



1882

KONYA TİCARET ODASI
KONYA CHAMBER OF COMMERCE

“21. YÜZYILDA PARA KAVRAMI...” “BITCOIN – KRİPTO PARA”



Araştırma Raporu

Ekonomik Araştırmalar ve Proje Müdürlüğü

Feyzullah Altay

KONYA
Ekim - 2017
www.kto.org.tr



İÇİNDEKİLER:

<u>BAŞLIK</u>	<u>SAYFA</u>
0. GİRİŞ	1
1. PARA NEDİR	1
1.1. Emtia Para	1
1.2. Altın ve Gümüş	1
1.3. Temsili Para	2
1.4. İtibari Para	3
1.5. Alternatif Para	3
1.6. Dijital Para	3
1.7. Sanal Para	4
1.8. Kripto-Para (Şifreli Para)	4
2. BITCOIN	5
2.1. Bitcoin Nedir?	5
2.2. Bitcoin’in Tarihçesi	7
2.3. Bitcoin’in Geleneksel Para Sisteminden Farkları	7
2.4. Bitcoin Piyasasının Altın ve Foreks Piyasası İle Karşılaştırması	9
3. BITCOIN SAHİPLİĞİ	9
3.1. Bitcoin Cüzdanı	9
3.2. Bitcoin Borsaları	11
3.3. Birebir Ticaret	11
3.4. Bitcoin ATM’leri	11
3.5. Ticaret Yoluyla	12
3.6. Fiziki Bitcoin	13
4. BLOK-ZİNCİR (BLOCKCHAIN)	14
4.1. Blok-Zincir Nedir?	14
4.2. Blok-Zinciri Kim Tutar?	14
4.3. Blok-Zinciri Veri Yapısı	14
5. BITCOIN MADENCİLİĞİ	15
5.1. Bitcoin Madenciliği Nedir?	15
5.2. Madenciler Nasıl Çalışırlar?	15
5.3. Para Arzı	16
5.4. Kimler Madenci Olabilir?	16
6. BITCOIN’İN YASAL STATÜSÜ	16



6.1. Bitcoin Dostu 10 Ülke	17
6.2. Bitcoin Düşmanı 5 Ülke	18
6.3. Türkiye’de Bitcoin’in Yasal Statüsü	18
7. DEĞERLENDİRME VE SONUÇ.....	20
7.1. Bitcoin Güvenlidir	20
7.2. Bitcoin Balon mudur veya Bir Tür Saadet Zinciri midir?	20
7.3. Bitcoin VISA veya PayPal’ın Alternatifi Olabilir mi?	21
7.4. Bitcoin ve Blok-Zincir’in Geleceği	21
7.5. Bitcoin Problemleri	22
7.6. Sonuç	23
8. KAYNAKÇA	23

0. 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 bilişsel gelişimine paralel olarak, soyutlaştırmaya devam etmektedir. Bitcoin, 21. yüzyılda, para kavramının nerelere kadar geldiğinin en uç örneklerindedir.

1. PARA NEDİR?

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

- **Değişim aracıdır** - İki malın değişiminde para, bir üçüncü mal olarak araya girer ve değişimi iki bölüme ayırır. Bir mal veya hizmet verilir karşılığında para alınır, başka bir yer ve zamanda ise para verilir başka bir mal veya hizmet alınır.
- **Hesap ve değer birimidir** - Farklı malların değişiminde, değişim oranları para ile belirlenir.
- **Değer biriktirme ve spekülasyon aracıdır** - Arz ve talebin rahatlıkla karşılanmasını sağlar. Aynı zamanda sermaye birikimi ve yatırım aracıdır.
- **İktisat politikası aracıdır** - Ulusal ekonomiler, para arzı ve faiz oranı kontrolüyle iktisat politikalarını gerçekleştirirler.

1.1. Emtia Para

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 kullanılması dahi, kendi kendine değerleri olduğu düşünülür. Bu sebeple, ekonomik çalkantı ve krizlerde bazı insanlar hükümetlerin bastığı paralar yerine emtia paraları kullanma eğilimi gösterirler.

1.2. Altın ve Gümüş

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 gümüşdür. İkisinin de göreceli olarak düşük erime noktasının olması, bozuk para, külçe ve takı haline getirilmelerini kolaylaştırır.

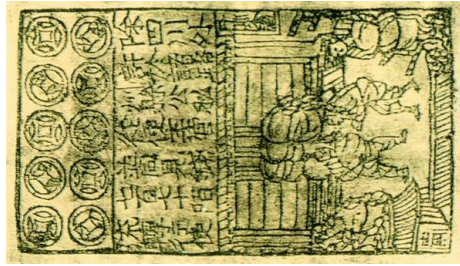
Gümüşün çabuk kararması, altının en yaygın ve değerli emtia para olarak ilk sıraya geçme sebeplerindendir.

Altın ve gümüş, farklı coğrafyalarda, değişim aracı, ödeme aracı, hesap birimi ölçüsü ve değer saklama aracı olarak kullanılmıştır. Antik Mısır'da M.Ö. 3200'lerde, altın çubukların para yerine kullanıldığı biliniyor.

1.3. Temsili Para?

Para olarak doğrudan veya alışılmışı 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 değer, sabit bir oranda karşılığını altın/gümüş olarak tutarlar.

Tarihte bugünkü anlamıyla ilk banknot olan “Jiaozi” (Şekil 1), 10.yüzyılda Çin'de Song Hanedanlığı döneminde basılmış olup, altın paralarla birlikte kullanılmıştır.



Şekil 1: Tarihin en eski banknotu “Jiaozi”

13. yüzyılda, Marco Polo gibi seyahatçilerin Çin'den öğrendikleri kağıt para, Avrupa'da da bilinir hale gelmiştir. Avrupa'da ilk kağıt para Stokholm Bankası tarafından 1661 yılında basılmıştır.

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. Şekil 2'de altına dayalı Dolar gösterilmektedir.



Şekil 2: 1928 tarihine ait altına çevrilebilen 10 Amerikan Doları

1.4. İtibari Para

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.

Altındaki imzalara, düzenlendiği kağıdın taklit edilemeyeceğine ve merkezi otoriteye güven üzerine kurulmuş, mal ve hizmet alışverişi için kullanılan kağıt paraya itibari para denir. Şekil olarak temsili paralara benzeseler de, itibari paralar altın veya gümüşe dayalı değildir.

1.5. 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.

Bölgesel alternatif paraların, bölge dışında kullanımları sınırlıdır. Ekonomik aktiviteleri geçici süreliğine artırdığı, uzun süreli kullanımlarında ekonomik istikrarsızlıklara sebebiyet verdiği de ciddi iddialardandır. 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.

1.6. 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 çıkmıştır.

Dijital paralar, elektronik olarak saklanan ve transfer edilebilen paralardır. 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 para ile 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.

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. 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.

1.7. 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 2015'de yaptığı tanıma göre sanal para; *“Herhangi bir merkez bankası, kredi kuruluşu veya e-para kuruluşu tarafından ihraç edilmediği halde, bazı durumlarda paranın yerine kullanılabilen bir değer dijital temsilidir”*.

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

1.8. 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.

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 dayalıdır ve o ülkenin merkezi otoritelerince düzenlenip denetlenebilirler. Bitcoin ise kendiliğinden bir para birimidir, hiçbir merkezi otorite tarafından düzenlenip

denetlenemez.

Kripto-paralar, merkezi elektronik paraların ve bankacılık sistemlerindeki 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 güvenirlir.

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.

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. Tamamen dijital olup, fiziki temsiline ihtiyaç yoktur. 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.



Şekil 3: Bitcoin sembol ve logoları

BTC kısaltması ile gösterilebilen 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.

Bitcoin istendiği an, TL, Amerikan Doları, Euro veya başka paralar ile takas edilebilir. 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. 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.

Bitcoin transferlerinin güvenliği ve üretiminde kriptoloji kullanıldığı için **kripto-para** 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.

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.

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 hiçbir kişisel bilgiyi içermeyen, karışık bir dizedir. Fakat, Bitcoin cüzdan adresini bildiğiniz birisinin, tüm Bitcoin işlemlerini görmemiz mümkündür, sistem bu anlamda çok şeffaftır.

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, hiçbir 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. 31.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.

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, 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.

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. Satoshi'nin getirdiği yenilik, dağıtık işlemci güçlerini kullanarak her 10 dakikada bir transfer işlemlerini onaylayan bir mekanizmayla, çifte harcamayı engellemiş olmasıdır.

2009 yılında çalışmaya başlayan Bitcoin ağının, şu anki toplam işlemci gücü, dünyanın en hızlı bilgisayarlarının gücünden fazladır. 31 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 hiçbir işlem masrafı alınmadan gerçekleştirilmiştir.

2.3. Bitcoin'in Geleneksel Para Sisteminden Farkları

Bitcoin'in itibari paradan, geleneksel para sisteminden, mali sistem ve işlem yapma açısından farkları;



- I. Bitcoin ağı, merkezi değildir, herhangi bir aracı, yönetici, denetleyici yoktur, uçtan uca birbirine bağlı, gönüllü katılım sağlayan bilgisayarlardan oluşur. Bağlı tüm bilgisayarlar, açık kaynak kodlu, aynı programı çalıştırır, hepsi tüm işlemleri görür, hepsi tüm işlem geçmişini isterse tutabilir, istedikleri an diğer uçlardan işlem geçmişlerini alabilirler.
- II. Dijital itibari paraların işlemlerinde, güvenilen bir aracıya ihtiyaç duyulurken, Bitcoin'de aracıya ve güvene ihtiyaç yoktur. Aracılık sisteminin maliyetleri yüksektir ve güvenlik açıklarına gebedir.
- III. Bitcoin borç değil, değer taşıyıcıdır. Banka hesaplarındaki paralar, bir tür borç senedir. 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.
- IV. 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.
- V. 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.
- VI. 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.
- VII. İtibari fiziksel para işlemlerinin 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.
- VIII. 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.
- IX. İzin gerektirmez. İşlem yapmak için hiçbir kimseden veya kuruluştan izin alınması gerekmez.
- X. Sistem güvenlidir. Güvenlik matematiksel olarak güvenilirliği ispatlanmış, kriptografik dijital imzalama metotları kullanılarak gerçekleştirilir. Kötü niyetli kişilerin veriler üzerinde manüplasyon yapması, gizli/açık anahtar şifreleme yöntemi kullanılması sebebiyle, mümkün değildir.

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.

2.4. Bitcoin Piyasasının Altın ve Foreks Piyasası İle Karşılaştırması

On binlerce yıldır, altının kalıcılığına, nadir bulunuşuna ve kolay parçalara ayrılabilmesine, enflasyon ve ekonomik çalkantılara karşı güvenli bir yatırım aracı olmasına alıştık. 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.

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

3. BITCOIN SAHİPLİĞİ

3.1. 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 yükledikleri 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. Bitcoin toplamak için Bitcoin adresine, sahip olunan Bitcoin'leri harcayabilmek için ise gizli anahtara ihtiyaç vardır.

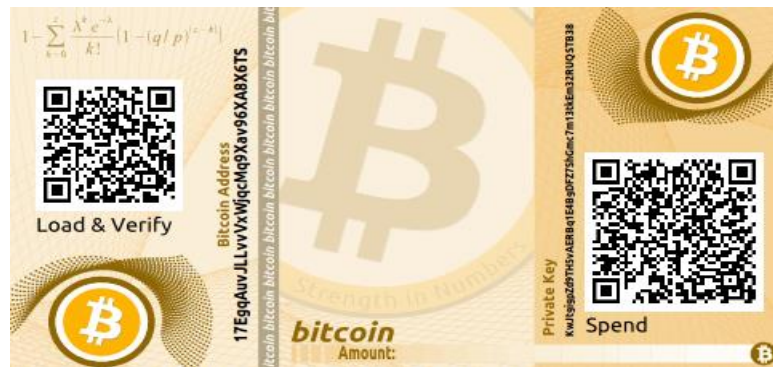
Bitcoin cüzdanları, temsil ettikleri Bitcoin adresine ilişkin tüm girdi, çıktıları gösterirler. Ayrıca, arzu edildiğinde başka bir Bitcoin adresine, Bitcoin transfer işlemini başlatabilirler. Bitcoin cüzdanları, aslında Bitcoin adresinin balansını, Blok-Zincir veritabanlarından okurlar. Tüm Bitcoin işlemleri, 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.



Şekil 4: Donanım olarak tasarlanmış bir Bitcoin cüzdanı

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. 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.

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



- A-

- B-

Şekil 5: Kağıt cüzdan A: Bitcoin adresi / B: Gizli anahtar

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. Bu sebeple, işlem yaparken Bitcoin adreslerinin QR kodlarının kullanılması tavsiye edilir.

3.2. Bitcoin Borsaları

Bitcoin temin etmenin en kolay yolu, Bitcoin satın almaktır. Ulusal paralarla, Bitcoin borsalarından (Bitcoin Exchange) 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.

<http://coinmarketcap.com/currencies/> veya [https:// bitcoin wisdom.com/](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.

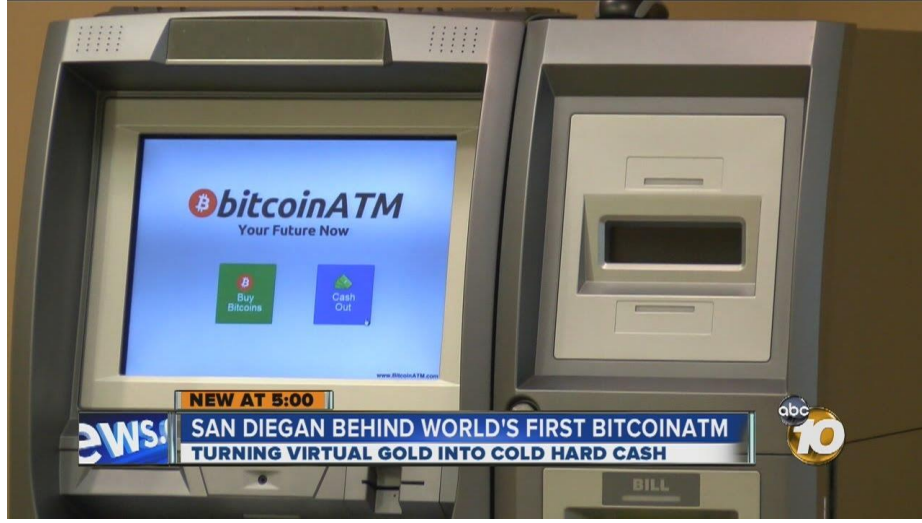
3.3. Birebir Ticaret

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 güvenilirliklerini <https://gemini.com> veya <https://kraken.com> gibi sitelerinden görmek mümkündür.

3.4. Bitcoin ATM'leri

Gittikçe yaygınlaşmakta olan, Şekil 6'da 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. 2013 yılı sonlarında Türkiye'de , İstanbul Atatürk Havalimanı'nda da bir Bitcoin ATM'si hizmete girmiştir

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 tuşlanması gerek kalmaz.



Şekil 6: Bir Bitcoin ATM'si

3.5. 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 7'de Bitcoin ödemesi kabul eden bir çikolata işletmesi görülmektedir.



Şekil 7: 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.

Sanal ticarete 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 kullanılabilir.

Kızılhaç ve GreenPeace gibi örgütlere Bitcoin bağışı yapmak mümkündür. Nepal'deki depremde sonra Nepal Yardım Fonu'na doğrudan Bitcoin bağışı yapanlar olmuştur. Otel rezervasyonu 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.

3.6. 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.

Şekil 8'de 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.



Şekil 8: Fiziki Bitcoin örnekleri

4. BLOK-ZİNCİR (BLOCKCHAIN)

4.1. Blok-Zincir Nedir?

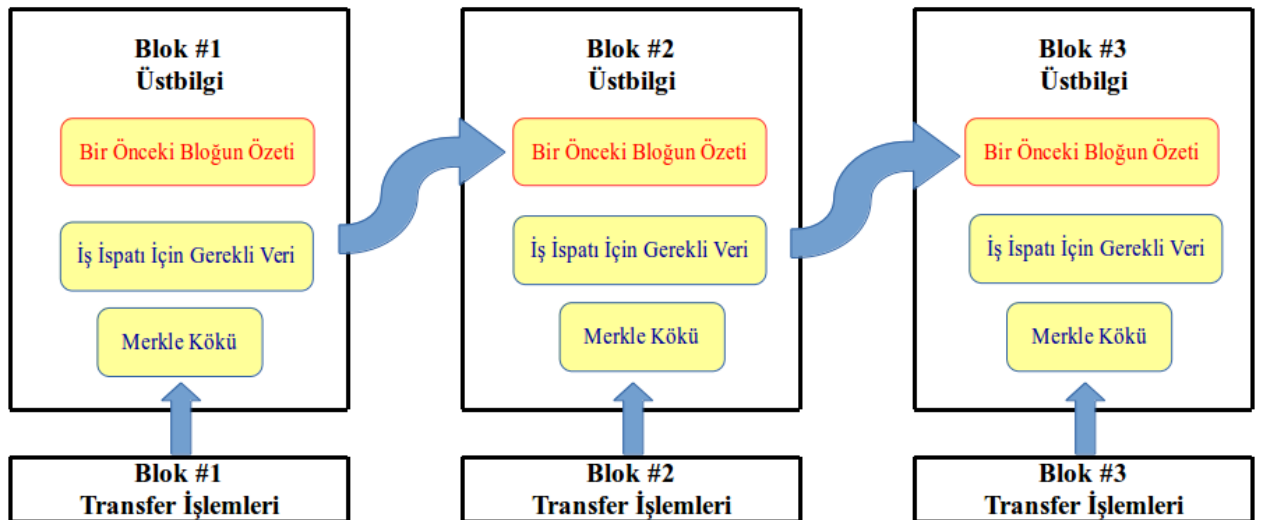
Herkese açık, şeffaf, dağıtık, sıralı ve zaman damgalı Bitcoin transfer işlemlerini içeren dijital küresel hesap defteridir, düz bir veri dosyası, basit bir veritabanıdır. Bitcoin'in ilk ortaya çıktığı 2009'dan bu yana yapılan tüm işlemlerin dijital olarak saklanmasıdır. Hali hazırda yapılan işlemler 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 metodu, merkezi olmayan bir ağ yapısındaki uç bilgisayarlarda, birbirinden bağımsız olarak saklandığından, herhangi bir merkezi hatadan kaynaklanacak problemlere karşı dirençlidir.

4.2. Blok-Zinciri Kim Tutar?

31 Aralık 2016 tarihi itibarı ile küresel hesap defterinin büyüklüğü 92 Gigabyte'dır. Dileyen herkes, merkezi olmayan Bitcoin ağına bağlanarak, bu verileri kendi bilgisayarına indirebilir, 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. 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.

4.3. Blok-Zinciri Veri Yapısı



Şekil 9: Sadeleştirilmiş Blok-Zincir Veri Yapısı

Şekil 9’da 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.

Bir blok içerisindeki tüm işlemler ikiye bölünmüş gruplar halinde özetlenir, ortaya çıkan özetler yine kendi aralarında ikiye bölünmüş gruplar halinde özetlenir. Bu işlem tek bir özet elde edene kadar devam ettirilir. İşlemlerin ikiye bölünmüş özetlenmelerinden oluşan ağ 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 olacaktır, o bloktan sonraki tüm bloklar doğrulanamaz hale gelecektir. Bu yapı hiçbir işlemin geriye doğru değiştirilememesini sağlar.

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 bir blokta geriye doğru bakmaya başlanırsa, en sonunda Genesis bloğuna ulaşılır.

5. BITCOIN MADENCİLİĞİ

5.1. 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 ekleyecek olan madenci, yeni blokla arz edilen parayı ve Bitcoin işlemlerindeki işlem masrafını alarak ödüllendirilir.

5.2. 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 oluşturularak, 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 eklemek isteyecek ve bu durumda ağ karmaşası olacaktır. Bunun önüne geçmek için, blok oluşturmak isteyen madencilerden, birbirleriyle yarışarak çalışmalarını ve bunu ispatlamalarını istenir. Bu, iş ispatı metoduyla yapılır. Blok

oluşturan madencilerden sadece bir tanesinin bloğu geçerli olur, blokların ortalama 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 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.

5.3. Para Arzı

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

5.4. Kimler Madenci Olabilir?

Dileyen herkes madenci olabilir. Bitcoin madenciliği aşırı yarış halinde ilerleyen bir sektördür. Bitcoin'in ortaya çıktığı tarihten bu yana toplam özetleme gücü üssel olarak artmaktadır. 31 Aralık 2016 itibarıyla, Bitcoin madencilerinin toplam özetleme kapasitesi saniyede 2 Milyon Tera $\approx 2 \cdot 10^{18}$ dir.

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

6. BITCOIN'İN YASAL STATÜSÜ

Pek çok ulusal merkez bankası veya bankacılık düzenleme kurumu Bitcoin kullanımını yasaklamamış, ancak finansal kurumları ve bireyleri karşılaşılabilecekleri 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.

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

6.1. 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.

Sayıda 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 metodu 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 metodu 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 metoduyla 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.

6.2. 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.

6.3. Türkiye’de Bitcoin’in Yasal Statüsü

25 Kasım 2013'te Bankacılık Düzenleme ve Denetleme Kurumu, Şekil 10'da 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.



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 itibarı ile ödeme hizmetleri sunan ya da elektronik para ihraç eden ve bu Kanun kapsamında ihdas edilen ödeme veya elektronik para kuruluşu kategorisine dahil edilebilecek olan kuruluşlar Kurumumuzca çıkarılacak ilgili yönetmeliklerin yayımı tarihinden başlayarak bir yıl içinde Kurumumuza başvurarak gerekli izinleri almak ve uygulamalarını bu düzenlemelerde yer alan hükümlere uygun hale getirmek zorundadır.

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

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

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

Kamuoyuna saygıyla duyurulur.

Şekil 10: BDDK'nın Bitcoin ile ilgili basın açıklaması

7. DEĞERLENDİRME VE SONUÇ

7.1. Bitcoin Güvenlidir

Bitcoin güvenlidir, çünkü;

- Merkezi değildir, merkezi bir arıza noktası yoktur, bireysel olarak kullanıcılar heklense de (hacked), sistemin bütünü bundan etkilenmez.
- Kriptografik olarak blokların ve blok içi işlemlerin bütünlüğü ve kronolojisi korunmaktadır.
- Bireysel olarak her Bitcoin cüzdanı gizli anahtar ile korunmaktadır. Gizli anahtar olmadan, cüzdanlar üzerinden işlem yapmak mümkün değildir.
- Bitcoin arzı, dağıtık olarak çalışan madencilerin konsensüsü ile sağlanır. Bunun haricinde, hiçbir 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.

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.

7.2. 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 değildir.

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.

7.3. 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. PayPal ise, 2015 yılında toplam 4,9 Milyar işlemle, saniyede ortalama 155 işlemle başa çıkabilmiştir.

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.

Bitcoin yaygınlaştığında, 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.

7.4. 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.

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 başlamışlardır. 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.

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 usulsüz kullanımlarının önüne geçilebileceği düşünülüyor.

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. Çin Siberuzay İdaresi, Ekim 2015'te dünyanın Bitcoin sonrası döneme girdiğini, bu devrimsel değişiklikleri kimsenin görmezden gelemeyeceğini ifade etmiştir.

7.5. Bitcoin'in Problemleri

İnsan doğası yeni ve değişim gerektiren hususlarda endişelidir. Alışkanlıklarımızı hemen ve tümenden 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.

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.

7.6. Sonuç

Onbinlerce yıldır alışık olduğumuz altın ve yüzlerce yıldır kullandığımız nakit paralarla karşılaştığımızda 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 kullanılabilir 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.

8. KAYNAKÇA

- “Bitcoin Elektronik Paraya Karşı” Dünya Bankası, 2014
- “Kripto-Para Bitcoin” SPK Araştırma Dairesi, 2016
- “Ekonominin Prensipleri” Carl Menger, Ludwig von Mises Institute
- “Kendime Yazılar-Bitcoin”, Mahfi Eğilmez, 2016
- http://en.Bitcoin.wiki.org/Bitcoin_address
- <https://en.Bitcoin.it/wiki/Address>
- <http://www.sosyalradar.com/turkiyede-ilk-Bitcoin-atmsi-acildi>
- https://en.Bitcoin.it/wiki/Trade#Auction_sites
- <https://Bitcoin.org/en/developer-guide#block-height-and-forking>