SERMAYE PİYASASI KURULU

ARAŞTIRMA DAİRESİ

KRİPTO-PARA BITCOIN

Dr. Abdurrahman ÇARKACIOĞLU

Aralık 2016

SERMAYE PİYASASI KURULU
Araştırma Dairesi

KRİPTO-PARA BITCOIN

Dr. Abdurrahman ÇARKACIOĞLU

Araştırma Raporu
Aralık - 2016

KRİPTO-PARA BITCOIN

Dr. Abdurrahman ÇARKACIOĞLU

SERMAYE PİYASASI KURULU
Araştırma Dairesi
Daire Başkanlık Makamının 20.10.2016 Tarihli Görevlendirmesi Uyarınca
ARAŞTIRMA RAPORU
Olarak Hazırlanmıştır.

Aralık - 2016

KABUL ve ONAY SAYFASI

Abdurrahman ÇARKACIOĞLU'nun ARAŞTIRMA RAPORU olarak hazırladığı "Kripto-para *Bitcoin*" başlıklı bu çalışma, Daire Başkanlığınca değerlendirilerek kabul edilmiştir.

...../...../.....

KRİPTO-PARA BITCOIN

Dr. Abdurrahman ÇARKACIOĞLU

Araştırma Raporu, 2016

ÖZET

Bitcoin, heryerde herkese anında ödeme imkanı sunan, merkezi olmayan dijital kripto-paradır. *Bitcoin*ler satın alınabilir, satılabilir ve diğer para birimleriyle takas edilebilirler. *Bitcoin* kabul edilebilir bir seviyede gizlilik ve anonimlik sağlar. *Bitcoin* kullanıcıları gizli anahtarlarıyla bitcoin ağındaki işlemlerinin sahipliğini ispatlar ve kendilerine ait değeri harcayabilir, yeni sahibine transfer edebilirler.

Bitcoin, transfer işlemlerini uçtan uca ağ bağlantısı kullanarak gerçekleştirir. Ödemeler bir kaç saniye içerisinde gerçekleşir. Ortalama her 10 dakikada bir, bir öbek transfer işlemi, küresel işlem defteri olan *Blok-Zincir*'e yazılarak onaylanır. Yeni bloklar, küresel işlem defterine, bir matematik problemini çözmek için yarışan madenciler tarafından yazılırlar. Başarılı madenciye yeni bitcoin hediye edilir. Dolaşımdaki bitcoin sayısı, kolayca tahmin edilebilen bir eğriye göre hesaplanabilir, 2140 yılında 21 milyon bitcoin üretilmiş olacaktır. *Bitcoin* teknolojileri kullanılarak tanımlanmış binlerce altcoin vardır. Kripto-para marketinin toplam kapitalizasyonu 14 Milyar Doların üzerindedir.

Dünyada pek çok hükümet *Bitcoin*'e karşı olumlu bakarken, vatandaşlarını fiyat oynaklığı, *Bitcoin*'in arkasında bir merkezi otorite olmaması ve *Bitcoin*'in herhangi bir fiziki varlık ile ilişkili olmaması hususlarında uyarmaktadır.

Blok-Zincir'in, *Bitcoin* olmasa dahi, evrakın, dijital ve fiziki varlıkların sahipliğinin izlenmesi veya oy kullanılması gibi çok geniş bir kullanım yelpazesi vardır.

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

CRYPTO-CURRENCY BITCOIN

Abdurrahman ÇARKACIOĞLU, Ph.D.

Research Report, 2016

SUMMARY

Bitcoin is decentralized digital cryptocurrency that enables instant payments to anyone anywhere in the world. *Bitcoin*s can be purchased, sold, and exchanged for other currencies. *Bitcoin* can provide acceptable levels of privacy and anonymity. Users of bitcoin own private keys that allow them to prove ownership of transactions in the bitcoin network, unlocking the value to spend it and transfer it to a new recipient.

Bitcoin uses peer-to-peer network to manage the transactions. Payments are done within seconds. Every 10 minutes on average, a block of transactions are confirmed by writing them on a global ledger, called BlockChain. New blocks are added to the ledger by *Bitcoin* miners while competing with each other to find solutions to a mathematical problem. Winner miner is rewarded with brand new bitcoins. The number of bitcoins in circulation closely follows an easily predictable curve that reaches 21 million by the year 2140. Using *Bitcoin* technologies, currently thousands of altcoin have been issued. Today, total cryptocurrency market capitilization is over 14 Billion dollar.

Most of the governments in the world have positive attitude toward bitcoin while explaining the risks to citizens in terms of bitcoin not being overseen by a central authority nor being tied to a physical asset and volatility of the market value.

Even without *Bitcoin*, *BlockChain* can be used for a wide variety of applications, such as tracking ownership or the provenance of documents, digital assets, physical assets or voting rights.

Keywords: Bitcoin, BlockChain, Crypto-currency

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

1. GİRİŞ

Mal ve hizmetlerin mübadele edilmesinde kullanılan takas yönteminden, emtia paraya, sonra altın/gümüşe, daha sonra altın karşılığı olan değerli kağıtlara, oradan altın karşılığı bulunmayan güvene dayalı itibari paraya derken, paranın evrimi dijital ve sanal paralara doğru yol almaktadır. İnsanlık, mübadele aracı olan parayı kendi ekonomik, bilimsel ve kognitif gelişimine paralel olarak, soyutlaştırmaya devam etmektedir. *Bitcoin*, 21. yüzyılda, para kavramının nerelere kadar geldiğinin en uç örneklerindendir.

1.1 Para Nedir?

Mal ve hizmetlerin takası için kullanılan en yaygın araçtır. Paranın 4 temel işlevi [1];

1. *Değişim aracıdır.* İki malın değişiminde para, bir üçüncü mal olarak araya girer ve değişimi iki bölüme ayırır. Bir mal veya hizmet verilip karşılığında para alınır, başka bir yer ve zamanda ise para verilip başka bir mal veya hizmet alınır.

2. *Hesap ve değer birimidir.* Farklı malların değişiminde, değişim oranları para ile belirlenir.

3. *Değer biriktirme ve spekülasyon aracıdır*. Arz ve talebin rahatlıkla karşılanmasını sağlar. Aynı zamanda sermaye birikimi ve yatırım aracıdır.

4. *İktisat politikası aracıdır.* Ulusal ekonomiler, para arzı ve faiz oranı kontrolüyle iktisat politikalarını gerçekleştirirler.

1.2 Emtia Para (Commodity Money)

Değeri, yapıldığı üründen gelen paralara "***emtia para***" denir. Emtia paralar fiziksel varlıklardır. Dünya üzerinde farklı bölgelerde ve farklı zamanlarda, bakır, tuz, çay, inci, fildişi, sığır, demir, köle, sigara vb. emtia paralar bin yıllar boyunca para olarak kullanılmıştır. Tüm zaman ve mekanlarda en yaygın olarak kabul gören emtia para ise, altın ve gümüş olmuştur.

Değişim aracı olarak kullanılmasalar dahi, kendiliklerinden değerleri (*intrinsic value*) olduğu düşünülür. Bu sebeple, ekonomik çalkantı ve krizlerde, hiperenflasyonda bazı insanlar hükümetlerin bastığı paralar yerine emtia paraları kullanma eğilimi gösterirler [2].

1.2.1 Altın Ve Gümüş

Altın ve gümüş evrende nadir bulunan ağır elementlerdendir. Oluşumları için, kozmik ölçüde yüksek sıcaklıklar ve basınç gerekir. Süpernovalarda veya çok yoğun nötron yıldızlarında oluştukları düşünülmektedir [3,4].

Altın ve gümüş; mücevher, para basımı, heykelcilik, gemicilik, bina dekorasyonu ve anıt yapımında antik çağlardan bu yana kullanılmaktadır. Periyodik cetveldeki 118 element arasında, zehirli olmayan, katı, renkli, diğer elementlerle hemen kolaylıkla tepkimeye girip patlamayan, yanmayan, oksitlenmeyen/paslanmayan, radyoaktif olmayan, eritmesi çok zor olmayan, çok yaygın değil ama bulması aşırı zor olmayan, sadece altın ve gümüştür. İkisinin de göreceli olarak düşük erime noktasının olması, bozuk para, külçe ve takı haline getirilmelerini kolaylaştırır. Gümüşün çabuk kararması, altının en yaygın ve değerli emtia para olarak ilk sıraya geçme sebeplerindendir [5].

2013 yılı itibarı ile, insanlık tarihi boyunca, yaklaşık 171.000 ton altın çıkartıldığı tahmin ediliyor [6]. Nüfusu 7 milyarı aşan dünyada kişi başına, yaklaşık 24 gram altın düşüyor [7].

Şekil 1.1: Lidyalıların bastığı altın paralar.

Altın ve gümüş, farklı coğrafyalarda, değişim aracı, ödeme aracı, hesap birimi ölçüsü ve değer saklama aracı olarak kullanılagelmiştir. Antik Mısır'da M.Ö. 3200'lerde, altın çubukların para yerine kullanıldığı biliniyor. *Şekil 1.1*'de gösterilen, günümüzdeki anlamına en yakın altın parayı (sikke) ise, M.Ö. 7. yüzyılda Lidya'lılar basmış ve kullanmışlardır [8].

1.3 Temsili Para

İçinde belli oranda altın olan madeni paralar, altın fiyatının yükselmesi halinde birileri tarafından eritilerek, içindeki altının alınma riskiyle karşı karşıyadır. "*Kötü paranın iyi parayı kovması*" olarak da bilinen bu kanuna *Gresham kanunu* denir.

Para olarak doğrudan veya alaşımlı değerli metal kullanmanın pek çok zorluğu olduğundan, emtia para sistemi zaman içerisinde temsili para sistemine evrilmiştir. Altın ve gümüş tacirleri veya bankalar, karşılığında emtia para olan, istendiğinde emtia paraya çevrilebilen temsili paralar basmışlardır. Altına dayalı mali sistemde, yasal para veya sertifika basanlar, bastıkları toplam değerin, sabit bir oranda karşılığını altın/gümüş olarak tutarlar.

Tarihte bugünkü anlamıyla ilk banknot olan "*Jiaozi*" (*Şekil 1.2*), 10.yüzyılda Çin'de Song Hanedanlığı döneminde basılmış olup, altın paralarla birlikte kullanılmıştır [9].

Şekil 1.2: Tarihin en eski banknotu *Jiaozi*[*].

---

* Resmin en solundaki yuvarlaklar paranın mühürleridir. Ortasındaki yazılar paranın, madeni para cinsinden değeri, en sağda ise bir alışveriş resmedilmiştir.

13. yüzyılda, Marco Polo gibi seyyahların Çin'den öğrendikleri kağıt para, Avrupa'da da bilinir hale gelmiştir [10]. Avrupa'da ilk kağıt para Stokholm Bankası (Stockholms Banco) tarafından 1661 yılında basılmıştır [11].

17.-19. yüzyıllar boyunca, Avrupa'da kağıt paralar veya kağıt sertifikalar yasal otoriteler tarafından basılmış, kullanımı özendirilmiştir. Kağıt paraların altına çevrilmesi konusunda ise caydırıcı olmaya çalışmışlardır. Altına dayalı mali sistemde, ülkelerin kağıt paralarının değeri doğrudan altına bağlıdır [12]. *Şekil 1.3*'te altına dayalı Dolar gösterilmektedir.

Şekil 1.3: 1928 tarihine ait altına çevrilebilir 10 Amerikan Doları

1.4 İtibari Para (Fiat Currency)

II. Dünya savaşı sonrası, 1944'te, 44 ülkenin katılımıyla, Amerika Birleşik Devletleri, New Hampshire eyaleti, Bretton-Woods'da, Birleşmiş Milletler Mali ve Finans Konferansı düzenlenmiştir. Bu konferansta, pek çok ülkenin kendi para birimini Amerikan dolarına endeksli itibari para yapması ve Amerikan Dolarının ise altına dayalı olmasına devam etmesi kararlaştırılmıştır. Başka bir deyişle, altına dönüştürülebilen tek para biriminin dolar olmasına, diğer para birimlerinin değerlerinin de dolara göre ayarlanmasına karar verilmiştir . Anlaşma ile 1 ons* altın = 35 Amerikan Doları ya da 1 dolar 0,88867 gram altın olarak belirlenmiştir [13].

Amerika Birleşik Devletleri Başkanı Richard Nixon, 1971 yılında Amerikan Dolarının,

---

* 1 ons =31.10 gram

altın karşılığının bulundurulması zorunluluğunu kaldırdı. Günümüzde ülkelerin dolaşımda bulunan paralarının, altın karşılıklarının olma zorunluluğu yoktur. 2012 itibarıyla, Amerikan Doları para arzının sadece %4.46'sının, İngiliz Sterlini'nin ise %4.05'inin altın karşılığı vardır [14].

Özetle; altındaki imzalara, düzenlendiği kağıdın taklit edilemeyeceğine ve merkezi otoriteye güven üzerine kurulmuş, mal ve hizmet alışverişi için kullanılan kağıt paraya ***itibari para*** (fiat money) denir [15]. Şekil olarak temsili paralara benzeseler de, itibari paralar altın veya gümüşe dayalı değillerdir.

1.6 Alternatif Para

Alternatif para birimleri geleneksel para sistemlerine alternatif olarak kullanılan özel para birimleridir. Deyim yerindeyse, bu paralar geleneksel ve yaygın para sistemlerine karşı isyancıdırlar. Geniş değerlendirecek olursak, bankacılık sistemleri kullanılmadan gerçekleştirilebilen borç ödeme şekline, alternatif para sistemi denebilir.

Alternatif para birimleri birey, kurum veya kuruluşlar tarafından, genelde ortaya çıktığı bölgedeki üretimi artırmak, ticareti geliştirmek ve bölge ekonomisini canlandırabilme amacıyla bir nevi ihtiyaçtan ötürü oluşur. Oluşturulan özel para birimi, bölge halkları tarafından kabul gördüğünde doğal bir şekilde yaygınlaşır ve kullanımı da artar [16].

Alternatif paralar lokal ekonomilerde dengeleyici rol oynarlar. Lokal ekonomi yavaşlarken, alternatif para hareketlilikleri artar, lokal ekonomi yukarı giderken ise hareketlilikleri azalır [17].

Bölgesel alternatif paraların, bölge dışında kullanımları sınırlıdır. Ekonomik aktiviteleri geçici süreliğine artırdığı, uzun süreli kullanımlarında ekonomik destabilizasyonlara sebebiyet verdiği de ciddi iddialardandır [18]. Kanada'da *Canadian Tire* parası, ABD'nin Massachusetts eyaletinde kullanılan *BerkShare,* İngiltere'de *Bristol Pound* ve Hollanda Amsterdam'da *Makkie* en bilinen alternatif para birimleridir [19].

1.6.1 Örnek alternatif para: ***Tumin***

2010 yılında, Castro Soto ve bir grup üniversite çalışanı, Meksika'nın El Espinal köyünde, bölgesel ekonomilerini güçlendirmek için bir proje başlattılar ve alternatif para ***tumin***'i ürettiler. 57 bin kişinin yaşadığı El Espinal'de 2 yıl gibi kısa bir sürede, yeni para köy sakinleri tarafından hemen benimsendi [20].

Meksika Ulusal Bankası, Meksika'nın ulusal para birimi Peso'ya alternatif geliştirmek, para basmak gibi suçlardan dolayı, Tumin'i üretenler hakkında dava açtı. Tumin'in üreticileri ise iddiaları yalanlıyarak "Tumin Meksika Pesosu'na alternatif değildir, Tumin bir takas aracıdır." savunması yapmaktadırlar. Davalar devam etmektedir.

2013 yılında yapılan bir çalışma, Tumin'in ekonominin canlanmasında etkisinin olmadığını ama dayanışma ve karşılıklılığı artırdığını göstermektedir [20].

1.7 Dijital Para

1980'lerin sonunda, Hollanda'da gece yarısı yakıt alan kamyon şoförlerini ve benzin istasyonlarını hırsızlığa karşı korumak için, akıllı kartlara para yüklenmesi ve bu paralarla yakıt alınabilmesi elektronik ödemenin ilk örneklerindendir. Yine o tarihlerde, Albert Heijn isimli bir perakendeci, müşterilerinin banka hesaplarından doğrudan ödeme yapabilmeleri için bankalara baskı yapıyordu. Bu baskı sonucunda, şimdilerde herkesin bildiği POS (Point Of Sale) cihazları ortaya çıktı [21].

Dijital paralar, elektronik olarak saklanan ve transfer edilebilen paralardır [22]. Banka hesabımızdaki dijital para kağıt paraların temsilidir. Bankaların her yerde her zaman hazır ve nazır olması, elektronik paranın yaygınlığı ve fiziki paranın kullanımdan neredeyse kalkması, dijital parayla gerçek fiziki paranın arasındaki farkı ortadan kaldırmak üzeredir. Altından, altına dayalı kağıt paraya, ondan itibari paraya, sonrasında ise dijital paraya geçiş, bilişim teknolojilerinin gelişmesi ile mümkün olmuştur. Paranın soyutlaşması ve kavramsallaşması, insanlık tarihinden bu yana sürüp gitmektedir.

Fiziksel parayla yapılan işlemlerin azaldığı günümüz dünyasında, geleneksel paranın da

dijitalleştiği pekala iddia edilebilir. Dijital paraların saklanması ve transfer işlemleri, merkezi olabildiği gibi dağıtık da olabilir. Merkezi dijital para işlemlerini, merkezi bir güç, otorite veya program denetler, gerçekleştirir.

DigiCash, Amerikalı şifreleme yazılım uzmanı David Chaum tarafından geliştirilen ilk merkezi olarak yönetilen kriptografik elektronik ödeme sistemidir. *Digicash*'in en önemli avantajı, kullanıcılara anonimlik sağlamasıydı. *DigiCash* tam anlamıyla bir para birimi değildi, ancak taraflar arası transfer işlemlerinin gizli ve güvenilir yapılmasını sağlayan bir araçtı. Şirket, aldığı yanlış kararlar sonucu 1998 yılında iflas etti [21]. *DigiCash*'in batmasının hemen ardından kripto-para olmasalar da, elektronik ödeme sistemi olarak *First Visual* ve *PayPal*[*] boşluğu doldurdu. *PayPal* gerçek para birimine dayalı, kısıtlı ve devletlerin yasal yükümlülüklerine uyumlu dijital para olarak kullanılmaktadır. *Webmoney* ise izole olarak Rusya'da kripto-para olarak varlığını devam ettirmektedir.

1990'ların sonunda Karayipler'de ise, fiziki altın karşılığında kaydi altın hesabı tutan ve müşterilerine altın kredisi açan *e-gold* adında Amerikan tabanlı bir firma kuruldu. “Herkesin bir hesabı olabilir” gibi özgürlükçü bir yaklaşımla yola çıkan *e-gold*, kısa zamanda saadet zincirlerinin, dolandırıcıların, kara para aklayıcılarının odağı haline gelmesiyle, kamu otoritelerinin dikkatlerini üzerine çekti [21]. Benzer şekilde, 2006'da kurulan *Liberty Reserve Doları/Eurosu* da dijital paradır. Kara para aklama faaliyetlerinden dolayı her iki kuruluşda kapatılmıştır [23].

1.8 Sanal Para

Sanal paralar dijital paradırlar, ancak sanal paraların temsil ettikleri bir fiziksel gerçeklik yoktur. Sanal para dışındaki dijital paralar ise itibari kağıt paraları temsil ederler.

Sanal paranın tanımı üzerinde literatürde karmaşa vardır. Avrupa Merkez Bankası'nın 2012'de yaptığı tanıma göre [24] sanal para; “*genellikle geliştiricileri tarafından kontrol edilen*,

---

* PayPal'in lisans başvurusu, Bankacılık Düzenleme ve Denetleme Kurumu tarafından, birincil ve ikincil sistemlerini Türkiye sınırları içerisinde tutulmadığı gerekçesiyle red edilmiştir. Bknz: http://aa.com.tr/tr/ekonomi/kanuna-uygun-olmadigindan-paypalin-lisans-basvurusu-onaylanmadi/582825

sınırlı sanal grup üyeleri tarafından benimsenip kullanılan, düzenlenmemiş/regüle edilmemiş, dijital paradır". Şubat 2015'te revize edilen tanıma göre [25] ise sanal para, "*Herhangi bir merkez bankası, kredi kuruluşu veya e-para kuruluşu tarafından ihraç edilmediği halde, bazı durumlarda paranın yerine kullanılabilen bir değerin dijital temsilidir*".

Yine 2014'te Avrupa Bankacılık Otoritesi'nin tanımına göre [26] sanal para; "*Bir merkez bankası veya kamu otoritesi tarafından ihraç edilmediği halde, doğal olarak veya yasal kişiler tarafından ödeme, transfer, saklama ve elektronik transfer şekli için kabul gören, karşılığının olması da şart olmayan değerin dijital temsilidir*".

Amerikan Hazine Bakanlığı'na göre sanal para; "*Gerçek paranın tüm özelliklerini taşımadığı halde, bazı ortamlarda para gibi kullanılabilen değişim medyasıdır*".

1.9 Kripto-Para (Şifreli-Para)

Kriptografik/şifreli olarak güvenli işlem yapmaya ve ek sanal para arzına olanak sağlayan dijital değerlere kripto-para denir. Kripto-paralar alternatif para birimidirler, dijitaldirler ve aynı zamanda sanal paradırlar [27].

Sıklıkla *Bitcoin* ve türevleri ile dijital ve sanal paralar karıştırılmaktadır. *Bitcoin* ve türevleri dışındaki dijital ve sanal paralar, kendi başlarına para birimi değillerdir, temsil ettikleri ülkenin ulusal para birimine dayalıdırlar ve o ülkenin merkezi otoritelerince düzenlenip denetlenebilirler. *Bitcoin* ise kendiliğinden bir para birimidir, hiç bir merkezi otorite tarafından düzenlenip denetlenemez [28].

Bu raporun konusu olan *Bitcoin*, 1990'lardan bu yana denenen, *DigiCash*, *e-gold* gibi. sistemlerin bilgi birikimi yardımıyla, onlardaki sorunları çözmek için 2009 yılında tanımlanmış, yönetimi ve işlemleri merkezi olarak yapılmayan kripto-paradır. 2009'dan bu yana, *Bitcoin*'e alternatif olan pek çok altcoin tanımlanmıştır [29].

Kripto-paralar, merkezi elektronik paraların ve bankacılık sistemlerindekinin aksine, merkezi olmayan yapıdadırlar. Merkezi olmayan bu yapının kontrolü *Blok-Zincir* (BlockChain) işlem veritabanları tarafından gerçekleştirilir.

Kripto-paralar, merkezi olmayan kripto sistemlerde, kamuya açık ve herkes tarafından bilinen yöntemlerle sistemin kuruluş aşamasında belirlenen oranlarda üretilirler. Geleneksel para sistemlerinde hükümetler, gerekli gördüklerinde ulusal merkez bankaları aracılığıyla ek para ihraç edebilirler. Oysa, hükümetler veya şirketler kripto-para üretemezler, başkalarının sahipliğindeki kripto-paralara onların izni olmadan el koyamazlar. Dolaşıma sunulan kripto-para miktarı ve para arzının şekli ve zamanlaması, kripto-sistemin kuruluş aşamasında belirlenir.

Geleneksel elektronik para saklama ve transfer işlemlerinde güven duyulan üçüncü bir kurum/kuruluş vardır. Örneğin; A kişisi, B kişisine para transfer etmek istiyorsa, bunu üçüncü bir taraf olan C bankasına veya aracı kuruluşuna iletir, C kurumu transfer işlemini gerçekleştirir ve bu transferin güvenliğinden ve doğruluğundan C sorumludur. A ve B kişisi, C'ye güvenirler.

Kripto sistemlerde üçüncü bir taraf/aracı yoktur, güven gereksizdir. Güvenlik, bütünlük ve küresel hesap defterinin doğruluğu, karşılıklı birbirine güvenmeyen madenciler aracılığıyla gerçekleştirilir. Sistem güvenilirdir, ama taraflar birbirine güvenmezler. Kripto-paranın güvenliği, madencilerin çoğunluğunun dürüstçe büyük defter tutma ve bundan finansal teşvik elde etme arzuları olduğu ilkesine dayanır.

Çoğu kripto-para sistemlerinde, dolaşımdaki toplam kripto-paranın sabitlenebilmesi için kripto-para üretimi zamanla azalmaktadır.

Ülkelerin ihraç ettikleri dolaşımdaki banknot kağıt paralar itibari paralar (fiat money) olup, onları ihraç eden, denetleyen, düzenleyen bir otoritenin güvencesi altındadırlar. Buna karşılık, sanal kripto-paralara olan güven, sanal para ihraç ve dolaşım sistemine ve sistem kullanıcılarının çoğunluğunun yanlış yapmayacağına olan inanç ile sağlanmaktadır.

1.7 Subjektif Değer Teorisi

"*Emtia paraların, altın ve gümüşün, altın ve gümüşe dayalı para veya sertifikaların, itibari paraların, dijital ve sanal paraların değeri nereden gelir?*" sorusunun cevabı paranın varlığı ve geleceği açısından önem arz etmektedir. Para gün geçtikçe soyutlaşmakta, elle tutulur gözle görülür olmaktan uzaklaşmaktadır.

Subjektif değer teorisi, bir ürün veya hizmetin değerinin, o üretim için harcanan emeğe eşit olduğunu iddia eden ***emek-değer teorisinin*** yanlışlığını iddia eder. Subjektif değer teorisine göre; mal ve hizmetlerin ölçülebilir ve objektif bir değeri yoktur. Malın veya hizmetin değeri, kişinin elde ettiği tatmine göre değişebilir, subjektiftir [30]. Teori, mal ve hizmetlerin değerinin, onların üretiminde kullanılan faktörlerin doğası ya da emek miktarından değil, fakat tüketicinin/alıcının kendi amaçlarının gerçekleştirilmesi ve ihtiyaçlarının tatmininde bu mal ve hizmetlere isnat ettiği önem ve faydadan doğduğunu öne sürer [31].

Üzerinde tartışmalar devam etse de subjektif değer teorisi, *kendiliğinden değeri olma* (*intrinsic value*) kavramını da kapsar. Kendiliğinden değeri olduğunu düşündüğümüz altın ve gümüşün de aslında kendi değeri yoktur, altın ve gümüşe değeri biz insanlar atfederiz. Altının kendiliğinden değeri olsaydı, altın madencilerinin bir kısmı, altın çıkarma maliyetlerini karşılayamadıklarından dolayı iflas etmezlerdi [32].

2012-13 yıllarında, altın fiyatlarındaki düşüş sonrası Türkiye iç piyasasında, çeyrek altına olan talep artmış ve çeyrek altın fiyatı, tam altın fiyatının dörtte bir değerinden daha fazla olmuştur [31]. Kabul etmekte zorlansak da, kendiliğinden değeri olduğunu düşündüğümüz altının değerini dahi, talebin ve tüketicideki tatmin duygusunun belirlediği bir gerçektir.

Subjektif değer teorisi, bir mal veya hizmet ne kadar kıt olursa olsun, ne kadar çok çalışma ve emekle elde edilirse edilsin, talebi olmazsa değerinin de olmayacağını söyler. Altın ve gümüşün kendiliğinden bir değeri yoktur, ondaki değer bizim ona olan talebimiz ve başkalarının ona talep duyacağına olan inancımızdır.

Altının insan psikolojisiyle doğrudan ilgisi olduğunu, ekonomik çöküntülerde ve kağıt paraya olan güvenin azaldığı durumlarda, insanların altına güvendiklerini, bu sebeple, kendiliğinden değeri olduğunu düşünenler de vardır [33].

2. BITCOIN

2.1 Bitcoin Nedir ?

Bitcoin, dijital para ekonomisini oluşturan kavramlar ve konular bütünüdür. *Bitcoin* sistemi, açık kaynak kodlu yazılımlardan oluşur. Yazılımlar laptop ve akıllı cep telefonu dahil geniş bir yelpazedeki işlemcilerde çalışırlar [34]. Tamamen dijital olup, fiziki temsiline ihtiyaç yoktur [35]. İşlem maliyetlerinin çok az olması, küresel olarak kullanılabilmesi, gün geçtikçe kullanım alanlarının artması, güvenli ve anonim olarak değer saklama aracı olması *Bitcoin*'i daha da popüler yapmaktadır [34,36].

Şekil 2.1: *Bitcoin* sembol ve logoları*

BTC kısaltması ile gösterilebilen *Bitcoin*'in sembol ve logoları *Şekil 2.1*'de gösterilmiştir. *Bitcoin*, 8 basamağa kadar bölünebilir, dolayısıyla 0,00000001 *Bitcoin*'lik bir işlem yapmak mümkündür. En küçük birime *Satoshi* (satoşi okunur) denir. Başka bir deyişle, 100 Milyon Satoshi 1 BTC'dir.

Bitcoin'in dayandığı teoriler oldukça teknik içerikli olsalar da, kullanımı çok kolaydır. *Cüzdan* (wallet) programlarından herhangi bir tanesini yükleyip, *Bitcoin* alıp-satmaya ve transfer etmeye hemen başlanabilir. *Bitcoin* cüzdanları, kişilerin sahip olduğu *Bitcoin*'leri saklayan ve üzerinde işlem yapılmasına olanak sağlayan programlardır.

---

* Logolar için kaynak https://en.*Bitcoin*.it/wiki/Promotional_graphics

Bitcoin istendiği an, TL, Amerikan Doları, Euro veya başka paralar ile takas edilebilir [37]. Normal paranın kullanımında olduğu gibi, *Bitcoin* kullanıcıları, ürün/hizmet almak veya satmak için, *Bitcoin* ağını kullanarak birbirlerine BTC gönderebilirler. *Bitcoin* satın alabilir ve takas yapabilirler [34]. Ticaret hayatında *Bitcoin*'in, küresel pazara kolay erişim, dolandırıcılığa ve sahtekarlığa karşı koruma, düşük komisyon oranları, finansal özgürlük ve anonimlik sağladığı için kullanımı artmaktadır. *Bitcoin* yeni sanal bir ekonomiye doğru sınırları zorlamaktadır [35].

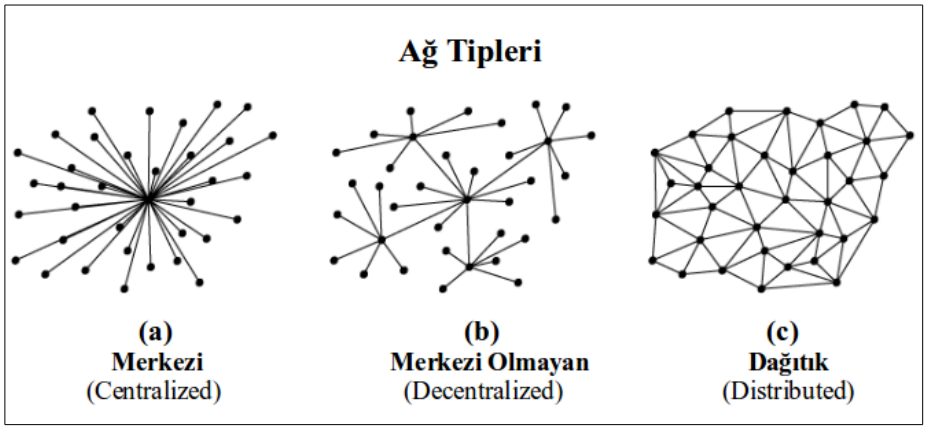
Bitcoin transferlerinin güvenliği ve üretiminde kriptoloji kullanıldığı için kripto-para (cryptocurrency) olarak da tanımlanır. *Bitcoin* bir şirket ya da kurum değildir, herhangi bir yönetim merkezi yoktur, herhangi bir kişi ya da kuruma ait değildir, resmi temsilcisi yoktur. Herhangi ülkenin merkez bankasıyla ilişkili olmadığı için hiçbir ülkenin ekonomik durumundan da etkilenmez [38].

Bitcoin sisteminde ödemelerde gecikme, sıkıntılı banka transferleri, EFT, Havale, SWIFT masrafları, hesap işletim ve kredi kartı ücretleri yoktur. Herhangi biri, *7/24*, ücretsiz olarak birkaç dakika içerisinde başka birine, bilgisayar veya cep telefonu kullanarak *Bitcoin* gönderebilir. Hiç bir hükümet yetkilisi bu fonlara el koyamaz ve hiç bir banka bu transferleri engelleyemez [39].

Bitcoin belirli bir seviyede anonimlik sağlar. Ne kadar anonimlik istendiği, kişisel bir tercih olup, %100 anonimliğin garantisi, hiç bir sistemde verilemez. *Bitcoin* transferleri, *Bitcoin* cüzdan adresleri arasında gerçekleşir. *Bitcoin* cüzdan adresi, geleneksel bankacılık sistemindeki, hesap numarasına benzetilebilir. Bu adresler rakam ve harflerden oluşan, kimlik, lokasyon ve diğer hiç bir kişisel bilgiyi içermeyen, karışık bir dizedir (string). Fakat, *Bitcoin* cüzdan adresini bildiğiniz birisinin, tüm *Bitcoin* işlemlerini görmeniz mümkündür, sistem bu anlamda çok şeffaftır [34,36,40].

Bitcoin ağı, merkezi olmayan ve uçtan uca bağlı bir yapıya sahiptir (*Şekil 2.2*). Merkezi bir sunucusu veya kontrol noktası yoktur. Geleneksel para aktarma (bankalar, aracı kurumlar, VISA, PayPal gibi) sistemleri genellikle merkezi veya uçları birbirine tam bağlı dağıtık yapıdadırlar. Merkezi ağlarda, merkezdeki sunucu arızalandığında veya hacklendiğinde, sistemin tamamı risk altındadır. Ayrıca tüm güvenlik, merkezi sunucuyu işleten kuruluşa teslim

edilmiş durumdadır. Kuruluş iflas ederse veya hileli işlemler yaparsa, kullanıcılar zor durumlarda kalabilirler.



Şekil 2.2: Ağ tipleri*

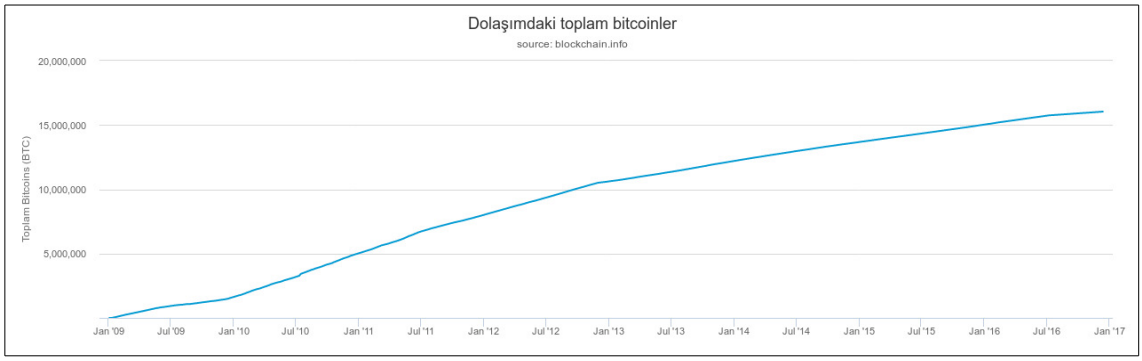
Bitcoin bir merkezden üretilmez, *Bitcoin* arzı, merkezi olmayan küresel ağdaki gönüllü bilgisayarların işlemci güçleriyle yapılır. Açık kaynak kodlu *madenci yazılımını* çalıştırarak, *Bitcoin* ağına dahil olan herkes, isterse ***madenci*** olabilir ve *Bitcoin* üretebilir. *Bitcoin*'ler, madencilik adı verilen, transfer işlemleriyle uğraşırken karmaşık bir matematik problemini, birbirleriyle yarışarak çözen, madenciler aracılığıyla arz edilir. Problemi çözen madenci belli miktar *Bitcoin* ile ödüllendirilir. Problem sürekli olarak zorlaşır ve madencilere verilen ödül yaklaşık her dört yılda bir yarıya iner. Maksimum BTC sayısı 21 milyonla sınırlıdır. Hiç kimse, hiç bir otorite, *Bitcoin* sistemine dışarıdan para arz edemez. Oysa, kağıt banknotlar halindeki itibari para, merkezi otoriteler tarafından basılır ve istediğinde ek para arzı sağlanır.

Bitcoin sistemi, toplam 21.000.000 *Bitcoin* üretilebilecek şekilde tanımlanmıştır. 1.Aralık..2016 itibarıyla, 16.018.575 *Bitcoin* dolaşımdadır. 2140 yılına kadar 4.981.425 *Bitcoin* ise madenciler tarafından yapılacak olan yeni blok üretimlerine karşılık, madencilere verilerek, *Bitcoin* arzı yapılacaktır. *Şekil 2.3*'ten kümülatif olarak arz edilen *Bitcoin*'ler görülebilir.

Bitcoin arzı azalarak devam ettiği ve 2140 yılından sonra *Bitcoin* arzı yapılmayacağı

* Her bir nokta bir bilgisayar olarak düşünülebilir.

için, *Bitcoin*'in deflasyonist bir para olma eğilimi olabilir. Yeteri kadar *Bitcoin* olmadığından, eğer *Bitcoin*'e talep artarsa, aşırı değer kazanabilecektir.



Şekil 2.3: *Bitcoin* sistemine arz edilen toplam *Bitcoin*'ler*

2009'dan bu yana gerçekleştirilen tüm transfer işlemleri, *Blok-Zincir* adı verilen, küresel hesap defterinde tutulur. *Blok-Zincir*, merkezi bir kayıt ve kontrol mekanizması olmadan değer üretilmesini, transfer edilmesini ve saklanmasını sağlar. Bu defteri, dileyen herkes tutabilir, inceleyebilir, işlemlerin doğruluğunu kontrol edebilir. Bu deftere kayıtları madenciler yazarlar, başka bir deyişle *Bitcoin* ağının güvenliğini **madenciler** sağlarlar. *Blok-Zincir* dağıtık, açık ve güvenilir mutabakat sistemidir.

Bitcoin, işlem protokolünün, merkezi olmayan ağın ve dağıtık işlem buluşlarının ilk uygulamasıdır [34]. Aynı zamanda, diğer kripto-paralar için dijital altın standardıdır. *Bitcoin*, kısaca itibari para sistemine alternatif, yeni dijital bir parasal sistemdir.

2.2 Bitcoin'in Tarihçesi

2008 yılındaki küresel finansal krizde, ülkeler uçurumun kenarına kadar yaklaştılar. 1930'lardaki *Büyük Dünya Bunalım*'ını tekrar yaşamamak için merkez bankaları, para basıp, faiz oranlarını azalttılar. Batmakta olan pek çok banka, iflasın eşiğinden kurtarıldı, ancak bu kurtarmanın bedeli, para birimlerinin değer kaybı ve vergi artışları olarak halka yansıdı [36].

---

* Kaynak: https://blockchain.info/tr/charts/total-*Bitcoins*?timespan=all#

Merkezi olmayan para birimi *Bitcoin*, tam da aracı kurumlara, bankalara ve merkez bankalarına, hatta hükümetlere güvenin azaldığı bir ortamda ortaya çıktı. *Bitcoin*, Satoshi Nakamoto mahlas ismiyle, 2008 yılında yazılan "*Bitcoin*: Uçtan Uca Elektronik Ödeme Sistemi" isimli makaleyle dünyaya duyuruldu [41]. Satoshi'nin getirdiği yenilik, dağıtık işlemci güçlerini kullanarak her 10 dakikada bir transfer işlemlerini onaylayan bir mekanizmayla, çifte harcamayı engellemiş olmasıdır.

Satoshi Nakamoto, güvensiz ve potansiyel olarak hileli, dağıtık bir işlemci ağında, bilgi paylaşımının nasıl olacağı problemi olarak bilinen "*Bizans Generalleri*" problemine, merkezi bir otorite kullanmadan, *"iş ispatı"* kavramıyla yeni bir çözüm önermiştir. Satoshi Nakamoto'nun Nisan 2011'de ortalıktan kaybolmasına rağmen, sistem tamamen şeffaf ve matematik prensipleri çerçevesinde çalışmaya devam etmektedir [34].

2009 yılında çalışmaya başlayan *Bitcoin* ağının, şu anki toplam işlemci gücü, dünyanın en hızlı bilgisayarlarının gücünden fazladır. 1 Aralık 2016 itibarıyla, *Bitcoin*'in toplam pazar değeri yaklaşık 12 Milyar Amerikan Doları'dır. Bugüne kadar, transfer yapılan en büyük tutar 194.993 BTC'dir (yaklaşık 147 Milyon dolar). Bu işlem Kasım 2013'te hiç bir işlem masrafı alınmadan gerçekleştirilmiştir.

2.3 Bitcoin'in Geleneksel Para Sisteminden Farkları

Bitcoin'in itibari paradan, mali sistem ve işlem yapma açısından farkları [34,36];

1. *Bitcoin* ağı, merkezi değildir, herhangi bir aracı, yönetici, denetletiyici yoktur, uçtan uca birbirine bağlı, gönüllü katılım sağlayan bilgisayarlardan oluşur. Bağlı tüm bilgisayarlar, açık kaynak kodlu, aynı programı çalıştırırlar, hepsi tüm işlemleri görür, hepsi tüm işlem geçmişini isterse tutabilir, istedikleri an diğer uçlardan işlem geçmişlerini alabilirler.

2. Dijital itibari paraların işlemlerinde, güvenilen bir aracıya ihtiyaç duyulurken, *Bitcoin*'de aracıya ve güvene ihtiyaç yoktur. Aracılık sisteminin maliyetleri yüksektir ve güvenlik açıklarına gebedir.

3. *Bitcoin* borç değil, değer taşıyıcıdır. Banka hesaplarındaki paralar, bir tür borç senedidir. Bir hesap, bir bankanın müşterisine olan borcunu temsil eder. *Bitcoin* bir borcu temsil etmez. Banka ve hükümetlerin, banka hesapları üzerindeki kontrol güçleri, *Bitcoin* de yoktur. Hiçbir güç *Bitcoin*'in kullanılmasını engelleyemez, yapılan işlemi geri alamaz.

4. Devletler para arzıyla ve kısıtlamasıyla bankadaki paranın değerini etkileyecek (enflasyon ve deflasyon) mali kararlar alabilirler. Oysa, *Bitcoin* arzı üzerinde banka ve devletlerin etkisi yoktur. Sisteme dışardan para arzı yapılamaz, dolayısıyla enflasyon oluşmaz. Para arzı, başarılı blok oluşturan madencilere verilen ödüller şeklindedir.

5. İşlemler anonimdir, takma adlarla yapılır. İşlemlerin gerçek kişilerle, kuruluşlarla, banka hesaplarıyla bağlantısı yoktur. İşlemler *Bitcoin* adresleri arasında gerçekleşir. *Bitcoin* adresleri dijital rumuzlardır. Tüm bunlara rağmen, %100 anonimlik mümkün değildir.

6. İşlemler şeffaftır, hızlı ve küreseldir. 2009 yılındaki ilk *Bitcoin* arzından bu yana, tüm işlemler, isteyen herkes tarafından görülebilir. Yapılan işlemler, neredeyse anında tüm dünyadaki bitcoin ağına dağıtılır, makul süre içerisinde de onaylanır.

7. İtibari fiziksel parada işlemlerin hafızası yoktur. *Bitcoin* işlem hafızası ise küresel hesap defteri olan *Blok-Zincir* veritabanlarında tutulur. *Bitcoin* kullanacak birisinin, *Bitcoin* sahibi olup olmadığı, daha önceki kayıtlarına bakılarak karar verilir.

8. İşlemler geri alınamaz. Hiçbir otorite, devlet, kişi, bilgisayar programcısı, hatta sistemi tasarlayanlar dahil, madencinin biri tarafından onaylanıp, diğerlerince de kabul edilmiş ve *Blok-Zincir'*e yazılmış, bir işlemi değiştiremez, geri alamaz.

9. İzin gerektirmez. İşlem yapmak için hiçbir kimseden veya kuruluştan izin alınması gerekmez, hiç kimse işlem yapılmasına engel olamaz.

10. Sistem güvenlidir. Güvenlik matematiksel olarak güvenilirliği ispatlanmış,

kriptografik dijital imzalama metotları kullanılarak gerçekleştirilir. Kötü niyetli kişilerin veriler üzerinde manüpülasyon yapması, gizli/açık anahtar şifreleme yöntemi kullanılması sebebiyle, mümkün değildir.

2.4 Bitcoin Piyasası

22 Mayıs 2010'da *Laszlo* takma isimli bir kullanıcı, *Bitcoin* kullanarak, 2 adet pizza satın almıştır. Pizzayı başka bir *Bitcoin* kullanıcısı, 10.000 *Bitcoin* karşılığında, Dominos'tan *Laszlo* adına satın alıp adresine göndertmiştir. 22 Mayıs 2010, *Bitcoin*'in tarihte ilk defa takas aracı olarak kullanıldığı gündür. Dünyanın pek çok yerinde 22 Mayıs *Laszlo'nun Pizza Günü* olarak kutlanmaktadır.

Bitcoin'in değeri, diğer her türlü mal, ürün ve parada olduğu gibi, talep ve arzın dengelendiği noktada oluşur. *Bitcoin*'in değeri, coğrafi olarak uygunluğu, yaygınlığı, kabul edilirliği, yatırımcının ona olan güveni, gerçek hayatta ödeme aracı olabilmesi ve marketin o anki duyarlılığı ile ilişkilidir [42].

1 Aralık 2016 tarihi itibarıyla**[*]**;

- Piyasada toplam ***16.018.575*** *Bitcoin* vardır.
- 1 *Bitcoin*, ***752*** Amerikan Dolarıdır.
- Piyasa Değeri (Market Capitalization) ***12.069.035.148*** Amerikan Dolarıdır
- Gün içi yapılan toplam işlem ***259.387*** BTCdir.
- Gün içi yapılan toplam işlem ***195.432.628*** Amerikan Dolarıdır.
- Gün içi 26.804.422 Amerikan Dolarlık, Dolar ile BTC takası yapılmıştır.

---

* Veriler http://www.blockchain.info/charts adresinden temin edilmiştir.

Bitcoin arkasında devletler, merkez bankaları, şirketler yoktur, bireylere dayalıdır. *Bitcoin*'i kullanan birey sayısı arttıkça, daha iyi çalışan ve speküle edilemez bir piyasa haline gelecektir. 02 Ocak 2011 tarihinde 0,30$ olan *Bitcoin*, 29 Kasım 2013'te 1,242 Amerikan Dolarına kadar yükselmiştir [43]. 2014 yılının sonlarında ise 300$'a kadar düşmüştür. Bu düşüş, doların değerlenmeye başlaması, *Bitcoin*'i yasal olmayan faaliyetlerde kullanan ***Silk Road*** sitesinin kapatılması, Çin hükümetinin *Bitcoin* aleyhine düzenlemeleri veya bunun olağan bir piyasa hareketi olması gibi görüşlerle açıklanmaya çalışılmaktadır [44,45]. Ancak, *Şekil 2.4*'ten de görülebileceği üzere *Bitcoin,* 2016 yılında tekrar yükseliş trendine girmiştir.

Bitcoin kullanıcısı arttıkça, *Bitcoin* kullanımı yaygınlaştıkça, fiyat oynaklığının azalması beklenmektedir. *Bitcoin* fiyatının, ucuz olduğunu düşünen yatırımcılar *Bitcoin* alıp, uzun vade saklayıp, hedeflediği fiyata geldiğinde satmayı planlayabilirler.

Silikon vadisi girişimcilerinden Chris Dixon, gelecekte 1 *Bitcoin* değerinin 100.000 Amerikan Doları olacağını tahmin etmektedir [46]. Uzun dönemde, 1 satoshi'nin 1 cent'e eşitleneceği ve 1 *Bitcoin*'in, 1.000.000 Amerikan Doları olacağını iddia edenler de vardır [47].

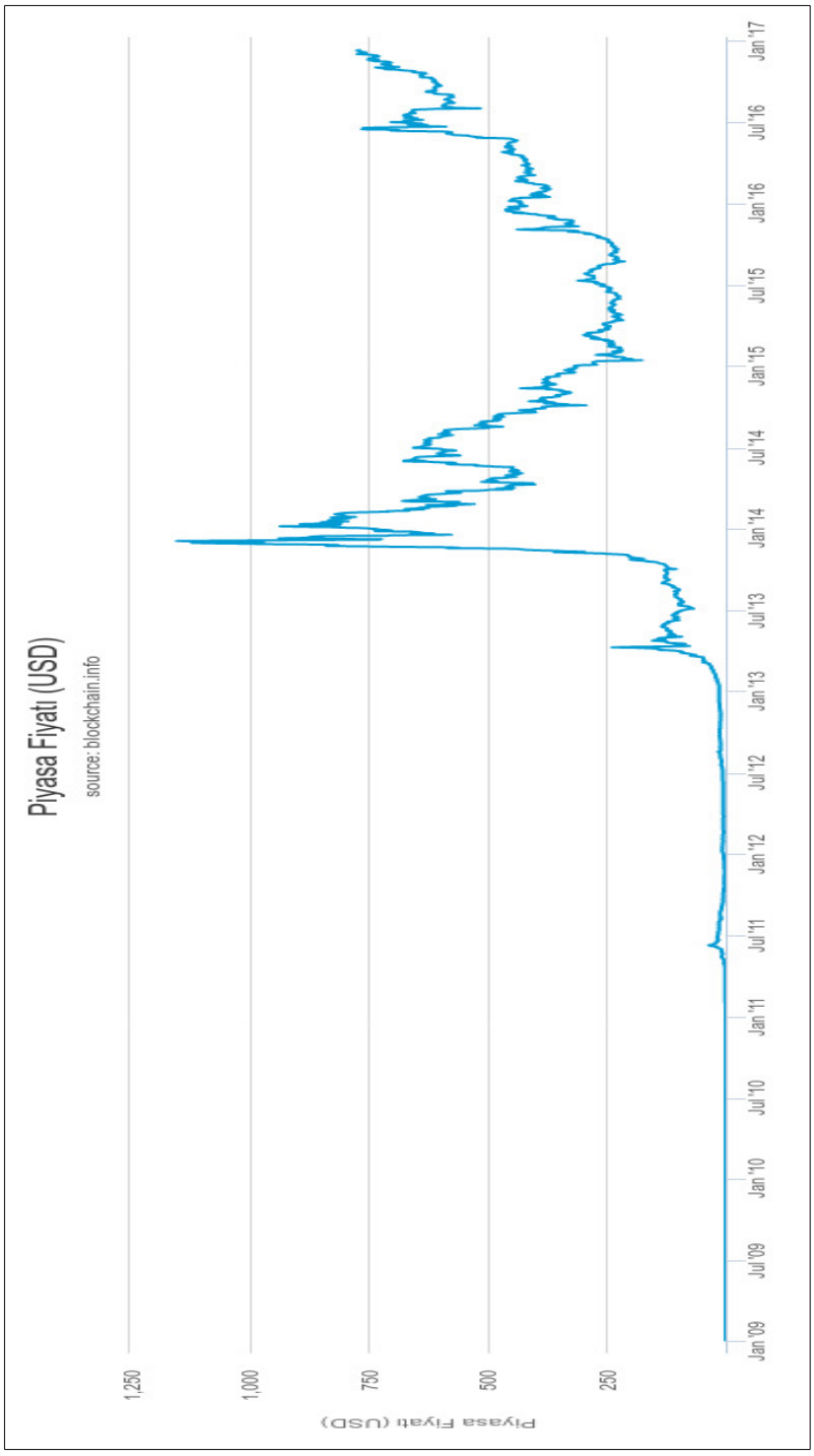
Hiç kimsenin geleceği tam olarak tahmin edemeyeceğini unutmamak gerekir. *Bitcoin*, çıktığı ilk günden bu yana yaygınlaşmakta ve insanların güvenini kazanmakta olsa da, hiç bir para birimi felaketler ve zor zamanlar karşısında tam olarak güvenli olamaz. Örneğin; Weimar Cumhuriyeti (1918-1933) döneminde, Alman Markı hiperenflasyon yüzünden değersiz hale gelmiştir. Günümüzde ise Zimbabve Doları değersizleşmiştir*. *Bitcoin*'in, para arzı sınırlı olduğundan, hiperenflasyon sebebiyle değerinin düşmesi beklenmez. Fakat, teknolojik başarısızlıklar, *Bitcoin* karşısında diğer para birimlerinin aşırı değer kazanması, politik konular ve ülkelerin düzenlemeleri *Bitcoin*'in değerini düşürebilecektir [48].

2.5 Bitcoin Piyasasının Altın ve Foreks Piyasası İle Karşılaştırması

Unutmamak gerekir ki, on binlerce yıldır, altının kalıcılığına, nadir bulunuşuna ve kolay parçalara ayrılabilmesine, enflasyon ve ekonomik çalkantılara karşı güvenli bir yatırım aracı

---

* 2006, 2008 ve 2009 yıllarında yapılan üç ayrı yeniden değerlendirmeye rağmen Zimbabve dolarının bir para birimi olarak kullanılması 12 Nisan 2009'da durduruldumuştur.



Şekil 2.4: *Bitcoin* Piyasa Fiyatı

olmasına alışığız. *Bitcoin* çok yeni fakat bir o kadar hızlı kabul gören yeni nesil para birimidir.

Bitcoin, altın ve forekste olduğu gibi, dalgalı bir piyasada, ana sermayeyi koruyarak kar etmek için, *zarar kes* (stop loss) ve *kârı al* (take profit) stratejileri ile işlem yapılabilen bir piyasadır. *Bitcoin*, fiziki olmamasından dolayı altından çok, kaldıraç kullanılmayan foreks kontratlarına benzetilebilir [42].

Foreks piyasalarında *5/24* işlem yapılabilirken, *Bitcoin 7/24* işleme hazırdır, ancak foreks piyasasında günlük trilyonlarca Amerikan Doları işlem yapılırken, görece daha küçük ve yeni olan *Bitcoin* piyasasında yaklaşık 200 milyon Amerikan Doları işlem yapılmaktadır [42].

3. TEKNOLOJİK ARKA PLAN

3.1 Kriptolojik Özet Fonksiyonu (Hash Function)

Özet fonksiyonları, farklı uzunluktaki dijital mesajlardan, sabit uzunlukta bir mesaj özeti çıkartırlar. Özet fonksiyonu hızlı çalışmalı, farklı girdilerin farklı çıktıları olmalı (çarpışmaya direnme), özet mesajdan yola çıkarak özetlenen mesaj hakkında çeşitli bilgiler üretilememelidir. Özet mesajları incelediğinizde rastgele oluşmuş gibi görünmelidirler.

Şekil 3.1: Sha-256 özet fonksiyonu örneği*

Bitcoin işlemlerinde SHA-256 isimli özet fonksiyonu kullanılır. SHA-256, girilen mesajın uzunluğundan bağımsız, 256-bit (32 byte) mesaj özeti oluşturur. Kriptografik olarak en güvenilir özetleme fonksiyonlarındandır. Başka bir deyişle mesaj özetine bakarak mesajın ne olduğu kestirilemez.

SHA-256'da, mesaj girdisi ne olursa olsun, mesaj özeti 256 tane ardışık, 0 veya 1'den oluşan bir dizedir. Okuma kolaylığı olması açısından genellikle, dörtlü gruplar halinde onaltılık sistemle yazılırlar. Bu durumda, mesaj özetleri ardışık 64 adet (*0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F*) harfleri kullanılarak yazılırlar.

---

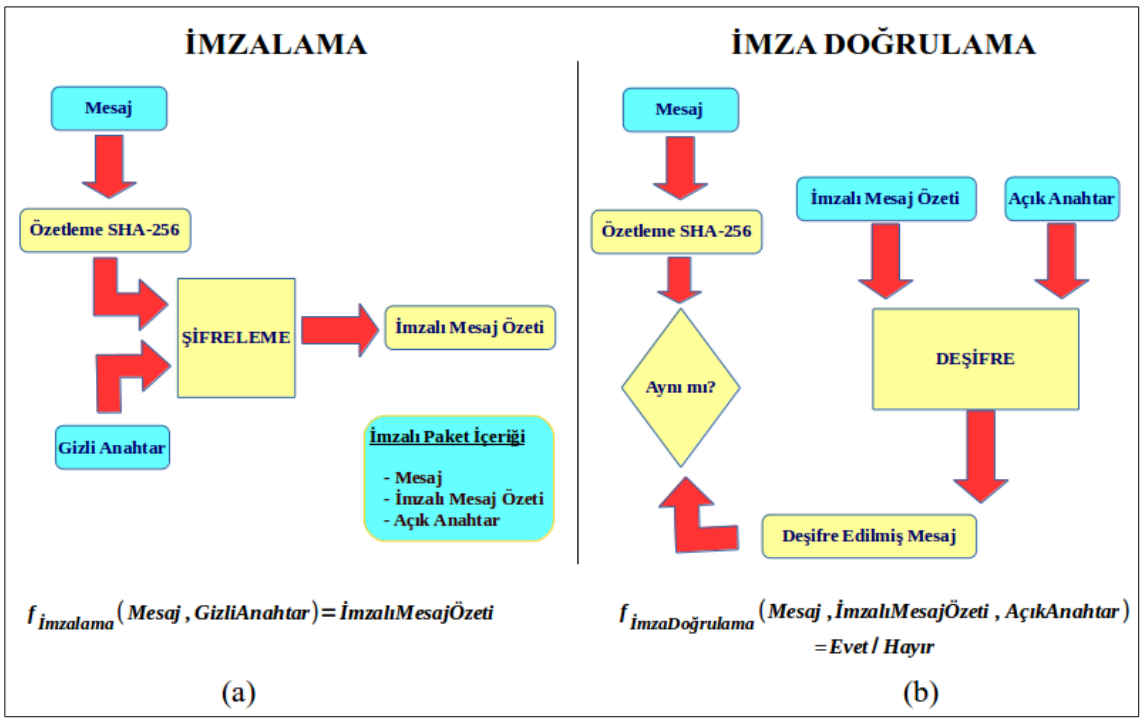
* Mesajda yapılan ufak bir değişiklik (nokta işareti ilave edilmiştir), özeti tamamen değiştirmektedir

Teorik olarak, 256 adet ardışık 0 veya 1'le, $2^{256} \approx 1.15 \times 10^{77}$ farklı özet elde edilebilir. Bu, çok büyük bir rakamdır.

3.2 Dijital İmza

Dijital imza, ***gizli*** (private) ve ***açık*** (public) anahtar ikilisiyle çalışan, matematiksel olarak güvenilirliği ispatlanmış şifreleme yöntemidir. Dijital imza atmak isteyen herkesin kendine ait, gizli ve açık anahtarı olması gereklidir. Gizli anahtarla şifrelenen bir mesaj, sadece şifreleyene ait açık anahtarla çözülebilir. Gizli anahtar adı üzerinde gizlidir, sadece imzalayanda bulunur, kimseyle paylaşılmaması gerekir. Açık anahtarın dağıtılmasında, hatta imzalı mesaja ek olarak gönderilmesinde hiç bir mahsur yoktur.

Gizli anahtarla yapılan şifreleme işlemine ***imzalama*** denir. Hızlı olması ve fazla yer kaplamasının önüne geçilmesi için genellikle, mesajın önce özeti çıkartılır, özet imzalanır, yani şifrelenir. *Şekil 3.2*'de *imzalama* ve *imza doğrulama* şematik olarak gösterilmektedir.



Şekil 3.2: İmzalama (a) ve İmza Doğrulama (b)

Mesaj gönderen kişi, mesajı ve imzalı mesaj özetini karşı tarafa gönderir. Alıcı, göndericinin açık anahtarı ile imzalı mesaj özetini deşifre eder. Deşifre edilen imzalı mesaj özeti, alınan mesajın özetiyle aynıysa, mesajın kesinlikle gönderici tarafından imzalanmış olduğu ortaya çıkar. Mesajda ufak bir değişiklik yapıldıysa, deşifre edilmiş mesaj özeti ile alınan mesajın özeti birbirine uymayacaktır.

İmzası doğrulanmış bir mesajda, mesajı imzalayan kişinin kimliği doğrulanmıştır (authentication), mesajı imzalayan tarafından inkar edilemezdir (non-repudiation), mesajın imzalandığı haliyle durduğu, hiç bir şekilde değiştirilmediği de (integrity) garanti altındadır.

Gizli anahtar, *Bitcoin* sisteminin temelidir, asla kaybedilmemeli, kimseyle paylaşılmamalıdır. Açık anahtar, gizli anahtardan eliptik eğri çarpım (elliptic curve multiplication, ECM) yöntemiyle elde edilir. Bu fonksiyon tek yönlü bir fonksiyondur. Başka bir deyişle, gizli anahtardan açık anahtar üretilebilir ancak, açık anahtardan gizli anahtarı bulmak mümkün değildir [34].

Gizli anahtar, 256 bit rastgele 0 ve 1'lerden oluşur. Her 4 biti, onaltılık gösterime göre yazılmış, örnek bir gizli anahtar şu şekilde olacaktır:

E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262

3.2.1 Dijital İmzanın Güvenilirliği

256 adet ardışık 0 veya 1'le, $2^{256} \approx 1.15 \times 10^{77}$ farklı gizli anahtar üretilebilir. Gizli anahtar üretmek, 1 ile 2^{256} arasında rastgele bir tam sayı üretmek olarak da görülebilir. Herhangi iki farklı kişinin gizli anahtarının aynı olma ihtimali, yaklaşık 10^{77} de 1'dir. 10^{77} çok büyük bir rakamdır, gözlemlenebilen evrende $\approx 10^{80}$ atom olduğu düşünülmektedir [49].

Eğer açık anahtardan, gizli anahtar elde edilebiliyor olsaydı, sistem tamamen güvensiz olmuş olurdu. Elinizde bir açık anahtar varsa, bunun gizli anahtarını bulmak isteyen birisinin, kaba kuvvet yöntemiyle (brute force), tüm olasılıkları denemekten başka çaresi yoktur. 1' den başlayıp 2^{256} 'ya kadar tüm gizli anahtarları, ECM (elliptic curve multiplication)

fonksiyonundan geçirip elde edilen açık anahtarın, aranan açık anahtar olup olmadığı kontrol edilmelidir. Ortalamada arama uzayının yarısında aranan gizli anahtarın bulduğu varsayılsa, $2^{256} \div 2 = 2^{255} \approx 10^{76}$ deneme yapılması gerekecektir. Günümüz süper-bilgisayarlarında dahi bu deneme, milyar kere milyar yıl sürebilecektir. Özetle, açık anahtardan, gizli anahtarı elde etmek pratik olarak mümkün değildir.

Henüz kuantum bilgisayarlar icat edilmemiş olmasına rağmen, bu bilgisayarlar sebebiyle, gelecekte açık/gizli anahtar çiftinin güvenilirliği risk altına girebilecektir. Bu durumda ileri kuantum açık/gizli anahtar çiftleri veya farklı kriptolama metotları devreye alınarak, dijital imzalamanın güvenilirliği korunmaya devam edilebilecektir [50].

3.3 Bitcoin Adresi

Bitcoin adresi veya *Bitcoin cüzdan adresi*, geleneksel bankacılıktaki hesap numarasına benzetilebilir. Tüm giriş ve çıkış işlemleri *Bitcoin* adreslerine yansır. *Bitcoin* adresi, 27 ile 34 adet sayı ve harften oluşur, 1 veya 3 rakamı ile başlar [36,51].

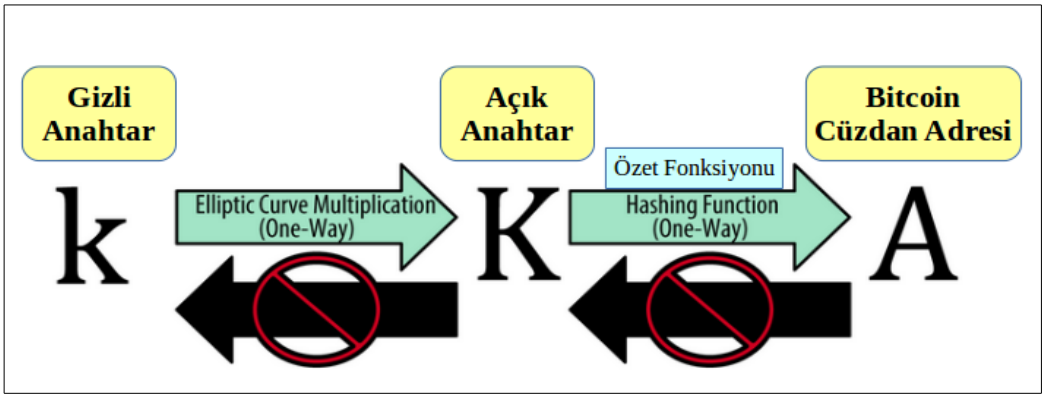
Örnek *Bitcoin* adresi: **`1L5wSMgerhHg8GZGcsNmAx5EXMRXSKR3He`**

Şekil 3.3'de gösterildiği gibi, bir *Bitcoin* adresi açık anahtardan, açık anahtar ise gizli anahtardan tek yönlü fonksiyonlarla üretilirler*. *Bitcoin* adreslerinin kullanılmasında büyük ve küçük harf duyarlılığı vardır [34,52].

Bir *Bitcoin* adresinden, açık anahtarı elde etmek mümkün olmadığı gibi, gizli anahtarı elde etmek de mümkün değildir. *Bitcoin* adresi olarak doğrudan açık anahtarın kullanılmaması, bazı durumlarda ekstra güvenlik önlemi olarak da görülebilir.

---

* Açık anahtardan, *Bitcoin* adresi üretmek için http://en.bitcoinwiki.org/Bitcoin_address



Şekil 3.3: *Bitcoin* Adresi Elde Edilmesi

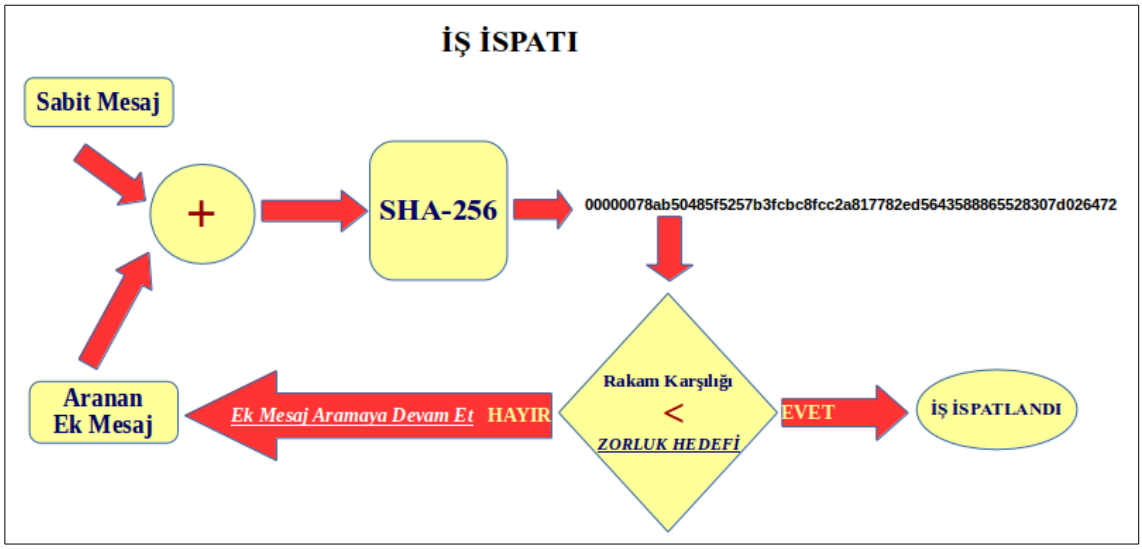
Harf ve rakamlardan oluşan *Bitcoin* adreslerini ezberlemek veya yazmak zor olduğundan, pratikte *Şekil 3.4*'te görüldüğü gibi iki boyutlu Barkod olarak bilinen QR kodları kullanılabilmektedir.

1L5wSMgerhHg8GZGcsNmAx5EXMRXSKR3He

Şekil 3.4: Bir Bitcoin adresinin QR Kodu

3.4 İş İspatı (Proof of Work)

Bir bilgisayarın, bir iş için çalıştığının ispatlanmasında kullanılan bir metottur. Bilgisayarlar bazı işlemleri, çok hızlı yapabilirler, örneğin e-posta atmak, çok hızlı yapılabilir bir işlemdir. Bu sebeple, bir bilgisayarın dakikalar içerisinde milyonlarca, istenmeyen e-posta atması da mümkündür. Bunu engellemek için, e-posta sunucusu, e-posta atan bilgisayardan, biraz çalışmasını ve bunu ispatlamasını isteyebilir. Bu sayede, e-posta atmak isteyen bilgisayar, biraz çalışarak, birkaç e-posta atabilecek ama milyonlarca e-posta atması için gerekli zamanı bulamayacaktır.



Şekil 3.5: İş İspatı Algoritması

İş ispatı için genellikle SHA-256 özet fonksiyonu kullanılır. SHA-256 özet fonksiyonu, 256 adet ardışık, neredeyse rastgele olan 0 ve 1'den oluşan bir çıktı üretir. 256 bitlik bu diziyi, tam sayı olarak ifade etmek mümkündür. Bu durumda, SHA-256, $0, 1, 2, 3, \ldots, (2^{256}-1)$ arasında rastgele bir sayı üretmiş olacaktır. İş ispatı yapmak isteyen bilgisayardan, *Şekil 3.5*'te görüldüğü gibi, sabit bir mesaja ek mesaj ekleyerek, SHA-256 ile özetledikten sonra, elde edilen özetin rakam karşılığının, önceden belirlenen bir rakamdan (***zorluk hedefinden***) küçük olması istenir. SHA-256 özet fonksiyonu kriptografik olarak güvenli bir algoritma olduğundan, sistem

defalarca deneme yapmadan, aranan ek mesajı bulması imkansızdır. Ayrıca ek mesajı bulmak zor, fakat ek mesajın bulunup bulunmadığının kontrolünü yapmak çok kolaydır. ***Zorluk hedefi***, ne kadar küçük olursa, iş ispatı o kadar zor olacaktır [53].

Çalıştığını ispatlayan bilgisayar, mesaj ve bulduğu ek mesajı ispat isteyen sunucuya gönderir, sunucunun ispatın doğru olup olmadığını kontrol etmesi çok kolaydır. Mesaja, ek mesajı ilave eder, özetleme algoritmasından geçirir, elde ettiği 256 bitlik özetin rakam karşılığının, ***zorluk hedefinden*** küçük olup olmadığına bakarak, iş ispatının yapılıp yapılmadığını kolayca kontrol edebilir. İş ispatı yapmak bulmaca çözmeye benzetilebilir, bulmaca çözmek zordur, ama çözülmüş bir bulmacanın kontrol edilmesi (iş ispatının kontrolü) kolaydır.

Bitcoin madencilerinin, transfer işlemlerinden bir blok oluşturması ve bunu yaparken birbirleriyle yarışmaları iş ispatı metotuyla gerçekleştirilir. Konu, "7.2 Madenciler Nasıl Çalışırlar ?" bölümünde de anlatılmaktadır.

4. BITCOIN SAHİPLİĞİ

4.1 Bitcoin Cüzdanı

Bitcoin dünyasına adım atmanın yolu, öncelikle bir *Bitcoin* cüzdanı edinmektir. Hem bilgisayarlar hem de tablet ve cep telefonları için pek çok *Bitcoin* cüzdan uygulaması bulunmaktadır. Bu yazılımlar yüklendikleri anda, yükleyene özel, gizli anahtar, açık anahtar ve *Bitcoin* adresini üretirler. Mevcut olan gizli anahtarın da, bu yazılımlara entegre edilmesi mümkündür. *Bitcoin* cüzdanlarında güvenlik, gizli anahtarla sağlanır, gizli anahtarın çalınması, gerçek fiziki para cüzdanınızı çaldırmaya benzetilebilir. Gizli anahtar güvenli bir ortamda saklanmalı, kimseyle paylaşılmamalıdır [35]. *Bitcoin* toplamak için *Bitcoin* adresine, sahip olunan *Bitcoin*'leri harcayabilmek için ise gizli anahtara ihtiyaç vardır.

Web tabanlı *Bitcoin* cüzdan servisleri, kullanıcıları adına gizli/açık anahtar üretir ve onların güvenliğinden sorumlu olurlar. Gizli anahtarı kendisinde saklayan şirketler, geçmişte bilgisayar korsanlarının saldırılarına maruz kalmış ve müşterilerinin *Bitcoin*'lerini çaldırmışlardır. Bu sebeple ünleri iyi değildir [36]. Haziran 2011'de, 478 farklı hesaptan, toplam 25.000 *Bitcoin* çalınmıştır. Oluşan güvensizlik ortamı sonucunda, bir saat gibi kısa bir sürede, 1 *Bitcoin*'in fiyatı, 19 Amerikan Dolarından, 0.01 Amerikan Dolarına düşmüştür.

Şekil 4.1'de görüldüğü gibi, özel donanım olarak üretilen *Bitcoin* cüzdanları da vardır*.

Şekil 4.1: Donanım olarak tasarlanmış bir *Bitcoin* Cüzdanı

* Donanımsal Bitcoin Cüzdanları için bakınız https://en.Bitcoin.it/wiki/Hardware_wallet

Bitcoin cüzdanları, temsil ettikleri *Bitcoin* adresine ilişkin tüm girdi, çıktıları gösterirler. Ayrıca, arzu edildiğinde başka bir *Bitcoin* adresine, *Bitcoin* transfer işlemini başlatabilirler. *Bitcoin* cüzdanları, aslında *Bitcoin* adresinin balansını, *Blok-Zincir* veritabanlarından okurlar. Tüm *Bitcoin* işlemleri, küresel hesap defterinde saklanır, cüzdanların bilgisayar veya cep telefonlarında sakladığı bir değer yoktur. Cüzdanlar yüklü oldukları bilgisayar veya cep telefonlarında, sadece gizli anahtar, açık anahtar ve *Bitcoin* adresini saklarlar.

Gizli anahtarınızı dijital hiç bir ortamda tutmaksızın, ürettikten hemen sonra bir kağıda bastırıp, kağıt cüzdan kullanma şansınız da vardır. Örneğin; http://bitaddress.org gibi adreslerden, kağıt cüzdan üretilmesi mümkündür. *Şekil 4.2*'de örnek bir kağıt *Bitcoin* cüzdanı gösterilmektedir.

Kağıt *Bitcoin* cüzdan adresine, *Bitcoin* transfer edilebilir, ancak cüzdandaki parayı harcamak için, gizli anahtarı kağıt ortamından, *Bitcoin* cüzdanlarından herhangi bir tanesine aktarmak gerekecektir. Gizli anahtarı, kağıt üzerindeki QR kodunu cep telefonlarına okutarak kolayca aktarmak mümkündür [34,36].

Kağıt cüzdanlar hırsızlığa açıktırlar, fotoğrafını çeken birisi dahi, cüzdanı ele geçirebilir. Buna engel olmak için, gizli anahtar, cüzdan sahibinin ezberindeki bir cümle ile şifrelenebilmektedir [34].

a) b)

Şekil 4.2: Kağıt Cüzdan (a) Bitcoin Adresi (b) Gizli Anahtar

Tüm *Bitcoin* işlemlerini tek bir *Bitcoin* adresinden yapmak mümkünse de, güvenlik ve anonimlik seviyesini artırmak için, her yeni *Bitcoin* işleminin yeni bir *Bitcoin* adresiyle yapılması tavsiye edilir. Farklı *Bitcoin* adresleri üretmek için, cüzdan uygulamaları farklı çözümler sunarlar. 100 tane rastgele açık/gizli anahtar üreterek çalışmaya başlayan cüzdanlara ***deterministik olmayan cüzdan***, tek bir gizli anahtarla başlayıp, her defasında özetini yeni gizli anahtar yaparak çalışan cüzdanlara ***deterministik cüzdan*** denir. Ayrıca bir grup kelimeyi, rastgele anahtar üretmek için kullanan cüzdanlar (mnemonic code) ve hiyerarşik deterministik cüzdanlar da mevcuttur (hierarchical deterministic wallets) [34].

Bitcoin transferi, *Bitcoin* cüzdan adresleri arasında gerçekleşir. *Bitcoin* adreslerinin kullanılmasında büyük ve küçük harf duyarlılığı vardır, yanlış kodlandığında, tanımsız adres oluşacağından transfer işlemi gerçekleşmeyecektir. Fakat, yanlış yazılan bir *Bitcoin* adresinin, 4.29 milyarda 1 ihtimalle, tanımlı bir adres olma ihtimali sebebiyle, yanlış işlem yapılma olasılığı vardır [36]. Bu sebeple, işlem yaparken *Bitcoin* adreslerinin QR kodlarının kullanılması tavsiye edilir.

4.2 Bitcoin Temini

4.2.1 Bitcoin Borsaları

Bitcoin temin etmenin en kolay yolu, *Bitcoin* satın almaktır. Ulusal paralarla, *Bitcoin borsalarından* (Bitcoin Exhange) *Bitcoin* satın almak mümkündür. Fiziki veya dijital itibari paralarla satın alınan *Bitcoin*, satın alana ait daha önceden tanımlanmış olan *Bitcoin* (cüzdan) adresine gider. *Bitcoin* cüzdanına para gelmesinin anlamı, *Bitcoin* adresine *Bitcoin* transfer edildiğinin küresel hesap defterine (*Blok-Zincir*) işlenmesinden başka bir şey değildir [36].

http://coinmarketcap.com/currencies/ veya https://bitcoinwisdom.com/ gibi adreslerden anlık olarak diğer para cinslerine göre, *Bitcoin* fiyatı izlenebilir.

Yasal problemler nedeniyle, henüz tüm dünyada hizmet veren *Bitcoin* borsası yoktur. https://howtobuybitcoins.info/#! ve http://www.coindesk.com/information/how-can-i-buy-bitcoins/ gibi adreslerden hangi ülkelerde, hangi *Bitcoin* borsalarının hizmet verdiğini görmek mümkündür. Farklı borsalar, farklı işlem masrafları almaktadırlar. Pek çok borsa, kendi

içerisinde alıcı ve satıcıları buluşturan alım-satım sistemi (trading engine) çalıştırmaktadır [36,54].

Bitcoin borsaları, kuruldukları ülkenin düzenleme ve denetlemelerine tabidirler, bu anlamda borsalar yatırımcılarından çeşitli kimlik bilgileri isteyebilmektedirler. Bazı *Bitcoin* borsaları *Bitcoin*'leri müşterileri adına saklasalar da, güvenlik açısından bireylerin kendi *Bitcoin*'lerini kendilerine ait cüzdanlarda saklamaları daha uygundur. Satın alınan *Bitcoin*'lerin bireylere ait *Bitcoin* cüzdanlarına aktarılabilmesi için, borsalara *Bitcoin* adreslerinin verilmesi gereklidir. Hem kimlik bilgilerine hem de cüzdan adreslerine sahip olan bir *Bitcoin* borsası, bireylerin anonimlik seviyesini düşürür. Bundan kurtulmak için, ikinci bir *Bitcoin* adresi daha tanımlanır ve ilk cüzdandaki *Bitcoin*'leri ikinci cüzdan adresine transfer ederek, anonimlik seviyesi yeniden arttırılabilir [36].

Bitcoin hiç bir otorite tarafından düzenlenip, denetlenmediği için *Bitcoin* borsalarında da benzer problemler vardır, örneğin *Bitcoin* borsasındaki bir hesap çalındığında, borsanın yükümlülüklerinin neler olduğu, halen tartışmalı konulardandır.

4.2.2 Birebir Ticaret

Bitcoin temin etmenin bir diğer yolu, satmak isteyen kişiden doğrudan satın almaktır. Alıcı ve satıcıyı buluşturan borsa gibi üçüncü bir taraf olmadığından, işlemler güven esasına göre gerçekleştirilmelidir. Örneğin; alıcı satıcının *Bitcoin* göndereceğine güvenerek ona havale veya EFT ile önce para göndermesi veya yüz yüze görüşmeleri gerekebilecektir. Doğrudan alıcı ve satıcı listelerini ve daha önce gerçekleştirdikleri işlemlerden dolayı güvenirliklerini https://gemini.com veya https://kraken.com gibi sitelerinden görmek mümkündür.

4.2.3 Bitcoin ATM'leri

Gittikçe yaygınlaşmakta olan, *Şekil 4.3*'te de gösterilen, *Bitcoin* ATM'lerinden *Bitcoin* almak da mümkündür. https://coinatmradar.com/ veya www.coindesk.com/bitcoin-atm-map/ adreslerinden nerelerde *Bitcoin* ATM'leri olduğu görülebilir [55]. 2013 yılı sonlarında Türkiye'de , İstanbul Atatürk Havalimanı'nda da bir *Bitcoin* ATM'si hizmete girmiştir [56].

Bitcoin ATM'leri genellikle, nakit veya kredi kartı ile *Bitcoin* adreslerine, *Bitcoin* transfer eden makinelerdir. *Bitcoin* ATM'leri, *Bitcoin* adresinin QR kodunu da okuyabilecek teknik donanımlara sahiptirler, bu sayede uzun ve karmaşık *Bitcoin* adreslerinin tuşlanmasına gerek kalmaz.

Şekil 4.3: Bir *Bitcoin* ATM'si

4.2.4 İlk Halka Arz Ve İlk Para Arzı

Pek çok ülkede, *Bitcoin* vergilendirilmemektedir. Bu nedenle, devam eden ve yeni başlayacak olan projelere, *Bitcoin* toplayarak küresel olarak fon sağlamak daha avantajlı olabilmektedir. Bu tür projelerin yasal alt yapıları henüz netleşmemiştir. *Bitcoin* transferinin geri alınması mümkün olmadığı için, bu yöntemler her türlü hile ve yolsuzluğa açıktır.

Bir *Bitcoin* veya altcoin şirketi, bir proje için ek fon sağlamak amacıyla, ***ilk halka arz*** (IPO- Initial Public Offering) gerçekleştirelebilir. Yatırımcılar hisse sahibi olur, temettü ödemeleri alabilirler [57,58].

Henüz madenciliği başlamamış *Bitcoin*'den türetilmiş olan altcoinler, yatırımcılara ***ilk para arzı*** (ICO - Initial Coin Offering) olarak sunulabilir. Yatırımcılar, yakın gelecekte fiyatının yükseleceğini düşündükleri altcoinlere yatırım yapabilirler [58].

4.2.5 Ticaret Yoluyla

Tüccarlar açısından *Bitcoin* temin etmenin elbette en klasik yolu, ürün ve hizmetlerini *Bitcoin* karşılığında satmaktır. Dünyanın pek çok bölgesinde, *Bitcoin* kullanarak her türlü ürün ve hizmeti, hem sanal hem de fiziki olarak temin etmek gün geçtikçe yaygınlaşmaktadır. *Şekil 4.4*'te *Bitcoin* ödemesi kabul eden bir çikolata işletmesi görülmektedir.

Şekil 4.4: *Bitcoin* ödemesi kabul eden bir işletme

Fazla yatırım yapmadan, Bitpay gibi servisler kullanarak, e-ticaret siteleri ve hatta dükkan veya bayi olarak hizmet veren geleneksel iş yerleri dahi *Bitcoin* kabul edebilirler [45].

Sanal ticarette alıcı ve satıcı arasındaki anlaşmazlıklar, Ebay ve PayPal gibi merkezi ödeme sistemlerinde geri ödeme ile çözülebilmesine rağmen, *Bitcoin* temelli sistemlerde geri ödeme söz konusu olmadığından, alıcı ve satıcı arasında doğrudan transfer yerine, güvenilir üçüncü bir *Bitcoin* adresine transferin gerçekleştirilmesi, anlaşmazlıkları çözmek için kullanılabilecektir [36].

Bir başka *Bitcoin* ticaret yönetimi ise açık artırma/müzayede düzenlemektir [59].

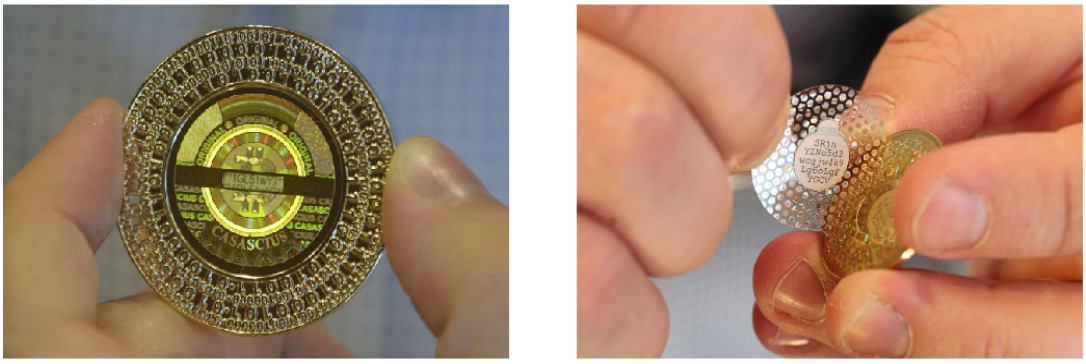
Kızılhaç ve GreenPeace gibi örgütlere *Bitcoin* bağışı yapmak mümkündür. Nepal'deki

depremden sonra Nepal Yardım Fonu'na doğrudan *Bitcoin* bağışı yapanlar olmuştur. Otel rezervazyonu yapmak için, https://btctrip.com/ gibi internet siteleri hizmet vermektedir. Ayrıca, kimlik bilgileri paylaşılmadan, yasal kumar ve gazino oyunlarının oynanması da mümkündür. https://www.vaultoro.com/ ve https://bitgold.com gibi sitelerden, *Bitcoin* ve Altın takası yapılabilmektedir. Ek olarak, bazı ülkelerde çeşitli faturaların *Bitcoin* ile ödenmesi de mümkündür [36].

4.2.6 Fiziki Bitcoin

Fiziksel olarak altın, gümüş ve bronz olarak *Bitcoin*'ler de üretilmiştir. Genellikle para koleksiyonerlerinin ilgi odağıdır. Yüz yüze yapılan işlemlerde kullanılmak üzere tasarlanmışlardır [60].

Şekil 4.5'te görüldüğü üzere, fiziki *Bitcoin*'lerin arkasında, bir *Bitcoin* cüzdan adresi ve gizli anahtar hologram olarak vardır. Gizli anahtar olmadan, *Bitcoin*'in dijitalleşmesi mümkün değildir. Gizli anahtara ulaşmak için ise fiziki *Bitcoin*'in üzerindeki hologramı kırmak gerekir. Başka bir deyişle, fiziki *Bitcoin* elden ele defalarca kullanılabilir ancak dijitalleşmesi istenirse tek kullanımlıktır [60,36]



Şekil 4.5: Fiziki Bitcoin örnekleri

4.2.7 Bitcoin Faiz Getirisi

Bitcoin sahiplerinin, tüm servetlerinin kontrolü kendilerindedir. Sahip oldukları servet, herhangi bir bankaya veya finansal sisteme emanet edilmiş değildir. *Bitcoin*'den faiz getirisi elde etmek isteyenler, *Bitcoin*'lerini başka bir *Bitcoin* adresine gönderip, faiz getirisi alabilirler. Fakat bu son derece riskli bir durumdur, gönderilen *Bitcoin*'lerin, gönüllülük esası dışında, geri alınma şansı yoktur. Örneğin; https://www.bsave.io/ sitesi, *Bitcoin*'e yaklaşık yıllık %2,51 faiz getirisi vermektedir. Bsave, dünyanın en büyük ve güvenilen *Bitcoin* borsası ve cüzdanı işleticilerinden olan *Coinbase* tarafından işletilmektedir. Faiz vermesinin amacı, kendi likiditesini sağlayabilmektir. Benzer şekilde *Bter*, *HaoBTC*, *BitBays*, *Bitcoincryptobank* gibi şirketler de, farklı faiz oranları ve yatırım seçenekleri sunmaktadırlar. *BTCJam* ise, kişiden kişiye borç verme sistemidir [61].

4.2.8 Diğer Temin Yöntemleri

www.bitcointalk.org forum sitesinde, imza kampanyası başlığında yapılan yapıcı yorumlara, diğer forum kullanıcıları da olumlu geri dönüşler yaparlarsa, ilgili forum üyesine *Bitcoin* hediye edilmektedir [62].

Bilgisayar programlama dillerinden PHP, SQL, JacaScript veya C# bilenlere, küçük programlar yazdırılarak, karşılığında *Bitcoin* ödemesi yapılabilmektedir [36].

Bazı internet siteleri ise, reklamlarını izleyen veya anket tarzı sitenin ihtiyacı olan bilgileri sağlayanlara, reklam giderlerinden olmak üzere, az miktarlarda (50 satoşi gibi) *Bitcoin* verebilmektedirler [63].

5. BITCOIN İŞLEMLERİ

5.1 İşlem Nedir ?

Bir *Bitcoin* adresine ait olan *Bitcoin*'leri başka bir *Bitcoin* adresine aktarmaya, işlem (transaction) denir. Sahip olunan *Bitcoin*'lerin harcanması, bir *Bitcoin* işlemidir. Bir işlemin girdileri ve çıktıları olur. Girdi toplamı ile çıktı toplamı eşit olmalıdır. İşlemin girdileri, daha önceki başka işlemlerin çıktılarıdır. Öteki deyişle, bir işlemdeki girdiler, daha önceki işlemlerin henüz harcanmamış olan çıktılarıdır. İşlemi yapan kişi, tüm girdileri ve transfer yapılacak olan *Bitcoin* adreslerini, gizli anahtarıyla dijital olarak imzalar.

Girdiler birden fazla işlemin çıktısı olabileceği gibi, çıktılar da birden fazla *Bitcoin* hesabına ait olabilir. Bir kişi, başka bir kişiye *Bitcoin* transferi yapmak istediğinde, ödeme yapacağı kişinin *Bitcoin* adresini bilmesi gerekir. Ödeme yapacağı kişinin QR kodunu kullanabileceği gibi, metin halinde *Bitcoin* adresini de kullanabilir. Transfer yapmak isteyen kişi *Bitcoin* Cüzdan programları ile işlemi başlatır.

Bitcoin işleminde girdiler, *Bitcoin* hesabına borç (debit), çıktılar transfere konu *Bitcoin* hesabına alacak (credit) olarak kaydedilir.

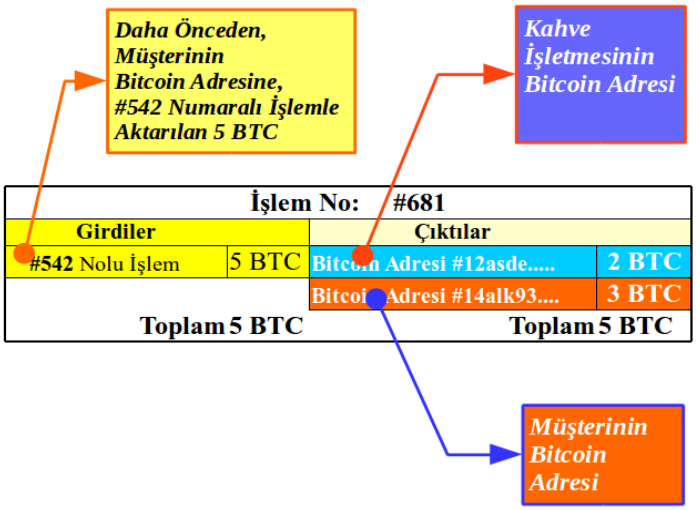
İşlem No: #192			
Girdiler		**Çıktılar**	
#112 Nolu İşlem	2 BTC	Bitcoin Adresi **#12asde.....**	3 BTC
#127 Nolu İşlem	5 BTC	Bitcoin Adresi **#13alk93....**	2 BTC
		Bitcoin Adresi **#14alk93....**	2 BTC
Toplam 7 BTC		**Toplam 7 BTC**	

Şekil 5.1: Sadeleştirilmiş örnek bir *Bitcoin* işlemi

Şekil 5.1'de, 7 BTC'ne sahip olan bir *Bitcoin* kullanıcısının, bunları 3 farklı adrese transfer işlemi örneklenmiştir. 192 numaralı işlemin girdileri, 112 ve 127 numaralı işlemlerin, daha önce harcanmamış (başka bir işlemde kullanılmamış) çıktılarıdır. 192 numaralı işlemin

çıktıları ise 3 farklı *Bitcoin* adresidir.

Bir işlem sonucunda, birden çok çıktı olabilir yani farklı adreslere *Bitcoin* gönderilebilir. Fakat, her bir çıktı, sadece 1 defa girdi olarak kullanılabilir. Tüm çıktılar, harcanmış veya harcanmamış (UTXO) olarak kategorize edilirler. Bir ödeme işleminin geçerli olabilmesi için, girdilerinin harcanmamış çıktılardan olması gereklidir. Harcanmamış çıktı harcandığında, harcanmış olarak tekrar kategorize edilir.



Şekil 5.2: *Bitcoin* ödemesi ile kahve içen bir müşterinin işlemi

Şekil 5.2'de ise 5 *Bitcoin*'i olan bir müşterinin, 2 *Bitcoin* karşılığında kahve alması ve işlem sonucunda artan 3 *Bitcoin*'i yine müşterinin kendisine ait olan *Bitcoin* adresine göndermesi örneklendirilmiştir. Güvenlik ve anonimlik seviyesini artırmak için, artan *Bitcoin*'lerin, yine müşteriye ait, fakat farklı bir *Bitcoin* adresine gönderilmesi tavsiye edilmektedir.

İstenirse, bir işlem sonucu aktarılan *Bitcoin*'lerin ne kadar zaman sonra kullanılabileceği de belirlenebilir. (Transaction Locktime) [34].

5.2 İşlem Masrafı ve İşlemin Onaylanması

Çıktıların değer toplamı girdilerin değer toplamından büyükse işlem reddedilir. Girdilerin değer toplamı çıktıların değer toplamından büyükse, aradaki farkı *Bitcoin* madencisi işlem masrafı olarak alabilir.

Ortalama bir *Bitcoin* işlemi 300-400 byte veri içerir. İşlem başlatıldığında, *Bitcoin* ağına bağlı uçlar arasında hızla yayılır. Kimse, işlemi gönderene güvenmek zorunda değildir, bağlı olunan ağın da güvenli olması gerekmez, zira işlem dijital imzalı olduğundan, işlemi alan uç önce dijital imzasını kontrol eder, imzası geçerli ise ağda işlemi yayar, aksi takdirde işlemi kabul etmez.

Bitcoin ağı uçtan uca bir ağdır. Her *Bitcoin* ucu, işlemlere başladığında, birkaç başka uçla iletişime geçer. Her uç ağa zayıf bağlıdır (loosely connected), zorunlu bir topoloji veya yapı yoktur. Tüm uçlar eşit öneme sahiptirler. *Bitcoin* işlemleri ve bloklar birbirleri arasında paylaşılır. Yeni bir *Bitcoin* işlemini doğrulayan her uç, bunu 3 ya da 4 komşu uca gönderir. Birkaç saniyede, yeni işlem tüm uçlara ulaşır.

Uçlar ağdan aldıkları *Bitcoin* işlemlerini veya blokları alır almaz, kendileri de doğrularlar. Böylelikle; ağ üzerinde bloklara veya işlemlere yapılacak her türlü atak veya saldırı geçersiz olmuş olur.

Bitcoin transfer işlemi saniyeler içerisinde gerçekleşir, ancak işlemin onaylanması zaman alır. *Bitcoin* madencileri ağdaki henüz onaylanmamış işlemlerden bir blok yapar ve işbirliği içerisinde bloğu ve içerdiği işlemleri onaylarlar. İlgili transferi içeren blok onaylanana kadar, transfer tam anlamıyla gerçekleşmiş değildir. Bloğun onaylanması, işlemin küresel işlem defterine işlenerek, geri dönüşü mümkün olmayan bir şekilde kesinleşmesi anlamına gelir. Küresel işlem defterindeki her blok ve her işlem kendi içerisinde tutarlıdır, kimse sahip olmadığı *Bitcoin*'i harcayamaz, her işlem işlemi yapan tarafından dijital olarak imzalanmıştır.

Alıcı tarafın, ödeme anında bilgisayarının açık olması, internete bağlı olması gerekmez. Çünkü transfer işlemi küresel hesap defterine işlenir. Alıcının *Bitcoin* cüzdanı, ilk internete bağlandığında küresel hesap defterinden kendi hesabının durumunu sorgular [36].

Normalde *Bitcoin* transferlerinden işlem masrafı alınmaz, fakat bazı *Bitcoin* cüzdanları işlemin madenciler tarafından onaylanmasını hızlandırmak amaçlı olarak, küçük miktarlarda işlem masrafı isteyebilmektedirler. Bir işlemin çabucak küresel hesap defterine, yani *Blok-Zincir* veritabanına işlenip onaylanması arzu edilen bir durumdur. Normalde işlem önceliği, işlemin onay için ne kadardır beklediği ve işlemin boyutuna göre hesaplanır. Temel prensip, işlemin onay için çok beklememesi ve dijital boyutu küçük işlemlerin öncelikli olmasıdır.

Bir işlemin onaylanması, ortalama olarak 10 dakika sürer. *Bitcoin* ağına gönderilmiş olan bir işlemin, madencilerin küresel hesap defterine işleyeceği ilk blokta olacağının garantisi yoktur. Çok büyük ihtimalle gelecek olan ilk blokta onaylanacaktır, fakat ağdaki gecikme veya diğer sebeplerle onaylanma işlemi sonraki bloklarda da olabilir [36].

Standart *Bitcoin* sisteminde, bir işlem eğer 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. Kullanıcı masrafı kabul ederse işlem yine öncelikli olur, eğer müşteri işlem masrafı ödemek istemezse işleminin önceliği düşürülür. Önceliği düşük olan işlemin, madenciler tarafından onaylanıp, küresel hesap defterine yazılması gecikebilir.

Bitcoin cüzdan uygulamalarının bir kısmı işlem emri verilmiş ama henüz onaylanmamış işlemleri "harcanmış" veya "onaylanmamış" (spent/unconfirmed) olarak gösterir, onaylandığında onaylandı bilgisi görülür. Pratikte, en az 6 uçtan onaylandı bilgisi gelmiş işlem, onaylandı olarak kabul edilir. *Bitcoin* sistemi her 10 dakikada bir, blok onayının üretilmesi için dinamik olarak kendini ayarlar. Alıcı tarafından alınan *Bitcoin*'lerin harcanabilmesi için gereken 6 ayrı uçtan gelecek olan "onaylandı" bilgisi, çok nadir de olsa, bazı durumlarda 1 saate kadar uzayabilir [36].

Bir işlemin çıktısı başka bir işlemin girdisi olabildiğinden, işlemler birbirine dede-baba-torun tarzında bağlıdırlar. Ancak *Bitcoin* ağı gevşek ve herhangi bir kısıtlaması olmayan bir ağ olduğundan, bazı durumlarda en alt işlem (torun) diğerlerinden önce sistemde yayılabilmektedir. Bu durumda işlemlerin bağlı olduğu ilk işlem (dede işlem) onaylanana kadar, diğer işlemler bekletilir (orphan transaction). Sistemin şişirilmesini engellemek için, bekletilebilecek işlem sayısı sınırlandırılmıştır [34].

5.3 Çifte Harcama

Bir *Bitcoin* işlemi ağda saniyeler içerisinde yayılır, fakat onaylanması zaman alır. Sahip olduğu *Bitcoin*'leri, dijital olarak imzalamak suretiyle harcayan bir kullanıcının başlattığı transfer işlemi, geçerli bir işlemdir. Geçersiz ödeme zaten hemen reddedilir. Kimse sahip olmadığı *Bitcoin*'leri harcayamaz. Bir *Bitcoin* adresine yapılan geçerli bir ödeme, birkaç saniye içerisinde tüm ağ kullanıcıları tarafından görülebilir hale gelir, ama bu işlemin onaylanacağının garantisi yoktur. Geçerli bir işlemin onaylanmasının, gecikmeli olması sebebiyle çifte harcama yapılma olasılığı vardır. Aynı paranın birden fazla harcanmasına ***çifte harcama*** denir. Bir işlem başlatıldığında ve henüz hiç onay almamışken, gerek alıcı gerek satıcı tarafından aynı *Bitcoin*'ler tekrar kullanılmaya kalkılırsa, çifte harcama riski oluşur. Çifte harcama riskini azaltmak için, *Bitcoin* ağına bağlı en az 6 farklı uçtan işlem onayı beklenir. Muhtemel çifte harcama atakları şunlardır [64]:

Yarış Atağı (Race Attack): Yeni başlatılmış bir işlemdeki *Bitcoin*, daha hiç onay almamışken, hızlı bir şekilde başka bir işlemde hileli olarak tekrar kullanılırsa, hangi işlemin onaylanacağını kestirmek zordur. *Bitcoin* ağına bağlanırken gelen bağlantı taleplerini reddedip, en iyi uca bağlanmayı tercih ederek bu ataktan korunulabilir. Kesin olarak zarar görmek istemeyen tüccar ise, hiç onay almamış ödemeyi kabul etmemeli, en az 6 onay beklemelidir. Daha sade anlatacak olursak; müşterinin gönderdiği *Bitcoin*'leri kendi cüzdanında onaysız olarak gören bir tüccar eğer 6 adet onay görmeden ürün ve hizmeti müşteriye sağlarsa, zarar etme olasılığı vardır. Zira bu işlem çifte harcama olmuş olabilir, sistem bunu ilerleyen zamanda reddedebilir. Bu durumda tüccar ödeme almadan ürün veya hizmet sunmuş olur, zarar eder.

Finney Atağı (Finney Attack): Bu atağın gerçekleşebilmesi için, dolandırıcılığa bir de madencinin dahil olması gerekir. Çok özel durumlarda, gerçekleştirmesi oldukça zor bir çifte harcama atağıdır. Sadece tek bir onayla, ödeme kabul edildiği durumlarda rastlanabilir.

Vektör 76 Atağı: Yarış atağı ve Finney atağının kombinasyonu şeklinde gerçekleştirilir. Tek onay almış bir işlemin, ikinci kez harcanması üzerine kurguludur. Ağa bağlanırken gelen bağlantı taleplerini reddedip, en iyi uca bağlanmayı tercih etmek bu ataktan koruyabilir.

Kaba Kuvvet Atağı (Brute Force Attack): Hızlı ve kötü niyetli madenciler grubu, çifte ödeme içeren bloğu onaylar ve onay bekleyen tüccara onaylandı bilgisi dönerler. Atağın başarılı olma şansı, atak yapmaya karar veren madencilerin, *Bitcoin* sisteminin toplam özet oranının ne kadarına sahip oldukları ve tüccarın kaç onay beklediği ile ilgilidir. Örneğin atak yapmaya karar veren madenciler, tüm ağın özetleme oranının %10'unu ele geçirmişler ve onay bekleyen tüccar ödemeyi kabul etmek için 6 onay bekliyorsa, atağın başarılı olma şansı %0,1 (binde bir)dir.

≥ %50 Atağı ya da **Çoğunluk Atağı**: Eğer *Bitcoin* ağının, %50'sinden fazlası kötü niyetli madencilerin eline geçtiyse, atağın başarılı olma şansı %100'dür.

5.4 Çifte Harcamadan Korunma

Tüccarlar, ödemenin kesinleştiğine karar vermek için kendi belirledikleri sayıda onaylama beklerler. Bu sayı genellikle 3-6 arasında verilir. Bar, restoran ve ucuz elektronik ürün satanlar ise bazı durumlarda, hızlı işlem yapabilmek adına, sıfır onayla yetinebilmektedirler. Sıfır işlem onayı ile, hızlı çalışmak isteyen tüccarlar *BitKassa*, *Coinbase* ve *BitPay* gibi ***ödeme işlemcileri*** (payment processor) kullanarak kendilerini çifte ödeme ataklarına karşı koruyabilirler. Ödeme işlemcileri, çift ödemeye karşı işlemleri sigortalatma olarak görülebilir.

Bitcoin sistemi, dijital imzanın kullanılması nedeniyle kendi içerisinde oldukça güvenilir bir sistemdir. Tek risk, aynı *Bitcoin*'in iki defa kullanılma, yani çifte harcama (double spending) olasılığıdır. *Bitcoin, Blok-Zincir* veritabanına eklenecek olan yeni bloktaki tüm işlemlerdeki girdilerin, daha önce kullanılmamış olmalarını şart koşarak, onaylanmış kayıtlarda çifte harcamayı engeller [36].

6. BLOK-ZİNCİR (BLOCKCHAIN)

6.1 Blok-Zincir Nedir ?

Herkese açık, şeffaf, dağıtık, sıralı ve zaman damgalı *Bitcoin* transfer işlemlerini içeren dijital küresel hesap defteridir, düz bir veri dosyası, basit bir veritabanıdır. *Bitcoin*'in ilk ortaya çıktığı 2009'dan bu yana yapılan tüm işlemlerin dijital olarak saklanmasıdır. Hali hazırda yapılan işlemler *Blok-Zincir*'e işlenmektedir, ileride yapılacak olan işlemler de, *Blok-Zincir*'e işlenecektir. *Bitcoin*'le beraber ortaya çıkan, farklı kullanım alanları da olan *Blok-Zincir* metotu, merkezi olmayan bir ağ yapısındaki uç bilgisayarlarda, birbirinden bağımsız olarak saklandığından, herhangi bir merkezi hatadan kaynaklanacak problemlere karşı dirençlidir.

6.2 Blok-Zinciri Kim Tutar ?

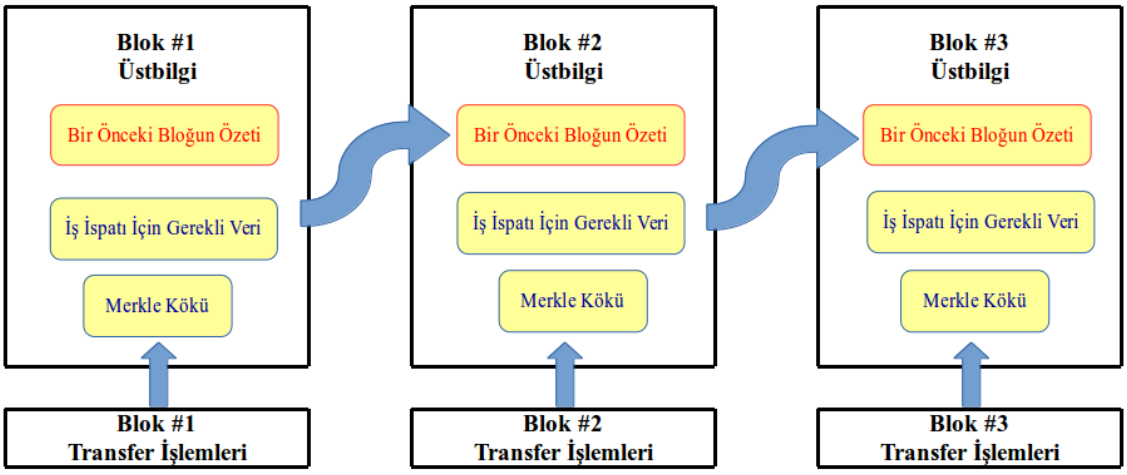
01 Aralık 2016 tarihi itibarı ile küresel hesap defterinin büyüklüğü 92 Gigabyte'dır. Dileyen herkes, merkezi olmayan *Bitcoin* ağına bağlanarak, bu verileri kendi bilgisayarına indirelebilir, kontrol edebilir, isterse küresel defterin bir kopyasını kendi bilgisayarında tutmaya başlayarak *Bitcoin* sistemine destek verebilir. *Blok-Zincir*'i kendi bilgisayarında tutan uçlara ***tam uç*** (full node) adı verilir. *Bitcoin* ağına bağlı tüm uçlarda (bilgisayar) *Blok-Zincir* erişilebilir durumdadır, ancak sadece tam uçlar 92 Gigabyte verinin tamamını tutarlar [36]. Tam uç olmanın şimdilik teşvik edici bir ödülü veya getirisi yoktur.

https://blockchain.info/, https://blockexplorer.com/, https://insight.bitpay.com/ veya http://blockr.io/ gibi adreslerden, *Bitcoin Blok-Zincir*'lerini anlık ve tarihsel olarak incelemek mümkündür. Gerçekte, bu siteler de *Bitcoin* ağına bağlı tam uçlardır.

Bitcoin ağına bağlı tam uçlar, sadece kendi doğruladıkları blokları saklarlar. Blok içerisindeki tüm işlemler geçerlidir, bloğu hazırlayan madenci iş ispatı yapmıştır, her bir tam uç ***iş ispatlarını*** da kontrol eder, tam uçlar doğrulayamadığı hiç bir bloğu saklamazlar. Eğer bir blok tüm uçlarda aynıysa, o blok üzerinde oy birliği veya mutabakat olduğu anlamına gelir. Nadir ve kısa süreli geçici durumlarda, son eklenen bloklar bazı uçlarda farklılık gösterebilir, bu sorun kısa sürede sistem tarafından otomatik olarak çözülür.

Her blok, kendinden bir önceki bloğun özetini içerir, bu sayede bloklar birbirine bağlanmış ve zincir oluşturmuş olurlar. Mevcut bloğun özet değeri bulunurken, bir önceki bloğun özeti değeri de işleme katılır. Herhangi bir bloğu değiştirmek isteyen kötü niyetli bir ucun, ileriye doğru tüm blokları değiştirmesi gerekecektir. Fakat her bir blok oluşturulurken ***iş ispatı*** istendiğinden, blokları değiştirmeye kalkan bir ucun ileriye doğru tüm bloklar için de ***iş ispatı*** yapması gerekecektir. Bu, devasa işlem gücü gerektireceğinden dolayı mümkün değildir. Bu özellik, *Blok-Zincir*'in ve tabii ki *Bitcoin*'in en güçlü yanlarından biridir. Bir blok ne kadar eskiyse, o kadar güvenilir ve değiştirilmesi imkansıza yakındır [34,36].

6.3 Blok-Zincir Veri Yapısı



Şekil 6.1: Sadeleştirilmiş *Blok-Zincir* Veri Yapısı

Şekil 6.1'de basitleştirilmiş bir blok zincir görülmektedir. Bir blokta en az bir işlem olmalıdır. Bir blok, 1 Mega Byte olarak tasarlanmıştır. Blok üst-bilgisi, bloğa ilişkin detay olmayan bilgileri içerir, 80 byte'lık yer kaplar. Detaylar *Bitcoin* transfer işlemleridir, bir işlem en az 250 byte'dır. Ortalama olarak bir blokta 350-500 adet işlem yer alır [34,65].

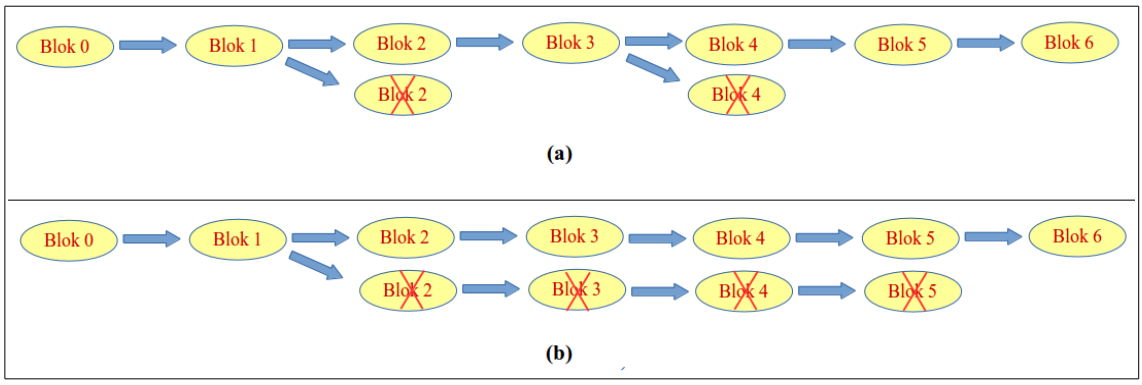
Bir blok içerisindeki tüm işlemler ikişerli gruplar halinde özetlenir, ortaya çıkan özetler yine kendi aralarında ikişerli gruplar halinde özetlenir. Bu işlem tek bir özet elde edene kadar

devam ettirilir. İşlemlerin ikişerli özetlenmelerinden oluşan ağaç yapısına ***Merkle Ağacı***, sonuçta ulaşılan tek özete ise ***Merkle Kökü*** denir. Bir bloğa ait herhangi bir işlemde değişiklik yaptığınızda, hem Merkle kökü değişecek hem de bloğun özeti değişmiş olacağından, o bloktan sonraki tüm bloklar doğrulanamaz hale gelecektir. Bu yapı hiç bir işlemin geriye doğru değiştirilememesini sağlar [66].

Bitcoin sisteminin ilk bloğunun adı "***genesis block***" olarak isimlendirilmiştir ve 4 Ocak 2009'da üretilmiştir. 50 *Bitcoin*'in, Satoshi Nakamoto'ya ait *Bitcoin* adresine aktarılmasıyla başlatılan ilk bloktur. Tüm blokların atasıdır, herhangi bloktan geriye doğru bakmaya başlanırsa, en sonunda Genesis bloğuna ulaşılır [34,36].

6.4. Yetim Bloklar

Normalde bir bloğun devam eden sadece bir bloğu olabilir. Bazı durumlarda, aynı anda birden fazla madenci iş ispatını yapar ve bulduğu bloğu anons ederek *Blok-Zincir*'e işletir. Madencilerin iş ispatını yaptıkları blokların içerikleri aynı olmayabilir. *Bitcoin* ağındaki diğer uçlar, ilk aldıkları yeni bloğu doğru kabul ederler. Her bir tam uç farklı bir bloğu doğru kabul edeceğinden, *Şekil 6.2*'de görüldüğü üzere bir çatallaşma olur [67]. Fakat uzun vadede, uçlar arasındaki protokol gereği, otomatik olarak çatalın en uzun ucu doğru kabul edilir, çatalın diğer ucundaki bloklar, bayatlamış veya yetim kalmış bloklar olarak adlandırılır. Uzun vadede, her bloğun bir çocuk bloğu, her çocuk bloğun bir ebeveyn bloğu olur. Bu konuya "7.4 Aynı Anda Birden Fazla Blok Üretilmesi Durumu"' başlıklı bölümde de değinilmiştir.



Şekil 6.2: Blok-Zincir'deki çatallaşma örnekleri (a) nadiren (b) çok nadiren görülen durumlar

Bitcoin sisteminde, iş ispatını yapan ve bulduğu bloğu *Blok-Zincir*'e ekleten madenciye ödül verilir. Blok içerisindeki ilk işlem, madenciye verilen ödüldür. Ancak, ödülü kazanan madenci, en az 100 blok (yaklaşık $10\,\text{dakika} \times 100 \approx 17\,\text{saat}$) kazandığı *Bitcoin*'i harcayamaz. Çünkü madencinin ürettiği blok, eş zamanlı olarak başka bir madenci tarafından da üretilmiş olabilir ve bu bloğun öksüz blok olma ihtimali vardır. Sadece, bloğunu *Blok-Zincir'*e ekleten madenci ödülü alabilir.

6.5 Değerlendirme

İnternet altyapısı *Blok-Zincir*'e, elektronik posta hizmeti ise *Bitcoin*'e benzetilebilir. *Bitcoin*, *Blok-Zincir*'in bir uygulamasıdır. *Blok-Zincir*'le yapabilecek çok farklı uygulamalar olabilir. *Blok-Zincir* şimdilik sadece finansal alandaki kullanımı üzerinde çalışılsa da, finans dışındaki konularda da kullanımı aktif araştırma ve geliştirme alanıdır. Güçlü merkezi bir otoriteye alternatif olan *Blok-Zincir,* merkezi otorite olmaksızın, göreceli olarak daha güçsüz bireyselliklerin birleşmesinden ortaya çıkan güvenilir, sağlam, şeffaf ve hesap verebilir bir sistemdir.

Bitcoin ağındaki her bir ucu karıncaya benzetirsek, hiç bir karınca tek başına koloniyi temsil edemez, tek bir karıncaya zarar vermekle, koloniye neredeyse hiç bir zarar verilemez. *Blok-Zincir* karıncaların uyguladığı basit kurallardan ortaya çıkan dev bir koloni aklıdır.

Blok-Zincir'in gelecekte kullanım alanlarının çok yaygınlaşacağı düşünülmektedir. Bu konuya “11.6 Bitcoin ve Blok-Zincir'in Geleceği” bölümünde değinilmiştir.

7. BITCOIN MADENCİLİĞİ

7.1 Bitcoin Madenciliği Nedir ?

Bitcoin madenciliği, sisteme yeni *Bitcoin* arz etmenin, hileli işlemleri engellemenin, olmayan *Bitcoin*'leri harcatmamanın ve çifte harcamayı engellemenin yoludur. Henüz onaylanmış *Bitcoin* transfer işlemlerinin, *Blok-Zincir'*e yani küresel hesap defterine işlenmesini *Bitcoin* madencileri yaparlar. *Blok-Zincir*'de bir bloğa yazılmış olan bir işlem onaylanmış demektir ve artık transfere konu olan alıcı tarafından kendisine gönderilen *Bitcoin* kullanılabilir durumdadır. *Blok-Zincir*'e bloğunu ekletecek olan madenci, yeni blokla arz edilen parayı ve *Bitcoin* işlemlerindeki işlem masrafını alarak ödüllendirilir.

7.2 Madenciler Nasıl Çalışırlar ?

Henüz onaylanmamış *Bitcoin* transfer işlemleri, geçici olarak *onaylanmamış işlemler* havuzunda tutulurlar, madencilerin havuzları ağdaki gecikmeler sebebiyle aynı olmak zorunda da değildir. Bu havuzdaki işlemlerden bir blok/öbek oluşturarak, küresel deftere bunu işlemek gerçekte çok basit ve hızlı yapılabilecek bir çalışmadır. Tüm madenciler hızlı bir şekilde blok oluştururlarsa, her madenci kendi bloğunu, *Blok-Zincir'*e ekletmek isteyecek ve bu durumda ağ karmaşası olacaktır. Bunun önüne geçmek için, blok oluşturmak isteyen madencilerden, birbirleriyle yarışarak çalışmaları ve bunu ispatlamaları istenir. Bu, ***iş ispatı*** metotuyla yapılır. Blok oluşturan madencilerden sadece bir tanesinin bloğu geçerli olur, blokların ortalamada 10'ar dakikalık aralıklarla üretilmesi, iş ispatının, zorluk hedefi otomatik olarak değiştirilerek sağlanır. Her bir bloğun üretimi için, madencilerin ortalama 10 dakikalık, işlemci gücü harcadıklarını sistem garanti eder*.

Bir madenci, iş ispatını yaptıktan sonra, bunu ağ üzerinde yayar, bunu alan diğer uçlar bloğu pek çok kontrolden geçirir, madencinin dürüst olduğu kanıtlanırsa, *Blok-Zincir'*e bulunan son blok eklenir.

İş ispatını yaparak bulduğu bloğu küresel hesap defterine işleten madenciye, sisteme

* İş İspatı kavramı "3.4 İş İspatı (Proof of Work)" bölümünde anlatılmıştır.

yeni arz edilen ***bitcoin*** hediye edilir. Başlarda bu hediye 50 BTC iken, her 210.000 blok üretiminde (yaklaşık 4 yılda bir) yarısına düşürülmektedir. Günümüzde başarılı madenciye, ***12,5 Bitcoin*** hediye edilmektedir. Sistemin tek para arz noktası da burasıdır.

7.3 Madenci Sayısı Artarsa veya Azalırsa

İş ispatı, kaba kuvvet yöntemiyle (tüm ihtimallerin denenmesi) yapılır. Özetleme kapasitesi yüksek olan madencinin, iş ispatını diğerlerinden daha önce yapma ihtimali yüksektir.

Madenciler, çözüm uzayını rastgele tararlar, bu sebeple, madenci sayısı arttıkça, madencilerden rastgele bir tanesi, iş ispatını daha çabuk yapar hale gelecektir. Aynı şekilde, madenci sayısı azalırsa, iş ispatını yapmak daha uzun zaman almaya başlayacaktır.

Bitcoin sisteminin hedefi, her 10 dakikada yeni bir blok üretilmesini sağlamaktır. 10 dakikadan daha kısa sürede blok üretilmeye başlandıysa, bu iş ispatı problemini çözmek için uğraşanların toplam özetleme kapasitesi arttı anlamına gelir ve problemin zorluğu *Bitcoin* sistemi tarafından otomatik olarak artırılır. 10 dakikadan daha uzun sürede, yeni blok üretimi olmaya başladıysa, bu sistemin toplam özetleme kapasitesi azaldı anlamına gelir (bazı madenciler madenciliği bırakmış olabilir) ve zorluk seviyesi otomatik olarak düşürülür. Her 2.016 blok ürettikten sonra, *iş ispatının zorluğu* tekrar hesaplanır. Detay için "3.4 İş İspatı (Proof of Work)" bölümüne bakılabilir.

Eğer son 2.016 bloğun üretilmesi, 1.209.600 saniyeden daha kısa sürdüyse, iş ispatının zorluğu %300 oranında artırılır (*zorluk hedefi* rakamının değeri düşürülür) daha uzun sürdüyse, iş ispatının zorluğu %75 oranında azaltılır (*zorluk hedefi* rakamının değeri artırılır).

7.4 Aynı Anda Birden Fazla Blok Üretilmesi Durumu

Blok-Zincir merkezi olmayan bir yapıda tutulduğundan, herhangi bir anda bakıldığında, "6.4. Yetim Bloklar" başlıklı bölümde de değinildiği üzere, *Blok-Zincir*'in farklı uçlarda (bilgisayarlarda) saklanan farklı kopyaları birbiriyle aynı olmayabilirler. *Bitcoin* ağının kuralsız ve dağıtık olmasından dolayı, farklı bloklar farklı tam uçlara farklı zamanlarda gelmiş olabilir. Fakat her uç, en çok iş ispatı olan zinciri, başka bir deyişle, genellikle en uzun olan zincir

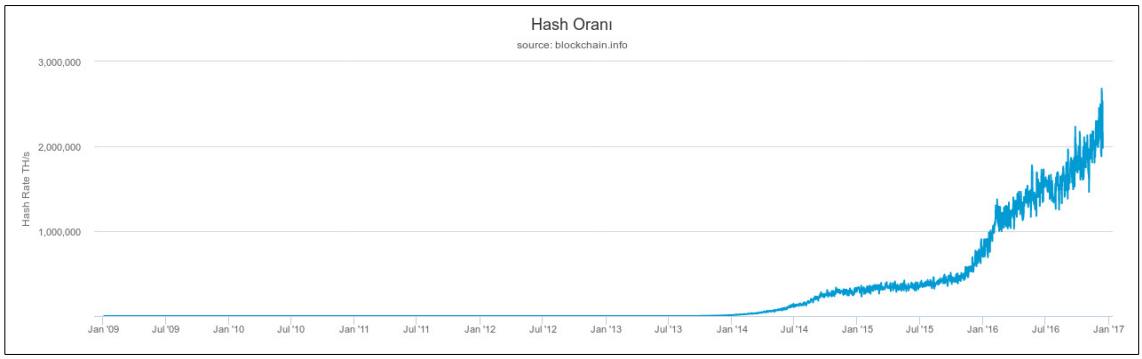
serisini doğru kabul eder, bu şekilde *Blok-Zincir*'ler eninde sonunda birbirleriyle uyumlu hale gelirler. Uyumsuz olma ihtimali olan bloklar son eklenen birkaç bloktur, yeni bloklar eklendikçe uyumsuz olan bloklar da tüm sistemle otomatik olarak uyumlu hale gelirler.

7.5 Para Arzı

Bitcoin'de para arzı, her 210.000 blokta yarıya indirilir. Para arzı azalarak devam ettiği için madenciliğe benzetilmiştir. 2016 yılında başarılı madenciye verilen ödül 12,5 BTC 'dir. Para arzı 2140 ylında bittiğinde tüm madenciler gelirlerini işlem masraflarından alacaklardır [68]. Madencilik merkezi olmayan takas sistemine benzetilebilir. Madencilik yapılmazsa sadece *Bitcoin* arzı durmaz, yapılan transfer işlemleri de onaylanmamış olurlar.

7.6 Kimler Madenci Olabilir ?

Dileyen herkes madenci olabilir. *Bitcoin* madenciliği aşırı yarış halinde ilerleyen bir sektördür. *Şekil 7.1*'de görüleceği üzere, *Bitcoin*'in ortaya çıktığı tarihten bu yana toplam özetleme gücü üssel olarak artmaktadır. 1 Aralık 2016 itibarıyla, *Bitcoin* madencilerinin toplam özetleme kapasitesi saniyede 2 Milyon Tera $\approx 2 * 10^{18}$ dir.



Şekil 7.1: Bitcoin ağının özetleme kapasitesi*

İlk başlarda, kişisel bilgisayarların merkezi işlem birimi (CPU), madencilik yapmak için

* https://blockchain.info/tr/charts/hash-rate#

yeterli iken, artan zorluk derecesi sebebiyle, kısa zamanda CPU kullanımı yetersiz gelmeye başlamıştır. Bunun üzerine bilgisayarların matematik işlemlerinde daha hızlı olan grafik kartlarının (GPU) kullanılması gündeme gelmiştir. Ancak GPU'ların elektrik sarfiyatının CPU'lardan fazla olması, *Bitcoin* madenciliğinin masraflı olmaya başlamasının ilk göstergelerinden olmuştur [69].

Günümüzde ise uygulamaya özel tasarlanmış entegre devreler (ASIC, Application-Specific Integrated Circuit) madencilik için kullanılmaktadır. ASIC makinelerinin elektrik sarfiyatı yüksektir, çok ısınırlar, gürültülüdürler [70]. *Şekil 7.2*'de 11.85 Tera/s (saniyede 11,850,000,000,000 defa SHA-256 özetleme algoritmasını çalıştırabiliyor) özetleme hızına sahip bir ASIC donanımı görülmektedir.

Şekil 7.2: Saniyede 11.85 Tera özetleme yapabilen ASIC Madencisi

Intel tabanlı bir ev bilgisayarının özetleme kapasitesi, ortalama 10-30 M/s olup bu kapasite, bir ASIC donanımının yaklaşık olarak milyonda biridir [71]. Bu sebeple, evlerdeki PC'lerden madencilik yapmak ekonomik değildir, madencilik için özel tasarlanmış ASIC donanımlarından satın almak gerekmektedir. Bu donanımlar için gereken elektrik ve ilk yatırım maliyetleri göz önünde bulundurularak, madenci olup-olmamaya karar verilir. Çin'de elektriğin ucuz olması, pek çok madencinin Çin'de olmasına sebep olmaktadır.

http://www.bitcoinx.com/profit/ veya http://www.coinwarz.com/calculators/bitcoin-mining-calculator gibi internet adreslerinden, elektrik fiyatı ve sahip olunan donanımın

özelliklerini (özetleme hızı ve elektrik sarfiyatı) girerek, madencilik yapmanın ekonomik olup olmadığını öğrenmek mümkündür. Elektrik maliyetleri, KW/Saat başına 0,15 Amerikan Dolarının üzerinde olduğu durumlarda, genel olarak madencilik yapmanın ekonomik olmadığı söylenebilir. Başka bir deyişle, 1 Aralık 2016 itibarıyla 12.5 BTC kazanmak için, $12{,}5\,x\,752 = 9{,}400$ Amerikan Dolarından daha fazla harcama yapılıyorsa, madenciliğin ekonomik olmadığına karar verilir.

Madencilik makinelerinin maliyeti ve elektrik sarfiyatının yüksekliği, bireysel olarak madencilik yapmanın ekonomik olmamasına sebebiyet vermektedir. Bu sebeple günümüzde, bireysel olarak madencilik, artık yerini ***madenci havuzlarına*** bırakmıştır. ASIC donanımlarına sahip olanlar dahi, doğrudan madencilik yapmak yerine, makinelerini bir madencilik havuzuna entegre etmektedirler. Özetleme güçlerini birleştiren madencilerin, 12.5 BTC'lik ödülü kazanma olasılıkları, bireysel olarak madencilik yapanların kazanma olasılığından yüksektir. Kazanılan ödül havuza yapılan işlem katkısı oranında madenciler arasında paylaşılmaktadır.

Bitcoin bulut madenciliği ise *Bitcoin* madenciliği yapan bir işletmeden, donanım ve işletiminin kiralanmasıdır, bir kısım yatırımcılar bunu da tercih edebilmektedirler. Sabit bir fiyattan, bir yıllığına veya ömür boyu sizin için madencilik yapacak bir firmayla anlaşmak, *Bitcoin*"nin gelecek yıllarda çok değerleneceğini düşünenler için bir seçenektir [78].

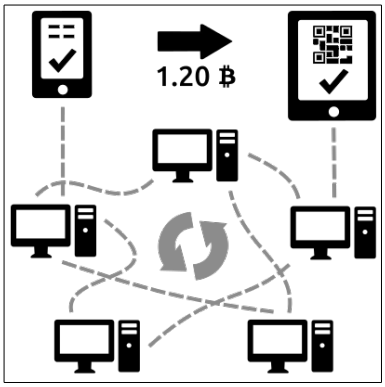
2140 yılı itibarıyla, *Bitcoin* arzı duracaktır. Başka bir deyişle, diğer madencilerle rekabet ederek, başarılı bir blok hazırlayan madenciye verilen ödül, 2140'dan itibaren yoktur. Madencileri o tarihten sonra teşvik edebilmek için, işlem masraflarının daha yoğun kullanılacağı düşünülmektedir [34,36,68].

8. BITCOIN AĞI

8.1 Genel Olarak Bitcoin Ağı

Bitcoin ağı internet ağını kullanır. *Bitcoin* ağına bağlı her bilgisayara uç adı verilir. Tüm uçlar eşittir, özel bir uç, sunucu, istemci yoktur, tüm uçlar gönüllülük esasına göre ağa dahil olurlar. İstedikleri anda ağdan ayrılabilirler. *Bitcoin* dışında en iyi bilinen uçtan uca ağ yapısı, dosya paylaşımı için kullanılan *Napster* ve *Bittorrent*'dir [34].

Şekil 8.1'de merkezi olmayan uçtan uca ağ bağlantısında, bir *Bitcoin* kullanıcısının diğerine *Bitcoin* transfer işlemi gösterilmektedir.



Şekil 8.1: Bir Bitcoin kullacısının, diğerine ağ üzerinden BTC göndermesi örneği

Bitcoin sisteminin kurallarını uygulayan, sistemin omurgası olan uçlara "***tam node***" (full node) adı verilir, diğer uçlar "***hafif uç***" (lightweight node) olarak adlandırılır. *Bitcoin* ağındaki uçların çoğu hafif uçtur.

Bitcoin ağında, tam uçlar *Bitcoin* P2P (uçtan uca) protokolü, madenciler ve cüzdan programları gibi hafif uçlar için ise Stratum gibi ek protokoller kullanılmaktadır.

8.2 Tam Uç (Full Node)

Tam uçlar, küresel hesap defterini, yani *Blok-Zincir*'i, tam ve eksiksiz olarak tutarlar. Genesis adı verilen ilk bloktan şu anki bloğa kadar tüm blokları, birbirlerinden bağımsız olarak kontrol eder ve saklarlar. Tam uçlar, bir *Bitcoin* transfer işlemlerindeki girdilerin daha önce kullanılmadığından emin olmak için, on binlerce bloğu kontrol ederler.

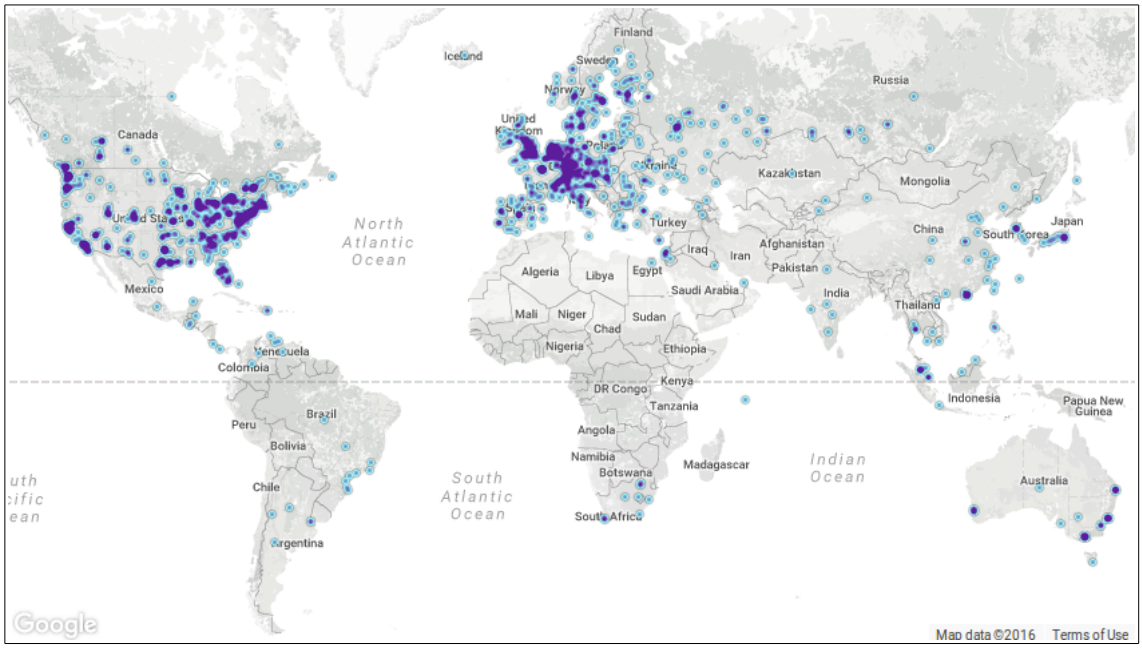
Tam uçlar, tüm blokları ve işlemleri aşağıdaki hususlar doğrultusunda kontrol ederler:

- Blokta belirli bir değerde Bitcoin arz edilmelidir.
- İşlemlerde harcanan paraların doğru bir şekilde imzalanması gerekir.
- İşlemler ve blokların formatı doğru olmalıdır .
- Hiç bir blokta, aynı Bitcoin birden fazla harcanmamalıdır.

Tam uç olmak isteyen bir uç, ilk bloktan başlayarak tüm blokları kendisine indirmesi gerekecektir. Tüm tam uçlar, aynı kontrolleri yaparlar ve birbirleriyle uyumlu kalırlar. Tam uçlar, tüm *Blok-Zincir'*i kendi sistemlerinde tutarlar. 1 Aralık 2016 itibarı ile bu bilgi yaklaşık 92 Gigabyte'dır. Bir tam ucun, madencilik yapması şart değildir.

Anlık olarak dünyadaki tüm tam uçları https://bitnodes.21.co/ adresinden görmek mümkündür. Aralık 2016 itibarıyla, sistemde yaklaşık olarak 5,500 adet tam uç bulunmaktadır.

Şekil 8.2'de, 19 Aralık 2106 itibarıyla, Bitcoin ağı üzerindeki tam uçların dünya üzerindeki dağılımı görülebilir.



Şekil 8.2: 19 Aralık 2016 itibarıyla Dünya üzerindeki Bitcoin ağındaki tam uçlar

8.3 Hafif Uç (Lightweight Node)

Hafif uçlar, tam uçların aksine *Blok-Zincir'*in tamamını indirip, güncel tutmak zorunda değildirler. Hafif uçlar, *Bitcoin* cüzdanları olarak da bilinirler. *Bitcoin* cüzdanları, tam uçlara istemci olarak bağlanır ve sadece kendi işlemleri ile ilgili verileri isterler. Hafif uçlar, daha az disk ve ağ kaynağı kullanırlar. *Blok-Zincir'*in sadece bir parçasının indirilmesine dayalı, *Sadeleştirilmiş Ödeme Doğrulama* (Simplified Payment Verification) sistemini kullanırlar. Sadeleştirilmiş Ödeme Doğrulaması, onaylanmış bir bloğun tamamının indirilmesine gerek kalmaksızın, sadece ilgili işlemlerin indirilerek doğrulanmasında kullanılan bir metottur.

9. ALTCOINLER

Bitcoin açık kaynak kodlu bir proje olduğundan, kendisinden sonra geliştirilen kripto-paralara temel olmuştur. *Bitcoin* teknolojileri kullanılarak geliştirilen kripto-paralara ***altcoin*** denir. Altcoinler para arzı, iş ispatı ve güçlü anonimlik gibi özellikleriyle birbirlerinden farklılaşmışlardır.

Bu raporun yazıldığı tarihte, 4.000'in üzerinde altcoin tanımlanmış durumdadır [36]. "http://build-a-co.in/" gibi otomatik altcoin projesi oluşturan siteler dahi hazırlanmıştır. Yakın geçmişe kadar, "60 saniyede kendi altcoin'ini oluştur" başlıklı internet sayfaları dahi hizmet vermişlerdir*[72].

Altcoinler, *Bitcoin*'in rakibidir, *Bitcoin*'le beraber ortaya atılan fikirlerin geliştirilmiş halleridir. Şimdilik, hiçbirisi *Bitcoin* kadar büyümüş ve kabul görmüş değildir. *Bitcoin*'in yaygınlığı artıp, fiyat hareketliliğindeki oynaklık azaldığında, altcoin'lerin spekülatif olarak kullanılması olasıdır [36].

Altcoin'lerin popüler olmaya başlamasının esas sebebi, *Bitcoin*'in arkasında bir devlet olmaksızın çalışmasıdır. Kripto para piyasasının toplam değeri (total market capitilization), 1 Aralık 2016 itibarıyla yaklaşık 14 Milyar Amerikan Dolarıdır. *Bitcoin* 12,5 Milyar dolar, Ethereum 724 Milyon dolar, Ripple 250 Milyon dolar, Litecoin 178 Milyon dolar ve Monero 107 Milyon dolarla, piyasa kapitalizasyonu en yüksek ilk 5 kripto paradır [73].

9.1 Para Birimi Olan Altcoinler

Bitcoin her 10 dakikada bir azalan bir fonksiyonla para arzı yapmaktadır. Buna karşın Litecoin 2.5 dakikada bir para arz eden, Dogecoin 60 saniyede bir para arz eden, Freicoin ise negatif faiz içeren, yani harcanmayan paranın zamanla azaldığı altcoin sistemleridir.

Bitcoin'de bir bloğun eklenebilmesi için bir madencinin çalıştığını ispatlaması ve bunu diğerlerinin kontrol edip, onaylaması gerekir. Bu iş ispatı SHA256 algoritması ile yapılır. İş

* http://coingen.bluematt.me

ispatı yönetimine alternatif olarak "***scrypt***" algoritması geliştirilmiştir. Scrypt, SHA256 kadar işlemci gücü harcamaz. Böyle olunca, devasa hızlara ulaşan ASIC makinelerine ihtiyaç kalmaz, ve sistemin merkezileşmesi engellenmiş olur. Ayrıca, iş ispatı (proof of work) metotu yerine ise alternatif olarak, pay ispatı (proof of stake) metotu geliştirilmiştir. *Peercoin*, *Myria*, *Blackcoin*, *VeriCoin* ve *NXT* bu metotları kullanan para birimlerine, örnek olarak verilebilir.

Bitcoin'de kullanılan iş ispatı metotunun tek amacı *Bitcoin* ağının güvenliğidir. Yeni geliştirilen bazı altcoinlerde madenciliğin farklı bir amaca da hizmet etmesi sağlanmaktadır. Örneğin; iş ispatı, *Primecoin*'de asal sayıları bulmakta, *Curecoin*'de yeni ilaç keşfi için kullanılan, protein katlanması (protein folding) araştırmalarını yapmakta, *Gridcoin*'de ise Berkeley Üniversitesi'nce geliştirilen açık dağıtık işlemeye (grid computing, BOINC) fayda sağlamaktadır.

CryptoNote, *Bytecoin*, *Monero*, *Zerocash/Zerocoin* ve *Darkcoin* gibi altcoinlerde ise kullanıcılarının anonimliği artırılmaktadır.

9.2 Para Birimi Olmayan Alt-Zincirler

Para birimi olmadığı halde *Blok-Zincir* yapısından etkilenerek kurulmuş sistemlere *Alt-Zincir* denir. Bir kısmı para veya jeton (token) kullanır. Para veya jeton arzı ve kullanımı olsa da esas amacı bunların kullanımı değildir. Örneğin, *Namecoin* alternatif alan adı (domain name) kayıt işlemleri için kullanılır.

Benzer şekilde, *Bitmessage* ise merkezi olmayan güvenilir mesajlama servisi sunar, kullanıcılar birbirlerinin *Bitmessage* adreslerine mesaj gönderirler, mesajlar kalıcı değildir, 2 gün içerisinde silinir.

Ethereum ise *Bitcoin*'de tanıtılıp duyurulan *Blok-Zincir'*in yeniden tasarlanmış halidir, kendi para birimi *Ether*'dir. Kontrat olarak tanımlanan veri saklama, *ether* ödemesi gönderme ve alma işlemlerini, *ether* saklanmasını ve bilgi işlemeyi merkezi olmayan otonom yazılımcısı olarak gerçekleştirir [34].

10. BITCOIN'İN YASAL STATÜSÜ

Pek çok ulusal merkez bankası veya bankacılık düzenleme kurumu *Bitcoin* kullanımını yasaklamamış, ancak finansal kurumları ve bireyleri karşılaşabilecekleri riskler konusunda uyarmıştır. *Bitcoin*'in merkezi bir otorite tarafından denetlenmemesi, oldukça yeni bir kavram ve teknoloji olması, her bir *Bitcoin* kullanıcısının *Bitcoin*'in geleceğini belirlemesi gibi hususlar, hükümetleri, düzenleyici ve denetleyici kurumları haklı olarak endişelendirmektedir.

Bitcoin bir tür gelir veya ücrettir. *Bitcoin* geliri, vergiye tabi tutulursa, hükümetlerin *Bitcoin*'e karşı olmaları da beklenmez. Brezilya, Kanada, Finlandiya, Bulgaristan ve Danimarka, *Bitcoin* kullanımının vergilendirilmesi konusunda düzenlemeler yapmışlardır. Singapur, *Bitcoin*'i bir varlık veya ürün olarak görüp vergilendirir, *Bitcoin* ile yapılan yerel alışverişlerden katma değer vergisi dahi almaktadır.

Ülkeler bazında Bitcoin'in yasal statüsünü detaylı araştırmak için, Amerikan Kongre Kütüphanesi'nin, Kanun Kütüphanesi bölümünde hazırlanmış, 40 ülkeyi kapsayan Ocak 2014 tarihli raporuna bakılabilir [74].

Genel olarak ülkeler, *Bitcoin*'e karşı olumlu bir endişelilik içerisindelerdir. Henüz bebeklik evresini yaşayan *Bitcoin* hakkında, ileride global bazda hükümetler arası bir düzenlemeye gidilmesi de değerlendirilebilecektir.

10.1 Bitcoin Dostu 10 Ülke

Estonya hükümeti *Blok-Zincir* teknolojisini sağlık, bankacılık ve hatta vatandaşlarının yönetime katılmalarını sağlamak için kullanmayı planlamaktadır. Vatandaşlarına *Blok-Zincir* tabanlı ilk ***elektronik-oylama*** sistemini getirmiştir.

Sayıca en çok kripto paraya ev sahipliği yapan ve dünya *Bitcoin* ticaret hacminin lideri **Amerika Birleşik Devletleri**'dir. Pek çok ülke, kripto paraların yasal düzenlenmesi ve regüle edilmesi konusunda Amerika'nın alacağı tavrı ve yaklaşımlarının sonuçlarını beklemektedir.

Danimarka, nakit kullanımını kaldırmak ve dijital para birimine geçmek isteyen ülkelerdendir. Kendi merkez bankasından da tamamen vazgeçmeden, *Bitcoin* ve itibari dijital parasını beraberce günlük yaşamda kullanmayı planlamaktadır. Danimarka Merkez Bankası, *Bitcoin*'in bir para olmadığını, bu sebeple regüle etmeyeceklerini açıklamıştır. Ülkede pek çok *Bitcoin* yenilikçi şirket kurulmaktadır.

İsveç de Danimarka gibi, nakit kullanımını kaldırmak isteyen ülkelerdendir. İsveç merkez bankası Riksbank'ın negatif faiz uygulamasından etkilenmemek için, İsveç vatandaşları *Bitcoin*'i kullanabilmektedirler, bu sayede servetlerini koruyabileceklerdir. İsveç Finansal Denetleyici Otoritesi, *Bitcoin*'i ödeme metotu olarak yasallaştırmıştır.

Samsung ve LG gibi dev teknoloji firmalarına ev sahipliği yapan **Güney Kore**'de, *Bitcoin*'i düzenleyen bir yasa olmamasına rağmen, *Bitcoin* bir ödeme metotu olarak kabul görmüştür ve her geçen gün yaygınlığı artmaktadır. Güney Kore, *Bitcoin* konferanslarına da ev sahipliği yapmaktadır.

Hollanda Arnhem, adeta bir *Bitcoin* şehridir. Şehirde 100'den fazla, *Bitcoin*'le alışveriş yapılabilen mekanlar vardır. Hollanda bankaları, *Blok-Zincir* metotuyla kendi teknolojilerini geliştirip, masrafları azaltmak için kullanmanın yollarını araştırmaktadırlar.

Finlandiya Merkezi Vergi Kurulu, *Bitcoin*'i bir finansal servis olarak tanımlamış, *Bitcoin*'i ve teminini katma değer vergisinden muaf tutmuştur.

Kanada da pek çok *Bitcoin* yenilikçi şirkete ev sahipliği yapar. Uzun tartışmalar sonunda *Bitcoin*, kara para aklama ve terörün finansmanı mücadelesi yasası kapsamında düzenlenmiştir.

Birleşik Krallık pek çok *Bitcoin* ve *Blok-Zincir* yenilikçi şirketlerine ev sahipliği yapar. *Bitcoin*'e özel para muamelesi yapılır, *Bitcoin*'le yapılan alışverişlere katma değer vergisi uygulanır.

Avustralya *Bitcoin*'e uyguladığı çifte vergilendirmeyi kaldırmıştır, ancak *Bitcoin* için özel bir düzenleme yapılmamıştır. Avustralya, *Bitcoin*'i emtia olarak değerlendirmektedir.

Avustralya Borsası *Blok-Zincir* teknolojisini test etmektedir. Avustralya Postası, servislerini iyileştirmek amacıyla, dijital kimlikleri *Blok-Zincir* metotuyla yapmayı hedeflemektedir.

10.2 Bitcoin Düşmanı 5 Ülke

İzlanda Merkez Bankası, Mart 2014'te *Bitcoin* satın almanın İzlanda Kambiyo Yasasına aykırı olduğunu açıklamıştır.

Bangladeş, *Bitcoin*'i yasal bir para olmadığı ve kullanıcılarını finansal tehlikelere atabileceği için yasaklamıştır.

Bolivya Merkez Bankası, "bir hükümet veya yetkili birimler tarafından çıkartılmayan ve kontrol edilmeyen paraları kullanmak yasal değildir" gerekçesiyle *Bitcoin*'i yasaklamıştır.

Ekvador, kendi elektronik parasını çıkartmak için çalıştığından, rekabeti önlemek için *Bitcoin*'i yasaklamıştır.

Tayland Merkez Bankası, Temmuz 2013'te *Bitcoin* için bir yasa olmadığından dolayı, kullanımının yasal olmadığını duyurmuştur.

10.3 Türkiye'de Bitcoin'in Yasal Statüsü

25 Kasım 2013'te Bankacılık Düzenleme ve Denetleme Kurumu, *Şekil 10.1*'de görüldüğü gibi, *Bitcoin*'le ilgili bir açıklama yapmıştır. Açıklamada, dijital para *Bitcoin*'in, 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" kapsamında olmadığını ve elektronik para olarak değerlendirilmediği için gözetim ve denetiminin mümkün olmadığını belirtilmiştir. Ayrıca, *Bitcoin* sisteminde kimliklerin bilinmemesi sebebiyle, *Bitcoin*'in yasadışı faaliyetlerde kullanılabileceği, değerinin aşırı oynak olması, dijital cüzdanların çalınabilmesi, kaybolabilmesi, usulsüz kullanılabilmesi ve işlemlerin geri döndürülemez olmasının risklere açık olduğu da vurgulanmıştır.

Bitcoin'in vergilendirilmesi tartışması, tüm dünyada olduğu gibi, Türkiye'de de devam

etmektedir. Merkezi olmaması sebebiyle sadece Türkiye'yi kapsayacak bir vergilendirme sisteminin mümkün olamayacağını düşünenler olduğu gibi, *Bitcoin*'in yasal statüsünü belirledikten sonra vergilendirmenin değerlendirilebileceğini düşünenler de vardır [75].

BDDK
BANKACILIK DÜZENLEME VE DENETLEME KURUMU

BASIN AÇIKLAMASI

Sayı : 2013 / 32 **25 Kasım 2013**

BASIN AÇIKLAMASI

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

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

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

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

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

Kamuoyuna saygıyla duyurulur.

Şekil 10.1: BDDK'nın Bitcoin'le ilgili basın açıklaması

11. DEĞERLENDİRMELER VE SONUÇ

11.1 Bitcoin Güvenlidir

Bitcoin güvenlidir, çünkü [36];

1. Merkezi değildir, merkezi bir arıza noktası yoktur, bireysel olarak kullanıcılar heklense de (hacked), sistemin bütünü bundan etkilenmez.

2. Kriptografik olarak blokların ve blok içi işlemlerin bütünlüğü ve kronolojisi korunmaktadır.

3. Bireysel olarak her *Bitcoin* cüzdanı gizli anahtar ile korunmaktadır. Gizli anahtar olmadan, cüzdanlar üzerinden işlem yapmak mümkün değildir.

4. *Bitcoin* arzı, dağıtık olarak çalışan madencilerin konsensüsü ile sağlanır. Bunun haricinde, hiç bir otorite ek *Bitcoin* arz edemez.

Bitcoin'i hacklemek, interneti hacklemekle aynıdır. İnterneti aynı anda, tüm dünyada hacklemek imkansıza yakındır, ülkeler internet çıkışını kapatsalar veya *Bitcoin*'in kullanımını yasaklasalar dahi, bu sistemin çalışmasına engel değildir.

Henüz kuantum bilgisayar icat edilmedilerse de, ileride kuantum bilgi işlemenin *Bitcoin*'i tehdit edeceği iddiası doğrudur, ancak bu sadece *Bitcoin*'e yönelik değil tüm kriptografik uygulamalara yönelik bir tehdit olabilecektir. Eğer, kuantum bilgisayarlar icat edilirlerse, şifreleme metotları ileri kuantum algoritmaları kullanılmak suretiyle yapılabilecek ve sistemin güvenilirliği yine korunabilecektir [48]. Bu konuya "3.2.1 Dijital İmzanın Güvenilirliği" bölümünde de değinilmiştir.

Kötü niyetli kullanıcılar *Bitcoin* ağının mevcut işlemci gücünün %51'inden fazlasına sahip olurlarsa, sistemin hacklenmesi mümkün hale gelir, ancak bu durumu gerçekleştirmek, bireyler ve hatta devletler için imkansıza yakındır. ***%51 atağı*** başarılı olsa dahi, diğer

kullanıcıların işlem yapmaları engellenemez, fakat işlemlerin onay alması engellenebilir, yeni blok oluşumu durdurulabilir. Atağı yapanlar, yeni *Bitcoin* kazanamazlar, her blok için başarılı madenciye verilen *Bitcoin* miktarını değiştiremezler, sahip olmadıkları *Bitcoin*'lere erişemezler ve üzerinde işlem yapamazlar.

Madenci havuzlarından olan ***Ghash.io***, Ocak ve Haziran 2014'te *Bitcoin* ağının toplam işlemci gücünün %51'ine kötü niyetli olmadan yaklaştı, bu duruma çözüm bulmak için diğer havuzlarla birlikte, hiç bir havuzun %29,99 işlem gücünü geçmemesi, geçtiği takdirde ilgili havuzun önlemler alması gerektiği konusunda ortak kararlar aldılar.

11.2 Avusturya Ekonomi Ekolü'nün Bitcoin'e Bakışı

Avusturya ekonomi ekolünden Ludwig von Mises (d. 1881–ö. 1973), itibari kağıt para sisteminin sonsuza kadar sürdürülemeyeceği, bir gün sonunun geleceğini iddia eder [76]. Mises'e göre, altın apolitiktir, merkezi olarak kontrol edilemez, hükümet veya grupların baskılarından uzaktır. 1973 yılında ölen Mises, elbette dijital çağı ve 2009 yılında tanımlanan *Bitcoin*'i göremedi.

Avusturya Mises Enstitüsü'nden Frank Shostak'a göre [77];

> Para *Bitcoin*'den çok daha karmaşık bir emtiadır, her türlü ürün ve hizmetin ticareti para ile yapılabilir, paranın değeri aslında, ürün ve hizmetlerle değiştirilebilmesinden kaynaklanır. *Bitcoin* sadece ve sadece, itibari paraya çevrilebildiği sürece fonksiyoneldir. *Bitcoin* maddi bir varlık değil, sanal bir para birimidir, bu sebeple itibari para sisteminin yerini alması mümkün değildir. *Bitcoin* yeni bir para değildir, sadece mevcut para sistemimizde tanımlanan yeni bir işlem şeklidir. *Bitcoin* fiyatının aşırı yükselmesi, *Bitcoin* sisteminin sunduğu hizmetlere, insanların yüksek değer atfetmesinden başka bir şey değildir. Para çıkışına izin verilmeyen bir ülkede, insanların parasını korumak için yüksek ücretler ödemesi ile *Bitcoin* fiyatının yükselmesi birbirine benzerdir.

Allen Scott'a göre [78];

> Avusturya Ekolü eğer bilebilselerdi, *Bitcoin* taraftarı olurlardı. 1951'de Ludwig von Mises, itibarı paranın tehlikelerinden bahsederek, apolitik olan ve merkezi bir otorite tarafından kontrol edilmeyen altın standardına dönülmesi gerektiğini iddia etti. İlginçtir ki; *Bitcoin* de bu açılardan altına benzerdir. Merkezi bir otorite olmaksızın, kişiden kişiye aktarım sağlayan *Bitcoin*, merkezi bir otorite ve aracı kurum olmadığı için dijital paradan çok, fiziki paraya benzerdir. *Bitcoin*'in fiyatı *7/24* bitcoin borsalarında, gecikme olmaksızın, tamamen arz ve talebin buluşmasıyla belirlenmektedir. Eğer Mises bugün yaşasaydı *Bitcoin*'i tercih edebilirdi.

Yine *Bitcoin* taraftarlarından Jeffrey Tucker'a göre [79];

> *Bitcoin*, itibari paranın kritik olan dayanıklılık, bölünebilirlik ve değiştirilebilirlik özelliklerine sahiptir. Bu özellikleri sayesinde *Bitcoin*, güvene ve kimliklere dayanmayan, yeni dijitial çağın, yeni parasal sistemidir (monetary system). “Hiç bir şeyden ya da bir parça bilgisayar kodundan para çıkar mı?” sorusu insanları yanıltmaktadır. *Bitcoin* bir efsane değildir, bir gerçektir, günlük hayatta kullanımını, değişim fiyatlarını görebilirsiniz. Ludwin von Mises'in "Paranın fiyatı, elde edebildiği ürün ve hizmetlerle belirlenir." prensibine tam olarak uyar, hatta yaşasaydı teorisinin hala çalıştığını görür, gurur duyardı.

Altına 10 binlerce yıldır alışığız, oysa kripto-paralar oldukça yeni, ne olup biteceğini zamanla göreceğiz.

11.3 Bitcoin Balon mudur Veya Bir Tür Saadet Zinciri midir ?

Bitcoin kaldıraç etkisiyle işlem görmez, satın alınması tam finansmanla olur, bu sebeple ***balon*** değildir. *Bitcoin*'in sahibi yoktur, fiyatı tamamen piyasa koşullarında belirlenir, fiyatındaki oynaklık sebebiyle kar veya zarar edilmesi önceden tahmin edilemez. Bu sebeplerle, bir tür ***saadet zinciri*** de (Ponzi Scheme) değildir [35].

Bitcoin'in başlardaki yatırımcılarının çok kazandığı iddiası da tam olarak doğru değildir. Yatırımcıların bir kısmı, o dönemlerde fazla önemsemediklerinden gizli anahtarını kaybetmiş durumdadır, ilk başlarda fazla değerli olmadığından, büyük tutarlar transfere konu olmuştur. Uzun dönemde baktığımızda, bugün *Bitcoin* satın alanların, yarınların "sisteme erken girenleri" olup olmayacağı da bilinemez [35].

11.4 Bitcoin VISA Veya PayPal'ın Alternatifi Olabilir mi?

VISA saniyede ortalama 2.000 işlemle başa çıkabilir durumdadır. IBM yaptığı bir testte, VISA'nın saniyede 56.000 işleme kadar başarılı bir şekilde çalıştığı gösterilmiştir [80]. PayPal ise, 2015 yılında toplam 4,9 Milyar işlemle, saniyede ortalama 155 işlemle başa çıkabilmiştir [81].

Bitcoin ise saniyede maksimum 7 işlem yapacak şekilde kısıtlandırılmıştır. 2016 itibarıyla *Bitcoin* sistemine saniyede ortalama 3 işlem girilmektedir. Fakat tüm *Bitcoin* kullanıcıları üzerinde hem fikir olurlarsa, *Bitcoin*'in saniyede 2.000 işlem yapması mümkün olabilecektir. Şöyle ki;

> *Bitcoin* ağına bağlı tam uç bilgisayarlarda, işlemciler en çok imza doğrulamada zaman kaybederler. "Quad core Intel Core i7-2670QM 2.2Ghz" işlemcili bir bilgisayar saniyede 8.000 imza doğrulama yapabilmektedir. Ayrıca, ortalama bir işlem 512 byte olduğundan, 2000tps * 512 * 8 = 7.8 MBit/s'lık bir ağ genişliği gerekecektir. Bu hız neredeyse evlerde bile sahip olunabilecek bir hız olup, sistem başarıyla çalışabilecektir.

Bitcoin yaygılaştığında, işlem sayısı artacaktır. Artan işlem sayısı ile birlikte, *Blok-Zincir* terabytelarca yer kaplayabilecek ve bu durumda da bireysel, gönüllü tam uçların sayısı azalacaktır. Sistem madencilere *Bitcoin* teşviği verdiği halde, tam uç olan bilgisayarlara önerdiği bir teşvik yoktur. Küresel hesap defterini tutan, tam uçların sayısının çok ve mümkün olduğu kadar küresel dağıtık olması hem güvenilirliği artırır, hem de sistemin her türlü kesintiye karşı dirençli olmasını sağlar. *Bitcoin* kullanıcıları, tam uçlara teşvik konusunda ortak bir karara varırlarsa, bu problem de aşılabilecektir.

11.5 Bitcoin'in Deflasyon Sorunu Var mıdır?

Bitcoin sisteminde, para arzının azalarak devam etmesi ve bir noktada talebi karşılayamayacağı için değerinin aşırı artma riskine *deflasyon riski* denir. Geleneksel mali sistemlerde, ücret deflasyonunda, paranın satın alma gücü zaman geçtikçe artar. Pek çok ekonomist deflasyonun ekonomik bir felaket olduğunu ve kaçınılması gerektiğini düşünür. Deflasyonda insanlar para harcamak yerine biriktirmeyi tercih eder ve fiyatların düşmesini beklerler. Japonya'nın "Kayıp 10 yılında" talebin yok olması, Japon Yeni'ni deflasyona sokmuştur [82].

Bitcoin uzmanları ise deflasyonun göründüğü kadar kötü olmadığını iddia ederler. Elimizdeki tek verinin, talebin daralmasından dolayı ortaya çıkan deflasyon olduğunu, *Bitcoin*'de talep daralması yaşanmayacağını, ancak para arzının bilinen şekilde azalmasından dolayı bir deflasyon olabileceğini, bunun Japonya'da olan deflasyondan çok farklı olduğunu söylerler [34,83].

Pratikte, tüketicideki biriktirme iç güdüsü, üreticide de vardır, fiyatları indiren üretici ve ihtiyacını karşılamak zorunda olan tüketicinin, denge bir fiyatta bulaşacağı düşünülmektedir. Yine de *Bitcoin*'deki deflasyon riski bir problem olabilecektir, bunu zaman gösterecektir. [34].

11.6 Bitcoin ve Blok-Zincir'in Geleceği

Bitcoin'in; para birimi, para transfer aracı ve dijital ödeme sistemi olarak kullanılması "***Bitcoin 1.0***" olarak tanımlanıyor. *Blok-Zincir* teknolojisi kullanılarak yakın gelecekte tahvil, bono veya kredi gibi tüm finansal ve iktisadi uygulamaların oluşturulması "***Bitcoin 2.0***" olarak nitelendiriliyor. "***Bitcoin 3.0***" ise, gelecekte *Blok-Zincir* altyapısı kullanılarak; sağlık, kültür, bilim ve sanat gibi tüm alanlarda, katma değer yaratan ve hayatı kolaylaştıran uygulamaların oluşturulması olarak tasvir ediliyor [84,85].

Bitcoin'in gelecekte geçerli bir para birimi olacağını kabul etmeyen pek çok finansal kurum dahi, kendi iç bünyelerindeki sistemlerini *Blok-Zincir* sistemiyle gerçekleştirmek için araştırmalara başlamışladır. *Bitcoin* ve *Blok-Zincir* Sürüm 2.0 ve 3.0 ile birlikte, uygulamalar çok daha çeşitlenecek, bloklarda sadece işlemler değil, dijital videolar, kopyalama hakları,

dijital sigorta gibi her türlü dijital veriler, şeffaf bir şekilde taraflar arasında gönderilebilecektir.

Şimdilik *Bitcoin* sisteminde, *Bitcoin*'ler alınabiliyor, harcanabiliyor ve saklanabiliyor. Fakat *Bitcoin* 2.0'da borç verilebilecek, faiz alınabilecek veya finansal ürünlerde çeşitli haklar satın alınabilecektir. Elektronik ticaret alanında da *Blok-Zincir* ve *Bitcoin* için büyük bir potansiyel vardır. Sanatçılar, ürünlerini bir aracı olmaksızın doğrudan sanatseverlerle paylaşabileceklerdir [34].

Mevcut durumda, kimlikleri ispat etmek için, pek çok hassas döküman aracı kurumlara veriliyor ve aracı kurumlar bu bilgileri merkezi bilgisayarlarında saklıyorlar. *Bitcoin*'in ilerleyen sürümlerinde, sanal kimlik kartlarının oluşturulabileceği ve hassas bilgilerin usülsüz kullanımlarının önüne geçilebileceği düşünülüyor [34].

Bitcoin teknolojilerinin, bir başka kullanım alanı da, bölgesel veya ülke genelinde demokratik seçimler, referandumlar yapılabileceği, temsili demokrasiyi, katılımcı demokrasi yapmak yolunda adımlar atılabileceğidir. Seçim veya oylama şeffaf olacak, ama katılanların kimlikleri anonim kalacaktır. İnsanların, evlerde, iş yerlerinde ya da cep telefonlarından oy kullanacağı günler hiç de uzak değildir. Ek olarak söylemek gerekir ki; güvenilir aracı ile yapılan tapu, noter, borsalar vs. gibi hemen her işlem *Blok-Zincir* teknolojisine adapte edilebilecektir.

Çin hükümeti, kendi kripto-para birimini çıkartmak için hazırlıklara başlamıştır [86]. Çin Siberuzay İdaresi, Ekim 2015'te dünyanın *Bitcoin* sonrası döneme girdiğini, bu devrimsel değişiklikleri kimsenin görmezden gelemeyeceğini ifade etmiştir [87].

11.7 Bitcoin'in Problemleri

İnsan doğası yeni ve değişim gerektiren hususlarda endişelidir. Alışkanlıklarımızı hemen ve tümden değiştirmeye direniriz. *Bitcoin*'e karşı bu anlamda, insanlarda bir direnç olduğunu da kabul etmek gerekir.

Gizli anahtarların kaybedilmesi durumunda hiçbir sahiplik kanıtının bulunmaması insanların alışmakta zorlandığı bir konudur. Ayrıca, anonim kullanılabilmesi sebebiyle yasa dışı

aktivitelerde çekici hale gelmesi, hem bireyleri hem kamu otoritelerini endişelendirmektedir. Örneğin; geçmişte *Silk Road* isimli sitenin illegal işlere karışması (çocuk pornosu ve uyuşturucu gibi), *Bitcoin* sistemine başlarda psikolojik olarak çok ciddi zararlar vermiştir.

Bitcoin'in sağladığı anonimliğin bedeli, bünyesinde barındırdığı güvenlik sorunlarıdır. Kimlik bilgilerinin gizliliği, bir otoritenin denetim ve düzenlemesine tabi olmayışı, sistemi her türlü yasa dışı finansal transfer işlemine açık hale getirmektedir. Hükümetler, *Bitcoin*'e karşı şimdilik olumsuz ve yasaklayıcı bir yaklaşım sergilemeseler de, bunun da bir garantisi yoktur.

Bitcoin'in yaygınlaşması fiyat oynaklığının azalmasını sağlar, fakat yaygınlaşması için de fiyat oynaklığının azalması gerekir. Bu bir yumurta-tavuk problemidir. Ancak, sistemin duyurulduğu günden bu yana yaygınlaşması umut vericidir.

Merkezi kontrol noktasının olmaması, transferlerde itiraz ve yapılan işlemlerin geri alınamaması sonucunu doğurur. Bu durum, çeşitle problemlere yol açabilecektir.

Her sistemin maliyeti vardır. *Bitcoin* sisteminin, en büyük maliyeti madencilikte harcanır. Aşırı elektrik sarfiyatı ve ilk kurulum masrafları olsa da, bu maliyet şeffaf bir şekilde hesaplanabilir. Mevcut durumda, *Bitcoin*'in toplam maliyeti, pek çok merkez bankasının toplam maliyetinden azdır.

11.8 Sonuç

Onbinlerce yıldır alışık olduğumuz altın ve yüzlerce yıldır kullandığımız nakit paralarla karşılaştırdığımızda sanal kripto-para olan *Bitcoin* oldukça yenidir. Getirdiği teknolojiler oldukça umut verici ve gelişmeye açık konulardır. *Bitcoin*'den sonra da pek çok altcoinler geliştirilmiştir, fakat en azından şimdilik, hemen hepsinin başarısı *Bitcoin*'e endekslidir.

Bitcoin; bankaların, aracı kurumların, otoritelerin ve hükümetlerin denetim ve düzenlemelerinden, her türlü işlem masraflarından ve kısıtlamalarından uzaktır. Kişilere finansal özgürlük sağlar. *Bitcoin*'in geleneksel ödeme aracı olan banknot veya dijital paraların yerini alması, günden güne artmaktadır. Sistem ne kadar yaygınlaşırsa, o kadar güvenli ve spekülasyonlara dayanıklı olacaktır.

Bitcoin'le beraber duyurulan *Blok-Zincir* teknolojisi ise, güvenilir bir aracıya ihtiyaç duyulan tüm hizmetlerde kullanılabilecek bir teknolojik çözümdür. *Blok-Zincir*, *Bitcoin*'in başarısına da endeksli değildir.

Bitcoin ve onun getirdiği teknolojilerin, kullanım alanı ve yaygınlığı gün geçtikçe artmaktadır, bunun karşısında ise hükümetler *Bitcoin*'e karşı olumlu bir endişelilik halindedirler.

Ülkemizin de, tüm dünya devletleriyle birlikte, *Bitcoin*'i olumlu bir endişelilikle izlemesinin uygun olacağı düşünülmektedir. Tüm riskleri değerlendirilerek, teşvik edici düzenlemeler yapılırsa, *Bitcoin* pazarından gelir elde etmemiz de mümkün olabilir. Örneğin; ülkemizde hizmet veren bir *Bitcoin* Borsası henüz kurulmamıştır, bunu düzenleyen bir mevzuat, ülkemizi Bitcoin pazarında bir adım öne çıkarabilecektir.

[1] Bankacılık terimleri, http://www.bankalar.org/bankacilik-terimleri/ *(Erişim 20.12.2016)*

[2] https://en.wikipedia.org/wiki/Commodity_money *(Erişim 20.12.2016)*

[3] Joel Achenbach, 17.Temmuz.2013,"Origin of gold is likely in rare neutron-star collisions", The Washington Post *(Erişim 20.12.2016)*

[4] Andrew Fazekas, 9.Eylül.2012, "Silver in Space: Metal Found to Form in Distinct Star Explosions", National Geographic News *(Erişim 20.12.2016)*

[5] Justin Rowlatt, 9.Aralık.2013, "Altın neden değerli?", BBC Türkçe *(Erişim 20.12.2016)*

[6] Ed Prior, 1.Nisan.2013, "How much gold is there in the world?", BBC News (Erişim 20.12.2016)

[7] http://www.numbersleuth.org/worlds-gold/ *(Erişim 20.12.2016)*

[8] Mark Cartwright, 4.Nisan.2014, "Gold in Antiquity", Ancient History Encyclopedia Limited *(Erişim 20.12.2016)*

[9] Coralie Boeykens, "Paper money, a Chinese invention?", National Bank of Belgium *(Erişim 20.12.2016)*

[10] Moshenskyi Sergii, 2008,."History of the Weksel: Bill of Exchange and Promissory Note", Xlibris, 355 s.

[11] "Stockholms Banco", The Riksbank, İsveç *(Erişim 20.12.2016)*

[12] Chizoba Morah, "What is the gold standard?" *(Erişim 20.12.2016)*

[13] Eğilmez Mahfi. "Bretton Woods Sistemi" *(Erişim 20.12.2016)*

[14] Simon Black, 28.Mart.2012, "Only One Currency Is Still Backed By Gold" *(Erişim 20.12.2016)*

[15] Bilge Kağan ÖZDEMİR, 2012, "Para Teorisi, Ödemeler Sisteminin Gelişimi", Anadolu Üniversitesi, 187 s.

[16] http://www.thrivemovement.com/use-alternative-currencies *(Erişim 20.12.2016)*

[17] Stodder James, Ocak 2005, "Implications for Macroeconomic Stability" *(Erişim 20.12.2016)*

[18] Gesell, Silvio, Çev. Philip Pye M.A, "Natural Economic Order " University of Konstanz ,207 s. *(Erişim 20.12.2016)*

[19] Lauren Mcmah, Ağustos 2015, "Artists design banknotes for popular community currencies" *(Erişim 20.12.2016)*

[20] Oracca Marcela; Oracca Maria Jose, Mayıs 2013, "Tumin, pesos, or wealth? Limits and possibilities of a local alternative to scarcity of money and abundance of richness.", United Nations Non-Governmental Liaison Service *(Erişim 20.12.2016)*

[21] Ken Griffith, Nisan 2014, "A Quick History of Cryptocurrencies BBTC — Before Bitcoin", Bitcoinmagazine *(Erişim 20.12.2016)*

[22] Andrew Wagner, Ağustos 2014, "Digital vs. Virtual Currencies", Bitcoin Magazine,Sayı:22 *(Erişim 20.12.2016)*

[23] http://odemeteknolojileri.com/2016/05/dijital-para-liberty-reserve-ceza/ *(Erişim 20.12.2016)*

[24] European Central Bank, Ekim 2012, "1.Virtual Currency Schemes (PDF).", Frankfurt am Main: European Central Bank, 55 s. *(Erişim 20.12.2016)*

[25] European Central Bank, Şubat 2015, "Virtual Currency Schemes – a further analysis (PDF)", Frankfurt am Main: European Central Bank, 37 s. *(Erişim 20.12.2016)*

[26] European Banking Authority, 4.Temmuz.2014, "EBA Opinion on virtual currencies(PDF)", 46 s. *(Erişim 20.12.2016)*

[27] Carter Graydon, Eylül 2014, "What is Cryptocurrency?" *(Erişim 20.12.2016)*

[28] Sarah Rotman, 2014, "*Bitcoin* Versus Electronic Money ",World Bank *(Erişim 20.12.2016)*

[29] Carter Graydon, Eylül 2014, "What is an Altcoin?" *(Erişim 20.12.2016)*

[30] Carl Menger, "Principles of Economics", Ludwig von Mises Institute, 330 s. *(Erişim 20.12.2016)*

[31] Ünsal Çetin, 2014, "Sübjektivist Paradigma" Liberal Düşünce, Yıl:19, Sayı:75, s. 115-122 *(Erişim 20.12.2016)*

[32] James Rickards, 2016, "The New Case for Gold",Barnes & Noble, 192 s.

[33] Cory Mitchell, Ağustos 2016, "Why Gold Always Had A Value", Investopedia *(Erişim 20.12.2016)*

[34] Andreas M. Antonopoulos, 2014, "Mastering Bitcoin", O'Reilly, 330 s.

[35] Katherine Sagona-Stophel, "Bitcoin 101: How to get started with the new trend in virtual currencies", White Paper, Thomson Reuters .

[36] A Wiley Brand, 2016, "Bitcoin for Dummies", Prypto, 208 s.

[37] https://www.weusecoins.com/what-is-cryptocurrency/ *(Erişim 20.12.2016)*

[38] Mahfi Eğilmez, "Kendime Yazılar, Bitcoin" *(Erişim 20.12.2016)*

[39] Mikal E. Belicove, Nisan 2014, https://www.entrepreneur.com/article/232118 *(Erişim 20.12.2016)*

[40] https://en.Bitcoin.it/wiki/Main_Page.*(Erişim 20.12.2016)*

[41] Satoshi Nakamoto, Mayıs 2009, "Bitcoin: A Peer-to-Peer Electronic Cash System" *(Erişim 20.12.2016)*

[42] Patrick "PK" McDonnell, Eylül 2015,"What is the Difference Between Bitcoin, Forex & Gold? A Tripod Theory" *(Erişim 20.12.2016)*

[43] 2013: Year of The Bitcoin Forbes *(Erişim 20.12.2016)*

[44] BBC, 6.Ekim.2014, "Bitcoin price falls to 11-month low", BBC News, *(Erişim 20.12.2016)*

[45] Why The Bitcoin Price Drop Is Really Good News *(Erişim 20.12.2016)*

[46] Rober McMillan, Ocak.2015 , "Silicon Valley VC Thinks a Single Bitcoin Will Be Worth $100,000", Wired Magazine *(Erişim 20.12.2016)*

[47] Christoffer De Geer , Aralık 2015, "Could *Bitcoin* Hit $1,000,000 in the Long Run?" *(Erişim 20.12.2016)*

[48] Ronald A. Glantz, 11.Mart.2014, "Pantera, Primer, What is Bitcoin?", *(Erişim 22.12.2016)*

[49] John Carl Villanueva, 24.Aralık.2015, "How Many Atoms Are There in the Universe?", Universe Today *(Erişim 22.12.2016)*

[50] Daniel J. Bernstein, 2009,"Introduction to post-quantum cryptography" *(Erişim 22.12.2016)*

[51] http://en.*Bitcoin*wiki.org/*Bitcoin*_address *(Erişim 22.12.2016)*

[52] https://en.*Bitcoin*.it/wiki/Address *(Erişim 22.12.2016)*

[53] https://en.*Bitcoin*.it/wiki/Target *(Erişim 22.12.2016)*

[54] Prableen Bajpai, 19.Kasım.2014, "A Look At The Most Popular Bitcoin Exchanges", Investopedia *(Erişim 22.12.2016)*

[55] https://en.wikipedia.org/wiki/Bitcoin_ATM *(Erişim 22.12.2016)*

[56] http://www.sosyalradar.com/turkiyede-ilk-Bitcoin-atmsi-acildi *(Erişim 22.12.2016)*

[57] Katy Barnato, 2.Şubat,2016, "World's first bitcoin mining IPO falls short", CNBC *(Erişim 22.12.2016)*

[58] https://www.smithandcrown.com/what-is-an-ico/ *(Erişim 22.12.2016)*

[59] https://en.Bitcoin.it/wiki/Trade#Auction_sites *(Erişim 22.12.2016)*

[60] https://en.Bitcoin.it/wiki/Casascius_physical_Bitcoins *(Erişim 22.12.2016)*

[61] http://cryptorials.io/how-to-earn-interest-on-Bitcoin-5-different-ways/ *(Erişim 22.12.2016)*

[62] https://Bitcointalk.org/index.php?board=52.0 *(Erişim 22.12.2016)*

[63] https://en.Bitcoin.it/wiki/Bitcoin_faucet *(Erişim 22.12.2016)*

[64] https://en.Bitcoin.it/wiki/Double-spending *(Erişim 22.12.2016)*

[65] https://blockchain.info/charts/n-transactions-per-block *(Erişim 22.12.2016)*

[66] https://Bitcoin.org/en/developer-guide#term-merkle-tree *(Erişim 22.12.2016)*

[67] https://Bitcoin.org/en/developer-guide#block-height-and-forking *(Erişim 22.12.2016)*

[68] https://en.Bitcoin.it/wiki/Controlled_supply *(Erişim 22.12.2016)*

[69] https://www.Bitcoinmining.com/Bitcoin-mining-hardware/ *(Erişim 22.12.2016)*

[70] https://en.Bitcoin.it/wiki/Mining_hardware_comparison *(Erişim 22.12.2016)*

[71] https://en.Bitcoin.it/wiki/Non-specialized_hardware_comparison#Intel *(Erişim 22.12.2016)*

[72] https://www.coursera.org/learn/cryptocurrency/lecture/Zdm9b/lifecycle-of-an-altcoin *(Erişim 22.12.2016)*

[73] https://www.weusecoins.com/altcoin-risks/ *(Erişim 22.12.2016)*

[74] The Law Library of Congress, Global Legal Research Center, Ocak.2014, "Regulation of Bitcoin in Selected" *(Erişim 22.12.2016)*

[75] http://coin-turk.com/turkiye-bitcoin-vergi *(Erişim 22.12.2016)*

[76] Ludwig von Mises, 1951, "The Free Market and Its Enemies: Pseudo-Science, Socialism, and Inflation", 118 s. *(Erişim 22.12.2016)*

[77] Frank Shostak, 17.Nisan.2013, "The Bitcoin Money Myth", *(Erişim 22.12.2016)*

[78] Allen Scott, 8.Nisan.2016, "Austrian School Economists were Bitcoiners, They Just Didn't Know It Yet" *(Erişim 22.12.2016)*

[79] Jeffrey Tucker, 27.Ağustos.2014, "What Gave Bitcoin Its Value?" *(Erişim 22.12.2016)*

[80] https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf *(Erişim 22.12.2016)*

[81] https://www.paypal.com/us/webapps/mpp/about *(Erişim 22.12.2016)*

[82] http://www.bbc.com/turkce/ekonomi/2010/03/100326_japan_deflation.shtml *(Erişim 22.12.2016)*

[83] Timothy B. Lee, 11.Nisan.2013, "Bitcoin Doesn't Have a Deflation Problem" *(Erişim 22.12.2016)*

[84] http://coin-turk.com/blockchain-teknolojisi-ve-bitcoin-1-0-2-0-ve-3-0 *(Erişim 22.12.2016)*

[85] Justin OConnell, 30.Ocak.2016, "Bitcoin 2.0: Fantasy Or Inevitability?" *(Erişim 22.12.2016)*

[86] Nathaniel Popperjune, 29.Haziran.2016, "How China Took Center Stage in Bitcoin's Civil War", NYTimes *(Erişim 22.12.2016)*

[87] Samburaj Das, 21.Ocak.2016, "China's Central Bank Will Look To Issue Its Own Digital Currency as Soon as Possible" *(Erişim 22.12.2016)*