T.C.

İSTANBUL TİCARET ÜNİVERSİTESİ
FİNANS ENSTİTÜSÜ

SERMAYE PİYASASI ANABİLİM DALI

SERMAYE PİYASASI TEZLİ YÜKSEK LİSANS PROGRAMI

KAYIT ZİNCİRİ TEKNOLOJİSİNİN FİNANSAL PİYASALARDAKİ YANSIMASI: KRİPTO PARA VE BITCOIN UYGULAMALARI

Yüksek Lisans Tezi

Anı Bulut

100043754

İstanbul, 2019

T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
.....Finans..... ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ ONAY FORMU

.....Sermaye Piyasası.....

Yüksek Lisans programı öğrencisi.....Ani Bulut.....'.....

...Kayıt Zincirci Teknolojisinin Finansal Piyasalardaki Yansıması: Kripto Para ve Bitcoin Uygulamaları.....başlıklı tez çalışması, Enstitümüz Yönetim Kurulu 18.01.19...tarih ve ...54-7.....sayılı kararıyla oluşturulan jüri tarafından oybirliği/oyçokluğu ile Yüksek Lisans Tezi olarak kabul edilmiştir.

	UNVANI, ADI SOYADI	İMZA
TEZ DANIŞMANI	: Doç. Dr. Oğuzhan Artar	
JÜRİ ÜYESİ	: Prof. Dr. Ercan Sandıkçı	
JÜRİ ÜYESİ	: Dr. Öğr. Üyesi Hicabi Ersoy	

(*) Yüksek lisans tez savunma jürileri en az biri kurum dışından olmak üzere danışman dahil en az üç öğretim üyesinden oluşur. Jürinin üç kişiden oluşması durumunda eş danışman jüri üyesi olamaz. Eş tez danışmanının jüri üyesi olması durumunda asıl jüri beş üyeden oluşur.

İÇİNDEKİLER

Sayfa No.

ÖZET

Küresel finans krizinin üzerinden on yıl geçmesinin ardından nakit ağırlıklı ekonomiyi daha nakitsiz bir topluma yöneltmek için kayıt zinciri teknolojisine yönelik gelişmelere ağırlık verilmiştir. Dijital paraların gelişmesiyle kayıt zinciri teknolojisini kullanan kripto paralar (bitcoin vb.) gibi finansal çözümler parayı saklamak ve transfer etmek için yenilikçi platformlar sağlamaktadır. Dijital para bilinen fiziksel ödeme aracı gerektiren kâğıt para veya çek gibi yöntemlerin aksine bir internet ödeme aracıdır. Kripto para, dijital para işlemlerinde dijital para arzıyla beraber siber güvenlik ve kontrol platformlarını sağlamak için şifreli algoritmalar kullanan bir dijital para birimi olmaktadır. Kayıt zinciri (Blockchain) teknolojisini kullanan, en dikkat çeken ve yaygın olan kripto para örneği olarak bilinen dağıtık şifreli algoritma kullanan Bitcoin'dir.

Bitcoin'e artan ilgiye rağmen kabul edilmesi ve anlaşılması oldukça zordur. Kripto paraların parasal işlemlerde geleneksel uygulamalara göre daha ayırt edici yeni yöntemleri olduğu için oldukça tartışılmaktadır. Ancak bu sistemin topluma etkisi yavaş yavaş ortaya çıkmaya devam etmektedir. Ödemeler ve bugün bildiğimiz merkezi olmayan ağlar açısından bir dönüm noktası olan Bitcoin önemli bir icat olarak görülmektedir. Bu buluş; pek çok yeniliği, bitcoinle uğraşan ve çalışan kullanıcıların bilincinde oldukları, göze aldıkları riskleri de beraberinde getirmektedir.

Bu çalışma; ağırlıklı olarak Bitcoinin temel özellikleri üzerinde durmuş olsa da diğer kripto paralarda da benzer özelliklerin bulunması sebebiyle, gelecekte kripto paralarla ilgili yapılacak araştırmalara önemli bir kaynak yaratarak ilgili literatüre önemli katkılar sağlamayı amaçlamaktadır.

Anahtar Kelimeler: Dijital Paralar, Kripto Paralar, Bitcoin

ABSTRACT

After a decade from the global financial crisis in 2008, developments in Internet-based payment platforms employing the blockchain technology known as “cryptocurrencies” contributed their integration in the official payment systems. Use of digital currency allows faster, more flexible, and more innovative payments in financing goods and services compared to payment systems that are based on fiat currency. A subset of a digital currency, cryptocurrency is a special class of digital currency and a form of programmable money which uses cryptographic algoritms in digital currency transactions for siber security and control platforms along with digital money supply. One of the most well well-known cryptocurrencies, Bitcoin uses a very complex cryptographic algorithm that requires a connected peer-to-peer network of computers to conduct computationally expensive mathematical processes.

Despite of the increasing interest in Bitcoin it is very complex for the financial institutions and mainstream to accept and have an insight on them for further use. Cryptocurrency (i.e. Bitcoin) are discussed broadly and widely in both financial instituons and regulators because of its distinctive and reformative new methods in monetary transactions. Consequently Bitcoin known as a milestone for payments and decentralized networks today has been seen as an important invention. This brings lots of known advantages and accepted risks together for the people who use this technology.

This thesis has focused on fundementals of Bitcoin however other crypto currencies also have these key features. Therefore this study aims to serve as a useful source for further studies and provide understanding into cryptocurrencies while explaining Bitcoin.

Keywords: Digital Currency, Cryptocurrencies, Bitcoin

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AFI: Alliance for Financial Inclusion (Finansal Tabana Yayılma Birliği)

AIIB: Asian Infrastructure Investment Bank (Asya Altyapı Yatırım Bankası)

BRICS: Brezilya, Rusya, Hindistan, Çin ve Güney Afrika ülkeleri

GIIN : Küresel Etki Yatırımı Ağı (The Global Impact Investing Network)

P2P: Peer to Peer (Eşten eşe)

PKI : Public Key Infrastructure (Açık Anahtar Altyapısı)

SNS: Social Networking Site **(**Sosyal paylaşım sitesi**)**

Dapp, dApp veya DApp: Decentralized application (Merkezi olmayan uygulamalar)

TOR: The Onion Routing (Anonim Ağ)

SSL: Secure Sockets Layer (Güvenli Giriş Katmanı)

API: Application Programming Interface (Uygulama Programlama Arayüzü)

KYC: Know your customer (Müşterini Tanı)

SAR: Suspicious Activity Report (Şüpheli İşlem Bildirimi)

GBI: Gold Bullion International LLC

CPP: Client Puzzle Protocol (istemci bulmacası fonksiyonu)

POW: Proof of Work (İş İspatı)

RPOW: Reusable Proof of Work (Yeniden Kullanılabilir İş İspatı)

DAO: Decentralized Autonomous Organization (Merkezi Olmayan Otonom Organizasyon)

SEC: U.S. Securities and Exchange Commission (ABD Menkul Kıymetler ve Borsa Komisyonu)

FINMA: Swiss Financial Market Supervisory Authority (İsviçre Mali Piyasalar Denetleme Kurumu)

AML/TF: Anti-Money Laundering and Terrorist Financing (Kara Para Aklama ve Terörizmin Finansmanı)

ICO: Initial Crowd Offering (İlk Kitleye Arz)

IPO: Initial Public Offering (İlk Halka Arz)

TCMB: Türkiye Cumhuriyeti Merkez Bankası

GİRİŞ

Milenyum olarak da bilinen 1980 ile erken 2000'li yıllar arasında doğan "y" kuşağında 2008 yılı oldukça derin ve etkisini uzun süre devam ettiren bir iz bırakmıştır. O yıl, Amerika'da finansal piyasaların çöküşünün başladığı ve hemen sonrasında Asya ve Avrupa'ya yayılarak patlamak üzere olan küresel finansal krizi tetikleyen yıl olmuştur. Her ülke daha önce denenmemiş parasal genişleme politikaları ve mali teşvik paketleriyle üstesinden gelmeye çalışırken henüz kariyerlerinin başlarında çoğu y jenerasyonlu ise yüksek işsizlik oranları ve sınırlı ekonomik imkanlarla mücadele etmiştir. Hayatlarının sadece başkent veya büyük kentlerdeki fırsatlarla değil aynı zamanda teknolojik imkanlarla da gelişebileceğine inanan küçük bir kesim içinse 2008 yılı, eşten eşe, merkezi olmayan kripto paranın yani Bitcoin protokolünün başlangıcı olarak hatırlanacaktır. Satoshi Nakamoto'nun "White paper[1]" olarak bilinen tanıtım yazısı küresel finansal krizden hemen sonra, dünyaya önemli bir katkı olarak, önceden yayınlanmış herhangi bir akademik makaleye dayanmaksızın, ilk kez Kasım 2008'de internette bir şifreli eposta listesinde[2] ortaya çıkmıştır[3].

Bu tezde, günümüzde kripto paranın çektiği büyük ilgi ve konuyla ilgili az sayıda akademik çalışma olması sebebiyle Bitcoin'e odaklanarak kripto para ve kayıt zincirinin finansal piyasalardaki yansımaları ve işleyişi araştılacaktır. Çalışma kripto para hem para birimi hem de bir sistem olarak Bitcoin; kayıt zinciri ve bu kavramlara ilişkin tartışmalara katkı sağlamayı amaçlamaktadır. Çalışmanın ilk bölümünde bu kavram çerçevesinde tanımlar verilmiş ve Bitcoin sisteminin işleyişi üzerinde durulmuştur. Çalışmanın ikinci bölümünde Bitcoin ve kripto paranın faydaları ve riskleri hakkında bilgi verilerek detaylı incelenmiştir. Çalışmanın son bölümünde kripto paraların başarı koşulları ve gelecekteki risk ve tehditleri incelenmiştir.

---

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (çevirimiçi), 2008 https://bitcoin.org/bitcoin.pdf, (Erişim Tarihi: 05.07.2018)

[2]Satoshi Nakamoto, "Bitcoin P2P e-cash paper", Cryptography Mailing List, 2008, (çevirimiçi) http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html. (Erişim tarihi 23.05.2018).

[3]David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015, s. 20.

1. KRİPTO PARALAR: KAVRAMSAL VE TEKNİK ÇERÇEVESİ

1.1 Para ve Ödemelerde Yeni Dönem: Alternatif Olarak Bitcoin

Küresel krizlerde finansal sistemdeki çatlaklar işletmelere yayıldıkça hükümetlerin yıkılmaz gibi görünen ancak sonradan zayıf düşen finansal kuruluşları kurtarmak zorunda kaldığı zamanlar olmaktadır. Kurtarma (bail-out), vergi artışı yoluyla edinilen kazancın veya kamu desteğinin kurtarılacak finansal kuruluşa hatasını düzeltmesi için verilmesi anlamına gelmektedir. İçeriden kurtarma (bail-in) ise finansal kuruluşların doğrudan müşteri hesaplarını kendi kayıplarını karşılayabilmek için paylaşmaları anlamına gelmektedir[4]. Güney Kıbrıs'ta 2013 yılında yaşanan kriz örneğinde olduğu gibi 25 Mart'ta kabul edilen kurtarma paketine göre Avrupa İstikrar Mekanizması ve IMF Güney Kıbrıs'a 10 milyar euro vermiş, 6 milyar euro ise ülkedeki 100 bin euro üzerindeki mevduatlardan değişen oranlarda kesilmiştir. Bankaların kapanmasından doğan kayıp, hisse senedi sahipleri ile mevduatı 100.000 Euro'yu aşan mudiler tarafından karşılanmıştır[5]. Bir başka örnekse 2015 yılında Yunanistan'da yaşanan ekonomik krizin sonucu olarak bankaların kapanması ve insanların mevduatlarına ulaşamamalarıyla beraber aynı zamanda ATM'lerden kısıtlı para çekebilmeleridir. Küresel krizin 2009 yılında başlayan Avrupa'daki görüntüsü bu şekilde olurken başlangıcı hemen hemen aynı yıla gelen Bitcoin, krizin yoğun olarak hissedildiği 2013-2015 yılları arasında Avrupa'da bankacılık sistemine bir alternatif olarak görülmeye başlanmıştır.

Paralar, para arzını kontrol eden merkez bir otorite tarafından basılmaktadır. Bitcoin ise bir eşten eşe sistemidir yani merkez bir otorite aksine Bitcoin'ler ağda işlemlerin oluşmasına yardımcı olan kullanıcılara verilir yani bitcoin madenciliği yapan madenciler tarafından bulunur. Çoğu paranın aksine Bitcoin sabit bir kurallar setine tabi oluşturulur. Ana fikir, "değeri merkez bir otorite tarafından belirlenmeyen" bir para oluşturmaktır. Çünkü ne kadar yaptırım uygulanırsa uygulasın bir matematik probleminin sonucu değiştirilemez, iki artı iki her zaman

[4] Gökben Altaş, "Gelişmiş Ülkelerde Mevduat Ve Yatırım Bankacılığının Ayrılması", Sermaye piyasasında Gündem Dergisi, TSPAKB, Sayı 132, Ağustos 2013, ISSN 1304-8155, s. 16/20.
[5] Seda Eren, "Güney Kıbrıs'ta Bankacılık Krizi", ASEM (Ankara Siyasal ve Ekonomik Araştırmalar Merkezi, Nisan 2013, (çevirimiçi) http://asem.org.tr/tr/publication/details/6083/G%C3%BCney-K%C4%B1br%C4%B1s'ta-Bankac%C4%B1l%C4%B1k-Krizi, (erişim tarihi 26.04.2018)

dört eder. Bitcoin'ler adına madencilik (mining) denilen bir süreç sonucunda oluşurlar. Bu madencilik sürecinde kullanılan araçsa bilgisayardır. Bitcoin madencileri denilen bu bilgisayarlar işlemleri doğrulamak için gereken işi yapan ve kayıt zincirine kaydeden çok özellikli ve profesyonel bilgisayarlardır. Kayıt zinciri, dünyanın her bir yanından binlerce bilgisayarın adına "bitcoin" denilen dijital bir madene sahip olabilmek için beraber çalıştığı açık bir muhasebe sistemi olarak kabul edilebilir. Birine para gönderdiğinizde bu işlem tüm ağa duyurulur. Bu işlem madenciler tarafından doğrulanarak onaylandığında adına kayıt zinciri denilen herkese açık ortak bir deftere kaydedilir. Kayıt zinciri, sistem başladığından bu yana yapılmış tüm Bitcoin işlemlerinin bir kaydını tutmaktadır. Böylelikle ağda bulunan herkes tarafından paylaşılmakta ve devam etmesi sağlanmaktadır. Yaptıkları işin karşılığı olarak madenciler bitcoin kazanırlar ve böylelikle kullanıma yeni bitcoin bırakılmış olur. Sistem sadece 21 milyon bitcoin oluşacak şekilde tasarlanmıştır. Zaman geçtikçe madencilik ödülü azalmakta ve belirli bir sayıdan arzının olması ise onu dijital bir altın gibi değerli kılmaktadır. Bitcoin internetin ilk parasıdır[6].

Bilgisayar bilimcileri yıllar boyunca yeni teknolojileri deneyerek dijital para oluşturmaya çalışmıştır. Ama Satoshi daha önce hiç yapılmamış bir yöntemle bunları birleştirmenin bir yolunu bulmuş ve Bitcoin'i icat etmiştir. Kasım 2009'da 1 USD karşılığı 1,309 bitcoin olan ilk değişim kuru yayınlanmıştır. Bitcoin o dönem ucuzdur ve devam eden yılda ticarette bir sentin kesirli halleriyle kullanılmaya devam edilmiştir. 2010 baharında Florida'da yaşayan ve adı Lazslo olan bir madenci bitcoinini somut bir şey satın almak için kullanmayı denemeye karar vermiştir. Ağdakilere ona pizza alınması karşılığında 10,000 bitcoin vermeyi teklif etmiştir. Londra'daki bir adam bu teklifi kabul etmiş ve uzaktan telefon siparişi ile Papa Johns'tan iki pizza siparişi vermiştir. Bu işlem somut bir ürün için yapılmış ilk Bitcoin işlemi olarak bilinmektedir[7]. 2010 yılında Tokyo'da yerleşik Mt. Gox

[6] Ken Griffith, "A Quick History of Cryptocurrencies BBTC — Before Bitcoin ", Nisan 2014, (çevirimiçi) https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/, (erişim tarihi 26.04.2018)
[7] Benjamin Wallace, "The Rise and Fall of Bitcoin", 2011, (çevirimiçi) https://www.wired.com/2011/11/mf-bitcoin/, (erişim tarihi 26.04.2018)

piyasaya atılan ilk takas ofisidir[8]. 2010 Kasım ayı itibariyle 4 milyon bitcoin bulunmuş ve değişim oranı ise her bir maden başına 50 sent olmuştur.

Bugün dünyada birçok yenilikçi para gönderme sistemi bulunmaktadır ve bunların çoğu mobil telefon, internet ve dijital depolama kartı gibi platformlarda yapılmıştır. Bu alternatif ödeme sistemleri PayPal (internet), Apple Pay (mobil uygulama), Google Wallet (internet), Alipay (internet), Tenpay (ödeme hizmetleri sağlayıcısı), Venmo (mobil uygulama), M-Pesa (mobil uygulama), BitPay (dijital depolama), Moven (mobil uygulama), BitPesa (dijital depolama), PayLah! (Dijital depolama), Dash (dijital depolama), FAST (ödeme hizmetleri sağlayıcısı), Transferwise (ödeme hizmetleri sağlayıcısı) ve benzerleri oldukça ilgi görmekte ve hızla büyümektedir.

Mal ve hizmetlerin finansmanında dolaşımdaki paraya dayanan ödeme sistemlerinin haricinde dijital paranın kullanımının artması daha hızlı, daha esnek ve daha yenilikçi ödeme yolları sağlamaktadır. Ancak tüm bunların içinde bir dijital para diğerlerinden ayrılmaktadır. Bitcoin bugün en bilinen dijital paralardan biridir. Daha belirgin bir ifadeyle Bitcoin, bilinen adıyla dijital paranın bir alt tipi olan kripto paradır. Bitcoin türünün ilk örneği olarak kabul edilen benzersiz bir kripto paradır. Ondan sonra oluşturulan diğer türlerde olduğu gibi işlemlerini sürdürmek için internetin gücünü kullanmaktadır.

1.2 Dijital Para

Bu bölümde dijital para tarihsel gelişimi, kavramsal yaklaşım, alternatif para özellikleri açısından incelenmiştir.

1.2.1 Paranın Gelişimi

Hayvanların evcilleştirilmesi ve tarımın başlamasıyla milattan önce 6000-9000 yılları arasında hem tarım hem de hayvan ürünleri bir “değişim aracı” olarak

[8] Jason Mick, "Inside the Mega-Hack of Bitcoin: the Full Story", 2011, (çevirimiçi) https://tr.scribd.com/document/166287990/DailyTech-Inside-the-Mega-Hack-of-Bitcoin-the-Full-Story-pdf, (erişim tarihi 25.05.2018)

kullanılmaya başlanmıştır[9]. Para ile ticaretin ilk örneklerinde değişim için seçilen ürünleri, en faydalı ve tekrar kullanımına ve tekrar pazarlanabilirliliğine göre en dayanıklı oluşları belirlemiştir. Aristotle'nin toplumlarda paranın ilk oluşumu ile ilgili görüşü "bir ülkenin halkı diğer bir ülkenin halkına daha bağımlı olduğunda ve ihtiyaç duyduklarını onlardan alıp kendilerinde çok olanı onlara verdiklerinde para zorunlu bir şekilde kullanılmaya başlandı" şeklindedir[10]. Dünya üzerinde çoğu kültürde mal parası yani hem para olarak hem de kendi içinde değeri olan nesnelerin kullanımı milattan önce 3000'li yıllarda başlamıştır[11]. Eski Çin, Afrika ve Hindistan'da deniz kabukları kullanılmıştır. Milattan önce 1000'li yıllarda bronzdan yapılmış küçük bıçak ve el kürekleri Çin'de para yerine kullanılmıştır. Üretilen ilk maden milattan önce 700 ve 500 yılları arasında Hindistan, Çin ve Ege denizi etrafındaki şehirlerde farklı farklı yapılmıştır. Metalin değişik formlarda işlenmesi yeni bir gelişme olarak kabul görmüştür.[12] Pheidon, Akdenizde ağırlık ve para standartlarını resmi olarak belirleyen ilk kişi olarak bilinmektedir. Madeni para basma milattan önce 7.yüzyıl sonlarında Ön Asya'nın Yunan şehirlerinde ve sonrasında milattan önce 500'lü yıllarda Ege ve İtalya'nın güney kesiminde başlamıştır. Üzerinde bir otorite resmi veya adı olan ilk madeni para ise Paris'te görülmüştür[13]. Mihenk taşının keşfi madeni para ve metal bazlı para kullanımına yol açmıştır. Bu taş sayesinde her türlü yumuşak metalin saflık değeri ölçülebilmiştir. Altın yumuşak bir metal aynı zamanda da bulunması zor, işlenebilir ve saklanabilir olduğu için de para olarak kullanımı önce Ön Asya'da ve sonra dünyada hızlıca yayılmıştır[14]. Kâğıt para ise 11. yüzyılda Çin'de kullanılmaya başlanmıştır[15]. Kökleri 618-907 yılları arasında büyük ticari anlaşmaları için ağır ve yüklü miktardaki madenleri yanlarında taşımak istemeyen tüccar ve toptancıların madenlerinin

[9] Glyn Davies, A History of Money from Ancient Times to the Present Day, Cardiff: University of Wales Press, ISBN 0 7083 1351 5. 1996.
[10] David Kinley, Money: A Study of the Theory of the Medium of Exchange, Simon Publications LLC, 1 September 2003, ISBN 193251211X.
[11] Arthur O'Sullivan ve diğerleri, Economics: Principles in action, Upper Saddle River, New Jersey 07458: Pearson Prentice Hall, 2003, ISBN 0-13-063085-3, s. 246
[12] David M. Schaps, "The Invention of Coinage in Lydia, in India, and in China", XIV International Economic History Congress, Helsinki, 2006, (çevirimiçi) http://www.helsinki.fi/iehc2006/papers1/Schaps.pdf.
[13] Adkins ve diğerleri, Handbook to Life in Ancient Rome, Oxford University Press, 1998, ISBN 0195123328.
[14] William Arthur Shaw, The History of Currency, 1252–1896. Augustus m Kelley Pubs., 1989, ISBN 0678002568.
[15] Daniel R. Headrick, Technology: A World History, Oxford University Press., 2009, ISBN 978-0-19-988759-0, s. 85.

saklanması karşılığında aldıkları depozit makbuzundan gelen Banknot gelişimi 7.yüzyılda yerel kâğıt para basımları şeklinde Çin'de başlamıştır. Merkezi hükümet kâğıt para basmanın ekonomik faydalarını görünce bu depozit makbuzlarını veren dükkanlara bunları basma hakkı vermeye başlamıştır. 12. yüzyıl başları itibariyle bir yılda düzenlenen banknot sayısı 26 milyonluk dizili madeni paraya karşılık gelmektedir[16]. Kâğıt para Avrupa'da 13.yüzyılda Marco Polo ve William of Rubruck gibi gezginler sayesinde öğrenilmiştir. Orta çağ'da İtalya'da uzun mesafelerde büyük meblağlı para taşımanın zor ve güvensiz olmasından ötürü para tüccarları ödeme senedi kullanmaya başlamıştır. Başlarda bu senetler sadece onları düzenleyen kişiye hak verirken sonrasında ona sahip herhangi bir kişiye üzerinde yazılı tutarı ödenmesi emrine dönüşmüştür. Bu senetler bilinen banknotların öncüleri olarak kabul görülebilmektedir.[17] Avrupa'da ilk banknot 1661 yılında bugünkü adıyla Bank of Sweden olan Stockholms Banco tarafından basılmıştır. Özel ticari bankacalarca basılan banknotların kullanımı sonradan devlet kontrolünde ve izninde basımı yapılan kanuni paraya dönüşmüştür. 1694 yılında İngiltere'de Bank of England, 1913 yılında Amerika'da Federal Reserve Bank, 1931 yılında Türkiye'de ise TCMB para basma hakkına sahip olmuştur[18]. Günümüzde devlet tarafından yasal ödeme aracı olarak tedarik edilen bu paralar kısmen altın veya gümüşle desteklendikleri ve teoride altına veya gümüşe çevrilebildikleri için temsili para biçimindedirler. 1980'li yıllardan itibaren denenmeye başlanan dijital para sistemleri ile gelen son gelişme ise kayıt zinciri adı verilen şifreleme yoluyla güven ve takas edilebilirliği tüm kullanıcılarına sağlamayı ve onlar tarafından bozulmadan geliştirilebilmeyi amaçlayan herkese açık dağıtılmış bir defterdir[19].

1.2.2 "Dijital" yerine "Sanal"

Bir elektronik ödeme birimi olarak parayı tanımlarken çoğunlukla dijital ve sanal birbirleri yerine kullanılabilen kelimeler olmalarına rağmen "sanal" kelimesinin

[16] Jacques Gernet, Daily Life in China, on the Eve of the Mongol Invasion, 1250-1276, Stanford University Press, 1962, ISBN 0804707200.
[17] Susanne König, The Evolutıon Of Money From Commodity Money to E-Money, UNICERT IV Program, 2001, (çevirimiçi) http://www.ww.uni-magdeburg.de/fwwdeka/student/arbeiten/009.pdf)
[18] TCMB, "Türkiye'de Banknot Basımının Tarihçesi, Banknot Üretim Süreci ve Emisyon Politikaları", Ankara, 2012, ISBN (elektronik): 978-605-5758-83-7.
[19] David Chaum, "Blind signatures for untraceable payments", Department of Computer Science, University of California, Santa Barbara, CA, Springer-Verlag. 1998. (çevirimiçi) http://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF)

olumsuz bir çağrışımı vardır. Dijital veya elektronik kayıt biçimde depolanan parayı tanımladığında "sanal", "görünüşte gerçek" olan ama tam olarak "gerçek" olmayan bir şeyi işaret etmektedir. Hatta, Çince gibi dillerde "sanal kelimesi "fiziksel" olarak bulunmayan ama bilgisayar ürünü veya simülasyonu anlamında "hiçbirşeyden yaratılmış" olarak kabul edilir. Ancak sıklıkla "sanal" olarak ifade edilen bu paralar, var olmaları açısından oldukça "gerçektir". İşte bu nedenle de genelde bu tip paraları belirtirken, sanal para yerine daha nötr bir anlam veren digital para ifadesi tercih edilir.

1.2.3 Alternatif Paraların Sınıflandırılması

Dolaşımdaki paralar haricindeki değişim araçlarına alternatif paralar denir. Tarih boyunca birçok alternatif para bulunmaktadır. Hileman[20] bunları iki geniş gruba ayırır: maddi ve dijital. Maddi paralar, "mal para" ile yakından ilişkilendirilmiştir ve değerleri, diğerlerine göre az bulunur oluşlarından ve parasal olmayan faydalarından gelir.

⇒ **İçsel Faydalı Paralar**

2. Dünya Savaşı sonrasında Berlin'deki metal ve sigaralar ve günümüzde ödemeli telefon kartları ve kısmen para değeri olan akıllı kartlar bu sınıftaki paralara girer. Bu sınıf, parasal araçlarda olduğu gibi idari yönetime dayalı değildir ve daha da önemlisi içsel değeri bir soyutlama değildir ve belirli bir coğrafi bölgeye has olması şart değildir.

⇒ **Simgesel Paralar (Token)**

17.ve19. yüzyıllar arasındaki İngiliz simgesel paraları ve Büyük Buhran dönemi 1930'ların geçici senetleri tarihsel örneklerdir. Günümüzde ise yerel veya bir topluluğa has paralar örneğin İngiltere'de Brixton Pound'u, Bristol Pound'u; Massachusetts eyaletindeki Berkshire bölgesinde kullanımda olan BerkShares ve Kanada'da Spring Dolar'ı. Kullanımları belirli özel bir amaca yönelik olduğu için simgesel paraların içsel değeri daha azdır, genellikle mal karşılığı veya mal tedariğini sınırlama gibi bazı sosyal sözleşmeler veya anlaşmalarla sınırlıdır.

[20] Garrick Hileman, The Bitcoin Market Potential Index, University of Cambridge; London School of Economics, 2014, (çevirimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752757

⇒ **Merkezi Dijital Para**

Örnekleri finansal, telefon veya parekendeci firmaların promosyon veya teşvik amaçlı verdiği ödül puanlar, havayolu firmalarının verdiği mil puanlar, içeriği internet tabanlı sanal dünya olan Second Life'taki Linden Dolar'ı ve World of Warcraft altını (bilgisayar oyunu) gibi kapalı sistemde belirli kuruluşlarla yapılan işlemler sonucu kazanılan ve serbest piyasa sisteminde diğer kuruluşlarla da işlem yapmayı mümkün kılan Flooz ve Beenz gibi firmaların paraları. Brixton Pound'u, BerkShares ve Salt Spring Dolar'ı gibi yerel paralar da simgesel olarak sınıflandırılmalarının yanında bu kategoriye girerler. Yönetim şekli merkezi değildir.

⇒ **Dağıtılmış ve/veya Merkezi Olmayan Dijital Paralar**

Bu sınıfa Bitcoin, Litecoin ve Dogecoin gibi kripto paralar girer. Dışarıdan herhangi bir acente vasıtasıyla işlem görebilir ve yönetimi, açık kaynaklı bir yazılım olması sebebiyle temel olarak merkezi değildir. Yapılan faaliyetlerden sorumlu herhangi bir yasal idare olmadığı için genel düzenlemelerin dışında kalırlar.

1.3 Alternatif Para Tercih Edilmesinin Nedenleri

Alternatif paralara talebi oluşturan birçok sosyo ekonomik güç vardır:

- **Yerelcilik**

Yerelcilik, ticaret birliklerini teşvik ederek, tüketimi, yeni iş olanaklarının sağlanması ve çalışma koşullarının iyileştirilmesi için belirli bir coğrafi bölgede veya bir bağımsız pazarlamacı grubu içinde tutmaktadır.

- **Teknoloji**

Gelişmiş yazılımlarla kullanımı çok daha kolaylaşmıştır ve pazara giriş engellerinin düşük olması ağ etkisine katkı sağlamaktadır.

- **Siyasi Ekonomi**

Bankacıların ve CEO'ların aldığı yüksek ödemelerin ortaya çıkarılması ve geleneksel bankalarla ilgili "başarısız olamayacak kadar büyük oldukları" düşüncesinin

yıkılmasına sebep olan olaylar yaşanmıştır. Aşırı borçlanma ve parasal genişleme ile oluşan ekonomik belirsizlik huzusuzluk yaratmıştır.

- **Çevrecilik**

Ekolojik kaygılar ve petrol ve benzeri doğal kaynakların çıkarılmasında sınıra gelinip gelinmediği ile ilgili sorular bulunmaktadır.

- **Verimsizlikler**

Finansal hizmetlerin olduklarından daha fazla fiyatlandırılmaları ve tüm finansal sistemin çok pahalı olmasıdır.

- **Finansal Özgürlük**

Kripto para gibi bazı dijital paralar kontrolün zayıf olduğu Internet üzerinden gönderilebilme avantajına sahiptir. Bu dijital paralar, kullanıcılarının, sermaye kontrollerini geçebilmelerini ve bir dolaşımdaki para krizinde onlara güvenli bir liman sağlamaktadır.

- **Spekülasyon**

Kripto para gibi bazı dijital para alıcıları, daha geniş kabul gördükten sonra, fiyatının değerleneceği yönünde beklenti taşımaktadır.

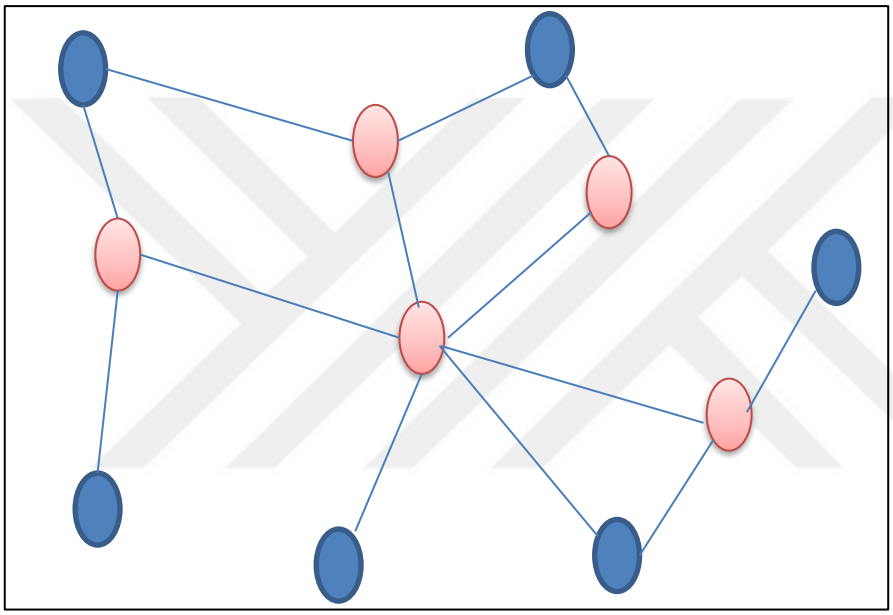
Bugün hiçbir bedel ödemeden alternatif para olarak bir kripto para yapmak kolaydır. Ancak bu yeni oluşumların çoğu nispeten kısa zaman içinde dolaşımdan kaybolmaktadır. Rekabet halindeki alternatif paralardan sadece birazı dünyaca kabul görmekte, yeterli hacme ulaşmakta veya uygun bir pazar bulamaktadır. Ulusal dijital para fikri başarılı olmazsa, büyük olasılıkla bu alternatif paraların çoğu, teknolojide yerini alacak gelişmeler, daha sıkı düzenlemeler ve yetersiz talep nedeniyle dolaşımdan silinecektir.

1.4. Kripto Para

Kripto paralar, bilgisayar bilimi (P2P ağ iletişimi), şifreleme bilimi (kriptografik özet fonksiyonlar, dijital imzalar) ve ekonomi (oyun teorisi) gibi çeşitli öğretilerdeki çok

yönlü başarıların bir kombinasyonu sonucu oluşmuştur. Kısaca bir kripto para genellikle eşten eşe bir ağ, ortak bir karar mekanizması, açık anahtar altyapısından (PKI) oluşan belirli bir kripto para sisteminde varolan dijital bir simgesel paradır[21]. Sistemi idare eden merkezi bir yönetim yoktur. Bunun yerine sistemi yöneten (bir işlemin geçerli olması için ne olması gerektiği, dijital para arzı ve bunun oluşturulma düzeninin belirlenmesi gibi) kurallar, ağdaki tüm katılımcılar (aynı zamanda bağlantı noktası (nodes[22]) olarak da adlandırılır) tarafından uygulanmaktadır.

Tablo 1. Bağlantı Noktaları (Nodes)



Kaynak: Caleb Meredith, "Explaining GraphQL Connections", s.1

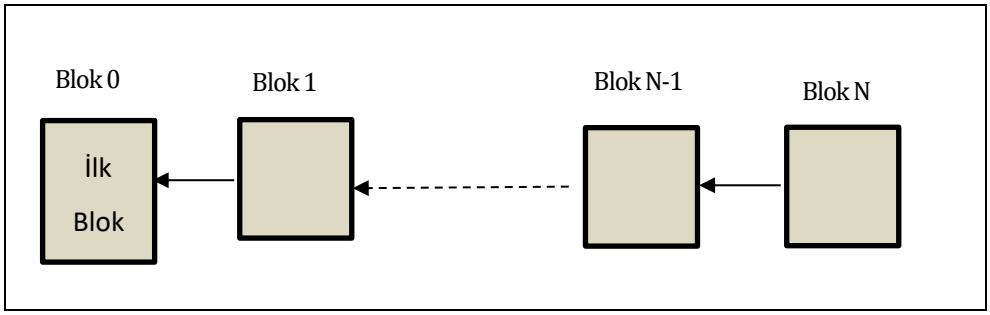
Herkeste paylaşılan kayıt defterinin bir kopyası olduğu için yapılan tüm işlemler birbirlerinden bağımsız olarak her bir bağlantı noktası tarafından doğrulanabilmektedir. Genellikle, doğrulanarak kaydedilen işlemlerden oluşan bir bloklar zinciri ('kayıt zinciri') şeklini alarak paylaşılan bu kayıt defteri, sürekli olarak, adına 'madencilik' denilen yeni sembolik para (örneğin kripto para) birimlerinin oluşturulduğu bir süreç

[21] Garrick Hileman ve Michel Rauchs, "Global Cryptocurrency Benchmarking Study", University of Cambridge, 2017, s. 151. (Erişim Tarihi: 14.06.2018) https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[22] Caleb Meredith, "Explaining GraphQL Connections", 23.02.2017, (Çevrimiçi) https://blog.apollographql.com/explaining-graphql-connections-c48b7c3d6976 (Erişim Tarihi: 15.06.2018)

yoluyla güncellenmektedir. Kayıt zincirini büyük bir muhasebe defteri gibi düşünebilir. Her bir bloksa bu defterin bir sayfasıdır[23].

Tablo 2. Bloklar



Kaynak: Jan Moller, "How The Bitcoin Protocol Actually Works", s.10

Herkes katılmakta serbesttir ve sistemden dilediği zaman ayrılabilmektedir. Kullanıcılara verilmiş kimlikler yoktur.

1.4.1 Kripto Paranın Yapısı ve Özellikleri

Kripto para en saf hali ile elektonik paranın eşten eşe olan halidir. Herhangi bir finansal aracı kuruluş katılımı olmadan çevirimiçi ödemelerin bir taraftan diğerine doğrudan gönderilebilmesini sağlar. Ağ, işlemleri kriptografik "iş ispatı" ile zamansal olarak etiketler. Bitcoin iş ispatı protokolü temel olarak bir şifre çözme yarışması ve katılımcıları ödüllendirmek için teşviktir. Bitcoin için, şifreyi ilk çözen yeni oluşturulan para ile ödüllendirilir. Bu yarışma, işlemlerin, "iş ispatını yeniden yapmadan" değiştirilemeyecek bir kaydını oluşturmaktadır.

Kripto para dijital paranın bir alt sınıfıdır. Havayollarınca verilen mil puanlar, bilgisayar oyunlarındaki simgesel oyun paraları, bahis sitelerinin verdiği puanlar, Londra'daki Brixton bölgesinde kullanılan Brixton Pound'u ve daha birçoğu, kapalı bir sistemde sanal ve gerçek eşyalar ve açık sistemde ise dolaşımdaki para ile takas edilebilen dijital paraya örnektir.

[23] Jan Moller, "How The Bitcoin Protocol Actually Works, International Software Development Conference, GOTO, Copenhagen, 23-24 Eylül 2014, s. 10.

Uygulanabilir dağıtık sistemli bir kripto paranın en temel özelliği simgesel parasının kısıtlanmaya dirençli bir dijital "hamiline" varlık sağlamasıdır[24] (Tablo 3). Kendi özel anahtarını elinde bulunduran kişinin o anahtarın uyumlu olduğu genel anahtara ilişiklendirilmiş belirli miktardaki kripto parayı idare etmesi bakımından hamiline varlıktır. Teoride kimsenin kripto para fonlarını bloke edememesi, haczedememesi ya da tümleştirilmiş ödeme ağında gerçekleştirilen işlemleri kısıtlayamaması bakımından kısıtlanmaya dirençlidir.

Tablo 3. Kripto Paraların Temel Özellikleri

Özellik	**Tanımı**
Dijital 'hamiline yazılı' varlık	Özel anahtarı elinde bulunduran kullanıcı hem spekülatif varlık hem de değişim aracı olarak kullanılabilen kripto paranın sahibidir. Fonlara el konulamaz ve işlemler kısıtlanamaz.
Tümleşik ödeme ağı	Genelde, hızlı, ucuz, küresel ve geri alınamayan ödemeler sağlar
Parasal olmayan kullanım şekilleri (Use case)	Para veya varlığın dışında kullanım şekilleri de sağlar. Bu kullanım şekillerini, dağıtık, merkezi bir otorite olmadan kısıtlamaya dirençli bir şekilde sağlar.

Kaynak: Global Cryptocurrency Benchmarking Study ,2017, s.106

Kripto para sistemleri belirli bir bölge veya idareye bağlı olmadığı için tümleştirilmiş ödeme ağının küresel erişimi bulunmaktadır ve bu özellik fonların dünyanın her yerinden kısa sürede (pek çok faktöre bağlı olarak değişen belirli bir saniye veya dakika içinde) transferine olanak sağlamaktadır[25]. İşlem ücretleri, genel itibariyle, geleneksel ödeme sistem sağlayıcılarının aldığı ücretlerden çok daha düşüktür. Ücretler trasfer edilen tutara göre değil işlemin bayt olarak ölçülen

[24] Garrick Hileman ve Michel Rauchs, "Global Cryptocurrency Benchmarking Study", University of Cambridge, 2017, s. 106. (Erişim Tarihi: 14.06.2018)
[25] https://coin.dance/stats/marketcaphistorical

büyüklüğüne göre belirlenir. Yani çok milyon dolarlık bir işlem 1 $'lık başka bir işlemdeki aynı masrafla yapılabilir. Bunun sonucu olarak kripto para sistemleri uygun maliyetle mikro ödemeler için kullanılabilir. Ödemeler fonların transferinden ve ağ tarafından onaylandıktan sonra geri alınamaz. Bu durum düşük masraflardan kar sağlayan ve iadelerden kaçınan ticari işletmelere büyük avantajlar sağlamaktadır. Ayrıca kullanıcılar sadece genel anahtardan oluşan kripto para adreslerinden belirlendiği için iletişim, kredi kartı numarası ve şifresi gibi kişisel bilgilerin, sağlam olmayan güvenlik ihlallerine açık sunuculardaki saklanmasına gerek kalmamaktadır.

Son olarak, bazı kripto para sistemlerinin dijital varlık ve paranın ötesinde parasal olmayan kullanım şekillerini sağlayan ilave özellikleri ve işlevsellikleri vardır[26]. Örneğin Bitcoin, 'özetler' (hashes) halinde belirli üstveriyi bitcoin ağı dışında özel anlamı olan işlemlere gömme yoluyla değiştirilemez bir veri deposu olarak ve merkezi olmayan bir zamansal etiketleme hizmeti olarak kullanılabilir. Bu mekanizma ana ağ üzerine yapılandırılan ve farklı işlevselliği ve kendi parası veya kripto parası gibi kullanım şekilleri olan 'bindirmeli ağ sistemleri (overlay networks) veya 'gömülü uzlaşı sistemlerinin oluşturulmasını sağlar (Dapp, dApp veya DApp). Bazı kripto para sistemleri de aynı zamanda sadece parasal olmayan kullanım şekilleri sağlamak amacıyla geliştirilmiştir (örneğin merkezi olmayan alan adı (domain name) kaydı, merkezi olmayan arama motoru, merkezi olmayan bilgisayar platformu gibi). Bu sistemler temel olarak kripto parayı, katılımcıları teşvik ederek, sistemin işlemeye devam etmesi için kullanmaktadırlar[27].

1.4.2 Başlangıç: eCash

Ticari olarak, herşey "DigiCash, Inc." adlı firmanın eCash sistemi ile 1990 yılında başlamıştır. Bu sistem, dayanağını kurucusu olan David Chaum'un iki makalesinden alır. İlki 1981 yılında Berkeley Üniversitesinde Bilgisayar Bilimleri profesörüyken yayınladığı "İzi sürülemeyen elektronik posta, iade adresler ve Dijital Rumuzlar (Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms)" adlı

[26] Garrick Hileman ve Michel Rauchs, "Global Cryptocurrency Benchmarking Study", University of Cambridge, 2017, s. 151. (Erişim Tarihi: 14.06.2018) https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[27] a.g.e., s.98

makalesidir. İnternet üzerinden şifreli iletişim kurma araştırmalarına temel olan bu makale sonrasında Tor gibi kişisel verilerin saklanması teknolojilerini (privacy-preserving technologies) içeren uygulamaların yolu açılmıştır. Ancak Chaum'un asıl hedefi "kişisel verileri saklı dijital para" (privacy-preserving digital Money) projesiydi. Buna yönelik 1982 yılında yayınladığı "İzi Sürülemeyen Ödemelerde Kör İmzalar" (Blind Signatures for Untraceable Payments) makalesi kör imzaları açıklamış ve güvenli dijital para kavramını ortaya çıkarmıştır.

Chaum'un dijital para sisteminin temelinde "kör imzalar" kavramı yatmaktadır. Kör imza kavramını anlayabilmek için açık anahtarlı şifrelemenin nasıl işlediğini ve şifreli imzanın ne olduğunu bilmek gerekmektedir. Açık anahtarlı şifreleme anahtar çiftlerini kullanır: açık anahtar ve özel anahtar. Görünürde rastlantısal sayılardan oluşan açık anahtar, matematiksel olarak, tamamen rastlantısal sayılardan oluşan özel anahtardan elde edilir. Özel anahtardan deneme yoluyla açık anahtara ulaşılabilir. Ancak sadece açık anahtarla özel anahtarı bulmak pratikte imkansızdır (tek yönlü yol).

Açık anahtar şifrelemesi iki kişi arasında özel iletişim kurma amaçlı kullanılabilir. Örnek vermek gerekirse (akademik çevrelerde verilen adlarıyla) Alice ve Bob açık anahtarlarını sadece birbirleriyle paylaşmakta ve sadece kendilerinin bildiği özel anahtarları bulunmaktadır[28]. Ancak Alice ve Bob genel anahtarları sayesinde özel olarak iletişim kurma haricinde kendilerine özel imza da oluşturabilmektedir. Alice (ve aynı zamanda Bob) herhangi bir veriyi şifreli olarak imzalayabilir. Bunu yapabilmek için Alice matematiksel olarak özel şifresini bu veri ile birleştirir. Sonuç "imza" olarak adlandırılan bir başka görünürde rastlantısal sayı dizisi olacaktır. Yine burada da Alice'in özel şifresine (veri olsun veya olmasın) imzasından ulaşmak imkansızdır (tek yönlü yol). Bu imzanın ilgi çeken kısmı Bob'un (veya herhangi biri) imzayı, Alice'in açık şifresi ile kontrol edebilmesidir. Alice'in açık şifresi, Bob'a, kendi özel şifresi ile (veriyi de ekleyerek) imzayı oluşturanın Alice olduğunu ispatlar. Bu tıpkı el yazısı ile atılan imzada olduğu gibi Alice'in veri içeriğini kabul ettiği anlamına gelmektedir Bob için.

[28] Aaron van Wirdum" The Genesis Files: How David Chaum's eCash Spawned a Cypherpunk Dream" , 24 Nisan 2018 (Çevrimiçi), https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream/ , par. 12.

Kör imza, şifrelenmiş imzanın bir adım daha ilerisidir. Bu defa Bob, adına "tek seferlik anahtar (nonce)" denilen rastlantısal bir sayı oluşturmakta ve bunu matematiksel olarak bir veri ile birleştirmektedir[29]. Karıştırılan bu veri böylelikle başka bir rastlantısal sayılar dizisi gibi görünür. Bob karıştırılmış veriyi Alice'e imzalaması için verebilir. Alice asıl verinin ne olduğunu bilemez, göremeden imzaladığı için de sonuç kör bir imzadır.

Kör imzada ilginç olan, bu imza sadece Alice'in anahtarlarına (aynı şifreli imzada olduğu gibi) ve karıştırılmış veriye bağlantılı değildir. Aynı kör imza aynı zamanda karıştırılmamış asıl veriyle de bağlantılıdır. Sadece Alice'in açık anahtarıyla, herkes Alice'in asıl verinin karıştırılmış halini imzaladığını ispat edebilir. İşte bu kör imza, Chaum'un bir dijital para sistemini oluştururken kullandığı şablondur.

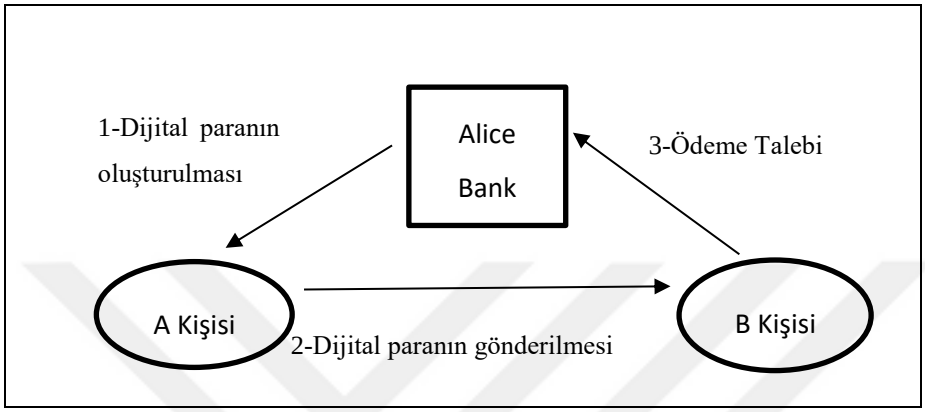
Bunu anlayabilmek için yukarıdaki örneklerde bahsi geçen Alice'in aslında bir banka olduğunu varsayılabilir[30]: Alice Bankası. Bu aynı günümüz bankaları gibi müşterilerinin paralarını yatırdıkları vadeli veya vadesiz hesaplarının olduğu normal bir bankadır. Diyelim ki Alice Bank'ın dört müşterisi var: Bob, Carol, Dan ve Erin. Bob'ın Carol'dan bir şey satın almak istemektedir.

İlk olarak, Bob Alice Bankası'ndan parasını çekmeyi ister. Bu parayı çekebilmek için Bob kendisi "dijital banknot" oluşturur: benzersiz sayılar şeklinde "seri numaralar". Bunun üstünde bu banknotları yukarıdaki paragraflarda anlatıldığı şekilde karıştırır ve Alice Bankası'na gönderir. Bob'tan karıştırılmış banknotları alan Alice Bankası, her bir karıştırılmış banknotu kör imzalar ve Bob'a geri gönderir. İmzaladığı karıştırılmış her bir banknot için Alice Bankası Bob'ın hesabından bir dolar düşer. Şimdi, Alice Bankası karıştırılmış banknotları kör imzaladığı için imzası aynı zamanda karıştırılmamış asıl banknotlarla da bağlantılıdır. Böylece Bob, sadece, asıl, karıştırılmamış banknotları Carol'a göndererek ödemesini yapabilir. Carol banknotları aldıkça bunları Alice Bankasına gönderir. Alice Bankası kendi özel imzasını içerdiği için her bir banknotu kör imzaladığını ispat eder. Alice Bank aynı zamanda çifte harcama olmadığından emin olmak için banknotlardaki seri numaralarından bu

[29] Aaron van Wirdum" The Genesis Files: How David Chaum's eCash Spawned a Cypherpunk Dream" , 24 Nisan 2018 (Çevrimiçi), https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream/ , par. 15.
[30] a.g.e., par. 18.

banknotların başka birisi tarafından daha önceden yatırılmadığını da ispat eder. Banknotları bozdukça Alice Bank karşılığı olan tutarı Carol'ın hesabına geçer ve Carol'ı bilgilendirir. Bu onaya istinaden Carol Bob tarafından geçerli banknotla ödeme yapıldığını anlar ve ona satın almayı istediği şeyi gönderir.

Tablo 4. Dijital Ödeme Örneği



Kaynak: Aaron van Wirdum, "The Genesis Files", s.1

Bu işlemde en önemli husus, Alice Bankasının karıştırılmamış banknotları ilk kez Carol onları yatırdığında görecek olmasıdır. Böylelikle Alice Bankası'nın bu banknotların Bob'a ait olduğunu bilmesine olanak bulunmamaktadır. Bu banknotların Dan veya Erin'den de gelme olasılığı da bulunmaktadır.

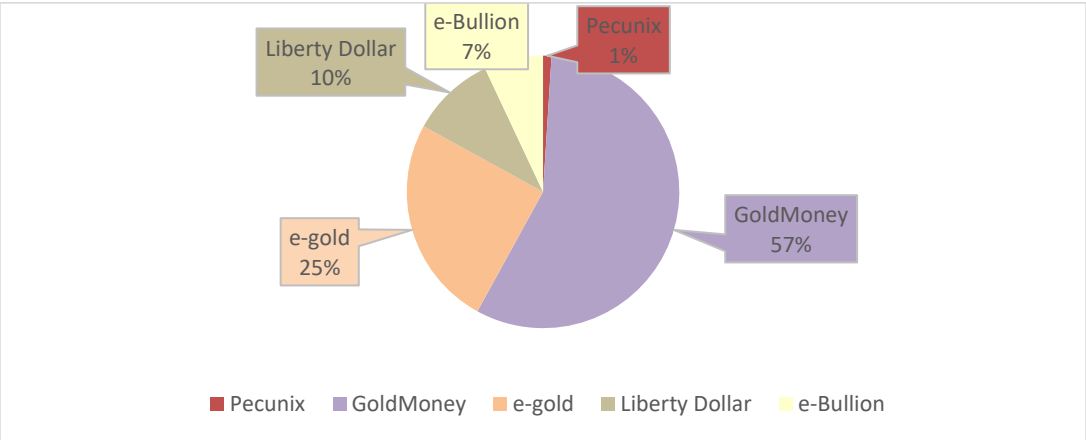
Chaum'un çözümü ödemelerde kişisel verilerin dijital olarak saklanmasını önermektedir. Ödemeler hem çevirim içi hem de çevirim dışı olarak çifte harcamayı önlemek için şifreleme protokolleriyle yapılmaktadır. Şifreleme protokolleri kullanıcılarının kişisel verilerini korumak için kör imzaları kullanmaktadır.

İlk kripto para olan eCash sistemi Amerika ve Finlandiya gibi birçok ülkedeki bankalar ve akıllı kartlar vasıtasıyla kullanılabilmiştir. Son yirmi yılda yazılımcıların yaptığı birçok geliştirmelerle yavaş yavaş kripto paranın bügünkü haline dönüşmüştür.

Önce "DigiCash, Inc." sonrasında "eCash Technologies" firmalarının sahip olduğu eCash merkezi bir sistemdi. Ancak InfoSpace tarafından 1999 yılında satın alındıktan sonra eCash ve kripto para arka planda kalmıştır.

1.4.3 Dijital Altınla Internet Ödemelerinin Başlaması

Dijital altın para 1999 ile 2000'li yılların başlarında ilgi görmeye başlamıştır. Onsluk altınlara dayanan elektronik paranın bu yeni türü külçeler halinde saklanmakta ve depo masrafları sahiplerine yansıtılmaktadır. Bu hesaplardaki altınlar bir anlamda para gibi olup, birimleri ons vb. şeklindedir[31]. Bu dönem firmalarına örnek e-dinar, Pecunix, iGolder, Liberty Reserve, gBullion, e-gold ve eCache gösterilebilir. Türkiye'de de elektronik altın paralar bankalar ve Gramaltın gibi firmaların internet tabanlı satış siteleri aracılığıyla yatırımcıların hizmetine sunulmuştur (TSPB[32], 2010).



Şekil 1. Dolaşımdaki Değerine Göre 2005 yılı Dijital Altın Pazar Payı
Kaynak: Dijital Gold Industry Overview, 2006, s.12

Dijital altın para, bir mevduat veya menkul kıymet hesabındaki altını temsil ettiği için temsili bir para şeklidir. Bu tedarikçiye bağlı değişir. Örneğin çoğu tedarikçi dijital para yükümlülüğünü fiziksel altın olarak mevduat hesabındaki altınla yerine getirmektedir. Tıpkı döviz kurlarının birbirleri arasında dalgalanmaları gibi dijital paralar da o kurdaki altın fiyatına göre döviz kurlarına karşı dalgalanırlar. Bu durum, yabancı para hesabı bulunan kişinin kur riski taşıması gibi altın hesabı sahibi herkes için kur riski yaratmaktadır. Bazı digital para sahipleri günlük parasal işlemlerini, çoğu gelir ve harcamaları yaşadıkları ülke parası üzerinden olmasına rağmen, dijital para ile

[31] Jim Davidson, "Dijital Gold Industry Overview", 2006, (Çevrimiçi) www.freemarketmoney.org, (Erişim Tarihi: 25.06.2018), s.12
[32] Gökben Altaş, "Altın Piyasaları", Sermaye piyasasında Gündem Dergisi, TSPAKB, Sayı 91 Mart 2010, ISSN 1304-8155, s. 14.

yapmaktadır. Dolayısıyla altın fiyatı, ülke parasına göre dalgalandıkça, dijital para hesaplarının değeri de ülke parasına göre değişmektedir.

Tablo 5. 1996/2018 Yılları Arası Dijital Altın Para Tedarikçileri

Dijital Para	Piyasa çıkış tarihi	Piyasadan kaldırıldığı tarih	Finansal piyasada düzenlenmiş	Dijital para borsasında kabul	Elektronik transfer	İşlem Ücreti
e-dinar	2000		Hayır	Evet	Evet	%1 (en çok 0.015 dinar altın)
Pecunix	2002	2015	Hayır	Evet	Hayır	%0.15- 0.50 (en az 0.0001 – en çok 3.0 gr altın)
iGolder	2005	2013	Hayır	Hayır	Evet	%1
Liberty Reserve	2004	2013	Hayır	Hayır	Hayır	%1
e-gold	1996	2008	Hayır	Evet	Hayır	Miktara Bağlı
GBI	2014		Hayır	Evet	Evet	30bit/Ripple
AUG	2015		Evet	Evet	Hayır	Miktara Bağlı
GoldMoney BitGold	2015		Evet	Evet	Evet	%0,5 bireysel işlemler/ %1 kurumlar

Kaynak: CoinMarketCap; Instant Exchange, E-DINARCOIN; Bloomberg, GBI

Birkaç istisna haricinde çoğu yasal uyum veya düzenle ihlali gibi sebeplerle dolaşımdan kaldırılmıştır. (Tablo 5)

e-Gold internet ödemelerinde öncü olmuştur. İlk başarılı çevirimiçi mikro ödeme sistemi olarak, daha sonra çevirimiçi diğer uygulamalarda da yaygın olarak kullanılan e-ticarette birçok yeni teknik ve yönteme öncülük etmiştir. Bu teknikler ve yöntemler, ödemeleri güvenli giriş katmanı (SSL) şifreli bağlantısı üzerinden yapmak ve diğer internet sitelerinin e-gold işlem sistemini kullanarak hizmet verebilmelerini sağlamak için uygulama programlama arayüzü (API) sunmaktır. Ancak "müşterini tanı (KYC)" ve "şüpheli işlem bildirimi (SAR)" yükümlülüklerine uymamak zayıf noktası olmuştur. Amerika'da 11 Eylül 2001 terör saldırılarının sonucu en önemli güvenlik tedbirlerinden biri olan Vatanseverlik Yasası'na (US Patriot Act) uyum, para gönderimine aracılık eden firmalar için en önemli konudur. İnternet dolandırıcılıkları ve bilgisayar korsanlarıyla da bir yandan mücadele etmiştir. 2008 yılında "mal varlığına el koyma

(asset forfeiture law)" yasasına istinaden tüm altın rezervlerinin paraya çevrilip el konulmasından önce e-gold değeri yılda 2 milyar doları aşan değerli maden işlemleri yapmıştır[33].

1.4.4 Kripto Paranın Geri Dönüşü

2008 küresel finansal krizin başlangıcıyla kripto paraya ilgi geri gelmiştir. Küresel krizin hemen başlarında bir blog yazısında[34] Szabo, kripto paranın itibari para sisteminden kaynaklanan bazı sorunların üstesinden gelebilme potansiyeli olduğunu savunmuştur. Malları kullanarak sözleşme yapmak ağır ve külfetli olduğundan "bit gold" kavramı öne sürülmüştür. Adından da anlaşılacağı üzere çıkarılacak bir altın ve dijital bir kayıtta oluşturulan bit bulunmaktadır. Dijital kayıt güvenilir bir üçüncü taraf sorunlarını çözebilmektedir. Bit gold başlıklı blog yazısında kendi sözleriyle şöyle açıklamıştır:

Böylece, güvenilir üçüncü taraflara en az bağımlılıkla, taklit edilemeyen veya sahtesi yapılamayan kıymetli bitlerin çevirimiçi oluşturulduğu ve yine benzeri az güvence ile güvenli bir şekilde depolandığı, gönderildiği ve ayarlandığı bir protokol yapılsaydı çok güzel olurdu. Bit gold.

Bit gold için önerim "istemci bulmacası fonksiyonu (CPP)", "iş ispatı fonksiyonu", "güvenli karşılatırmalı değerlendirme fonksiyonu (secure benchmark function)" olarak farklı isimlerle adlandırılan fonksiyonlar yardımıyla bir dizi kimlik sorgulayıcı bitler arasından bir bit serisi hesaplamaya dayanmaktadır. Elde edilen bit serisi iş ispatıdır (POW). Tek yönlü bir fonksiyonun tersine hesaplamasının yasaklayıcı bir şekilde zor olduğu yerde, hesaplama döngüleriyle ölçülen belirli bir değer karşılığı, bir güvenli karşılaştırmalı değerlendirme fonksiyonu kullanmak tersine hesaplamak için ideal olacaktır.

[33] Garrick Hileman ve Michel Rauchs, "Global Cryptocurrency Benchmarking Study", University of Cambridge, 2017, s. 106. (Erişim Tarihi: 14.06.2018) https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[34] Nick Szabo, "Bit gold", 27.12.2008, (Çevrimiçi) http://unenumerated.blogspot.com/2005/12/bit-gold.html, (Erişim Tarihi: 25.06.2018).

Bu teknik ifade şekline karşın, Szabo'nun anlatmaya çalıştığı dijital altını veya bit gold'u çıkarmak için kaynakları harcayan, ödüllendirilen ve bu süreç içinde herkese açık dijital kaydı onaylayan katılımcılar gerektiren basit bir protokoldür. Yaklaşımını geçmişte başarısız olan dijital paralardan farklı kılan finansal krizin yaşandığı dönemde çıkmış olması ve protokolün dağıtıklık özelliğiydi. Madencilere verilen ödül kavramı bir yeniliktir ve kullanıcıların dijital kayda erişim hakkının serbest olması ise diğer bir yeni buluştur. Bunlara ihtiyaç duyulmasının sebeplerinden biri internetin yapısı zorunlu ücretlerin toplanmasını daha zorlaştırırken gönüllü katılımı daha kolaylaştırıyor olmasıdır. Bu nedenle, içeriğe veya dijital kayda erişime hiçbir engel olmamalı, kullanım kolaylığı ve isteğe bağlı ödemeler olmalıdır.

Eski ve yeni birçok kriptografi bilimcisi tarafından literatürde fikirler tartışılmış ve teknolojisi zamanla geliştirilmiştir. Bu grup, DigiCash ile Chaum[35] (1983), Hashcash ile Back[36] (1997), b-money ile Dai[37] (1998), para kavramı üzerine Szabo[38] (1999, 2002, 2008) ve eşten eşe ağlarla ilgili çalışmasıyla Shirky[39] (2000) gibi kriptografi bilimcilerinden oluşmaktadır. Cypherpunk, 1980'li yılların başlarından bu yana sosyal ve politik değişimlerin yolunun güçlü şifreleme biliminin yaygın kullanımı olduğunu savunan eylemci bir gruptur[40]. Bir cypherpunk üyesi olarak iki kaynağı belirsiz remailer[41] programı çalıştıran Finney[42], ilk tekrar kullanılabilen iş ispatını (RPOW)

---

[35] Burton Rosenberg, Handbook of Financial Cryptography and Security, ISBN-13: 978-1-4200-5982-3 (Ebook-PDF), 2011, s. 14.
[36] Adam Back, Hashcash - A Denial of Service Counter-Measure, 2002, (Çevrimiçi) http://www.hashcash.org/papers/hashcash.pdf (Erişim Tarihi: 25.07.2018).
[37] Wei Dai, "B-Money", 1998, (Çevrimiçi) http://www.weidai.com/bmoney.txt, (Erişim Tarihi: 25.07.2018), Appendix A
[38] Nick Szabo, "Bit gold", 27.12.2008, (Çevrimiçi) http://unenumerated.blogspot.com/2005/12/bit-gold.html, (Erişim Tarihi: 25.06.2018).
*Nick Szabo, "Micropayments and Mental Transaction Costs", 1999, (Çevrimiçi) https://nakamotoinstitute.org/static/docs/micropayments-and-mental-transaction-costs.pdf, (Erişim Tarihi: 25.06.2018).
*Nick Szabo, "Intrapolynomial Cryptography", 1999, (Çevrimiçi) https://nakamotoinstitute.org/intrapolynomial-cryptography/#selection-7.7-7.35, (Erişim Tarihi: 25.06.2018).
*Nick Szabo, "Shelling Out: The Origins of Money", 2002, (Çevrimiçi) https://nakamotoinstitute.org/shelling-out/, (Erişim Tarihi: 25.06.2018).
[39] Clay Shirky vd., 2001 P2P Networking Overview: The Emergent P2P Platform of Presence, Identity, and Edge Resources, "O'Reilly Media, Inc.", 2001.

[40] David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015, s. 20
[41] Sameer Parekh, "Prospects for remailers: where is anonymity heading on the internet?", First Monday, Sayı 1, 5 Ağustos, 1996., (Çevrimiçi) http://ojphi.org/ojs/index.php/fm/issue/view/71, (Erişim Tarihi: 25.06.2018), s.2.

oluşturmuştur. RPOW, hizmet engelleme (DOS) saldırılarını ve bilgisayar ağına hizmet istemcisinin belirli bir işi yapmasını talep ederek gönderilen elektonik postalar gibi diğer hizmet ihlallerini tespit etmek için kullanılan ekonomik bir ölçüdür. Bunun anlamı bilgiyi isteyen kişinin bilgisayarda, sağlayan kişiden, daha fazla işlem zamanına maruz kalması gerektiğidir. Bitcoin tarafından kullanılan Hashcash, istenmeyen elektronik postaları ve hizmet engelleme saldırılarını kısıtlamak için tasarlanan bir iş ispatı sistemidir[43].

Aynı dönem kripto paraya olan sosyopolitik ilgi artmıştır. Altın standartı sisteminde, paranın karşılığı altındır. 5 gram altın, 10 gram altın gibi. 1. Dünya Savaşı'ndan önce 1 ons altın 20,67 dolar olarak kaydedilmitir. Gümüş standartı da benzer bir mantıkla işlemektedir. İngiliz para birimi sterlinin özgün anlamı 1 poundluk som gümüştür. Altın standartı sisteminde bankalar ve benzeri ticari kuruluşlar kağıt para veya vadesiz hesap karşılığı altınları saklamaktadır. Bunlar ilgili kuruluşlara ibraz edildiğinde karşılığı altın temin edilmektedir. Geçmişe bakıldığında altına dayanan paraların alım gücünün hemen hemen sabit olduğu görülmektedir. Bunun aksine, paranın altın veya başka bir değerli maden tarafından desteklenmediği bugünkü itibari para sisteminde bir değer garantisi yoktur. Herhangi bir bankaya Amerikan Merkez Bankası'nın bastığı 20 doları ibraz ettiğinizde talep edilen yine merkez bankasının piyasaya sürdüğü başka paradır. İtibari para sisteminin getirdiği olumsuzluklardan biri enflasyondur. Bugünkü itibari para sisteminde paranın ne miktarda arz edileceği kararı devletler ve merkez bankaları tarafından verilmektedir. Bu sistemde, çok fazla para basılmasına mâni olacak kendini kontrol eden bir piyasa mekanizması bulunmamaktadır[44]. 1971 yılında Altın standartı uygulamasının bırakılması ve itibari para sisteminin kullanılmaya başlanmasından bu yana kriz dönemlerinde merkez bankaları kendi insiyatifleriyle diledikleri miktarda para basmıştır. Bu varlık enflasyonu ortamı yaratmış ve gelir dengesini bozmuştur. Kripto para veya madenlerin arzı sınırlı olabilmekte veya olmayabilmekte ancak yenileri genellikle önceden belirlenmiş kuralla oluşturulmaktadır. Temel olarak parasal genişleme ve çok büyük miktarlardaki devlet borçlarından ötürü itibari para sistemine

[42] Hal Finney, " Reusable Proofs of Work", 2004, (Çevrimiçi) https://nakamotoinstitute.org/finney/rpow/index.html, (Erişim Tarihi: 25.06.2018).
[43] Adam Back, Hashcash - A Denial of Service Counter-Measure, 2002, (Çevrimiçi) http://www.hashcash.org/papers/hashcash.pdf (Erişim Tarihi: 25.07.2018).
[44] Lawrence H. White, "Is the Gold Standard Still the Gold Standard among Monetary Systems?", Cato Institute Briefing Papers, 2008, no.100.

olan güvenin azalması belirli bir arzı olan para ile poziyonlarını güvenceye almak (hedge) isteyen kişileri kripto paraya dikkat etmeye yöneltmiştir.

Kripto para, devleti mali disipline zorlayabilen bir paranın özelliklerine sahip ve sonlu arzı ile sabit büyüyen borçsuz bir para olarak öngörülmüştür. Ana portföylerinde sürekli negatif ilişki arayışındaki varlık yöneticileri için kripto para, negatif ilişkili alternatif varlık sınıfından olan Bitcoin ile portföy getirisini arttıran yüksek risk ve geleneksel olmayan varlık sınıfı (türev araçlar, özel sermaye, banka sendikasyon kredileri vb) için ümit ışığı olmuştur. Ancak Bitcoin köklerini 1992 yılında başlayan kripto anarşi hareketinden almaktadır[45]. Aşağıdaki paragraf bu hareketi başlatan May'in makalesinden alıntı bir paragraftır[46]:

Basım teknolojisi orta çağ loncalarının yetkilerini ve sosyal güç yapısını nasıl değiştirip azalttıysa, şifreleme bilimi metotları da aynı şekilde kurumların yapısını ve ekonomik işlemlerde devlet müdahalelerini temelde değiştirecektir. Gelişmekte olan bilgi pazarları ile kripto anarşi, kelimelerle ve resimlerle ifade edilebilecek her türlü malzeme için likit bir piyasa oluşturacaktır. Ve nasıl görünüşte çok küçük bir icat olan dikenli tel örgü uçsuz bucaksız tarlaların ve otlakların çitle ayrılmasını sağlayarak toprak ve mülk hakkı kavramlarını batı sınırında toptan değiştirdiyse, yine aynı şekilde matematiğin gizli bir dalının görünüşte küçük bu buluşu da fikri mülkiyetin etrafındaki tel örgüyü kesen makas olacaktır (May 1992).

Kripto paranın güvenilir liman ve alternatif varlık sınıfı olarak kullanımı, 2013'te Güney Kıbrıs'ta yaşanan menkul kıymet kaynaklı banka krizi nedeniyle 100 bin euro altındaki mevduatlardan yüzde 6,75 ve 100 bin euro üzerindeki mevduatlardan ise yüzde 9,9 oranında kesintiye gidildiğinde görülmüştür. Geleneksel bankacılığa güveni sarsılan yatırımcılar daha istikrarlı bir alternatif sunmak için ağırlıklı olarak en iyi bilinen kripto para bitcoin'i tavsiye etmiştir. Çoğu yatırımcı itibari paralarını (ve böylece fiyatı ve hacmini hızla arttırarak) kripto paraya çevirmiştir. Bitcoin'in fiyatı bir hafta içerisinde %57 artarak 74 dolara ulaşmıştır. Altın ve benzeri diğer mallar gibi Bitcoin'in fiyatı belirsizlik zamanlarında fırlamaktadır. Her iki varlık da alternatif

[45] David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015, s. 20
[46] Timothy C. May, "The Crypto Anarchist Manifesto", 22.11.1992, (çevirimiçi) https://www.activism.net/cypherpunk/crypto-anarchy.html, (erişim tarihi 21.05.2018).

yatırım işindeki küçük bir grup yönetici ve çağdaş para politikası makalelerinde çoğunlukla tercih edilmiştir. Bitcoin'e yönelik yapılan en bilinen eleştiriler: (i) merkez bankası gibi para basan merkezi bir otoritenin olmaması, (ii) sabit arzı ve tasarımından kaynaklanan deflasyonist yapısı (iii) fiyatının para olarak kullanımını sağlayabilecek derecede istikrarlı olup olamayacağı yönündeki şüpheler ve (iv) taşıdığı risktir.

1.5 Token

En genel tabiriyle token bir nesnenin "bağlı olduğu ekosistemdeki" temsilidir. Bu, bir değer, hisse, oy hakkı veya başka herhangi bir şey olabilir. Token tek bir rolle sınırlı değildir, bağlı olduğu ana ekosistemde pek çok rolü üstlenebilir. Kayıt zinciri tokeni, teknik veya başlangıç aşamasındaki bir kripto firmanın o teknoloji platformunun veya projenin ekosisteminin bir parçası olmak için çıkardığı bir değer birimidir. Tokenler kayıt zincirleriyle desteklenirler. Fiziksel varlıkları ilgili kayıt zincirinde kayıt girişi şeklindedir. Token, kripto para biriminden farklıdır. Bitcoin, Bitcoin Cash, Ethereum gibi bir kripto para birimi herhangi bir platformdan bağımsız olabilir. Bulundukları çevre dışında da para birimi olarak kullanılabilirler. Temelinde bilinen kripto paralar bunlardır. Ancak bir başka açıdan, sadece belli bir platformda bulunan, Ethereum platformundaki OmiseGO, Golem ve benzeri gibi örneklerse tokendir.

Tokenler, bitcoin ve altcinslerinden kullanıcıları tarafından çıkarılmamaları ve de (onları çıkaran firma kamuoyu gözünde değerli olmadığı sürece) borsada takas amaçlı kullanımamaları bakımından farklıdır. Bunun yerine Tokenler, yeni başlamakta olan bir firmanın teknoloji projesini finanse etmek için dolaşımdaki para veya kripto para karşılığı satılmaktadırlar.

1.5.1 Token Kullanımı

Genel itibari ile tokenler aşağıdaki durumlarda kullanılmaktadırlar:

- **Uygulama İçinde:**

Uygulama kullanıcıları tokenleri, kayıtzincirindeki mal ve hizmetleri ödemek için içsel para birimi olarak satın alırlar.

- **Finansman Amaçlı:**

Tokenler dolaşımdaki (veya fiziksel) parayı, likiditesi yüksek kripto para projlerine yatırım yapmak için kullanmaya olanak verir. Karlılık prensibine göre bu tokenler borç alınan tahvillere benzemektedir; finansal işlemler için araç olarak kullanılabilirken aynı zamanda belli bir süreden sonra sabit bir getiriyi de garanti etmektedir.

- **ICO (İlk Dijital Para Arzı):**

ICO kripto para projelerine finansman bulma yoludur. Tokenlerin çıkarılması, herhangi bir girişim projesine yatırım yapan herkese kardan pay alma veya ödeme sisteminde tedavülde olan tüm kripto para işlemlerinden ücret alma garantisi sağlar. Bilinen ilk halka arzların (IPO) aksine kayıt zinciri hisse senetlerinin sahipliği kişiye bir firmanın yönetim hakkını (özellikle belirtilmediği müddetçe) vermez.

ICO'lar yani ilk dijital para arzları temelinde kitle satışıdır yani kitle fonlamasının kripto para ile yapılanıdır ve aşağıdaki durumlarda kullanılmaktadır:

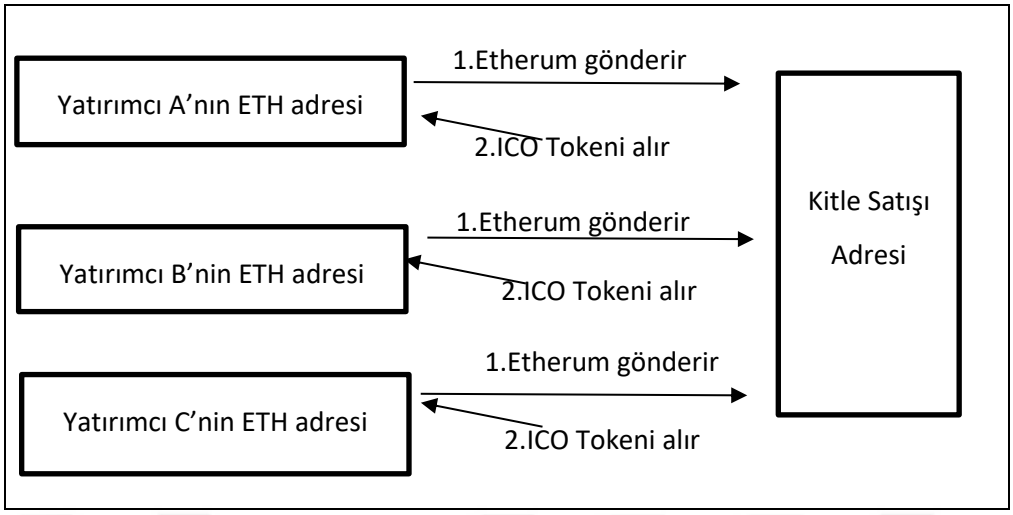
- Merkezi olmayan uygulama (DAPP) geliştiricilerinin projelerine ihtiyaç duydukları finansmanı bulmalarında
- Herhangi bir merkezi olmayan uygulamanın (DAPP) tokenini alan herkes hem projenin bir parçası olurlar hem de ilgilendikleri projeye yatırım yapmış olurlar.

1.5.2 ICO (İlk Dijital Para Arzı) Nasıl Yapılır?

İlk olarak, yazılımcı belirli bir miktar token çıkarır. Miktarın sınırlı olmasının sebebi tokenlerin kendi içinde bir değerinin olmasını sağlamak ve ilk dijital para arzına ulaşacağı bir hedef belirlemiş olmaktır. Tokenlerin fiyatı önceden belirlenmiş ve statik veya kitle satışına göre artarak ya da azalarak değişebilmektedir[47].

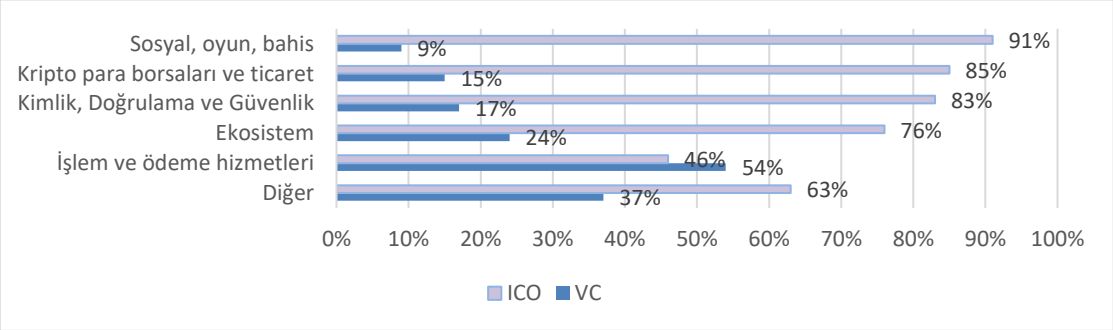
[47] Tokenomics—A Business Guide to Token Usage, Utility and Value, William Mougayar, 10.07.2017. (Çevirimiçi) https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416. erişim tarihi 11.09.2018

Tablo 6. ICO İşlem Örneği



Kaynak: bitsonblocks.net, 2018

Basit bir şekilde örneklemek gerekirse eğer biri token almak isterse kitle satışının yapıldığı adrese belirli bir miktar "ether" gönderir. Sözleşme, işlemin tamamlandığı bilgisini verdiğinde gönderilen ether karşılığı tokeni alırlar. Etherum yapısı merkezi olmadığı için iyi dağıtılmış ve büyük çoğunluğu sadece tek bir tarafça alınmamışsa ICO'nun başarılı olduğu düşünülmektedir.

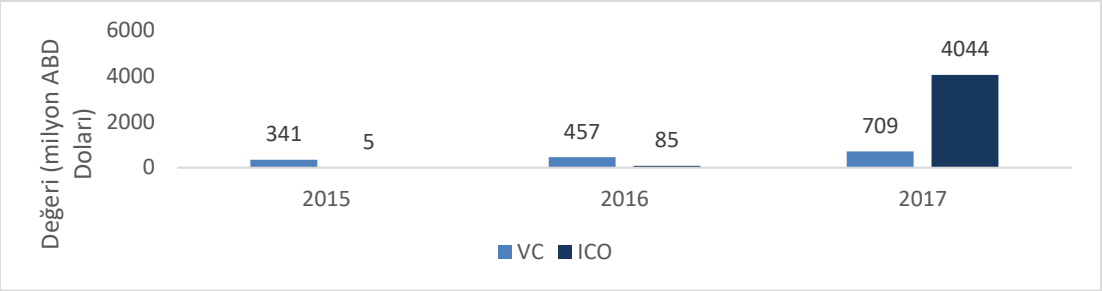


Şekil 2. Sektörel İlk dijital para arzı (ICO) ve risk sermayesi finansmanı (VC) Dağılımı, Dünya, Nisan 2018

Kaynak: Statistica, GP Bullhound; PitchBook, CoinMarketCap

GP Bullhound[48] tarafından toplanan Şekil 2 verilerine göre kripto para borsalarına ve ticaret sektörüne yapılan finansmanın %85'i 2015 ve 2017 yılları arasındaki ilk dijital para arzlarından tedarik edilmiştir.

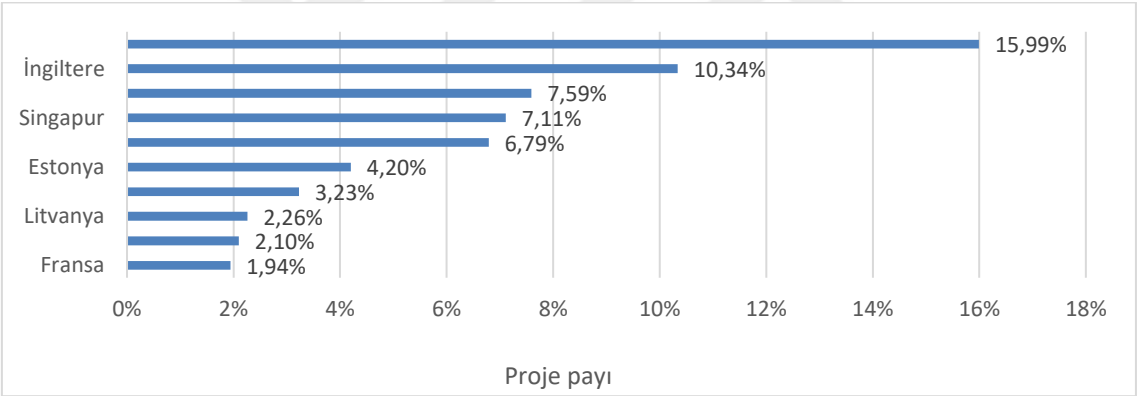
[48] GP Bullhound, VC Versus ICO Funding, (Çevirimiçi) https://www.statista.com/statistics/863868/vc-vs-ico-funding-by-category/, erişim tarihi 11.09.2018



Şekil 3. Dünyada ilk dijital para arzları ile risk sermayesi finansmanının 2015 ve 2017 yılları arasındaki karşılaştırılması

Kaynak: Statista 2018

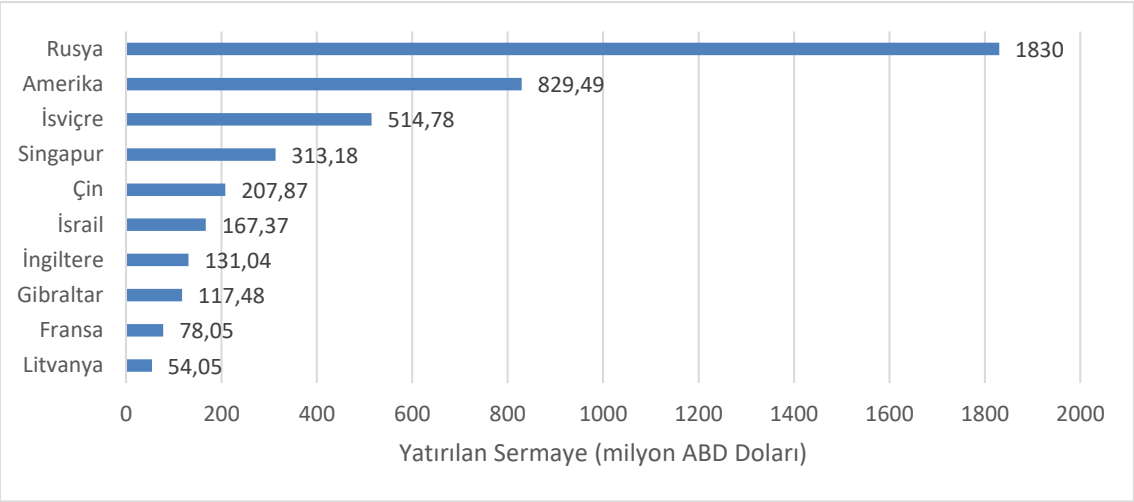
GP Bullhound tarafından toplanan yukarıdaki şekil verilerine göre ICO finansmanının değeri 2015 yılında 5 milyon ABD Dolarından 2017 yılında 4,04 milyar ABD Dolarına yükselmiştir.



Şekil 4. Dünyada kripto para ilk dijital para arzı (ICO) projelerinin payı, ülke bazlı, Temmuz 2018 itibari

Kaynak: Statista 2018

Yukarıdaki şekle göre Temmuz 2018 itibari, Kripto para ICO projelerinin %16'sı Amerika Birleşik Devletleri'nde gerçekleştirilmiştir.



Şekil 5. Dünyada Kripto para ilk dijital para arzı (ICO) projelerine yapılan yatırım miktarı, Temmuz 2018
Kaynak: Statista 2018

Yukarıdaki şekle göre Temmuz 2018 itibari kripto para proje yatırımlarının değeri Amerika Birleşik Devletleri'nde yaklaşık 829,5 milyon Doları'dır.

1.5.3 Token Değeri

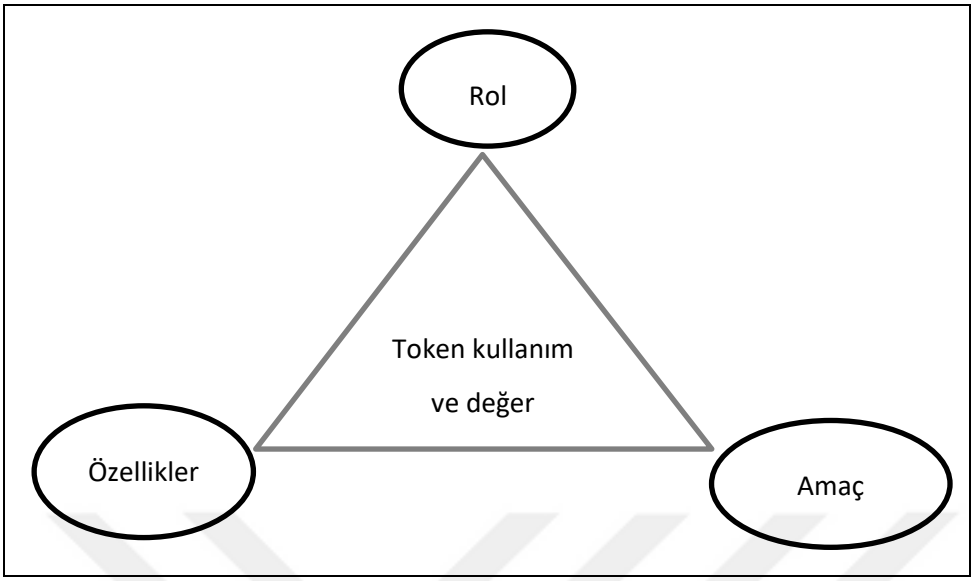
Tokenlerin finansal değeri günlük piyasa değerlerine yani nihai olarak kullanıcın proje olan güvenine bağlıdır. Genellikle kurulum aşamasında ICO'ya başlayan girişim firmalarının, tasarlanan iş ve takımlarından başka güvenceleri yoktur.

William Mougayar'a göre[49] token değerinin 3 temel unsuru vardır:

- Rol
- Özellikler
- Amaç

Bu üç unsur aşağıdaki üçgeni oluşturur:

[49] William Mougayar "Tokenomics – A Business Guide to Token Usage, Utility and Value". 2017. (Çevrimiçi) http://startupmanagement.org/2017/06/10/tokenomics-a-business-guide-to-token-usage-utility-and-value/ (Erişim Tarihi: 25.01.2018).



Şekil 6. Token kullanım ve değer değişkenleri
Kaynak: startupmanagement.org, 2018

Her token rolünün kendine has özellikleri ve amacı bulunmakta olup aşağıdaki tabloda detaylı bir şekilde gösterilmektedir:

Tablo 7. Kripto Token Kullanım ve Değeri

ROL	AMAÇ	ÖZELLİKLER
Hak	Yükümlülüğü başlatma	Ürün kullanımı, İdare, Oy, Ürün Erişimi, Sahiplik, Katkı
Değer Takası	Ekonomi oluşturma	İş Ödülleri, Bir şey satma/ alma/ harcama, aktif/pasif iş, Ürün Yaratma
Santral	Giriş	Akıllı Sözleşmeleri Kullanma, Güvence depoziti, Kullanım Ücretleri
Özellik	Kullanıcı deneyimi kazandırma	Bir ağa katılma, kullanıcılara bağlanma, Kullanımı özendirme
Para	Uyumlu işlemler	Ödeme birimi, işlem birimi
Kar	Kazanç dağıtımı	Kar paylaşımı, gelir paylaşımı, artış geliri

Kaynak: startupmanagement.org, 2018

Tablo 7'de belirtilen tokenin üstlenebileceği her rol aşağıda açıklanmaktadır[50].

Hak:

Belirli bir tokene sahip olmak hamilini ekosistemdeki belirli haklardan faydalandırmaktadır. Bu rol, Merkezi Olmayan Otonom Organizasyon (DAO) yapısında görülebilmektedir. DAO, akıllı sözleşmeler adı verilen bilgisayar programları aracılığıyla kendi kendine çalışan bir organizasyondur[51]. Bu organizasyonun finansal işlem kayıtları ve programlanmış kuralları kayıt zincirinde bulunmaktadır. DAO parasına sahip olmak DAO içinde hangi projelerin finansman alacağına karar vermede oy kullanma hakkını vermektedir.

Değer Takası:

Tokenler projenin kendi sınırları içerisinde kalan bir içsel ekonomik sistem oluşturmaktadır. Tokenler alıcıların ve satıcıların bu eko sistem içinde değer takası yapmalarına yardım etmektedir. Bu da insanların belirli görevlerin tamamlanmasıyla ödüllendirilmelerini sağlamaktadır. Bireysel, içsel ekonomilerin oluşturulması ve sürdürülmesi Tokenlerin en önemli işlevselliklerinden biridir.

Santral:

Tokenler aynı zamanda belirli bir sistemin özelliklerinden faydalanabilmek için bir geçiş ücretinin ödendiği santral görevi de görmektedir. Örneğin Golem kayıt zinciri teknolojisiyle çalışan, dağıtılmış bilgisayarların işlem güçlerinin toplanarak oluşturduğu süper bilgisayardır. Golem tokenleri bu süper bilgisayara erişimi sağlamaktadır.

Özellik:

Tokenler belirli bir çevre sınırları içerisinde kullanıcı deneyimini arttırmaktadır. Örneğin bir internet tarayıcısı olan Brave'i kullananlar bu tarayıcıda kullanılan BAT

---

[50] William Mougayar "Tokenomics – A Business Guide to Token Usage, Utility and Value". 2017. (Çevrimiçi) http://startupmanagement.org/2017/06/10/tokenomics-a-business-guide-to-token-usage-utility-and-value/ (Erişim Tarihi: 25.01.2018).

[51] Usman W. Chohan, The Decentralized Autonomous Organization and Governance Issues, University of New South Wales, Canberra Discussion Paper, 2017 (Çevirimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055, Erişim Tarihi15.07.2018

tokenleri ile reklam ekleyebilmekte veya diğer dikkati çeken hizmetleri bu platformda kullanarak müşteri deneyimini arttırabilme hakkına sahip olmaktadır.

Para:

Tokenler bir ekosistem içinde ve dışında işlemleri gerçekleştirmek için tasarruf aracı olarak kullanılabilmektedir.

Kar:

Tokenler belirli bir proje içindeki yatırımcılar arasında karların veya diğer finansal kazançların adil dağıtımına yardımcı olmaktadır.

Daha değerli olabilmek için bir token bu rollerin en az birinden daha fazlasına sahip olmalıdır. Üstlendiği rol sayısı arttıkça değeri de artmaktadır.

1.5.4 Token Çeşitleri

ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) ve İsviçre Mali Piyasalar Denetleme Kurumu (FINMA) tokeni iki geniş kategoride sınıflandırmaktadır.

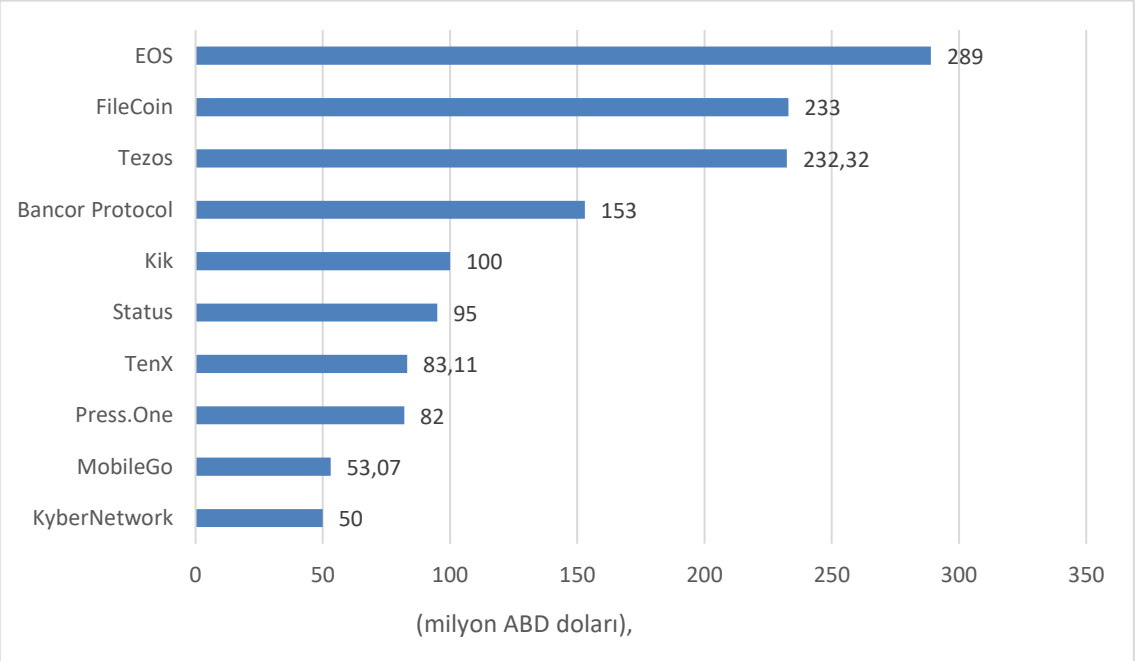
1.5.4.1 Hizmet Tokeni

Hizmet tokeni sahibine farklı hizmet ve hizmet ürünlerini alma hakkını vermektedir. Hizmet tokenleri daha öncesinde yeterli ölçüde finansman bulamamış ortak altyapı projelerinin finansmanında kullanılmaktadır. Özünde belirli bir mal veya hizmeti alabilmek gibi belirli bir amaca yönelik kullanılan kripto paralardır. Örneğin, çevirimiçi bilgi saklamak için bugün en bilinen yöntem Google Drive, Dropbox veya Amazon İnternet Hizmetleri gibi bir veri sağlayıcısının müşterisi olmaktır. Bu firmaların sunucularında belirli bir miktarda saklama alanına sahip olma hakkına Euro, yen veya diğer ulusal para birimlerinden herhangi birini ödeyerek sahip olunmaktadır[52].

Diğer bir yol ise örneğin Filecoin ağıdır. Filecoin benzeri bulut saklama hizmetini bilgisayar sunucusu yığınlarıyla dolu binaları kullanmadan sağlayabilmektedir. Bunun yerine, kullanıcıları verilerini şifreli bir formatta kendileri gibi olan diğer kişilerin boş

[52] Stephen McKeon, "What is a blockchain token?", PBS Conversation Paper, 2018, https://www.pbs.org/newshour/science/what-is-a-blockchain-token, (erişim 12.09.2018)

kalan sabit sürücülerinde saklamaktadır. Bu farklı bir şekilde bir kişinin ne kadar alan kullandığını izleme ve sabit sürücülerinde veriyi saklayan kişilere yeni bir ödeme yöntemi gerektirmektedir. Filecoin adı verilen hizmet tokeni ile bu sağlanmaktadır. Müşteri daha fazla veri sakladıkça ağ, Filecoin token hesabından düşmekte ve bunları her bir alan sağlayıcısına sakladıkları veri miktarına göre göndermektedir. Müşteriler istedikleri herhangi bir para birimi ile daha fazla token alabilmekte ve sağlayıcılarsa bunları istedikleri herhangi bir para birimine dönüştürebilmekte veya kendi verilerinin saklanmasına harcamak üzere tutabilmektedir.



Şekil 7. ICO yöntemiyle önde gelen kayıt zinciri girişim firmaları, 2017 yılında dünya çapında
Kaynak: Statistica, 2018

Yukarıdaki tabloda 2017 yılında ilk dijital para arzı (ICO) yöntemiyle dünya çapında başta gelen kayıtzinciri riskli girişim firmalarını göstermektedir. O yıl, EOS, ICO yoluyla elde ettiği yaklaşık 289 milyon ABD doları ile en önde gelen kayıtzinciri girişim firması olmuştur.

1.5.4.2 Menkul Kıymet (Yatırım) Tokeni

Tokenli menkul kıymet veya kripto menkul kıymet olarak da bilinen menkul kıymet tokeni herhangi bir para birimi olmaktan çok bağlı olduğu gerçek dünyadaki bir varlıkta

sahipliği temsil etmektedir. Bilinen hisse senedi ve tahviller gibi ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) tarafından düzenlenmektedirler. Normal menkul kıymetler kâğıt üzerinde veya günümüzde çoğunlukta olduğu gibi merkezi bir veri tabanında izlenmektedir. Menkul kıymet tokenlerinde kimin hangi varlığa sahip olduğunu izlemek için merkezi olmayan bir veri tabanı olan kayıt zinciri sistemi kullanılmaktadır. Kayıtzinciri tabanlı menkul kıymet tokenlerini kullanmak ticareti bilinen bankacılığın ve borsa saatlerinin ötesine genişletmekte ve hatta işlemlerin daha hızlı sonuçlandırılabilmesini sağlamaktadır. Buna ek olarak akıllı sözleşmelerin kullanımını sağlayan bir yazılıma dayanan bir pazar yeri, düzenleme ve raporlamanın çoğu yönünü de kendiliğnden işler hale getirebilmektedir. Menkul kıymet tokenleri müşterilerin çoklu yatırımlara erişimini kolaylaştırmaktadır. Tıpkı tek bir e-ticaret yatırım hesabının farklı çeşitte hisse senedi ve tahvil kaydını tutabilmesi gibi, kayıt zinciri tabanlı dijital bir cüzdan da aynısını hisseyi, borcu ve hatta emlağı temsil eden birçok farklı çeşitte menkul kıymet tokenleri için yapabilmektedir.

1.6 Bitcoin'in Yükselişi

Kripto paraya bir örnek bitcoin'dir. Satoshi Nakamoto 2008 yılında kripto bilimcilerin ortak olarak kullandığı özel bir eposta grubu internet sitesinde eşten eşe elektronik para üzerine bir makale yayınlamıştır. Her türlü girişime rağmen Satoshi'nin kimliği gizli kalmıştır. Ya bir grup ya da bir kişi olduğu düşünülmektedir.

Bitcoin adı verilen ve Satoshi Nakamoto tarafından bulunan kripto para kaynağı açık yazılım kullanarak işletilmektedir. Herkes tarafından yüklenebilmekte ve sistem merkezi olmayan eşten eşe bir ağ üzerinde çalışmaktadır. Merkezi olmayışının yanında aynı zamanda tamamıyla dağıtık olduğu varsayılmaktadır. Yani her bağlantı noktası (node) veya bilgisayar terminali birbirine bağlıdır. Her bağlantı noktası istediği zaman ayrılabilmekte, yeniden katılabilmekte ve sonra kayıt zinciri (blockchain) olarak bilinen en uzun iş ispatını (proof of work), güvenilir kayıt olarak kabul etmektedir.

Bu en uzun kayıt zinciri, bu bağlantı noktaları (nodes) gittiğinde olanların ispatıdır. Kripto para bazı nedenlerden ötürü belirsiz kalmakta ve yanlış anlaşılmaktadır.

İlk olarak, bazı kripto para sistemlerinin ardında gerçekte kimin olduğu bilinmemektedir. 3.tarafın güvencesine ihtiyaç duyulmayacak şekilde, arkasında tüzel bir kişiliğin olmadığı ama kaynağı açık yazılım olarak tasarlanmıştır.

İkincisi, kripto para çıkarmayı (mining) yani iş ispatını içermektedir. Çıkarma işi (madencilik) için ödül vardır ve ödül bir kriptografi problemini çözebilen ilk kişiye verilmektedir. Bitcoin için problemin zorluk derecesi, problemi çözme süresinin yaklaşık 10 dakika almasını sağlayacak şekildedir. Kripto para çifte harcama (double-spending) sorununu akıllıca çözmüştür: her bir kripto para sadece bir defa harcanabilmektedir. Bu finansal bir teknolojidir ve finansal düzenlemeyi gerektirmektedir ancak algılanılmasında ve uygulanmasında uzmanlar açısından bile zorluklar bulunmaktadır. Bu nedenle araştırmacılar, düzenleyiciler, yatırımcılar ve tüccarlar için büyük bir ilgi alanı olmaktadır.

Başarılı bir dağıtık kripto para için genel parametreler aşağıda belirtilmiştir[53]:

1. Kaynağı açık yazılım: Yazılım kodunu ve uyum için ağ tarafından gerek duyulan olası değişiklikleri teyit edecek güvenilir ve çekirdek bir yazılımcı grubu şarttır.
2. Merkezi olmama: Tamamıyla dağıtık olmasa da bir grup kişi veya kuruluş tarafından kontrol edilmiyor olması gerekmektedir.
3. Eşten eşe: Aracıların olmaması düşüncesine rağmen alt ağ havuzlarının oluşması ihtimali vardır.
4. Küresel: Paranın dünyanın her yanında kullanılabilir olması oldukça olumlu bir durumdur ve taraflar arasında akıllı sözleşmeler[54] olsun olmasın finansal bütünleşmenin sağlanması açısından elverişlidir.
5. Hızlı: İşlem süresi daha hızlı olabilir ve onaylama süresi kısaltılabilir.
6. Güvenilirlik: Mutabakat riskinin olmaması ve geri alınamaz olması avantajdır. Mali işlemlerden sorumlu büyük bir mutabakat takımının maliyetleri potansiyel olarak büyük oranda düşecektir.

[53] David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015.
[54] Eliza Mik, "Smart Contracts: Terminology, Technical Limitations and Real World Complexity", Singapore Management University Paper, 2017, (çevirimiçi) http://dx.doi.org/10.2139/ssrn.3038406, (erişim 12.09.2018)

7. Emniyetli: Gizlilik yapısı kimlik ispatının şifrelenmesi yoluyla daha iyi tasarlanabilir. Böylelikle müşterini tanı (KYC), kara para aklama ve terörizmin finansmanının (AML/TF) engellenmesi sorunları çözülebilir.
8. İçerikli ve Esnek: Sistem her türlü varlık çeşidine, finansal araca ve piyasaya hitap edebilecek ve destekleyebilecektir.
9. Otomatik: Ödeme ve sözleşmeler için algoritma kolayca eklenebilir.
10. Ölçeklenebilir: Sistem milyonlarca kullanıcıyı destekleyebilir.
11. Bütünleşme platformu: Finansal işlemli akıllı sözleşmeleri destekleyecek bir ekosistemle, dijital finans ile dijital hukuğu bütünleştirecek şekilde tasarlanabilir. Çok taraflı programlanır hazır maddeler, şartlar, değişkenler içeren özel sözleşmeler yapılabilir.

Yapılması mümkün uygulamalar çok çeşitlidir ve küresel ödeme ve transfer sistemleri, merkezi olmayan takaslar, ticari çözümler, çevirimiçi oyunlar, dijital sözleşme sistemlerini içeren her kripto para önemli ve büyük bir deneyim olmaktadır. Kimse bu kripto para deneyimlerinin nereye kadar gidebileceğini bilememektedir ancak bu deneyimlerle beraber gelişen teknoloji sebebiyle ilgi çekici bulunmaktadır.

Kayıt zinciri teknolojisi geleneksel ödeme sisteminin önünü kesmektedir çünkü para transferlerinin maliyeti hemen hemen hiç olmamaktadır. Kripto para teknolojisi hem dünyada finansal sistemin dışında hem de bu sistemin kullanım oranının altında kalan kesime ulaşılabilmesini sağlamayı amaçlamaktadır. Ödeme ve fonlarda bir kanal olması planlanmaktadır. Akıllı muhasabe olsun akıllı sözleşmeler olsun işlerin yapılış şeklini aracıların rolünü azaltarak değiştireceği düşünülmektedir.

Finansal dünyanın işleyişini de özellikle fon sağlama ve kredi verme konularında değiştireceği öngörülmektedtir. Temel olarak, aracıları eleyerek, tümü eşten eşe çerçevesinde, ilk kitleye arz (ICO) veya kitle kredisi (Crowd Lending) yapmak mümkün olmaktadır.

Ancak kripto paranın da olumsuz tarafları veya olması muhtemel riskleri bulunmaktadır. Kripto para Bitcoin gibi çıkarmaya (madencilik) (mining) dayanmaktadır. Çıkarma işi (madencilik) için özendirici unsurlar bittiğinde kimse sözkonusu kripto paranın dijital kayıtta ortak karara sahip olmaya devam edeceğini

bilememektedir, 400'den fazla kripto para bulunmaktadır ve bu sayı her gün artmaktadır. Ancak bunların çoğu işlevini yitirmiştir.

Uluslararası taşımacılıkta kullanılan teslim şekillerinden (incoterms) biri olan işyerinde teslimde (ex-works) mal satıcının işyerinden tüm risk alıcıya ait olmak üzere teslim alınmaktadır. Benzeri risk kripto para için de bulunmaktadır. Çünkü sahip olunan şey, kayıt zinci ile ilgili en küçük bir şüphe olması durumunda bir anda değerini yitirebilmektedir. Eğer kripto para çok hızlı ve erken bir şekilde arzını tüketirse bu paranın işlevini itirme olasılığı çok yüksek olacaktır. Bu paralardan bazıları için arkasında kimin olduğunu veya birinin sistemi kontrol etmesine olanak sağlayan bir arka kapı olup olmadığını bilmek zordur. Yazılım geliştiricilerinin bilinmediği kripto paranın, işlevini yitirme olasılığı çok yüksektir.

Kayıt zincirine saldırı ihtimali de bulunmaktadır. Kayıt zinciri, olaylar dizisinin bir ispatı ve aynı zamanda işlem gücünün en büyük olduğu havuzdan gelen iş ispatıdır. İşlem gücü, ağa saldırmak için ortaklaşa çalışan bağlantı noktalarınca (node) kontrol edilir edilmez kendi tercih ettikleri iş ispatlarından oluşan en uzun zinciri oluşturabilirler ve böylece de kayıt zincirinin geçerliliği şüphe yaratabilir. Bu durum belirli bir paraya olan ilgi ve ardından madencilerinin sayısı azaldıkça, ortak uzlaşının sağlandığı birkaç kayıt zincirinin kalması olasılığı sonucunda kolayca olabilir. Kayıt zincirinin doğruluğu hakkında en küçük bir şüple oluşması durumunda, bu durum kısa zamanda düzeltilse bile o para işlevini yitirecektir.

Madencileri ödüllendirecek yeni paraların olmaması halinde o sistemin işlemeye devam etmesi küçük bir olasılıktır. Çıkarma işi (mining) ödülü olarak yeni paralar oluşmamaya başladığında madencilerin işlem ücretleri ile özendirileceği beklenmektedir. Bu bir problem olabilir. Diğer yandan, eğer işlem ücretleri hızla yükselir veya makul olmayan bir seviyede artarsa paraya olan ilgi de azalacaktır. Çıkarma işinin kullanılan bilgisayar ve parçalarının pahalı oluşundan ötürü yüksek maliyetli olması ortak madenci havuzlarının (mining pool) oluşmasına sebep olacaktır. Bunun nedeni madencilerin kodu kırmada yüksek başarı olasılığını tercih etmeleridir. Ancak bu da ağın %30 hatta %50'sini geçen ortak havuz oluşumu gibi istenmeyen bir sonuca sebep olacak böylelikle kripto parayı saldırılara maruz bırakacaktır. Gerçekten de bu durum 2014 yılı ortalarında Bitcoin'de ortak havuzun %50'yi bulmasında

yaşanmıştır. Bu geç kalınmadan çözülmesi gereken önemli bir sorun ve “çıkarma işi (madencilik) olmadan uzlaşım defteri veya dijital kayıt” çözümlerden biri olarak düşünülmektedir.

2. BİTCOİN

Bu bölümde kayıt zinciri teknolojisinin ortaya çıkmasına neden olan Bitcoin anlatılmaktadır. Bu süreç içinde Bitcoin kayıt zincirine, Bitcoin mekanizmasının gelişiminde kayıt zincirlerinin nasıl oluşturulduğuna değinilmektedir.

2.1 Satoshi Nakamoto'nun Tezi

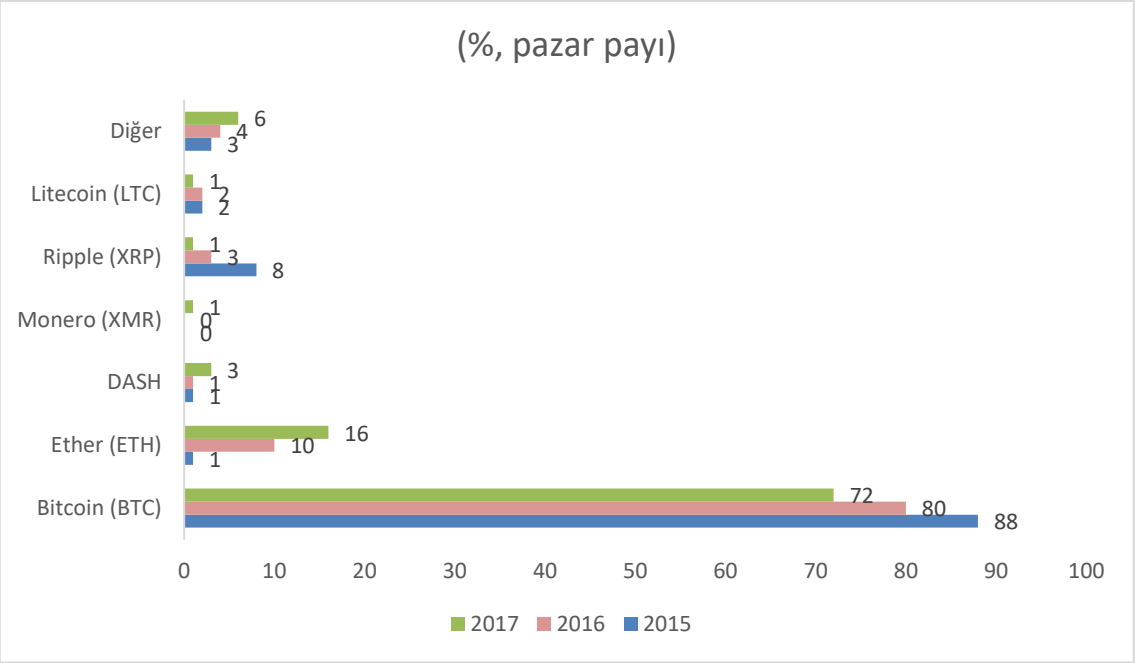
2008 Kasım'ı sonlarında Satoshi Nakamoto isimli biri tarafından kriptografi bilimcilerinin bilgi paylaşımında bulunduğu bir Amerikan eposta listesi grubuna bir tez gönderilmiştir. Bu Bitcoin'in başlangıcı olarak kabul edilmektedir[55]. "Bitcoin: Eşten Eşe Elektronik Nakit Sistemi" başlıklı tezinde Nakamoto aşağıdakileri Bitcoin özellikleri olarak aktarmıştır[56].

- √ Güvenilir üçüncü taraf olmadan doğrudan işlem yapmayı mümkün kılma;
- √ Geri alınamayan işlemleri sağlama;
- √ Günlük küçük işlemlerde maliyeti azaltma;
- √ İşlem masraflarını azaltma; ve
- √ Çifte harcamayı önleme.

Posta listesindeki tartışmalar bir müddet devam ettikten sonra 2009 Ocak ayında ilk blok oluşturulmuştur. Böylece Bitcoin işlemleri ve Bitcoin kayıtzinciri başlamıştır.

O zamandan bu yana Bitcoin sistemi aksamadan çalışmaktadır.

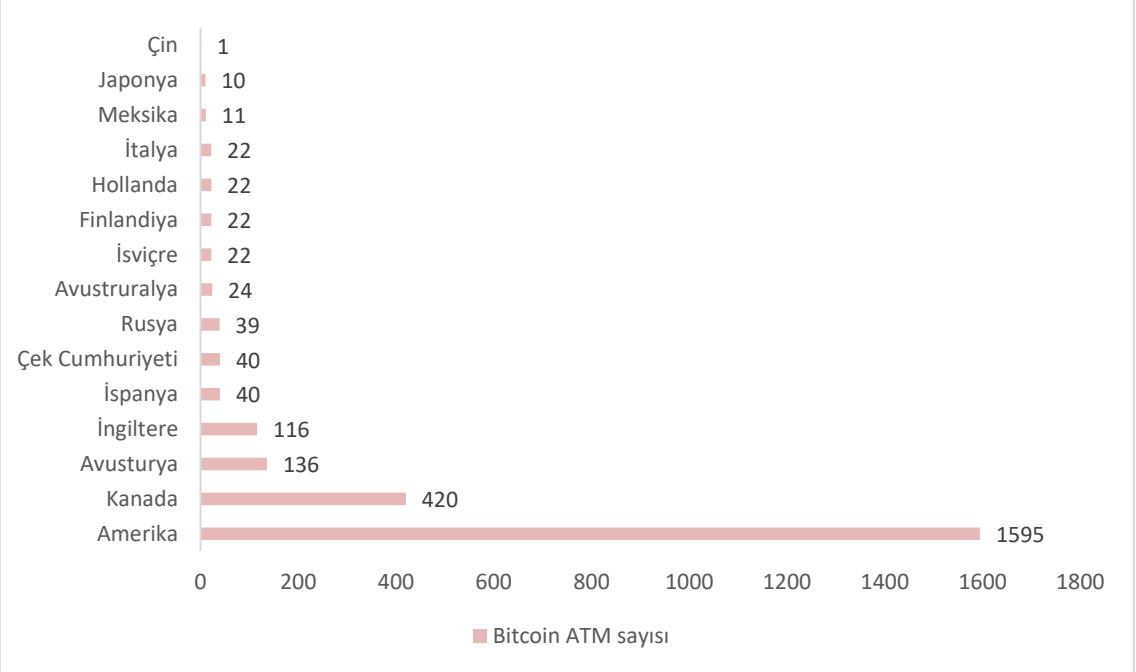
[55] Satoshi Nakamoto, "Bitcoin P2P e-cash paper", Cryptography Mailing List, 2008, (çevirimiçi) http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html. (erişim tarihi 23.05.2018
[56] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (çevirimiçi), 2008 https://bitcoin.org/bitcoin.pdf, (erişim tarihi 23.05.2018)



Şekil 8. 2012-2017 yılları arası önde giden kripto paralar, piyasa kapitalizayonuna göre

Kaynak: Cambridge Judge Business School; CoinMarketCap ID 730782; Statista

Kullanıcıları tüm dünyada artmaktadır.



Şekil 9.9 Nisan 2018 itibari dünyadaki Bitcoin ATM'leri, ülkelere göre

Kaynak: Coin ATM Radar ID 343147; Statista

2.2 Bitcoin'in Özellikleri

Bitcoin sanal para veya kripto para sınıfındandır ve bir yazılım programı içeriğindeki verilerin iç değerlerini ortaya çıkarma yoluyla dağıtılır.

Tablo 8. Bitcoins, İtibari Para, Elektronik Para

Özellikler		**Bitcoins**	**İtibari Para**	**Elektronik para (3.taraf işletmeler için ön ödemeli**
Basım /İdare	**Basan**	Sistem tarafından otomatik olarak basılır	+Devlet +Merkez Bankası	Elektronik para hizmetsağlayıcıları (3.taraf işletmeler)
	Yöneten	Eşten eşe ağ katılımcıları	+Devlet +Merkez Bankası	Elektronik para hizmetsağlayıcıları (3.taraf işletmeler)
Değer	**Arz miktarı**	Belirli (21 milyon BTC)	Sınırsız	Karta önceden yatırılan ücret kadar (depozit)
	Değer Kaynağı	Sisteme duyulan güven	Devlete duyulan güven	+depozit meblağı +kartı basan işletmeye güven
Para Transferi	**Transfer Yönü**	İki yönlü	İki yönlü	Tek yönlü (kullanıcılardan üye işyerlerine)
	Transfer Süresi	+ her 10 dakikada bir blok oluşur +sistem onayının yaklaşık 60 dakika sürdüğü düşünülür	+Doğrudan alıcıya gönderiliyorsa anında +Büyük meblağ gönderiminde zaman alabilir	Üye işyerleri ödemeleri tamamlanana kadar (1 gün ile 1,5 ay arası)
	Transfer Ücreti	+küçük miktarlar +gönderene ait	+pahalı +aralarındaki anlaşmaya göre gönderen veya alıcı veya her ikisi	Alıcıya ait (üye iş yerleri)
Anonimlik	**İşlemlerin Anonimliği**	+işlem kayıtları açık ancak tarafların kimlikleri bilinmez	+Kayıtlar yüksek derecede gizli	+düşük gizlilik (kayıtlar ilgili elektronik para servis sağlayıcısın da tutulur)
	İşlem Kayıtlarının gösterilmesi	Gösterilir	Gösterilmez	Genelde gösterilmez

Kaynak: METI, 2016, s.5

Tablo 8 bitcoin, itibari para ve elektronik para (3.taraf işletmeler için ön ödemeli ödeme araçları) arasındaki kıyaslamayı göstermektedir[57]. İhraççısının net olmadığı Bitoin'de itibari ve elektonik paranın aksine Bitcoin sitemine olan itimat bitcoin değerini desteklemektedir. Ayrıca kullanıcılarının gerşek kimlikleri gizli olsa da işlem kayıtlarının gösterilmesi ve kayıtların izlenebilir olması bitcoin'e has özellikler olarak görülmektedir.

2.3 Bitcoin'i Oluşturan Temel Teknoloji Unsurları

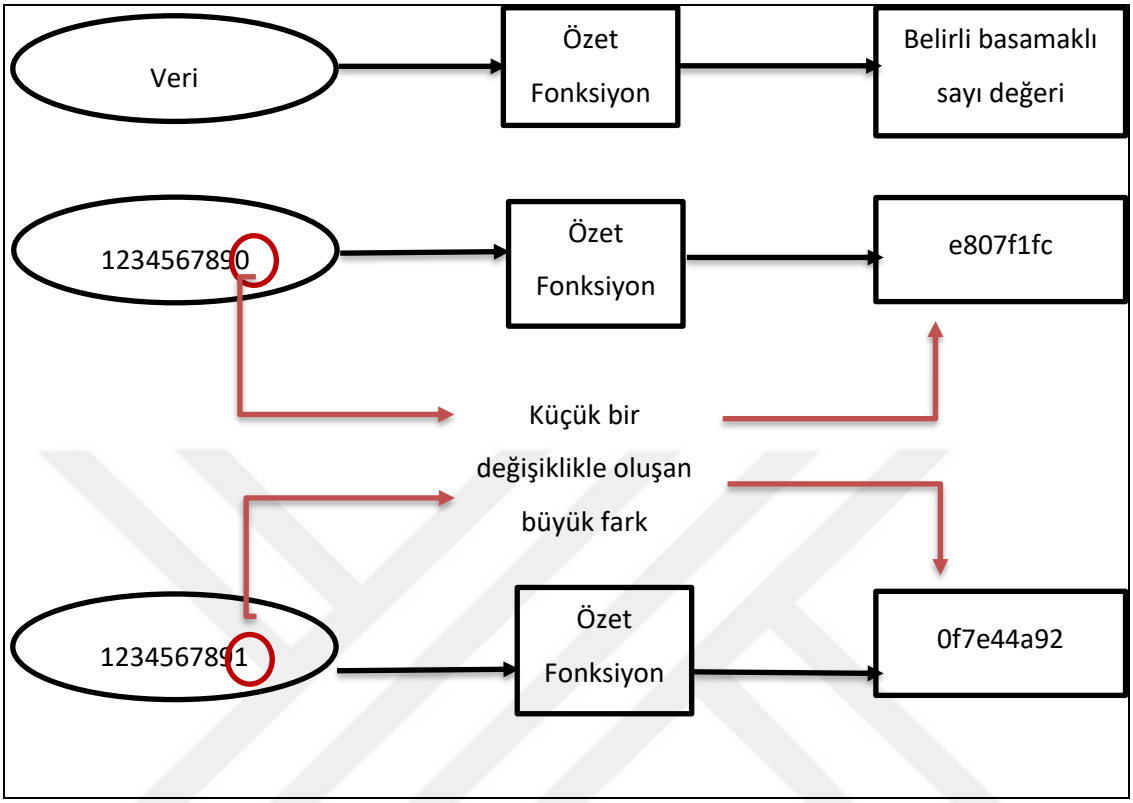
Bitcoin'in varolan teknolojileri kullanarak yeni uygulamalar yarattığı düşünülmektedir. Hiçbir merkezi otorite olmadan, örneğin elektronik paradaki gibi bir sistemi işletebilmek için, verinin sahtesinin yapılmasını veya mükerrer ödemeleri önlemek için ölçüler koymak ve yine aynı zamanda sistemin kötü niyetli girişimlere maruz kalmasını engellemek için bir mekanizma oluşturmak şart değildir. Bitcoin'i oluşturan temel teknolojiler; özet (fonksiyonlar), açık anahtarlı şifreleme ve dijital imza, eşten eşe, iş ispatı aşağıda anlatılmaktadır.

2.3.1 Özet (Kriptografik Özet Algoritmaları)

Veriyi bir özet fonksiyona girmek belirli basamakta sayılardan oluşan bir özet değer sonucunu vermektedir. Bu mekanizmanın temel özelliği, aynı özet değerin sadece aynı veriden elde edilmesi ve asıl verideki sadece küçük bir farklılığın tamamen farklı bir özet değer vermesidir. Özet değerden asıl veriye ulaşmak aşırı derecede zordur. İşte bu temel özelliğe dayanan bu mekanizma verinin sahtesinin tespitinde ve Bitcoin sisteminde ise kayıt zinciri verisini doğrulamak ve teyit etmek ve özet değerlerin hesaplanması yoluyla yapılan iş ispatı ile kayıt zincirlerinin oluşturulmasında kullanılmaktadır.

[57] Japan's Ministry of Economy, Trade and Industry (METI), "Survey on Blockchain Technologies and Related Services FY2015 Report", Nomura Research Institute, 2016, s.5

Tablo 9.Özet Mekanizması

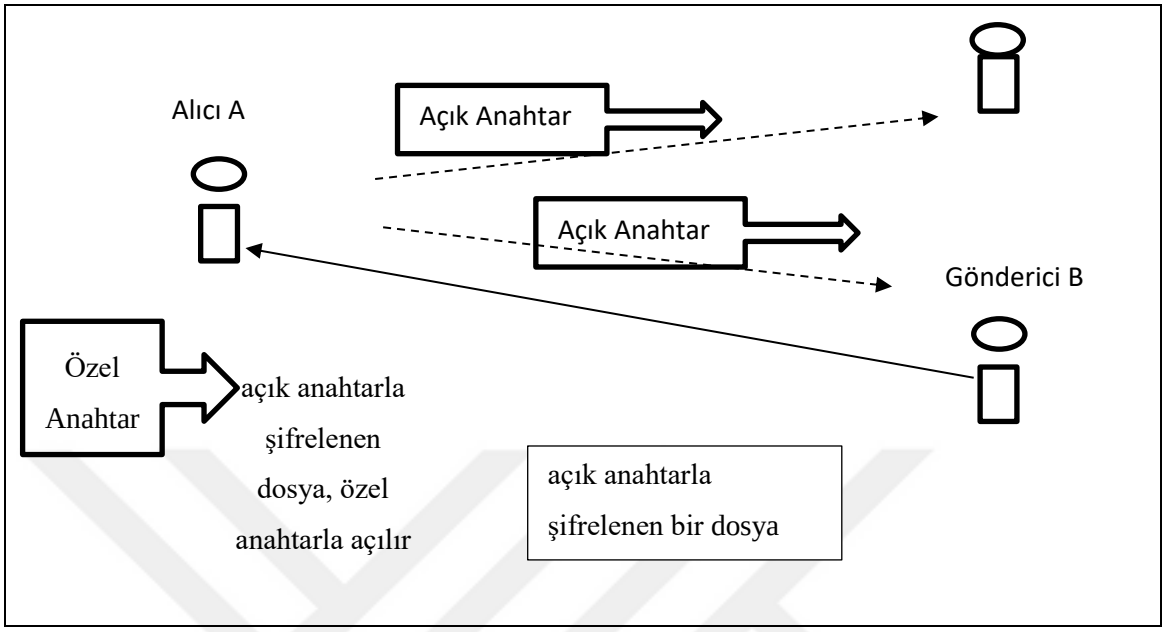


Kaynak: METI, 2016, s.8

2.3.2 Açık Anahtarlı Şifreleme ve Dijital İmza

Açık anahtarlı şifreleme, şifrelemek ve şifreyi çözmek için farklı anahtarların kullanıldığı bir kriptografi yöntemidir. Anahtar teslim sorunu, anahtarı biri özel kullanım (özel anahtar) ve diğeri herkesin kullanımına açık (açık anahtar) olacak şekilde ikiye bölerek çözülmüştür. Şifreleme ve şifre çözme için aynı anahtarı kullanan simetrik anahtarlı şifrelemede anahtarı sadece ilgili tarafa teslim etmek için çok çeşitli güvenlik önleminin alınması gerekmektedir. Bunun aksine açık anahtarlı şifreleme dosyaların güvenli bir şekilde gönderilmesini ve teslim alınmasını sadece alıcının biri özel diğeri açık bir anahtar çifti hazırlaması ve açık anahtarı önden göndericiye yollaması ile mümkün kılmaktadır. Diğer kişiler açık anahtarı kullansalar bile alıcı kendi özel anahtarını koruduğu müddetçe güvenlik sağlanmaktadır.

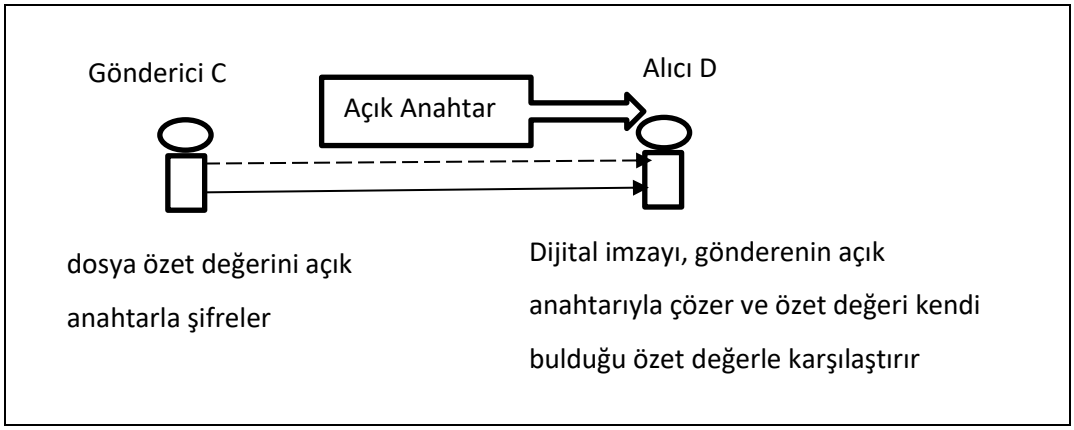
Tablo 10. Açık Anahtarlı Şifreleme Mekanizması



Kaynak: METI, 2016, s.9

Dijital imza, bir ağ üzerinden gönderilen verinin gerçekliliğini ispatlayan mekanizmadır. Açık anahtarlı şifrelemede kullanılan anahtar çiftleri burada da kullanılmaktadır. Genellikle, bir dijital imza, alıcıya gönderilecek dosyanın özet değerinin gönderenin özel imzasıyla şifrelenmesi ile yapılmaktadır. Dijital imza ve dosya alıcıya gönderilir. Alıcı gönderenin yaptığı aynı özet fonksiyonla, dosyanın özet değerini hesaplar ve bulduğu özet değeri gönderenin açık anahtarıyla çözdüğü dijital imzadaki özet değerle karşılaştırır. Böylelikle dijital imzanın doğruluğunu onaylar. Dijital imza özet değer içerdiği ve gönderilen dosya içeriğindeki en küçük bir değişiklik özet değeri de değiştireceği için verinin doğruluğu, dijital imzayı çifti açık anahtardan başka bir anahtar çözemeyeceği için de imzanın gönderene aitliği ispatlanmış olmaktadır.

Tablo 11. Dijital İmza



Kaynak: METI, 2016, s.10

Bitcoin sisteminde, açık anahtarlı şifreleme ve dijital imza, işlem verisinin kimin tarafından oluşturulduğunu belirlemek için ve bir bitcoin cüzdanının adresi olarak kullanılmaktadır. Bitcoin cüzdanı, bitcoin paralarının gönderilebileceği bir adres olarak belirlenmiş numaradır.

2.3.3 Eşten-Eşe (P2P)

Genel olarak istemci-sunucu ağında, sunucu verinin tutulması ve sağlanması işini görürken istemci sunucudan veri ister ve ona erişir ve böylece rolleri değişmez. Bunun aksine eşten eşe ağda tüm katılımcı bağlantı noktaları (bilgisayarlar, eşler) verileri herbiri ayrı ayrı tutar ve talep edilen ve sağlanan verinin bu bağlantı noktalarında eşit olduğu kendiliğinden bir ağ oluştururlar. P2P ağında herbir bağlantı noktasının rolü sunucu veya istemci olarak değişebilir.

Eşten eşe ağı uygularken arama ve veri transfer yöntemlerini dikkate almak gerekmektedir. Arama yöntemleri bağlantı noktalarının yerlerini ve verileri yönetmek için kullanılan yollardır. Örnekleri sadece bir eşten eşe ağıyla yönetim, dizin sunucusu kurulumu ve işlem gücü büyük olan bağlatı noktalarının (süper nodes) yönetimidir. Veri iletim yöntemleri bağlantı noktaları arasında veriyi iletme şekilleridir ve bağlantı noktaları arasında doğrudan iletim ve başka bir bağlantı noktası aracılığıyla aktarılmış iletim olmak üzere ayrılmaktadır. Bitcoin'de kullanılan eşten eşe ağda, arama yöntemi

olarak eşten eşe kullanılırken veri iletimi, ilgili bağlantı noktalarına aktarma yoluyla yapılmaktadır.

2.3.4 İş İspatı (PoW)

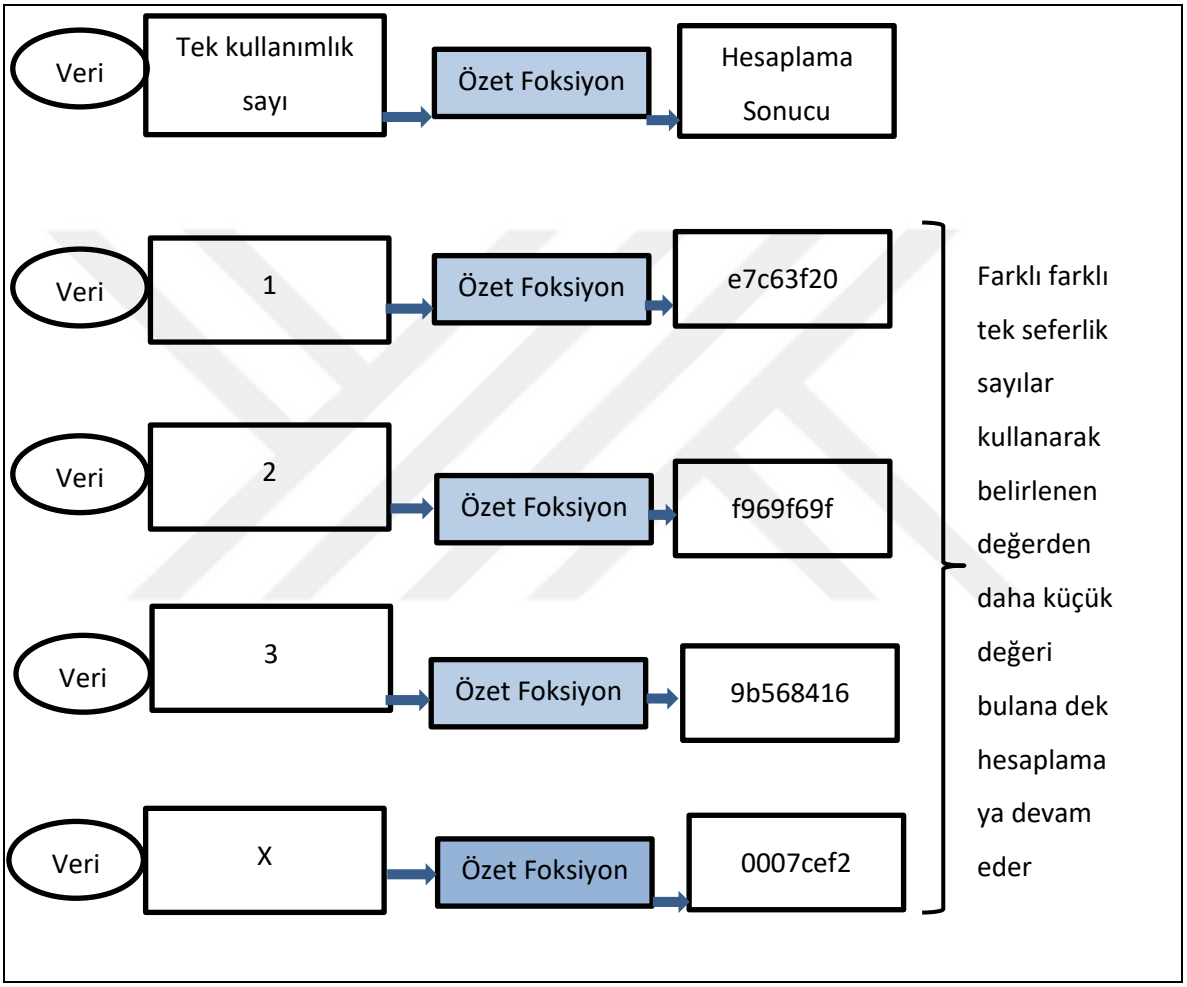
İş ispatı genellikle birinin suçsuz olduğunu doğrulamak (veya yanlış davranmaktan caydırtmak) için temelinde basit ama yapılması zahmetli olan ve bittiğinde doğrulaması kolay belirli bir işi o kişiye yaptırtan bir mekanizmadır. Örneğin, elektronik posta gönderimlerinde bir iş ispatı algoritması olan Hashcash kullanılmaktadır. Her posta gönderimi için belirli bir özet hesabının yapılması gerekmektedir, böylelikle istenmeyen postalar (zamandan olabildiğince kazanmak ve maliyeti azaltmak için toplu posta gönderenler) engellenir.

Bitcoin'de iş ispatı (POW), çıkarma (madencilik-mining) işidir. Bitcoin gönderirken ona ilişkin işlem verisi tüm eşten eşe ağa gönderilmektedir. Bu nedenle, her bir bağlantı noktasına ulaşan "işlem verisi" eşten eşe ağın o anki durumuna bağlı olarak belirli bir zamanlarda farklı olabilmektedir. Ağ katılımcıları onlara iletilen işlem verilerine tek seferlik bir sayı (nonce) ekleyerek bir özet değer hesaplar. Bu özet değerin belirli bir değerden daha küçük olması gerekir ve katılımcı bağlantı noktaları istenilen özet değere ulaşana dek farklı farklı tek seferlik sayılar kullanarak hesaplamaya devam etmelidir. Söz konusu özet değer bulununca, ağ katılımcıları hep birlikte bu özet değerin doğruluğunu onaylamakta ve hesaplamada kullanılan işlem verileri yeni bir blok içindeki resmi işlem sonuçları olarak kabul edilmektedir. Özet değeri bulma zorluğu doğru değere ulaşmak için harcanan zamanın ortalama 10 dakika sürmesi olacak şekilde tasarlanmıştır. Hesaplamalar sonucunda, doğru değeri bulmada başarılı olan kişiye ödül olarak bitcoin verilmektedir. Kazanılan miktar, ödül miktarı 12,5BTC ve ilgili bloktaki işlemlerden gelen ücretlerdir. Verilen ödül her 210 bin blokta bir (yaklaşık dört yılda bir) yarıya düşürülmektedir, dolayısıyla bu ödül yaklaşık olarak 2020 yazında 6,25 BTC olacaktır[58]. Bundan sonra tüm katılımcılar söz konusu blokta içerilmeyen ve yeni iletilen işlem verilerini kullanarak bir sonraki çıkarma işine geçerler.

[58] Japan's Ministry of Economy, Trade and Industry (METI). "Survey on Blockchain Technologies and Related Services FY2015 Report". Nomura Research Institute, 2016.

Bitcoin iş ispatını (PoW) merkezi bir otorite olmadan verinin bozulmasını, çifte ödemeyi önleyen ve sistemi kötü niyetli kullanıcılardan koruyan bir mekanizma oluşturmak için kullanır.

Tablo 12. İş İspatı Algoritmasında Özet Hesaplamaları



Kaynak: METI, 2016, s.12

2.4 Ağ ve Dijital Para

Bitcoin işlemleri yürütmek ve doğrulamak için eşten eşe sistemi kullanan, merkezi olmayan bir ağ ve dijital bir paradır. Bitcoin teknolojisi, ödemelerde, bankalar veya elektronik para hizmet sağlayıcıları gibi güvenilir üçüncü taraflara dayanmak yerine işlemleri sürdürmek ve Bitcoin'lerin geçerliliğini doğrulamak için bilgisayar

yazılımında şifreleme yöntemi ile ispatı kullanmaktadır[59] ve devam eden işlemi ağ üzerine yaymaktadır. Simge olarak büyük B harfinin kullanıldığı Bitcoin, Bitcoin sistemini ifade etmektedir. Bitcoin sistemi (B) ve Bitcoin para birimi (bitcoin) (BTC) veya Bitcoin sistemince oluşturulan dijital adres farklı kavramlardır.

Bitcoin'in icadıyla ödemeler ilk kez, internette kontrolsüz ve merkezi bir otoritenin getirdiği maliyetler olmadan (Bitcoin projesi) yapılabilmektedir. Bu yenilikten önce, çevirimiçi yapılan ödemeler, işlemleri doğrulaması için güvenilir arabulucu olarak daima üçüncü bir tarafa ihtiyaç duymuştur[60]. Örneğin, Alice Bob'a 10 dolar göndermek istediğinde kredi kartı ağı veya Paypall gibi ödeme ödeme hizmet sağlayıcısı bir kuruluş kullanmak zorundadır. Üçüncü taraf hizmetinin temel işlevi gönderici Alice'in transfer edeceği bir parası olduğuna ve paranın alıcı Bob'a başarılı bir şekilde ulaştığına dair güvence sağlamasıdır. Aracı kuruluşların hesap sahiplerinin kaydını, defterini veya bakiyelerini tutmalarına yardımcı olması bu güvenceyi sağlamaktadır. Bu örnekte, Alice Bob'a 10 dolar gönderdiğinde banka gibi bir aracı kuruluş, transfer masrafını almak koşuluyla, Alice'in hesabını borçlandırırken Bob'ın hesabına alacak kaydı verecektir.

Ancak Bitcoin ağında kullanılan ödemelerde para birimi Bitcoin'dir, itibari bir para değildir. Bu nedenle, kendi içinde bitcoin, dijital bir biçimde var olması sebebiyle aynı zamanda bir "dijital paradır" ve özünde bir değişim aracı, hesap birimi ve tasarruf aracı olması yönleriyle paranın ekonomik tanımına uymaktadır. Geleneksel olarak, büyük B ile yazılan ("Bitcoin") ağı ve teknolojiyi küçük harfle yazılan ("bitcoin") para birimini ifade eder. Para birimi kısaltması BTC olarak gösterilmekle beraber bazı borsalarda ISO 4217 standartıyla uyumlu olduğunu ifade eden henüz yapılması planlanan para birimi XBT[61] kısaltmasıyla da kullanılmaktadır.

2.5 Kökeni ve Merkezi Olmayan Kontrol

İlk bitcoin, 2009 yılında Satoshi Nakamoto tarafından, oluşturulması ve işlemlerinin idaresinde merkezi otoriteye güven yerine şifreleme bilimine dayanan bir para kavramı

[59] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (çevirimiçi), 2008 https://bitcoin.org/bitcoin.pdf, (Erişim Tarihi: 05.07.2018)
[60] Jerry Brito ve diğerleri, Bitcoin: A Primer for Policymakers, Mercatus Center, George Mason University, 2.basım, 2016.
[61] David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015, s. 14.

ispatını[62] anlatan bir yazının internette yayınlanmasının ardından çıkarılmıştır veya oluşturulmuştur. Nakamoto projeyi 2010 yılında terketmiştir ve kimliği hala bilinmemektedir. Ancak Bitcoin yazılım protokolünün açık kaynaklı olması sebebiyle diğer yazılım geliştiriciler protokol üzerinden çalışmaya ve Bitcoin topluluğu büyümeye devam etmiştir.

Aynı zamanda Nakamoto'nun kimliğinin bilinmemesine karşın kullanıcıların hiçbiri onun gizlice Bitcoin'in tüm kontrolünü elinde tuttuğunu düşünmemektedir. Bitcoin'in açık kaynaklı bir yazılım olması kaynak kodunun herkes tarafından görülebilir olduğu anlamına gelmektedir. Bu açık gösterim her yazılım geliştiricinin protokolü incelemesine ve kontrol etmek veya geliştirmek için kendi sürümlerini oluşturmalarına izin vermektedir. Bu zamana dek Nakamoto veya gizli kontrolü olan herhangi birinin varlığına dair bir şüphe oluşmamıştır. Ayrıca, Bitcoin tüm ağ kullanıcılarının onayıyla çalışacak şekilde oluşturulmuştur. Bu kendi sürümlerinde Bitcoin kaynak kodunu değiştiren yazılım geliştiricilerin geri kalan ağla uyumlarını bozmadan protokolde kötü amaçlı bir değişiklik yapamamalarını sağlamaktadır. Bitcoin protokolünü değiştirme gücü Bitcoin'in tüm kullanıcılarının ve geliştiricilerinin onayını gerektirmektedir.

2.6 Bitcoin'in İşleyişi

İşin uzmanı olmayan birisi için Bitcoin elektronik ortamda oluşturulan ve saklanan bir dijital paradır. Bitcoin'ler bir mobil uygulama, bilgisayar veya bir bitcoin cüzdanı hizmet sağlayıcısı kullanımıyla gönderilir ve alınır. Cüzdan, banka hesap numarasına benzeyen bir adres oluşturmaktadır. Ancak cüzdan adresinin banka hesap numarasından farkı, kullanıcının ödemelerini almaya başlayacağı Bitcoin adresinin hem alfabetik sayılardan hem de rakamlardan oluşan (alfanümerik) karakterler dizisi olmasıdır. Bitcoin genellikle, Bitcoin takas ofislerinden veya otomatlarından alınarak ya da mal ve hizmet ödemelerinden kazanılmaktadır.

Çifte harcama sorununu üçüncü bir tarafa ihtiyaç duymadan çözebildiği için Bitcoin üçüncü taraf görevini üstlenen kurumların yenileştirilmesi, yeniden biçimlendirilmesi ihtiyacını ya da bu alanda birdenbire gerçekleşecek olası bir kökten değişikliği başlatan

[62] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (çevirimiçi), 2008 https://bitcoin.org/bitcoin.pdf, (Erişim Tarihi: 05.07.2018)

icat olarak görülmektedir. Bilgisayar biliminde, çifte harcama sorunu, aynı dijital paranın kolayca, bir defadan fazla harcanabilmesi anlamına gelmektedir. Bunu bir örnekle açıklamak gerekirse; bilgisayar dosyasının dijital tıpkı bir belge gibi dijital para olduğunu varsayalım. Alice Bob' a elektronik posta ile içinde 10 dolar olan dijital dosyayı kolayca gönderebilir. Ancak, bir dosyayı elektronik posta ile göndermek aslında o dosyanın bir kopyasını göndermek demektir, çünkü gönderildikten sonra bilgisayardaki dosya silinmez. Alice, Bob'a yolladığı elektronik posta ekine bu dijital dosyayı ekleyip Bob'a gönderdiğinde 10 doları harcamış olsa bile kopyası hala bilgisayarındadır. Güvenilir bir üçüncü taraf aracı kuruluşu engel olmadığı sürece Alice kolayca aynı dijital dosyayı bir başkasına göndererek 10 doları tekrar harcayabilir.

Bitcoin çifte harcama sorununu, tek bir güvenilir üçüncü tarafın kontrolünü gerektirmeyen, sorumluluğu tüm ağa dağıtan bir bakiyeler defteri sağlayarak çözmektedir. Bitcoin ağı, bitcoin bakiyelerinin kaydını, adına kayıt zinciri denilen herkese açık bir defterde sürekli tutmaktadır. Kayıt zinciri, Bitcoin yazılımını kullanan herkesin bir işlemin geçerliliğini doğrulamasına izin veren ve daha önceden işlenmiş tüm işlemlerin herkesin erişebildiği güvenilir kaydıdır. Bitcoin gönderimleri, yani işlemler, tüm ağa duyurulmakta ve kayıt zincirine başarılı bir doğrulama ile eklenmektedir ve böylece harcanan paralar tekrar harcanamamaktadır. Çifte harcama sorunu, yeni işlemlerdeki bitcoin'lerin, kayıt zincirinde daha önceden harcanmamış olmalarına yönelik kontrol edilmeleri yoluyla çözülmektedir.

Bitcoin çifte harcama sorununu çözmek için derinlemesine açık anahtarlı şifrelemeyi kullanmaktadır. Açık anahtarlı şifrelemede her işlem bir dijital imza ve sahteliği kolayca tespit eden bir özet içermektedir. (Tablo 13 ve Tablo 14.'teki şekiller bir Bitcoin işlemine örnektir[63].)

[63] David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015, s. 16-17-18

Tablo 13. Bir işleme ait işlenmemiş veri örneği


```
{
“hash”:e966845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b8
0c1d”,
   “ver”:1,
   “vin_sz”:1,
   “vout_sz”:1,
   “lock_time”:0,
   “size” :225,
   “in” :[
    {
        “prev_out”: {
“hash”:”f4515fed3dc4a19b90a317b9840c243bac26114cf637522373a7d486b372
600b”,
            “n”:0
        },
“scriptSig”  :  ” 3046022100bb1ad26df930a51cce110cf44f7a48c3c561fd977500b
1ae5d6b6fd13d0b3f4a022100c5b42951acedff14abba2736fd574bdb465f3e6f8da
12e2c5303954aca7f78f301
04a7135bfe824c97ecc01ec7d7e336185c81e2aa2c41ab175407c09484ce9694b449
53fcb751206564a9c24dd094d42fdbfdd5aad3e063ce6af4cfaaea4ea14fbb”
     }
  ],
  “out”:[
     {
       “value”:”0.01000000” ,
       “scriptPubKey”:”OP_DUP
OP_HASH160
39aa3d569e06a1d7926dc4be1193c99bf2eb9ee0                    OP_EQUALVERIFY
OP_CHECKSIG”
      }
   ]
}
```


Kaynak: Handbook of Digital Currency, 2015, s. 16-17-18

Tablo 14. İşleme ait ham verilerin açıklamaları

İşlemle ilgili genel açıklamalar		
Özet	e966845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b80c1d	İşlem özeti
Blok	100000 (2010-12-29 11:57:43)	Kayıt zincirinde bu işlemin bulunduğu bloğun gözlenmesinden elde edilmiştir
Sürüm	1	Bitcoin yazılım sürümü
Boyut	225	İşlem verisinden alınan işlem baytı olarak dosya boyutu
Girdi		
Önceki çıktı	f4515fed3dc4a19b90a317b9840c243bac26114cf637522373a7d486b372600b	Bu işlemde harcanan bitcoin'leri sağlayan önceki işlemin kesilmiş özeti
Önceki miktar	0,01	Bu işlemde gönderilen bitcoins'leri sağlayan önceki işlemdeki miktar
Açık adres	1JxDJCyWNakZ5kECKdCU9Zka6mh34mZ7B2	gönderenin açık adresi (Kayıt zincirinin gözlemlenmesinden elde edilen)
İmza	3046022100bb1ad26df930a51cce110cf44f7a48c3c561fd977500b1ae5d6b6fd13d0b3f4a022100c5b42951aced ff14abba2736fd574bdb465f3e6f8da12e2c5303954aca7f78f301 04a7135bfe824c97ecc01ec7d7e336185c81e2aa2c41ab175407c09484ce9694b44953fcb751206564a9c24dd094d42fdbfdd5aad3e063ce6af4cfaaea4ea14fbb	Gönderenin atttığı, işleme ait dijital imza
Dönüştür		
Dizin	0	"0" işlemdeki ilk alıcıyı göstermektedir; bu işlemde sadece bir alıcı bulunmaktadır
Miktar	0,01	İşlemde bu kullanıcıya gönderilen miktar
Açık adres	16FuTPaeRSPVxxCnwQmdyx2PQWxX6HWzhQ	scriptPubKey'den sağlanan alıcının açık adresi
Bitcoin adresi (ScriptPubKey)	39aa3d569e06a1d7926dc4be1193c99bf2eb9ee0	Açık adresin "hash160" özeti
Koşullar	OP_DUP OP_HASH160 OP_EQUALVERIFY OP_CHECKSIG	bitcoins'lerin alıcı tarafından geri alınabilmesi için scriptPubKey ile beraber sağlanması gereken koşullar

Kaynak: Handbook of Digital Currency, 2015, s. 16-17-18

2.7 Bitcoin'lerin Alınması ve Saklanması

Teknik altyapısına karşın bitcoin'ler çoğunlukla mal ve hizmet karşılığı bir ödeme aracı olarak kolayca kullanılmaktadırlar[64]. Bitcoin ödemelerini kabul eden, işlerinin çoğunu fiziksel temsilciler vasıtası ile fiziksel ürünler satarak gerçekleştiren eski ve geleneksel işletme sayısının az olmasına rağmen hem fiziksel hem de dijital mal ve hizmet satışlarında bitcoin kabul eden birçok internet satışı yapan firma bulunmaktadır. Bu malların fiyatları genellikle internetten kolayca bulunabilen, Bitcoin ile gerçek dünya parası arasındaki değişim kuruna dayanmaktadır[65].

Bitcoin harcamak isteyen biri genellikle gerçek dünya parasını bitcoin ile takas etmek yoluyla satın almaktadır. Bu takas, bitcoin'leri otomat makinelerinden, döviz değişim büroları ya da basitçe bir başkasından almak yoluyla yapılabilir. Sadece makineye para koyma yoluyla bitcoin alınabildiği için ATM adı verilen bitcoin otomatları en uygun yerler olarak görülmektedir[66]. Bitcoin döviz büroları da bitcoin almak için en çok tercih edilen yollardan biridir ancak kullanıcılar çoğunlukla banka transferlerinin tamamlanması için beklerken zaman gecikmesi yaşamaktadırlar[67]. Bitcoin'i itibari para ile almak da mümkündür ancak eğer hemen isteniyorsa elverişsiz bir seçenektir. Buna karşın, piyasada yeni yeni oluşmaya başlayan, bitcoin alıp satmak isteyen insanları buluşturan LocalBitcoins gibi internet siteleri bunu yüz yüze veya internetten özel olarak yapabilmelerini sağlamaktadır. Bu seçenek, Bitcoin otomatlarına veya döviz bürolarına erişimin olmadığı veya kısıtlı olduğu ülkelerde daha çok tercih edilmektedir.

Bitcoin'ler genellikle bir cüzdanda saklandığı için bir kullanıcının bitcoin alıp satabilmesi için müsait bir cüzdana sahip olması gerekmektedir. Temelinde, bir cüzdanda saklanan özel anahtarlardır[68]. Bu anahtarlar Bitcoin adreslerine erişim ve işlemlerin imzalanmasında kullanıldığı için güvenli bir şekilde saklanması

---

[64] Nikolei M. Kaplanov, Nerdy money: bitcoin, the private digital currency, and the case against its regulation, Temple University Legal Studies Research Paper, 2012, (çevirimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203, (erişim tarihi 14.05.2018)
[65] Jerry Brito ve diğerleri, Bitcoin: A Primer for Policymakers, Mercatus Center, George Mason University, 2.basım, 2016.
[66] Bogdan Ulm, Bitcoin ATMs boom: new locations, CoinTelegraph, 2014, (çevirimiçi) https://cointelegraph.com/news/bitcoin-atms-boom-new-locations, (erişim tarihi 27.06.2018).
[67] Ulm, a.g.e.
[68] David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015, s. 332.

gerekmektedir. Masaüstü, mobil, internet ve donanım cüzdanları başta gelmek üzere birçok çeşitte Bitcoin cüzdanı bulunmaktadır.

Bilgisayarına bir masaüstü cüzdan kurmayı seçen kullanıcılar cüzdanları bilgisayarlarında oluşturabilmekte ve saklayabilmektedirler. Bugün hala kullanılmakta olan orijinal Bitcoin istemci yazılımı, Bitcoin Core, bitcoin göndermek ve almak için bir bitcoin adresi oluşturma ve ilgili adresin özel anahtarını saklama işlevlerine sahiptir. Kullanıcıların bilgisayarlarına kurabilecekleri MultiBit çoklu platform yazılımı, güvenliğe karşı duyarlı Armory gibi daha birçok alternatif cüzdan yazılımı bulunmaktadır[69]. Bir cüzdanın en temel işlevi, bitcoins adreslerinin bağlı olduğu ilgili özel anahtarları saklamak olsa da farklı cüzdan yazılımları ve değişen ek özellikleri bulunmaktadır. Kullanıcı her zaman kendi masaüstü cüzdanının kontrolünü elinde tutuyor olsa da bu tarz cüzdanlar, kötü niyetli kullanıcı veya yazılımlar tarafından yapılacak olası hırsızlıklara karşı savunmasızdır.

Masaüstü cüzdanları cüzdanlar içinde ilk olsalar da sonradan birçok türde cüzdan yapılmıştır. Fiziksel bir mağazada işlem yaparken genellikle mobil cüzdan bitcoin harcamak için en elverişli uygulama olarak görülmektedir. Mobil cüzdanlar, telefonlara Bitcoin cüzdanı işlevselliği sağlayan bir uygulamalardır. Sadece mobil platformda bulunan Bitcoin Wallet ve Mycelium gibi uygulamalarla beraber Blockchain.info gibi bazı masaüstü cüzdanların aynı zamanda mobil uygulamaları da bulunmaktadır[70]. Ancak resmi olmayan sürümlerin ve mobil tarayıcı tabanlı cüzdanların kullanımı devam etse de 2014 yılı başlarında Apple Bitcoin.info gibi Bitcoin cüzdan uygulamalarına son vermiştir[71].

Kullanışlı diğer bir cüzdan çeşidi ise kullanılan alet ne olursa olsun internet erişimi olan herhangi bir tarayıcı ile heryerden ulaşılabilen çevirimiçi cüzdanlarıdır[72]. Kullanıcının Bitcoin adreslerinin özel anahtarları çevirimiçi cüzdanın hizmet sağlayıcısı tarafından saklanmakta ve depolanmaktadır. Bu durum eğer güvenlik yeterli derecede

[69] Chuen, a.g.e. s.333
[70] David LEE Kuo Chuen, Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier Science & Technology, eBook ISBN: 9780128023518, 2015, s. 18.
[71] Jon Southurst, Apple Removes Blockchain Bitcoin Wallet Apps from its App Stores, CoinDesk, 2014, (çevirimiçi) https://www.coindesk.com/apple-removes-blockchain-bitcoin-wallet-from-app-stores/, (erişim tarihi 27.05.2018)
[72] Chuo, a.g.e. s.18

sağlanmamışsa hizmet sağlayıcısı veya üçüncü bir tarafın paraları kaçırması riskini oluşturmaktadır. Blockchain.info en çok bilinen internet tabanlı çevirimiçi cüzdanına sahiptir. Bazı çevirimiçi cüzdanlar fazladan şifreleme ve iki aşamalı hesap doğrulama hizmetleri ile ek güvenlik seçenekleri sunmaktadır.

Son olarak küçük ama büyüyen bir ilgiye sahip donanım cüzdanları bulunmaktadır. Donanım cüzdanları anahtarları elektronik olarak tutan bitcoin gönderip alabilen özel araçlardır. Trezor, güvenli Bitcoin işlemleri için yapılmış tek kullanımlık özel token cihazlara[73] örnektir.

2.8 Yeni Bitcoin Oluşturmak ve İşlemlerin Yürütülmesi

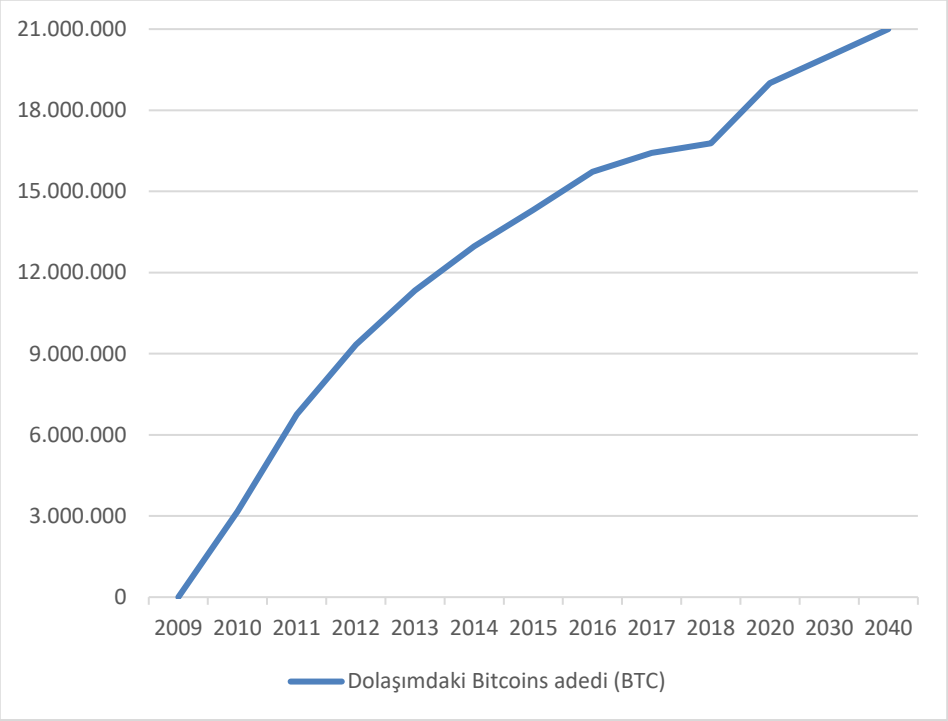
Bitcoin 2040 yılına kadar tamamlanacağı beklenen 21 milyon net arz ile oluşturulmuştur. (Şekil 10). Şu an için bitcoin'ler çıkarma işi (madencilik) yoluyla oluşturulmaktadır. Madenciler yani özel donanıma sahip bilgisayarlarında yazılımı çalıştıran Bitcoin kullanıcıları, işlemleri yürütmekte ve ağın sürmesine bilgisayar güçleri ile katkıda bulundukları için de yeni bitcoinlerle ödüllendirilmektedirler. Çıkarma işi (madencilik) sadece yeni bitcoin'lerin oluşturulması için değil aynı zamanda işlemlerin kayıt zincirine eklenmesi ve hemen ardından da onaylanması için gerekli bir süreç olduğu için önemlidir. Doğrulama süreci sadece geçerli işlemlerin doğrulanmasını ve kayıtzincirine kaydedilmesini sağlayan hesaplama açısından oldukça zor ve ayrıntılı bir süreçtir. İşlemlerin gerçekleşmesi ve kaydedilmesi için hesaplama gücünü sağlayan ağdır.

Çıkarma işi (madencilik) aslında matematiksel bir süreçtir. Buna bir örnek, asal sayıları bulmaya çalışmak olabilir: küçük olanları bulmak kolayken büyük asal sayıları bulmak gittikçe zorlaştığı için araştırmacılar özel yüksek performanslı bilgisayarlar kullanmaya başlamıştır[74].

Çıkarma işi madencilerin yeni bir blok oluşturabilmek için önceden belirlenmiş matematik probleminin çözümünü bulmalarını gerektiren hesaplayarak yapması zor ve ayrıntılı bir görevdir. Bu işin matematiksel ispatıdır. Çıkarma işi zordur çünkü

[73] Chuo, a.g.e. s.19
[74] Ken Tindell, Geeks Love The Bitcoin Phenomenon Like They Loved The Internet In 1995, Business Insider, 2013, (çevirimiçi) https://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4, (erişim tarihi 15.04.2018)

işlemlerin geçerli olduğunu sağlamanın yanında madenciler veriyi kayıt zincirine ekleyebilmek için onu özel bir şekilde bağdaştırmak zorundadırlar. Madenciler gerekli karakteri çıkaracak bir veri dizini için tahminde bulunmalı ve araştırmalıdır.



Şekil 10. Dolaşımdaki Bitcoins (BTC) adedi
Kaynak: Statistica, 2018

Problemin zorluğu, yeni bir bloğun sadece ortalama her 10 dakikada bir oluşturulabilmesini sağlar şekilde kendiliğinden ayarlanmaktadır. Bitcoin protokolü yeni bitcoinleri, tahmin edilebilir ama azalan bir oranda dereceli olarak oluşturacak şekilde tasarlanmıştır. Yeni bitcoinlerde sürekli bir büyümeyi temin etmek için bir bloğu çözmenin ödülü kendiliğinden her 4 yılda bir yarıya indirilmekte ve çözme zorluğu ise zaman geçtikçe artmaktadır. Bu iki etki, zaman geçtikçe bitcoinlerin çıkarılma oranının altın gibi bir malın üretilme oranına yakın olacağı etkisi yaratacak şekilde beraber işlemektedir (Şekil 10). Gelecekte bitcoin kesin arz sınırına ulaşılacağı ve madencilerin kazancının sadece işlem ücretleri olacağı bir zaman olacaktır. Bitcoin sayısının sınırı olarak belirlenen itibari rakam 21 milyondur. Çıkarma işiyle en son bitcoin veya net bir ifadeyle en son satoshi (bir bitcoinin 0,00000001'i)

oluşturulduğunda, işlemleri doğrulamak için hesaplama gücü sağlayan madenciler artık işlem ücretleri ile ödüllendirilecektir. Bu durum, ödemeleri bitcoine dayanan ve işlem ücreti ödemek zorunda kalacak olan insanlar ve işletmeler için en son istenecek bir durum olsa da son bitcoin çıkarıldıktan sonra bile madencilerin ağı hala çalışır ve işler tutmalarını özendirecek bir teşviğe sahip olmasını sağlamaktadır.

Kayıt zincirine başarılı bir şekilde eklenen her yeni bloğun kendisinden bir önce gelen bloğa ilgi tutması önceki bloklardaki işlemlerin geriye alınmasını katlanarak zorlaştırmaktadır. Çünkü kayızincirinde bir bloğu değiştirmek o bloktan sonra gelecek blokların iş ispatlarının yeniden hesaplanmasını gerektirmektedir (bitcoin projesi). Kötü niyetli bir kullanıcı için ardına birçok blok eklenen bir bloğu değiştirmeye çalışması imkânsız olmaktadır. Bu nedenle Bitoin protokolü birbirine eklenen bloklardan oluşan en uzun zincirin tercih edilmesini sağlayacak şekilde tasarlanmıştır. Bu nedenle madenciler işlemleri doğrularken ve kayıt zincirinin değiştirilerek bozulamamasını sağlarken oldukça önemli bir görev üstlenmektedirler.

Bitcoin işlemleri ağ üzerinde hemen yayınlanmasına rağmen uygulamada, bir işlemin onaylanması için 10 dakikalık gecikme olmaktadır. Bu 10 dakikalık gecikme bir bloğun oluşturulması ve kayıtzincirine eklenmesinin sonucudur. Onaya sahip olmak ağın (madencilerin) bitcoinlerin geçerli ve daha önce harcanmamış olduğunu doğrulaması demektir. Çoğu kullanıcı bir işlemi "onaylanmış" kabul etmek için genellikle 6 onay yani bir saat beklemektedir. Ancak her kullanıcı işleminin onaylandığını düşünmek için ne kadar süre bekleyeceğine karar vermekte serbesttir.

2.9 Güvenlik ve Şifreleme Bilimi

Kullanılan teknolojinin güvenliği güvenilir özet algoritmalar ile desteklenmektedir ve kayıt takibi iyidir. Bitcoin protokolü açık bir kaynaktır ve tüm ağ kullanıcılarının onayına bağlı olarak geliştiriciler tarafından sürekli güncellenmektedir. Bitcoin'de kullanılan özet fonksiyon çoğunlukla SHA-256'dır[75]. Bu algoritma aslında Amerika'daki NSA tarafından tesadüfen bulunmuştur. NSA tarafından tasarlanması, kamuya açık bir yazılımın parçası olması ve güvenilir olması için ayrıntılı bir biçimde

[75] Chris Pacia, Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics, Escape Velocity, 2013, (çevirimiçi) https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/, (erişim tarihi 27.06.2018)

incelenmiş olması bu algoritmayı güvenilir kılan unsurlardır[76]. SHA-256, SHA-1 serisinin bir üst versiyonudur ve Bitcoin'de işlemleri ile kayıtzincirini güvenceye alan dijital imzalarda kullanılmaktadır. SHA-256, iş ispatı matematik probleminin temelini oluşturmaktadır.

Bitcoin teknolojisinin temelinde açık anahtarlı şifreleme yöntemi bulunmaktadır. Açık anahtarlı şifreleme yönteminde SHA-256 özet fonksiyonu Bitcoin adreslerini oluşturmada, işlemleri imzalamada ve ödemeleri doğrulamada kullanılmaktadır. Açık anahtarlı şifreleme, dijital imzaları kullanan Bitcoin işlemlerininin gerçekliliğine güvenilir bir şekilde karar verme tekniğidir. Bu yöntem asimetrik olarak birbirine bağlı açık anahtar ve özel anahtar adında iki ayrı anahtar oluşturan asimetik algoritmayı kullanır. Anahtarlar asimetriktir çünkü açık anahtar özel anahtardan oluşturulur ama açık anahtardan özel anahtarı bulmak matematiksel olarak imkansızdır. Böyle bir sistemde, açık anahtar işlemlerdeki dijital imzaların doğrulanmasında özel anahtar ise dijital imzaları oluşturan işlemleri imzalamakta kullanılmaktadır. Açık anahtar herkese açıktır, Bitcoin'de ödemelerin gönderildiği Bitcoin adresi olarak kullanılır. Özel anahtar ise güvenli ve özel bir şekilde saklanmalıdır. İşlemlerin imzalanmasında kullanılan özel anahtarın kimseyle paylaşılmadan açık anahtarla işlemlerin kolayca doğrulanması bu sistemi yararlı yapan bir unsurdur.

2.10 Takma Adlık (Pseudoanonymity)

Tablo 13 ve Tablo 14'te görüldüğü gibi bir Bitcoin adresi alfanümerik karakterler dizisidir. Bitcoinleri göndereni ve alanı belirten başka bir bilgi yoktur. Ancak, bitcoinin gizli (anonymous) bir para olduğunun söylenmesi yaygın bir yanlış kanıdır. Bu yanlış algı çoğunlukla teknolojinin anlaşılmasındaki eksiklikten kaynaklanmaktadır[77].

Bitcoin'den önce internetten yapılan hiçbir ödeme gizliye yakın bile değildir, çünkü üçüncü taraf aracı kuruluşları üzerinden yapılmaktadır. Üçüncü taraf aracı kuruluşların risk değerlendirme amaçlı ve ilgili yasa ve düzenlemelere uyumluluk uygulamaları nedeniyle müşterilerini bilmeleri gerekmektedir. Örneğin, Alice PayPal hizmetiyle Bob'a 10 dolar gönderdiğinde PayPal'da bu işlemin bir kaydı olacaktır. Buna ek olarak,

[76] Pacia, a.g.e.
[77] Jerry Brito ve diğerleri, Bitcoin: A Primer for Policymakers, Mercatus Center, George Mason University, 2.basım, 2016.

herbirinin PayPal hesabı kimlikleri hakkında bilgi sağlayan bir kredi kartı veya banka hesabına iliştirilmiştir. Diğer taraftan, eğer Alice Bob'a nakit olarak elden 10 dolar verirse ne bir aracı kuruluş ne de bu işleme ait bir kayıt olacaktır. Eğer ikisi birbirlerini tanımıyorsa bu durumda bu işlemin tamamen gizli olduğu söylenebilmektedir.

Bitcoin bu iki uç örnek arasında bir yerde bulunmaktadır. Bitcoinlerin, Alice Bob'a bitcoin verdiğinde artık onlara sahip değilken Bob'un sahip oluşu bakımından, nakit para gibi oldukları söylenebilir. Arada bir üçüncü taraf aracı kuruluşu olmadığı için kimse kimliklerini de bilmemektedir. Ancak nakit paradakinden farklı olarak işlem kayıtzincirine kaydedilmektedir. Kaydedilen işlem, alıcı ve göndericinin açık anahtarları, miktar ve zaman damgası gibi bilgileri içerir. Bitcoin geçmişindeki her işlem kayıt zincirine kaydedilmiştir ve kaydedilmeye devam etmektedir ve herkesçe görüntülenebilmektedir.

Biraz gizliliğin olmasına karşın kayıt zinciri tüm işlemlerin herkese açık bir kaydıdır. Özellikle eğer bir kimsenin kimliği açık anahtar şifresiyle ilişiklendirilmişse herkesin işlemlerin ardındaki tarafları belirlemesi mümkün olabilmektedir. Bitcoinler nakit paradaki gibi tarafların birbirlerinin kimliklerini belirtmeden işlem yapabilmeleri açısından gizli olabilir ama aynı zamanda nakittekinden farklı olarak Bitcoin adresine giden ve adresinden gönderilen tüm işlemlerin izleri sürülebilmektedir. Bu nedenle Bitcoin takma adlıdır ama gizli değildir.

Doğru araçlara ve erişime sahip herhangi biri için takma adlı Bitcoin adresi ile ona sahip kişinin gerçek hayattaki kimliği arasındaki noktaları birleştirmek zor değildir. Bir internet sitesinde işlem yaparken IP adresi gibi bazı belirleyici kişisel bilgiler sıklıkla yakalanabilmektedir. Bitcoin adresine bağlı kimlik belirleyici bilgilerini gizleyerek veya örterek kimliğinin Bitcoin adresinden farkedilmesini daha da zorlaştırmak isteyen birinin yazılım yöntemleri kullanması gerekmektedir.

İlk çalışmalar Bitcoin'in takma adını ortaya çıkarabilen potansiyel analizleri göstermiştir. Bitcoin adreslerini gerçek kimliklere bağlamakta istekli olanların çalışmaya kayıt zincirinden başlamaları gerekmektedir. Bir çalışmada, temsili bir deneydeki Bitcoin kullanıcılarının %40'ının, davranışa dayalı kümeleme yöntemiyle

kişisel olarak tanımlanabildiğini göstermiştir[78]. İşlem diyagramınının istatiksel özellikleri de ilgili analizlerle Bitcoin kullanıcılarınıın kimliklerini ve etkinliklerini ortaya çıkarabilmektedir[79]. Öğe birleşmesi, aynı anda iki ya da daha fazla açık anahtarın bir işlem girdisinde gözlemlenmesidir. İşlem diyagrami analizlerinde, kullanıcının birden fazla farklı açık anahtarı olsa da gözlemleyen kişi bunları adım adım birbirine bağlayabilmekte ve çoklu açık anahtarın sağladığı varsayılan görünürde gizliliği ortaya çıkarabilmektedir. Bu sayede, çoklu açık anahtarların kullanımı işlem diyagramı analizlerinde tespit edilebilmektedir[80] ve gözlemci, öğe birleşmesi yöntemiyle adım adım açık anahtarları birbirlerine bağlayan kullanıcı davranışlarındaki kalıpları ayırt edebilmektedir[81].

Bitcoin'in teknik özelliklerinin dışında Bitcoin aracı kuruluşlarına düzenleyiciler tarafından uygulanan baskı da göz önünde bulundurulması gereken bir unsurdur. Bitcoin düzenlemesi halen gelişme aşamasındadır. Bitcoin aracıları düzenlendiğinde gizliliğin (kimlik belirsizliğinin), aracıların kişisel tanımlayıcı bilgileri müşterilerinden edinmelerini gerektirecek çoğunlukla müşterini tanı prensibi ve raporlama şartlarıyla azalacağı beklenmektedir[82].

2.11 Bitcoin'inYararları

Çoğu insan Bitcoin'i ilk öğrendiğinde aklına gelen "dolaşımdaki parayı kullanabiliyorken neden bitcoin kullanmak isteyeyim?" sorusu olmaktadır. Bitcoin çoğu işletmecinin kabul etmediği hala yeni ve istikrarsız bir para olarak algılanmaktadır. Bu nedenle de Bitcoin kullanımı çoğunlukla deneysel görülebilmektedir. İnsanların neden Bitcoin kullanmak isteyebileceğini anlamak için onu itibari paranın yerini alan bir para türü değil de yeni bir ödeme yöntemi olarak düşünmek faydalı olacaktır. Çünkü üçüncü taraf aracı kuruluşu olmadığı için Bitcoin işlemleri geleneksel ödeme yöntemlerinden daha ucuz ve daha hızlı olabilmektedir.

---

[78] Androulaki ve diğerleri, Evaluating User Privacy in Bitcoin, FC 2013: Financial Cryptography and Data Security s. 34-51, 2012 (çevirimiçi) https://link.springer.com/chapter/10.1007%2F978-3-642-39884-1_4, (erişim tarihi 27.06.2018)

[79] Fergal Reid ve diğerleri, An Analysis of Anonymity in the Bitcoin System, Cornell University Library, 2013, (çevirimiçi) https://arxiv.org/abs/1107.4524, (erişim tarihi 27.04.2018)

[80] Micha Ober ve diğerleri, Structure and Anonymity of the Bitcoin Transaction Graph, Future Internet, cilt 5, sayı 2, s. 237-250 2013 (çevirimiçi) https://www.mdpi.com/1999-5903/5/2/237.

[81] Jerry Brito ve diğerleri, Bitcoin: A Primer for Policymakers, Mercatus Center, George Mason University, 2.basım, 2016.

[82] Jerry Brito ve diğerleri, a.g.e.

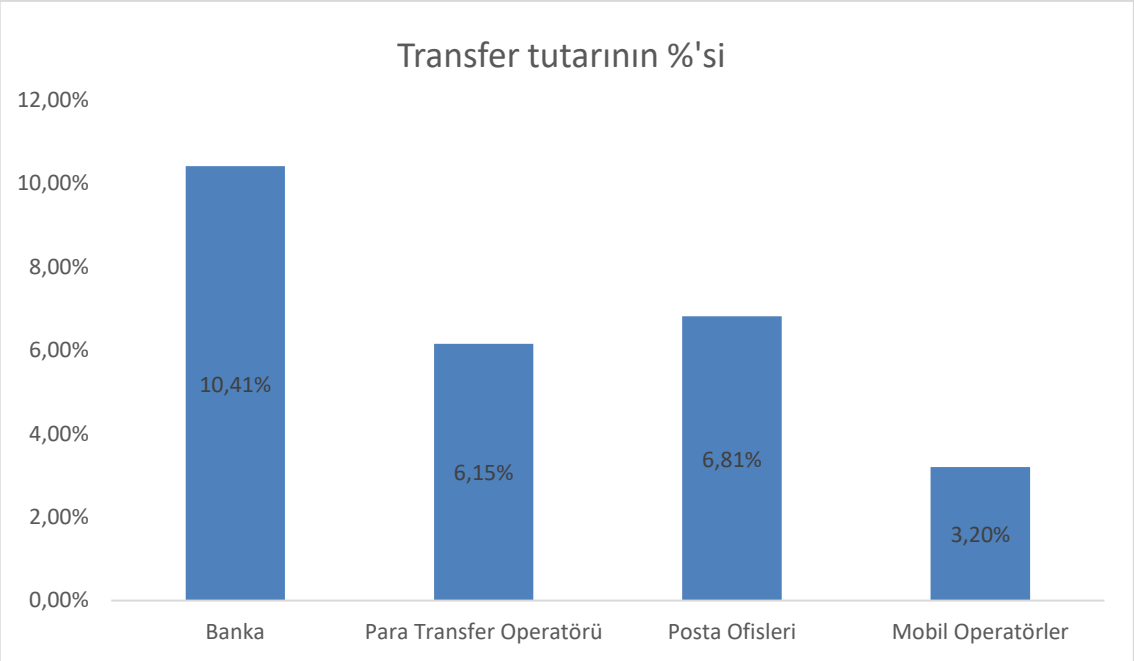
İşlemler daha ucuz olabildiği ve para birimi 8 haneye kadar bölünebildiği için Bitcoin, mikro ödemeleri ve diğer yenilikleri gerçek anlamda ilk kez düşük maliyetli yapabilmektedir. Ayrıca, Bitcoin küçük işletmeler ve uluslararası ödemeler için işlem maliyetlerini düşürme, sermayeye erişim yollarını geliştirerek küresel fakirliği azaltma, bireyleri sermaye kontrolleri ve sansüre karşı koruma, azınlık gruplara finansal gizliliği sağlama, yeniliğe teşvik etmeyi (Bitcoin prorokolü) vaat etmektedir. Bu bölüm Bitcoin'in en bilinen faydalarını özetlemektedir.

2.11.1 Ödeme Özgürlüğü Vermesi

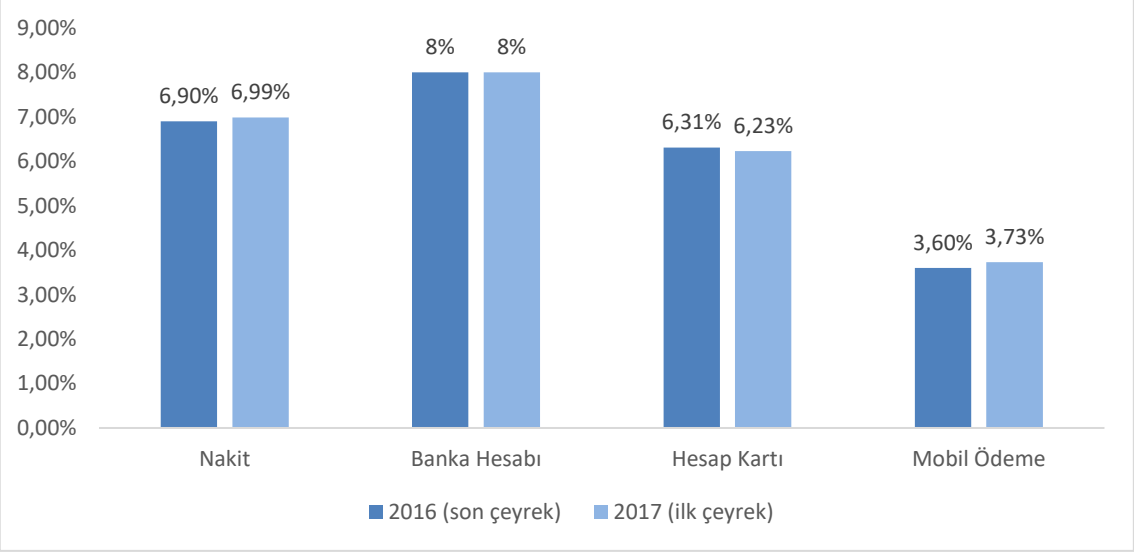
Bitcoin özellikle işlemlerin hızlı ve düşük maliyette yapılması için tasarlanmıştır[83]. Ödemeler gönderenin daha hızlı onaylanması için işlem masrafı eklemesi seçeneğine bağlı olarak çok az masrafla veya masrafsız yapılabilmektedir. Hiçbir üçüncü taraf aracı kuruluşu olmadığından düşük bir işlem maliyeti mümkün olmaktadır. İşlemlerde kısıtlamaların olmayışının yanında kullanıcılar bitcoinlerinin tüm kontrolünü ellerinde tutmakta, onları istedikleri zaman istedikleri yere gönderme ve herhangi bir yerden alma özgürlüğüne sahip olmaktadırlar.

Kullanıcılar pahalı transfer ücreti ödemeden uluslararası transferleri hızlı ve kolayca yapmak için Bitcoin kullanmayı tercih edebilmektedir. Gelişmekte olan ülkere gönderilen para akışı 2016 yılında %2,4 düşerek 429 milyar dolar olmuştur ancak bu rakam resmi kalkınma yardımlarından daha fazladır ve özel sermaye akışlarına göre daha istikrarlıdır. Gelişmekte olan ülkere gönderilen para akışının 2017 yılında %3,3 artarak 444 milyar dolar olacağı tahmin edilmektedir[84]. Bu transfer akışlarında Bitcoin ödeme sistemi kullanılırsa azaltılmış transfer maliyetleri azımsanmayacak derecede büyük olacaktır. Aşağıdaki şekil transfer hizmet sağlayıcısı tipine göre maliyetleri göstermektedir.

[83] Satoshi Nakamoto, "Bitcoin P2P e-cash paper", Cryptography Mailing List, 2008, (çevirimiçi) http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html, (erişim tarihi 23.05.2018).
[84] World Bank, World bank trends in migration and remittances, Migration And Development Brief 27, 2017, (çevirimiçi) http://www.worldbank.org/en/news/infographic/2017/04/21/trends-in-migration-and-remittances-2017, erişim 14.07.2018.



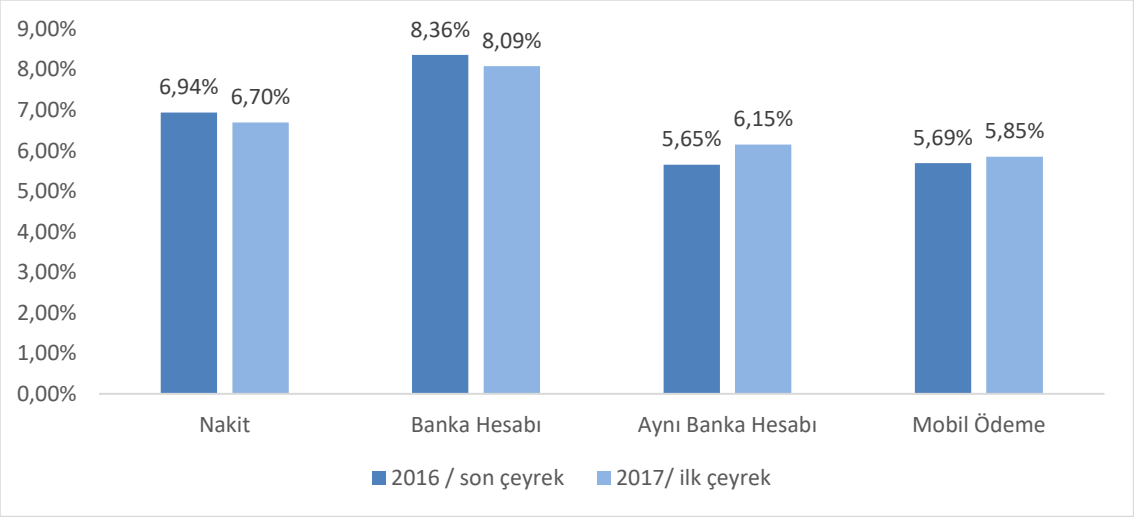
Şekil 11. Transfer Hizmet Sağlayıcısına göre Ortalama Maliyet
Kaynak: WBO, Remittance prices, 2018, s. 12



Şekil 12. Transfer Kaynağını Karşılama Aracına Göre Maliyet
Kaynak: WBO, Remittance prices, 2018, s. 13

Transfer işlemi için kullanılan kaynak ile alıcıya dağıtımı yapan kaynak yukarıdaki şekilde gösterilmektedir. Şekil 12'ye göre 2017 birinci çeyrekte transfere en ucuz

kaynak bulma yolu %3,73 ile mobil ödeme (31 hizmet sağlayıcısı), banka kartı (debit/credit card) %6,23 (724 hizmet sağlayıcısı) ve nakit %6,99 ile en ucuz yöntem (2,139 hizmet sağlayıcı) olduğu görülmektedir. %8 ile en pahalı yöntemse banka hesabından gönderim (1,433 hizmet sağlayıcı) olmuştur.



Şekil 13. Transfer Bedelinin Dağıtım Yöntemine Göre Ortalama Maliyet
Kaynak: WBO, Remittance prices, 2018, s. 13

Şekil 13'e göre aynı bankanın başka bir şubesine veya iştirakine para göndermenin maliyeti 2017 ilk çeyreğinde %6,15 (90 hizmet sağlayıcı), bir başka bankaya göndermek %8,09 (1,372 hizmet sağlayıcı) ile en pahalı yöntem, buna karşın en ucuz dağıtma yönteminse %5,85 ile mobil cüzdan olduğu (90 hizmet sağlayıcı) görülmektedir. Nakit ile dağıtım hizmetinde (2,507hizmet sağlayıcı) ise ortalama maliyet %6,70 olarak tespit edilmiştir.

2.11.2 Ticari Faydaları

İlk olarak işletme maliyetlerini düşürmenin yollarını arayan maliyete karşı duyarlı firmalar için Bitcoin çekici gelmektedir. Kredi kartları geniş ölçüde ticari işlemleri kolaylaştırmış olsa da kullanım maliyetleri işletmeciler için çoktur. Müşterilerine kredi kartı ile ödeme seçeneğini sunmak isteyen işletmeler öncelikle ilgili kart firmasına ticari işletme hesabı açtırmak için ödeme yapmalıdır. Her bir kart kuruluşuna göre değişen sözleşme şartlarına göre işletmelerin sonrasında yetkilendirme ücreti, işlem ücreti, değişim ücreti, müşteri hizmet ücreti gibi çeşitli masrafları karşılamaları gerekmektedir.

Bu masraflar kolayca biraraya gelmekte ve önemli ölçüde işletme masraflarını arttırmaktadır. Ancak eğer bir işletme masraflardan kaçınmak için kredi kartı ödemelerini kabul etmezse bu durumda kredi kartı kullanımına alışmış müşterileri kaybedecektir.

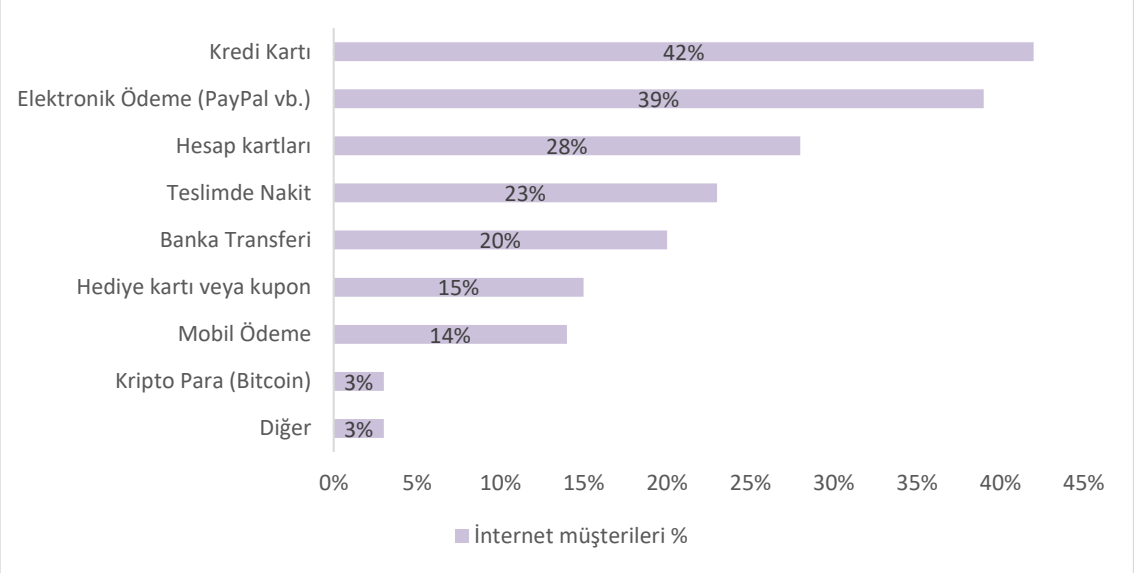
Bitcoin işletmeler tarafından kabul edilen diğer elektronik ödeme yöntemlerine alternatif getirmektedir. Geleneksel kredi kartı kabulü işletmeciler için pahalı olmaktadır. Bitcoin üçüncü bir taraf olmadan doğrudan işlemlere olanak verdiği için kredi kartı işlemleriyle gelen maliyetli masrafları ortadan kaldırmaktadır. 2014 Mayıs ayında Virgin Group, AME Cloud Ventures, Founders Fund gibi güçlü yatırımcıların 30 milyon dolarlık desteğini alan ödeme hizmetleri sağlayıcısı kuruluş BitPay'in uluslarası elektronik ticaretle uğraşan firmaların işletme maliyetlerini azaltması beklenmiştir[85]. Bu Bitcoin kuruluş desteği rekorunu 2015 yılında müşterilerine cüzdan ve takas hizmetleri veren ve yaygın bilinen Coinbase firması BBVA, New York Stock Exchange, Andreessen Horowitz gibi kuruluşlardan 75 milyon dolarlık yatırım alarak kırmıştır[86]. Kredi kartı firmaları ile işlem yapmanın maliyetlerinden kaçınmak isteyen küçük işletmeler ve işlemleri gerçekleştirmesindeki hızı ve verimliliği nedeniyle işletmeler tarafından kabul görmeye başlamıştır. Kredi kartı firmalarının "yüksek risk" kategorisinde izlediği ve kendileriyle çalışacak ödeme hizmet sağlayıcısı bulmakta zorlanan işletmeler kredi kartı firmalarına ekonomik ve elverişli bir alternatif olarak BitPay gibi Bitcoin ticari hizmet sağlayıcılarına yönelmiştir. Kullanıcıları çoğaldıkça Bitcoin onu kabul eden işletmelerin işlem maliyetlerini azaltmaya devam edeceği düşünülmektedir.

Kredi kartı ödemelerinin kabulü işletmeleri geri ibraz hilesi[87] (chargeback fraud) sebebiyle zor duruma sokmaktadır. Geri ibraz hilesi veya bir ürünün teslim edilmediğine yönelik müşteri tarafından başlatılan yalan beyana dayanan iade

[85] Pete Rizzo, "BitPay Raises $30 Million in Record-Breaking Bitcoin Funding Round," CoinDesk, May 13, 2014, http://www.coindesk.com /bitpay-closes-30-million-funding-round-led-by-index-ventures erişim tarihi 14.07.2018
[86] Vigna and Casey, "Coinbase Raises $75 Million; https://www.wsj.com/articles/coinbase-raises-75-million-in-funding-round-1421762403, erişim tarihi 14.07.2018
[87] Havacılıkta Sahte İşlemleri Önleme Yönetimi, s.24; http://www.havais.org.tr/uploaded/magazine/mart-nisan-2018-1525269987-2.pdf, erişim tarihi 15.07.2018

talepleri işletmelere uzun zamandır rahatsızlık veren bir konudur[88]. İşletmeler bu nedenle sattıkları ürünün yanında ödemesini kaybetmekle beraber aynı zamanda geri ibraz masrafını da ödemektedir. Bitcoin'in bir "geri alınamayan ödeme sistemi" oluşu müşteri geri ibrazlarının suistimali ile yapılan "dostane dolandırıcılığı" ortadan kaldırmaktadır. Bu küçük işletmeler için oldukça önemlidir.

Bitcoin işlemleri aynı zamanda sağlam olmayan manyetik şerit ve bozulmaya elverişli veya taklit edilebilir imzaları olan kredi kartı ödemelerinin aksine güvenlidir. İşlemlerdeki düşük maliyet unsuru işletmelerin aynı zamanda mikro ödemeleri kabul etmesini mümkün kılmakta ve Bitcoin'in genel kabul görmesine imkan vermektedir. Aşağıdaki tablodaki istatistik Mart 2017 itibari dünya çapında internet alışverişlerinde tercih edilen ödeme yöntemlerini göstermektedir. Araştırma internet alışverişi yapanların %42'sinin kredi kartı ödemesini tercih ettiklerini göstermektedir.



Şekil 14. Dünyada İnternet Alışverişlerinde Tercih Edilen Ödeme Yöntemleri, Mart 2017 itibari
Kaynak: Statista 2018, CIGI, Ipsos

[88] Emily Maltby, "Chargebacks Create Business Headaches," Wall Street Journal, February 10, 2011, https://www.wsj.com/articles/SB10001424052748704698004576104554234202010 erişim tarihi 15.07.2018

2.11.3 Kullanıcı Denetimi Sağlaması

Her Bitcoin işleminin sadece özel anahtara sahip kullanıcı tarafından gerçekleştirilebilmesi kullanıcısına bitcoinlerinin tam denetimini vermektedir. Kredi kartı bilgilerine sahip etik olmayan bir işletmecinin sonradan karttan çektiği beklenmedik masraflara karşı sınırlı koruma sağlayan kredi kartlarının aksine işletmeler sonradan masraf yükleyemezler. İşlemler aynı zamanda sızdırılması veya çalınması riski olan kişisel bilgileri içermemektedir.

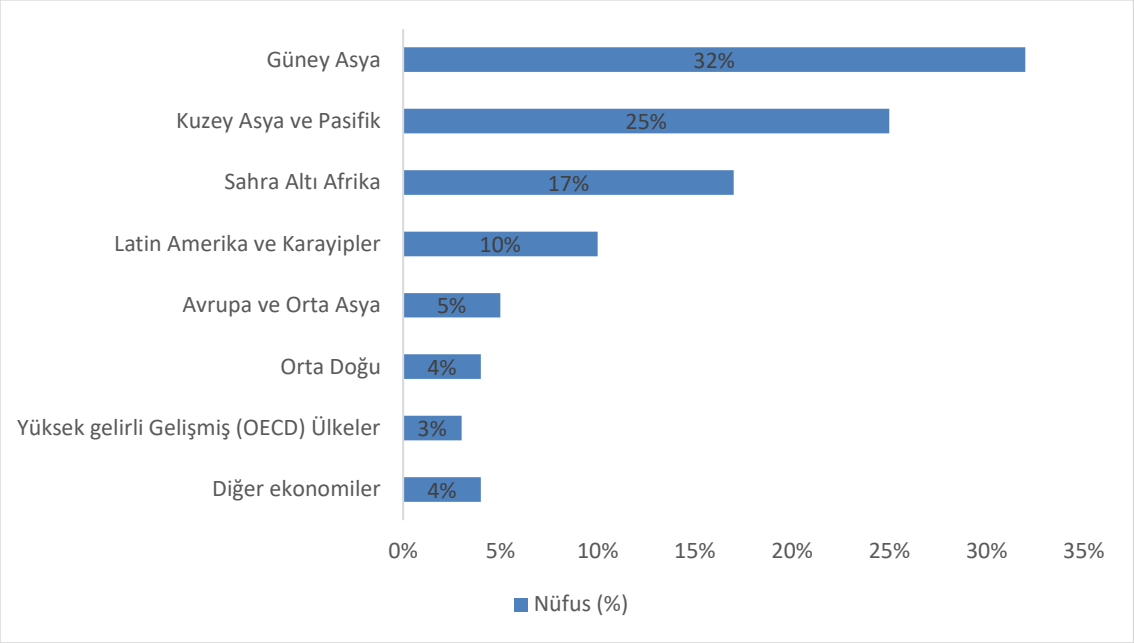
Ancak, özel anahtarın erişimi sağlaması bitcoinlerin tam denetiminin kullanıcıda olmasının ters etkisidir. Dijital para olarak Bitcoin, özel güvenlik sorunları getirmektedir[89]. Son kullanıcı için belki de en önemli risk özel anahtarın kaybolması durumunda bitcoinlere erişimin tekrar sağlanamamasıdır. Yetersiz cüzdan koruması kullanıcıları çalıntı olasılığına karşı savunmasız bırakmaktadır, özellikle bitcoinleri çalmak için yapılmış kötü amaçlı yazılımlara karşı[90]. Bu nedenle Bitcoin kullanıcıları tıpkı diğer finansal işlemlerinde oldukları gibi Bitcoin güvenlik bilincinde olmalıdır[91].

2.11.4 Fakirlik ve Baskı ile Mücadele Potansiyelinin Olması

Bitcoin'in dünyanın en fakir bölgelerinde yaşayanlar için yaşam kalitesini başka yollarla da geliştirme potansiyeli bulunmaktadır. Temel finansal hizmetlere erişim yollarını geliştirmek ümit verici bir fakirlikle mücade yöntemidir[92]. Şekil 15, 2014 yılı itibari dünyada finansal erişimi olmayan veya yetersiz bulunan bölgeleri göstermektedir. Gelişmekte olan ülkelerde finansal erişimin yetersiz olmasının

[89] Graciela L. Kaminsky, "Varieties Of Currency Crises",2003, NBER Working Paper Series No. 10193, (çevirimiçi) http://www.nber.org/papers/w10193.pdf. (Erişim tarihi 15082018)
[90] Stephen Doherty, "All your Bitcoins are ours…", Security Response, Symantec, 2011, (çevirimiçi) https://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours, (erişim tarihi:28.06.2018)
[91] Jerry Brito ve diğerleri, Bitcoin: A Primer for Policymakers, Mercatus Center, George Mason University, 2.basım, 2016.
[92] Muhammad Yunus, Banker to the Poor: Micro-Lending and the Battle against World Poverty, ABD, Public Affairs, 2003.

sebeplerinden biri geleneksel fianansal kuruluşlar için fakir ve kırsal alanda yaşanlara hizmet vermenin maliyetli bulunmasından kaynaklanmaktadır[93].

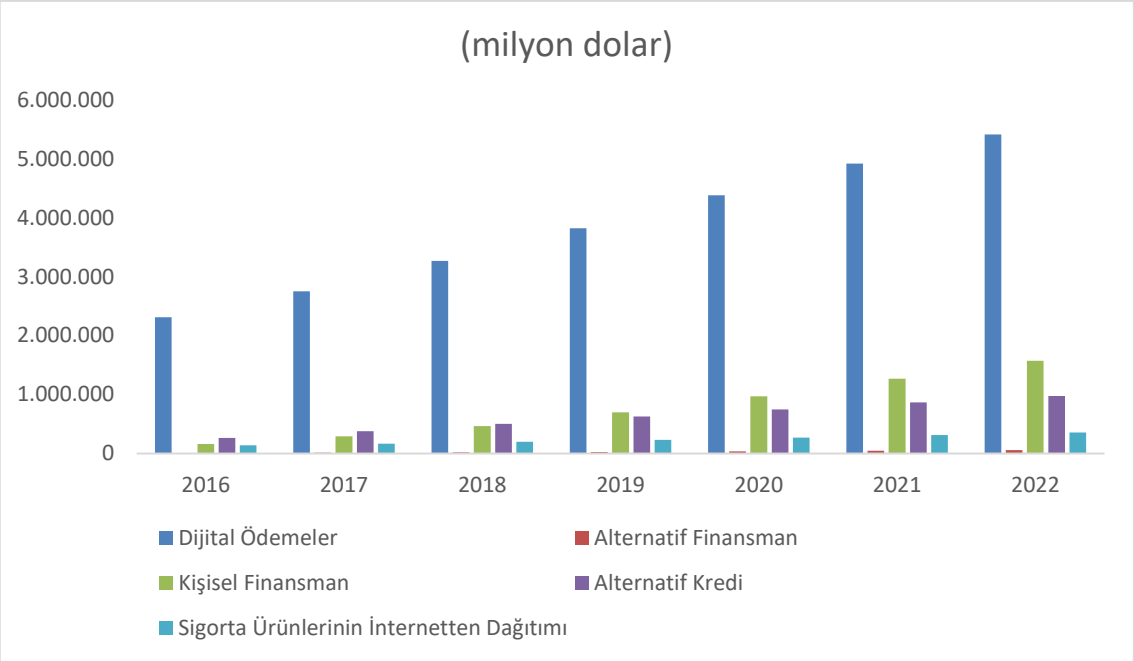


Şekil 15. 2014 Yılı İtibari Finansal Erişimi Yetersiz Veya Bulunmayan Bölgeler
Kaynak: Statista 2018

Alışılmış şube bankacılığının fakir bölgelerde geliştirilmesindeki engellerden ötürü gelişmekte olan ülkelerde yaşayan insanlar finansal ihtiyaçlarını mobil bankacılık hizmetleriyle karşılamaktadır. Kapalı sistem (sadece üyelerine açık) mobil ödeme hizmeti olan M-Pesa özellikle Kenya, Tanzanya ve Afganistan gibi ülkelerde başarılı olmuştur[94]. Gelişmekte olan ülkelerde mobil bankacılık hizmetleri Bitcoin'in benimsenmesiyle daha da geliştirilebilir.

[93]Yunus, a.g.e.

[94] Jeff Fong, "How Bitcoin Could Help the World's Poorest People," PolicyMic, May 2013, (çevirimiçi) http://mic.com/articles/41561/bitcoin-price-2013 -how-bitcoin-could-help-the-world-s-poorest-people. (Erişim 15.07.2018)



Şekil 16. FinTech 2016/2022 Sektör Bazlı Potansiyel İşlem Değerleri, 2018
Kaynak: Statista Haziran 2018, FinTech Digital Market Outlook

Şekil 16'da, FinTech'in 2018 raporundaki 2016/2022 yılları arasında seçili finans sektörlerinin potansiyel işlem değerleri gösterilmektedir. Piyasadaki en geniş sektörün 2018 yılında $3,265,209 milyon dolar ile dijital ödemeler olduğu görülmektedir.

Tablo 15. FinTech 2016/2022 belirli sektörlerde potansiyel işlem değerleri, 2018

Milyon $	2016	2017	2018	2019	2020	2021	2022	CAGR %
Dijital Öd.	2.311.407	2.753.714	3.265.209	3.818.909	4.381.401	4.920.468	5.411.354	15,2
Alt.Fin.	10.061	14.602	20.551	27.910	36.588	46.422	57.200	33,6
Kiş.Fin.	161.818	293.704	467.688	697.335	971.956	1.270.468	1.571.094	46,1
Alt.Kredi	263.945	380.644	502.600	626.461	749.041	867.511	978.436	24,4
Sig.Ür.İnt.	140.330	168.274	199.411	233.808	271.319	311.636	354.342	16,7
Toplam	2.747.231	3.442.664	4.256.048	5.170.616	6.138.986	7.104.868	8.018.084	19,5

Kaynak: Statista Haziran 2018, FinTech Digital Market Outlook

Diğer Bitcoin işletme modelleri gelişmekte olan ülkelerde bitcoin kullanımını yaymaya çalışmaktadır. Örneğin bireysel az miktarlı bitcoin kullanıcılarına listeleme ve saklama hizmeti veren LocalBitcoins.com sitesi Bangladeş, Zimbabve, Demokratik

Kongo Cumhuriyeti, Pakistan, Venezuela, Romanya, Hindistan ve Libyayı içeren 190'ın üzerinde ülkede işlemci bilgisi tanıtımı yapmaktadır.

Amerika'da yardım kuruluşları da Bitcoin'i fakirliği azaltabilecek bir yol olarak görmektedir. Bitcoin'in kolay kullanılırlığı ve para gönderimlerinin karşılanabilir olması düşük işletme maliyetleriyle çalışan ve para sıkıntı çeken yardım kuruluşları için çekici bir seçenek olarak görülmektedir[95]. Açık sistem (tüm dünyadan erişilebilen) ödeme hizmeti olan Bitcoin gelişmiş ve gelişmekte olan ülkelerde yaşayan düşük gelirli insanların kürel ölçekte finansal hizmetlere erişimini çok ucuza sağlayabilmektedir.

Bitcoinlerin toplam arzı belli olduğu ve değiştirilemeyeceği için Bitcoin aynı zamanda katı sermaye kontrolleri olan ülkelerde yaşayan insanlara rahatlama sağlayabilmektedir. Ayrıca, ülkeler arasında işlemleri geri çevirecek veya bitcoinlerin takasını engelleyecek merkezi bir yönetim yoktur. Bu nedenle Bitcoin ülkelerinin değeri düşürülmüş parasına veya dondurulmış sermaye piyasalarına alternatif arayan insanlara bir çıkış noktası sağlamaktadır. Sermaye kontrollerinin ve merkez banaksının hatalı uygulamalarının zarar verici etkilerinden kaçınmak için insanların Bitcoin'i tercih ettiği örnekler bulunmaktadır. Örneğin bazı Arjantinliler, 2013 yılında devletin aldığı kararla yüklenen %25'lik enflasyon ve katı sermaye kontrollerine tepki olarak Bitcoin kullanmaya başlamıştır[96]. Aynı dönem Arjantin'de tüketici güven endeksi de düşmeye başlamıştır[97]. Bugün Arjantin'de bitcoin yasal para birimi olarak görülmese de kullanımı yasaldır. Aralık 2017'de vergi yasalarında yaptıkları değişiklikle bitcoin herhangi bir mal veya hizmet olarak görülmekte ve bitcoin alımından ve satımından elde edilen gelir vergiye tabi tutulmaktadır[98].

---

[95] Kyle Torpey, "Chris Odom Explains How Open Transactions Make Altcoins Irrelevant at Inside Bitcoins Conference", CryptoCoinsNews, 2014, (çevirimiçi) https://www.ccn.com/chris-odom-explains-how-open-transactions-makes-altcoins-irrelevant-at-inside-bitcoins-conference/, (erişim tarihi 15.07.2018).

[96] Jon Matonis, "Bitcoin's Promise in Argentina," Forbes, 2013, (çevirimiçi) https://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/#77e0d21933d5, (erişim tarihi 15.07.2018)

[97] Roberto A. Ferdman, "Argentina's Unofficial Consumer Confidence Metric Is Free-Falling Again", Quartz, 2013, (çevirimiçi) https://qz.com/138498/argentinas-unofficial-consumer-confidence-metric-is-free-falling-again/, (erişim tarihi: 15.07.2018)

[98] USA The Law Library of Congress, Global Legal Research Center, "Regulation of Cryptocurrency Around the World", 2018, (çevirimiçi) https://www.loc.gov/law/help/cryptocurrency/argentina.php, (erişim tarihi: 15.07.2018)

Baskı altındaki ve acil durumdaki kişiler de Bitcoin'in sağlayabildiği finansal gizlilikten faydalanabilmektedir. Bitcoin geleneksel olarak nakit para ile sağlanan gizliliği dijital transfer özelliği eklenmiş yeniliğiyle yapabilmektedir.

2.11.5 Finansal ve Teknolojik Yeniliklere Teşvik Etmesi

Bitcoin'in en faydalı kullanımlarından biri yenilikler için bir platform oluşturmasıdır. Bitcoin protokolü programcıların kolayca geliştirebileceği finansal ve yasal hizmetler için yararlı sayısız dijital plan içermektedir. Bitcoinler temelinde veri paketleri olduğu için sadece para transferi değil aynı zamanda menkul kıymetler, bahis, hassas bilgilerin transferinde de kullanılabilmektedir[99]. Bitcoin protokolü yapısında bulunan özelliklerden bazıları mikro ödemeler, anlaşmazlık aracılığı, güvence sözleşmeleri ve akıllı mülkiyettir. Anlaşmazlık aracılığı (dispute mediations) işlem yapan tarafın birbirine güvenmediği durumlarda alan veya satanın 3.bir tarafı işleme dahil etmesidir. Örneğin kitap alan birinin bitcoinlerini 3.birine (escrow) göndermesi ve kitap satanın kargo makbuzunu 3.kişiye (escrow) yollaması durumunda, 3.kişinin kitap alanın parasını, kitabı satana iletmesi gibi birbirine güvenmeyen iki tarafın 3.tarafın arabuluculuğu hizmetiyle (escrow service) işlemlerini tamamlamasıdır. Güvence sözleşmeleri (assurance contracts) bir kamu malının yapılabilmesi için yapılan fonlama yöntemidir. Fonlama sonu elde edilen para ile yapılan kamu malını herkes bedava kullanabilmektedir. Bu model Bitoin'de şöyle işlemektedir: Bir gişimci örneğin yeni bir adres oluşturur ve herkese en az 1000BTC toplanırsa bu malın yapılacağını duyurur. Katılmak isteyen herkes kendi katılımını içeren bir işlem oluşturur ve bu adrese gönderir ama bunu (ağın onaylaması için ağa duyurmazlar) adreste toplanan tüm işlemler 1000BTC olduğunda birleştirilip tek işlem olarak ağa onaylanması için duyurulur. Kitle oyunu (Crowdacting) olarak da adlandırılmaktadır[100]. Akıllı mülkiyet (Smart property) sahipliği sözleşmeler yoluyla Bitcoin kayıt zinciri tarafından kontrol edilen araba, telefon veya ev gibi fiziksel varlıklardır. Akıllı mülkiyet bir şirketin hisse senedi, uzaktan bir bilgisayara erişim hakları gibi fiziksel olmayan hakları da içermektedir. Mülkiyetin akıllı yapılması ticaretinin tamamıyla daha az güvenle

[99] Jerry Brito, "The Top 3 Things I Learned at the Bitcoin Conference," Reason, 2013, (çevirimiçi) http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoin; (erişim tarihi 16.07.2018)

[100] Arvind Narayanan ve diğerleri, Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016, ISBN9781400884155.

yapılabilmesine olanak vermektedir. Bu sahteciliği, aracılık masraflarını azaltmakla beraber aksi halde olması mümkün olmayan işlemlerin gerçekleşmesine olanak vermektedir. Örneğin, tanımadığınız insanların internet üzerinden bir varlığınızı teminat olarak alarak size ödünç para vermesini sağlamaktadır. Bu borç verme yöntemi finansman hizmetinin daha rekabetçi ve böylelikle daha ucuz olmasını sağlamaktadır[101]. Bununla ilgili bir diğer kavramsa akıllı sözleşmelerdir (smart contracts). Akıllı sözleşme, bir sözleşmenin yerine getirilmesini veya iştirasını dijital olarak sağlayan, kanıtlayan veya yaptıran bir bilgisayar protokolüdür. Akıllı sözleşmeler 3.taraflar olmadan mal veya hizmetin sahipliğinin takasını belirli bir şartın yerine getirilmesi koşuluyla sağlamaktadır. Bu sözleşmeler izlenebilir ve geri alınamazlar. (Merkezi olmayan kripto para protokolleri, Bitcoin, Ethereum, RootStock (RSK), Namecoin, Ripple akıllı sözleşmelere örnektir[102]. Bu özellikler küçük işlemleri anında yapan internet aktarım hizmetlerinin gelişimine olanak sağlamıştır. Örneğin WiFi ölçme programları sabit bir modem çevresindeki sinyalleri gösterebildiği gibi ölçümlerini de birkaç saniye içerisinde aktararak kullanıcıların doğru kanalı, doğru modu seçerek modemlerinden en iyi verimi almalarını sağlamaktadır[103]. Kickstarter gibi kitle fonlaması uygulamaları da internet aktarım hizmetlerine örnektir. Kickstarter New York'ta yerleşik, moda, dans, video, fotoğrafçılık, oyun, tasarım film, teknoloji ve müzik gibi farklı alanlarda projeleri bulunan ama yeterli sermayesi olmayanlara destek sağlayan dünya genelinde bir bağış sitesidir. 3.taraf internet hizmet sağlayıcısı veya telefon şirketi olmadan bilgisayar ve araçların birbirlerine doğrudan bağlanmalarını sağlayan dağıtık mesh bilgisayar ağları da internet aktarım hizmetlerine örnektir[104].

İlk başlardaki girişimlerden bugün hayata geçirilip aktif bir şekilde kullanılmakta olanlar bulunmaktadır. Kitle fonlaması platformu Pozible, 2013 yılında çok küçük bir işlem masrafı karşılığında proje yapımcılarının bitcoins cinsinden mikro yardımları

---

[101] Houman Shadab, "What Are Smart Contracts, and What Can We Do with Them? A Backgrounder for Policymakers," Coin Center, 2014, (çevirimiçi) https://coincenter.org/entry/what-are-smart-contracts-and-what-can-we-do-with-them, (erişim tarihi 16.07.2018).

[102] Nick Szabo, Smart Contracts, (çevirimiçi) http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, (erişim tarihi: 16.07.2018)

[103] Hamza Şamlıoğlu; "NetSpot WiFi Durumu ve Kablosuz Sinyali Ölçümü", TEAkolik Blog, 2016 (çevirimiçi) https://www.teakolik.com/netspot-wifi-durumu-ve-kablosuz-sinyali-olcumu/, (erişim 17.07.2018)

[104] Şafak Durukan Odabaşı, Kablosuz Mesh Ağlar, Yönlendirme Metrikleri ve Protokolleri, Akademik Bilişim Konferansı Bildirileri, İnönü Üniversitesi, Malatya, 2011, (çevirimiçi) https://ab.org.tr/ab11/kitap/_AB11_tek.pdf (erişim tarihi 28.04.2018).

toplamalarına imkan vermiştir[105]. Swarm gibi merkezi olmayan platformlarda kayıtzinciri teknolojisi girişimcileri ve yatırımcıları buluşturarak projelerin kitle fonlaması ile hayata geçirilmesine olanak sağlamıştır. Tüm ağın temeli ve ağı çalıştıran yazılım olan orijinal Bitcoin istemcisi Bitcoin Core geliştiricilerine prim sağlama amaçlı kurulan Lighthouse açık kaynak projesi, benzeri bir proje olmakla beraber bu primler diğer projelerin desteklenmesinde de kullanılabilmiştir. Hayır kurumlarına sağlık malzemeleri satın almak ve GnuPG şifreleme yazılımı, Lighthouse kitle fonlaması ile sağlanmış başarılı uygulamalara örnektir. Yazılım ve teknoloji geliştiricilerinin projelerine kaynak sağlayabilmeleri için mikro ödemeler almalarını imkan veren BitHub platformu 2013 yılında oluşturulmuştur. Açık kaynaklı ödeme platformu Bitmonet internet içeriği tasarımcılarının blog veya portföylerinden bitcoin geliri sağlamalarına yardımcı olmuştur. Bitcoin ekonomisi oturdukça bu tarz yenilikçi uygulamalar hayata geçmeye devam edecektir.

Bitcoin aynı zamanda finansal yeniliklerin getirdiği karmaşık yöntemleri kolaylaştırmaktadır[106]. Profesyonel bitcoin türev ürünler borsaları lisans ve yönetim ruhsatları için başvurma ve alma sürecine başlamış veya tamamlamıştır. TeraExchange, LedgerX, Cantor Exchange, Nadex, trueEX bugün vadeli işlemler ve opsiyon piyasalarında faaliyet gösteren takas ofisleridir. Nasdaq Inc. de bitcoin vadeli sözleşmeler piyasasına girmeyi düşündüğünü açıklamıştır. TeraExchange kullanılabilir tezgahüstü swaplar için hem merkezi limit fiyatlı emirler (CLOB) ve emir iletim hizmetleri sunan ticari bir platformudur. TrueEX bitcoin fiyatlarına bağlı "teslim edilemeyen vadeli işlem" (non-deliverable forward) ürününü sunmaya hazırlandığını belirtmiştir. Bu sözleşmeler döviz piyasasında sık kullanılmaktadır. İki tarafın örneğin dolar ve Euro gibi iki farklı para birimi karşılığı bir miktarı gelecekte birbirilerine ödeme yapmak üzere anlaşmalarına imkan vermektedir. Yasal olarak düzenlenme süreçleri hala belirsiz olmakla beraber ICBIT Trading, MPEx (aynı zamanda bitcoine dayanan menkul kıymetler borsası hizmeti veren), Magnr (eskiden BTC.sx) gibi sayısız

[105] JD Alois, "Pozible Now Allowing Bitcoin for Crowdfunding Pledges," Pozible, 2013, (çevirimiçi) https://www.crowdfundinsider.com/2013/10/25251-pozible-allowing-bitcoin-crowdfunding-pledges/. (Erişim tarihi: 17.07.2018)

[106] Jerry Brito ve diğerleri "Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling," Columbia Science and Technology Law Review, 2014, Columbia Law School, SSRN Paper, Elsevier, 2014, sayı 16, s.144–221.

girişimci kuruluş, yıllardır dolar veya başka bir itibari para değil bitcoin karşılığı alınıp satılan bitcoin türev ürünlerini sunmaktadır.[107]

Bitcoin cinsinden hisse senedi paylarının alınıp satıldığı internet siteleri bulunmaktadır. Bazı girişimci firmalar bu siteleri bitcoin karşılığında sermayelerini arttırmak ve hisse senetlerini satmak için kullanmaktadır. Bu tipteki takas bürolarının listelerinde yer alan firmalar ve fon kuruluşları örneğin çıkarma işi (madencilik) için gerekli ekipmanı sağlayan üretici firmaları gibi genellikle bitcoin ile alakalı işlerle ilgili faaliyette bulunan firmalardır. Söz konusu ofisler aynı zamanda Satoshi Dice ve BitBet gibi bitcoinle çalışan bahis sitelerini de içermektedir. Bitcoin hisse senetleri piyasasının bu karışık yapısı yatırımcılara tazmin hakkının çok az olduğu sahtecilik ve dolandırıcılık girişimlerine sebebiyet verebilmektedir. Buna örnek bir durum artık bulunmayan Global Bitcoin Stock Exchange (GLBSE) borsasında yer alan firmalardan biri olan Bitcoin Savings and Trust (BTCST) fon kuruluşunda yaşanmıştır. ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) tarafından açılan bir federal davada BTCST kuruluşunun Ponzi sahtekarlığı yaptığına karar verilmiştir[108]. Bundan farklı olarak MPEx menkul kıymetler borsası gibi platformlar aktif bir şekilde yeni başlayan yatırımcıları karmaşık arayüze sahip sitelerde işlem yapmaktan caydırmakta ve dönemsel hissedar raporları ile şeffaflığı desteklemektedir. Kendi kendini düzenleyen piyasa olarak sınıflandırılan bitcoin tabanlı türev ürün ve hisse senedi piyasaları ilgili yargı kuruluşları tarafından yapılacak yasal incelemelerle karşılaşmaya devam edecektir.

Yazılımcılar ve girişimciler Bitcoin teknolojisini kullanarak aynı zamanda tahmin piyasaları kavramını geliştirmişlerdir. Tahmin piyasaları (aynı zamanda öngörücü piyasalar, bilgi piyasaları, karar piyasaları, tahminli vadeli işlem piyasaları[109], olaya dayanan türev piyasalar veya sanal piyasalar olarak da bilinen) olayların sonuçları üzerinden işlem yapma amacıyla oluşturulmuş borsalardır. Tahmin piyasalarına bir

---

[107] Alexander Osipovich, "Another Exchange Jumps on Bitcoin Bandwagon", The Wall Street Journal, 2018, (çevirimiçi) https://www.wsj.com/articles/another-exchange-jumps-on-bitcoin-bandwagon-1520868955, (erişim tariihi 21.07.2018).

[108] Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, Civil Action No. 4:13-CV-416 (E.D. Tex. 2014), http://www.law.du.edu/documents/corporate-governance/securities-matters/shavers/SEC-v-Shavers-No-4-13-CV-416-E-D-Tex-Sept-18-2014.pdf. (erişim tarihi 02.08.2018)

[109] Robin Hanson, "Idea Futures (a.k.a. Prediction Markets, Information Markets)", 1992, (çevirimiçi) http://mason.gmu.edu/~rhanson/ideafutures.html, (erişim 02.08.2018)

örnek olarak bir rastgele sayı üretecinin birini bir bitcoin kazananı yapıp yapmayacağı üzerine tahminlerin yapıldığı BitBet gibi bahis siteleri gösterilmektedir[110]. Daha karmaşık ve sosyal anlamda yararlı tahmin piyasaları bireylerin gelecekte olmasını bekledikleri politik, ticari, spor ve kültürel olayların sonuçları üzerine tahminde bulunmalarına izin vermektedir. Bireylerin kendi düşünceleri üzerine tahminde bulunabilmelerine izin vermekle tahmin piyasaları insanları ilgili bilgiyi paylaşmaya ve önemini anlamaya teşvik ederek olayların olasılıkları ile ilgili yararlı fikirlerin ortaya çıkmasını sağlayabilmektedir. Buna başarılı bir örnek olarak Bitcoin olmayan popüler tahmin piyasası Intrade gösterilmektedir. Intrade'in Amerikan seçim sonuçları ile ilgili bulguları politik projeksiyon uzmanlarının görüşlerinden çoğunlukla daha doğru sonuçlar vermiştir[111]. Intrade çalışmaları, ABD Emtia Vadeli İşlemler Komisyonu (CFTC) tarafından yasal olmayan bir şekilde vadeli işlem sözleşmeleri sattıkları için dava edildikten sonra durmuştur. Ancak tahmin piyasaları Predictious.com, BTCOracle ve Bets of Bitcoin gibi platformlarda devam etmektedir. Ethereum platformunda kurulmuş olan Augur tahmin piyasası Ekim 2016'da başlatılmıştır. Tahmin piyasaları, ikili alım satım opsiyonlarına benzedikleri ve hepsi ya da hiçbiri prensibi üzerine dayandıkları için Augur platformunda, kullanıcılar sadece doğru sonucu tahmin ettiklerinde ödül almakta ve bilgileriyle katkıda bulundukları için de ödüller kazanmaktadırlar. Örneğin bir kullanıcı herhangi bir olayın sonucu olarak hisse satın alabilmektedir. Fiyat, gelecekteki etkinliğin gerçekleşmesi olasılığı üzerine belirlenmekte ve belirli bir sonucun fiyatı ise daha fazla insanın bu sonucu almasıyla artmaktadır[112]. İnsanların bilgilerini alıp sattıkları bu katıksız bilgi piyasaları Bitcoin teknolojisinin kullanımıyla işlemektedir.

Bitcoin'in temel yeniliği bilginin düzenlenmesini, doğrulanmasını ve kaydedilmesini dağıtık biçimde sağlayan kayıtzinciri defteri teknolojisidir. Bu yenilik herkes tarafından anlaşıldığında kendi dijital para birimlerine uyarlayabilmelerine imkan verecek özelliktedir. Yazılım geliştiriciler ve girişimciler Bitcoin'in uzlaşıya varma yöntemini

[110] Jerry Brito ve diğerleri, Bitcoin: A Primer for Policymakers, Mercatus Center, George Mason University, 2.basım, 2016.
[111] CFTC Charges Ireland-based "Prediction Market" Proprietors Intrade and TEN with Violating the CFTC's Off-Exchange Options Trading Ban and Filing False Forms with the CFTC. https://www.cftc.gov/PressRoom/PressReleases/pr6423-12, erişim tarihi 14.08.2018
[112] Jack Peterson ve diğerleri, "Augur: a Decentralized Oracle and Prediction Market Platform",3 Şubat 2018, (Çevirimiçi) http://www.augur.link/augur.pdf, (Erişim tarihi 14.08.2018)

bir üst seviyeye taşıyarak farklı şekillerde uygulamaktadırlar. Bitcoin'in doğuşu ile alternatif madenler grubu veya altmadenler hızla çoğalmaya başlamıştır[113].

Bitcoin'in en bilinen altmadenlerinden biri olan Litecoin, Bitcoin sistemine oldukça benzemekle beraber önemli farklılıklar içermektedir. Tasarımında, çıkarma (madencilik) sürecinde Bitcoin'de olduğu gibi donanım gücü gerektirmeyen alternatif bir maden oluşturabilmek için uzlaşı yöntemi olarak Bitcoin'deki SHA-256 fonksiyonu yerine "scrypt" fonksiyonunu kullanılmıştır[114]. Zcash projesi Bitcoin ile aynı işlevselliği sağlayan gizliliği ve takas edilebilirliği arttırılmış yeni bir kripto para düzenlemeyi hedeflemektedir[115]. Kripto para dünyasında internet şakaları bile dikkatleri çekebilmek için kullanılabilmektedir. NASCAR sponsorluğunda piyasaya kazandırılan Litecoin'in bir benzeri olan Dogecoin, "dog" (İngilizce köpek) yerine yanlışlıkla "doge" yazılması ile başlayan ve internette uzun bir süre dikkatleri toplayan Doge karikatürlerinde ismi geçen Shiba Inu cinsi köpeği logo olarak kullanmıştır. Sonuç olarak. 2009 yılında Bitcoin ile başlayan kripto para piyasasında sayısız altmadenler oluşturulmuş ancak bunlardan çok azı piyasada 1 milyonun üzerinde toplam hisse değerine sahip olmuştur. İlk olması nedeniyle Bitcoin'in ağ etkisi diğer kripto paralardan daha fazla olmakla birlikte piyasa değeri, kullanıcı sayısı, işlem sayısı, ağ üzerindeki bilgi işlem kapasitesi ve benzeri açılardan rakipleri içinde büyüklük sıralamasında önde gelmektedir. Tablo 16'da piyasadaki toplam hisse değeri 1 milyar dolardan fazla olan kullanımdaki kripto para birimleri ve uzlaşı yöntemlerinde kullandıkları özet fonksiyonlar verilmiştir.

---

[113] Lawrence H. White, "The Market for Cryptocurrencies" (GMU Working Paper in Economics No. 14-45, December 15, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538290. erişim tarihi 1582018

[114] Adam B. Levine, "Episode 71: Blockchain Tools and Litecoin Devs," (interview with Charlie Lee) Let's Talk Bitcoin!, December 31, 2013. https://tr.scribd.com/document/232718300/Let-s-Talk-Bitcoin-Episode-71-Blockchain-Tools-and-Litecoin-Devs. erişim tarihi 27.08.2018

[115] Eli Ben-Sasson ve diğerleri., "Zerocash: Decentralized Anonymous Payments from Bitcoin," Proceedings of the 2014 IEEE Symposium on Security and Privacy, May 18, 2014 https://www.researchgate.net/publication/286668243_Zerocash_Decentralized_Anonymous_Payments_from_Bitcoin. erişim tarihi 27.08.2018

Tablo 16. Piyasa Değeri 1 milyar dolardan fazla olan Kripto paralar ve algoritmaları

Kripto Para Adı ve	Piyasa Değeri (Dolar)	Fiyatı (dolar)	Kullandığı Özet Fonksiyon	Çıkış Tarihi
Bitcoin-BTC	116.419.561.269	6.755,03	SHA-256	2009
Ethereum-ETH	28.323.548.274	278,80	Dagger-Hashimoto	2015
XRP- XRP	12.996,32	0,328817	ECDSA	2013
Bitcoin Cash-BCH	9.205,21	531,60	SHA-256	2017
EOS- EOS	4.709.930.098	5,20	DPOS	2017
Stellar-XLM	4.109.188.550	0,218889	Rippleruen	2017
Litecoin-LTC	3.355.011.187	57,81	Scrypt	2011
Tether-USDT	2.817.504.153	1,00	SHA-256	2014
Cardano-ADA	2.517.741.218	0,097109	Ouroboros	2017
IOTA-MIOTA	1.652.798.631	0,594632	IRI	2018
Monero-XMR	1.594.135.174	97,47	CryptoNight	2014
TRON- TRX	1.571.123.202	0,023896	ECDSA	2018
Ethereum Classic-ETC	1.301.232.390	12,50	Dagger-Hashimoto	2015
Dash-	1.263.625.413	152,59	X11	2014
NEO- NEO	1.228.161.703	18,89	DBFT	2014
Binance Coin- BNB	1.052.251.615	11,02	Ethash	2017

Kaynak: Coinmarketcap.com

Programcılar, Internette TCP/IP protokolleri ile çalışan web sitesi ve e-posta veri iletimlerinde olduğu gibi Bitcoin protokolünü tamamlayan veya onun üzerinde çalışan alternatif protokoller geliştirebilmektedir. Birçok proje Bitcoin protokolü ile doğrudan arayüzlenen yazılım geliştirmeye çalışmaktadır. Örneğin Renkli Madeni Paralar (Colored Coins) projesi kullanıcılarına Bitcoin protokolü üzerinde, bellirli bitcoinleri renklendirerek gerçek dünyadaki altın, mülk veya emtiaları temsil eden sonrasında bu varlıkların ağ üzerinden alınıp satılabilmesini sağlayan yazılım katmanı geliştirmiştir.

2015 yılında Nasdaq, renkli madeni para özelliğini, Bitcoin kayıt zinciri üzerinde menkul kıymetlerin transferi ve basımı için kullanmayı planladığını duyurmuştur. 2015 yılı sonlarında Nasdaq'ın özel pazarlar kayıtzinciri projesi Linq, 6 yeni firma ve yatırımcı tarafından ticari varlık ve tasarruf yönetimi aracı olarak denenmiştir. Bir başka programcı Bitcoin protokolü üzerinde, özel belgelerin güvenilir ve gizli bir şekilde "varlık ispatının" tutulduğu dijital bir noter hizmeti oluşturmuştur. Bitcoin protokolünden önce yapılmış olan Açık İşlemler Platformu (The Open Transactions platform), Bitcoin protokolünde hiçbir değişiklik gerektirmeksizin, dijital para işlemlerinin güvenirliliğini ve gizliliğini arttırmak için Chaumian'ın izi sürülemeyen para tekniklerini ve birleşmiş sunucular sistemini kullanmaktadır.

Diğer projeler kayıtzinciri yeniliğine ilişkin farklı bir yaklaşım denemektedir. Bitcoin ağını büyütme ve iletişim kurmak için yazılım geliştirmek yerine bu programcılar kendi istedikleri parasal olmayan fikirleri için yeni kayıtzincirleri oluşturmaktadır. Örneğin, Bitmessage takımı Bitcoin modelini dijital iletişimi şifreleme yolu olarak kullanmıştır. Bitcoin yazılımının ilk ayrımı veya türevi olan Namecoin, kayıt zinciri teknolojisine dayanan, internette ana yönlendirme hizmetini sağlayan hiyerarşik Alan İsmi Sisteminin (DNS) teoride merkezi olmayan bir şekilde yerini alan dağıtık açık kaynaklı bilgi kayıt sistemidir. Ödeme işlemcisi BitPay'in Foxtrot uygulaması kayıt zinciri yöntemlerini kullanarak merkezi olmayan bir mesh bilgisayar ağını oluşturmayı amaçlamaktadır.

Diğer araştırmalar genel olarak kayıt zinciri teknolojisini bilgi işlemi dağıtmaya yönelik çalışmalarda kullanmaya odaklanmaktadır. Bu tarz projeleri anlamaya yönelik en başarılı örnek bulut bilişimin gelişimidir. Yıllardır çoğu uygulama masa üstü bilgisaylarlarda kullanılmaktadır. Daha karmaşık işlemler kullanıcının çevresindeki fiziksel sunucular yardımıyla sürdürülmektedir. Ancak çoğu bilgisayar kullanıcısı en önemli verilerini kişisel sabit sürücülerinde saklanmakta ve o verilere ulaşmayı sağlayan uygulamalarsa yine kişinin sadece kendi bilgisayarında çalışmaktadır. Bu sabit sürücünün bozulması durumunda tüm veriler daha önceden yedekleri alınmamışsa kaybolmaktadır. Bulut bilişimin gelişi tüm bunları değiştirmektedir. Bugün, uygulamalar ve veriler hızla buluta aktarılmaktadır. Kişinin sadece kendi bilgisayarında çalışan Microsoft Word programı yerine bir internet tarayıcısında çalışan Google Dokümanlar uygulaması kulllanılabilmektedir. Aile fotoğraflarını sabit sürücüde

saklamak yerine Flickr veya Facebook uygulamaları hem saklamak hem de paylaşmak için kullanılabilmektedir.

Ethereum ve MaidSafe gibi projeler bulut bilişim mantığını dağıtık sistemlere genişletmeyi amaçlamaktadır. Bulut sunucu tutabilmek için HP, Amazon veya Miscrosoft programlarına dayanmak yerine kayıt zinciri teknolojisi benzeri işlevleri dağıtık bilgi işlemle (distributed computing) sağlamaktadır. Bu yazılımcılar, şifreleme bilimi ile dağıtık uzlaşı mekanizmalarının, girişimcilerin ve programcıların yeni uygulamaları, para birimlerini ve işletme modellerini düşük maliyetle ve güvenilir üçüncü taraflara daha az bağımlılıkla tecrübe edebildikleri platformları oluşturduğu bir geleceği öngörmektedir. Bu, bulut uygulamaların, tıpkı YouTube veya Google Dokümanlarda olduğu gibi yine bulutta çalışmaya devam edeceği ancak bugün Google sunucularının kullandığı "bulut" metaforu yerine herhangi bir merkezi otorite tarafından kontrol edilmeyen binlerce dağıtılmış bilgisayarın paylaştığı kaynakların oluşturacağı ortak bir bulut anlamına gelmektedir.

2.11.6 İçsel Yenilenme ve Değişkenlik

Topluluğa dayalı bir proje olarak Bitcoin, yazılımın ağ kullanıcılarının uzlaşımıyla yazılım geliştiriciler tarafından geliştirilmesi ve değiştirilmesiyle yenilenmektedir. Aynı zamanda bitcoin fiyatı, güncel olaylar fiyatı etkilediği için dalgalanmaya devam etmektedir. Bazı önemli fiyat değişikliklerinin, olumlu medya ilgisinin yatırımcıların dikkatini çekmesiyle oluşabilen bir geleneksel spekülatif balona benzediği söylenmektedir[116]. Bu durum bitcoinlerin tasarruf aracı olarak ne kadar iyi olduklarının belirlenmesini zorlaştırmakta ve bitcoin kabul eden işletmeler bu nedenle bitcoinleri dolaşımdaki paraya oldukça hızlı bir şekilde çevirmektedir. Araştırmacılar Bitcoin dünyasındaki davranışları açıklamayı deneyen modeller üzerinde çalışmalara başlamış olsalar da aynı zamanda geniş çapta erişimi olan ilk kripto para olduğu için Bitcoin ekonomisinin gelecekte nasıl olacağını tahmin etmek de zor olmaktadır. Bununla beraber Bitcoin'in tanınması zamanla arttıkça bitcoin değerinin daha az değişken olması mümkün olabilmektedir.

[116] Felix Salmon, "The Bitcoin Bubble and the Future of Currency", 2013, (çevirimiçi) https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb. (Erişim tarihi 14.08.2018)

2.12 Bitcoin'in Riskleri

Faydalarına karşın Bitcoin'in potansiyel kullanıcıların göz önünde bulundurması gerektiği zarar olasılığı gösteren yönleri bulunmaktadır. Oluşturulduğu zamandan bu yana büyük ölçüde fiyat istikrarsızlığı sergilemektedir. Yeni kullanıcıların dikkatli olmadıkları müddetçe hatalı saklama ve hatta yanlışlıkla bitcoinlerini silme riskleri bulunmaktadır. Ek olarak olası sistem saldırılarının bitcoin ekonomisini zayıflatıp zayıflatmayacağı yönünde endişeler bulunmaktadır.

2.12.1 Suç Faaliyetlerinin Kolaylaştırılması

Bitcoin'in sağladığı takma adlılık ve ödemelerin kolaylığı kanun uygulayıcıların suç faaliyetlerinin kolaylaştırılmasında Bitcoin kullanımıyla ilgilenmelerini kaçınılmaz hale getirmiştir. Gerçekten de Bitcoin'in suç unsuru içeren en bilinen kullanımı yasadışı uyuşturucu madde ve sahte pasaport satışının yapıldığı bir karaborsa olan Silk Road internet sitesinde olmuştur. Silk Road, Bitcoin ödemeleri ile kullanıcısının izinin sürülmesini engelleyen Tor ağını beraber kullanarak benzeri yasal olmayan mallar ve hizmetler için bir pazar yaratmıştır[117]. Bitcoin'e dair dikkati çeken bir diğer önemli husussa kara paranın aklanması ve terörist faaliyetlerin finanse edilmesindeki kullanımıdır. Bu konulara ilgi özellikle özel ve merkezi bir dijital para olan Liberty Reserv'in kara para aklama iddiasıyla kapatılmasından sonra ivme kazanmıştır[118]. Ancak bitcoinler de itibari para gibidir ve paranın da hem yasal hem de yasadışı amaçlarla kullanılabildiğinin unutulmaması gerektiği önemlidir. Bitcoin oluşturulmadan önce de diğer para transfer yöntemleriyle suç gelirlerinin ve kara paranın aklanmasının finansmanı yapılmaktaydı. Ancak, çoğu Bitcoin borsasının, müşterilerin kaydını tutma gibi kara paranın aklanmasının engellenmesine yönelik önlemleri iş uygulamalarına dahil etmeleri Bitcoin'in suçlularca cazip bulunmasını azaltmaktadır.

Bitcoin, aynı zamanda geleneksel paradan farklı olarak bazı finansal suçlara karşı koruma sağlamaktadır. Örneğin, çifte harcama sorununu çözen, işlemlerin doğrulandığı

[117] Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable", 2011, (Çevrimiçi) http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 (Erişim Tarihi: 25.01.2018).
[118] Paul Rubens, "Liberty Reserve: Criminals face online cash dilemma", 2013, (Çevrimiçi) https://www.bbc.com/news/technology-22766406 (Erişim Tarihi: 25.01.2018).

çıkarma (madencilik) süreci aynı bitcoinin birden fazla kullanılmasını veya sahteciliği oldukça zorlaştırmaktadır. Kötü niyetli kişinin, varolan ve gelecekteki işlemleri ağın geri kalanı farketmeden değiştirebilmesi için ortak bilgisayar ağı gücünün üstesinden gelebilecek yeterli bilgisayar gücünü toplaması gerekmektedir.

2.12.2 Yasal Düzenleyici Yaklaşım

Bitcoin yeni olduğu için yasal uygulayıcıların yaklaşımı yapılan yasaklamalara karşı müdahaleci olmamalarıdır. Devletler Bitcoin'in ülkelerine olan faydaları ve riskleri ile karşılaştıkça yasal düzenlemeler değişmeye devam etmektedir. Başlangıç olarak bazı hükümetlerde yasal düzenleyiciler ülkelerinde dijital paraya yönelik uygulamalara yönelik özellikle kara para aklanmasının engellenmesi ve terörizmin finansmanı ile mücadele ve aynı zamanda vergilerle ilgili değerlendirmelerde kurallar koymaya ve yönlendirmelerde bulunmaya başlamıştır. Düzenleyici kuruluşların çalışmaları faydalı kullanıcıları ve ilerideki gelişmeleri teşvik ederken yüklenen riski en aza indirmeye yönelik olmaktadır.

Yasa ve düzenlemeler Bitcoin gibi bir teknolojiyi kapsamamaktadır. Bu nedenle bugün Bitcoin yasal bir gri bölgede bulunmaktadır. Bitcoin, varolan para birimi, diğer finansal araçlar veya kuruluşların yasal tanımlarına tam olarak uymamaktadır. Bu durum hangi kanunun ve nasıl uygulanacağını belirsiz hale getirmektedir.

- **Dünyadaki Kripto Para Düzenlemeleri**

Tüm dünyadaki yasal düzenleyicilerin 2018 yılında karşılaştıkları en büyük sorunlardan biri genel itibari ile kripto para ve kayıt zinciri teknolojisi olmaktadır. Halen hiçbir ülkede kripto paralarla ilgili tüm yasal meseleleri kapsayan bir kılavuz olmamakla beraber yetkililer yeni teknolojiyi aktif bir şekilde yasal sınırlar çerçevesinde idare etmeye çalışmaktadır. Bugün, bu faaliyetler çoğunlukla yasalarla düzenlenmemiş olduğundan yetkililer ya bunları yasaklamaya ya da yasal amaçlı kullanımlarına göz yummaya mecbur kalmaktadırlar. Çin gibi, risk almak istemeyen ülkeler benzeri aktiviteleri tamamen yasaklarken sermaye ihracı riskini göz ardı etmek istemeyen diğer ülkeler işletmelerin gri alanda uygun yasalar getirilinceye kadar çalışmalarına müsade etmektedirler.

Yasal düzenleyicilerin karşılaştıkları birçok zorluk bulunmaktadır. Öncelikle emsal teşkil edebilecek başka bir yasa veya örnek alınabilecek bir başka ülke bulunmamaktadır. Düzenleyicilerin en baştan başlayarak uygun bir çerçeve belirlemeleri gerekmektedir. İkinci olarak, oldukça ilerlemiş bir teknoloji içeren kripto paralar, programlama diline hakim olmayan insanlar için belirsiz kalmaktadır. Bu zamana dek konuyu finansal olarak ele alan yasal düzenleyiciler bu teknolojinin üstesinden gelebilecek ölçüde kalifiye olmayabilmektedir. Teknoloji nispeten yeni olduğu için iş piyasasında da uzman eksikliği bulunmaktadır. Ancak yine de dünyada kripto para düzenlemeleri ile ilgili gelişmeler görülmektedir.

- **Amerika Birleşik Devletleri**

2018 yılı itibariyle kripto para düzenlemesine yönelik Amerika'da tutarlı bir yönelim bulunmamaktadır. ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) kripto para yatırımcılarını riskleri ile ilgili uyarmakta, çoğu ilk dijital para arzını (Initial Coin Offering-ICOs) durdurmakta ve genel ve kapsamlı bir kripto para düzenlemesi ihtiyacını işaret etmektedir[119].

ABD Emtia Vadeli İşlemler Komisyonu (CFTC) kripto para türev araçlarının borsada işlem görmesine izin veren ilk Amerikan düzenleyici kuruluştur. Kripto para türev araçlarının takasına ilişkin kuralların değiştirilmesi ile ilgili toplantılar düzenlemektedir. Ancak bu toplantılardan biri federal hükümet müdahalesi ile kapatılmıştır[120].

[119] Francine McKenna, "Here's how the U.S. and the world regulate bitcoin and other cryptocurrencies", 2017, (Çevrimiçi)https://www.marketwatch.com/story/heres-how-the-us-and-the-world-are-regulating-bitcoin-and-cryptocurrency-2017-12-18 (Erişim Tarihi: 25.01.2018).
[120]Bitcoin Magazine, "Cryptocurrency regulation in 2018: Where the world stands right now", 2018, (Çevrimiçi) https://thenextweb.com/hardfork/2018/04/27/cryptocurrency-regulation-2018-world-stands-right-now/ (Erişim Tarihi: 05.09.2018).

Tablo 17. Amerika'da Otoritelere Göre Yasal Kripto Para Düzenlemeleri

Düzenleyici Otorite	Kripto Para ile ilgili görüşü/düzenlemesi
Menkul Kıymetler ve Borsa Komisyonu (SEC)	SEC kripto para tutan hiçbir borsa yatırım ürününü veya kripto para ile ilgili diğer varlıkların borsaya kote edilme veya işlem görmesini onaylamamaktadır. Hiçbir ilk dijital para arzını tescil etmemiştir.
Emtia Vadeli İşlemler Komisyonu (CFTC)	CFTC bitcoini emtia olarak görmektedir ve sahtecilik ve manipülasyon içeren eyaletlerarası bitcoin takas işlemlerinde ve bitcoine bağlı vadeli işlemler düzenlemerinde yetkili otorite olduğunu açıklamıştır.
Milli Gelirler İdaresi (IRS)	IRS bitcoinin vergi amacına yönelik işleme alınması için varlık olarak görülmesi gerektiğini belirtmiştir. Bu varlık içeren herhangi bir takas olmuş gibi belirli bir sermaye geliri veya kaybının kaydedilmesi gerektiği anlamına gelmektedir. Eğer tekrar satış için tutuluyorsa envanter olarak görülmelidir ve dolayısıyla da olağan bir kazanç veya kayıp olarak kaydedilmelidir. Eğer ödeme olarak kullanılıyorsa bir döviz olarak işlem görmeli ama dönüştürülmeli ve piyasa değeri ile değerlemesi yapılmalıdır.
Eyaletler	Çoğu Amerikan eyaleti bitcoin ve kayıtzinciri teknolojisinin kullanımını ve tesisini onaylamayı planlamaktadır. Arizona (akıllı sözleşmerin kabulü), Vermont (kayıt zinciri) ve Delaware (onay bekleyen kayıtzinciri formatında hisse senedi kayıtları bulunan firmalar) eyaletleri yasalaştırmıştır.
Hazine Bakanlığı	Kasım 2017'de bakanlık denetleme dairesi başkanı, Finansal Suçlarla Mücadele Biriminin (FinCEN) kripto para uygulamalarını para aklama ve terörizmin finansmanı riskleri ile ilgili olduğu için inceleyeceğini belirtmiştir. FinCEN'in FIN-2013-G001 kılavuzunda "sanal paranın hiçbir yetki alanında yasal para statüsünde olmadığı" belirtilmiştir.

Kaynak: Marketwatch, 2018

- **Küresel Düzenleyici Kuruluşlar**

Küresel olarak bitcoin yasal bir ödeme aracı olarak kabul edilmekle beraber ülkeden ülkeye değişiklik göstermektedir[121]. Küresel düzenleyici bir kuruluş ve bitcoin üzerine bir döviz politikası bulunmamaktadır.

- **Avrupa Birliği**

Hiçbir Avrupa Birliği üyesi ülke kendi para birimini getirememekle beraber bitcoinin yasal bir ödeme aracı olarak görülmesi ülkeden ülkeye değişmektedir. Kripto paranın günlük işlem hacminin %4'ü Cryptocompare' göre Euro ile yapılmaktadır[122].

Avrupa Birliği liderlerinin para aklanması ile ilgili endişeleri bulunmaktadır. Avrupa Birliği komisyonu dijital varlıkların paranın aklanması ve yasal olmayan faaliyetlerin finansmanında kullanılması riski taşıdığını belirtmektedir. Komisyona göre sanal borsalar ve cüzdan sağlayıcılar "Kara para aklama yönetmeliği" altında olmalıdır[123].

- **Diğer Belli Başlı Ülkeler**

⇒ **Abu Dabi**

Abu Dabi'de sanal para ve menkul kıymet tokeni ihraççıları ve aracıları, ürün ve hizmetin yapısına bağlı olarak düzenlemeye tabi tutulabilmektedir. Kasım 2017'de Abu Dabi Finansal Hizmetler Düzenleyici Kurumu (FSRA) ilk dijital para arzı (ICO) faaliyetleri ile dijital paranın düzenlenmesine yönelik mevcut Finansal Hizmet ve Piyasalar Düzenlemerine ek talimatname çıkarmıştır.

⇒ **Arjantin**

Merkez Bankasını yasal para çıkarmada tek kuruluş olarak atayan ülke anayasasına göre sanal paralar yasal ödeme aracı olarak kabul edilmemektedir.

---

[121]Kate Rooney, "Your guide to cryptocurrency regulations around the world and where they are headed", 2018, (Çevrimiçi) https://www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html (Erişim Tarihi: 13.09.2018).

[122] Rooney, a.g.e.

[123] Rooney, a.g.e.

⇒ **Avusturya**

Sanal paraları içeren finansal hizmetler yasal olarak düzenlenmektedir.

⇒ **Avusturalya**

Dijital para borsaları 2018 yılının ilk yarısından itibaren kayda ve düzenlemeye tabi olmuştur. Dijital para işlemleri, servis ve hizmetler altında değil, gelir ve sermaye kazançları altında vergilendirilmektedir.

⇒ **Bangladeş**

Bangladeş Bankası kripto para ile yapılan işlemler için uyarı yayınlamış ve resmi olarak bu kullanımların 12 yıla kadar hapis ile cezalandırılacağını belirtmiştir.

⇒ **Belçika**

Belçika Ulusal Bankası, yatırımcıları ve kamuyu yasal paraların taşıdığı riskler hakkında uyarmıştır ve yasal ödeme aracı olarak kabul edilmediğini açıklamıştır. Adalet Bakanlığı sanal para faaliyetlerine katı yaptırımlar uygulamayı planladığını duyurmuştur.

⇒ **Bermuda**

Sanal paralar ve ICO faaliyetlerin 2018 yılından itibaren devlet tarafından düzenlenmeye başlanacağı belirtilmiştir.

⇒ **Brezilya**

Brezilya Merkez Bankası sanal paraların düzenlenmesine yönelik faaliyetlere başlamamıştır ancak kullanımlarıyla ilgili standart uyarılarda bulunmaktadır.

⇒ **Bulgaristan**

Bitcoin satışı veya takasından gelen kişisel gelir vergiye tabidir ve finansal varlıkların satışından kaynaklanan gelir olarak görülmektedir.

⇒ **Kanada**

Kripto para Kanada'da yasal ödeme aracı olarak kabul edilmemektedir ancak teknik olarak menkul kıymet olarak görülmektedir. Dijital para üzerine yasa tasarısı sunan ilk ülkedir ve 2014 yılından bu yana devlet tarafından uygulanmaktadır.

Kanada aynı zamanda kayıt zinciri teknolojisini uygulamaya geçirmekte de aktiftir. Jasper adlı projesi diğer ülkelerce de çalışmaktadır[124]. Kanada Merkez Bankası kayıt zincirini toptan ödeme sistemi için kullanmak istemektedir. Eğer başarılı olursa proje dağıtık kayıt defteri teknolojisini (DLT) bu alanda kullanan ilk kamusal çalışma olacaktır.

⇒ **Çin**

Finansal kuruluşlar ve 3. taraf ödeme hizmet sağlayıcıları sanal paraları kabul etmek, kullanmak veya satmaktan men edilmiştir. Çin Merkez Bankası, bankaları sanal para işlemleri yapan firmalarla çalışmamaları konusunda uyarmaktadır.

⇒ **Almanya**

Sanal paralar Alman anayasasına göre finansal araçtır ve sermaye olarak vergilendirilebilen özel bir para şeklidir. Belirli durumlarda devlet kuruluşlara lisans veya izin vermektedir.

⇒ **Japonya**

Japonya kripto para konusunda Asya bölgesindeki en serbest alanlardandır. Bitcoini yasal bir ödeme aracı olarak kabul eden birkaç ülkeden biridir. Aynı zamanda açık bir şekilde ortaya konmuş dijital para borsalarına kayıt süreçleri bulunmaktadır. Ülkenin diğer alternatif kripto paralara karşı zorlayıcı tutumuna karşın, bu yaklaşımın yalnızca Bitcoin ile ilgili işlemler için olduğuna dikkat edilmelidir.

[124] Aleksandre Natchkebia, "Cryptocurrency regulation around the world in 2018", 2018, (Çevrimiçi) https://www.forexnewsnow.com/forex-analysis/cryptocurrency/cryptocurrency-regulation-overview/ (Erişim Tarihi: 05.09.2018).

⇒ **İsviçre**

İsviçre aktif bir şekilde kendisini kripto para ile ilgili projelerin cenneti yapmaya çalışmaktadır. Ülkenin ekonomi bakanı Johann Schneider-Amann ülkeye "kripto-ulus" demektedir[125]. Ülke ICO girişimleri için merkez olmaya başlamış ve yasal düzenlemeler bu yönde uygulanmaya başlamıştır. Amacı yasal kesinliği arttıran, finasal merkezin bütünlüğünü sağlayan ve teknoloji ağırlıklı düzenleme getirmek olan bir ICO çalışma grubu bulunmaktadır.

⇒ **Singapur**

Singapur, yeni teknoloye has işlemlere karşı oldukça açıktır. Aslında tıpkı Kanada'nın Jasper projesine benzeyen, bankalar arası günlük hesap kapama sürecini kayıt zinciri üzerinde gerçekleştirmeyi amaçladığı bir projesi bulunmaktadır. Yasal olarak düzenlenlenmemiş olsa bile kripto para gibi değer transferi içeren işlemlerin diğer herhangi bir para birimi ile yapılan işlemler gibi görülmesi yaklaşımı bulunmaktadır.

⇒ **İngiltere**

İngiltere'de borsaların para aklama düzenlemeleri altında kayıt olma zorunlulukları bulunmamaktadır. Sanal paralar mal ve hizmet vergileri altında satış kazancı olarak vergilendindirilmektedir.

⇒ **Rusya**

Dijital paraların itibari paranın yerini alacak şekilde kullanımı yasalar çerçevesinde yasaklanmıştır ancak 2017 yılından itibaren kripto para düzenlemelerine yönelik çalışmalar başlamıştır.

[125] Aleksandre Natchkebia, "Cryptocurrency regulation around the world in 2018", 2018, (Çevrimiçi) https://www.forexnewsnow.com/forex-analysis/cryptocurrency/cryptocurrency-regulation-overview/ (Erişim Tarihi: 05.09.2018).

⇒ **Venezuela**

3 Aralık 2017 yılında ülke kendi dijital para birimi olan petrol, gaz, altın ve elmas rezervleri ile desteklenen "petro'yu" oluşturmuştur.

⇒ **Türkiye**

Türkiye'de ödeme hizmetleri ve elektronik paranın bitcoini kapsamadığına yönelik yasa bulunduğu için diğer ödeme hizmetleri ve elektronik para kuruluşları için sayılan güvence ve denetimlerden de yararlanamamaktadır.

2.12.3 Ekonomik Risk

Bitcoin yasal düzenleyicilerin tecrübe ettiği finansal sistemden oldukça farklıdır. Bitcoinin yenilikçi kullanımı varolan finans ve ödeme piyasalarında yıkıcı etkileri olabileceği söylenmektedir. Örneğin Bitcoin para transferi ve kart ödemesi hizmetlerinin ve hatta hisse senedi borsalarının yerini aldığında bu görevi üstlenen hizmet sağlayıcılarına artık ihtiyaç duyulmayacaktır. Bu değişikliklerin hızlı olması finans ve ödeme piyasalarını karıştırma ve nihayetinde de piyasada fiyat istikrarsızlığı riski yaşanması olasılığını arttırmaktadır.

2.13 Dijital Para Döneminin Etkisi

Dijital para döneminin hem dijital hem de fiziksel dünyada pek çok etkisi olacaktır.

2.13.1 Yakın Saha İletişimi

Yakın saha iletişimi (NFC) yoluyla birçok cihaz birbirine bağlanacaktır. Kişilerin yanlarında taşıyabildikleri veya üzerlerine giyebildikleri bu cihazlar onların tercihleri, mevcut sağlık durumu, ne kadar varlığa sahip oldukları da dahil olmak üzere tüm kişisel kayıt bilgilerini içerecektir. Bunun sonucu olarak insanların artık fiziksel cüzdan ve kimlik kartları taşıması gerekmeyebilecektir.

Bu cihazlar bireyleri gözlemleyip sağlık bakımı, eğitim ve finansal hizmetler dahil her yönüyle yaşam tecrübelerini geliştirebilmektedir. Kayıt zinciri teknolojisi

maliyetlerin çıkarma (madencilik) yoluyla paylaşımıyla finansal hizmet maliyetlerini azaltmada önemli bir rol oynayabilir ve bu sayede finansal kuruluşlar, finansal sistemin dışında kalan veya az kullanan nüfusa ulaşabileceği gibi aynı zamanda finansman ihtiyacı olanlara ve kaynak geliştirmek isteyenlere de erişme imkanı bulabilecektir. Tüm bunların hepsi ya merkezi olmayan ya da dağıtık bir şekilde kripto paranın eşten eşe ağı ile yapılabileceği düşünülmektedir. Bu gelişmeler finansal hizmetleri özellikle bankacılığı olumsuz etkileyeceği ve 1990lı yıllarda eCash'in yaptığı gibi kazançlarını azaltacağı söylenmektedir.

2.13.2 Paylaşım Ekonomisi

Paylaşım ekonomisi çoğunlukla çevirim içi işlemleri içeren ekonomik faaliyetleri ifade eden ve pek çok anlamı olan genel bir terim olarak tanımlanmaktadır[126]. Başlangıçta açık kaynak topluluğunun eşten eşe sistemde mal ve hizmetlere erişim paylaşımı kavramından çıkmış olup günümüzde ise daha geniş bir anlamda çevirim içi pazar yerlerinde yapılan eşten eşe olmaktan çok şirketler arası (B2B) satış işlemlerini ifade etmek için kullanılmaktadır[127].

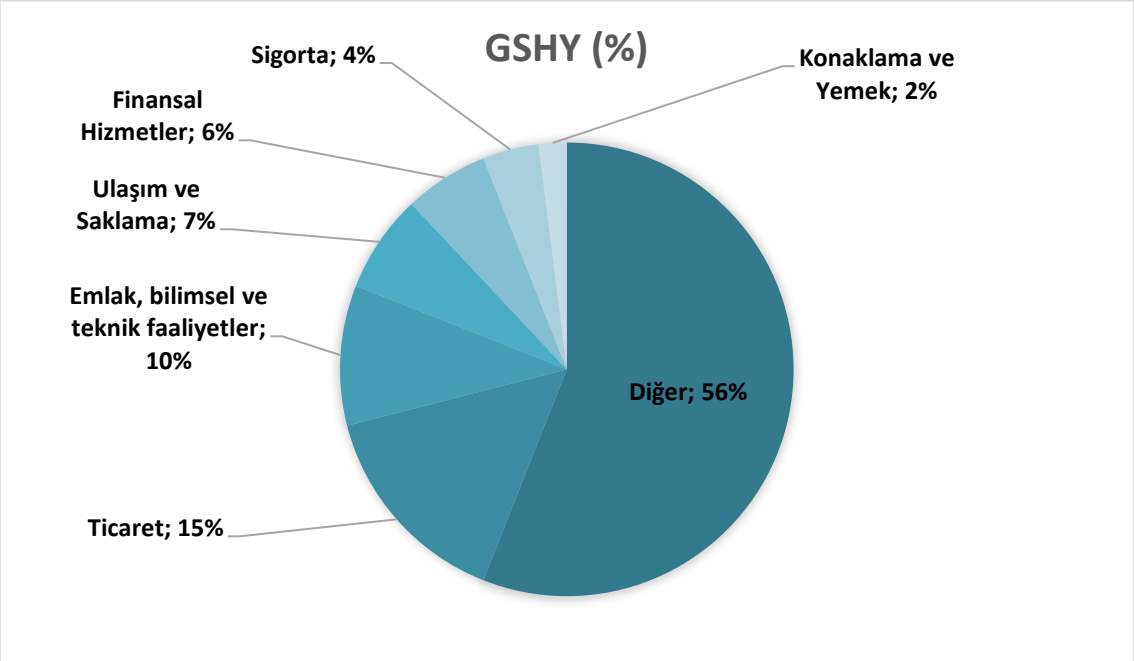
Uber ve Airbnb gibi firmaların büyümesi ve bunların yasal düzenlemeleriyle ilgili tartışmalar dikkati internet ve mobil teknolojiyi kullanarak pazar yeri oluşturan veya görevlendirme mekanizmasıyla birbirlerinden farklı alıcı ve satıcıları eşleştiren işletmelerin üzerine çekmiştir. Bu işletmeler birçok sektörde görülebilmektedir:

- Ulaşım (Uber, Lyft, Blablacar, Didi Kuaidi)
- Konaklama (Airbnb, Kozaza, Couchsurfing)
- Ev Hizmetleri (TaskRabbit, Care.com),
- Teslimat (Postmates, Instacart),
- Perakende Satış (eBay, Etsy, Taobao),
- Tüketici Kredileri (Lending Club, Prosper),
- Döviz Bürosu (TransferWise, Currency Fair),

[126] Taeihagh, Araz (19 June 2017). "Crowdsourcing, Sharing Economies, and Development". Journal of Developing Societies. https://arxiv.org/ftp/arxiv/papers/1707/1707.06603.pdf, erişim tarihi 16.09.2018
[127] Hamari, Juho; Sjöklint, Mimmi; Ukkonen, Antti (2016). "The Sharing Economy: Why People Participate in Collaborative Consumption". Journal of the Association for Information Science and Technology. 67 (9): 2047–2059.

- Proje Finansmanı (Kickstarter),
- Bilgisayar programlama (oDesk, Freelancer)

Bazı durumlarda bu firmalar tüketici ürünlerinin taksi hizmeti veya küçük krediler gibi daha etkili veya daha düşük maliyetli versiyonlarını, diğer durumlarda ise çoğu kişinin erişiminin olmadığı talebe göre teslim hizmeti veya girişim işletmesi finansmanı gibi hizmetleri sunmaya çalışmaktadır[128].



Şekil 17. Sektörlerin Paylaşım Faaliyetlerine Göre GSHY İçindeki Payları
Kaynak: Credit Suisse, Eurostat

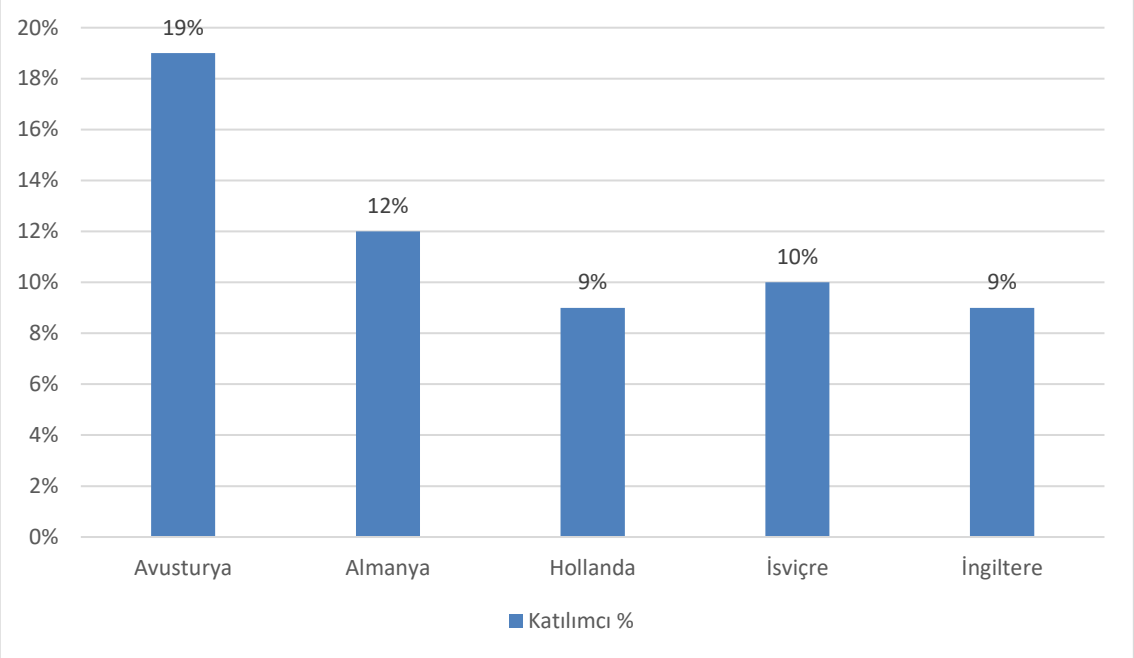
Yukarıdaki şekilde paylaşım ekonomisinden en çok etkilenen sektörler gösterilmektedir. Buna göre %15 ile ticaret (toptan satış ve perakende) en çok ve %2 ile konaklama ve yemek hizmetleri en az etkilenen sektörlerdir. Birbirine yakın ve oranlarda ve nispeten daha az etkilenen diğer sektörlerse Emlak, bilimsel ve teknik faaliyetler %10, ulaşım ve saklama %7, ve finansal hizmer %6, sigorta %4'tür.

[128] Chiara Farronato ve diğerleri, "The rise of peer-to-peer businesses", The sharing economy, Global Investor 2.15, Credit Suisse, 2015, (çevirimiçi) https://www.oxfordmartin.ox.ac.uk/downloads/GI_215_e_GesamtPDF_01_high.pdf. (erişim tarihi 16.09.2018)

2.13.3 Eşten-Eşe Kitle

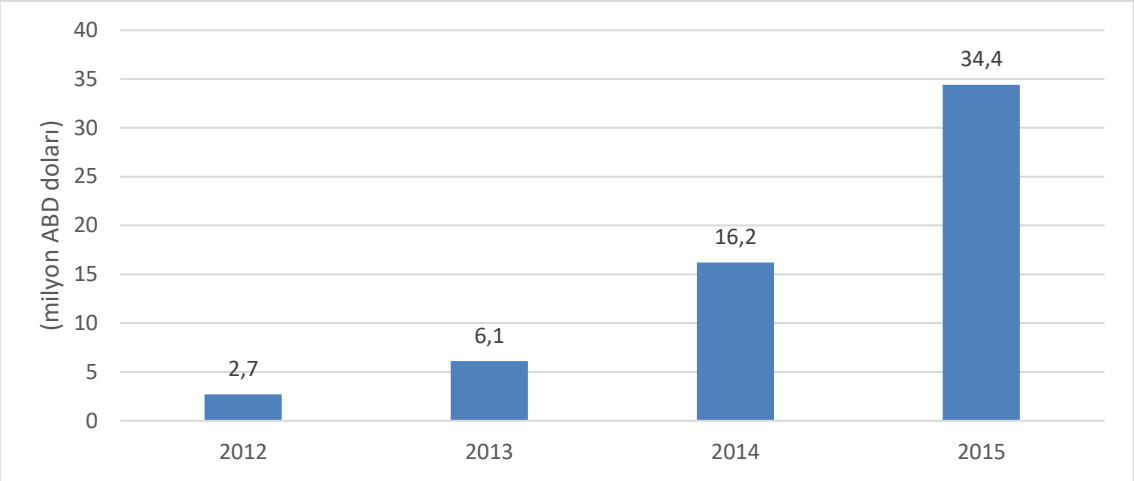
Kitle fonlaması, kitle kullanımı ve kitle işi kayıt zincir teknolojisinin eşten eşe özelliği ile gelen yeniliklerdir. Dijital varlıklar veya dijital ortaklıklar kitle tarafından eşten eşe sahip olundukça tüm varlığa sahip olma ihtiyacı daha az olacaktır. Kitle işi ise en geniş anlamıyla çevirim içi platformlarda ortak katılımcılar yoluyla belirli ücret karşılığı yapılan iş anlamına gelmektedir.

Aşağıdaki tablo Avrupa'da 2016 yılında ülkelerinde herhangi bir kitle işinde çalışmış katılımcıların istatistiklerini göstermektedir.



Şekil 18. 2016 Yılında Avrupa'da Ülke Bazında Yapılan Katılım İşi Yüzdesi
Kaynak: Foundation for European Progressive Studies; UNI Europa

Avusturya %19 ile en çok katılım işi yapan ülkedir. İkinci en yüksek katılım işi yüzdesine sahip %12 ile Almanya'yı İsviçre %10 ile takip etmiştir.



Şekil 19. 2012 ile 2015 Yılları Arasında Dünyada Toplam Kitle Fonlaması Hacmi
Kaynak: Statista 2018

Yukarıdaki tablo 2012 ile 2015 yılları arasında yapılan dünyadaki toplam kitle fonlaması hacmini göstermektedir.

2014 yılında 16,2 milyar ABD doları kitle fonlaması yoluyla sağlanmıştır.

2.13.4 Zaman Bankacılığı

Zaman bankacılığı, toplumların en az parasal maliyetle bireylerin yeteneklerinin kayda alınması ve ihtiyaçlarına göre hizmetlerin düzenlenmesi yoluyla değer bulma yöntemidir[129]. Zamana dayalı para, değer biriminin iş saati veya bir başka zaman birimi olduğu alternatif bir takas sistemi veya para birimi olarak tanımlanmaktadır[130]. Bazı zamana dayalı para birimleri herkesin katkısına eşit bir şekilde değer vermektedir, örneğin bir saatlik iş bir hizmet bedeline eşittir. Bu sistemlerde bir kişi bir başkası için bir saatlik gönüllü çalışması karşılığında bir başka gönüllüden bir saatlik hizmet talep

[129] Sara Singh, "The Evolution of Giving: An Exploration of Time Banking as a Community Development Instrument", 2017, University of South Carolina, Scholar Commons, Senior Theses, (çevirimiçi) https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1211&context=senior_theses, (erişim tarihi 23.07.2018)
[130] Gill Seyfang, "Time banks: Rewarding community self-help in the inner city?", Community Development Journal, NO.39(1), 2004, (çevirimiçi) https://www.researchgate.net/publication/31202656_Time_banks_Rewarding_community_self-help_in_the_inner_city/download, (erişim tarihi 21.06.2018)

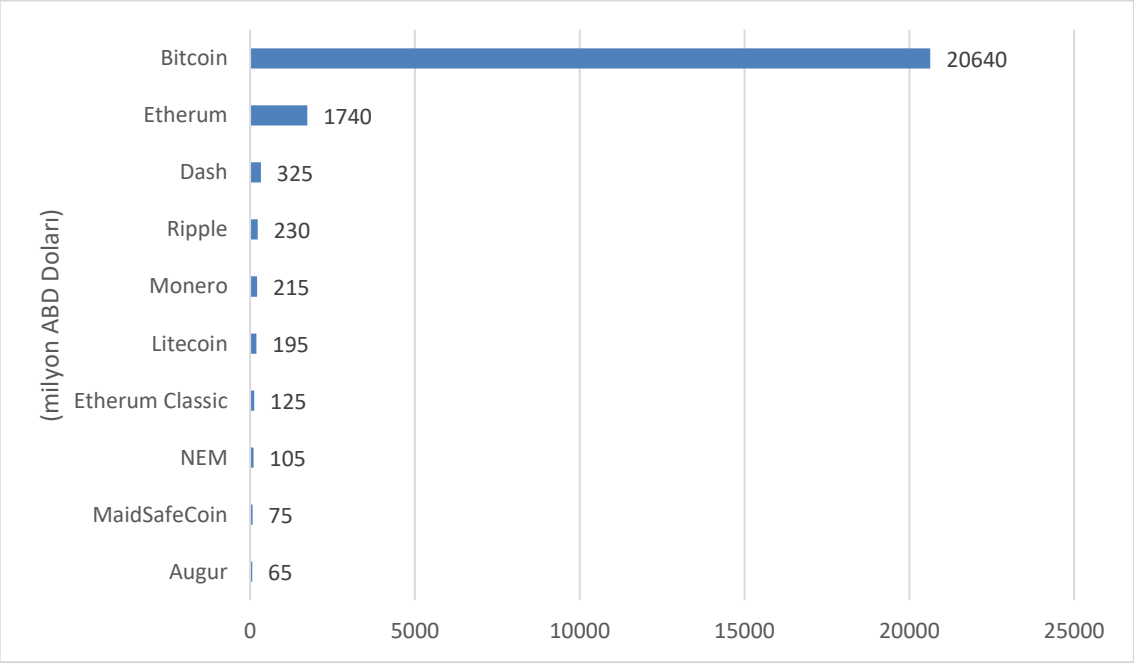
etme hakkı olur. Gorbals Time Bank ve The Arroyo SECO Network of TimeBanks (ASNTB) zaman bankacılığı örnekleridir.

Kripto paranın iş saatleri olarak saklanabildiği zaman bankacılığı olasılığı bulunmaktadır. Bu yolla bir kişi örneğin gençken yaşlılara bakarak harcadığı zamanı saklayarak, yaşlandığında ihtiyaç duyduğu bakım saati ile takas edebilir. Bunlar merkezi bir sistemde de yapılıyor olmasına karşın dağıtılmış veya merkezi olmayan kayıtzinciri sisteminde özellikle dağıtık bilgi işlemle (distributed computing) kendine has avantajları olacağı söylenmektedir. Kripto para itibari paranın yerini almayabilir ancak sahip olduğu kayıt zinciri teknolojisinin kesinlikle insanların rahatlığı üzerinde ve belki de eşitsizliğin dağıtılmasında çok büyük etkisi olacağı söylenmektedir.

3. KRİPTO PARANIN BAŞARILI OLABİLMESİNİN KOŞULLARI VE GELECEKTEKİ OLASILIKLAR

3.1 Ekosistem

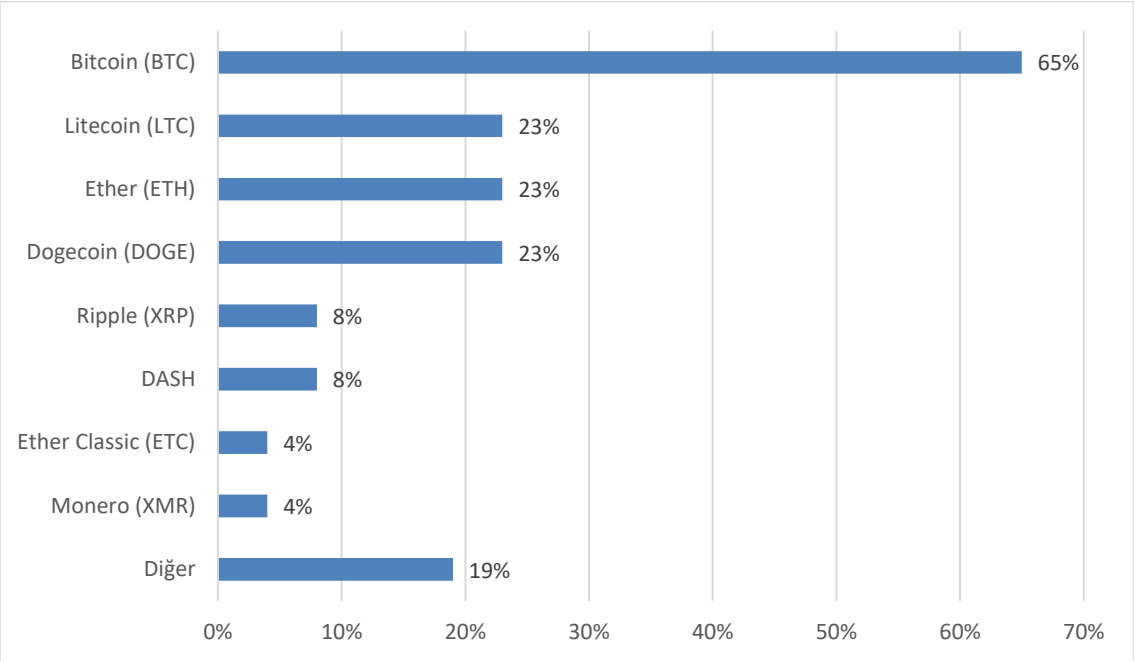
Pazarlama stratejisinde ilk girişimci avantajı, bir piyasa sektöründeki önemli yeri ilk kaplayanın (ilk girişimci) elde ettiği avantajdır. İlk girişimci avantajı teknolojik liderlikle veya kaynakların erken alınmış olmasıyla kazanılabilir. Bir pazar katılımcısı, eğer piyasaya giren ilk kişiyse ve kaynak kontrolüyle rekabet üstünlüğü sağlamışsa ilk girişimci avantajına sahip olduğu söylenmektedir[131]. Bu avantajla, ilk girişimciler çok büyük kar marjları elde edebilmekte ve pazarda tekel statüsü kazanabilmektedirler. Bu durum bitcoin için geçerlidir. Bitcoin'in ilk girişimci avantajı bulunmaktadır ve pazarda tahmini 6 milyon elektronik cüzdan, 70,000 bayisi, piyasa değerinin toplam 20,640 milyon ABD doları olduğu hisseleri ile önde giden kripto paradır.



Şekil 20. Mart 2017 İtibari Dijital Para Piyasasında Toplam Hisse Değerine Göre Önde Gelen Sanal Paralar
Kaynak: Statista, 2018

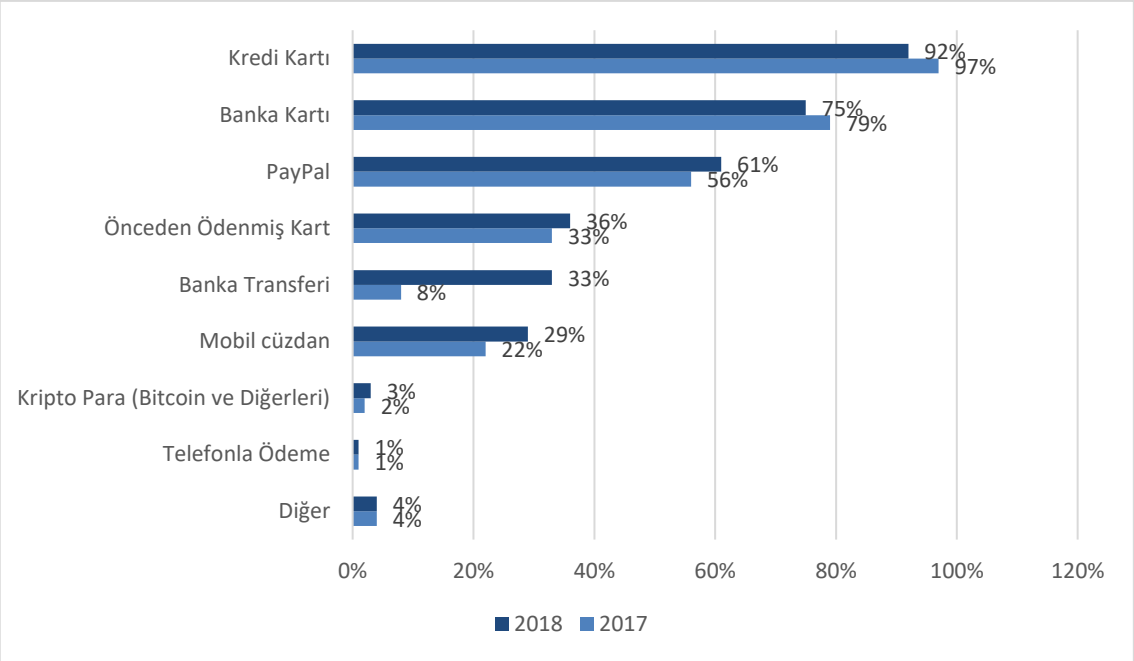
[131] Robert M. Grant, "Cases in Contemporary strategy analysis", 2003, United States, UK, Australia, Germany: Blackwell publishing. ISBN 1-4051-1180-1.

Mart 2017 itibari piyasadaki toplam hisse değerleri ile önde gelen sanal paralar yukarıdaki şekilde gösterilmektedir. 2017 yılında Bitcoin'in piyasadaki toplam hisse değerinin 20,640 milyon ABD Doları olduğu görülmektedir.



Şekil 21. Kullanılan Cüzdan Yüzdesine göre Kripto paraların dağılımı, 2016
Kaynak: Statista 2018

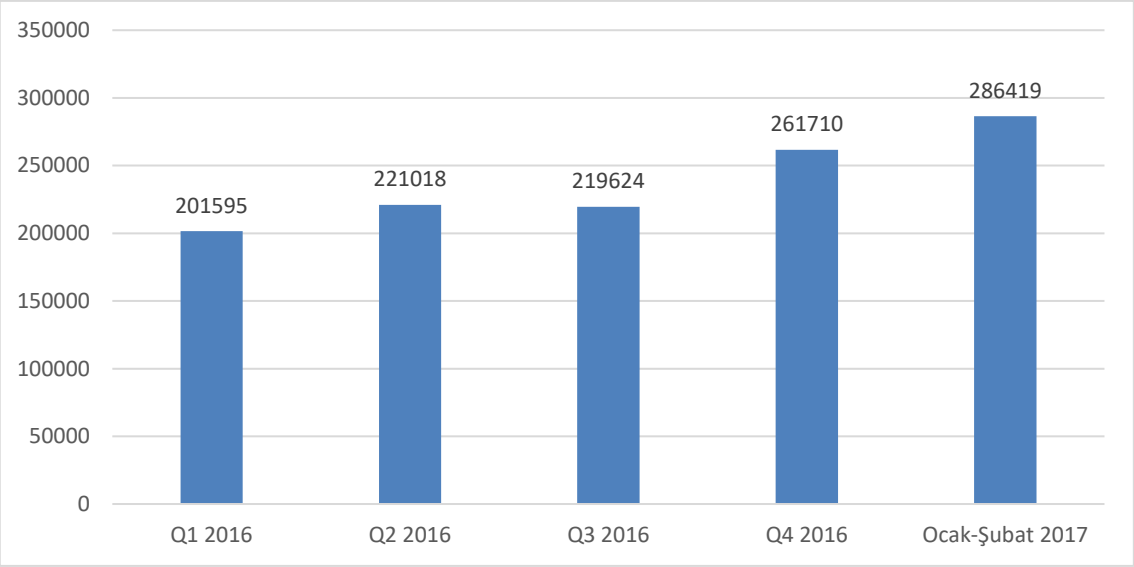
Şekil 21, kripto paraların dağılımını 2016 yılında kullanılan elektronik cüzdan yüzdesine göre göstermektedir. Bu tabloya göre 2016 yılında cüzdanların %65'i Bitcoin sağlamaktadır.



Şekil 22. İşletmelerce Kabul Edilen Ödeme Yöntemleri 2017-2018
Kaynak: Statista 2018

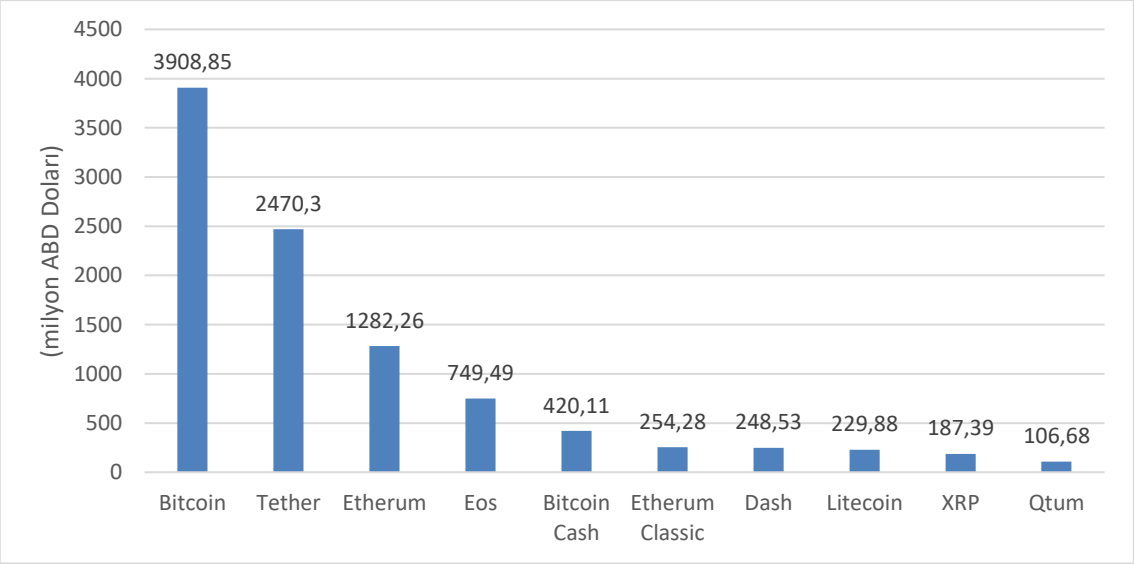
Şekil 22, Mart 2018 itibari dünyada işletmelerce kabul edilen mobil ödeme yöntemlerinin paylarını ödeme tipi ve yılına göre göstermektedir. Bulgulara göre 2017 yılında işletmelerin %79'u mobil ödemede banka kartını en kullanışlı yöntem olarak kabul etmiştir ancak 2018 yılında bu oran %75'e düşmüştür. Bitcoin ve benzerleri ise %1 artış göstermiştir.

2016 yılı başından bu yana Bitcoin'in ortalama günlük işlem sayısı yaklaşık 286,419 adet gerçekleşmiş ve 2018 itibari 3,91 milyar ABD Doları alış hacmine ulaşmıştır. (2018 haziran itibari dolaşımda 17,12 milyon Bitcoins bulunmaktadır) Cüzdan sayısı dünyada 7 milyardan fazla insanın yaşadığı düşünüldüğünde küçüktür ancak Bitcoin bu zamana dek başarılı bir grafik çizmiştir ve ekosistem varlığını destekleyecek seviyeye gelmiştir.



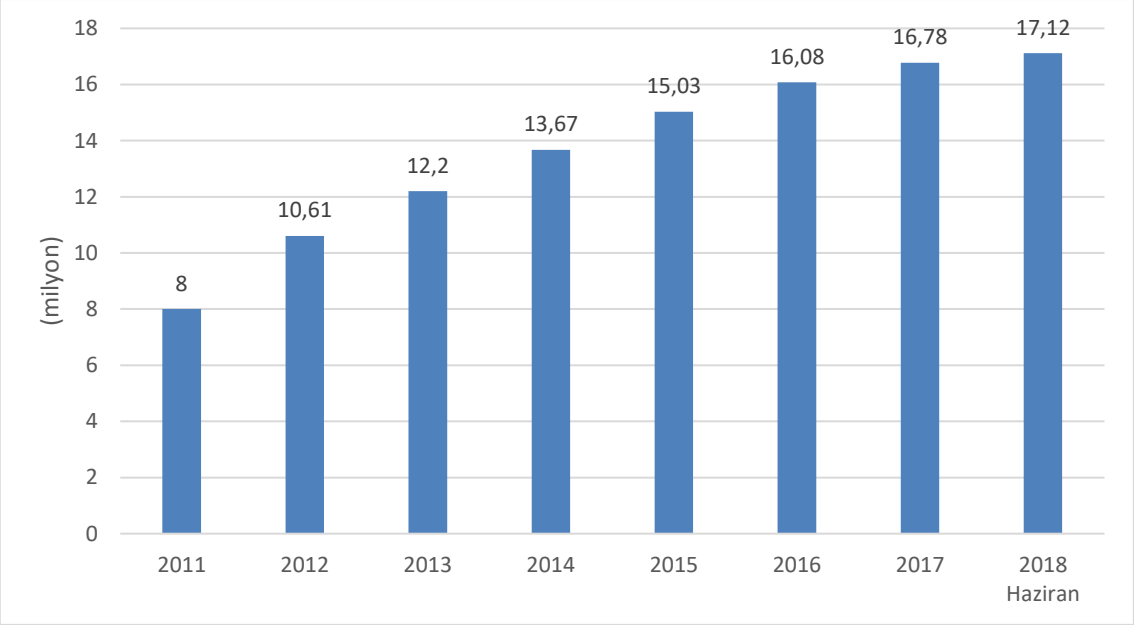
Şekil 23. Bitcoin Günlük Ortalama İşlem Sayısı, 2016 İlk çeyreğinden Şubat 2017' ye kadar
Kaynak: Statista 2018

Yukarıdaki tablo 2016 ilk çeyreğinden Şubat 2017'ye kadar günlük Bitcoin işlemlerinin ortalama sayısını göstermektedir. 2016 dördüncü çeyreğinde tüm dünyada toplam 261,710 Bitcoin işlemi gerçekleştirilmiştir.



Şekil 24. Alış Hacmine göre Eylül 2018 itibari dünyada önde gelen sanal paralar
Kaynak: Statista 2018

Şekil 24, 3 Eylül 2018 itibari dünyada alış hacimine göre önde gelen sanal paraları göstermektedir. Bu verilere göre Bitcoin 3,91 milyar ABD doları ile en çok satın alınan kripto paradır.



Şekil 25. 2011-2018 yılları arası Dünyada Dolaşımdaki Bitcoin adedi
Kaynak: Statista 2018

Yukarıdaki tablo 2011 ve 2018 yılları arasında dolaşımdaki Bitcoin adedini göstermektedir. Oluşturulduğu 2009 yılından bu yana Bitcoin adedi artmakta olup 2018 haziran itibari 17,12 milyona ulaşmıştır.

Kullanıcı sayısının artmasına bağlı olarak kullanım hareketliliğini arttıran ağ etkisine karşın Bitcoin'in önünde uzun bir yol bulunmaktadır.

Başarılı bir dijital para ilk başarısının devamını getirebilmeli ve ağ etkisinin üzerine çıkabilmelidir. Kullanıcı sayısı artıkça değeri daha da artacaktır. Daha değerli oldukça çıkarmanın (madencilik) ödülü artacak ve daha çok madenci bu hesap yarışına katılacaktır.

3.2 Teşvikler

Donanım fiyatları sürekli yükseldiği için çıkarma (madencilik) maliyetleri yükseldikçe genellikle riskten kaçınan ve çıkma olasılığı yüksek sonuçları isteyen madencilerin, ortak madenci havuzlarını oluşturmaya başlaması olasılığı bulunmaktadır. Bu durum ağa yapılabilecek herhangi bir saldırı ihtimalini arttımaktadır. 2018 Haziran itibari 17,12 milyon Bitcoin bulunmaktadır. 2013 yılından 2016 yılına dek yaklaşık her 10 dakikada 25 bitcoins oluşturulmuştur veya çıkarılmıştır. Oluşturulan her yeni bitcoin sayısı 4 yılda bir yarıya düşmektedir.

Hala uzak görünen 2040 yılı itibari 21 milyon bitcoin arzı tamamlandığında vazgeçen madencilerin sayısının artması ihmali bulunmaktadır. Eğer tek ödül işlem ücretleri olursa ve ücretler çok yükselirse işletmeciler ödeme olarak bitcoin kabul etmekten veya kullanmaktan büyük olasılıkla vazgeçecektir.

3.3 Kimlik Tespiti

Para aklama veya terörizmin finansmanı faaliyetlerinde kullanılması ihtimalini azaltmak için kimlik ispatı arayan kripto paralar bulunmaktadır. Eğer bu sorun çözülebilirse kripto paranın tercih edilme potansiyeli yüksek olacaktır.

Eğer belirli bir kripto para, yasa koyucunun, ekosistemin bir parçası olduğunu kabul eder ve kullanıcıları bu ekosistemin oluşturulmasında hükümetle yapıcı ilişkiler kurarsa bu kripto paranın daha fazla kabul göreceği düşünülmektedir. Toplumsal gelişimin büyük kısmının refah piramidinin en alt seviyesinden geldiği düşünülürse gelişmekte olan piyasaların bu girişimci firmaları merkezi olmayan ve her zaman dağıtık olması gerekmeyen sistem sayesinde kripto paranın ilk meyvelerini toplamaktadır. Bahsi geçen bu konuları ele alan bir kripto paranın parlak bir geleceği olacaktır.

3.4 Gelecekteki Olasılıklar

- Pay İspatı (Proof of Stake)

Elbette ki tüm bunların teknik bir çözümü bulunmaktadır. İş ispatına dayanan Bitcoin sistemine alternatif olarak geliştirilen pay ispatı madencilerin bir blok oluşturabilmek için çözmek zorunda oldukları zorlu matematik problemine harcadıkları

elektrik enerjisi maliyetini ve dışarıdan saldırılara açık olma problemini sisteme madenci olarak katılımı güçlü bilgisayarlarla değil yatırım yapmayı şart koşarak çözmektedir. Pay ispatında iş ispatında olduğu gibi bir ödül yoktur. Aynı iş ispatı algoritmasında olduğu gibi ortak bir uzlaşı sağlama ve işlemleri doğrulama amacı vardır ancak buna ulaşma yolu farklıdır. Pay ispatında madenci sistem tarafından sahip olduğu madene ve o madene ne kadar süredir sahip olmasına göre sistem tarafından rastgele seçilir. Yani sistemdeki tüm madenlerin %2'sine sahip bir madenci sonraki bir bloğun oluşturulmasında %2 şansı olacaktır ve sistemin madenciyi rastgele seçiyor olması en yüksek madene sahip madencinin sürekli seçilmesini yani merkezileşmeyi engellemektedir. Pay ispatı algoritması herhangi birinin süper güçlü bilgisayarı ile tüm sistemin çökmesine sebep olması riskini azaltmaktadır.

- Sisteme Saldırı Senaryoları
  - Çoğunluk Saldırısı (%51 saldırısı veya>%50 saldırısı)

Çoğunluk saldırısı, ağa yapılan bir saldırı çeşididir. 51% saldırısı ifadesi, kayıt zincirine, genellikle varsayımsal olarak bitcoine, ağın özetleme veya hesaplama gücünün %50'sinden fazlasına sahip bir grup madenci tarafından yapılan saldırı için kullanılır. Bu senaryoda saldırı eylemini yapan kişiler yeni işlemlerin onaylanmasını engelleyebilmekte, bazı ya da tüm kullanıcıların ödemelerini bekletebilmektedir. Bu kişiler aynı zamanda ağı kontrol altına aldıklarında tamamlanmış işlemleri geri alabilmekte yani çifte harcama yapılabilmesine olanak vermektedirler. Oldukça zarar verici görünüyor olmasına karşın bu eylemi yapanların yeni blok oluşturamamaları (geri kalan madencilerin onaylamaması) ve eski blokları geri alamamaları sebebiyle bitcoin sistemini veya başka bir kayıt zinciri sistemini yok etmeleri imkansızdır. Öte yandan %51 saldırısının bir alternatif şekli olan, gerçekleşme ihtimalinin az olduğu, ağın hesaplama gücünün %50'den az olduğu durumlarda ortaya çıkan saldırı örnekleri bulunmaktadır.

  - Ghash.io

Bir ortak madenci havuzu olan ghash.io'nun hesaplama gücü 2014 Temmuz ayında bitcoin ağının toplam gücünün %50'sini geçmiştir. Bu durum sonucunda ağdaki payını gönüllü olarak azaltmıştır.

- Krypton and Shift

Ethereum tabanlı bu iki kayıt zinciri Krypton and Shift, 2016 Ağustos ayında %51 saldırılarına maruz kalmıştır.

- Bitcoin Gold

2018 Mayıs ayında, Bitcoin Gold, 26. en büyük kripto para olduğu dönemde %51 saldırısına maruz kalmıştır. Bitcoin Gold'un özetleme gücünün büyük kısmını kontrol etmekte olan bu zararlı eylemciler Bitcoin Gold sürekli olarak takas eşiğini yükseltmeye çalışsa da günlerce çifte harcama yapmıştır ve sonuç olarak 18 milyon ABD doları değerinde Bitcoin'i çalmıştır.

- %34 saldırısı

Temelde kayıt zincirinden oldukça farklı ancak benzeri amaçları hedefleyen bir dağtık kayıt defteri olan Tangle, teorik olarak ağının hesaplama gücünün üçte birinden fazlasına sahip olunması durumuna %34 saldırısı adını vermektedir.

- Teknoloji ve Finans

Çoğu kişi internetin büyümesi ile kripto paranın gelişimi arasındaki benzerlikleri görmekte ve kripto paranın tıpkı internet gibi katlanarak gelişim göstereceğine inanmaktadır. Ancak, internetin iş dünyasına etkisi finans sektöründen çok elektronik ticaret ile ilgilidir. Diğer bir açıdan kripto para ile insanlık tarihinde ilk kez teknoloji, finans sektöründe baş rolü üstlenmiştir. Gelecekte büyük olasılıkla, bankaların dijital teknoloji konusunda deneyimli olmaları gerekecektir.

- Kripto paralar ve Serbest Yatırım Fonları

Sektör bazında tıpkı internet örneğinde olduğu gibi kripto para ile serbest yatırım fonlarının (hedge fonları) ortaya çıkışı arasında benzerlikler bulunmaktadır. Serbest yatırım fonları sektörü ilk evresindeyken para sistemine yıkıcı etkisi olduğu düşünülmüştür. Çünkü fon yöneticileri sektördeki yüksek komisyon payları ile büyük işleri toplayan kişiler olarak görülmüştür. Para sistemine saldırıp ve sermaye piyasalarını dağıttıkları düşünülmüştür. Bazı bankalar yüksek uyum maliyetleri

sebebiyle serbest yatırım fonları işine girmeyi istememiştir. Bugün aynı sorunlarla kripto para sektöründeki başlangıç firmaları da yüzleşmektedir.

Yapıları itibari ile sayısal oluşları ve zor anlaşılmaları açısından serbest yatırım fon stratejileri ile de arasında pek çok benzerlik bulunmaktadır. Serbest yatırım fonu stratejileri ilk desteği, geleneksel yöneticilere göre daha az kısıtlanmış olan üniversite bağış ve araştırma fonlarından bulmuştur. Kripto para da desteği öncelikli olarak araştırmalar yapan üniversiteler ve finansal girişimcilerden bulmaktadır.

- Kripto para ve toplumsal refah

Kripto para gelip geçici bir buluş olmamakla beraber hala gelişimini tamamlamamış olan bir icattır. Eğer Bitcoin herhangi bir nedenden ötürü popülerliğini yitirirse daha kullanışlı özellikleriyle yerini almak üzere yeni bir kripto para ortaya çıkacaktır. Büyük borç altındaki ülkelerin kendi kripto paralarını yapma çalışmaları bulunmakla beraber finansal bütünleşmeye öncelik veren ülkelerin de sırf merkezi olmayan kısmen dağıtık bir sistemin oluşturulması düşük maliyetli olduğu için kripto parayı tercih etme olasılığı bulunmaktadır. Merkezi olmayan ve tamamen dağıtık olması gerekmeyen kripto para dünyasında, kimlik ispatıyla, pay ispatıyla ve paylaşım ekonomisi için akıllı sözleşmelerin dahil edilmesine elverişli olabilmesiyle bir refah gelişimi olacağı düşünülmektedir.

Finans ve işletme dünyasında nihayetinde herşey işletme maliyetlerinin kısılabilmesiyle ilgili olmaktadır. Bu nedenle de toplumsal gelişim, refah piramidinin tabanındakilerden başlayarak bu yeniliğin yeni peşinden gelecektir. En sonunda tüm bunlar bir paylaşım ekonomisi içinde serbest bırakılmış bir verimliliği getirecektir. Kripto paranın gelişimi, kayıt zinciri teknolojisi sebebiyle dışarıdan çok daha fazla iyimser bir bakış açısı getirmektedir. Altında yatan yakın saha iletişimi ve benzeri mobil teknolojisi faktörüyle kullanımında büyük bir sıçrama görülmesi büyük bir olasılık olarak görülmektedir. Aynı zamanda, kripto para dünyasında hala birçok belirsizlik olduğu için kripto paranın bu zamana karadr ki en büyük yenilik olduğunu söylemek zor da olsa bunun finansal kuruluşların göz ardı edemeyeceği bir teknoloji olduğu bir gerçektir.

SONUÇ

Bitcoin'in ortaya çıktığı 2008 yılından bu yana bu Satoshi Nakamoto'nun tanıtım yazısı çok fazla ilgi çekmiştir.

İlk olarak, çıktığı tarihinin zamanlaması, rezerv paraya olan güvenin azalması krizine doğrudan bir tepki olmuştur. 1971'de ortaya çıkan itibari para sistemine olan güvenin azalmaya başladığı ve parasal genişleme yani yoğun miktarda para arzının yaşandığı bir dönemde bu tanıtım yazısı merkezi para sistemine güveni sarsılan kesime makul alternatif çözümler sunmuştur.

İkinci olarak, Satoshi'nin tanıtım yazısı dağıtılmış bir parasal sistemi öneren ilk yazı olup para arzını kontrol eden merkezi otoriteye karşı çıkmıştır. Önerilen bu sistem merkezi sistemin üstesinden gelemediği konulara işaret edecek şekilde tasarlanmıştır. Özellikle kontrol merkezi değildir ve para arzı önceden belirlenmiştir. Bitcoin protokolünün açık kaynaklı yapısı sistemin tüm paylaşımcıları tarafından izlemesini ve düzenlemesini mümkün kılmaktadır. Ülkeler ilk kez, kanuna aykırı herhangi bir durumdan ötürü sorumlu tutmak bir yana, bu merkezi olmayan yapının, tüzel bir kişiliği ya da birkaç kuruluşu düzenlemeyi isteyen kişiler için önemli sorunlar getirdiğinin farkına varmıştır.

Üçüncü olarak Bitcoin sistemiyle ilgili cevapsız birçok konun olması gelişmeyi takip edenler arasında merak uyandırmaktadır. Öncelikle Bitcoin'i bulan kişi ya da kişiler hala belirsizdir. Özellikle, kişisel eposta hesabına erişmeyi başardıktan sonra Nakamoto'nun kim olduğunu bildiğini iddia eden bir bilgisayar korsanı da dahil olmak üzere, Nakamoto'nun kimliğini ortaya çıkarmaya yönelik birçok deneme olmuşsa da kamuoyunda kimliği hala belirsizdir. Bitcoin'in etrafındaki bu kimlik belirsizliği daha da fazla takipçinin oluşmasına neden olmuştur. Bu yeniliği izleyenler Bitcoin'i oluşturanların sessizliğine saygı duymakta ve öngörüsünden etkilenmektedir.

Dördüncü olarak, Bitcoin'in icadı yasal düzenleyicilerin de ilgi odağındadır. Kripto para uygulamasını düzenlemeye yönelik her girişim oldukça zor olmaktadır. Ancak, aracıları düzenlemekle ilgili konularda çalışmakta ve tüketicinin korunması, kara paranın aklanması ve terörizmin finansmanı ile mücadele ilgili alanlara odaklanmıştırlar. Yasal düzenleyiciler için en zor durumun yasa ve girişim arasındaki

dengeyi sağlayabilmek olduğu görülmektedir. Vergi kurumları, merkez bankaları, hukukçular tarafından bu nedenle dikkatle izlenmektedir. Daha önce hiçbir teknolojik gelişme aynı anda hem uluslararası finans hem parasal sistem hem de yenilikçi finansal teknoloji ile siber güvenliği içermediği için bu kadar dikkat çekmemiş ve zorlukla karşılaşmamıştır.

Beşinci olarak, parasal genişleme modelinin uygulanmasından bu yana dünyadaki servete sahip olanlar ve olmayanlar arasındaki farklılıklar yani servetin çok yüksek düzeyde eşitsiz dağılımı (servete karşı gelir oranı) hızla artmaktadır. Bitcoin'in ucuz bir ödeme yöntemi sunuyor olması kripto parayı alternatif bir ödeme biçimi olarak ortaya çıkarmıştır. Hem finansal tabana yayılma hem de sosyal etki yatırımı günümüzde değer verilen kavramlar olmakla beraber Kripto para bu kavramların ilgi odağında bulunmaktadır.

Altıncı olarak, Kripto para birçok teknolojik gelişmeye ve ilginç yeniliklere vesile olmuştur. Bu gelişmeler akıllı muhasebe (smart accounting), kitle kaynak tedariği (crowdsourcing), akıllı sözleşme (smart contract), kitle fonlaması (crowdfunding), kripto-pay (crypto-equity) ve birçok benzeri gibi ticari işlemlerin yapılışını ve yönetimini değiştirecek yeniliği içermektedir. Uzlaşım defteri (Consensus ledger), dijital kayıt (digital register), Kayıt zinciri (Blockchain) geleceğin gelişmekte olan unsurlarıdır.

Yedinci olarak, 2000'li yılların getirdiği dijital vatandaşlık ve akıllı kent kavramları kripto paranın gelişimine daha da çok ilgi duyulmasına sebep olmuştur. Dijital vatandaşlar, erken yaşlarda teknoloji ve bilgisayara alışmış ve teknolojiyi hayatların ayrılmaz ve önemli bir parçası olarak görmektedir. Günümüzün gençleri ve çocukları temel olarak bilgisayar, SNS ve mesajlaşma yoluyla iletişim kurdukları ve öğrendikleri için dijital vatandaş olarak düşünülmektedir. Akıllı kent ise sürdürülebilir bir yaşam ve kentleşme için teknolojinin su yönetimi, temiz ve yenilenebilir enerji, akıllı trafik kontrolü, e-devlet, şehir içi hareketlilik, kablosuz internet erişilebilirliği ve atık yönetimi ve benzeri alanlarda kentlere uygulanması olarak tanımlanmaktadır[132]. Örneğin, Singapur gibi tüm ülkenin dijital dünyaya ve planlanan büyümenin dijital

[132] Fatih Terzi ve diğerleri, "Kentlerin Geleceği: Akıllı Kentler", İTÜ Vakıf Dergisi, S. 77 (Temmuz-Eylül 2017), ss. 10-13.

ekonomiye bağlı olduğu ülkelerin vatandaşları da dünyanın dijital vatandaşları olarak kabul edilebilimektedir. Sanal alanda geliştirilen bu teknoloji, altyapıyı dijital ekonomiye hazır hale getirmek için milyonlar hatta milyarlar harcayan bu ülkelerin en büyük ilgi alanlarından biri olacaktır. Yeni işletmelere sağlanan, sanal güvenlik ve bağlanırlık başta olmak üzere şifrelemeyi, finansal şifreyazımı, merkezi olmayan depolamayı ve mobil ödemeleri ve benzeri teşvik yatırımlarını daha da ilgi çekici hale getirecektir. Kripto para ise ödemelerin güvenli olmasında, dağıtık kayıt defterinde ve şifrelemedeki yeniliklere önderlik etmesi sebebiyle en büyük ilgiyi çekecektir.

Sonuç olarak ödemeler ve bugün bildiğimiz merkezi olmayan ağlar açısından bir dönüm noktası olan Bitcoin önemli bir icat olarak görülmektedir. Bu buluş pek çok yeniliği ve bitcoinle uğraşan ve çalışan kullanıcıların bilincinde oldukları ve göze aldıkları riskleri de beraberinde getirmektedir. Bu çalışma çoğunlukla Bitcoinin temel özellikleri üzerinde durmuştur ancak diğer kripto paralarda da benzer özelliklerin bulunması muhtemeldir. Bu nedenle bu çalışma ile Bitcoini anlatarak ileride kripto paralarla ilgili yapılacak araştırmalara bir kaynak sağlamakla beraber diğer kripto para türlerinin anlaşılmasına da yardımcı olunması amaçlanmıştır.

TANIMLAR

Anonim Ağ (Tor-The Onion Routing): Kullanıcılarının gerçek kimliklerini gizleyerek iletişim imkanı sunan bir yazılım projesidir. Tor üzerinden bir internet sitesine istek yolladığında birçok sunucu üzerinden istek gönderilir. Bu sayede internet trafiğini çok sayıda sunucu aracılığıyla yansıtarak Tor ağındaki kullanıcılara erişmek zorlaşır ve kullanıcının konumu ve verilerinin bulunması imkansız hale gelir.

Bilgi Pazarları (Information Market): Ağlar yoluyla dağıtılan dijital bilgi pazarıdır. Ticareti yapılan ürünler her türlü yazılım uygulaması ve içeriktir (bloglardaki resimler, filmler, oyunlardan bilimsel makaleler ve markalara kadar her şey). Bilgi Ticareti (I-Commerce) dijital bilgili elektronik ticarettir[133] (e-commerce).

Bindirmeli Ağ Sistemleri (Overlay networks): Varolan ağ üzerine yeni iletişim kuralları ve servislerinin denenmesi için kullanılırlar[134].

Bit (binary digit): 0 ve 1 ikili rakamlarından oluşan bilgisayar terimidir. Bilgisayarlarda kullanılan verileri ifade etmede kullanılır. Bit bilgisayardaki en küçük veri boyutu biriminin adıdır.

Chargeback Fraud (friendly fraud): Dostane dolandırıcılık.

Crowd Lending: Kitle finansmanı, firmaların kendilerini, bir bankaya gitmek zorunda kalmadan, farklı ve çok sayıda insanlar grubu katılımıyla ortak bir platformda finanse etmeleridir.

Finansal Bütünleşme (Financial Integration): Bir ülkenin finansal piyasalarının diğer ülkelerdeki veya dünyadaki piyasalara daha fazla yakınlaşmasını sağlayan süreçtir[135].

---

[133] Linde ve diğerleri; Information Markets: A Strategic Guideline for the I-Commerce., De Gruyter Saur, Berlin, Germany, pp. 617, 2011 (ISBN: 978-3-11-203609-5).

[134]Enis Karaarslan, "Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme", 2013, (çevirimiçi) http://dergipark.gov.tr/download/article-file/207215), (erişim tarihi 11.05.2018).

[135] Nurhan Erkan, "Finansal Bütünleşme", Sermaye Piyasası Kurulu Araştırma Raporu, 2005, (çevirimiçi) http://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/936, erişim tarihi 16.04.2018)

Geri Alınamaz İşlem (NonRepudiable Transaction): Gerçekleşmesi veya yasallığı inkar edilemeyen işlem.

Gömülü Sistem: Bilgisayarın kendisini kontrol eden cihaz tarafından içerildiği özel amaçlı bir sistemdir. (Banka ATM'leri, kişisel bilgisayarlar)

Güvenli Giriş Katmanı (SSL-Secure Sockets Layer): Sunucu ile alıcı arasında veri alışverişi sırasında verilerin şifrelenerek alınıp gönderilmesidir. Sunucu ve istemci arasında SSL oluşturmak için sunucu tarafında bir anahtar ve istemci tarafında da sertifika gerekmektedir.

İlk kitleye arz (Initial Crowd Offering) (ICO): Menkul kıymet piyasalarından sermaye bulmak isteyen firmaların ilk girişimlerini ifade eden İlk halka arz (IPO) kavramı gibi yatırımcı veya katılımcıları akıllı sözleşme teklifleri yoluyla toplayan bir dijital platform.

İstemci Bulmacası Fonksiyonu (CPP- Client Puzzle Protocol): Kullanılan (paylaştırıcı bilgisayar ağı) sunucu kaynaklarının suiistimalini olanaksız hale getirmek için internet iletişiminde kullanılan bir bilgisayar algoritmasıdır. İş ispatı sisteminin (proof-of-work system (POW)) uygulanmasıdır. CPP'de ana fikir eğer sunucu saldırı altındaysa, ona bağlanmaya çalışan tüm istemcilerin ağa bağlanmadan önce matematiksel bir bulmacayı çözmeleri istenir. Bulmacayı çözdükten sonra istemci sonucu, sunucuya iletir ve sunucu bağlantıyı onaylar veya reddeder.

Küresel Etki Yatırımı Ağı (GIIN-The Global Impact Investing Network): 2007 yılında sosyal etki yaratımının yaygınlığını ve etkisini arttırmak amacıyla New York'ta kurulmuş, Birleşik Devletler İç Gelirler Kanunu'nun 501 (c) Maddesi kapsamına giren, kar amacı gütmeyen ve vergi muafiyeti olan bir kuruluştur.

Merkezi Olmayan Uygulamalar (Dapp, dApp veya DApp-Decentralized Application): Birçok kullanıcı tarafından ortak onay mekanizmasıyla merkezi olmayan sistemde banka veya finasal bir aracı olmadan çalıştırılan uygulamaların genel adı.[136]

[136] Siraj Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology", O'Reilly Media, Inc., Amerika, 2016.

Mikro Ödeme: Çok az bir miktarda parayı içeren ve genellikle çevirimiçi yapılan finansal bir işlemdir. 1990'lı yılların ortalarından sonlarına kadar çoğu başarısız bir şekilde sonlanan birçok mikro ödeme sistemi planlanmış ve geliştirilmiştir. Mikro ödeme sistemlerinin 2. nesli 2010'lu yıllarda ortaya çıkmıştır[137]. Mikro ödemeler başlarda çok küçük meblağlar için tasarlandığı halde 1 USD altındaki işlemleri içeren sistemler rağbet görmemiştir. Mikro ödeme sistemlerinin geşimini engelleyen bireysel işlem maliyetlerinin az tutulmak istenmesiydi ki bu böyle küçük miktarlarda işlem yaparken işlem masrafı birkaç sent olsa da avantajlı bir durum sağlamamaktaydı. Mikro ödeme ile ilgili pek çok tanım vardır. PayPal mikro ödemeyi 5 sterlin, Visa 20 dolar altındaki işlemler olarak tanımlar. Bugün en bilinen mikro ödeme sağlayıcıları Flattr (İsveç kökenli mikro bağış hizmeti), GNU Taler (Fransa kökenli elektronik ödeme sistemi), Jamatto (Amerika kökenli elektronik ödeme sistemi), M-Coin (Portekiz mobil ödeme hizmet sağlayıcısı), PayPal (Amerika kökenli elektronik ödeme sistemi), SatoshiPay (Bitcoins ile gerçekleştirilen mikro ödemeler) ve Swish (İsviçre bankaları arasında kullanılan bir sistem)'tir[138].

Mining Pool: Ortak madenci havuzu, madencilerin ağ üzerinde bilgisaylarının işlem gücünü paylaşma yoluyla arttırarak bir ortak kaynak havuz oluşturmalarıdır. Bu kaynak havuz sayesinde blok şifresini kıracak güce erişmekte ödülü ise blok bulma olasılığına yaptığı iş miktarı katkısına göre eşit olarak bölüşmektedirler.

Nonce (Number only used once): Sadece bir kere kullanılan sayı, tek seferlik sayı.

Mutabakat Riski (Settlement Risk): İşleme taraf olanlardan birisi yükümlülüğünü yerine getirmekte gecikirse diğer taraf kaçıracağı yatırım fırsatları dolayısıyla bir kayba uğrayabilir.

Müşterini Tanı (KYC-Know your customer): (Finansal) Aracı kuruluşların, müşterileri ve müşterilerinin faaliyetleri hakkında yeterli düzeyde bilgi sahibi olması (geçerli kimlik belgesi olmadan işlem yapmama, müşterisi olan bir kuruluşun bağlı ortaklıkları hakkında da bilgi sahibi olma, kuruluşun iş konusu bilmek vb) şüpheli işlem bildirimi İşlemlere konu malvarlığının yasa dışı yollardan elde edildiğine veya yasa dışı

[137] Burton Rosenberg, "Handbook of Financial Cryptography and Security", CRC Press. ISBN-13:978-1-4200-5982-3 (e-Book-PDF), 2011.
[138] A.g.e

amaçlarla kullanıldığına dair herhangi bir bilgi, şüphe veya şüpheyi gerektirecek bir hususun bulunması halinde bu işlemlerin yükümlüler tarafından bildirimi. **Uygulama Programlama Arayüzü (API-Application Programming Interface):** Bir uygulama özelliklerinin başka bir uygulamada da kullanılabilmesini sağlayan arayüz programıdır.

Remailer: Kaynağı belli olmayan, böylelikle orijinal göndereneninin izlenemediği e-posta hizmeti sağlayan bir internet servisidir.

Şüpheli İşlem Bildirimi (SAR-Suspicious Activity Report): İşlemlere konu malvarlığının yasa dışı yollardan elde edildiğine veya yasa dışı amaçlarla kullanıldığına dair herhangi bir bilgi, şüphe veya şüpheyi gerektirecek bir hususun bulunması halinde bu işlemlerin yükümlüler tarafından bildirimi.

Üstveri: Bilgi kaynaklarına ilişkin bibliyografik kayıtlar, dijital nesnelere ait boyut, ebat ve format gibi bilgiler üstveridir[139].

[139] Tolga Çakmak, "Bilgi merkezlerinde üstveri paylaşımı ve entegrasyonu". Hüseyin Odabaş ve Mehmet Ali Akkaya (2017) Bilişim Teknolojilerinin Bilgi Merkezlerine ve Hizmetlerine Etkileri kitabı içinde (s.49-65). Hiperyayın, İstanbul; 2017. (ISBN: 978-605-201-526-1)

WEB SİTELERİ

https://coinmarketcap.com

http://theinstantexchange.com

https://edinarcoin.com/tr

https://www.bloomberg.com

www.bullioninternational.com

https://nakamotoinstitute.org/literature/

https://www.xe.com/currencyconverter/

https://localbitcoins.com/

https://bitcoin.org/tr/

KAYNAKÇA

ADKINS Lesley, Roy A. Adkins. Handbook to Life in Ancient Rome. Oxford University Press, 1998. ISBN 0195123328.

ALCAZAR, Vincent. 2017. "Data You Can Trust: Blockchain Technology." Air & Space Power Journal, Cilt 31 Sayı 2, sayfa 91-101.

ALOIS, JD. "Pozible Now Allowing Bitcoin for Crowdfunding Pledges". Pozible. 2013. (çevirimiçi) https://www.crowdfundinsider.com/2013/10/25251-pozible-allowing-bitcoin-crowdfunding-pledges/. (erişim tarihi 17.07.2018).

ALTAŞ, Gökben. "Gelişmiş Ülkelerde Mevduat Ve Yatırım Bankacılığının Ayrılması". Sermaye piyasasında Gündem Dergisi. TSPAKB. Sayı 132. Ağustos 2013. ISSN 1304-8155. s. 16/20.

ALTAŞ, Gökben, "Altın Piyasaları". Sermaye piyasasında Gündem Dergisi. TSPAKB. Sayı 91. Mart 2010. ISSN 1304-8155. s. 14.

ANDROULAKI, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, Srdjan Capkun. Evaluating User Privacy in Bitcoin. FC 2013: Financial Cryptography and Data Security s. 34-51. 2012. (çevirimiçi) https://link.springer.com/chapter/10.1007%2F978-3-642-39884-1_4. (erişim tarihi 27.06.2018).

ANDRYCHOWICZ, M., Dziembowski, S., Malinowski, D., and Mazurek, L. 2016. "Secure Multiparty Computations on Bitcoin," Communications of the ACM Cilt 59 Sayı 4 sayfa 76.

ARORA, A. 2014. "Banking Law" Pearson Education, sayfa 545.

BACK, Adam; "Hashcash - A Denial of Service Counter-Measure". 2002. http://www.hashcash.org/papers/hashcash.pdf. (Erişim Tarihi: 25.07.2018).

BAILIS, Peter, Song Han. 2017. "Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts; Hardware for Deep Learning" Communications of the ACM. Mayıs, Cilt 60 Sayı 5, sayfa 48-51.

BOOKSTABER, Richard M. 2017. “The End of Theory: Financial Crises, the Failure of Economics, and the Sweep of Human Interaction” Princeton University Press., sayfa 171

Bitcoin Magazine. “Cryptocurrency regulation in 2018: Where the world stands right now”. 2018. (Çevrimiçi) https://thenextweb.com/hardfork/2018/04/27/cryptocurrency-regulation-2018-world-stands-right-now/ (Erişim Tarihi: 05.09.2018).

BRITO, Jerry, Houman SHADAB, Andrea CASTILLO. “Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling”. Columbia Science and Technology Law Review. 2014. Columbia Law School, SSRN Paper, Elsevier, 2014, sayı 16, s.144–221.

BRITO, Jerry, Andrea Castillo. Bitcoin: A Primer for Policymakers. Mercatus Center, George Mason University. 2.basım. 2016.

BRITO, Jerry. “The Top 3 Things I Learned at the Bitcoin Conference”. Reason. 2013. (çevirimiçi) http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoin. (erişim tarihi 16.07.2018)

CASU, Barbara; Girardone, Claudia ve Molyneux Philip 2015. “Introduction to Banking” 2.basım, sayfa 31/34-46. stems(AMCIS), D. Alan and P. Souren (eds.), Puerto Rico

CHAUM, David; "Blind signatures for untraceable payments". Department of Computer Science, University of California, Santa Barbara, CA, Springer-Verlag. 1998. (çevirimiçi)http://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF)

CHEN, Adrian. “The Underground Website Where You Can Buy Any Drug Imaginable”. 2011. (Çevrimiçi) http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160. (Erişim Tarihi: 25.01.2018).

CHOHAN, Usman W. The Decentralized Autonomous Organization and Governance Issues. University of New South Wales, Canberra. Discussion Paper. 2017. (Çevirimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055.

CHUEN, David LEE Kuo. Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Elsevier Science & Technology. eBook ISBN: 9780128023518. 2015.

COHEN, Ivan K. 2015. "Economics for Business: A Guide to Decision Making in a Complex Global Macroeconomy" Kogan Page, Limited, sayfa 81-228-341.

CONNOLLY, A. J. ve Kick, A. 2015. "What Differentiates Early Organization Adopters of Bitcoin from Non-Adopters?," Twenty-first Americas Conference on Information Systems.

Credit Suisse Private Banking & Wealth Management. "Credit Suisse Global Wealth Databook 2014". (Çevrimiçi) (http://economics.uwo.ca/people/davies_docs/credit-suisse-global-wealth-report-2014.pdf). 2014.

CUSUMANO, M. 2014. "Technology Strategy and Management: The Bitcoin Ecosystem," Communications of the ACM (57:10), sayfa. 22.

ÇAKMAK, Tolga. Bilgi merkezlerinde üstveri paylaşımı ve entegrasyonu. Hüseyin Odabaş ve Mehmet Ali Akkaya. 2017. Bilişim Teknolojilerinin Bilgi Merkezlerine ve Hizmetlerine Etkileri kitabı içinde (s.49-65). Hiperyayın, İstanbul; 2017. (ISBN: 978-605-201-526-1)

ÇARKACIOĞLU, A. (2016). Kripto-para Bitcoin. Sermaye Piyasası Kurulu Araştırma Dairesi

DAI, Wei. "B-Money".1998. (Çevrimiçi) http://www.weidai.com/bmoney.txt. (Erişim Tarihi: 25.07.2018).

DAVIES, Glyn. A History of Money from Ancient Times to the Present Day. Cardiff: University of Wales Press. ISBN 0 7083 1351 5. 1996.

DAVIDSON, Jim. “Dijital Gold Industry Overview”, 2006, (Çevrimiçi) www.freemarketmoney.org, (Erişim Tarihi: 25.06.2018).

DİLEK, Şerif; Blockchain Teknolojisi ve Bitcoin, Seta Yayınları, İstanbul, 2018.

DİNÇER, Hasan; Hacioğlu, Ümit 2016. “Risk Management, Strategic Thinking and Leadership in the Financial Services Industry: A Proactive Approach to Strategic Thinking” Springer International Publishing, sayfa 346.

DOHERTY, Stephen. “All your Bitcoins are ours…”. Security Response, Symantec. 2011, (çevirimiçi) https://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours. (erişim tarihi:28.06.2018).

DYSON, J. R., Franklin, Ellie 2017. “Accounting for Non-Accounting Students” Pearson Education Limited 9. Basım, sayfa 48-168

EITEMAN, David K., Stonehill Arthur I., ve Michael H. Moffett 2015. “Multinational Business Finance, Global Edition” Pearson Education Limited 14.Basım, sayfa 27-28 ve 101.

EREN, Seda. “Güney Kıbrıs'ta Bankacılık Krizi”. ASEM (Ankara Siyasal ve Ekonomik Araştırmalar Merkezi. Nisan 2013. (çevirimiçi) http://asem.org.tr/tr/publication/details/6083/G%C3%BCney-%C4%B1br%C4%B1s'ta-Bankac%C4%B1l%C4%B1k-Krizi. (erişim tarihi 26.04.2018).

ERKAN, Nurhan. “Finansal Bütünleşme”. Sermaye Piyasası Kurulu Araştırma Raporu. 2005. (çeivirmiçi) (http://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/936). (erişim tarihi 16.04.2018)

EXTANCE, Andy 2015. “The future of cryptocurrencies: Bitcoin and beyond” Nature Cilt. 526 Sayı 7571, sayfa21-23.

FARRONATO, Chiara, Jonathan Levin. “The rise of peer-to-peer businesses”. The sharing economy. Global Investor 2.15. Credit Suisse. 2015. (çevirimiçi) https://www.oxfordmartin.ox.ac.uk/downloads/GI_215_e_GesamtPDF_01_high.pdf. (Erişim tarihi 16.09.2018)

FERDMAN, Roberto A. “Argentina’s Unofficial Consumer Confidence Metric Is Free-Falling Again”. Quartz. 2013. (çevirimiçi) https://qz.com/138498/argentinas-unofficial-consumer-confidence-metric-is-free-falling-again/. (erişim tarihi 15.07.2018).

FINNEY, Hal. “Reusable Proofs of Work”.2004. (Çevrimiçi) https://nakamotoinstitute.org/finney/rpow/index.html. (Erişim Tarihi: 25.06.2018)

FONG, Jeff. “How Bitcoin Could Help the World’s Poorest People”. PolicyMic.2013. (çevirimiçi) http://mic.com/articles/41561/bitcoin-price-2013 -how-bitcoin-could-help-the-world-s-poorest-people. (erişim 15.07.2018).

GEORGOULA, I., Poutnarakis, D., Bilanakos, C., Sotiropoulos, D. N. ve Giaglis, G. M. 2015. “Using Time-Series and Sentiment Analysis to Detect the Determinants of Bitcoin Prices” Ninth Mediterranean Conference on Information Systems (MCIS) Proceedings, E. Loukis and Y. Charalabidis (eds.), Samos, Yunanistan.

GERNET Jacques. Daily Life in China, on the Eve of the Mongol Invasion, 1250-1276. Stanford University Press, 1962. ISBN 0804707200

GLASER, F., Zimmermann, K., Haferkorn, M., Weber, M. C. ve Siering, M., Goethe. 2014. "Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions," Twenty Second European Conference on Information Systems (ECIS) 2014 Proceedings, D. Dganit (ed.), Tel Aviv.

GLASER, F., and Bezzenberger, L. 2015. "Beyond Cryptocurrencies-a Taxonomy of Decentralized Consensus Systems," 23rd European Conference on Information Systems (ECIS), J. Becker, J.V. Brocke and M. De Marco (eds.), Münster, Almanya.

GRANT, Robert M. “Cases in Contemporary strategy analysis”. 2003. United States, UK, Australia, Germany: Blackwell publishing. ISBN 1-4051-1180-1.

GREEN, Phil 2015. “Risk Management: A Common Framework for the Entire Organization” Elsevier Science & Technology, sayfa 95.

GRIFFITH, Ken. “A Quick History of Cryptocurrencies BBTC — Before Bitcoin “. Nisan 2014. (çevirimiçi) https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/. (erişim tarihi 26.04.2018).

HANSON, Robin. “Idea Futures (a.k.a. Prediction Markets, Information Markets)”. 1992. (çevirimiçi) http://mason.gmu.edu/~rhanson/ideafutures.html. (Erişim 02.08.2018)

HARWICK, Cameron 2016. “Cryptocurrency and the Problem of Intermediation” Independent Review Cilt. 20 Sayı 4 sayfa 569-588.

HAYES, A. 2015. "Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin," in: Ninth Mediterranean Conference on Information Systems (MCIS), E. Loukis and Y. Charalabidis (eds.). Samos, Yunanistan.

HEADRICK Daniel R. Technology: A World History. Oxford University Press. 2009. ISBN 978-0-19-988759-0. s. 85.

HILEMAN, Garrick ve Michel Rauchs. “Global Cryptocurrency Benchmarking Study”. University of Cambridge. 2017. (Çevirimiçi) (Erişim Tarihi: 14.06.2018) https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf.

HILEMAN Garrick. The Bitcoin Market Potential Index. University of Cambridge. London School of Economics. 2014. (çevirimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752757.

HUR, Y., Jeon, S., and Yoo, B. 2015. "Is Bitcoin a Viable E-Business?: Empirical Analysis of the Digital Currency’s Speculative Nature," Thirty Sixth International Conference on Information Systems (ICIS) 2015 Proceedings, Y.J. Kim, M. Spann and Y. Yoo (eds.), Fort Worth.

HUTCHINSON, Martin; Dowd, Kevin 2015. “Bitcoin Will Bite The Dust “CATO Journal, Cilt. 35 Sayı 2, sayfa 357-382.

INGRAM, C., and Morisse, M. 2016. "Almost an Mnc: Bitcoin Entrepreneurs' Use of Collective Resources and Decoupling to Build Legitimacy," 49th Hawaii International Conference on System Sciences (HICSS), Hawaii, USA: IEEE, pp. 4083-4092.

INGRAM, C., Morisse, M., and Teigland, R. 2015. "'A Bad Apple Went Away': Exploring Resilience among Bitcoin Entrepreneurs," Twenty-Third European

Conference on Information Systems (ECIS), J. Becker, J.V. Brocke and M. De Marco (eds.), Münster, Almanya.

Japan's Ministry of Economy, Trade and Industry (METI). "Survey on Blockchain Technologies and Related Services FY2015 Report". Nomura Research Institute. 2016.

KAMINSKY, Graciela L.. "Varieties Of Currency Crises",2003, NBER Working Paper Series No. 10193. (çevirimiçi) http://www.nber.org/papers/w10193.pdf. (Erişim tarihi 15082018).

KAPLANOV, Nikolei M. Nerdy money: bitcoin, the private digital currency, and the case against its regulation. Temple University Legal Studies Research Paper. 2012. (çevirimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203. (erişim tarihi 14.05.2018).

KARAARSLAN, Enis. Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme. 2013. (çevirimiçi) http://dergipark.gov.tr/download/article-file/207215). (erişim tarihi 11.05.2018).

KATZ, M. L., and Shapiro, C. 1985. "Network Externalities, Competition, and Compatibility," The American Economic Review (75:3), pp. 424-440.

KAZAN, E., Tan, C.-W., and Lim, E. T. K. 2015. "Value Creation in Cryptocurrency Networks: Towards a Taxonomy of Digital Business Models for Bitcoin Companies" Pacific Asia Conference on Information Systems (PACIS) 2015 Proceedings, H.-H. Teo and V. Sambamurthy (eds.).

KINLEY, David. Money: A Study of the Theory of the Medium of Exchange. Simon Publications LLC. 1 September 2003. ISBN 193251211X.

KONDOR, Dániel; Pósfai, Márton; Csabai, István; Vattay, Gábor 2014. "Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network" PLoS ONE. Şubat, Cilt. 9 Sayı 2, sayfa 1-10.

KÖNIG, Susanne. The Evolutıon Of Money From Commodity Money to E-Money. UNICERT IV Program, 2001. (çevirimiçi) http://www.ww.uni-magdeburg.de/fwwdeka/student/arbeiten/009.pdf)

LEWIS, Antony. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them. Mango Publishing. 2018.

LINDE Frank, STOCK Wolfgang G; Information Markets: A Strategic Guideline for the I-Commerce., De Gruyter Saur, Berlin, Germany, pp. 617, 2011 (ISBN: 978-3-11-203609-5).

LUSTIG, C., ve Nardi, B. 2015. "Algorithmic Authority: The Case of Bitcoin," in: 48th Hawaii International Conference on System Sciences (HICSS). Hawaii, ABD IEEE, sayfa. 743-752.

LUTHER, William J. 2016. "Bitcoin and the Future of Digital Payments" Independent Review, Cilt. 20 Sayı 3, sayfa 397-404.

MAI, F., Bai, Q., Shan, Z., Wang, X. Ve Chiang, R. H. L. 2015. "The Impacts of Social Media on Bitcoin Performance," Thirty Sixth International Conference on Information Systems (ICIS) 2015 Proceedings, Y.J. Kim, M. Spann and Y. Yoo (eds.), Fort Worth.

MATONIS, Jon. "Bitcoin's Promise in Argentina". Forbes. 2013. (çevirimiçi) https://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/#77e0d21933d5. (erişim tarihi 15.07.2018).

MAURER, Bill; Nelms, Taylor C.; Swartz, Lana 2013. "When perhaps the real problem is money itself! : the practical materiality of Bitcoin" Social Semiotics. Nisan, Cilt. 23 Sayı 2, sayfa 261-277.

MAY, Timothy C. "The Crypto Anarchist Manifesto". (çevirimiçi) https://www.activism.net/cypherpunk/crypto-anarchy.html. 22.11.1992. (erişim tarihi 21.05.2018)

MCKENNA, Francine. "Here's how the U.S. and the world regulate bitcoin and other cryptocurrencies". 2017. (Çevrimiçi) https://www.marketwatch.com/story/heres-how-the-us-and-the-world-are-regulating-bitcoin-and-cryptocurrency-2017-12-18. (Erişim Tarihi: 25.01.2018).

MCKEON, Stephen. "What is a blockchain token?". PBS Conversation Paper. 2018. https://www.pbs.org/newshour/science/what-is-a-blockchain-token.

MCKNIGHT, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," Information Systems Research (13:3), pp. 334359.

MEIKLEJOHN, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. ve Savage, S. 2016. "A Fistful of Bitcoins: Characterizing Payments among Men with No Names," Communications of the ACM (59:4), sayfa. 86.

MEREDITH, Caleb. "Explaining GraphQL Connections". 23.02.2017. (Çevrimiçi) https://blog.apollographql.com/explaining-graphql-connections-c48b7c3d6976.

MIK, Eliza. "Smart Contracts: Terminology, Technical Limitations and Real World Complexity". Singapore Management University Paper. 2017. (Çevirimiçi) http://dx.doi.org/10.2139/ssrn.3038406. (erişim 12.09.2018).

MOLLER, Jan. "How The Bitcoin Protocol Actually Works". International Software Development Conference. GOTO. Copenhagen. 23-24 Eylül 2014.

MORISSE, Marcel 2015. "Cryptocurrencies and Bitcoin: Charting the Research Landscape," Twenty-first Americas Conference on Information Systems (AMCIS), A. Dennis and S. Paul (eds.), Puerto Rico, sayfa. 1-16

MOUGAYAR, William. "Tokenomics – A Business Guide to Token Usage, Utility and Value". 2017. (Çevrimiçi) http://startupmanagement.org/2017/06/10/tokenomics-a-business-guide-to-token-usage-utility-and-value/ (Erişim Tarihi: 25.01.2018).MICK, Jason, "Inside the Mega-Hack of Bitcoin: the Full Story". 2011. (çevirimiçi) https://tr.scribd.com/document/166287990/DailyTech-Inside-the-Mega-Hack-of-Bitcoin-the-Full-Story-pdf. (erişim tarihi 25.05.2018)

MUELLER, Ingo 2017. "No Revolution Yet for Blockchain "Communications of the ACM. Şubat, Cilt. 60 Sayı 2, Sayfa 9-9.

MUHAMMAD, Yunus. Banker to the Poor: Micro-Lending and the Battle against World Poverty.ABD.Public Affairs. 2003.

MUTLU, Elis. "Sosyal Etki Yatırımı". Kentsel Vizyon Platformu. (çevirimiçi) http://www.kentselvizyon.org/assets/sosyaletkiyatirimi.pdf. 2016.

NAKAMOTO, Satoshi. Bitcoin P2P e-cash paper. Cryptography Mailing List. 2008. (çevirimiçi) http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html. (erişim tarihi 23.05.2018).

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. (çevirimiçi), https://bitcoin.org/bitcoin.pdf, (erişim tarihi 23.05.2018).

NARAYANAN, Arvind, Joseph BONNEAU, Edward FELTEN, Andrew MILLER, Steven GOLDFEDER. Bitcoin and Cryptocurrency Technologies. Princeton University Press. 2016. ISBN9781400884155.

NARAYANAN, Arvind, Clark Jeremy. 2017. "Bitcoin's Academic Pedigree" Communications of the ACM Aralık, Cilt 60 Sayı 12, Sayfa 36-45.

NATCHKEBIA, Aleksandre. "Cryptocurrency regulation around the world in 2018". 2018. (Çevrimiçi) https://www.forexnewsnow.com/forex-analysis/cryptocurrency/cryptocurrency-regulation-overview/. (Erişim Tarihi: 05.09.2018).

NW3C (The National White Collar Crime Center)." Digital Currency and the Threats Involved". The Bureau of Justice Assistance U.S. Department of Justice.2017. (Çevirimiçi) https://www.nw3c.org/docs/research/digital-currency.pdf.

OBER, Micha, Stefan Katzenbeisser, Kay Hamacher. Structure and Anonymity of the Bitcoin Transaction Graph. Future Internet. cilt 5, sayı 2, s. 237-250. 2013. (çevirimiçi) https://www.mdpi.com/1999-5903/5/2/237.

ODABAŞI, Şafak Durukan. Kablosuz Mesh Ağlar, Yönlendirme Metrikleri ve Protokolleri. Akademik Bilişim Konferansı Bildirileri. İnönü Üniversitesi. Malatya. 2011. (çevirimiçi) https://ab.org.tr/ab11/kitap/_AB11_tek.pdf (erişim tarihi 28.04.2018).

OLIVER, R. L. 1980. "A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions," Journal of marketing research (17:3), pp. 460-469.

OSIPOVICH, Alexander. "Another Exchange Jumps on Bitcoin Bandwagon". The Wall Street Journal. 2018. (çevirimiçi) https://www.wsj.com/articles/another-exchange-jumps-on-bitcoin-bandwagon-1520868955. (erişim tariihi 21.07.2018).

O'SULLIVAN, Arthur, Steven M. Sheffrin. Economics: Principles in action. Upper Saddle River, New Jersey 07458: Pearson Prentice Hall. 2003. ISBN 0-13-063085-3. s. 246.

PACIA, Chris. Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics. Escape Velocity. 2013. (çevirimiçi) https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/. (erişim tarihi 27.06.2018).

PAREKH, Sameer. Prospects for Remailers: Where is the Anonymity Heading on the Internet. First Monday, Sayı 1, 5 Ağustos, 1996. (Çevrimiçi). http://ojphi.org/ojs/index.php/fm/issue/view/71. (Erişim Tarihi: 25.06.2018), s.2.

PECK, Morgan E. 2013. " The Bitcoin Arms Race is on!," IEEE Spectrum (50:6), sayfa 11–13.

PETERSON Jack, Joseph Krug, Micah Zoltu, Austin K. Williams, and Stephanie Alexander. "Augur: a Decentralized Oracle and Prediction Market Platform". 3 Şubat 2018. (Çevirimiçi) http://www.augur.link/augur.pdf, (Erişim tarihi 14.08.2018)

PIKETTY, Thomas; Capital In The Twenty-First Century. The Belknap Press of Harvard University Press. Cambridge, Massachusetts London, England. 2014

PRENSKY Marc; Digital Natives, Digital Immigrants. MCB University Press, Vol. 9 No. 5, October 2001.

POLASIK, M., Piotrowska, A. I., Wisniewski, T. P., Kotkowski, R., ve Lightfoot, G. 2016. "Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry," International Journal of Electronic Commerce (20:1), sayfa. 9-49

RAVAL, Siraj; Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, O'Reilly Media, Inc., Amerika, 2016.

REID, Fergal, Martin Harrigan. An Analysis of Anonymity in the Bitcoin System. Cornell University Library. 2013. (çevirimiçi) https://arxiv.org/abs/1107.4524, (erişim tarihi 27.04.2018).

ROONEY, Kate. "Your guide to cryptocurrency regulations around the world and where they are headed". 2018. (Çevrimiçi) https://www.cnbc.com/2018/03/27/a-

complete-guide-to-cyprocurrency-regulations-around-the-world.html. (Erişim Tarihi: 13.09.2018).

ROSENBERG, Burton. “Handbook of Financial Cryptography and Security”. CRC Press. ISBN-13:978-1-4200-5982-3 (e-Book-PDF), 2011.

RUBENS, Paul. “Liberty Reserve: Criminals face online cash dilemma”. 2013. (Çevrimiçi) https://www.bbc.com/news/technology-22766406 (Erişim Tarihi: 25.01.2018).

RUTLEDGE, Susan L., Nagavalli Annamalai, Rodney Lester, Richard L. Symonds. Good Practices for Consumer Protection and Financial Literacy in Europe and Central Asia: A Diagnostic Tool. ECSPF Working Paper. World Bank. (çevirimiçi) (https://openknowledge.worldbank.org/bitstream/handle/10986/12828/703420ESW0P1120008Oct080for0release.pdf?sequence=1&isAllowed=y), 2010.

SALMON, Felix. “The Bitcoin Bubble and the Future of Currency”. 2013. (çevirimiçi) https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb. (Erişim tarihi 14.08.2018)

SCHAPS, David M.. "The Invention of Coinage in Lydia, in India, and in China,". XIV International Economic History Congress. Helsinki. 2006. (çevirimiçi) http://www.helsinki.fi/iehc2006/papers1/Schaps.pdf.

SEYFANG, Gill. “Time banks: Rewarding community self-help in the inner city?”. Community Development Journal. NO.39(1). 2004. (çevirimiçi) https://www.researchgate.net/publication/31202656_Time_banks_Rewarding_community_self-help_in_the_inner_city/download. (Erişim tarihi 21.06.2018).

SHADAB, Houman. “What Are Smart Contracts, and What Can We Do with Them? A Backgrounder for Policymakers”. Coin Center. 2014. (çevirimiçi) https://coincenter.org/entry/what-are-smart-contracts-and-what-can-we-do-with-them. (erişim tarihi 16.07.2018).

SHAW, William Arthur. The History of Currency, 1252–1896. Augustus m Kelley Pubs. 1989. ISBN 0678002568.

SHIRKY, Clay, Kelly TRUELOVE, Rael DORNFEST, Lucas GONZE. 2001 P2P Networking Overview: The Emergent P2P Platform of Presence, Identity, and Edge Resources. O'Reilly Media, Inc. 2001.

SINGH, Sara. "The Evolution of Giving: An Exploration of Time Banking as a Community Development Instrument". 2017. University of South Carolina. Scholar Commons. Senior Theses. (Çevirimiçi) https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1211&context=senior_theses, (erişim tarihi 23.07.2018).

SİRER, Emin Gün 2016. "The State (and Security) of the Bitcoin Economy" Communications of the ACM. Cilt. 59 Sayı 4 sayfa85-85.

SKLAROFF, Jeremy M 2017. "Smart Contracts And The Cost Of Inflexibility" University of Pennsylvania Law Review, Kasım, Cilt 166 Sayı 1, sayfa263-303.

SOMPOLINSKY, Yonatan; Zohar, Aviv 2018. "Bitcoin's Underlying Incentives" Communications of the ACM. Mart, Cilt 61 Sayı 3.

SOPPE, Aloy Routledge 2016. "New Financial Ethics: A Normative Approach" Routledge, sayfa 203-209

SOUTHURST, Jon. Apple Removes Blockchain Bitcoin Wallet Apps from its App Stores. CoinDesk. 2014. (çevirimiçi) https://www.coindesk.com/apple-removes-blockchain-bitcoin-wallet-from-app-stores/. (erişim tarihi 27.05.2018).

SZABO, Nick. "Bit gold". 27.12.2008. (Çevrimiçi) http://unenumerated.blogspot.com/2005/12/bit-gold.html. (Erişim Tarihi: 25.06.2018).

SZABO, Nick. "Micropayments and Mental Transaction Costs". 1999. (Çevrimiçi) https://nakamotoinstitute.org/static/docs/micropayments-and-mental-transaction-costs.pdf. (Erişim Tarihi: 25.06.2018).

SZABO, Nick. "Intrapolynomial Cryptography". 1999. (Çevrimiçi) https://nakamotoinstitute.org/intrapolynomial-cryptography/#selection-7.7-7.35. (Erişim Tarihi: 25.06.2018).

SZABO, Nick. “Shelling Out: The Origins of Money”. 2002. (Çevrimiçi) https://nakamotoinstitute.org/shelling-out/. (Erişim Tarihi: 25.06.2018).

SZABO Nick. Smart Contracts. (çevirimiçi) http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. (erişim tarihi: 16.07.2018).

ŞAMLIOĞLU, Hamza. “NetSpot WiFi Durumu ve Kablosuz Sinyali Ölçümü”. TEAkolik Blog. 2016. (çevirimiçi) https://www.teakolik.com/netspot-wifi-durumu-ve-kablosuz-sinyali-olcumu/. (erişim 17.07.2018).

TCMB. Türkiye’de Banknot Basımının Tarihçesi, Banknot Üretim Süreci ve Emisyon Politikaları. Ankara. 2012. ISBN (elektronik): 978-605-5758-83-7.

TERZİ, Fatih, Mehmet OCAKÇI. “Kentlerin Geleceği: Akıllı Kentler”. İTÜ Vakıf Dergisi. S. 77 (Temmuz-Eylül 2017). ss. 10-13.

TINDELL, Ken. Geeks Love The Bitcoin Phenomenon Like They Loved The Internet In 1995. Business Insider. 2013. (çevirimiçi) https://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4. (erişim tarihi 15.04.2018).

TOMAŠ, B., ve Švogor, I. 2015. "The Bitcoin Phenomenon Analysis," in: 28th Bled eConference, J. Versendaal (ed.). Hırvatistan.

TORPEY, Kyle. “Chris Odom Explains How Open Transactions Make Altcoins Irrelevant at Inside Bitcoins Conference”. CryptoCoinsNews,. 2014. (çevirimiçi) https://www.ccn.com/chris-odom-explains-how-open-transactions-makes-altcoins-irrelevant-at-inside-bitcoins-conference/. (erişim tarihi 15.07.2018).

TSUKERMAN, Misha 2015. “The Block is Hot: A Survey Of The State Of Bitcoin Regulation And Suggestions For The Future” Berkeley Technology Law Journal, Özel sayı 30, sayfa 1127-1169.

ULM Bogdan. Bitcoin ATMs boom: new locations. CoinTelegraph. 2014. (çevirimiçi) https://cointelegraph.com/news/bitcoin-atms-boom-new-locations. (erişim tarihi 27.06.2018).

UNDERWOOD, Sarah 2016. “Blockchain Beyond Bitcoin” Communications of the ACM. Kasım, Cilt. 59 Sayı 11 sayfa 15-17.

USA The Law Library of Congress. Global Legal Research Center. Regulation of Cryptocurrency Around the World. 2018. (çevirimiçi) https://www.loc.gov/law/help/cryptocurrency/argentina.php. (erişim tarihi: 15.07.2018).

ÜZER, Betül. 2015. "Sanal Para Birimleri" Türkiye Cumhuriyet Merkez Bankası Ödeme Sistemleri Genel Müdürlüğü Uzmanlık Yeterlik Tezi

VALDEZ, Stephen; Molyneux, Philip 2015. “An Introduction to Global Financial Markets“ Palgrave Macmillan, 2.bölüm.

VAN Alstyne, Marshall 2014. “Why Bitcoin Has Value” Communications of the ACM. Mayıs, Cilt. 57 sayı 5, sayfa 30-32.

WALLACE, Benjamin. "The Rise and Fall of Bitcoin". 2011. (çevirimiçi) https://www.wired.com/2011/11/mf-bitcoin/, (erişim tarihi 26.04.2018)

WATSON, Liv A.; Mishler, Chris 2017. “Get Ready For Blockchain” Strategic Finance. Ocak, Sayfa 62-63.

WAUPSH, John 2016. “Bankruption: How Community Banking Can Survive Fintech” Hoboken: Wiley, sayfa 192-249.

WHITE, Lawrence H. “Is the Gold Standard Still the Gold Standard Among Monetary Systems?”. CATO Institute Briefing Papers. 2008. no.100.

WHITE, Lawrence H. 2015. “The Market For Cryptocurrencies” CATO Journal, Cilt. 35 Sayı 2, sayfa 383-402.

WIRDUM, Aaron van, ” The Genesis Files: How David Chaum’s eCash Spawned a Cypherpunk Dream”. 24 Nisan 2018. (Çevrimiçi). https://bitcoinmagazine.com/articles/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream/. (Erişim Tarihi:14.06.2018)

World Bank Group. World bank trends in migration and remittances. Migration And Development Brief 27. Recent Developments and Outlook. 2017. (çevirimiçi) http://www.worldbank.org/en/news/infographic/2017/04/21/trends-in-migration-and-remittances-2017. erişim 14.07.2018.

WÖRNER, Dominic.; Von Bomhard, Thomas; Schreier, Yan-Peter; Bilgeri, Dominik 2016. " The Bitcoin Ecosystem: Distruption Beyond Financial Services?" 24. Avrupa Bilişim Sistemleri Konferansı (ECIS) İstanbul, Türkiye, 2016.

YLI-Huumo, Jesse; Ko, Deokyoon; Choi, Sujin; Park, Sooyong; Smolander, Kari 2016." Where Is Current Research on Blockchain Technology?—A Systematic Review" PLoS ONE. Cilt. 11 Sayı 10 sayfa 1-27.

ZARIFIS, A., Efthymiou, L., Cheng, X. ve Demetriou, S. 2014. "Consumer Trust in Digital Currency Enabled Transactions," in Business Information Systems Workshops: Bis 2014 International Workshops, Larnaca, Cyprus, May 22-23, 2014, Revised Papers, W. Abramowicz and A. Kokkinaki (eds.). Cham: Springer International Publishing, sayfa. 241-254.

ZOHAR, Aviv. 2015. "Bitcoin: Under the Hood," Commun. ACM (58:9), Sayfa. 104-113.