoin'ler için güvenliğin ve ayrıca fiziki olarak saklanması gerekliliğinin önemine değinmiştir. Fakat bu fiziki kâğıt cüzdanlardaki kare kodların fotoğraflanmasının Bitcoinlerin çalınmasına sebep olabileceği ifade edilmiştir. Bank of Kanada'nın 2014 yılında yapılan çalışmasına göre, kripto paralar herhangi bir merkezden etkilenmeyen ve bağımsız bir elektronik para olarak tanımlanmıştır. Çalışmada, basımı veya ihracı olmayan bu tür para birimlerinin tamamen sayısal olarak üretiminin yapıldığı belirtilmiştir.

**Nakamoto (2008)**, gerçekleştirdiği araştırmasında sanal para terminolojisine kripto para isminde yeni bir terim ilave etmiştir. Kripto paraların ilk prototipi olan Bitcoin bu araştırmayla birlikte küresel bazda ilan edilmiştir. Gerçi yeni bir teknoloji ile alternatif sanal para sisteminin anlatıldığı araştırmasında ileriki dönemlerde faydalanılabilecek veri tabanı yapılarının ilk tipi prezante edilmiştir. Nakamoto bu araştırmasında sistemin hayati noktalarını ve anonimlik yapısını teferruatlı biçimde izah etmiştir. Nakamoto, açık kaynaklı yazılım ile tasarladığı bu modülde müşterilerin meydana getireceği beraberlik ile sistem üzerinde iyileştirmeler olabileceğini dile getirmiştir. Araştırmasında, kodlama algoritmalarının hâlihazırda kullanılmakta olan sistemlerden bir farkı bulunmasa da modern dağıtık dosya bilgisi ve kronolojik sıralama dizilimiyle güvenlik unsurunun üst düzeyde tutulduğu ifade edilmiştir.

## İKİNCİ BÖLÜM

### SANAL PARA VE UYGULAMA ORTAMLARI

Bilgi çağının başlaması ile birlikte, ağ ile iletişimden artan bir şekilde bağımlı olmaktadır. Bilgisayara dayalı teknolojinin, bilginin erişimi, saklanması ve dağıtılması gibi konularda önemli etkisi vardır. Bu teknolojinin en önemli kullanım alanlarından birisi ise elektronik ticarettir. Elektronik ticaretin etkin bir biçimde ifa edilebilmesi için güvenli ve uygun elektronik ödeme sistemlerinin geliştirilmesi gereklidir.

Perakende mağazalardaki satış noktası sistemlerine ilave olarak, internet gibi ticaret ve işlemlerin yeni şekilleri ortaya çıkmaya başlamıştır. Elektronik teknolojinin gelişimi ticaret yapmak için yeni yollar ve fırsatlar sunmaktadır.

#### 2.1. Sanal Para Tanımı

Sanal paranın tanımını yapmadan önce paranın tanımını yapmakta fayda bulunmaktadır. Çoğunlukla insanların para olarak kabul ettiği her şey paradır. Paranın üç ana işlevi bulunmaktadır. Bunlar; değişim aracı, tasarruf aracı ve hesap birimi olmasıdır (Çay ve Bilir, 2016: 27).

Elektronik paranın bir türü de sanal paradır. Söz gelimi sanal para, elektronik paranın alt kümesidir. Elektronik para ve sanal parabil dijital para formatındadır. Fakat sanal para ve dijital para arasında bir takım farklar vardır. Elektronik parada hesap birimi Avrupa Birliğinin kullanmış olduğu Euro, Amerika Birleşik Devletleri başta olmak üzere bazı diğer ülkelerinde kullandığı Dolar veya da Türkiye'nin resmi para birimi TL gibi klasik, hukuki dolanımı olan para çeşitleridir. Hâlbuki sanal para birimleri Bitcoin, Linden Doları, vb. gibi daha sonra keşfedilen ve yasal donanımı olmayan para türleridir.

Elektronik para, onu çıkaranlar haricindekiler tarafından, dijital mevduat terimleriyle dijital bir kitle içerisinde kabul görmektedir. Dijital mevduat hukuki yapı olacak şekilde düzenlenebilmektedir. Ancak mevcut dijital para birimlerinin hukuksal bir yapısı bulunmamaktadır. Kripto para birimlerini içeren yasal bir mevzuat bulunmamakla birlikte dijital paraların kendi teamülleri bulunmaktadır. Sanal parayı mali alanda bulunmayan hususi bireyler arz etmektedir. Dijital mevduatın sunumu belirli bir düzene bağlıdır. Dijital mevduatlardaysa para arzı değişkendir, dijital mevduatı arz eden kesimin isteğine bağlanmıştır. Dijital mevduatın itibari kıymeti garanti edilmekteyken kripto mevduatınki

garanti edilememektedir. Dijital mevduat, kontrol altındaiken, Kripto mevduatta kontrol bulunmamaktadır. Elektronik mevduat riski  $\frac{işletimsel/}{operasyonel}$  şeklinde oluşabilir. Kripto mevduatta hem  $\frac{işletimsel/}{operasyonel}$  yönünden hem de, yasal mevzuat olarak, kredi, tedavül yeteneği şeklinde risk unsurları barındırmaktadır. (European Central Bank, 1998, s.16. ). Avrupa Merkez Bankası tarafından: “düzenlemesi olmayan onu geliştirenler tarafından çıkarılan ve kontrol edilen ve belli bir sanal çevre içinde kabul gören dijital para” biçiminde sanal paranın tanımı ifade edilmektedir. “Avrupa Merkez Bankası” ileriki zamanlarda kripto mevduatın yapısında büyük farklılıklar yaşanması durumunda tarifinin de başkalaşacağını söylemektedir (European Central Bank: Virtual Currency Schemes, Germany 2012: 13).

Günümüzde farklı kripto mevduat çeşitleri bulunmaktadır. Kripto mevduat ve türevlerinin oluşturulabilmesinin 2 ana yöntemi vardır. Bu yöntemlerden ilki evvelinde tespit edilmiş olan kur üstünden reel mevduatın kripto mevduata çevrilmesi, fiziki mevduat ile kripto mevduatın satın alınması şeklinde olabilir. Sanal paranın varlığa dayanan bir geçmişi çoğunlukla yoktur. 2. yöntemse müşterilerin ellerinde bulunan dijital mevduat birikimlerini kendi çabalarıyla fazlalaştırmalarıdır. Mesela reklama katkı sağlayarak yâ da anketi yanıtlarak olabilmektedir (European Central Bank, 2012: 13).

## 2.2. Sanal Paranın Gelişimini Etkileyen Faktörler

Sanal paranın yaygınlaşma düzeyi, sanal para temin edicilerinin ve sanal para satan kişiler için yapılan teşvikler ile doğru orantılıdır. Sanal para temin edicileri için muhtemel teşvikler bireyler ile üye işyerinden alınan her türlü komisyonlardan sağlanan kazançlardır. Sanal mevduat arz eden finans kurumları içinse, nakit paraya ikame edilen dijital mevduat kadar azalan nakit mevduat işletmekten kazandıkları maliyet unsurları daha cazip hale gelecektir. Bu duruma engel teşkil edecek bir olgu var ise yürürlükte olan yada yürürlüğe girmesi beklenen düzenlemelerle ilgili oluşabilecek masrafları ödemek olacaktır.

Müşterilerin sanal mevduat talebini belirleyecek etkenler;

- Sanal para tedarikçilerince alınacak masrafların öteki ödeme yöntemleri ile mukayese edilmesine,
- Kişisel hakların muhafaza edilmesi ve sanal paranın sağladığı güvenlik,
- Sanal para araçlarının kullanılmasındaki pratiklik ve rahatlık,
- Sanal para satımı yapanların sanal parayı kabul etme rağbetine bağlı olacaktır.
- Sanal para satımı yapanların sanal parayı kabul etme istekleri ise;

- Sanal para temin edicilerin yâ da operatörler tarafından talep edilecek giderlerin tutarı.
- Terminallerin maliyeti ile ilişkili olacaktır.

Lakin en önemli husus satıcılar ve tüketicilerin bu yeni teknolojiyi önem vermeleridir. Potansiyel kullanımı ve gelişimine bakıldığında, karta dayalı dijital ürünler miktarı az olan ödemelerde işlemleri pratikleştirmek maksadıyla oluşturulmuş ve bu sebeple madeni ve kâğıt paralar için bir ikame ödeme yöntemi olarak kullanılmaktadır. Kredi kartı yâda banka kartı ile gerçekleştirilen işlemlerde çevrim içi yetkilendirme gerekmesi sebebiyle, miktarı az olan alım satımlarda kullanılması üye satıcı kurumlar nezdinde maliyetinden dolayı çok sıcak karşılanmamaktadır. Ancak bu yeni karta bağlı dijital transfer çeşitlerinin belirli bir onay akışına gerek kalmaması sebebiyle küçük tutarlı transferlerde kullanılması uygun olmaktadır.

Software (Yazılım programlarına) dayanan işlemciler, bilhassa online olarak belirli bir mesafe üzerindeki ödemelerde kullanım yapılabilir.

Nakit paraya dayalı ekonomik sistemlerde sanal para ürünlerinin sağlamış olduğu verim artışları daha fazladır. Son zamanlarda iletişim ve bilgi işlem maliyetlerinin azalması gelişmiş piyasa ekonomilerinde nakitsiz perakende ödeme altyapıları olan ülkeler, bu altyapıların sanal para işlemlerini sanal para modelleri ile de yapabilmektedirler.

### **2.3. Sanal Para Modellerinin Genel Özellikleri**

Sanal para teknik uygulamaları yönünden birbirinden farklılıklar ihtiva etmektedir. Sanal para modeli sürecinde ağ operatörleri, sanal para tedarikçisi, özel bilgisayar yazılım ve donanım satıcıları ile sanal para işlemlerini tahsil edenler olmak üzere 4 tip hizmet sağlayıcı bulunmaktadır. Tedarikçiler hizmet sağlayıcıları içerisinde en önemlileridir. Buna karşılık satıcılar ve ağ operatörleri yalnızca teknik hizmet sunmaktayken, değişim kurumları, nakde dayalı olmayanenstrümanlarına mevcut uygulamadaki sistemden farksız bir hizmet sunan finans kurumları ve/veya bu kurumların sahibi olan teşekkülleri bu hizmeti vermektedir. Genellikle en az iki tedarikçi bulunmaktadır. Lakin bazen bir tek tedarikçiyle bundan ürünü “satın alıp” alıcılara “satan” farklı kurumlarda bulunmaktadır. Ürünler değer aktarılma biçimlerinde birbirlerinden farklılaşmaktadır. Bazı modeller 3. bir tarafın karışmasına ihtiyaç olmadan bir tüketiciden ötekine dijital bakiyelerin yollanmasına imkân verirler. Fakat çoğunlukla kullanılan ödeme biçimi ise tüketiciden-satıcıya tarzındadır. Bunun yanında sınırlı sayıda sanal para modelleri şahsi işlemlerde yalnızca kısıtlı kayıt yapılmasını yâda hiçbir kaydın yapılmamasını programlamaktadırlar. Tüketiciden-tüketicie doğrudan işlemlerin gerçekleştirilmesine imkân tanınan hallerde, yapılan işlemlerle alakalı ayrıntılar yalnızca

tüketicie ait “depolama” cihazına kaydedilir ve tüketici sanal para model operatörüyle sanal bağlantıya girdiğinde izlenebilmektedir.

#### 2.4. Sanal Para ve Diğer Ödeme Sistemlerinin Karşılaştırılması

Akıllı katlara dayalı sanal para ürünleri perakende işlemlerde düşük değerli ödemelerin yüz yüze gerçekleştirilmesi için geliştirilmişlerdir. Düşük değerli ödemelerde kredi kartı ve banka kartının kullanımı, her işlem başına kesilen komisyonlar nedeniyle hem maliyetli hem de elverişsizdir. Bu özellik yanında akıllı kartların sunduğu diğer faydalar eklenince, yüz yüze ödemelerde merkez bankası parasının ve kredi kartı ile banka kartının yerine geçme olasılığı vardır. Network para ürünlerinin ise daha çok yüz yüze olmayan, yani online (internet üzerinden) gerçekleştirilen ödemelerde çek, keri ve banka kartlarının kullanımını azaltacağı muhtemeldir.

Değişik özelliklere sahip çeşitli sanal para ürünleri geliştirilmektedir ve bunlar mevcut kullanımda olan kredi kartı, banka kartı gibi diğer ödeme araçlarına göre bankası parasına, yani nakit paraya daha yakın bir ikame olmaktadır. Çünkü sanal para bakiyeleri eş zamanlı olarak iletişim ağları üzerinden transfer edilmektedir. Sanal para ve bazı ödeme araçlarının karşılaştırılması aşağıda verilmiştir.

**Tablo 1.** Sanal Para, Nakit Para, Çek, Banka Kartının Özellikleri.

Özellikleri	Sanal Para	Nakit Para	Çek	Banka Kartı
Kanuni Para	Hayır	Evet	Hayır	Hayır
Kabul Edilebilirlik	?	Yaygın	Sınırlı	Sınırlı
İşlem başına son birim maliyeti	Düşük	Orta	Yüksek	Orta
Yüz yüze işlemlerde nihai ödemenin gerçekleşmesi	Evet	Evet	Hayır	Hayır
Yüz yüze olmayan işlemlerde nihai ödemenin gerçekleşmesi	Evet	Hayır	Hayır	Hayır
Kullanıcının gizliliği	Evet	Evet	Hayır	Hayır

### **2.4.1. Bağımsızlık**

Sanal para herhangi bir fiziksel koşuldan bağımsız mıdır? Sanal para açık ağlar üzerinden transfer edilebilmeli, çeşitli cihazlar üzerinde ve bu ağların içinde ve dışındaki çeşitli yerlerde saklanabilmelidir. Nakit para ise fiziksel şartlarından bağımlıdır. Para, para olmaya devam etmeksizin başka bir araca transfer edilemez. Diğer taraftan para ekonomisi açık bir ağıdır. Buraya her çeşit fiziksel para serbestçe girip çıkabilmektedir (Stalder, 1997:4).

### **2.4.2. Sistem Güvenliği**

Her çeşit ödeme sistemi için sistem güvenliği en önemli koşuldur. Ödeme sistemlerini uygun ve geçerli kılabilmek için sahtekârlığın her çeşidine karşı koruma sağlanmalıdır. Sadece sanal para program yazılımı güvenli olmayacak, aynı zamanda bir işlemin tarafları arasındaki iletişimin arasına da girilmeyecek olması gerekmektedir. Nakit para fiziksel özelliklerine dayalı olarak bu sorunu çözmektedir. Nakit transferi her iki tarafın da karşılıklı bulunması halinde yapıldığında sorun çıkmaktadır.

Çeşitli modellerin altyapıları farklı koruma mekanizmalarını gerektirmektedir. Bir çok sistem kullanıcı onaylama mekanizmasını veya erişim kontrol sistemlerini gerektirmektedir. Buda çoğunlukla gizli kişisel kimlik numarası (PIN-Personel İdentification Number)'nın kullanımı ile yerine getirilmektedir. Bunun dışında akıllı kartlarda kullanılan dijital imzalar da güvenliği sağlamada yararlı olmaktadır.

### **2.4.3. Kişisel Hakların Korunması**

Kişisel hakların korunması teknik olarak mümkündür. Kişisel hakların korunması, sistemin güvenlik özelliklerinde kullanılan şifreleme teknolojisi ile ilişkilidir. Buna rağmen bu ikisi arasında karşılıklı bir bağlantı yoktur. Nakit para ile yapılan işlemler tamamen anonim iken, kredi kartı ile yapılanlar da sınırlı bir anonimite söz konusudur. Çünkü kullanım bilgilerinin tümü Mastercard veya Visa gibi işleme kurumlarının merkezi veri tabanında toplanmaktadır. Ayrıca kredi kartının bağlı olduğu hesabın bulunduğu bankanın veri tabanında da bu bilgiler toplanmaktadır. Tüm sanal para sistemleri tam anonimite ve tam denetim gibi iki uç nokta arasında kişisel hakların korunması alanını belirlemelidir (Aynı, s.4).

#### **2.4.4. İşlem Maliyetleri**

İşlem maliyetleri, bir işlemin gerçekleştirilmesi için gerekli zaman ve genel giderleri, bilgisayar donanım maliyetleri ve diğer mali harcamalar (sahtekârlık ile yol açılan zararlar gibi) olarak tanımlanmaktadır.

İşlem maliyetleri sadece sistem kullanıcısının yaptığı bir alışverişte satış fiyatı üzerinden alınan masraflar ile ilgili değildir. Aynı zamanda bu sistemin kullanıcı açısından ne ölçüde yararlı kullanıma elverişli olduğuna daha büyük bağlıdır (Purche, 1996:80).

Yüksek işlem maliyetleri sistemin düşük miktarlı işlem için kullanımı ekonomik olmaktadır. Bunlar arasında kredi kartlarının EFTPOSVİ ile kullanımı sayılabilir.

İnternet üzerinden online-sanal para sistemleri ise daha düşük işlem maliyetlerini gerektirmektedir. Kuruluş maliyetleri ve iletişim masrafları diğer sistemlere oranla çok düşük kalmaktadır. Bunun yanında akıllı kart kullanımı da kredi kartı gibi otorizasyon gerektirmediği için zaman ve para tasarrufu sağlamaktadır. Ancak akıllı kartların bankalara maliyeti, diğer manyetik şeritli plastik kartlara göre daha maliyetlidir.

#### **2.4.5. Transfer Edilebilirlik**

Dijital ödeme sistemlerinde kişiler arası transferler nakit ile olduğundan çok daha zordur. Çünkü dijital ödeme sistemlerinde işlemin takas edilmesinde bankada işe karışmaktadır. Merkezi otoriteleri işleme karışmadan paranın çok sayıda kullanıcılar arasında el değiştirebileceği, sınırsız transfer edilebilirliğe sahip tam olarak güvenli, bir sistem günümüz şifreleme yöntemleri ile mümkün değildir.

#### **2.4.6. Bölünebilirlik**

Para bölünebilirlik özelliğine sahiptir. Ancak Sanal para bu özelliğe sahip değildir. Çünkü teknik olarak ifade edilecek olunursa, dijital para birimleri birbirine eşittir. Sanal paranın da daha küçük miktarlara bölünebilmesi ve tekrar toplandığında aynı toplamı vermesi gerekmektedir (Daniel, 1996: 101).

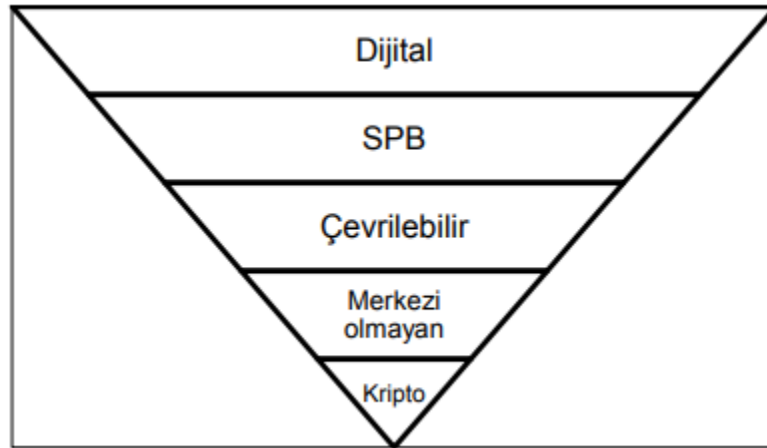


### 2.4.7. Ödemelerin İspat Edilebilirliği

Kredi kartı gibi, yaygın olarak kullanılan elektronik ödeme sistemleri günümüzde yapılan her ödeme için bir kayıt yaratmaktadır. Kredi kartı sistemi kurulduğunda bu, tüm ödemelerin tahkik edilmesini sağlamak için gerekiyordu. Günümüz şifreleme teknolojisi, sistemin güvenlik standartlarını tehlikeye atmadan ödemelerin izlenmesine gerek olmayan ödeme sistemlerinin kurulmasını olanaklı kılmaktadır. Ödemelerin sınırlı anonimitesini sağlayan para benzeri sistemlere örnek olarak akıllı kartlar ve internet üzerinden yapılan Network ödemeleri gösterilebilir.

### 2.5. Sanal Paraya Dayalı Ödeme Sistemleri

Sanal mevduat 3 sınıfa ayrılabilir. Birincisinde kapalı sistem sanal mevduat çeşitleri bulunmaktadır. Bu gruba dahildir dijital mevduatların günlük yaşamla irtibatı yer almamaktadır. Bu kategorideki para yalnızca bir oyun içinde tüketilebilmektedir. Bireyler kayıt yaptırabilmek için bir miktar para ödemesi gerçekleştirerek bir nevi sanal gerçeklik içinde kendi başarımlarına bağlı olarak kazanç elde etmektedirler. Elde edilen sanal mevduat kazancını da yalnızca sanal ürün gruplarının ilgili gruplarında satılıp alınmasında kullanılmaktadır. (European Central Bank, 2012: 13).



**Şekil 1:** Sanal Mevduat Birimlerinin Sınıflandırılması.

**Kaynak:** IMF, 2016.

İkinci kategoride tek taraflı akışa sahip sanal mevduatlar bulunmaktadır. Bu modülde reel mevduat sanal mevduata çevrilmektedir. Söz gelimi fiziki mevduatla sanal mevduat

alınmasıdır. Sanal mevduatların fiziki mevduatlara çevrilmesi imkansızdır. Bu kategorideki bir takım dijital mevduat terimleriyle reel yaşamdaki hizmet ve ürünlerin de satın alınması imkân dâhilindedir (European Central Bank, 2012: 14).

Üçüncü kategoride ise çift taraflı akışa sahip sanal mevduat terimleri yer almaktadır. Sanal para kullanan bireyler ulusal mevduatlarını sanal mevduatlara çevirebilmekte, dilerse de tekrardan sanal mevduat birimlerini reel mevduata çevirebilmektedirler. Bu kategorideki sanal mevduatı aynı reel yaşamdaki yabancı mevduat cinslerine çevrilebilir durumda olup, sanal ve gerçek hizmet ve ürünlerin satın alınması imkân dâhilindedir (European Central Bank, 2012: 28).

## **2.6. Elektronik Ödeme Sistemleri**

Sanal paraların kategorisel bazda sınıflandırılmasından sonra elektronik ödeme yöntemlerinde değinmekte fayda bulunmaktadır. Çok sayıda değişik elektronik ödeme yöntemi bulunmaktadır. Burada en çok kullanılan elektronik ödeme yöntemlerine değinilmiştir.

### **2.6.1. Kredi Kartı**

Elektronik ödeme şekillerinde kredi kartı en fazla kullanılanlardan biridir. Bunda toplum tarafından kullanılmasındaki pratiklik, başka bir donanıma ihtiyaç duyulmamasının etkili olduğu söylenebilir (Sarıakçalı, 2008:106).

Kredi kartında dörtlü bir bağ mevzu bahistir. Bu bağa göre, kredi kartını meydana getiren kart şirketleri; kredi kartını kullanan kişiler; kart kullanan kişiler hizmet yâda mal satanlar ve bankalardır. Tarafların aralarındaki protokoller birbirinden bağımsızdır. Ancak birbirini etki etmektedirler (Şeker, 2011:59).

Kredi kartı ile ödemede internetten ödeme, harcama belgesi veya POS (Point of Sale ya da Point of Service) aleti de kullanılabilir.

Kredi kartı harcamalarında başlıca problem kredi kartının ayrıntılarının çalınmasıdır. Bu kredi kartı güvenliğinin sağlanması için çok sayıda yöntem ve protokol bulunmaktadır (Şeker, M. 2011: 59).

Kredi kartı bilgilerinin başka kişilerce çalınmasının engellenmesi için yararlanılan yöntemlerden biri kredi kartı ayrıntılarının şifrelenmesine varan SET (Secure Electronic Transactions) ve öbürü SSL (SecureSocket Layer)'dir (Keser Berber, 2002: 55).

Müşterilerin kredi kartı detaylarının finans kurumları ya da firmaların İnternet sitelerinden çalınmasının önlenmesi amacıyla bugün“SET Standardım”yerine“3D Güvenlik (3D Secure)”modeli uygulanmaktadır. Mastercard ve Visa tarafından kullanılan 3D Secure, bilgisayar üzerinden yapılan kredi kartı işlemlerinde kart sahibinin kimliğini doğrulaması ile daha fazla güvenlikimkânı vermektedir. **Kaynak:** (<https://www.securepay.com.au/>, (Erişim 10.05.2018).

### **2.6.2. Elektronik Fon Transferi (EFT)**

Elektronik fon transferi kısaca “EFT (Electronic Fund Transfer)”, bir finans kurumu hesabında bulunan mevduatın, elektronik alanda başka bir finans kurumunda yer alan hesaba internet olan herhangi bir sistemle transfer edilmesidir (Şeker, M. 2011: 63).

EFT sisteminin kullanılması ile beraber kâğıda gerek duymayan bir ödeme ortamı oluşturulmuştur. EFT bu manadabir takım gider ve masrafları düşürmekte, etkinliği artırmakta ve daha çok güvenlik imkânı sunmakta olup, bu özellikleri sebebiyle tüketici bazında daha pratik ve kullanışlı bir ödeme yöntemi olarak kendini göstermektedir. (<https://searchwindowserver.techtarget.com/definition/Electronic-Funds-Transfer-EFT>, Erişim 09.05.2018).

Kişinin internet üstünden EFT işlemi yapabilmesi için banka hesabının yer aldığı finans kurumuyla bu hususta bir protokol yapılmış olmalıdır. EFT ile para gönderme talebi bulunan birey sahip olduğu mevduatı karşı tarafa iletilmesi için çalışmış olduğu finans kurumuna otomatik talimat verir ya da bu işlemi kendi internete bağlı cihazıyla yapabilir. (Sözer, 2002: 142).

### **2.6.3. Elektronik Çek**

Elektronik çek, ABD’de “Finansal Hizmetler Teknoloji Konsorsiyumunca“ İmzalı Doküman Biçimleme Dili” olarak isimlendirilen bir anlaşma dili vasıtasıyla oluşturulan ve en az 15 finans kurumunun, merkez bankalarının, teknoloji tedarikçilerinin ve küresel dünyadaki

e ticaret şirketlerinin beraber çalışmasıyla meydana getirilmiş bir ödeme aracıdır (Keser Berber, 2002: 51).

Elektronik çeki “e-çek” olarak isimlendirmekte mümkündür. Elektronik işlemlerin güvenli ve seri özelliklerini içine alarak standart sistemlerin kolaylığıyla birleştirilen bir ödeme metodudur. Elektronik çeklerde, kâğıt çeklerde yer alan bilgiler yoktur. Elektronik çek, her iki tarafa da direkt verilip alınabilir. Elektronik çekler Bankalarda bulunan çek hesaplarının fonksiyonunu fazlalaştırır (Keser Berber, 2002: 52).

Geleneksel olarak elektronik çek, kâğıt çekle aynı mantıkta çalışmaktadır. Kişi çeki düzenler iken elektronik ortamda doldurmakta ve doldurduğu çeki yine elektronik imzayla imzalamaktadır. İmzaladığı çeki, PC ve benzeri diğer bir elektronik vasıtayla elektronik ortamda satıcıya yollamaktadır. Çeki alan alacaklı yine bu ödeme aracını dijital alanda çalıştığı finans kurumuna iletmektedir. Satıcının kendi finans kurumu, ödeme aracını müşterinin finans kurumuyla iletişime geçip, müşterinin hesap bakiyesi ödeme aracını sistemden düşürmeye yeterliyse, satıcının finans kurumuna belirtilen miktarda mevduat aktarımı yapar. Bu işlem neticesinde satıcının banka hesabına gönderilen tutar kadar alacak bakiyesi oluşacaktır (Keser Berber, 2002:53).

#### **2.6.4. Akıllı Kart**

Akıllı kartlar, entegre devre kartı veya çip kart ismi ile debilidir. Kartın üstünde veya içerisinde silikondan yapılmış bir mikroçip yer alır. Kartta bulunan çip içerisinde bir takım datalar muhafaza edilebilir. Akıllı kartlar; Nakliye sektörü, Sağlık sektöründe, iletişim sektöründe, finans sektöründe yâda eğitim sektöründe kullanılmaktadır. Mesela telefonla arama yapmada kullanılan kartlar akıllı kartlara örnek verilebilir. 2018 yılında kullanıma giren yeni nüfus cüzdanları üzerinde bulunan mikroçipler sayesinde nüfus cüzdanları da akıllı kartlara örnek olarak verilebilir. Bu kimlik kartları hastanelerde muayene işlemlerinde, SGK (Sosyal Güvenlik Kurumu) uygulamalarında bankalarda, eczanelerde kısacası hayatın her alanında kullanılabilir.(<http://www.ekds.org/kimlik-karti/t.c.kimlik-karti-ozellikleri.html>, Erişim 14.03.2018).

#### **2.6.5. Elektronik Para**

Elektronik para bölümünde kullanılan veya daha önceden kullanılmış olan elektronik para türlerinden olan. E-Cash, Cyber Cash, Netchash ve Mondex incelenecektir.

### **2.6.5.1. E-Cash**

DigiCash ortaklığı tarafından ortaya çıkarılan E-cash (electronic cash), bir elektronik para uygulamasıdır. Bu uygulama ile birlikte bilgisayar ağlarında güvenilir bir biçimde ödeme işlemleri yerine getirilebilmektedir. Bu yönden ağ tabanlı bir elektronik para sistemidir. E-Cash sisteminin kullanılabilmesi için başka bir ekipmana ihtiyaç duyulmamaktadır(Keser Berber, 2002: 60-61).

E-Cash ön ödeme esasına dayanan bir modüldür. Tacirin mevduatını emin bir biçimde elde etmesini tüketicinin detaylarının muhafaza edilmesine olanak vermektedir. Müşteriler E-cash hesaplarından para alabilme veya para yatırabilme imkânları haricinde hesapta bulunan parayla ödeme yapabilme imkânına da sahiptirler. Bir kişinin E-cash ile işlemde bulunabilmesi için bankada bulunan cari hesaplarından E-cash hesabına havale yapmalarına ihtiyaç vardır. Kişiler İnternet’te E-cash amblemini gördükleri web sitelerinde bulunan satıcılardan alışveriş yapabilirler. Alım-satım sırasında ödeme direkt elektronik mevduat hesabından gerçekleştirilmektedir. Transfer esnasında mevduat alıcının internetinden satıcı kişiye transfer edilir. Havale edilen mevduatlar tacirin bilgisayar ekranlarına klonlanmaz. Tacir mevduatların sadece bir defa işlem gördüğünü finans kurumundan onay almasının akabinde söz konusu miktar satıcının hesabına alacak olarak yazılır. Her işlem bir kullanım olduğunu göstermektedir. Transferin vaktinde kullanılmasıyla değer birimlerinin işlevi son bulmaktadır(Öztürk ve Koç, 2006: 207 ).

### **2.6.5.2. CyberCash**

Cyber Cash internet üzerinden yapılan ve elektronik ticarete kullanılan ödeme sistemlerinden bir tanesidir. Cyber Cash sisteminde ödemenin gerçekleşmesine dair veriler satıcı, alıcı ve banka arasında emin bir şekilde transfer edilir. Bu sistemde değişik şekillerdeki ödeme araçları birlikte kullanılır. Bu ödeme araçlarından bazıları; C5-kredi kartı, Edd, ve Cybercoin ödemeleridir. “Cybercoin”, düşük tutarlardaki ödemeli işlemlerinin yapılabilmesine olanak tanımaktadır. “Edd”, alacak kaydetme temelinde işlem yapmaktadır. “C5-kredi kartı” ise kredi kartlarının İnternet üzerinden kullanılabilmesi amacıyla yapılmış olan bir şifreleme ölçütüdür.(Keser Berber, s.67-69).“CyberCash” işlemleri tamamıyla anonim bir yapıya sahip değildir. İşlemlerin doğru olduğu çevrimiçi biçimde doğrulanır (Weber, 1998: 44).

Müstahakkı evvelinden plase edilmiş “E-cash” türü modüllerden değişik olarak “CyberCash” modülünde alıcı işlem yapılmasının peşinden borç yükümlülüğü taşımaktadır. Mesela, alıcı İnternet üzerinden yaptığı alım-satımları kredi kartı ile yapma isteğinde olursa tacir alıcıya üçüncü taraflara karşı parola ile kilitlenmiş bir belge yollar. Alıcı gönderilmiş olan bu belgeyi bahse konu ürününürün numarasını, karşılığını ve malı satanın çözemeyeceği kredi kartı bilgilerini kayıt eder. Alıcı bu belgeyi elektronik ortamda onaylar. Bahse konu “imza anahtarı” müşteri, tacir ve finans kurumu üçgeninde iletişim birimi vazifesini üstlenen “CyberCash” işletmesince temin edilmektedir. Malı satan, alıcının vermiş olduğu kredi kartı bilgilerini çözmesi amacıyla “CyberCash” işletmesine sunar. “CyberCash işletmesi” de bankanın vereceği yanıt üstüne malı satan kişiye kredi kartıyla yapılacak ödemeyi kabullendiği hususunda onay verir. Akabinde alıcının hesabına borç kaydı yapılır, malı satan kişinin hesabına da alım satıma konu miktar alacak olarak kayıt edilir. Bu işlemde bir miktar anonimlik bulunmaktadır. Nedeni şu ki bu işlemlerde ödeme muamelelerine komisyoncu olan “CyberCash şirketi” ve finansal kurum işlemlerine dâhil olan tarafları ve konu işlemlere ait tutardan bilgi sahibidirler. Malı satan kişinin haberi yalnızca alım-satıma konu mal ve tutarı nasibindedir. Müşterinin kim olduğunu bilmemektedir. “CyberCash şirketi” ve banka ise müşterinin kim olduğunu ve ödenen tutarı hakkında bilgi sahibidir. Fakat alım satıma konu malı bilmemektedir. Müşterinin kimliğinin malı satan nazarında anonimliği sağlanmış olmaktadır. “CyberCash Şirketi” 2001’de batmıştır.

### **2.6.5.3. Netcash**

Bu sisteminde herhangi bir banka kıymet beyanı ve belli bir seri numarası ile elektronik belge formatındaki elektronik kıymet ürünlerini elektronik imzayla piyasaya sürer. Bu kuponlardan elde etmek isteyen müşteri, bankaya belli bir tutarda mevduat yatırmaktadır. Akabinde banka daalıcıya e-mail yoluyla bu kuponlardan yollar. Alışveriş yapmak isteyen müşteri, malı satacak kişiye bu elektronik kuponlardan yollar. Malı satacak kişinin yollamış olduğu kuponları Netcash finans kurumuna yönlendirir. Kuponları alan finans kurumu kuponların üzerinde yazan numaraları kontrol eder ve bahse konu tutarı aktive kayıt eder. Her bir kuponun üzerinde yazılan numara bir defa kullanılabilir. Finans kurumları müşterilerin bilgi ve ödeme işlemlerine dair ayrıntıları saklamaktadır. Bu itibarla Netcash sistemi anonim bir yapıya sahip değildir (Öztürk ve Koç, 2006: 226.).

#### 2.6.5.4. Mondex

Mondex adı ile tanınan E-cash İnternet'e gereksinim duyulmadan kullanılan biçimidir. Mondex sistemi İngiltere'de yer alan "National Westminster Bank" şirketince 1990'da güncelleştirilmiş ve sonrasında ise "Mastercard International" firmasına devredilmiştir. Mondex modülükâğıt ve metal paraya alternatif bir sistemdir. Elektronik mevduat, Sanal Para, Btc ve Linden Doları'na ait Hukuki Bir Bakış bir elektronik mevduat kartı olarak ifade edilmektedir. Modex sistemini kullanan kişilere içerisine para yüklemesi yapılabilen ve üstünde elektronik çip bulunan elektronik kart verilmektedir. Öte yandan bu kişilere para yükleme işlemini gerçekleştirebilecekleri cüzdan ismi verilen bir elektronik bir cihazda verilmektedir. İşletiminde düşük meblağlardaki ödemeler genellikle nakit parayla yerine getirilmektedir. Eğer debit yada kredi kartıyla ödemede bulunulacaksa paranın bir mali kuruluştan istenmesi gerekecektir. Mondex cüzdana sırf kendisinden başka, herhangi bir onaylama işlemine ihtiyacı olmadan veri depolayabilme olanağı sunmaktadır. Mondex'de depolanan veriler kartın üstünde bulunan mikroçipte yer alır. Alıcı satış yerindeki cihazda bu kartını kullanarak transfer ettiğinde söz konusu tutarelektronik şekilde karttaki çiptenindirilir ve satıcı firmanın çipi üzerine eklenir. Söz konusu bu işlemler alıcının finans kurumu cüzdanına girmeden gerçekleştirilir. Mondex'in en önemli avantajı, minimum tutarlardaki transferler için de faydalanılabilesidir. Karta kıymet yüklenmesi ATM cihazlarından ya da mobil kanallar ile gerçekleştirilebilir. Bir karttan diğer bir karta şifre korumalı elektronik cüzdan sayesinde kıymet aktarımı gerçekleştirilebilir. Elektronik bir anahtar kartı sahibi olan kişilerin hesaplarını denetim altında tutmalarını sağlar. Kaybedilmesi veya çalınması durumunda kart sahibinin fiziki mevduatını da kaybetmesine sebep olmaktadır. Bu durumla beraber Mondex kart sahiplerini kollamak için 4 basamaklı bir şifreyle değeri kartta gizleyebilme olanağı vermektedir. Şifre hatalı girildiğinde kart kilitlenecektir. Mondex kartın detayları aşağıdaki gibidir;

- Çevrim dışı bir transfer sistemidir,
- Kullanan kişilere işlemlerin anonim olmasına olanak verir,
- Çip kart biçiminde bir elektronik cüzdandır,
- Küçüktutarlardaki ödeme işlemlerinin gerçekleştirilmesini sağlar,
- İşlem masrafları düşüktür, satış yapan kişinin kullananın banka bilgilerine erişebilmesini olanak sunmaz ve kullanılabilmesi için başka bir cihaz gerekir (Öztürk ve Koç, 2006: 227)

## ÜÇÜNCÜ BÖLÜM

### BİTCOİN'E GENEL BAKIŞ

Bitcoin, dijital para ekonomik yapısını meydana getiren konuların ve kavramların tamamıdır. Açık kaynak koduna sahip uygulamalardan meydana gelir. Programlar laptoplar ve android telefonlar dâhil büyük ölçekteki işlemcilerde çalışmaktadırlar (Andreas M. Antonopoulos, 2014). Bitcoin sistemi tümüyle dijital olup, fiziksel temsiline gerek duyulmamaktadır (Katherine Sagona-Stophel). İşlem masraflarının çok düşük olması, küresel olarak kullanılabilmesi, zamanla kullanılma sahasının fazlalaşması, güvenilir ve anonim şekilde veri muhafaza etme vasıtası olması Btc' yi çok daha tanınmış kılmaktadır (A Wiley Brand, 2016).

Bitcoin İlk kripto paradır. Btc, 2008 Kasım ayının ilk günü Japon yazılım firmalarından birinde çalışan S.Nakamoto' nun yoğun çalışmaları neticesinde meydana gelmiştir. Bu sanal paranın dünya kamuoyuna tanıtılması S.Nakamoto' nun imzasının yer aldığı "Bitcoin: A Peer To Peer Electronic Cash System" (kişiden kişiye dijital nakit gönderim modülü) adlı küçük bir makalesiyle gerçekleştirilmiştir. (Nakamoto 2008, s.1).

Bitcoinler, "BTC" kısaltmasıyla kullanılmakta olup, simgesi Şekil 2'.'de görüleceği üzere B harfinin üst ve alt kısmından inen 2 çizgiden oluşmaktadır. Kripto paralar yerel mevduatlar gibi gruplandırılabilir. Yerel mevduatlar, karşılığında kıymetli madenler bulunmayan ancak emtia veya hizmet ile değişim yapılabilen maddi değer ölçüsünü ifade eden varlıklardır. Yerel mevduat değerlerinin belirlenmesi, yasalardan veya onu benimseyen kurumlardan aldığı belirtilmektedir. (Velde 2013, s.2). Bitcoin' in yerel mevduatlardan farklılık gösterdiği tarafıysa herhangi bir merkezi otoriteye bağlı olmaması ve denetimden uzak olması söylenebilir.



Şekil 2: Bitcoin'in Logosu

**Kaynak:**<https://www.bitcoin.org>, Erişim tarihi:30 Nisan 2018

Maddesel olarak gümüş, bronz ve altın olarak Bitcoin'ler de imal edilmiştir.  
**Kaynak:**[https://en.Bitcoin.it/wiki/Casascius\\_physical\\_Bitcoins](https://en.Bitcoin.it/wiki/Casascius_physical_Bitcoins),ErişimTarihi:30.Nisan.2018).



Fiziki Bitcoin'lerin arka yüzünde, bir gizli anahtar ve Bitcoin cüzdan adresi hologram biçiminde yer almaktadır (Şekil 4.5.). Gizli anahtarı olmayan, Btc' nin sanallaştırılması olanaksızdır. Gizli anahtarı görebilmek içinse madeni BTC' nin üzerindeki hologramın kırılması gereklidir. Diğer bir ifadeyle, madeni BTC' nin kişiden kişiye çok sayıda dolaşabilir fakat dijitalleşmesi istenirse tek kullanımlıktır. Çoğunlukla para koleksiyoncularının meyilli fiziksel bitcoin'ler üzerindedir. Yüz yüze yapılan işlemlerde kullanılmak üzere tasarlanmışlardır.

**Kaynak:** ([https://en.Bitcoin.it/wiki/Casascius\\_physical\\_Bitcoins](https://en.Bitcoin.it/wiki/Casascius_physical_Bitcoins), Erişim Tarihi: 30.04.2018).



**Şekil 3:** Fiziki Bitcoin Örnekleri

### 3.1. Bitcoin'nin Tarihçesi

Bitcoin'nin Tarihsel sürecini Global çaptaki gelişiminin ve ülkemizdeki serüvenini daha net anlayabilmek adına, Dünyada ve Türkiye'de Bitcoin'nin tarihsel süreci olarak iki bölümde incelemekte fayda bulunmaktadır

#### 3.1.1. Dünyada Bitcoin'nin Tarihsel Süreci

Bitcoin'in tarihi 2008 yılındaki küresel finansal krizle başlar. 2008 yılında uluslararası bu finansal krizde dünya ülkeleri 24 Ekim 1929 da kara Perşembe olarak başlayan ve 1930' lu yıllarda etkisini en yüksek seviyede gösteren Büyük Dünya Burhan'ını bir daha hatırlamamak amacıyla merkez bankalarında, para basıp, faiz oranlarını azaltma yolunu tercih etmişlerdir.

Batmanın eşine gelen birçok banka, bu durumdan kurtarılmış, fakat bu kurtarılmışın karşılığı, mevduatlarda yaşanan değerlerin düşmesi ve vergilerin yükselmesi şeklinde topluma yansımıştır. (A Wiley Brand, 2016: 208).

Merkezi bir yapısı bulunmayan Btc, tam da aracılık yapan kuruluşlara, merkez bankasına, diğer bankalara ve hatta ülkelerin idaresinde olan iktidarlara inancı eksildiği bir zamanda doğmuştur. Btc, S. Nakamoto kullanıcı adıyla, 2008’ de yayımlanan “Bitcoin: Uçtan Uca Elektronik Ödeme Sistemi” adlı çalışmasıyla herkese ilan edilmiştir (Satoshi Nakamoto, Mayıs 2009).

Nakamoto' nun ortaya attığı değişim, dağıtık sistem güçlerinden yararlanılarak transfer işlemlerini on dakika içerisinde doğrulayan bir sistemle, mükerrer tüketimi önlemiş olmaktadır.

Satoshi Nakamoto, kuşku ve potansiyel bir şekilde sahte, dağıtık bir işlemci modülünde, veri dağılımının ne şekilde gerçekleşeceği sorunu olarak algılanan "Bizans Generalleri" meselesine, merkezi bir güç olmadan, “iş ispatı” tanımıyla yeni bir çare öngörmüştür. Satoshi Nakamoto' dan 2011 yılı 4. ayından itibaren haber alınmamasına karşın, düzen tümüyle saydam ve matematik kuralları sınırlarında işlemeye devam etmiştir (Andreas M. Antonopoulos, 2014: 330 ).

2009 yılında faaliyete geçen Bitcoin sisteminin şimdiki toplam işlemci gücü, dünyanın en hızlı bilgisayarlarının gücünden daha yüksektir. 04.12.2017 Pazartesi, saat 12:01 itibarıyla, Btc' nin toplam piyasa hacmi yaklaşık 200 milyar USD’ dir (Bloomberght.com, Btc' nin Pazar hacmi Buffett ve Gates'in toplam servetinin kat kat üstünde olduğu söylenmektedir. **Kaynak:**<http://www.bloomberght.com/haberler/haber/2075385-bitcoin-un-piyasa-degeri-buffett-ve-gates-in-toplam-servetinin-uzerinde>).

Bu zamana değin gönderilen en fazla tutar 194.994 Bitcoindir (yaklaşık 147 Milyon USD). Söz konusu transfer 2013 Kasım ayında herhangi bir komisyon talep edilmeden yapılmıştır.

### **3.1.2. Türkiye’de Bitcoin’in Tarihsel Süreci**

Türkiye’de Bitcoin’in tarihsel süreci; Bankacılık Düzenleme ve Denetleme Kurumu’nun 2013 yılı Kasım ayının yirmi beşinde Bitcoin’le ilgili bir açıklama ile başlamaktadır (Şekil 1’). İzah namede, dijital mevduat olan Btc' nin, 6493 sayılı “Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun” çerçevesinde bulunmadığını ve dijital para şeklinde değerlendirilmediği için gözetim ve kontrolünün olanaksız olduğu ifade edilmiştir.

Diđer taraftan, Btc modülünde gerçek kişisel bilgilerin bilinmiyor olması nedeni ile Bitcoin'in illegal işlerde kullanılabileceđi, deđerinin aşırı deđişken olması, dijital cüzdanların başkaları tarafından ele geçirilebilir olması, kaybedilebilmesi, amacına uygun kullanılmaması ve yapılan işlemlerin iptalinin olmaması gibi riskleri beraberinde getirdiđi de özellikle belirtilmiştir.

Btc' ye vergi uygulanması hakkındaki görüşler, bütün dünya ülkelerinde olduđu gibi, ülkemizde de halen sürmektedir. Belli bir merkeze bađlı bulunmaması nedeniyle yalnızca ülkemizi kapsayacak bir vergilendirme biriminin imkan dahilinde olmayacağını savunanlar olduđu gibi, Btc' nin kanuni durumunu tespit ettikten sonra vergilendirmenin konuşulabileceđini savunanlar da bulunmaktadır (Türkiye'de Bitcoin ve Vergi, Erişim Tarihi: 30.04.2018).



**BASIN AÇIKLAMASI**

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

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

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

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

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

Kamuoyuna saygıyla duyurulur.

**Şekil 4: BDDK'nın Bitcoin'le İlgili Basın Açıklaması.**

**Kaynak:**([https://www.bddk.org.tr/websitesi/turkce/duyurular/Basin\\_Aciklamalari/12574bitcoin\\_hk\\_basin\\_aciklamasi.pdf](https://www.bddk.org.tr/websitesi/turkce/duyurular/Basin_Aciklamalari/12574bitcoin_hk_basin_aciklamasi.pdf))

### 3.2. Bitcoin İle Geleneksel Para Sistemi Arasındaki Farklılıklar

Btc' nin yerel paradan, finansal yapı ve işlemlerin gerçekleştirilmesi bakımından farklılıkları (Brand, 2016);

1. Btc ağında, ne bir yönetici, aracı ne de kontrol edici bulunmamaktadır. Bitcoin ağında, uçtan uca birbirine endeksli, gönüllü iştirakte bulunan bilgisayarlardan meydana gelir. Bağlı bütün bilgisayarlar, açık kaynak kodlu, aynı programı çalıştırırlar, Tümü yapılan işlemlerin tamamını görür, herkes tüm işlem geçmişini dilerse saklayabilir ve diledikleri zaman diğer uçlardan işlem geçmişlerini alabilirler. Özetle Bitcoin ağı merkezi bir yapıya sahip değildir.
2. Dijital itibari paraların muamelelerinde, güvenilir üçüncü bir taraf olması gerekirken, Bitcoin sisteminde üçüncü bir tarafa ve güvenceye gerek bulunmamaktadır. Aracılık sisteminde maliyetler bir hayli fazla ve güvenlik açıklarının yaşanması da ihtimal dâhilindedir.
3. Bitcoin'in en önemli özelliklerinden biri borç değil, değer taşıyıcı olmasıdır. Bankaların hesaplarında bulunan paralar, bir çeşit borç bonosudur. Bankadaki bir hesap, müşterisine olan borcunu gösterir. Bitcoin de ise bir borcu göstermez. Bankalardaki ve ülke yönetimindeki idarelerin, banka hesapları üstündeki denetim iradeleri, Bitcoin de söz konusu değildir. Dünyada hiçbir otorite Bitcoin'in kullanılmasını önleyemez, meydana gelmiş bir Bitcoin işlemini geri alamaz.
4. Ülkeler para arzıyla ve sınırlamasıyla bankada bulunan paranın değeri üzerinde etkide bulunabilecek ekonomik tedbirler alabilirler. Hâlbuki Bitcoin arzı üzerinde banka ve devletlerin herhangi bir tesiri bulunmamaktadır. Sisteme harice para ilavesinde bulunulamaz. Para arzı, başarılı blok meydana getirebilen üreticilere sağlanan mükâfatlar biçimindedir.
5. İşlemler anonimdir, kullanıcı adlarıyla gerçekleştirilir. İşlemlerin gerçek bireylerle, firmalarla, finans kurumlarındaki hesaplar ile ilişkisi bulunmamaktadır. İşlemler Btc hesapları arasında meydana gelir. Btc hesapları kripto işaretlerdir. Söz konusu koşullara karşın, yüzde yüz anonimdir denilemez.
6. Transferler saydam, süratli ve uluslararası çaptadır. 2009' daki ilk Btc üretiminden bu zamana, bütün işlemler, talep eden herkesçe izlenebilir. Söz konusu transferler, hemen hemen o anda bütün dünyadaki kripto para sistemine yayılır, çok kısa zaman zarfında tasdiklenir.

7. Yerel mevduatlarda transfer işlemlerinin belleği bulunmamaktadır. Btc işlem belleği ise küresel hesap defteri olan Blockchain veri tabanlarına kaydedilir. Btc kullanımı yapacak birinin, Btc sahibi olup olmadığı, daha evvelki kayıtları izlenerek tespit edilir.
8. Bitcoin sisteminde herhangi bir güç, idare, şahıs, bilgi sistemleri uzmanı, yada bu sistemin programlayanlar da dahil, madencilerden herhangi bir tanesince onaylanıp, öbürleri tarafından da kabullenilmiş ve Blok-Zincir'e eklenmiş, bir işlem üzerinde değişiklik yapamaz ve geri almaya yönelik bir işlem yapamaz.
9. Bitcoin'de işlem yapabilmek için önceden herhangi bir kurum ya da şahıstan izin alma mecburiyeti yada herhangi bir kuruluşun yada kimsenin engel olma durumu yoktur.
10. Sistem güvenilirdir. Sistemin güvenliği matematiksel olarak güvenilirliği kanıtlanmış, kriptografik dijital imzalama yöntemlerinden yararlanılarak sağlanır. Art niyetli kişilerin veriler üstünde sahte yönlendirmede bulunması, açık/gizli anahtar şifreleme yöntemi kullanılması nedeniyle, olanaksızdır.

### **3.3. Bitcoin Kullanmanın Avantajları ve Dikkat Edilmesi Gereken Noktalar**

Kripto paraların kullanılma alanları gün geçtikçe çoğalmaktadır. Bilhassa üçüncü şahısların transferlere karışmaması ve yapısındaki gizlilik esası sayesinde ekosistemi büyümektedir.

Bitcoin elde edebilmek için önceki bölümlerde dedeğinilen ve açık kaynak kodlu cüzdan olarak isimlendirilen uygulamanın bilgisayarda kurulu olmasına ihtiyaç olmaktadır. Bu sanal cüzdanla kullanıcılar öncelikle blockchain alt yapısına sahip veri tabanı sistemine bağlantı kurmaktadır. Bu kademenin peşine, çift taraflı modülzeminde gerçek ekonomi ile ilişkili biçimde Btc işlemlerine başlanabilmektedir. Btc transferlerine veya alım satım faaliyetlerine start vermek için ilk önce Bitcoin edinilmiş olunmalıdır. Bitcoinler değişik yöntemlerle sağlanabilir. Bu yöntemlerden birincisi, küresel çapta var olan Bitcoin piyasalarından belli kur oranları ve aracılık komisyonu mukabilinde Bitcoin temin edilmesidir. Bu piyasalara Coinbase, BTCTurk, Coinhouse, Binance, OKEEx, Bittrex, Bitmex örnekleri verilebilmektedir. Bu türdeki web sitelerinde alım ve satım ücretleri bulunmaktadır. Komisyon miktarları birbirleri arasında değişiklik taşımakla beraber 2017 yılı Mart ayında en çok % 0.5 dolaylarındadır. Bir başka "BTC" sağlama metodu da madencilik yapılması yöntemidir. Bu metotta ise, bilgisayarların işlemcilerinden faydalanılarak algoritmalarından

oluşan yapıları çözümlenerek karşılığında mükâfat olarak BTC almak veya transfer işlemlerini doğrulamak yoluyla yapılmaktadır.

Kazanılan hizmet veya mal alımı için parasal değer olarak kullanılabilir. Bitcoin bilhassa Amerika Birleşik Devletlerinde geniş olanaklara sahip olduğu bilinmektedir. Avrupa ülkelerinde ise her geçen zaman kullanıldığı yerler ve kullanım oranları çoğalmaktadır. Btc temin etme yöntemi Btc satışı yapan borsalara mevduat göndererek yapılır. Madencilik işlemi yapan kişilerin transfer işlemlerini doğrulama yani mutabakatı sağlama işlemi ortalama on dakika içerisinde yapılmaktadır.

Bitcoin'in halk tarafından tutulması gün be gün artmaktadır. Bitcoin, piyasaya sürüldüğünden bu yana yapılan işlemlerin toplam hacmi 6 trilyon Amerikan Doları'nı aştığı ve 2018 yılında 10 milyar dolar günlük işlem hacmi olan bir piyasa haline geldiği görülmektedir.

Josiah Hernandez, istatistik veriler ve yayımlanan araştırmalar baz alındığında fiyat düşüşüne karşın, Bitcoin'in halkça tutulması aşikâre bir biçimde fazlaştığını belirtmektedir.

Btc' yle pratik bir transfer modülü oluşturulmaya uğraşmaktadır. Mesela, Btc, mobil araçlar ile yapılacak mobil transferlerin de kolaylıkla yapılmasına imkân tanımaktadır.

Bitcoin'de herhangi bir kart okutma işlemine, İmza atmaya, şifre girmeye lüzum olmadan transfer gerçekleştirilebilmektedir. Btc'yle gerçekleştirilecek transferleri kabul edebilmek için tek lazım olan Btckripto cüzdan programındaki şifreyi telefonun ekranına getirmek ve transfer etmek isteyen müşterinin bu şifreyi okutmasına imkan tanımaktır. NFC radyo teknolojisi ile iki telefonu birbirine temas ettirerek de bu transfer gerçekleştirilebilmektedir. Herhangi biri başkası namına mevduatını harcayamaz veya mevduatı götüremez. Şayet sanal para kripto cüzdanını muhafaza etmek için zorunlu kurallara uyulduğu takdirde dolandırıcılığa karşı güçlü bir kalkan sağlanmış olacaktır. Btc müşterilerinin cüzdanlarını muhafaza etmeleri için uyulması icap eden kurallar söz konusu borsanın web sayfasında belirtilmektedir.

**Kaynak:** Some things you need to know, <https://bitcoin.org/en/you-need-to-know>, Erişim Tarihi: 01.05.2018).

Kripto paraya istenilen yer ve zamanda başvurulabilir. Bu konuda zaman, mekan kısıtlaması bulunmamaktadır. Yeryüzünün herhangi bir alanından, yeryüzünün başka bir alanına Btc gönderilip alınabilir. Söz konusu transfer işlemlerine finans kurumlarının aracılık etmesine, işlem komisyonu verilmesine gerek bulunmamaktadır. Bazı durumlarda ödeme yapılması gereken ufak miktarlar haricinde Btc ile para gönderiminde ya da almada herhangi

bir komisyon alınmayacağına dikkat çekilmiştir. Bu durum yapılacak olan işleminize öncelik verilmesi ve hızlı bir şekilde gerçekleştirilmesini istediğinizde söz konusu olacaktır. (Bitcoin for Individuals, <https://bitcoin.org/en/bitcoin-for-individuals>, Erişim Tarihi: 01.05.2018 ).

Bitcoin'le transferdefiziki mevduatta olduğu gibi anonim kalınması olanak dahilindedir. Ancak gizlilik ilkesi gereği izlenmesi gereken kurallara riayet etmek gerekir. Bununla beraber btlerin tümü anonim olarak nitelendirilmez Dijital para aktarımlarının tamamına yakını açık bir şekilde yapılmakta olup söz konusu aktarımlar sistem içerisinde daima yer edinmektedir. Bu şekilde talep eden kişi herhangi bir sanal para cüzdanına ilişkin sanal para aktarım işleminin ne kadar olduğunu izleyebilecektir. Fakat o cüzdanın mülkiyetini elinde bulunduran kişinin kimlik bilgileri gizlenmiştir. Bu sebeple bir btc cüzdanının bir kez kullanılması tavsiye edilmektedir. Btc sahiplerinin gizlilik ilkesi gereği transferlerini muhafaza edebilmeleri amacıyla transfer ve takas yapılan site ve piyasalarda izlenilmesi gereken prosedürleribelirlenmiştir. (Bitcoin for Individuals, <https://bitcoin.org/en/bitcoin-for-individuals>, Erişim Tarihi: 01.05.2018).

Bitcoin ile gerçekleştirilen aktarım işlerinde transferin geri çağrılması imkândâhilinde değildir. Yalnızca ödeme yapılan şahısalnız fazla aldığı miktarı geri iade edebilir. Bu sebeple yalnızca güvenilen ve belli bir şahıs ile Btc alışveriş işleminin gerçekleştirilmesi tavsiye edilmektedir. Btc yazım hatalarını fark edebilen bir modeldir. Ekseriyetle bilmeden yanlış kaydedilmiş bir cüzdan hesabına nakit transferini model onaylamayacaktır.(Some things you need to know, <https://bitcoin.org/en/you-need-to-know>, Erişim Tarihi: 01.05.2018).

- Her zaman her yerde gönderilebilir.
- Kullanan kişi anonim kalabilir.
- Enflasyon yoktur.
- Ekonomik istikrarsızlıklardan etkilenmez.
- Eşitler arası işlemlere imkân verdiğiinden bankalar veya merkezi otoriteler işleme dâhil değildir.

#### **Bitcoin Kullanımının Dikkat Edilmesi Gereken Hususlar:**

- Ekonomik suçların işlenmesinde suçlular nezdinde kullanılabilir.
- Örneğin İnternet'te alınan bir malın ücretinin Bitcoin ile ödenmesi ancak malın hiç teslim edilmemesi durumunda para geriye alınamamaktadır. Ödemenin kaydı olmadığından işlem anonim kalmaktadır. Ödeme işleminin izinin sürülmesi zordur.



- Bilgisayara virüs bulaşırsa ya da bilgisayar fiziksel zarar görürse Bitcoinler kaybedilebilir (Er, 2006: 66).

### 3.4. Btc İle Alakalı Mali ve Teknik Eleştiriler

Btc sistemi deflasyonist bir yapıya sahip olduğu için eleştiri almaktadır. Lakin enflasyon bulunmamaktadır. Bitcoin üretimi yirmi bir milyon ile sınırlı olup ilgili miktara varıncaya dek matematiksel şekilde çoğalması öngörülmektedir. Btc sahiplerinin artarak fazlaşmasına rağmen mevduatın transfer ivmesi buna paralel şekilde yükselmemesinden dolayı Btc ile değeri oluşmuş emtia değerinin düşmesi beklenecektir. Bu durum bireylerin ellerinde tuttukları coinleri satmayıp bekletmelerine neden olacak bu da deflasyon etkisinin fazlaşmasını özendirecektir. (European Central Bank, 2012: 25).

Btc' nin hâlen yeteri kadar bireyin kullanmaması ve Btc kullanan işletmelerin sanal paradan ayrı olarak diğer paraları da (₺-\$-€) kullanmalarından dolayı deflasyonist beklentiyi gerçek olarak görmeyen düşüncelerin oluşmasına neden olmuştur.

Dijital para modeli olası virüs ataklarına karşı direnç gösteremeyeceğinden dolayı da eleştiri almaktadır. 2011 senesinde dijital hackerlarca dijital para modelini hedef alan bir virüs saldırısı gerçekleştirilmiş ve bunun sonucunda Btc' nin o günkü kurlarıyla oynanmış olup 17.55USD olan kur, 0.011USD' ye düşürülmüştür. Diğer taraftan hackerlar Mt.Goxadlı Btc borsasının veritabanına sızarak müşterilerinin cüzdan hesaplarına, ad-soyadlarına, şifreleme sistemlerindeki bilgilere de erişmişlerdir. Bu sebepten dolayı ilgili borsanın veritabanı modülü 3-4 gün devre dışı kalmıştır. Btc' nin güvenilir olduğunu düşünenler söz konusu saldırıda problemin Mt.Gox'un yeteri kadar güvenlik tedbiri almamasından kaynaklandığını öne sürmüşlerdir. (European Central Bank, 2012: 26).

2012 senesinde diğer bir Btc borsası olarak ifade edilen Bitcoinica'ya düzenlenen virüs saldırısında ilgili borsada işlem yapanların kimlik ve hesap dokümanlarının çalındığı düşünülmektedir.

Bitcoin ile alakalı bir başka tenkit mevzusu ise reel para birimlerinin Bitcoin'e dönüştürülmesi fakat Bitcoin'in yeniden reel para birimlerine dönüştürülmesinin ise yalnızca Bitcoin elde etmek isteyen biri olduğunda olabilmesidir.

Söz gelimi btc satın alınması sebebiyle sisteme ilk defa dahil olmak isteyen bireyler olduğunda sahip olduğumuz Btc'yi reel para birimine dönüştürmek imkan dahilinde düşünülebilir. Btc ek getirisi olan bir yatırım argümanı şeklinde değil bir dönüşüm argümanı şeklinde herhangi bir noktaya ilişkisi bulunmadan faaliyet gösteren bir modül olmakla

beraber modülün kendisi sisteme yeni dahil olan bireyler için epeyce kompleks ve kavranması güçtür. Diğer taraftan modülden tümüyle ayrılmak istenildiğinde nakit noksanlığı sebebiyle gerçekleşemeyebilecektir. Tüm bu gelişmeler Btc'nin kanuni konumunu, güvenilirliği konusunda yaşanan belirsizlikleri ve illegal maksatlar sebebiyle kullanılabilme olasılığıyla alakalı kaygıları gün yüzüne getirmektedir.

Btc'nin kur oranları seri şekilde farklılaşmaktadır. Btc'de artış ve azalışların maksimum seviyede olması evvelden öngörülemez, süratli bir biçimde fiyatının yükselip / düşmesine sebep olacağından müşterilere tüm tasarruflarını Btc şeklinde değerlendirmemeleri tavsiye edilmektedir. Bu hususta btc' nin aşırı risk taşıyan bir varlık olduğu, kaybedilmesi durumunda söz konusu kayba tahammül edilebilecek derecede mevduatın Btc şeklinde muhafaza edilmesi gerektiği vurgulanmaktadır. Bunun yanında müşterilerin alış verişi yaptıkları Btc borsalarında, btc sahiplerinin ellerinde bulundurdukları mevduatı kendi yerel para birimlerine endeksli bir şekilde tutmalarının taşıdıkları kur değişim riskinin minimize edeceği ifade edilmektedir.

Btcyle alakalı sunulan düşüncede değinilen diğer bir eleştiri, ülkelerin merkez bankalarının piyasaya nakit sürme hususundaki tekelinin sona erdirilmesi konusunda Btc'nin bir başlangıç oluşturacağı düşünülmektedir. (Rumellili, 2006).

Bitcoin için eleştiri ve takdirin en fazla yapıldığı nokta, anonim bir biçimde yapılan Bitcoin nakilleridir. Bitcoin ekosistemin illegal alışverişler (esrar, eroin...vb.) için rahat bir şekilde kullanılması bir tenkit unsurudur. SilkRoad adlı dijital bir piyasa, müşterilerine menedilmiş ürünleri dijital para karşılığında temin etme olanağı sağlamakta olup; sonrasında söz konusu ürün posta ile alıcıya kargo edilmektedir. Aynı biçimde çok sayıda online bahis siteleri Btc ile işlem yapabilmektedir. Öte taraftan anonim alışverişler dijital para modülünün reel paraya en çok benzetildiği durum olarak görünmektedir. Btc (ya da başarılı görünen her tür dijital mevduat) elektronik mevduat şeklinde ifade edilir. Anonim aktarımlar vasıtasıyla, etik olan fakat herhangi bir sebeple bazı devletlerce engellenen işlemleri de uygulamak olasılık dahilindedir. Örnek olarak, Visa veya Mastercardla WikiLeaks'e bağışta bulunulamamasına rağmen, dijital para ile yardım yapılabilir.

Gelecekte finans sistemin Bitcoin ekosisteminin yayılmasına engel olacağını düşünebilir, fakat bu durumun tam zıttı da ihtimal dâhilindedir. Finansal sistem, iktidarlar üstündeki gücünden yararlanarak bitcoin kullanımına mani olmak çabasının içerisinde olabilirler, böyle bir çabanın her iki tarafa da olumsuz neticelerinin olabileceği tahmini zor bir konu değildir. Bu sebeple finansal sistemin bitcoin teknolojisine ve bitcoine savaş açma yerine bundan yararlanmayı düşünmesi her iki taraf içinde daha sağlıklı olacaktır.

### 3.5. Bitcoin'in Çalışma Mekanizmasının Özellikleri

Bitcoin çalışma mekanizmasının özellikleri aşağıdaki şekildedir.

- Bitcoin kullanabilmek için bilgisayara ücretsiz indirmek gerekir.
- Sahip olunan Bitcoinler bilgisayardaki dijital cüzdanda saklanır.
- Bir Bitcoin dijital imza zincirinden oluşmaktadır.
- Klonlanması imkânsızdır.
- Çifte harcama için kullanılması olarak dâhilinde değildir.
- Bitcoin ile gerçekleştirilen transfer işlemlerinde yapılan işlemin alınması olarak dâhilinde değildir.



## DÖRDÜNCÜ BÖLÜM

### BİTCOİN VE DİĞER PARA BİRİMLERİ ÇALIŞMA MEKANİZMASI VE TEKNOLOJİK ALTYAPISI

#### 4.1. Teknolojik Arka Plan

Bu bölümde Bitcoin'nin teknoloji alt yapısı detaylı bir şekilde incelenecektir.

##### 4.1.1. Kriptolojik Özet Fonksiyonları (Hash Function)

Özet fonksiyonlar, değişik boyutlardaki sayısal iletilerden, belli ölçekte bir ileti özeti oluşturması anlamına gelmektedir. Özet fonksiyonu süratli çalışması, değişik girdinin değişik çıktısının olması (çarpışmaya dayanma), özet iletiden hareketle özetlenen mesajla ilgili muhtelif bilgiler ortaya çıkarılmalıdır. Özet iletileri analiz ettiğimizde gelişmiş güzel ortaya çıkmış izlenimi vermektedir.



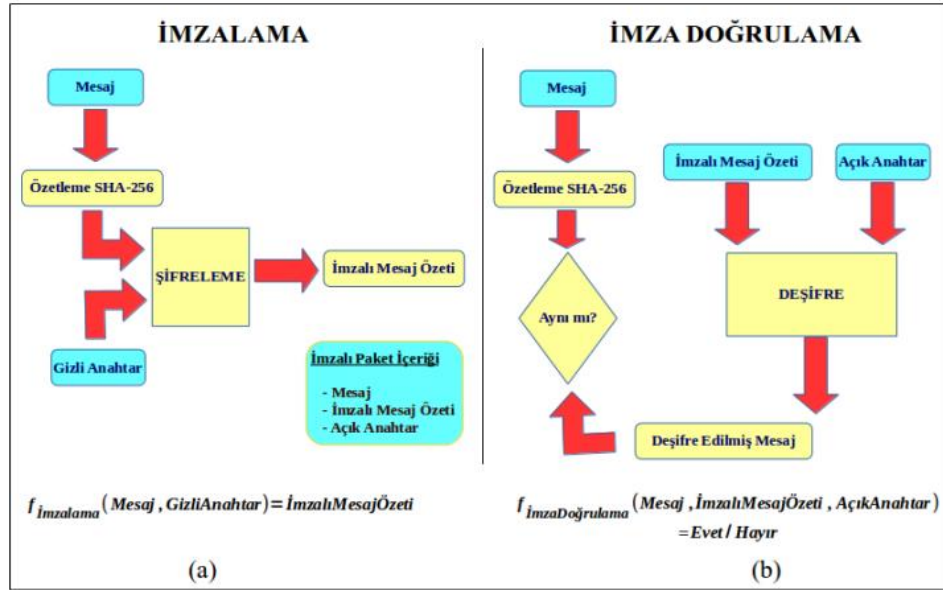
Şekil 5: Sha-256 Özet Fonksiyonu Örneği

Btc transferlerinde "SHA – 256" adı verilen özet fonksiyondan faydalanılır. "SHA – 256", girişi yapılan iletinin boyutundan serbest, 256-bit (32 byte) ileti özeti meydana getirir. Kripto grafik şekilde en sağlam özetleme fonksiyonlarından biridir. Diğer bir ifadeyle ileti özetine bakılarak iletinin ne olması gerektiği hakkında yargıya varılamaz. "SHA – 256" 'da, hangi ileti girdisi olursa olsun, ileti özeti 256 adet peş peşe, 1yâda 0'dan meydana gelen bir seridir. Okunmasında pratiklik olması için çoğunlukla, dörtlü kümeler biçiminde 16'lık düzenle kaydedilirler. Bu hususta, mesaj iletilerinin özetleri artarda 64 tane "0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F" harfin kullanılmasıyla oluşturulurlar. Kurgusal olarak, 256

tane peş peşe a 1 yâda0 ile " $2^{256} \approx 1.15 * 10^{77}$ " değişik özete ulaşılabilir. Bu, devasa boyutta bir sayıdır (Columba, 2008: 317).

#### 4.1.2. Sanal İmza

Sanal imza, açık (public) ve gizli (private) kilit ikilemesiyle işleyen, istatistiksel şekilde doğruluğu kanıtlanmış kodlama metodudur. Sanal imza kullanma talebinde bulunan müşterilerin kendine özgü, gizli ve açık bir güvenlik anahtarı olması icap eder. Gizli anahtar ile kodlanan bir ileti, yalnızca kodlanana ait açık anahtar ile açılabilir. Gizli anahtar, yalnızca gizli imzayı kullananda olmalıdır ve kendisinden başka kimseye de vermemelidir. Açık anahtarın paylaşılmasında ya da imzalı iletiyle ve şekilde postalanmasında herhangi bir problem bulunmamaktadır. Gizli anahtar ile gerçekleştirilen kodlama faaliyetine imzalama adı verilir. Seri olması ve az alan kaplaması için genel olarak, iletinin önce özeti oluşturulur, özet imzalanır, yani kodlanır. Aşağıdaki şekilde imza doğrulama ve imzalama şematik olarak ifade edilmektedir.



Şekil 6:(a) İmzalama (b) İmza Doğrulama

Mesaj nakleden şahıs, imzalı iletiyi ve iletinin özetini muhataba nakleder. Mesajı alan gönderenin açık anahtarı yardımıyla imzalı mesaj özetini çözer. Çözülen imzalı ileti özeti, alınan iletinin özeti ile birbirini tutuyorsa, iletinin kesin olarak gönderen kişilerce imzalanmış olması meydana gelir. İletide minimal seviyede de olsa herhangi bir değişiklik yapılmışsa, çözülen ileti özeti ile alınan iletinin özeti arasında tutarsızlık yaşanacaktır. İmzası teyit edilmiş

bir iletide, iletiyi imzalayan şahsın kimlik bilgilerinin doğruluğu kanıtlanmış (authentication), bu durum iletiyi imzalayanlarca inkâr edilemeyecektir (non-repudiation). İletinin imzalandığı şekliyle durmakta olduğu, hiç bir suretle değişime uğratılmadığı da (integrity) garantidedir. Gizli anahtar, Sanal paraişlemlerinin en önemli parçasıdır, kesinlikle kaybedilmemeli, bir başkasına verilmemelidir. Açık anahtar, gizli anahtardan eliptik eğri çarpım (elliptic curve multiplication, ECM) yoluyla bulunur. Bu bağıntı tek doğrultuda bir bağıntıdır. Diğer bir ifadeyle, gizli anahtar sisteminden açık anahtar sistemi üretilebilmekte fakat açık anahtar sisteminden gizli anahtar sistemini üretebilmek imkânsızdır (Andreas, 2014: 330).

Gizli anahtar, 256 bit geliş güzel 0 ve 1 rakamlarından oluşmaktadır. Her 4 biti, 16'lık düzene istinaden kodlanmıştır. Örneğin gizli bir anahtar aşağıdaki şekliyle kodlanır:

*E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262*

Dijital imzanın güvenilirliğinde 256 tane peş peşe 1 veya 0 ile,  $2^{256} \approx 1.15 \times 10^{77}$  değişik gizli anahtar oluşturulabilir. Gizli anahtar oluşturmak, 1 ile  $2^{256}$  arasında alelade bir tam rakam oluşturmak biçiminde de varsayılabilir. Herhangi iki değişik bireyin gizli anahtarının özdeş olabilme olasılığı, takribi  $10^{77}$  de 1'dir.  $10^{77}$  Muazzam büyüklükte bir değerdir, izlenebilen dünyada  $\approx 10^{80}$  atom bulunduğu varsayılmaktadır (Villanueva, "How Many Atoms Are There in the Universe?", Erişim 20.04.2018).

Şayet gizli anahtar, açık anahtardan, oluşturulabiliyor olabilseydi, sistem tümüyle güvenli olmayan bir durumda olabilirdi. Elinde açık anahtarı olan birinden gizli anahtarını elde edebilmenin yolu neredeyse kaba kuvvete başvurmaya varabilmektedir. 1' den start verip  $2^{256}$  'ya değin bütün gizli anahtar sistemini, ECM (elliptic curve multiplication) fonksiyonundan süzüp, bulunmuş olan açık anahtarın, olması gereken açık anahtar olup olmadığına bakılmalıdır. Kısaca, açık anahtardan, gizli anahtarı elde etmek uygulamada herhangi bir olasılığı yok denilebilir. Hala kuantum teknolojisine bağlı bilgisayarlar üretilmemiş olmasına karşın, bu bilgisayarlar nedeniyle, gelecek bir zaman diliminde açık/gizli anahtar çiftinin güvenilirliğinin sağlanması tehlike altına girecektir. Bu konuda ileri kuantum, gizli/açık anahtar çiftleri ya da değişik şifreleme yöntemleri sisteme alınarak, sanal imzalamanın güvenilirliğinin sağlanmasına onay verilebilecektir (Daniel, 2009).

### **4.1.3 Bitcoin Adresi**

Klasik bankacılık sistemindeki hesap numarasının benzeri sayılabilecek Bitcoin adresine, Bitcoin cüzdan adreside denilmektedir. Bütün çıkış ve giriş faaliyetleri Btc hesaplarına aksetmektedir. Bir Btc hesabı, yirmi yedi ila otuz dört harf ve rakamdan meydana

gelmekte olup genellikle üç yâda bir rakamlarından herhangi bir ile başlamaktadır (Bitcoin adres, [https://en.bitcoinwiki.org/wiki/Bitcoin\\_address](https://en.bitcoinwiki.org/wiki/Bitcoin_address), Erişim Tarihi: 25.05.2018).

Bitcoin adresine: 1S4xaN32verilebilir. Rakamlardan ve harflerden meydana gelen Bitcoin adreslerini akılda tutmak yada herhangi bir yere yazabilmenin zorluğundan dolayı uygulamada Şekil 7’de görüldüğü biçimde iki boyutlu Barkod olarak isimlendirilen QR kodlarından yararlanılmaktadır.

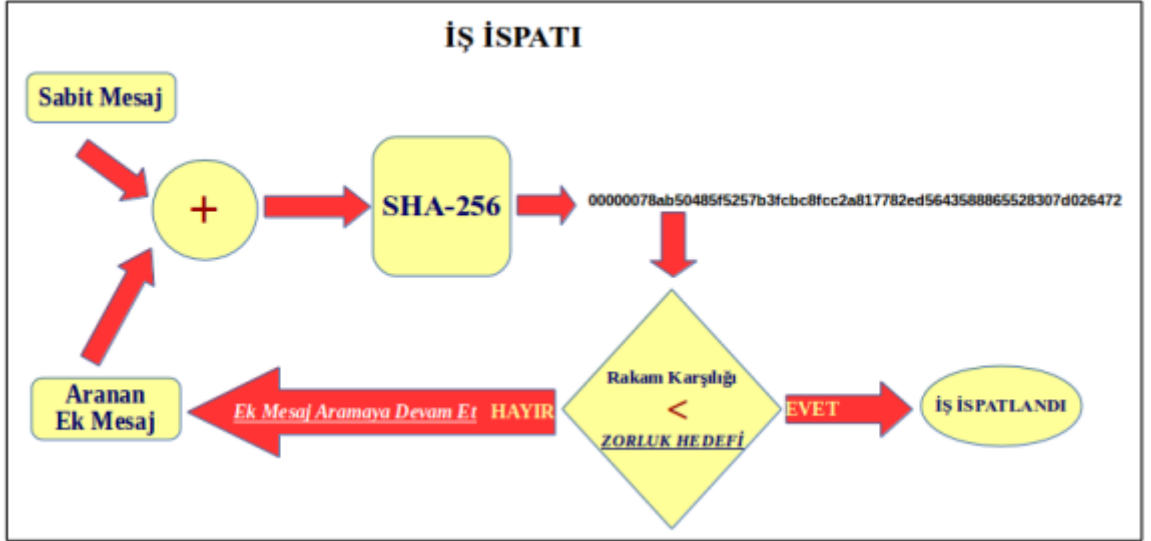
1K5wSNgerhlg8GZGcsNmAx5EYMRXSRR3Ae



**Şekil 7:**Uygulamada Kullanılan Bir Btc hesabının Örnek Bir Kare Kodu:

#### **4.1.4. İş Kanıtı (Proof of Work)**

İş İspatı bilgisayarların, herhangi bir iş için faaliyette bulunduğunun ispat edilmesinde faydalanılan bir yöntemdir. Bilgisayarlar bir takım uygulama ve fonksiyonları, süratli bir biçimde yerine getirebilirler, mesela elektronik posta gönderme işlemini, çok süratli biçimde gerçekleştirebilecekleri bir faaliyettir. Bilgisayarın saniyeler içinde milyarlarca, istenilmeyen elektronik posta göndermesi de imkan dâhilindedir. Bu şekildeki bir elektronik posta gönderimine mani olmak maksadıyla, elektronik posta ileticisi, e-mail gönderen bilgisayarlardan, bir miktar çalışarak kalmasını ve bu durumu ispat etmesini talep edebilir. Bununla birlikte, elektronik posta göndermek üzere faaliyette bulunan bilgisayarlar, bir miktar faaliyette bulunarak, bir miktar elektronik posta yollayabilecek ancak milyarlarca elektronik posta gönderilmesine yeterli vakti olmayacaktır.



**Şekil 8:İş kanıtı**

Uygulamada İş kanıtı sebebiyle çoğunlukla SHA-256 özet işlemi kullanılmaktadır. SHA-256 özet işlemi, 256 tane peş peşe olan, hemen hemen gelişi güze 11 ve 0' dan meydana gelen/ bir çıktı oluşturur. 256 bitlik bu sırayı, tam rakam şeklinde açıklamak imkan dahilindedir. İş ispatı yapacak bilgisayarlardan, stabil bir mesaja ilave mesaj daha eklendikten ve SHA-256 ile kısaltıldıktan sonra, meydana gelen özetin dijital numara karşılığının, daha öncesindentespit edilmiş olan bir rakamdan daha küçük olması talep edilir. SHA-256 özet işlemi kriptografik şekilde güvenilir bir algoritmayı temsil ettiğinden, modül birçok kezişimde bulunmadan, aranan ilave iletiyi onaylaması olanaksızdır. Diğer taraftan ilave iletinin bulunması zor bir iş olmasına karşın ilave iletinin bulunduğunu ya da bulunmadığının sağlanmasını yapabilmek daha pratiktir. İş kanıtının zorluk derecesinin küçüklüğüne bağlı olarak daha da zorlaşacağı belirtilmektedir.(Target, <https://en.bitcoin.it/wiki/Target>, Erişim Tarihi 30.04.2018).

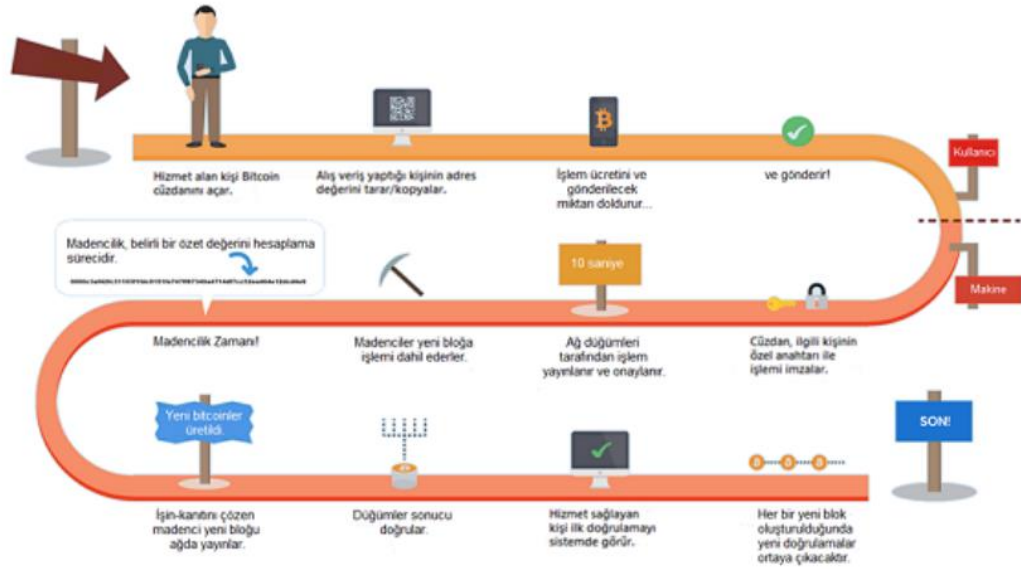
Çalıştığını ispat eden bilgisayar, ileti ve bulduğu ek iletiyi kanıt olarak talep eden programa iletir, programın kanıtın doğru şekilde çalışıp çalışmadığını ayırt etmesi çok kolaydır. İletiyeye, ek iletiekler, özetleme algoritmaları içerisinde süzer, meydana getirdiği 256 bitlik özetin rakamsal değerini, zorluk hedefinden daha düşük bir değerde olup olmadığına kontrol ederek, iş ispatının yapılmış veya yapılmamış olduğunu rahatlıkla saptayabilir. İş ispatının mantıksal altyapısının anlaşılabilmesine en iyi verilecek örnek bulmaca çözmedir. Şöyle ki bulmacayı çözebilmek bir hayli zor bir işken, çözümlenmesi yapılmış olan bulmacanın kontrolü (iş ispatının kontrolü) çok daha kolay bir eylemdir. Bitcoin



üreticilerinin, alış veriş faaliyetlerinden bir blok meydana getirmesi ve bunun gibi durumu gerçekleştirirken kendi aralarındaki rekabetleri iş kanıtı metoduyla sağlanabilir.

## 4.2. Bitcoin Transferi

Bitcoin ağına ilk defa dâhil olan bir kişinin izlemesi gerek adımları tarif etmek gerekirse; ilk olarak, sahibi olacağı Bitcoin'lerini saklayabilmesinde lazım olan sanal cüzdanını bilgisayar, telefon, tablet vb. gibi cihazına yüklemelidir. Sanal cüzdanın yüklenmesinin peşinden ise şahsına ait bir adres değerine, bütün kişilerin erişebileceği açık anahtara ve yalnızca kendisine özel anahtarının bulunması gerekmektedir. Bu işlemin tamamlanmasının ardından Bitcoin kullanarak bir alım yapabilmek için lazım olan sanal para 4 şekilde sağlanabilir. Bu dört yoldan en çok kullanılanı Bitcoin kullanan tanıdık birinden elde edilmesidir, diğer metotlara Btc çekme makinelerinden (ATM) döviz/btc kuruna endeksli şekilde temin edilmesi, şahsına has emtiyada hizmetin Btc alınarak satışının yapılması ve bir takım web adresleri üstünden Btc satışı yapan insanlara ulaşarak belli bir para ödeyerek Bitcoin alınması olarak belirtilebilir.



**Şekil 9:** BitcoinSisteminde Gerçekleşen İşlemlerin Genel Görünümü

(<https://www.bitcoindesigned.com/infographics/the-bitcoin-transaction-life-cycle/>).

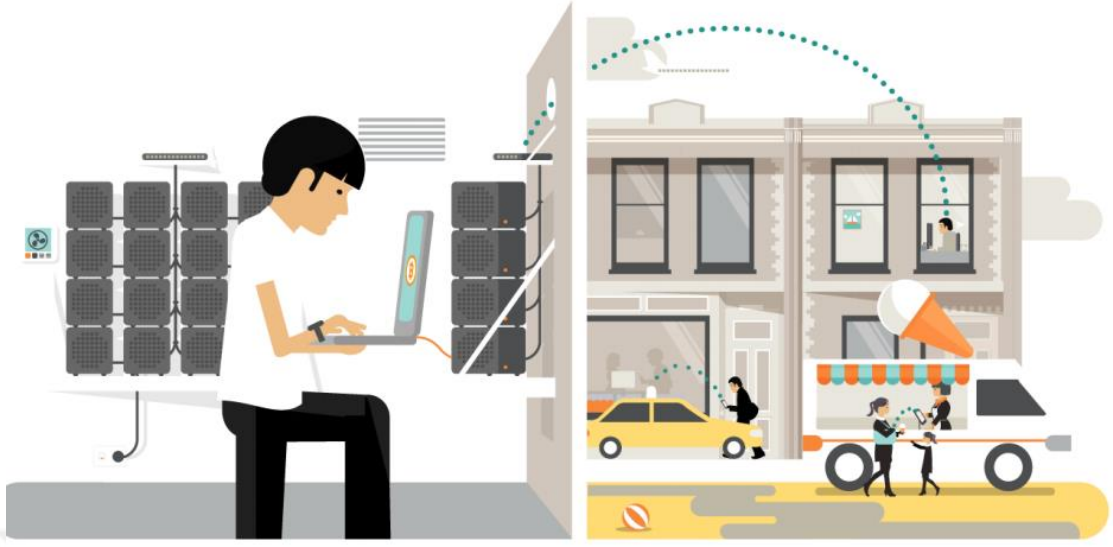
Bitcoin ağına ilk defa dahil olan kişi, yukarıda görülen işlemleri gerçekleştirmesinin peşinden elde ettiği Bitcoin ile herhangi bir alım-satım gerçekleştirmek istediğinde sistemde oluşan işlemler zincirini Şekil 8'de belirtildiği biçimde; ilk önce hizmet yada ürün alacak olan şahıs (varlık) mobil cihazı yada bilgisayarda yer alan dijital hesabını aktif ederek almış olduğu ürün ve hizmete sahip olan bireyin hesabını barındıran QR kodu okutarak söz konusu

şahsın bilgisine rahatlıkla erişebilmektedir. Ayrıntılarına eriştiği şahsa ödenmesi icap eden meblağı ve Bitcoin madenciliği yapan kişiye verilmesi gereken işlem ücretini de ilave ederek sanal para gönderim işlemi nihayete erer. Artık kullanıcının gerçekleştireceği bölüm sona ermiş olup ve daha sonra gerçekleşecek uygulamalar Btc modülünün çalıştığı cihazlar ve Btc üreticileri nezdinde ifa edilecektir. Bu kademedeki transferi yapılan dijital mevduatı ile birlikte cüzdanı, hesap sahibinin kendine has anahtarıyla sanal imza meydana getirir. Bu ayrıntılar Btc modülündeki bütün müşterilere sunulup ve onaylanacaktır. Btc modülünde yer alan üreticiler bu uygulama bilgileri iletildiğinde yeni Btc mükâfatı elde edebilmek için çok sayıda uygulamayı, blok ismi verilen uygulama kümesine eklerler. Daha sonrasında üreticiler üreticiler iş ispatı sorununu halletmek için sahibi buldukları araçlarda SHA256 özet algoritmalarını kullanmaktadırlar. Üretici iş ispatı probleminin çözülmesinin peşinden uygulamalarını bulunduğu yeni bloğu Btc sisteminde duyururlar. Sistemde yer alan nokta birimlerinde bloğun doğrulanma işlemi yapılır, bu bloğu oluşturan madenci yaklaşık 12,5 bitcoin ile mükâfatlandırılmaktadır. Bu şekilde düğümler bloğu kabul etmektedirler. Kabul edilmiş olan bloğun ardından başka bir blok meydana getirildiğinde bitcoin'i alacak kişi bitcoin karşılığında vereceği hizmeti yâda ürünü alıcıya yollamaktadır. Bitcoin'in çalışma kuralları en sade haliyle yukarıda anlatıldığı biçimdedir ve gerçekleştirilecek her bir işlemde aynı olaylar ifade edildiği biçimde tekrarlanmaktadır.

#### **4.3. Bitcoin'in Çalışma Sistemi**

Bitcoin'de mevduat terimi "bitcoin" olup "BTC" şeklinde kısa yazılmaktadır. Mevduat teriminin en ufak tutarlı değeri ise bir btc'nin 1/100.000.000'a denktir ("0.00000001 BTC") ve adını Satoshi Nakamoto'dan almış olup "satoshi" şeklinde isimlendirilmektedir (Prior, "How much gold is there in the world?", BBC News, Erişim20.03.2018).

Bitcoin, çalışma yönünden sterlin, yen, Euro vb. mevduat terimleri şeklinde değerlendirilebilir; herhangi bir mevduat terimi mukabilinde satımının ve/veya alımının yapılabiliyor olmasından dolayı, Bitcoin'ni kabul eden işletmelerde karşılığında mal ve hizmet satımı ve alımı ve satımı da yapılmaktadır.



**Şekil 10:**Bitcoin'in İşleyiş Mekanizması.

Bünyesinde çok sayıda sanal cüzdan modülü bulunmakta olan Btc, açık kaynaklı şifreleme yönteminin olması sebebiyle özel istemci uygulamalarının güncelleştirilmesine de imkân sunmaktadır. Btc sistemine katılan kişilere ait Btc hesapları arasında mevduat değişimleri gerçekleştirilmektedir. Mevduat değişimini gerçekleştirme talebinde olan bir kişinin gerçekleştireceği işlem, bunu belli bir ileti biçiminde sisteme iletmektir; şayet uygulamanın geçerli olabilmesi sebebiyle lüzum eden koşullar yerine getiriliyorsa, işlem onaylanarak yerine getirilmiş sayılır. Kullanıcıların kendilerine ait gerçek bilgilerini belirtme mecburiyetleri bulunmamaktadır; dışarıdan görünen, Bitcoin adreslerince birbirlerine para gönderimi yapıldığıdır, fakat hangi adresin, hangi kişinin olduğu belli değildir; bu yapısı ile borsa işleyişini andırmakta ve bireysel mahremiyetini bir nebze yerine getiren bir düzene sahip olduğu gözlemlenmektedir. Merkezi bir otoritenin bulunmaması ile birlikte hareketlerin yönlendirilmesi ve onaylatılması Btc sahiplerince karma biçimde meydana getirilmektedir. Bitcoin'in başlıca işleyiş sistemi blockchain şeklinde isimlendirilen, gerçekleştirilen bütün hareketleri gösteren sıralı işlem düzenidir. Herkesin ulaşabileceği biçimdedir. Blockchain, ortak ve tek paylaşım yapılan bir hareket düzeni şeklinde tanımlanmaktadır. Blockchain ağında, onay görmüş hareketler bir blok sistemi içinde bir araya gelerek zincir sisteminin sondaki halkasına ilave edilmektedir. Hareketlerin onay görmesiyle "mining" olarak isimlendirilen aşamasıyla ifa edilmektedir. Bu aşamada "miner" olarak isimlendirilen Btc üreticileri yeni ilan edilen ve onaylanma aşamasında olan hareketleri blok düzeni şeklinde derleyerek, o bloğun geçerli olabilmesi için çözülebilmesi icap eden algoritmik yapıya

sahipbir problemi çözümlenmesi amacıyla işlemsel enerji sarf ederek önce tamamlamaya çalışırlar. Problemin çözümlenmesini yapan ve blok bütünlüğünü tamamlayabilen ilk kişi “miner”, oluşturduğu bloğunu zincir halkasının sonuna ilave etme hakkını elde eder. Bloğunu eklemesi ile birlikte, mükâfat olarak her blok içindaha önceden miktarı saptanmış olan bitcoin ödülünü de kazanır. Bu biçimde, “mining” aşaması ile aynı anda bitcoinlerin piyasaya sürümü de tamamlanmış sayılmaktadır. Söz gelimi bitcoinlerin fizikibir karşılığı olmamakta, tüketilen sistemsal gayret, bir manada mevduata çevrilmektedir. Blok meydana getirme mükâfatı her 210,000 blokta bir yarıya düşmektedir; en başta 50 Bitcoin, sonra 25 Bitcoin olan blok üretme mükâfatı 2016 yılı Temmuz ayı içerisinde 12,5 BTC’ye indirilmiştir. Bu zamanda bir bitcoin’in 701 Amerikan doları düzeyinde olduğu göz önüne alınırsa, blok meydana getirmenin çekiciliği, “mining” için kullanıcıların işlem güçlerinin bir araya getirildiği “miner havuzlarının” (mining pool) meydana getirilmesi ve özelleştirilen donanımın yenilenmesi anlamlandırılabilir. Blok yapımında ise her on dakika içerisinde bir blok üretme kapasitesinin yakalanmasına çaba gösterilmektedir. Bu da sistem genelinde blok tesis etmek sebebiyle çözümlenecek algoritmik işlemlerin zorluk derecesinin parametrelerini revize ederek yapılmaktadır. Şayet blok üretme seviyesi istenilenden daha fazlaysa zorluk fazlaştırılmakta, tam aksi olması gerekenden daha düşükse zorluk seviyesi düşürülmektedir. Blockchain sisteminde tesis edilecek toplam btc miktarı, 21.000.000 şeklinde saptanmıştır, bu sayı yakalanmasının akabinde btc imalatı yapılmayacak; blok üretim mükâfatı tesis edilemeyecektir. Her on dakika içinde bir tane blok meydana getirileceği varsayımı doğrultusunda hedeflenen bu rakama 2140 tarihinde varılabileceği tahmin edilmektedir.2016 yılı Kasım ayındaki verilere göre dolaşımdaki total bitcoin adeti 15.9 milyonu ve total piyasa değeri de 11.000.000.000 doları geçmiştir. Bitcoin’in işleyişi, ağdaki işlem gücünü elinde bulunduran kesimin güvenilir olması ile doğru orantılıdır. Her yeni blok, daha evvelki bloğun “hash”olarak adlandırılan bir işlem ile sabit miktarda bit’e sıkıştırılmış olan bir grafiğini içermektedir. Bu şekilde“block chain” üstünde eskiye dairbir oynamada bulunulması önlenerek güvenli olması yönünden bütünleşme tamamlanır; onaylanma işlemi yapılmış bir işlem üstünde yeniden bir düzenlenmede bulunulmak istenirse o işlemin bulunduğu bloğun tamamlanabilmesi için çözümlenmesine ihtiyaç olan algoritmik problem yeniden çözümlenmesi gerekmektedir. Diğer taraftan her blok birevvelki bloğun benzerini yansıttığı için, değiştirilmek istenilen bloğun peşinden gelen bütün bloklar için benzer uygulama yenilenmeli özetle başka bir“block chain” oluşturulmalıdır. Block zincir altyapısında bütün Btc kullanıcılarının sürekli üzerinde çalışması bu güvenlik tehlikesine olanak vermemektedir; Eskiye dair yapılacak bir değişikliğin kabul edilmesi yalnızca alternatif block chain’in daha

süratli bir biçimde meydana getirilmesi ile olabilir ki bunun yapılabilmesi içinde ağ üzerinde bulunan işlemsel gücün büyük çoğunluğunu elinde bulundurması gerekir.

#### **4.4. Bitcoin Cüzdanı**

Bitcoin cüzdanı edinmek Bitcoin dünyasına girmenin ilk adımdır. Bitcoin cüzdanı bir uygulamadır. Bitcoin cüzdanı uygulamaları bilgisayar, mobil telefon ve tablet bilgisayarlar da çalıştırılabilmektedir. Bitcoin cüzdanı yazılımları yüklendiklerinde, kullanıcıya özel, açık anahtar, gizli anahtar ve Bitcoin adresini oluştururlar. Var olan herhangi bir gizli anahtar varsa, bu yazılımlara adapte edilmesi imkân dâhilindedir. Bitcoin cüzdanlarında güvenliğin sağlanması, gizli anahtarlar sayesinde sağlanmasından dolayı, gizli anahtarın yitilmesi veya başkası tarafından ele geçirilmesi, gerçek fiziki para cüzdanınızı çaldırmayla eş değer sayılabilir. Gizli anahtar emin bir ortamda muhafaza edilmeli, bir başkası ile paylaşılmamalıdır (Brand, 2016:208).

Bitcoin sağlamak amacıyla Btc hesabına, elde edilen Btc 'leri kullanabilmek amacıyla gizli anahtar olması gerekir. İnternet tabanlı Bitcoin cüzdan servisleri, kullanıcılarının namına açık veya gizli anahtar oluşturur ve kullanıcılarının güvenliğinin sağlanmasından mesuldürler. Gizli anahtarları kendi bünyelerinde saklamış olan firmalar, geçmiş dönemlerde hackerlerin saldırıları neticesinde, müşterilerinin Bitcoin'lerinin çalınmasına sebep olmuşlardır. Bu nedenle çokta iç açıcı olmayan bir üne sahiptirler ( Brand, 2016: 209).

2011 yılı Haziran ayında, 478 değişik hesaptan, toplamda 25 bin Bitcoin çalındığı bilinmektedir. Güvensiz bir ortam oluşması neticesinde, 1 saatte, 1 Btc' nin değeri, 19 USD' den, 0.01 USD' ye gerilemiştir.

#### **4.5.Bitcoin İşlemleri**

Bir dijital para hesabına özgü olan coinleri başkabir coin hesabına iletme uygulamasına transfer (transaction) adı verilir. Elde bulunan Btc' lerin tüketilmesi, bir Btc uygulamasıdır. Bu modülün çıktıları ve girdileri bulunmaktadır. Çıktı miktarıyla girdi miktarları toplamı denk olmak zorundadır. Modülün girdileri, daha evvelki diğer girdilerin çıktı tutarlarıdır. Başka bir ifadeyle, söz konusu modüldeki girdi miktarları, daha evvelki

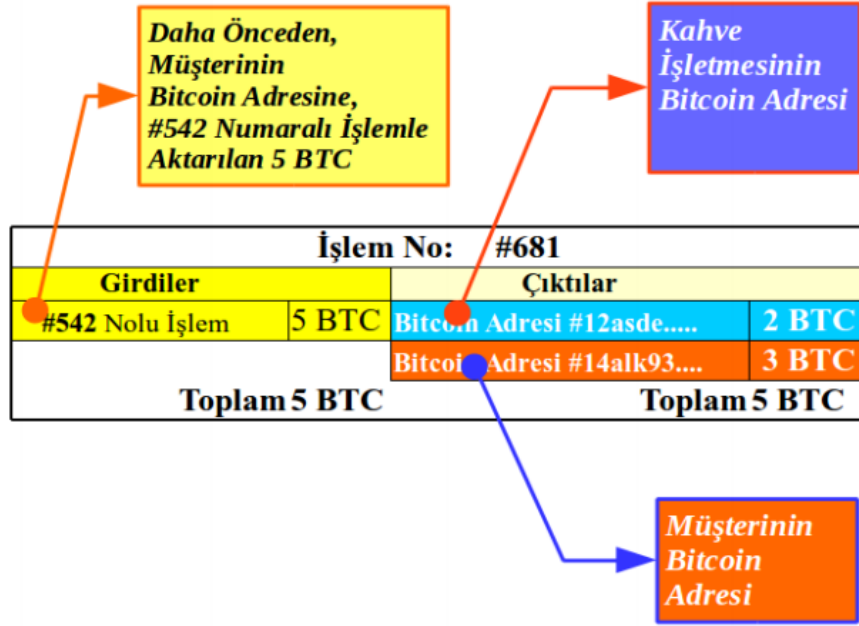
modüllerin henüz tüketilmemiş olan çıktı miktarlarıdır. Kaydı oluşturan şahıs, bütün girdileri ve aktarımda bulunduğu Btc hesaplarını, gizli anahtarı ile dijital bir şekilde imzalar.

Girdi miktarları çok sayıda hareketin çıktısı olacağı gibi, çıktı miktarları da birden fazla sayıda Btc cüzdanına ait olmalıdır. Bir müşteri, diğer bir müşteriye coin göndermek istediğinde, aktarım yapılacak müşterinin coin hesabının bilinmesi gereklidir. Aktarımda bulunacağı bireyin Kare kodundan faydalanabileceği gibi, metinsel şekilde şifrelenen coin hesabındanda faydalanabilir. Aktarımda bulunmak isteyen müşteri Btc hesap programları ile işlemleri başlatabilir. Btc uygulamasında girdi miktarları, Btc cüzdanına borç (debit), çıktı miktarlarına aktarım işlemine konu Btc cüzdanına alacak (credit) şeklinde kaydedilmektedir.

**Tablo 2.**Basitleştirilmiş Bir Btc Uygulamasının Örneği.

İşlem No: 195			
Girdiler		Çıktılar	
115 Nolu İşlem	3 Btc	Bitcoin Adresi 13 Adse....	2 BTC
117 Nolu İşlem	6 Btc	Bitcoin Adresi 14 Alk93....	4 BTC
		Bitcoin Adresi 15 Alk93....	3 BTC
Toplam 9 Btc		Toplam 9 Btc	

Tablo 2'de, 9 Bitcoin'i mülkiyetinde tutan bir Btc tüketicisinin, bu 3 coini değişik hesaba aktarım uygulamasının örneği verilmiştir. 192 numaraya ait işlemin girdi miktarı, 112 ve 127 numaralı uygulamaların, daha önceden tüketilmemiş (diğer bir aktarımda tüketilmemiş) çıktı miktarlarıdır. 195 numaraya ait hareketin çıktı miktarları ise 3 değişik Btc hesabıdır. Bir aktarım sonunda, birden fazla çıktı olabilmesi muhtemeldir. Çünkü değişik cüzdanlara Btc transfer edilebilir. Ama her bir çıktı miktarı, yalnızca bir kez girdi şeklinde kullanılabilir. Bütün çıktı miktarları, tüketilmiş yada tüketilmemiş (UTXO) olacak şekilde gruplandırılabilir. Bir transfer hareketinin doğru sayılabilmesini için girdi miktarlarının tüketilmemiş çıktı miktarlarından oluşması gerekli koşuldur. Tüketilmemiş çıktı miktarı tüketildiğinde tüketilmiş olacak şekilde yeniden gruplandırılır.



**Şekil 11:**Çay İçen Bir Tüketicinin Btc İle Ödemede Bulunması

Şekil 10’de ise beş Btc’ si bulunan alıcının, iki Btc mukabilinde çay satın alması ve kayıt sonrasında geriye kalan üç Btc’ yi yine alıcının kendine ait olan Btc cüzdanına transfer etmesi gösterilmiştir. Güvenlik ve anonimlik düzeyini yükseltmek hususunda, çoğalan Btc’lerin, yine aynı alıcıya ait, ancak değişik bir Btc cüzdanına transfer etmesi önerilmektedir. İstenildiği takdirde, bu ticaret neticesinde transfer edilen Btc’lerin ne kadar süre sonrasında kullanılabileceği de gösterilebilir (Andreas, 2014: 330).

#### 4.5.1. İşlem Masrafı ve İşlemin Onaylanması

İşlem masrafı ve işlemin onaylanmasında girdilerin değerlerinin toplam tutarı çıktıların değerlerinin toplam tutarından küçük ise işlem onaylanmaz. Eğer girdilerin değerlerinin toplam tutarı çıktılarınkinden fazlaysa arda bulunan tutarı btc üreticisi operasyonel gider şeklinde kendisinin hesabına aktarabilir. Bir Btc işleminde “300-400 byte” data bulunmaktadır. İşlemin yapılmasına start verildiğinde, Bitcoin ağına ilişik uçlar arasında süratle iletimi sağlanır. Hiç kimse, işlemi transfer edene güvenme mecburiyetinde değildir, bağlı olunan ağın da güvenilir olması şartı yoktur, öte yandan yapılan işlem elektronik ortamda sayısal imzaya sahip olduğundan, işlemin iletildiği uç ilk önce dijital imzasının sağlanmasını yapar, gönderilen imzanın geçerli olduğunu tespit ederse ağ ortamında işlemin yayılmasını sağlar, güvenli olmadığını saptaması durumunda bu işlemi onaylamaz ve yayılmasına izin vermez. Bitcoin ağı uçtan uca bir ağ yapısına sahip olması nedeniyle her bir

uç işlemin başlamasıyla birlikte, başka uçlarla irtibata geçmektedir. Bütün uçlar seviyede önem derecesine haizdirler. Herhangi bir Bitcoin işlemini doğrulayan her uç, bunu üç veya dört komşu uça iletir. Çok az bir zamanda (Bir, iki saniyede), işlem bütün uçlara iletilmiş olur. Bu uçlar ağ üzerinden kendilerine gelen blokları yâda işlemleri kendileri de doğrular. Bu şekilde; ağ üstünde işlemlere yâda bloklara gerçekleştirilecek saldırı girişimi etki etmez ve işlevsiz olur. Bitcoin aktarım işlemi birkaç saniyede gerçekleşirken onaylanması uzun sürer. Bitcoin madencileri ağ üzerindeki imzalanmamış işlemlerden bir blok meydana getirir ve el birliği ile oluşturulan bloğu ve bu blokta bulunan işlemlerin onaylanmasını yaparlar. Bloğun onaylanması demek bahse konu işlemin blok zincire işlenip geri dönmesi mümkün olmayacak biçimde kesinleşmesi manasını taşır. Blok zincirdeki her işlem ve her blok kendi içinde tutarlıdır ve hiç kimse kendisine ait olmayan bir bitcoini kullanamaz çünkü bahse konu her bir işlem bu işlemi yapan kişi tarafından elektronik ortamda imzalanmıştır. Alıcı konumundaki muhatabın ödemenin yapıldığı sırada internete bağlı veya bilgisayarının açık durumda bulunmasında ihtiyaç yoktur. Çünkü aktarım işlemi blok zincire işlenmektedir. Alıcı internete bağlandığı ilk anda kendi Bitcoin cüzdanı, blok zincirden kendisine ait hesabının durumunu kontrol eder. Olağan koşullarda Bitcoin aktarımından herhangi bir işlem harcı alınmazken, birtakım Bitcoin cüzdanları işlemin madenciler tarafından onaylanma süresini azaltmak maksatlı düşük meblağlarda işlem masrafı talep edebilmektedirler. Bir işlemin hemencecik Blok Zincir veri tabanına işlenip imzalanması istenilen bir durumdur. Olağan şartlarda işlemin bekleme süresi ve önceliği işlemin büyüklüğüne göre hesap edilmektedir. Başlıca kuralı, işlemin onay süresinin çok uzun olmaması ve sayısal büyüklüğü daha az olan işlemlere öncelik verilmesidir. Ortalama bir işlem 10 dakikalık bir zaman diliminde onaylanmaktadır. Ağa yollanmış olan herhangi bir işlemin madenciler tarafından blok zincire işleyeceği ilk blokta olacak diye bir garanti bulunmamaktadır. Büyük olasılıkla ilk blokta onaylanması beklenirken, bu onaylanma işlemi akabindeki bloklarda da olabilmektedir. (Brand, 2016: 208).

Standardize dijital paraağında, herbir işlem şayet “1000 byte'dan küçük (girdi ve çıktıları az ise) ve işlem miktarı 0,01 BTC 'den çoksa, işlem masrafı alınmaksızın yüksek öncelik verilir. Bu şart sağlanmıyorsa, her ekstra 1000 byte için 0,0001 BTC işlem masrafı kullanıcıya sorulur”. Şayet talep edilen masraf kullanıcı tarafından kabul edilirse işlem önceliği de alınmış olur, masrafın reddedilmesi durumunda öncelik düzeyi de düşürülmektedir. Bir kesim cüzdan uygulamaları işlemin yapılmasına dair emri verilmiş fakat onaylanma işlemi yapılmamış işlemleri "harcanmış" ya da "onaylanmamış" şeklinde



göstermektedir. Onaylanmasının peşinde bu görünüm onaylandı ya dönüşür. Uygulamada minimum altı farklı uçtan onaylandı bilgisi gelen işlem “onaylandı” kabul edilmektedir. Sistem her 10 dakikada bir, blok onayının verilmesi konusunda kendiliğinden ayarlanmaktadır. Müşterilerce talep edilen Btelerin tüketilebilmesi için icap eden altı farklı uçtan gelmesi gereken "onaylandı" mesajı, çok az da olsa, bazen 60 dakikaya değin varabilir. (Brand, 2016: 208).

Bir kaydın çıktısı diğer bir kaydın girdisi olabileceğinden, kayıtlar birbirilerine “dede-baba-torun” biçiminde bağlı bulunmaktadır. Fakat Bitcoin ağı gevşek ve herhangi bir sınırlaması bulunmayan bir ağ olması sebebi ile bazı hallerde en alttaki kayıt (torun) öbürlerinden evvel dağılabilmektedir. Bu hususta kayıtların ilişkili bulunduğu ilk kayıt (dede kayıt) tamamlana değin, öteki kayıtlar beklemeye alınır. Ağın genişlemesinin engellenmesi maksadıyla, beklemeye alınabilecek kayıt adedi lokalize edilmiştir (Brand, 2016: 208)

#### **4.5.2. Çifte Harcama**

Bitcon işlemleri ağ içerisinde çok kısa bir zamanda yayılırken bir işlemin onaylanması daha uzun sürer. Elinde bulundurduğu bitcoini elektronik ortamda imzalayarak tüketen bir kimsenin start verdiği alışveriş işlevi olumlu bir başlangıçtır. Geçerli olmayan bir tahsilat söz konusu ise anında reddedilir. Hiçbir kullanıcı kendisine ait olmayan Btc'lerle harcama işlemini gerçekleştiremez. Herhangi bir sanal para hesabına gerçekleştirilen ve olumlu olan ödemeler çok kısa bir zaman zarfında ağda bulunan bütün kullanıcılarca görülebilir pozisyona gelir, fakat bu işlemin kesinlikle onaylanacağı manasını taşımaz. Geçerli sayılan herhangi bir işlemin gecikmeli onaylanmasına bağlı çifte harcama ihtimali bulunmaktadır. Aynı paranın çok sayıda harcanmış olma durumuna çifte (mükerrer) harcama denilmektedir. Herhangi bir tüketim işleminin startı verildiğinde daha onaylama süreci yaşanmamışken hem arz eden hem de talep eden kişiler tarafından söz konusu coinler kullanılmaya devam edilirse ya da buna kalkılırsa mükerrer tüketim riski oluşmuş olacaktır. Mükerrer tüketim yapılma durumunu düşürmek amacıyla ağa bağlı minimumaltı değişik uçtan işlem onayının gelmesi beklenir. Olası çifte harcama atakları aşağıdaki gibidir.

**1.Yarış Atağı (Race Attack):** Henüz başlamış olan bir işlemde bulunan bitcoin hiçbir onay yapılmamışken sürat bir biçimde hile yapılarak yeniden kullanılmış olursa onaylanacak olanın hangi işlem olacağı hususunda tahmin yapmak güç olacaktır. Kullanıcılar ağa bağlandıkları esnada kendilerine iletilen bağlantı isteklerini geri çevirip, uçlardan en iyisine bağlanmayı

yeğleyerek bu türlü ataklardan kendilerini koruyabilirler. Bu türlü bir ataktan en garanti şekilde kendilerini muhafaza etmek isteyen kullanıcılar hiçbir uçtan onayı bulunmaya ödeme işlemini reddedip minimum altı onay olmasını beklemelidir. Kısaca; altı onayı görmeden hareket eden bir kullanıcının çifte harcama olma durumu ve bundan zarar görme olasılığı bulunmaktadır.

**2.Finney Atağı (Finney Attack):** Dolandırıcılık aşamasına bir bitcoin madencisinin de katıldığı bir atak çeşididir. İstisnai durumlarda görülür.

**3. Vektör 76 Atağı:**Finney atağı ve Yarış atağının birleşimi biçiminde meydana gelmektedir. Atak bir adet onayı bulunan bir işlemin, ikinci defa harcanması anlamına gelmektedir. Bu tür ataktan kullanıcının kendisinin muhafaza etmesi gönderilen bağlantı taleplerini kabul etmeyip en iyi ucu seçmesi ile sağlanabilir.

**4. Kaba Kuvvet Atağı (Brute Force Attack):** Art düşünceli vehızlı üretici ekibi, mükerrer tahsilat barındıran hücreyi onayladıktan sonra söz konusu işlemin onaylanmasını bekleyen satıcıya onaylandığını belirten yanıt gönderirler. İşlemin olumlu olma ihtimali, üretimi sürdürme kararlı olan üreticilerin, Btc yapısının projenin ortalama özet miktarının ne kadarlık kısmına erişebildikleri ve bu erişimin sonunda al sat yapan kesimin, işlemin sonuçlanması için ne kadarlık onaya ihtiyaçları oldukları ile alakalıdır. Mesela işlem yapma kararında olan üreticiler, bütün sistemin özetleme tutarının yüzde onunu elde etmişler ve diğer taraftan transfer işlemleri için onay aşamasında olan tacir kesim ödemeyi onaylatmak için 6 onay bekliyor ise, işlemin amacına ulaşma ihtimali binde bir' dir.

**5.%50 Atağı ya da Çoğunluk Atağı:** Eğer Btc sisteminin, yarısından çoğu art düşünceli madenciler tarafından ele geçirilmişse, atağın başarılı olma ihtimali %100'dür.

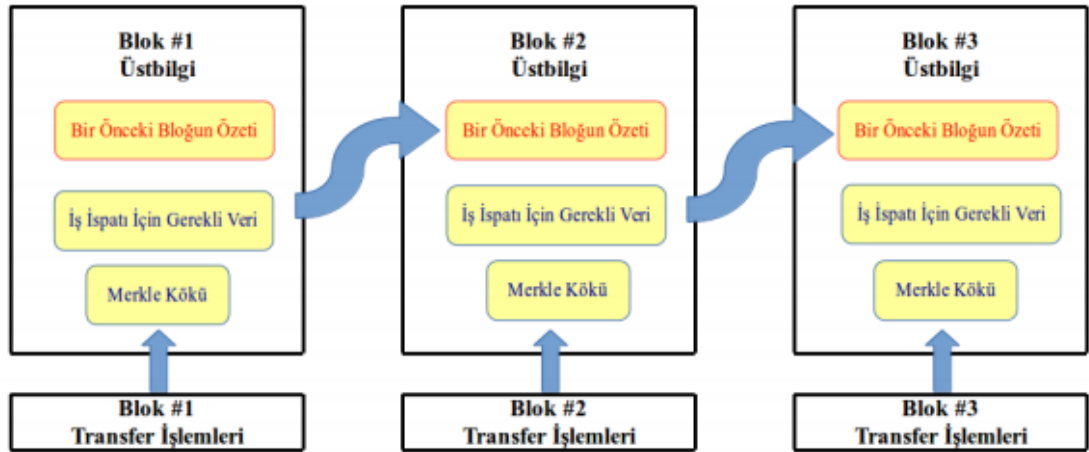
Tüccarlar, ödemenin kesinleştiğine kanaat getirmek için kendilerinin kararlaştırdığı miktarda onaylama sayısını beklerler. Çoğunlukla bu üç ila altı arasındaki bir sayıdır. Gece kulübü, lokanta ve ekonomik elektronik mal satışı yapan işletmelerse bir kısım hâllerde, işlemleri hızlı yapabilmek için, sıfır onaya kanaat edebilmektedirler. İşlem onayı olmadan seri şekilde çalışma talebinde bulunansatıcılar “BitKassa”, “Coinbase” ve “BitPay” gibi tahsil araçlarından faydalanarak mükerrer kayıt hilelerine karşı kendilerini muhafaza edebilirler.

“Ödeme işlemcileri”, mükerrer ödeme olması riskine karşın işlemleri güvende tutma yöntemi şeklinde de tanımlanabilir. Btc ağı, sanal imzalama yönteminin olması sebebiyle ağ içinde güvenli sayılabilecek bir düzendedir. Var olan yegâne sıkıntı, bir Btc'nin birden fazla kullanılması olarak düşünülebilir. Bunu ise mükerrer (çifte) harcama olarak adlandırabiliriz. Btc, Blok-Zincire dâhil olacak yeni bloktaki bütün işlemlerdeki girdilerin, daha önce

harcanmamış olmaları koşulunu koyarak, onaylanmış kayıtlarda çifte harcamayı engeller (Brand, 2016: 208).

#### 4.6.Blok Zincir (Blockcham)

Herkes tarafından kullanılabilen, açık bir düzeni olan, sıralı, şeffaf aynı zamanda vakit vurgulu Btc alışveriş işlemlerini barındıran sanal ve aynı zamanda küresel hesap defterleridir. Ayrıca sade bir bilgi dokümanı, kolay bir işlemcidir. Btc 'nin var olduğu 2009 yılından bu zamana dek gerçekleştirilen bütün alış veriş ve takas sürecinin dijital biçimde muhafaza edilmesi olarak da ifade edilebilir. Şuan bile gerçekleştirilen muhasebesel transfer kayıtları blokchaine kayıt edilmektedir. Gelecekte yapılacak transfer kayıtları da Blokchaine kayıt edilecektir. Btc ile birlikte meydana gelen, değişik uygulama yerleri de bulunan Blockchain yöntemi, merkezi olmayan bir ağ sistemindeki ayrı bilgisayarlar, birbirlerinden ilişkisiz şekilde bulundurulduğundan, bazı sistemsel yanlışlıktan ötürü oluşabilecek sorunlara karşı dirençlidir.



Şekil 12:Basitleştirilmiş Blok Chain Sistemi

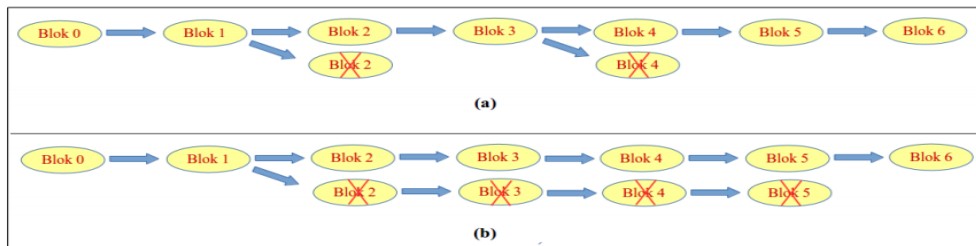
Şekil 11'de sadeleştirilmiş bir blokchain örneği yer almaktadır. Her blokta minimum bir işlem bulunmalıdır. Her blok, 1 MB şeklinde programlanmıştır. Bloğun üst-bilgisi, bloğa dair ayrıntısı bulunmayan verileri bulundurur, 80 byte'lık alanı kapsar. İşlemlerin ayrıntıları Btc alış veriş ticaretinden kaynaklanmakta olup tek işlem minimum 250 byte'dır. Takribi her blokta 350 ile 500 adet işlem bulunmaktadır. (Bitcoin Developer Guide, <https://bitcoin.org/en/developer-guide#block-chain>, Erişim 11.05.2018).

Bir blok içindeki bütün işlemler ikişerli kümeler biçiminde özetlenir, meydana gelen özetler tekrar kendi içlerinde ikili kümeler biçiminde kurgulanır. Söz konusu bu işlemler tek özet özet sağlanana değin sürdürülür. Bu şekilde gerçekleşen işlemlerin, ikili olarak özet oluşturması sonucu meydana gelen ağaç sistemine “Merkle Ağacı”; bu ikili işlemler sonrasında oluşan tek özet sistemini ise “Merkle Kökü” olarak adlandırılmaktadır. Bir aşamada yapılan değişiklik Merkle Kökünü değiştirdiği gibi söz konusu işlem ağacında da değişikliğe neden olacaktır. Aynı zamanda işlem kollarının tamamında değişiklik yaşanacaktır. Bu da işlem basamaklarından sonraki kısımlar için doğrulama ihtimalini sıfıra indirecektir. Söz konusu bu sürecin tamamı yapılan işlemlerin geriye doğru değiştirilemeyeceğini ifade eder.(Bitcoin Developer Guide, <https://bitcoin.org/en/developer-guide#block-chain>, Erişim 11.05.2018).

Btc ağınınbirinci bloğuna "genesis block" ismi verilmiş ve04.01.2009 yılında imal edilmiştir. Btc’ nin kurucusu, S. Nakamoto'ya ait Btc cüzdanına transfer edilmesiyle start verilen işlemdir. Tüm blok yapısının ilkidir. Söz konusu bloktan başlangıca doğru gidildiğinde son olarak ulaşılabacak bloğun adı “Genesis bloğudur.(Brand, 2016: 208).

**Yetim Bloklar** Normal şartlarda bir bloğun önceki zamanlardan süre gelen yalnızca biradet bloğu bulunabilir. Bir takım hususlarda, aynı zamanda çok sayıda üretici iş kanıtını gerçekleştirir ve keşfettiği bloğu işaret ederek Blokchain'e kaydettirir. Üreticilerin iş kanıtını oluşturdukları blokların detayları farklı olabilir. Btc sistemindeki öbür noktalar, yeni keşfettikleri ilk bloğu doğru olarak görürler. Tam noktaların her biri değişik blokları doğru olarak göreceğinden, Şekil 16'da görüldüğü gibi bir çatallaşma olur (Block Height And Forking, <https://bitcoin.org/en/developer-guide#proof-of-work>, Erişim 11.05.2018).

Ne var ki uzun zamanda, uçlar arasındaki antlaşma doğrultusunda, çatalın otomatik şekilde oluşan en uzun ucu doğru olarak değerlendirilir. Öbür tarafta kalan çatal uzantıları çoraklaşmış ve tek kalmış blok tipleri şeklinde ifade edilir. Uzun sürede, bir bloğun bir alt bloğu, her alt bloğun küçük bir alt bloğu oluşmaktadır.



**Şekil 13:** Blokchain'deki Çatallaşma Örneklemeleri (A) Az (B) Çok Az Oluşan Durumlar

Btc ağında, iş kanıtını oluşturan ve tespit ettiği bloğu Blokchaine ilave ettiren üreticiye mükâfat verilmektedir. Blok içindeki ilk işlem, üreticiye ödül olarak sunulacaktır. Fakat mükâfatı hakeden üretici, minimum yüz blok (takribî 10dakika×100≈17saat ) boyunca mükâfatı olan Btc' yi tüketemez. Şu nedenledir ki madencinin imal ettiği blok, aynı zamanlı diğer bir üretici tarafından da oluşturulmuş ihtimali olabilir ve bu bloğun öksüz blok olma olasılığı olabilir. Yalnızca, bloğunu Blokchaine ilave ettiren üretici mükâfatlandırılır.

#### 4.7. Bitcoin Üretimi ( Bitcoin Madenciliği)

Bitcoin madenciliği, Bitcoin sistemine yeni Bitcoin kazandırmanın, sahte işlemleri önlemenin, gerçekte var olmayan Bitcoin'leri kullanılmasını ve çifte harcamayı engel olmanın yöntemidir. Bitcoin madencileri yeni onaylanmış Bitcoin işlemlerinin, Blok-Zincir'e kaydedilmesini ifa ederler. Blockchain üzerinde bir bloğa işlenmiş olan bir işlem onay verilmiş manasına gelmektedir dolayısıyla işleme mevzu olan talep eden kesim kendine iletilen Btc harcanabilir aşamadır. Blokchaine bloğunu dâhil edecek olan üretici, yeni bloklarla birlikte verilen ve Btc aşamalarındaki operasyonel giderlerinin karşılığını alarak mükâfatlandırılmış olur.



**Şekil 14:**Bitcoin Üretimi ( Bitcoin Madenciliği)

Onaylama işlemi yapılmamış bitcoin aşamaları, belirli bir süre onay bekleyen işlemler grubunda muhafaza edilirler, üreticilerin havuzları ağda yaşanabilen beklemler sebebiyle benzer olmak mecburiyetinde değildirler. Havuzda tutulan transferlerden bir blok meydana getirerek, blok zincire bunu işletmek normal şartlarda süratli ve kolaylıkla gerçekleştirilebilecek bir faaliyettir. Bütün bitcoin madencileri hızlı bir biçimde blok meydana

getirirlerse, madencilerden her biri kendisine ait bloğunu, Blok zincire dâhil etmek isteğinde olacağından bir ağ kargaşası oluşacaktır. Bu durumun oluşmaması amacıyla, blok yapmak isteyen bitcoin madencilerinden, birbirleriyle rekabet ederek faaliyete bulunmaları ve bunu kanıtlamaları talep edilir.



<http://www.instructables.com/id/Build-your-Own-Portable-Bitcoin-Mining-Rig-Battles/>

**Şekil 15:**Bitcoin Madencileri Ne türlü Çalışırlar.

Bu, iş ispatı yöntemiyle yapılır. Blok meydana getiren bitcoin madencilerinden yalnızca bir âdet blok geçerli sayılır, blokların ortalama on dakikada bir meydana getirilmesi, iş kanıtının, zorluk noktası sistemsel biçimde değişime uğratılarak elde edilir. Her bir bloğun meydana getirilmesi için, üreticilerin yaklaşık on dakika süren, işlemci gücü sarf ettiklerini sistem garanti eder. Bir madenci, iş ispatını yapar ve bu iş ispatını, ağ üstünde dağıtır, bunu alan öteki uçlar bloğu çok sayıda kontrole tabi tutar, madencinin güvenilir olduğu ispat edilirse, Blokchaine eklenen enson blok ilave edilir. İş kanıtını oluşturarak tespit ettiği bloğu blok zincire ekleyen üreticiye, ağa yeni ilave edilen btc mükâfat olarak verilir. İşlem başında bu mükâfat elli bitcoinken, her 210.000 blok imalatında (aşağı yukarı dört senede bir) yarıya indirilmektedir. Güncel olarak başarılı olan madencilere, 12,5 Btc ödül olarak verilmekte ve tek para arzı yapılan alanda bu kısımdır.

Rast gele bir zamanda bakıldığında blok zincirin değişik uçlarında muhafaza edilen kopyaları birbiri ile aynı olmayabilirler. Standartlaşmış kuralları bulunmayan bitcoin ağında değişik zamanlarda, değişik uçlara, değişik blokların gelmiş olma durumu vardır. Lakin her uç çoğunlukla daha uzun zincir uzantısını doğru sayar, bu biçimde Blokchainler nihayetinde

biri diğeri ile uyumlu duruma ulaşırlar. Başına buyruk davranma olasılığı bulunan bloklar en son eklenmiş olan birkaç bloktur, yeni bloklar eklendikçe düzensiz davranan bloklar da bütün yöntemle kendiliğinden düzgün davranmaya başlarlar.

#### 4.8. Bitcoin Ağı

Bitcoin Ağını Tam Uç (Full Node) ve Hafif Uç (Lightweight Node) Bitcoin ağı olarak incelemekte fayda bulunmaktadır. Bitcoin ağı internet ağı üzerinde çalışır. Bitcoin ağına dâhil olan her bir bilgisayara uç ismi ile nitelendirilir. Uçların tamamı özdeştir, hususi bir uç, server, istemci bulunmamaktadır, bütün uçlar gönüllülük temelinde ağa katılırlar. Diledikleri zaman ağdan çıkabilirler. Bitcoin haricinde en meşhur uçtan uca ağ düzeni, belge gönderimi için yararlanılan Bittorrent ve Napster'dir.

Aşağıda bulunan şekilde; bitcoin kullanıcısı olan bir kişinin merkezi olmayan uçtan uca ağ bağlantısından ötekine Bitcoin transfer işlemi görülmektedir (Şekil 15').



**Şekil 16:** Bir Bitcoin Sahibinin, Başka Birine Sistem Üstünden Bitcoin transfer etmesi

Btc düzeninin kaidelerini gösteren, projenin iskeleti olarak tabir edilen noktalara "tam uç" İngilizce ismi ile "full node" ismi verilmektedir. Tam uçlar haricindeki öteki uçlara "hafif uç" yani "lightweight node" ismi verilmektedir. Bitcoin ağında yer alan uçların ekseriyeti hafif uçlardan oluşmaktadır. Bitcoin ağında bulunan, tam uçlar "Bitcoin P2P" kişiden kişiye transferi; cüzdan programları ile madenciler vb. hafif uçlar içinse "Stratum" gibi ek transfer anlaşmaları yer almaktadır.

#### 4.8.1. Tam Uç (Full Node)

Tam uçlar, Blok-Zincir'i eksiksiz ve tam olarak kayıt altında tutmakla görevlidirler. Genesis ismi verilen birinci bloktan en son bloğa değin bütün blokların, birbirlerinden serbest biçimde kontrolünü yaparlar. Tam uçların dikkat çekici bir diğer özelliği de, Bitcoin transfer işleminde kullanılan girdilerin öncesinde başka bir işlemde de kullanılmamış olduğundan emin olabilmek adına, sayıları on binlerce olan blokların kontrolünü yaparlar: Tam uçlar bütün işlemlerin ve blokların kontrolünü aşağıdaki biçimde yaparlar.

- Blok üstünde bellioranda Btc üretimi yapılmalıdır.
- Yapılan faaliyetlerde tüketilen mevduatların düzgünce imzalanmış olması gerekir.
- Blokların ile işlemlerin biçimi eksiksiz olması gerekmektedir.
- Sistem üzerinde bulunan hiç bir blokta, aynı Bitcoin birden çok defa harcanmamış olmalıdır. Tam uç olma isteğinde bulunan bir uç, birinci aşamadan ilerleyerek bütün aşamaları kendine göre belirlemesi gerekmektedir. Bütün tam uçlar, özdeş denetimleri gerçekleştirerek ve birbirleri arasında da bir uyum meydana gelecektir.

Tam uçlar, bütün Blok-Zincir'i kendi sistemleri üzerinde muhafaza ederler. 18 Mayıs 2018 itibarı ile bu bilgi takribi 100 Gigabayttır. Online olarak dünya üzerinde bulunan bütün tam uçları <https://bitnodes.21.co/> internet adresinden takip edilebilmektedir

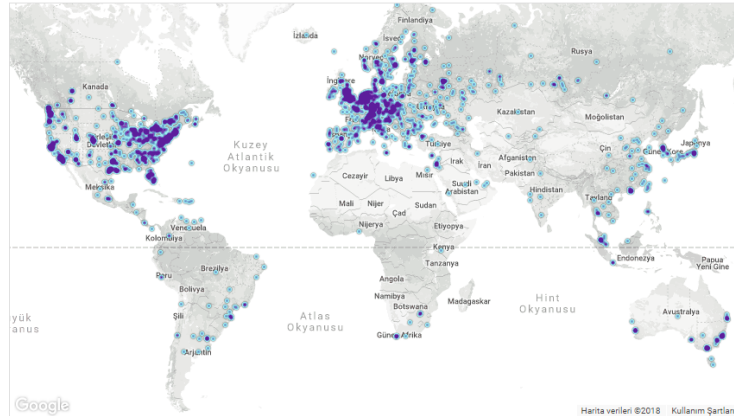
GLOBAL BITCOIN NODES  
DISTRIBUTION  
Reachable nodes as of Sun May 20 2018  
18:05:13 GMT+0300 (Tonga Gündüz Saati).

10231 NODES  
24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2489 (24.33%)
2	Germany	1836 (17.95%)
3	China	801 (7.83%)
4	France	686 (6.71%)
5	Netherlands	491 (4.80%)
6	Canada	374 (3.66%)
7	United Kingdom	367 (3.59%)
8	Russian Federation	362 (3.54%)
9	n/a	340 (3.32%)
10	Japan	215 (2.10%)

More (103) »



Şekil 17: 18 Mayıs 2018 İtibarıyla Dünya Üzerindeki Bitcoin Ağındaki Tam Uçlar

2018 yılı Mayıs ayında, bitcoin sisteminde takribi 10,231 tane tam uç yer almaktadır. Yukarıda bulunan şekilde 18 Mayıs 2018 tarihinde, Bitcoin ağındaki tam uçlar ve bu tam uçların dünya genelindeki dağılımları görülmektedir (Şekil 17’):



#### 4.8.2. Hafif Uç (Lightweight Node)

Tam uçların tersine hafif uçlar, Blok-Zincir'in tümünü indirip, en son durumunu tutmak mecburiyetleri bulunmamaktadır. Hafif uçlar, dijital para cüzdanı şeklinde de nitelendirilirler. Dijital para cüzdanları, tam uçlara istemci şeklinde bağ kurar ve yalnızca kendilerine ait hareketleri ile alakalı dataları talep ederler. Hafif uçlarda, çok daha düşük boyutta disk ve ağ kaynağından yararlanırlar. Blok-Zincir'in yalnızca tek bölümünün indirilmesine yönelik, Basitleştirilmiş transfer teyitleme sistemini kullanırlar. Basitleştirilmiş transfer teyitleme, imzalamış bir bloğun tümünün indirilmesine lüzum olmaksızın, yalnızca ve bahse konu işlemlerin indirilerek doğrulanmasında yararlanan bir yöntemdir.

#### 4.9. Altcoinler

Bitcoin teknolojilerinden yararlanılarak geliştirilen kripto-paralara altcoin ismi verilir. Açık kaynak kodlama yapısına sahip bitcoin, kendisinin peşinden ortaya çıkarılmış olan diğer kripto paralara temel oluşturmuştur. Altcoinler iş ispatı, para arzı ve güçlü anonimlik gibi bazı özelliklerinden dolayı birbirlerine göre farklılaşmış oldukları görülmektedir. (Lifecycle of an Altcoin, <https://www.coursera.org/learn/cryptocurrency/lecture/Zdm9b/lifecycle-of-an-altcoin>, Erişim Tarihi: 11.04.2018).

Alt türev coinler, Btc' nin rakibidir, Btc ile birlikte birlikte öne sürülen düşüncelerin iletmiş formlarıdır. Şu anlık, altcoinlerden hiçbir tanesi, bitcoin kadar büyük boyutlara ulaşmış ve toplumsal zeminde bitcoin kadar yaygın bir kullanım alanına ulaşabilmiş değillerdir. Bitcoin'in kapsamı fazlalaşıp, fiyat farklılıklarındaki oynaklık hafiflediğinde, altcoin'lerin vurguncu bir mantıkla kullanılması ihtimal dâhilindedir.

Altcoin'lerin tanınıp meşhur olmaya başlamasının asıl nedeni, Bitcoin'in gerisindeher hangi bir ülkeye ihtiyaç duymadan çalışabilmesidir. Dijital mevduat sektörünün genel hacmi, 18Mayıs 2018'de yaklaşık olarak 370 Milyar ABD dolarıdır. BTC 142,5 Milyar USD, Ethereum (Eth) 70,7 MilyarUSD, Ripple (XRP) 27 MilyarUSD, Bitcoin Cash (BCH)21 Milyar USD ve EOS 11,8 MilyarUSD ilesektör toplamının ilk beşte yer alan dijital parası olarak göze çarpmaktadır. (<http://www.kriptoparapiyasasi.com/>, Erişim Tarih: 18.05.2018).

Altcoinleri; Para birimi olan altcoinler ve Para birimi olmayan altcoinler şeklinde sınıflandırmakta fayda bulunmaktadır.

**Para Birimi Olan Altcoinler ve Para Birimi Olmayan Alt-Zincirler:** Bitcoin yaklaşıkon dakikada bir eksilen bir fonksiyonla para arzı oluşturmaktadır. Diğer taraftan

örnekleri çoğaltılabilmekle birlikte Litecoin 2,5 dakikada bir, Dogecoin bir dakikada bir para arzı oluşturan altcoin sistemleridir. Bitcoin sisteminde yeni bir blok ilave edilebilmesi için sistemdeki bir madencinin çalışmış olduğunu ispat etmesi ve bunun öteki madenciler tarafından kontrolünün yapılıp onaylanması gerekmektedir. Yapılacak iş ispatı “SHA256” algoritması ile gerçekleştirilir. İşispatında “SHA256” baş bir alternatif olarak "scrypt" algoritması da bulunmaktadır (Andreas, 2014: 325 ).

Bitcoin sisteminde kullanılmakta olan iş ispatı yöntemi Bitcoin ağının güvenliğinin sağlanmasını amaçlamaktadır.

Mevduat terimi bulunmayan Alt-Zincirler mevduat terimi olmamasına rağmen Blok-Zincir sisteminden etkilenme yoluyla meydana getirilmiş sistemlerdir. Bu sistemlerin bir bölümü jeton (token) yada para şeklinde kullanır. Jeton yada para kullanımı ve arzı olsa da asıl amaç bunların kullanılması değildir (Andreas, 2014:330 ).

## BEŞİNCİ BÖLÜM

### BITCOİN VE GENEL KARAKTERİSTİK ÖZELLİKLERİ

#### 5.1. Bitcoin Alımı

Bitcoin alım satımı yapabilmek için ilk önce Bitcoin işlemi yapılan herhangi bir borsadan hesap açılması gerekmektedir. Bitcoin borsalarına üye olunması yapılan bu üyelik işleminin doğrulanması ve bunun peşinden bakiye yüklenmesi gerekmektedir. Yurt dışında ve yurt içinde çeşitli bitcoin borsaları bulunmaktadır. Yurt dışında bulunan bitcoin borsalarına; Binance, Poloniex, Kraken ve Coinbase gibi borsalar örnek olarak verilebilirken Türkiye’de işlem yapan borsalar ise; Bitturk, BTC Turk ve Koinim örnek olarak verilebilir.

Bitcoin alım satımı bitcoin borsalarının yanı sıra bitcoin ATM’lerinden, ticaret yapılması veya birebir ticaret yapılması SQL, PHP, C# yâda JavaScript bilenlere, küçük programlar yazdırılarak, karşılığında Bitcoin ödemesi alınması gibi yöntemlerle de yapılabilmektedir Bitcoin alımı veya satımı yapılabilen bu yöntemlere daha detaylı değinmekte fayda bulunmaktadır.

#### 5.1.1 BTC Piyasaları

Btc tedarik etmenin en basit yöntemi, herhangi bir borsadan TL/YP karşılığı BTC değişiminin yapılması olarak ifade edilmektedir. Milli mevduatla BTC satın alınması sanal para borsalarından yapılabilmektedir. Dijital yada fiziki itibari paralar ile satın alınabilen Bitcoin satın alacak kişi namına önceden tanımlanmış bitcoin adresine gönderilir. Bankalarda yer alan mevduat karşılığında tedarik edilen Btc, sahip olan kişi ya da kuruluşlara önceden tanımlanmış olan sanal para cüzdanlarına aktarılmasını ifade eder. Btc cüzdanında mevduat gözükmemesinin manası, sanal para sitesine Btc gönderildiğinin Blok-Zincir’e eklenmesidir. Diğer para çeşitlerine göre Bitcoin fiyatları çeşitli web adresleri üzerinden (<http://coinmarketcap.com/currencies/>, örnek olarak verilebilir) istenilen anda gerçek zamanlı olarak takip edilebilir. Hukuksal sorunlar sebebiyle hala küresel çapta faaliyette bulunan herhangi bir Bitcoin borsası bulunmamaktadır. Web tabanlı çeşitli sitelerden Bitcoin fiyatlarının takibi ve hangi devlette hangi Bitcoin borsasının faaliyette bulunduğu takibi de yapılabilmektedir. Bitcoin borsalarında her borsa kendine özgü işlem masrafları alabilmektedirler. Çok sayıda borsa kendi bünyelerinde satıcıları ve alıcıları bir araya

getirensatım-alım sistemi çalıştırmaktadırlar. (Prableen Bajpai, "A Look At The Most Popular Bitcoin Exchanges", Investopedia, Erişim 17.04.2018).

Bitcoin borsaları, sistemsal olarak üretildikleri devletin kontrolüne bağlıdırlar, bu manada borsalar yatırım yapan kişilerden bir takım kişisel verileri talep edebilmektedirler. Birtakım Bitcoin borsaları Bitcoin'lerini müşterileri adına tutsalar da, güvenliğinin temin edilmesi açısından kişilerin, kendilerine ait dijital paralarını firmalarına has sistem içerisinde tutmaları güvenli olmaktadır. Mevduat karşılığında alınan sanal paranın gerçek veya tüzel kişilerin Btc cüzdanlarına transfer edilebilmesi için, sanal para borsalarına Bitcoin hesaplarının verilmiş olması icap etmektedir. Kişilerin kimlik bilgileri ve cüzdan adreslerini ellerinde tutan Bitcoin borsaları, kişilerin anonimlik düzeylerinin azalmasına neden olur. Bu durumu başlarında atabilmek için, bir başka Bitcoin adresi daha oluşturulur, akabinde mevcut cüzdandaki Bitcoin'lerin yeni oluşturulan cüzdan adresine nakledilerek, anonimlik düzeyi tekrardan yükseltilebilir (Brand, 2016: 208).

Bitcoin'lerin denetiminin ve düzenlenmesinin hiçbir güç tarafından yapılamasından dolayı Bitcoin borsalarında da bu şekilde sorunlar bulunmaktadır. Söz gelimi Bitcoin borsasındaki herhangi bir hesabın çalınması durumunda, borsanın sorumluluklarının neleri ihtiva ettiği günümüzde de üzerinde çok sayıda tartışmanın bulunduğu bir alandır.

### **5.1.2. Birebir Ticaret Yoluyla Bitcoin Alım Ve Satımı**

Ticaret yapan kişiler yönünden Bitcoin sağlamanın şüphesiz bilinen yöntemi, verilecek hizmetlerin veya satılacak malların karşılığının bitcoin olmasıdır. Birçok dünya devletinde hem fiziki hem de sanal ortamda bitcoin karşılığında mal ve hizmet satılması veya her geçen gün yaygın hale gelmektedir. Aşağıdaki şekilde ödemelerini Bitcoin ile kabul etmiş olan bir işletme bulunmaktadır.



**Şekil 18:** Bitcoin Ödemesi Kabul Eden Bir İşletme

Çok büyük çapta plasman gerektirmeden, “Bit pay” veya benzeri yöntemlerden yararlanarak bitcoin kabul eden interaktif ticaret siteleri, dükkanlar yada klasik iş yerleri de bulunmaktadır.

Sanal ticarete satıcı ve alıcı arasındaki problemler, “PayPal ve Ebay” benzeri ödeme yöntemlerinde tahsilatın iadesiyle giderilebilmesine rağmen, Btc yapısında faaliyette olan metotlarda tahsilatın iadesi mevzu bahis olmazken, satıcıyla alıcı nazarında ilk elden aktarımından ziyade, bir güvenilir bir başka Bitcoin adresine gönderimin yapılması, bu meselelerin halledilmesinde faydalı olacaktır (Brand, 2016: 208).

Bitcoin ticaretinde diğer bir şekli de müzayedeler (açık artırma) yapmaktır. Greenpeace ve Kızılhaç gibi dünya çapında bilinirliği olan örgütlere Bitcoin bağıışı da yapılabilmektedir. Nepal’de meydana gelen depremin peşinden “Nepal Yardım Fonu’na” direkt Btc hibe etmiş kişiler bulunmaktadır. Konaklama rezervasyonunda bulunmak için, “<https://btctrip.com/>” benzeri internet siteleri bulunmaktadır. Diğer taraftan, cüzdan da yer alan kişisel verileri vermeden, legal şans oyunları ve gazino oyunlarının oynanması da imkân dâhilindedir. “<https://www.vaultoro.com>” ve “<https://bitgold.com>” Gibi web sitelerinden, Altın ve Bitcoin değişimi yapılması mümkündür. Ayrıca, birtakım ülkelerde birtakım fatura ödemeleri de Bitcoin ile yapılabilmektedir (Brand, 2016: 208).

Birebir Ticaret yolu ise bitcoin sağlamanın başka bir yöntemi, Bitcoin satışında bulunacak kişiden bitcoinin satın alacak kişinin direkt almasıdır. Bitcoin’i alacak olan ile Bitcoin’i satacak olan kişileri bir araya getiren borsa gibi üçüncü bir muhatap bulunmadığından, işlemler güvenli olması temelinde meydana getirilmektedir. Söz gelimi;

Bitcoin'i alacak olan kiři Bitcoin'i satacak olan kiřinin Bitcoin transfer edeceđine inanarak satacak olan kiřiye para havalesi yâda EFT ile önce para transfer etmesi yâda yüz yüze bir araya gelmeleri icap etmektedir. Doğrudan doğruya satıcı ve alıcı tablolarını ve daha evvelinde meydana getirdikleri işlemler açısından güven derecelerini "<https://geminicomveyahttps://kraken.com>" gibi web sitelerinden takip edilebildikler söylenebilmektedir.

### 5.1.3 Bitcoin ATM'leri Yoluyla Bitcoin Alım Ve Satımı

Günden güne daha çok sayıda kullanılan, Bitcoin ATM' lerinden Bitcoin satın alınabilmektedir (Şekil 19). [coinatmradar.com](http://coinatmradar.com)veya [coindesk.com](http://coindesk.com) Web sitelerinden Bitcoin ATM'lerinin hangi yerlerde bulunduđuna ulaşılabilir. 2013 yılında ülkemizde, ilk Bitcoin ATM'si Atatürk Havalimanı'nda adet hizmet vermeye başlamıştır. Bitcoin ATM'leri çođunlukla, kredi kartı veya nakit olarak Bitcoin adreslerine, Bitcoin nakli yapan cihazlardır. Bitcoin ATM'leri, Bitcoin adresinin "QR" koduyla da hizmet verebilecek teknolojik alt yapıya sahiptirler, bunun neticesinde karmaşık ve uzun bir yapısı bulunan Bitcoin adreslerinin akılda tutulmasına yâda tıklanmasına ihtiyaç duyulmaz.



Şekil 19: Bir Bitcoin ATM'si

### 5.1.4. Diğer Alım Satım Yöntemleri

Bilgisayar programlama dillerinden SQL, PHP, C# ya da JavaScript hakkında bilgi sahibi olanlara, ufak bilgisayar yazılım programları oluşturmak suretiyle ödöl olarak Btc verilebilmektedir. ( Brand, 2016: 208 ).

Birtakım web siteleri ise, tanıtımlarını takip eden yâda anket şeklinde sitenin gereksinimi olan verileri elde edenlere, reklam masraflarında düşük meblağlarda Bitcoin verdikleri bilinmektedir. Örnek vermek gerekirse "[www.bitcointalk.org](http://www.bitcointalk.org)" Forum sitesinde, düzenlenen imza kampanyasında yapılan olumlu açıklamalara, diğer üyeler tarafından dapoitif açıklama yapılması durumunda, ilgili kişiye Bitcoin hediye verilmektedir ([https://en.Bitcoin.it/wiki/Bitcoin\\_faucet](https://en.Bitcoin.it/wiki/Bitcoin_faucet), Erişim 22.03.2018).

### **5.1.5. Bitcoin Piyasası ve Para Arzı**

Dünyanın çok sayıda ülkesinde, Bitcoin'den vergi alınmamaktadır. Bu sebeple, halen sürmekte olan ve faaliyete geçecek programlara, Btc biriktirerek global bir ödenek oluşturmak çok fazla yararlı olacaktır. Bunun gibi programların hukuki zemini hala açıklığa kavuşturulmamıştır. Btc ticaretinin iadesi imkânsız olduğundan, bu sistemler dolandırıcılık, hile ve kanunsuz faaliyetlere müsait bir ortam oluşturmaktadır. Herhangi bir altcoin yada btc işletmesi, bir proje için ilave kaynak yaratmak maksadıyla, "IPO-Initial Public Offering" (ilk halka arz) yapabilir. Sermayedarların payları olmuş olur, gelir ödemesi elde edebilirler (Barnato, "World's first bitcoin mining IPO falls short", CNBC, Erişim 15.04.2018).

Hala üretim süreci oluşmamış Btc' nin alt kolu olarak dizayn edilmiş olan alt türev coinler, onları destekleyen ve yatırım amacıyla para bağlayan kişilere önerilebilir. Bu durum söz konusu coinlerin daha jeton (ICO) döneminde ucuza alınıp sanal para evresine ulaştığında ise pahalıya satılabilmesi için bir avantaj oluşturabilir. (Barnato, "World's first bitcoin mining IPO falls short", CNBC, Erişim 15.04.2018).

Btc de üretim süreci zorlaşarak devam eder. Arz edilen btc miktarı iki yüz on bin blokta yüzde elli azalacak şekilde programlanmıştır. Buna bağlı olarak arz edilen nakit miktarı da düşerek devam ettiğinden dolayı bu sistemin madencilik olarak ifade edilmesini sağlamıştır.

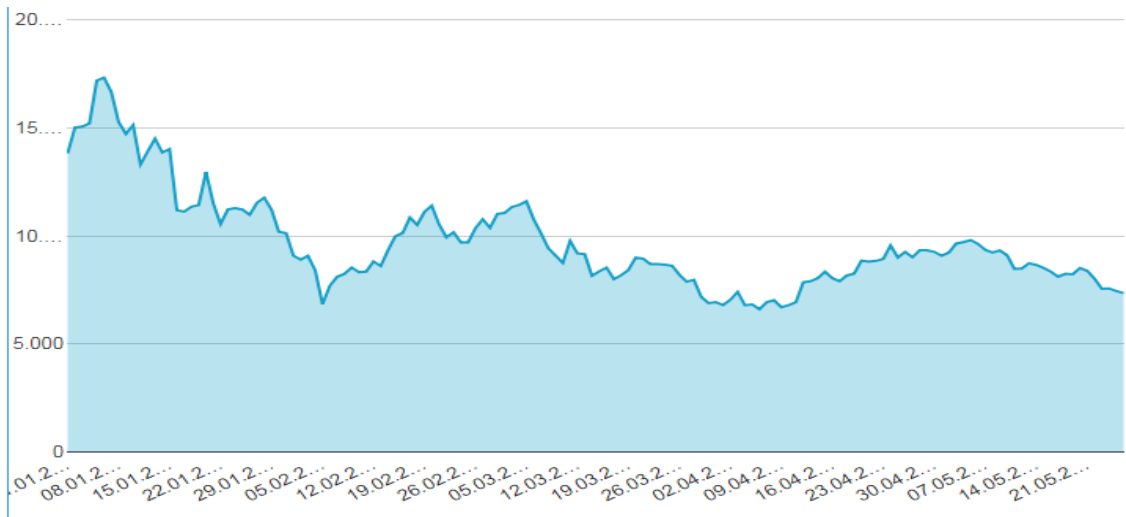
2018 senesinde üretimde başarılı olan kişilere tahsis edilen bedel 12,5 Bitcoindir. Bitcoin basımı 2140 yılında son bulacak şekilde programlandığından dolayı üretim yapan kişiler, hâsılatlarını yaptıkları işlem hizmetlerinden temin edeceklerdir. (Controlled supply, [https://en.bitcoin.it/wiki/Controlled\\_supply](https://en.bitcoin.it/wiki/Controlled_supply), Erişim Tarihi: 27.04.2018).

**Tablo 3.** Bitcoin Alış & Satış Komisyonları

30 günlük ticaret büyüklüğü (TRY)	Arz miktarı	Talep miktarı
0 – 100.000,00	%0,20 (0,0020)	%0,30 (0,0030)
100.000,00 - 500.000,00	%0,15 (0,0015)	%0,25 (0,0025)
500.000,00 - 1.000.000,00	%0,10 (0,0010)	%0,20 (0,0020)
1.000.000,00 - 5.000.000,00	%0,08 (0,0008)	%0,18 (0,0018)
5.000.000,00 - 10.000.000,00	%0,06 (0,0006)	%0,12 (0,0012)
10.000.000,00 - 50.000.000,00	%0,04 (0,0004)	%0,10 (0,0010)
50.000.000,00+	%0,02 (0,0002)	%0,08 (0,0008)

**Kaynak:**<https://www.btcturk.com/yarim/komisyonlar>, Erişim Tarihi:30 Nisan 2018.

Sanal para üretimi merkezi bulunmayan değişim yöntemleri ile ilişkilendirilebilir. Üretim olmazsa yalnızca Btc basımı sonlanmış olmaz btc ticareti de durma noktasına gelecektir. Laszlo lakap adını kullanan bir kullanıcı, 22 Mayıs 2010'da Bitcoin ile 2 tane pizza siparişi vermiştir. Almış olduğu ürünü diğer Btc sahibi, “10.000 Bitcoin” mukabilinde, Dominos firmasından Laszlo namına temin edip Laszlo'nun evine yollamıştır. Btc' nin kuruluşundan bu yana ilk kez değişim argümanı şeklinde kullanıldığı tarih 2010 yılı 22 Mayıs'tır. Günümüzde 22 Mayıs Dünyanın birçok yerinde “Laszlo'nun Pizza Günü” şeklinde kutlanılmaktadır. Btc' nin kıymeti, bilumum ürün, emtia ve mevduatta olduğu gibi, arzile talebin eşitlendiği bölümde meydana gelir. Btc' nin kıymeti, kabul edilebilirliği, yaygınlığı, jeopolitik konumu, destekçilerin coinlere olan inancı, reel yaşamda tahsil amacı olarak kullanılması ve piyasanın o zamanki etkinliğiyle ilişkilidir. (Elliot, 2008).



**Şekil 20:** Bitcoin 2018 Yılı Fiyat Grafiği.

**Kaynak :**<http://www.bitcoinfiyati.com/2018-yilinda-btc-fiyati-ne-kadardi.html>, Erişim Tarihi

27.04. 2018



27 Mayıs 2018 itibari ile, 2018 'de ortalama btc fiyatı 9.679,48 \$, 2018 en düşük btc fiyatı 6.603,88 \$, 2018 en yüksek btc fiyatı 17.319,19 \$, yıllık değişim yüzdesi % -46,837 btc, 2018 yılbaşı btc fiyatı 13812,18 \$, 2018 yıl sonu btc fiyatı 7342,9083 \$'dır.

## 5.2. Bitcom'in Yasal Statüsü ve Btc' nin Kara Para Aklama İle İlişkisi

Bitcoinle kara para aklama sorununa değinmeden önce dünyada bitcoinin ülkeler nezdindeki yasal statüsüne bazı örnekler vererek değinmek durumun anlaşılabilmesinde faydalı olacaktır.

Dünyada bir çok alanda liderliğini sürdüren A.B.D miktar bazında en fazla kripto parayı bulundurmakta ve dünyadaki bitcoin ticaret hacminin lideri konumundadır. Çok sayıda devlet, şifreli paraların hukuksal düzenlenmesi mevzusunda Amerika Birleşik Devletleri takınacağı tutumu ve bu tutumun neticelerin neticelerini izlemektedir.

Avrupa ülkelerine bakıldığında yurttaşlarına Blok-Zincir tabanlı ilk dijital-oylama yöntemini getiren ülke Estonya'dır. Estonya, bu teknolojiyi sağlık, bankacılık ve vatandaşlarının yönetime katılmalarında dahi faydalanmayı düşünmektedir. Estonya'nın haricinde İsveç ve Danimarka ülkelerinde nakit kullanımının yerine dijital para kullanımını isteyen ülkelerdir. İsveçli Finans Denetim Merkezi, dijital parayı yerel para gibi bir değişim ve tahsilat yöntemi olarak kullanılmasını kanunlaştırmıştır. Hollanda ve Finlandiya'da bitcoin'le alışveriş yapılabilen işletmeler bulunmaktadır. Finlandiya hükümetisanal parayı (BTC' yi) mali yapı içerisinde kullanılan bir değişim sistemi olarak ifade etmiştir. Btc' yi ve tedarik edilmesini KDV alınmadan yapılabileceğini duyurmuştur. Bu ülkelerin dışında Avustralya, Birleşik Krallık, Güney Kore Kanada vb. gibi daha birçok ülkede bitcoin'in popülerliği günden güne artmaktadır. Bitcoin kullanımının arttığı bu ülkelerin yanı sıra, Ekvator, İzlanda, Bolivya, Tayland, Bangladeş, vb. gibi ülkeler ya bitcoin'e uzak durmuş yâda yasaklamışlardır.

Bitcoinin küresel bazdaki yasal statüsüne değindikten sonra yakın zamanlarda birçok yazılı ve görsel alanda konu olan bitcoin ile kara para aklama konusuna değinmekte fayda bulunmaktadır.

**Kara para aklama**, yasalara uygun olmayan yollarla kazanılan fakat dışardan bakıldığında legal yollardan elde edildiği görüntüsü verilmek istenen malvarlığı karşılığının, bir takım kamuflej metotlarından yararlanılarak kaynağının bilinmesinin zorlaştırılması veya engellenmesidir (Rebscher ve Vahlenkamp, 1988: 112-170).

Çok sayıda devletin müşterek problemi olan “kara para” iki kaynaktan doğar. Birincisi; devletin ulusal düzeydeki ekonomi politikası, vergilendirme politikaları vb. gibi mevzuatlarının dışarısında tutulmasını sağlayarak bir artırım yaparak bunun peşinden türlü işlemlerden bir bölümünün faturalandırılmamış satışa dayalı kazancı olabileceği gibi, uyuşturucu türevi maddeler gibi yasaklanmış kanunsuz kazançlarıdır. Kara parayı meydana getiren işlem ve nakde çevrilmeleri ülke içinde ve ülkenin ulusal parasıdır.

İkinci kara para işlemi ise uluslararası çaptadır. Yani kara para, uluslararası illegal finans piyasalarında bulunan kaynaklardır. Bunların arasında; illegal silah satışları, uyuşturucu satışlarından sağlanan gelirler, insan ticareti, fuhuş, kalpazanlık ve sahtekarlık, ülkelerden illegal çıkan sermaye, kumar, zehirli ve radyoaktif maddelerin ortadan kaldırılması gelirleri gösterilebilir.

Kara para banka yönetmeliğinin çok zayıf olduğu az gelişmiş ekonomilerde, finansal sisteme zarar verebilir. Halkın güvenini sarsabilir. Kara paranın artmasıyla beraber yapay olarak kıymetli mal fiyatları da artabilir yada azalabilir. Kar oranlarını ya da döviz kurlarında dalgalanmalara neden olabilir.

**Bitcoin ile kara para aklanmasını** tespit etmek sebebiyle evvela kara para aklama sürecini ve basamaklarını bilmenin yararlı olacağı kanaatindeyiz. Kara para aklama süreci genellikle bir takım karmaşık işlemlerden meydana gelse de çoğunlukla 3 ana aşamadan meydana gelmektedir.

**Kara para aklamada birinci aşama** paranın fiziksel yatırıma dönüştürülme aşamasıdır. Klasik yatırım işlemi paranın yerel banklara yada diğer finansal kuruluşlara yatırılması ile oluşmaktadır. Yâda paranın ülke sınırlarında geçirilerek yabancı banka hesaplarına yatırılması, kıymetli maden, uçak, kıymetli taşlar vb. gibi değeri yüksek olan mal alımında kullanılması ve bunun ardından satın alınan bu malların banka havalesi veya çek gibi ödeme karşılığı satılmasıdır. Suçtan sağlanan kazançların mali konjonktüre ilavesidir. Bu hususi illegal fonların dijital bir ortamdaki finans hesaplarında giriş çıkışlar oluşturarak ya da devralma bölümleriyle mali bir konjonktüre tanıtılması durumunu meydana getirmektedir.

Bitcoin ile kara para aklamada, para denetime tabi olmayan bir finansal kuruluşa kişisel bilgisayar aracılığı ile yâda kredi kartı ile zahmetsizce yatırılabilir.

**Kara para aklamada ikinci aşamada;** yatırılan paranın ağlar üzerinden transfer edilmesi, hisse senetleri, tahviller vb. gibi parasal araçlar ile değiştirilmesi, kıymetli malların ve bu parasal araçların elden çıkarılması gayrimenkul özellikle turizm işlemlerine yatırılması gibi olayları kapsar. Offshore olarak kayıtlı olan şirketlerde bu işlemlerde büyük rol oynar. Sanal para sisteminde “yatırım” işlemleri kişisel bilgisayar aracılığı ile yapılabilir.

Çoğunlukla banka işlemlerinin takibini sağlayan hiçbir basılı kayıt olayı yoktur. Diğer taraftan sanal para sistemleri hiçbir sınırı olmayan bir sistem üzerinde fonların anında transferine imkân vermektedirler. Mali konjonktüre enjekte edilmiş paranın hareketini yok etmek amacıyla işlemlere yer verilmesidir. İlegal fonların mali bir yapı içinde yer değiştirmesi ve pay edilmesi biçiminde meydana gelmektedir. Bu tarz finansal konjonktürlerde, finans kuruluşları ve firmalar gibi aktörleri içine alan karmaşık hareketlerin yer almasıyla mümkünken; dijital alemde bir sürü bilinmeyen operasyonla BTC gönderip almak gayet basit bir iştir.

**Kara para aklamada üçüncü ve son aşama;** illegal yollardan elde edilen paraların legal hale getirilmesidir. Çoğunlukla başvuru yöntemleri içerisinde hayali ihracat faturaları düzenlemek veya ifa edilen ihracat işlemlerinde faturaları olması gerekenden daha yüksek tutarla düzenlemek, paravan şirketlerden borç almak vb. gibi. Üçüncü aşama en tehlikeli aşamalardan biridir. Paranın, orijinalinin olumlu bir biçimde saklanması akabinde, gerçeğine yakın ve merkezi tespit edilebilir bir unsur neticesinde kazanılmış hissi uyandıracak biçimde geri alınmaktadır. Bu durum genellikle kara parayı tutarak legal firmalar oluşturulması biçimindeki haberlerde yer almaktadır. Söz konusu firmaların kazanımı hususunda belirtilen nakit, devletin ekonomi kuruluşları ile diğer ekonomi aktörleri eliyle yasal bir iktisadi icraat neticesinde kazanılmış nakit olarak nitelendirilmektedir.

Bitcoin’de ise kişisel bilgisayarlar aracılığı ile hiçbir finansal kuruluşun hizmetlerine başvurmadan yatırımları için ödeme yapılabilir yâda varlık satın alınabilir.

Kara para aklama veya hukuki deyimle taksirli elde edilen servetin değerini aklama eylemi “5237 sayılı Türk Ceza Kanunu’nun 282. Maddesinde” cezayı gerektiren işlemler bütünü olarak tanımlanmıştır. Kara para aklama işleminde önce cezayı gerektiren eylemden kazanılmış olan emtia kıymetinin (kara para) bulunması gerekmektedir. Kara para aklamada malın varlık değeri ekonomik sistem içerisinde bir takım muamelelerden sonra malın kaynağını meydana getiren taksirle bağının yitirilmesi ve yasal bir para izlenimi kazandırılması “aklama” aşamasını meydana getirmektedir. Sağladığı işlem pratikliği, meşakkatsizliği ve izlenebilmesi güç olması sebebiyle aklama aşamasında Bitcoin sisteminden geniş çaplı yararlanılmaktadır. Bir kara para aklama işlemine mevzu teşkil eden mevduat (kara para) teknik bir ifadeyle fiziki paradır. Sanal mevduatın ceza gerektiren işlemin kazancı olduğundan çok ta imkân dâhilinde değildir. Nedeni şu ki suç kabul edilen faaliyetlerden kazanılan para genellikle nakit para biçimindedir ve kuşkusuz narkotik madde tüketimi yakın bir zamanda bile dışardaki satıcılara btc vererek sağlanamayacaktır (Hermann, 2011: 42.).

Lakin bedeli anonim elektronik değer birimleri ile verilebilen yasa dışı faaliyetlerin yeni ortamlarını illaki oluşturacaktır. Bunun gibi suç olarak ifade edilen tekliflerin kıymetinin tahsil edilmesinde, kullanıcısı belli olmaması nedeniyle özellikle Bitcoin ve türevi olan elektronik paralar elverişli bir vasıtaadır (Keser Berber, 2002: 108).

Günümüz ekonomik sistemlerinde para transferi yapabilmek için bir bankanın aracılığına ihtiyaç varken, bitcoin bu araçları ortadan kaldırmakta ve bir kullanıcıdan ötekine direkt bitcoin gönderebilmektedir. Bu husus kara para aklama konusunda dikkate değer bir avantaj gibi görünmektedir. Birçok akademik çalışmanın yanında hukuki dayanak ve gizli birimlere ilişkin belgelere göre, kara para aklanmasında Btcileri düzeyde kullanılmaktadır. 2012 senesinde “The Economist’de Bitcoin’in” zirvede olma sebebi “şüpheli online ticaretteki rolüne” endekslenmiştir. Gene yakın zamanlarda FBI’ın eroin, esrar gibi zararlı maddelerin alış-verişinde ustalaşmış olan bir Btc şirketinin faaliyetlerine son verdiği öğrenilmiştir. Oyun alanları ile internet dünyası da para aklama konusunda çok sayıda boşluklar arz etmektedir. Çünkü bahse konu kanallardan yararlanılarak gerçek mevduat merkezlerinin herhangi bir denetim sistemine bulaşmadan dijital kredilere dönüştürülmesi olanaklı duruma dönmektedir. Siber ortamda mali düzenin kontrolsüzleşmesi, sanal mevduat kullanımı aklama operasyonlarını ileri düzeyde müsait hale getirirken, eylemin ispatlanmasını zorlaştırmaktadır. Diğer taraftan siber aklama fenomeni için herhangi bir iyileştirme olmaması da bu fenomenle baş edebilmeyi güçleştirmektedir. “5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun”; başta finans kurumları olmak üzere değişik sektörlerde icraatta bulunan kuruluşların, kişilerin özlük bilgilerinin tespit edilmesi ve anormal işlemlerin bildirilmesi durumunu içermektedir.

Türkiye’de elektronik mevduat piyasalarına dair hususi bir kanun ve bu kapsamda meydana getirilmiş dijital para kurumu olmadığından Bitcoin ve diğer kripto para türevleri “5549 sy. kanun” maddelerine bağlı değildir. Sanal mevduat birimlerine dair yasal düzenleme olması durumunda sanal para piyasaları da 5549 sy. Yasa maddelerine dahil edilecektir. (Yurtçiçek, 2015: 211).

Genel itibari ile Bitcoin kara para aklamada kullanılmaktadır.

### 5.3.Bitcoin' inAvantajları ve Dezavantajları Nelerdir?

#### Avantajları:

- **Enflasyon Riski Düşüktür:**

Enflasyona neden olan etkilerden biri de tedavüldeki reel para arzlarındaki artıştır. Tedavüldeki para arzı ile enflasyon doğru orantılı olarak arttırır. Ancak bu sistem Bitcoin için geçerli değildir. Çünkü Bitcoin sistemi, sonu olan bir sistemdir. Teknik tasarımı itibariyle maksimum 21 milyon adet Bitcoin üretilebilir. Dolayısıyla Bitcoin'in enflasyon riski çok düşüktür.

- **Çökme Riski çok düşüktür.**

BTC sistemi herhangi bir hükümet politikasına tabi olmadığından dolayı çökme riski çok düşüktür.

- **Güvenli, Basit ve Ucuz olarak nitelendirilebilir.**

Btc sisteminde ödemeler herhangi bir aracı olmadan (P2P) transferler kişiden kişiye seri ve basit bir şekilde yapılmaktadır.

- **Taşıması kolay**

Milyarlarca dolar değerindeki bitcoinlerinizi küçük bir hafıza kartında bile taşıyabilirsiniz. Bunu nakit para ile ya da başka bir sistem ile yapmak imkansız sanırım.

#### Dezavantajları:

- **Kaybetmesi Riski:** Kredi kartınızı kaybettiğinizde yada banka hesabınız başka birisi tarafından ele geçirildiğinde, ilgili banka yetkililerini arayarak durumu anında kurtarabilirsiniz. Hatta yetmezse polisi bile devreye sokup kaybınızı giderebilirsiniz. Ancak Bitcoin için aynı şeyler geçerli değil. Bitcoin sisteminde; kaybettiğimiz bitcoinleri ve ya ele geçirilen Bitcoin cüzdanınızı geri almak için kullanabileceğiniz bir mekanizma yok. Bunun önüne geçebilmek için izleyebileceğiniz en iyi yöntem, Bitcoinlerinizi internet bağlantısı olmayan hard disklerde saklamak olacaktır.
- **Alıp satmak zor:** Taşıdığı risklerden dolayı Bitcoinlerinizi bir ürün satın alır gibi alamıyorsunuz. Bitcoin satın almak veya bitcoinleriniz satmak için birçok servis bulunuyor ancak bunu gerçekleştirmek o kadar da kolay değil. Her geçen gün geliştirilmesine rağmen (Bitcoin ATM'leri açılmaya başlandı), işler reel para birimlerinde olduğu kadar kolay ilerlemiyor.
- **Hala çok yeni:** Bitcoin sisteminin 2009 yılında kurulmuş olması; yani hala yeni bir teknoloji olması, yeni Bitcoin rakiplerini de beraberinde getirebilir; hatta Bitcoin sisteminde büyük açıklıklar bulabilen yeni teknolojiler hala geliştirilebilir.

- **Harcama alanı darlığı:** Ödeme sistemi olarak Bitcoin sisteminin de kullanıldığı çok fazla yer yok. Her ne kadar gelişim aşamasında olsa da, şu anda Bitcoin sahibi olmanın en büyük amaç; yatırım.
- **Değişken:** Bitcoin'in değer grafiğine baktığımızda herkesin aklından Bitcoin yatırımı yapmak geçebilir, ancak Bitcoin değeri nasıl hızla yükseldiyse düşme riski de o kadar fazla. Dolayısıyla yapılacak olan yatırımların dengeli ve düşünerek yapılması gerekmektedir



## ALTINCI BÖLÜM

### SONUÇ

Teknolojik gelişmeler çerçevesinde geleneksel para sistemi yani madeni veya kağıt para yerini elektronik ödeme araçlarına geçiş eğilimi göstermiştir. Ödeme aracı olarak kullanılan para günümüzde parasal değer ifade eden farklı araçlar ile yer değiştirmeye başlamıştır.

İnsanların sanal paralara olan yaklaşımlarını incelediğimiz bu çalışmada, söz konusu sanal paraların hangi şartlarda ortaya çıktığı, gelişim evresinde ne gibi aşamalardan geçtiği, insanlar arasında hızla yayıldığı, para transferlerindeki kolaylığın insanların hayatlarına nasıl etki ettiğine vurgu yapılmıştır. Bir bitcoin tüketicisi ve alım satımı yapmakta olan Semih Başaran ile yapılan görüşme sonucunda, sanal paraların dünya üzerinde, insanlar arasında hızlı bir şekilde yayılmasının en önemli nedeninin gelişmekte olan ve gelişmiş olan teknolojik yeniliklerin yanında görsel ve yazılı medyanın çalışmalarının (reklamlarının) etkili olduğu ifade edilmiştir. Ayrıca trampa ekonomisinden bugüne kadar birçok para ve ekonomi sistemi kullanılmış olup gelen her yeni sistem bir önceki sistemin eksikliğini giderilmesi şeklinde ortaya çıktığı ifade edilirken söz konusu sanal paraya dayalı ekonomik sistemde mevcut ekonomik sistemin eksik noktalarının tamamlamak ve gelişen teknolojik yeniliklere adapte olmak şeklinde geliştiği tahmin edilmektedir.

Türkiye’de bulunan yerleşik kişilerin sanal paralar ile alım satım yapmak istemesi ve bu konuda bir muhatap arayışı içinde olmaları Semih Başaran’ın sosyal medya grupları vasıtasıyla çok geniş kitlelere hitap etmesine olanak sağlamıştır.

Sosyal medya grupları (Facebook, Twitter ve Telegram), Bitcoin ve diğer sanal paraların insanlar arasında hızla yayılmasına ve market hacmini hızla genişlemesine uygun zemin hazırladığı Semih Başaran ile yapılan anketle anlaşılmıştır. Bu bağlamda sosyal medya organlarının bilgi paylaşımında ve iletişim ağında sağladığı kolaylık birçok alanda olduğu gibi sanal paraların gelişimi geleceği ve insanlar arasındaki bilinirliğinde de büyük kolaylıklar sağlamaktadır. Yapılan anket çalışması neticesinde sanal paralarda yaşanan iniş ve çıkışların olumlu olumsuz etkilerinin minimize edilmesi için sosyal medya grupları vasıtasıyla geniş kitlelere ulaşıldığı belirtilmiştir.

Ayrıca yapılan görüşme neticesinde çıkarılan bir diğer sonuç ise, Türkiye’de bitcoin alım satım yapan şahısların ‘Aversion to risk’ (riskten kaçınma) durumlarının oldukça düşük seviyelerde olduğu görülmektedir.

Bir diğerk sonuç ise Türkiye’ de kısa vadede hızlı ve çok sermaye elde etmeye imkan sağladığı için bitcoinin insanlar arasında bu kadar hızlı yaygınlaştığı ve işlem hacminin artmasına olanak sağladığı vurgulanmaktadır. Başka bir deyişle bitcoinin tercih edilmesinin arkasında fiyat oynaklığının sebepleri yatmaktadır. Yüksek risk yüksek kazanç anlamına geldiği için risk almaktan korkmayan ve asimetrik bilginin var olmasından endişelenmeyen alıcılar bitcoin üzerinden işlem yapmayı tercih ettikleri anlaşılmaktadır.

Günümüzde bitcoin kullanımının önündeki en büyük engellerden biri bitcoin ile gerçekleştirilen işlemler yönünden sağlıklı ve yasal bir zeminin olmaması veya bazı ülkelerde yeni yeni oluşturulmaya çalışılmasıdır. Bitcoin ile gerçekleştirilen ödemeler net bir biçimde kendine özgü yasal çerçeveden ve öte yandan tarafların hak ve sorumluluklarını düzenleyen kanunlardan yoksun bulunmaktadır.

Bitcoinin gelişimi ve geleceği ile insanlar arasında bilinirliğinin artması Satoshi Nakamoto’ nun ilk başta koymuş olduğu kurallara bağlı olduğu düşünülmektedir. Kendi kurallarına bağlı olma kapasitesi geleceğini başarıya ulaştırmada önemli bir rol üstlendiğini düşünmekteyiz.

Ancak bitcoinin arkasındaki şahıslar ya da kurumlar net olarak bilinmemekle birlikte sınırlı sayıda üretimi (21 Mio adet) yapılması beklenen btcnin ne kadarlık kısmının yapılacağı ve üretim sürecinin tamamlanmasının akabinde tekrardan üretim yapılıp yapılmayacağı yönünde kesin bir kanıt bulunmaması söz konusu sistemin tartışılması gereken bir noktası olarak göze çarpmaktadır. Bu durumda söz konusu sisteme duyulan güven de tartışma konusu olacaktır.

Çalışma sonucunda Bitcoinin ortaya çıktığı andan günümüze değin çok mesafe kaydettiği, mevcut zaman zarfında güvenilirlik konusunda soru işaretleri taşıması sonucuna ulaşılsa da gelişimini devam ettiren bir ivme içerisinde olması henüz dünya genelinde tam anlamı ile ekonomi yönetimleri tarafından kabul edilmediği, konvansiyonel paranın yerini alamayacağı da ayrıca ifade edilmektedir. Bu gerçeklerin yanında yüz yüze değişim işlemlerinde konvansiyonel paranın sağladığı pratik işlem kabiliyetini taşımadığı görülmektedir.

Bitcoin’ in anonim bir yapıya sahip olması, belirli bir hukuki dayanağının bulunmaması, dünya genelinde tümüyle kabul görmemiş olması, takibinin zor olması ayrıca kontrol mekanizmasının eksikliği gibi nedenler bir araya geldiğinde yasa dışı işlemlerin, illegal faaliyetlerin gerçekleşmesi için uygun bir zemin oluşturacağını düşünmekteyiz.



## KAYNAKÇA

Andreas, M. A.(2014). *Mastering Bitcoin*. O'Reilly.

Ateş, B. A.(2016). *Kripto Para Birimleri, Bitcoin ve Muhasebesi*. Çankırı Karatekin Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi, Çankırı.

Barber, S., Boyen, X., Shi, E. ve Uzun, E. (2012). *Bitter To Better—How To Make Bitcoin A Better Currency*. In *Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg.

Barnato, K. (2016). *World's first bitcoin mining IPO falls short*. CNBC, Erişim (15.04.2018).

BDDK, Duyurular, Basın Açıklamaları Hakkındaki Bildiri. (2018). *Bitcoin Hakkında Basın Açıklaması*.[https://www.bddk.org.tr/websitesi/turkce/duyurular/Basin\\_Aciklamalari/12574bitcoin\\_hk\\_basin\\_aciklamasi.pdf](https://www.bddk.org.tr/websitesi/turkce/duyurular/Basin_Aciklamalari/12574bitcoin_hk_basin_aciklamasi.pdf), (Erişim 30.04.2018).

Berber, K. (2018). *İnternet Üzerinde Yapılan İşlemlerde Elektronik Para ve Dijital İmza*, 108. <http://coinmarketcap.com/>.(Erişim 14.03.2018).

Bernstein, D.J. (2009). *Introduction to post-quantum cryptography*.Erişim (25.05.2018).

Bitcoin Developer Guide. (2018).<https://bitcoin.org/en/developer-guide#block-chain>. Erişim (11.05.2018).

Bitcoin Address. (2018).[https://en.bitcoinwiki.org/wiki/Bitcoin\\_address](https://en.bitcoinwiki.org/wiki/Bitcoin_address). Erişim (25.05.2018).

Bitcoin For Everyone Individuals. (2018).<https://bitcoin.org/en/bitcoin-for-individuals>. Erişim (01.05.2018).

Block Height And Forking. (2018). <https://bitcoin.org/en/developer-guide#proof-of-work>. Erişim (11.05.2018).

Bloomberght. (2018).*Bitcoin'un piyasa değeri Buffett ve Gates'in toplam servetinin üzerinde*.<http://www.bloomberght.com/haberler/haber/2075385-bitcoin-un-piyasa-degeri-buffett-ve-gates-in-toplam-servetinin-uzerinde>. Erişim (11.05.2018).

Brand, A. W. (2016). *Bitcoin for Dummies*. Prypto, ss. 208-209.

Columba, F.(2008). *Narrow money and transaction technology: new disaggregated evidence*. Journal of Economics and Business. 61, ss. 312-325.

Controlled supply. [https://en.bitcoin.it/wiki/Controlled\\_supply](https://en.bitcoin.it/wiki/Controlled_supply). Erişim (27.04.2018).

Çarkacıoğlu, A. (2016). *Kripto-Para Bitcoin*. Daire Başkanlık Makamının 20.10.2016 Tarihli Görevlendirmesi Uyarınca Hazırlanan Araştırma Raporu.

Çay, Ş. ve Bilir, H.(2016).*Elektronik Para Ve Finansal Piyasalar Arasındaki İlişki*. Niğde Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Dergisi. 9(2), ss. 20-29.

Daı, W. (1998). *B-money*. Consulted, 1, 2012.

Er, E. E. (2006). *Elektronik para ve finansal yönetim üzerine etkileri*. Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Elliot, J. (2008). *Help – Somebody Robbed my Second Life Avatar*. Journal of Virtual Worlds, Research, Vol.1, No.1.

Elly, P. (2013). *How much gold is there in the world?*. BBC News. (Erişim 20.03.2018).

Erich, R. And Werner, V. (1988). *Organisierte Kriminalitaet in der BRD*. BKA Forschungsreihe, 1988, 112, 170.

European Banking Authority. (2013). *EBA warns consumers on virtual currencies*. Journal of Virtual Worlds, Research, Vol.1, No.1.

European Central Bank. (2012).*Virtual Currency Schemes*. Germany, October 2012, <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, (Eriřim 28.04.2018).

European Central Bank. (2012).*Virtual Currency Schemes*. [https://www.ecb.europa.eu/ecb/legal/pdf/1\\_12520130507en00170033.pdf](https://www.ecb.europa.eu/ecb/legal/pdf/1_12520130507en00170033.pdf).(Eriřim10.05.2018).

Gandal, N. And Halaburda, H. (2014).*Competition in the Cryptocurrency Market*.Bank of Canada working paper, 33.<http://www.econstor.eu/bitstream/10419/103022/1/791932281>.(Eriřim12.08.2016).

Görmez, Y.ve Budd, C.(2012). *Electronic money free banking and some implications for central banking*. Central Bank Review Report,Türkiye Cumhuriyet Merkez Bankası, Ankara.

Herbert, S. H., Josef, B. H.and Jürgen, L. (2011).*Bankrecht-Handbuch*. München, Verlag, s. 42.

Karabıyık, A. (2018). *Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek) – 1*. <http://www.mufad.org/journal/attachments/article/323/8.pdf> (Eriřim 23.03.2018).

Katherine, S.S. (2018).*Bitcoin 101: How to get started with the new trend in virtual currencies*. White Paper, Thomson Reuters.

Keser, B. L.(2002). *İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Yetkin Yayınları*, Ankara 2002.

Jürg-Beat, A. (1992).*Geldwaescherei – MoneyLaundering*. Zürich, 1992, s.33.

Kripto Para Piyasası. (2018).*Dijital Para Kurları, Sanal Para Fiyatları*. <http://www.kriptoparapiyasasi.com/>, (Eriřim: 18.05.2018).

Leyla Keser, B. (2002).*İnternet Üzerinde Yapılan İşlemlerde Elektronik Para ve Dijital İmza. Yetkin*, 2002, Ankara, s.108.

- Lifecycle of an Altcoin. (2018).*Bitcoin' in alt türevleri*.<https://www.coursera.org/learn/cryptocurrency/lecture/Zdm9b/lifecycle-of-an-altcoin>, (Erişim: 11.04.2018).
- Loyd, K. M. (2014).*Coining Bitcoin's Legal-Bits: Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, Harvard Journal of Law And Technology, Volume 27, Number 2, Spring 2014, s.592.
- Macchetti, M. And Dadda, L. (2005).*Quasi-Pipelined Hash Circuits, 17th IEEE Symposium on Computer Arithmetic*. Massachusetts, USA, June 27-29.
- Nakamoto, S. (2009).*Bitcoin: A peer-to-peer electronic cash system*.  
<https://bitcoin.org/bitcoin.pdf>. (Erişim: 13.03.2018).
- Öztürk, N. Ve Koç, A. (2006). *Elektronik Para, Diğer Para Türleriyle Karşılaştırılması ve Olası Etkileri*.Selçuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Sosyal ve Ekonomik Araştırmalar Dergisi, S.6(11), s.207.
- Praleen, B.(2014).*A Look At The Most Popular Bitcoin Exchanges*. Investopedia (Erişim:17.04.2018).
- Raiborn, C. S.(2015). *Accounting Issues Related to Bitcoins*. The Journal of Corporate Accounting Finance. 01/02, s. 25-34.
- Rickards, J. (2016). *The New Case for Gold*. Barnes and Noble, s.192.
- Rumelili, Ö. M.(2006). *Ödeme Sistemlerinde Bilgi Teknolojileri Riskleri*. Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.
- Sarıakçalı, T. (2008). *İnternet Üzerinden Akdedilen Sözleşmeler*.Seçkin Yayınevi, Ankara.
- Some things you need to know. (2018). *Bitcoin Hakkında Bilinmesi Gereken Bazı Gerçekler*.  
<https://bitcoin.org/en/you-need-to-know>, Erişim: 01.05.2018.

Sözer, B.(2002). *Elektronik Sözleşmeler*.Beta Yayınevi, İstanbul.

Sutherland, J. and Canwell, D. (2009). *Key Concepts in Leisure*. Palgrave Macmillan.

Stalder, F. (1997). *E lectronic Money: Preparing The Stage*.<http://www.fis.utoronto.ca/-stalder/html/e-cash1.html>.Erişim: 01.05.2018.

Şeker, M. (2011).*Elektronik Ödeme Sistemleri*. İstanbul Ticaret Üniversitesi, Sosyal Bilimler Dergisi, Y.10, S.20, Güz 2011, s.59.

Villanueva, J.C. (2015). *How Many Atoms Are There in the Universe?.*Universe Today.

Özdani, V. (2011).*22 Soruda Bitcoin ve Litecoin nedir, ne değildir*. İstanbul Ticaret Üniversitesi, Sosyal Bilimler Dergisi, Y.10, S.20, Güz 2011, s.45.

Velde, F.(2013). *Bitcoin: A primer online*. Chicago, [http://www.chicagofed.org/digital\\_assets/publications/chicago\\_fed let](http://www.chicagofed.org/digital_assets/publications/chicago_fed let). (Erişim: 02.03.2018).

Weber, R.(1998). *Chablis-Market Analysis of Dİgital Payment Systems*. Technischen Universität München, August, s.44.

Yakupoğlu C.(2016). *A comparative study of bitcoin and alternative cryptocurrencies*. Yıldırım Beyazıt Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Yurtççek, M.S. (2015). *Hukuki Açıdan Elektronik Para*.Seçkin Yayıncılık, İstanbul, 2015.s. 211.

## **EKLER**

### **Ek 1:Bitcoin Hakkında Yapılan Bir Görüşme**

Semih Başaran ailesine ait bir işletmede ziraat mühendisi olarak faaliyet göstermektedir. Kendisine İşlerinin kötüye gittiği bir dönemde bir çıkış yolu olarak gördüğü sanal paralar üzerine bir görüşme gerçekleştirilmiştir.

Bitcoin kullanan Semih Bey ile yapılan görüşme:

#### **Bitcoin İle Tanışma**

Bitcoin ile 2016 yılı içerisinde gerek görsel basın gerekse arkadaş çevresinin kendisini bilgilendirmesi ile tanışmış olduğu belirtilmiştir. İnsanlar arasında yayılan haberler neticesinde 2-3 günlük kişisel araştırma ile birlikte kripto para piyasası hakkında yüzeysel bir bilgiye sahip olduğu ifade edilmiştir. O zamanlarda Türkiye’ de ilk olarak BTC TÜRK borsası, kripto para alım satımına aracılık etmekte iken zamanla kripto paralar ile ilgili yeni ticaret borsalarının açılması sanal paralara ulaşılması yönündeki imkanları daha da artırdığı dile getirilmiştir.

Bitcoin’ i nasıl alınacağına yönelik ilgili borsa sitelerinin site ziyaretçilerini yönlendirmesi ile kişisel banka hesaplarından kripto para borsa hesaplarına TL/YP cinsi mevduat aktarımı ile satın alma, değişim ve transfer işlemleri mümkün olabileceği belirtilmiştir.

2016 yılında sanal paralara olan ilginin Türkiye’ de yaşayan insanlar gibi faaliyette bulunduğum sektörden daha çok kazanç olanağı sağlaması olduğu şeklinde dile getirilmiştir.

#### **Ne Zaman Bitcoin Kullanmaya Başladınız?**

2016 yılının sonlarına doğru kişisel araştırmalarım sonuca bağlayıp herhangi bir sanal para borsasında hesap açmaya ve TL transfer edip Bitcoin almaya karar verdim. 2016 Aralık ayında BTC almaya karar verdiğimde 1 BTC =740 USD’ idi ve aralık ayı içerisinde bir miktar yatırım yapmaya karar verdim.

#### **Neden Bitcoin Talep mi, Merak mı?**

Aslına baktığımızda bu soruya ham talep ondan biraz daha fazlası merak ve en nihayetinde ise daha fazla kazanç elde etme güdüsü beni bu alana çektiğini söyleyebilirim. İnsanlar arasında yayılan ve dünya genelinde yoğun bir ilgi görmeye başlayan sanal paralar konusunda benim de piyasada bir şeyler yapıp kendime yer edinme düşüncesi hakim olmaya başlamıştı. Başta bu işe girerken 100-150 Bin ile girip 2 ay sürede 400-450 bin TL mevduatla çıkmayı hedefliyorduk, beklediğimiz kadar yatırım yapamadık ama kar yüzdeleri çok yüksek olduğu da bir gerçektir.

## **Sanal Paralar Güvenli midir? Kara Para Aklama Konusundaki Düşünceleriniz Nelerdir?**

Dünya üzerinde Bitcoin ve bitcoinin alt türevleri olan coin piyasaları hakkında uzman olan kişilere göre aslında Sanal Paranın bir yatırım emtiası olarak güvende olmadığı bunun sebebinin ise dünya üzerinde çok az sayıda kişinin sanal paralarla ilgilenmesi ve birçok kişinin kripto para birimleri hakkında kısıtlı bilgi sahibi olması ayrıca dalgalanmanın çok fazla olması, spekülasyona ve manipülasyona açık olması gösterilebilir. Ancak benim düşünceme göre sanal paralar güvenlidir. Çünkü; dünden bugüne gelen dünya üzerindeki ekonomik konjonktür artık sınırları aşar hale gelmiştir. Uluslararası para transferlerindeki yaşanan sıkıntılar, uluslararası ticarete yaşanan gümrük kotaları, vergiler vs. gibi kısıtlamalar insanları alternatif ödeme araçlarını kullanmaya yönlendirmektedir. Örneğin, Dünyanın akaryakıt ve enerjiden sonra en fazla kazandıran sektörü yazılım bilişim teknolojisi olduğu herkes tarafından kabul gören bir gerçektir. Yazılım sektöründe birçok alış-veriş internet üzerinde olduğundan dolayı fiyat-money denilen ülkelerin bilinen para birimlerinden farklı olarak dijital paralar insanların hayatına girmiştir. Bu durumu 2009 yılına giderek incelediğimizde 2009 yılında 1 BTC 0,003 USD iken bugün 6.000 USD ‘ yi görmüştür. 9 yıllık süre zarfında 2 milyon kat artan bir para biriminden bahsedilmektedir. Böylesine ilginç bir durum karşısında ekonomi yorumcuları sistemin manipülasyona ve spekülasyona açık olduğundan dolayı güven konusunun irdelenmesi gerektiğini savunmaktadırlar. Oysa ki bana göre kullanımı yeni başlayan kısa sürede uzun bir yol kat eden bir para biriminin ilerleyen zamanlarda kullanım alanlarının daha da yaygınlaşacağı ve benimseneceği kanaatindeyim.

Kara para aklama konusunda söz konusu sanal paraların kullanılmaya çok müsait olacağı tartışılmaz bir gerçektir ancak kripto paralar kullanılmadan önce kara para aklama yoktur demek çok yanlış olacaktır. Sistemin bir merkezine olmaması denetime tabi olmaması gibi sebepler kara para aklama konusunda uygun bir zemin oluşturmaktadır.

Kara para aklama hakkındaki görüşlerimi sanal paralara mal etmeden maalesef ki dünya üzerinde böyle bir (kara para aklama) sistemin var olması sebebiyle şu şekilde açıklanabilir: Ülkeler savaş çıkartır ve savaş lordları denilen silah satan kesimin dijital paraları kullanmış olabilmeleri muhtemeldir. Çünkü sanal paranın transferinin hızlı, işlem maliyetlerinin düşük, fiziki olarak çok olmaması ve denetimden uzak olması sebebiyle illegal yolların kullanılmasına aracılık eden bir sistem olarak da değerlendirilebilmektedir.

## **Ülkelerin Sanal Paralara Olan Yaklaşımları Hakkındaki Görüşleriniz Nelerdir?**

Bu konuya aslında kronolojik olarak yaklaşmak gerekiyor. Satoshi Nakamoto 9 sayfalık makalesi yayınlandığında herkes bunun uzak doğudan yayıldığını gördü ve bu konuya Japonya ve Çin gibi ülkelerin çok daha ilgili olduğu görüldü. Bizim ülkemizde yaygınlık kazanması 2016 ‘ yı bulduğunda uzak doğu ülkeleri o kadar hızlı ilerleme kaydetti ki daha sonraki yıllarda Çin hükümeti sanal paralara olan yaklaşımda katı bir politika izlemeye başlayıp çeşitli yasaklar getirerek piyasanın geriye gitmesine neden olmuştur. Bunun sebebine bakacak olursak Çin’ de aşırı bir nüfus yoğunluğu var bu da katı bir yönetim şeklinin uygulanması anlamına geliyor. İnsanların parayı ülke dışına çıkarıp başka ülkelerde yeni bir

hayat kurması çok zor görünmesine karşın dijital paraları bir kurtuluş yolu olarak görüyorlardı. Aslında dijital paralar doğal hayatın sıkışmasından doğan alternatif bir çözüm yolu olarak ortaya çıktı ve bu denli gelişti. O zamanlar Çin hükümeti durumu yakından izlemekle yetinmiş ancak dijital para piyasası sınırları aşan bir piyasa olmaya doğru giderken duruma müdahaleyi zorunlu görmüştür.

İngiliz kraliyet ailesi güdümündeki altınlar ile BTC aldığı bunu duyan Hindistan hükümetinin İngiltere' nin bu tutumunun doğru olduğunu belirtmiş ancak İngiltere elinde bulunan btc'leri satışa çıkarmasının ardından Hindistan'da piyasadan uzak durulması yönünde açıklamalarda bulunmuşlardır.

Venezüella devlet başkanı ülkelerinde yer alan petrol kaynaklarına endeksli olarak çıkardıkları Petro coin karşılığında ülkelere petrol ihracında kolaylıklar sağlanabileceği yönünde açıklamalarda bulunmuşlardır. Bu dönemde ülkemizde de dijital paralar ile ilgili "yakından takip ediyoruz" şeklinde açıklamalar yapılmıştır.

Sonuç olarak; ülkeler önemi uluslararası boyutlara ulaşan konularda acil karar vermezler zamana yaygın ve açık kapı bırakacak açıklamalarda bulunurlar. Art niyetli borsa şirketlerinin almış olduğu kararlar ülke vatandaşlarının zarar etmesine sebep olduğundan dolayı ülkeler, vatandaşlarının haklarını korumak adına ve insanlara zarar verebilecek işlemlerin, piyasaların kapatılması yönünde kararlar vermişlerdir. En somut örnekleri ABD, Kuzey Kore, Kanada ve Çin hükümetleri tarafından alınmıştır.

### **İnsanların Sanal Paralara Olan Yaklaşımları Nasıldır?**

İnsanları sanal paralara olan yaklaşımı her geçen gün artış göstermekte ancak ülkelerin uyguladığı sınırlamalar sebebi ile şuan biraz duraksamış durumdadır. Alternatif bir ödeme aracı olarak yerel ve uluslararası bazı işletmeler BTC ve BTC türevleri ile mal alım satımı yaptıkları görülmektedir. Örneğin; BTC CASH ile Sturbucksta kahve alınabilmesi gibi. Ripple alt yapısını güçlendirerek her ülkeden bir banka ile anlaşma sağlayıp TL/YP karşılığı ripple satın alınabileceğini duyurmuştur.

Türkiye' de çek ile ödeme gibi bir sistemin varlığını sürdürmesi mümkün iken sanal paralar ile ödeme neden mümkün olmasın. Bir çek yaprağıyla birbiriyle ilişkili olan ya da olmayan sektörlerin ticareti aşırı risk içerirken dijital paralarda bu risk neden alınmasın?

Sonuç olarak; dünya üzerine gelen yeniliklerin hemen kabul görüp benimsenmesi imkânsız denecek kadar düşük bir ihtimal olmasına karşın gelecekteki bir zamanda özellikle arzı sınırlı olan BTC' nin daha da bir popüler olması ve alt türevlerinin daha yaygın olarak kullanılması kaçınılmazdır.

İnsanlar arasında hızlı bilgi paylaşımını sosyal medya (Facebook, twitter, Telegram) gruplarıyla mümkün kılınmakta olup bu şekilde sisteme daha fazla kişiyi çekmenin mümkün olduğu ifade edilmiştir. Ayrıca coinlerin henüz oluşum aşamasında (ico döneminde ) ilgili coin borsalarına ve sitelerine üye olunması akabinde ödül coin verilmesi insanların söz konusu sisteme dahil olmasını cezp etmektedir.



## **Dijital Paraların Geleceği Hakkında Görüşleriniz Nelerdir?**

Sanal paraların geleceği konusunda dünya tarafından her geçen gün kabul gören ve gelişmesi beklenen bir durum olarak görünmektedir. Fiyat konusunda bir öngörü olmamasına karşın günlük hayatımıza yerleşmesi gelecek için muhtemel bir öngörüdür. Çünkü dünya gelişip değişmektedir. Trampa ekonomisinden dijital ekonomiye geçişin temelleri atılıyor gibi düşünebiliriz.

Geleceği konusunda hızlı ilerlemenin olabilmesi için belli bir merkezi sisteme oturtulup kontrol mekanizmasının oluşturulması gerekiyor. Saniyelik transferlerin mümkün olabilmesi için teknoloji alt yapılarının geliştirilmesi gerekiyor. İnsanların daha rahat kullanabilmeleri için sistemin daha basite indirilmesi ve riskin minimize edilebilmesi için fiyat dalgalanmalarından arındırılması da yapılması gereken iyileştirmeler arasında sayılabilir.

## **Sanal Paralar Yatırım Aracı Olarak Görülebilir mi?**

Bugüne kadar hiçbir yatırım uzmanı ve danışmanı dijital paraları yatırım emtiası olarak görmemiştir. Yatırım aracı olarak kullanılmasından daha çok harcama ve değişim yani kullanım amacı olarak görülmesinde fayda vardır. Yatırım aracı olarak görülmesi elbette ki borsa mantığına dayanır. Bu da borsaya ilgisi olan kişilerin yapıp yapmayacağı sadece kişisel tercihlerine bağlı olan bir olgudur.

## **Sizin İçin Nakit Para mı, Dijital Para mı Önemlidir?**

Elbette ki nakit para önemlidir. Her ne kadar diğer para birimleri karşısında değişimi olumsuz yönde olsa da riski çok düşüktür. Dijital para bir merkezinin olmaması fiyat değişimlerinden aşırı etkilenmesi ve aşırı kar, aşırı zarar söz konusu olduğu için tercih sebebi risk sevenlere daha yakın gelebilmektedir.

## **Ticarette Alınan Ücret Ve Komisyonlar Hakkında Neler Söyleyebilirsiniz?**

Bitcoin madenciliğinde gerekli olan enerji tüketimi çok yüksek rakamlara ulaştığından dolayı özellikle BTC transfer işlemlerinde transferlere aracılık eden ve Block Chain sistemine dahil olan borsalar her bir transferden 0,001 oranında transfer ücreti komisyonu almaktadır. Normal TL/YP uluslararası transfer işlemlerinde işlem maliyetleri hem daha yüksek hem de çok daha uzun sürede gerçekleştirilmektedir.

## **Sanal Para Teknolojileri ve Üretim İşlemi Nasıl Yapılmaktadır?**

Sanal para teknolojisini bir yazılım grubuyla oluşturmak oldukça zor özellikle kendi blockchain sistemi ile birlikte oluşturmak oldukça güçtür. Bu sebepten dolayı Ethereum platformu üzerinden çıkan ERC20 tokenlar smart contract sisteminin herkes tarafından rahatlıkla kullanılabilir olması daha kolaydır. Bu da Ethereum teknolojisinin ve kullanımının daha ileri düzeye taşınmaktadır. Kendi block chain sistemini oluşturmak mining işlemi yapmak oldukça fazla enerji ve maliyet gideri gerektirmekte olduğundan var olan blockchain üzerinden üretim yapmak daha cazip gelmektedir.