Yayın Geliş Tarihi: 21.09.2019

Yayın Onay Tarihi: 29.12.2019

DOI No: 10.35343/kosbed.623097

Cemil ERARSLAN •

Bitcoin'in Özellikleri, Teknolojik Altyapısı, Ulusal Para Sistemleri İçin Oluşturduğu Fırsat ve Tehditler

Features, Technological Infrastructure, Opportunities and Threats for National Monetary Systems of Bitcoin

Özet

Çalışmada bir dijital kripto para birimi olan Bitcoin'in ortaya çıkışı, özellikleri, dayandığı teknolojik temeller ile oluşturduğu fırsat ve tehditler incelenmiştir. Bu bağlamda Bitcoin'in ulusal para sistemleri için alternatif bir ödeme aracı olarak kullanılıp kullanılamayacağı sorunsalına yanıt aranmıştır. Bitcoin'in dayandığı blok zinciri teknolojisi, bankacılık faaliyetlerine hız kazandırması, maliyetleri düşürmesi, hatalı işlemleri minimuma indirmesi ve bilgisayar korsanlığı gibi dolandırıcılık faaliyetlerine karşı güvenli olması sebebiyle, ulusal bankacılık ve finans sistemleri tarafından kullanılabilecek etkin ve verimli bir çözüm yöntemi olabilir.

Anahtar Kelimeler: Bitcoin, Blok Zinciri Teknolojisi, Dijital Kripto Paralar

JEL: E0, E4, E5, E6

Abstract

In this study, the emergence of Bitcoin, a digital crypto currency, its features, technological foundations on which it is based, the opportunities and threats it creates are examined. In this context, a response to the question of whether Bitcoin can be used as an alternative payment instrument for national monetary systems has been sought. Blockchain technology on which Bitcoin relies can be an effective and efficient sol*ving* that can be used by national banking and financial systems, as it accelerates banking activities, reduces costs, minimizes erroneous transactions and is highly secure against fraud activities such as hackers.

Key Words: Bitcoin, Blockchain Technology, Digital Crypto Currencies

JEL: E0, E4, E5, E6

• Doç. Dr., Yalova Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İktisat Bölümü, Orcid ID:0000-0002-3923-7633, email: cemilerarslan@hotmail.com

Giriş

ABD'de Mortgage Sistemi'nden kaynaklı olarak başlayan ve 2008/2009 döneminde AB ekonomilerine sıçrayarak küresel bir hale gelen finansal krizle mücadele etmek için, Amerikan Merkez Bankası (FED) öncülüğünde, politika faiz oranlarını düşürücü nitelikte genişletici para politikası uygulamalarına geçiş yapılmıştır.

Bu süreçte FED, satın aldığı sorunlu (toxic) varlıklar karşılığında bilançosunda önemli bir büyümeye giderek, tüketim ve yatırım harcamalarını teşvik ederek büyüme oranlarındaki kayıpları telafi etmek için piyasaya yoğun biçimde para arz etmiştir. Böylece FED'in bilanço büyüklüğü, finansal kriz öncesinde yaklaşık olarak 800 milyar $ iken, tahvil alım programı sebebiyle 4 trilyon $'ı aşmıştır.

Bu süreçte piyasada bollaşan para arzı nedeniyle, başta ABD doları olmak üzere, genişlemeci para politikası izleyen ülkelerin ulusal para birimleri sert değer kayıpları ile karşılaşmışlardır. Bu da söz konusu para birimlerinin değer saklama aracı olma özelliklerine olan güveni sarsmıştır.

Satoshi Nakamoto'nun 2008 yılında yazdığı bir makaleye dayanan ve 2009 yılında çalışmaya başlayan dünyanın ilk merkezi olmayan para birimi olan bitcoin, yeni bir parasal değer ölçü birimi arayan yatırımcıların dikkatini çekerek kısa sürede popüler olmuştur.

2010 yılındaki değeri yaklaşık olarak 0.30 $'a eşitken, 2017 yılının Aralık ayında 19.890 $'a kadar yükselmiştir. 2019 yılı itibariyle toplam kripto para sayısı 4.900'ün üzerine çıkmış, bunların toplam büyüklüğü ise 250 milyar $'a yaklaşmıştır.

Bitcoin'in dayandığı teknolojik temel olan blok zincirleri, dağıtılmış bir veri ağı üzerinden, matematiksel denklemler aracılığı ile çalışmaktadır. Sistemin en büyük avantajı ise dışarıdan müdahaleye imkan tanımamasıdır.

Kripto paraların gelişim sürecinin incelenmesi, çalışma prensiplerinin ortaya konulması, ulusal para sistemlerinin geleceğinde oynayacakları rollerin belirlenmesi açısından oldukça önemlidir. Böylece ulusal para sistemlerine bir alternatif olup olamayacaklarının anlaşılmasına aracılık edecektir.

Çalışmada ilk dijital kripto para birimi olan bitcoin'in ortaya çıkışı, özellikleri, dayandığı teknolojik temeller ile oluşturduğu fırsat ve tehditler incelenmiştir. Bu bağlamda bitcoin'in ulusal para sistemleri için alternatif bir ödeme aracı olarak kullanılıp kullanılamayacağı sorunsalına yanıt aranmıştır.

Bunun için öncelikle bitcoin'in tarihçesi ve temel özellikleri incelenmiş, blok zincirleri üzerinde durulmuş, son olarak ise ulusal para sistemleri için sunduğu fırsatlar ve tehditlere yer verilmiştir.

Çalışmanın literatüre katkısı, bitcoin'in çalışma prensiplerinin ve sahip olduğu yeni yazılım teknolojilerine dayalı altyapısının daha iyi tanınmasını sağlamak ve bu sayede ulusal para sistemlerinin işleyişinde meydana getirdiği değişiklikleri açıklamaktır.

1. Bitcoin'in Tarihçesi ve Temel Özellikleri

Bitcoin, Satoshi Nakamoto tarafından 2008 de tanıtılan ve açık kaynak kodlu yazılımlara dayanarak, çevrim içi ağlar üzerinden alınıp satılabilen ilk dijital para birimidir. Bu anlamda Nakamoto, bitcoin'in kurucusu olarak kabul edilir. Nakamoto'ya göre bitcoin, "güven yerine şifreleme kanıtı üzerine kurulu, iki tarafın birbirleri ile doğrudan bağlantılı olduğu, elektronik bir ödeme sistemidir" (Nakamoto, 2008: 1).

Kripto paralar, blok zinciri teknolojisi üzerine kurulmuştur. Söz konusu veri tabanı, çift harcama sorununa çözüm getirmek için geliştirilen, yapılan işlemlerin kronolojik sıralamasını hesaplama kanıtı oluşturmak amacıyla saklayan ve *"denkler arası (peer to peer)"* dağıtılan bir ağdır. Sistem, ağa dahil olan dürüst işlemci gücünün, ortak çalışan saldırgan işlemci gücünden fazlalığı oranında güvenlidir. Dağıtılmış veri ağı, bitcoin işlemlerini tersine çevirmek için hesaplanması zor olan formülleri de bünyesinde bulundurur. Bu sayede tarafları dolandırıcılıktan koruma özelliğine de sahiptir (Nakamoto, 2008: 1-2).

Kriptografi adı verilen bir gizli yazılım ve kodlama yöntemine dayalı olarak üretilen bitcoin, 2009 yılında açık erişime imkan veren blok zinciri sayesinde, alım ve satım işlemlerine konu olacak şekilde piyasaya sunulmuştur. Sistem, açık kaynak kodlarından oluştuğu için kayıtlar herkese açıktır ve kolayca doğrulanabilmektedir. Bitcoin'in tamamen dijital oluşu, fiziki olarak basılmasına ihtiyaç duyulmaması, işlem maliyetlerinin düşük oluşu, popülaritesini gün geçtikçe artırmaktadır (Antonopoulos, 2014: 1-5).

Bitcoin, geleneksel para birimlerinden ve elektronik ödeme yöntemlerinden farklı olarak, bir merkez bankasının varlığına ihtiyaç duymaz. Kullanıcılara, sistem tarafından otomatik olarak iki farklı anahtar tanımlanır. Bunlardan birincisi "genel anahtar (public key)" ve diğeri de "özel anahtar (private key)" dır. Genel anahtardaki tüm bilgileri herkes görebilir, fakat özel anahtarlardaki bilgiler kişiye özeldir. Dağıtılmış veri ağları, kamuya açık biçimde kopyalanan bilgiler içermektedir. Bu sebeple kullanıcılar, gizliliklerini artırmak için sahte kimlik (veya takma ad) kullanabilirler (Ben-Sasson et.al., 2014: 459).

Bitcoin, blok zincirlerinden oluşan kripto para sistemlerinin odak noktasındaydı. Kripto para sayısının giderek artması nedeniyle, yeni gelişen teknolojilerin sayısız uygulama alanından ilki ve en önemlisi olarak düşünülmektedir. Blok zincirlerinin merkezi olmayan bir teknoloji olması, kripto paraların anonim olmasına yol açmaktadır. Kripto para satın alabilmek için bir coin borsasına (Binance, Bittrex, Bitfinex gibi) üye olunması ve dijital cüzdan (wallet) alınması yeterli olmaktadır. Bitcoin ile ödeme kabul eden firmaların ürün ve hizmetlerini, dijital cüzdan hesaplarına saniyeler içerisinde transfer yaparak, kolayca ve güvenli şekilde satın almak mümkün olmaktadır (Antonopoulos, 2014: 15-20).

Bitcoin'in dağınık bulunan işlemci güçler sayesinde, transfer işlemlerini anlık olarak onaylayan bir mekanizmayla, çifte harcama problemini engellemesi en büyük özelliklerinden birisidir. İşlemci ağı içerisinde bilgi paylaşımları için yeni çözümler

getirmesi ve sistemin tamamen şeffaf olma özelliğini de barındırması, kullanıcılarına önemli avantajlar sağlamaktadır (Çarkacıoğlu, 2016: 15).

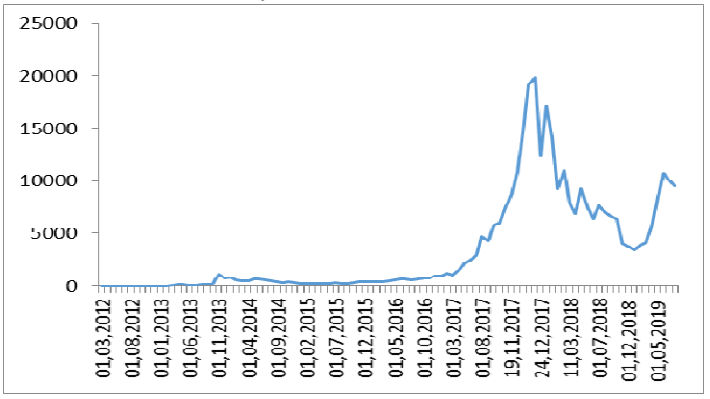
Blok zincirleri, kullanıcılar arasında kripto para işlemlerini seri hale getirmek ve fon taşıyan işlemleri korumak için tasarlanan bir yazılımdır. Çekirdek teknolojik yenilik gücü, hataları görme ve ayıklamaya son derece duyarlı işlem mekanizması, güçlü algoritmalara sahip altyapısı, yeni nesil internet etkileşimleri için anonim çevrim içi ödemelere, dijital varlıkların hızlı ve maliyetsiz biçimde havalesine izin vermesi ve akıllı dijital sözleşmelere sahip olması gibi özellikleri bünyesinde barındırır (Eyal, et.al., 2016: 46-47).

Bitcoin dışındaki diğer dijital kripto paralara "altcoin" denilmektedir. Altcoinlerin sayısı gün geçtikçe artmaktadır. Coinmarketcap verilerine göre 30 Ağustos 2019 tarihi itibariyle, piyasada toplamda 2.538 kripto para vardır. Bunların toplam büyüklüğü ise 249 milyar $'a eşittir. Bitcoin (BTC), 172 milyar $'lık piyasa hacmi ile ilk sıradadır. İkinci sırada 18 milyar $'a eşit Ethereum (ETH), üçüncü sırada ise 11 milyar $'lık piyasa hacmi ile Ripple (XRP) gelmektedir.

Piyasa payı en yüksek olan diğer sanal para birimleri ise sırasıyla şunlardır: Bitcoin Cash (BCH, 5.06 milyar $), Litecoin (LTC, 4.11 milyar $), Tether (USDT, 4.02 milyar $), Binance Coin (BNB, 3.46 milyar $), EOS (2.99 milyar $), Bitcoin SV (BSV, 2.31 milyar $), Stellar (XLM, 1.23 milyar $), Monero (XMR, 1.17 milyar $), Cardano (ADA, 1.16 milyar $), Tron (TRX, 1.04 milyar $), Huobi Token (HT, 951 milyon $), Dash (DASH, 728 milyon $), Ethereum Classic (ETC, 723 milyon $), IOTA (MIOTA, 698 milyon $), Tezos (XTZ, 697 milyon $), NEO (620 milyon $).[1]

Grafik 1'de Bitcoin'in 2012-2019 dönemindeki Amerikan doları cinsinden fiyat hareketleri gösterilmiştir.

Grafik 1: Bitcoin'in Fiyat Hareketleri



Bitcoin, tarihteki en yüksek değerine, 2017 yılının Aralık ayında ulaşmıştır. 17 Aralık 2017 tarihinde 1 Bitcoin, 19.891 $ olmuştur. Yükseldiği hızla değer kaybetmeye başlamış

[1] Bitcoin ve diğer kripto para birimlerinin fiyat hareketleri, hacimleri, piyasa büyüklüğü ve sıralamaları hakkında ayrıntılı bilgi için bkz. https:/coinmarketcap.com/30.08.2019.

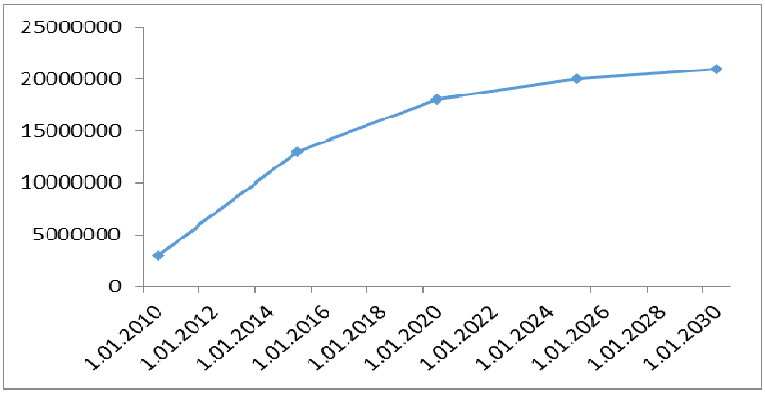
ve düşüş eğilimi, 2018 yılında da devam etmiştir. Fiyatında en yüksek dalgalanmanın gözlendiği dönemler, 2017 ve 2018 yılları olmuştur.

Fiyat dalgalanmaları, kripto paraların alternatif bir ödeme aracı olarak kullanılmasını güçleştirmektedir. Tasarruf sahipleri ve yatırımcılar, mallarının değerini korunmasını isterler ve istikrar kazanmayan varlıklara güven duymazlar.

Bitcoin, 8 basamağa kadar bölünebilir ve en küçük birimi Satoshi olarak isimlendirilir. Buna göre 1 BTC aynı zamanda, 100 milyon Satoshi'ye eşittir. Diğer bir ifadeyle dijital para kullanıcıları, 0,00000001 Satoshi'lik işlemler dahi yapabilirler. Kripto paralar, dijital imza zinciri olduğu için, borsaya kayıt olunup bir cüzdan (wallet) alındığında, aynı zamanda açık ve özel anahtar sahibi de olunmuş olur. Anahtarlar, belirli kombinasyonlar ile dizilen sayı ve rakamlardan oluşmaktadır. Bunları banka hesap numaralarına ya da IBAN numaralarına benzetmek mümkündür. Cüzdan adresi bilinen bir kişinin tüm yaptığı işlemler görülebildiğinden, blok zincirleri oldukça şeffaf biçimde çalışmaktadır.

Kripto paralar, istenildiği an dolar, TL ya da Euro gibi para birimlerine dönüştürülebilir. Sistem, toplamda en çok 21 milyon BTC arzı üretilecek şekilde sınırlandırılmıştır. 30 Ağustos 2019 itibariyle, dolaşımda 17.906.337 BTC bulunmaktadır. Grafik 2'de 2010 ile 2030 yılları arasında üretilen ve üretilmesi muhtemel miktarlar gösterilmiştir.

Grafik 2: Üretilen ve Üretilmesi Muhtemel Bitcoin Sayısı



Kaynak: Antonopoulos, et.al., 2014.

Bitcoin üretimi, 2010 yılında 3 milyon iken 2015 yılında 13 milyona, 2019 yılında ise 17 milyona yükselmiştir. Bu sayının 2020 yılında 18 milyona, 2025 yılında 20 milyona ve 2030 yılında ise 21 milyona ulaşarak sonlanması beklenmektedir.

Kripto para üretimi, madenci adı verilen ve merkezi olmayan küresel ağdaki gönüllü kişilerin bilgisayarlarının işlemci güçleri ile yapılır. Bu kişiler transfer işlemlerini doğrulayarak onay verirler. Karmaşık matematik formüllerini çözerek, sistem tarafından bitcoin ile ödüllendirilirler. Problemler giderek zorlaşır ve verilen ödüller, her 4 yılda bir yarıya iner (Çarkacıoğlu, 2016: 12-13).

Tüm işlemler bir bloğa kaydolduğundan, kripto paraların üretimi, yüksek işlem gücü gerektiren bir matematiksel bulmacayı çözmeye benzetilebilir. Bitcoin üretimi, sadece bulmaca doğru biçimde çözüldüğünde gerçekleşebilir. Tüm işlemler, temel defterlere her kullanıcı tarafından görülecek şekilde kaydedilir. Çözülen her bulmaca için, protokol ya da blok ödülü adı verilen değerler, ilişkili işlemin sonraki kayıtlı bloğuna yerleştirilmektedir. Alınan sabit miktar, her bir kayıt bloğunun protokolü, yıllar içinde azalma eğilimindedir (Dimitri, 2017: 31).

Transfer işlemleri sistem tarafından şifrelenip, özel anahtarlar ile çözümlenir. Buna "açık anahtar şifrelemesi (public key encryption)" denir. Özel anahtarlar, kullanıcılara özgüdür ve kesinlikle başkaları ile paylaşılmamalıdır. Çünkü satın alınan miktarlar, özel anahtarların bağlı olduğu dosyalarda saklanmaktadır. İlgili dosyaların bilgisayardan silinmesi durumunda, cüzdanın içinde bulunan tüm coinler kaybedilmiş olacaktır. Kullanıcılar, hacklenme olasılığına karşı, işlem yaptıkları elektronik aygıtlara, güncel anti-virüs programları yüklemeli ve yedekleme işlemlerini zamanında yapmalıdırlar (European Central Bank, 2012: 20-22; Usta ve Doğantekin, 2017: 118-120).

Kodlama dilinin uygulamalı olarak kullanılması, başka birçok etkileşim türünü mümkün kılmaktadır. Bitcoin'in temel özellikleri aşağıdaki gibi sıralanabilir: (Bonneau, et.al., 2015: 118-119)

- **Aracısızlaşma:** Üretiminin ve kullanımının genel tasarım süreci, güvenilir bir aracıya olan ihtiyacını gidermektedir. Buna göre alımlar, satımlar ve transferler, işleme giren taraflar arasında doğrudan yapılabilmektedir.

- **Atomsallık:** Çoğu durumda istenen bir güvenlik özelliği tarafından sağlanan işlevler kullanılarak, yapılan işlemlerin birden fazla taraf imzalayana kadar geçersiz olmasıdır. İşlemler, katılan tüm taraflarca görülebilmektedir. Tüm taraflar imzalayana kadar, katılımcıların varlıkları değişmeden kalmaktadır. Ödemeler protokolü adı verilen bu yöntemle, bir tarafın yetkilendirilmesine izin vermek için, diğer bir grubun onayının alınması gerekmektedir. Bu onay çıkmadıkça, kullanıcıların ellerindeki coinleri takas etmesine izin veren çapraz zincir değişim protokolü, iki bağlantılı işlemlerle, varlıkların değişimini durdurmaktadır. Böylece katılımcıların işlemden vazgeçme hakkı korunmuş olur.

- **Teminat Garantisine Sahip Olma:** İşlem güvenliğini artırmak için, istenen bir güvenlik özelliği doğrudan uygulanamadığında, sisteme teminat yatırılabilmesine izin verilmesidir. Sisteme yatırılan teminatlar, işlemlerin onaylanması ve transferlerin gerçekleşmesi durumunda, sistemden geri alınabilmektedir.

- **Denetlenebilirlik:** Blok zincirleri sisteminde tanımlanmış güvenli adresler olarak bilinen yeşil adresler, sisteme yönelik suçların kanıtlanmasında önemli bir rol oynamaktadır. Yeşil adres alan kullanıcılar, tanınmış bir ortak anahtara sahip ödeme işlemcileri, geçersiz veya çelişkili bir faaliyette bulunmayacaklarına dair söz vermiş olurlar. Kullanıcılar, tüm işlemlerin bloklarda yer almasını sağlarlar ve bunu istedikleri her an görebilirler. Eğer bir noktadaki işlemler birbirleriyle çakışırsa, sistemde yer alan kullanıcılar, aldatan tarafa dair bilgileri kolayca görecekleri için ona karşı kontrol edilebilir bir kanıt elde ederler. Bu sayede bitcoin'in arz güvenliği sağlanmış olur. Hatalı

veya dürüst olmayan işlemler, kullanıcılar tarafından önlenir. Bu işlemlere giren kullanıcılar da, sistem tarafından uyarılır ve tekrarı halinde de sistemden çıkarılır.

● **Güvenli Zaman Damgası:** Sistemlerin, arz kaynağında yer alan güvenli bir zaman işlemcisine sahip olmasıdır. Servis sağlayıcılardan, güvenilir verileri toplamayı mümkün kılar. Bu da kullanıcılara istedikleri verileri depolama şansı vermektedir. Bitcoin'in yeni türlerinin doğması anlamına gelen "çatallaşma (fork)" dönemlerinde, geçmiş fiyat ve miktar hareketleri görülerek durum değerlendirmesi yapılabilir.

● **Dijital Belirteçler (Renkli Paralar):** Sistem, kullanıcılara tuttukları bireysel veriler ve kayıtları, diğerlerinden ayırt etmek için izin vermektedir. Bir dizi kuralı tanımlamak üzere oluşturulan protokollere, "renkli paralar" adı verilmektedir. Bireysel işlemlere yazılmış verilerden oluşan bu paralar, başlangıçta yalnızca geçmiş verileri izleme işlevine sahipken, alım/satım stokları, mülkiyet hakları uygulamalarında da kullanılmaya başlamıştır. Protokol kuralları, işlemlerin doğrulanması için tüm blok zincirini taramayı gerektirir. Çünkü her işlem çıktısının, farklı kullanıcılar için taramalara, her defasında sistem tarafından otomatik olarak bir renk atanır. Kullanıcılar, bu verilere ihtiyaç duyduklarında kolayca ulaşabilirler.

3. Bitcoin'in Teknolojik Altyapısı: Blok Zincirleri

Blok zincirleri, dijital verilerin kopyalanmasına değil, dağıtılmasına izin veren internet tabanlı oldukça yeni bir sistemdir. Başlangıçta bitcoin için tasarlanmış olsa bile, finansal işlemlerin yürütülmesinde sağladığı büyük kolaylıklar ve ortaya çıkardığı geniş potansiyel sebebiyle, bankacılık kesimi tarafından da kullanılmaya başlanmıştır. Blok zincirlerindeki bilgiler, paylaşılan ve sürekli güncellenen bir veri tabanı halinde varlığını sürdürmektedir. Blok zinciri veri tabanı, tek bir konumda saklanmadığı için, hackerların erişip bozabileceği merkezi sürümü de bulunmamaktadır. Aynı anda milyonlarca bilgisayarda barındırıldığından, veri tabanındaki bilgilere internet kullanıcısı olan herkes erişebilmektedir.

Blok zincirleri, kıymet içeren her türlü verinin, güvenilir biçimde saklanarak yönetilmesine dayanmaktadır. Kapalı merkezi sistemlere ve aracı kurumlara ihtiyaç duymayan, aynı zamanda tüm taraflara açık olduğu için şeffaf bir sistemdir. Bu sistemde veriler, zamansal olarak doğrusal biçimde saklanırlar. Bilgilerin dağınık şekilde bulunma özelliği nedeniyle, veriler açık ağlar üzerinden sisteme giren tüm ortak katılımcılar tarafından görülüp, işletim sistemlerinde saklanmaktadır. İşlem maliyetlerinin ve bilgilerin çalınma risklerinin azalmasına olanak sağlamaktadır. Sistemlerde, veri hırsızlığı ancak kimseye fark ettirilmeden olabilir. Ancak bunun için de hedef blok ile sonra gelen blokların tamamının farklı olması gerekir. Buna karşılık sistemde sürekli yeni bloklar inşa edildiği için (blok devamlılığı), bunun gerçekleşme olasılığı pratikte imkansıza yakındır (Usta ve Doğantekin, 2017: 123-127).

Bir blok zinciri, esasen dağıtılmış kayıtlı veri tabanından, genel olarak tüm işlemlerin muhasebesi ile dijital olarak gerçekleştirilen olaylardan ve katılan tüm taraflar arasında paylaşılan bilgilerden oluşmaktadır. Kripto paraları, popüler yapan temel unsur, arkasındaki bu mükemmel işleyen sistemlerdir. Bu sayede kullanıcılar, düzenleyici işlemler ile uğraşmadan, yüksek hızda tüm alım ve satımlarını

gerçekleştirebilmektedirler. Dolayısıyla blok zincirleri, ilk sanayi devriminin ortaya çıkmasında kilit rol oynayan buharlı ve içten yanmalı motorlar gibi algılanabilir (Crosby, et.al., 2016: 8).

Blok zincirleri, yeni bir dijital devrimin öncüsü olarak, internetten sonra geliştirilmiş en büyük buluşlardan birisi olarak değerlendirilebilir. Çevrim içi işlemlerin riskli olduğu ve güvenilir ortamların arandığı noktada, farklı sektörlerde kullanılmaya elverişli özellikleri ile öne çıkmaktadır. Temel avantajı, akıllı sözleşmeler yoluyla mahremiyetten ödün vermeden, istenilen her an doğrulanabilir bilgilere ulaşabilme çerçevesinde işlemesidir. Bu anlamda ana özelliğinin, "anonimlik" olduğu söylenebilir. Günlük yaşamda internette, elektronik postalarda, mobil uygulamalarda ve program indirimleri konusunda en çok yaşanan sorun olan tüm hesap bilgilerinin çalınması riski bu sayede düşmektedir. Akıllı sözleşmeler kullanıldığı için otomatik olarak yapılan ödemeleri, tamamen şeffaf bir şekilde mülkiyet sistemine kaydetmektedir. Bu sayede ev, araba, telefon gibi fiziksel ya da bir şirketin hisseleri gibi fiziksel olmayan varlıkların ticaretine de kolaylıkla uygulanabilir. Yenilikçi fırsatlar arayan finans kuruluşları, blok zincirlerini, kendi sistemlerine entegre etmeye çalışmaktadırlar. Estonya'nın LHV Bankası, bu sistemi test ederek, uygulama altyapısında kullanmaya başlayan ilk finans kurumu oldu. Blok zincirlerinin daha fazla tanınması ve kullanılması sonucunda, gelecekte tüm yasal belgelerin, banka, sigorta, sağlık ve ilaç kayıtlarının, harç, vergi ve noter ödemelerinin, özel menkul kıymetlerin, hatta evlilik lisanslarının bile sistem üzerinden tutulduğu bir dönem görülebilir (Crosby, et.al., 2016: 8-9).

Blok zincirlerinde benzersiz bir kimlik ve önceki kodun kimliği bulunur. İlk blok, "Genesis Bloğu" olarak adlandırılır. Aynı zamanda protokolün bir parçası olarak tanımlanır. Geçerli bir blok, üç ayrı unsurdan oluşmaktadır. Bunlar sırasıyla (1) karma işlemlerin şifresini içeren kriptografik çözüm öncesi blok, (2) geçerli bloktaki işlemlerin kökenleri ve (3) madeni para tabanı olarak adlandırılan özel bir alanın bulunmasıdır. Tüm fonksiyonlar, kriptografik tekniklerle korunmaktadır. Bir müşteri olarak X miktarda bitcoin'in sahibi, söz konusu kişinin X miktarda hak sahibi olmasını sağlar. Burada sistemin mantığı, kullanıcıların fonlarını iki kez harcamasını engelleme üzerine kurulmuş olmaktadır (Eyal, et.al., 2016: 47).

Kripto para sistemleri, büyük ölçüde madencilik işlemleri sayesinde yürümektedir. Sistem tarafından oluşturulan bloklar, madenciler tarafından onaylanmaktadır. Bitcoin üretimi karşılığında, tüm kullanıcılar tarafından sisteme bir ücret ödenir. Kullanıcıların bitcoin alıp satarken ödedikleri miktarlar, kripto para üretimi için bilgisayarlarının CPU güçlerini kullanan madencilere gitmektedir. Bu kişiler zincire geçerli bir blok ekleyebilirler. Bunu da bir paylaşım ağı üzerinden duyururlar. Çatallaşma adı verilen bu süreç, birden fazla blok oluşturulması ile ortaya çıkmaktadır. Bunu bir ağacın dallarının uzamasına benzetebiliriz. Hacim olarak en ağır olan, üretimi için en fazla işlem gücü gerektiren blok zinciri çoğalacaktır. Yaklaşık olarak her 60 blokta bir kez bu durum meydana gelir (Eyal, et.al., 2016: 47).

Kripto paralar, blok zincirleri üzerinden çok sayıda fırsat sunduğu gibi yeni riskleri de beraberinde getirmektedir. İzleyen kısımda bitcoin'in ulusal para sistemleri için oluşturduğu fırsatlar ve tehditler incelenmiştir.

4. Bitcoin'in Ulusal Para Sistemleri İçin Oluşturduğu Fırsat ve Tehditler

Bitcoin'in gelecekte yeni para birimi olarak yaygınlaşması, basılı para birimlerinin miktarında bir sınırlamaya yol açarak, ekonomide deflasyonist baskılara neden olabilir. İktisadi birimlerin, bitcoinleri harcamaya değil de, biriktirmeye istekli oldukları ekonomilerde, bu durum daha fazla hissedilebilir. En tehlikeli senaryo ise fiyatlar genel düzeyinin harmonik olarak azalması sonucunda, istikrarsızlıkların kalıcı hale gelmesidir (Bonneau, et.al., 2015: 115).

Bitcoin'i çıkaran bir kurumun olmaması, sistemin çalışma prensibini bilmeyen kişilerde bir güvensizlik oluşturmaktadır. Bu nedenle dalgalanmalardan olumsuz etkilenmemek için, genellikle yatırımcılara tüm birikimlerini bitcoin olarak tutmamaları tavsiye edilmektedir. Ancak giderek fazla sayıda kişinin kripto paralara ilgi göstermesi nedeniyle, bazı devletler ve küresel olarak tanınır şirketler, resmi olarak sanal paralar çıkarmaya başlamışlardır. Bu trendin gelecek yıllarda yaygınlaşması ile merkez bankalarının para basma tekelinin ve dolayısıyla da senyoraj gelirlerinin azalacağı da ileri sürülmektedir (Yüksel, 2015: 203-204).

Kripto para kullanımı yaygınlaştıkça, merkez bankalarının uyguladıkları para politikalarına duyulan ihtiyaç giderek düşecektir. Bu durumda parasal aktarım kanalları etkinliğini yitirebilir. Merkez bankaları üretim, istihdam ve milli gelir gibi değişkenleri etkileyemeyebilir. Bir başka önemli riskte, blok zincirlerinin, işlem sayısı ve nominal değerlerin miktarı gibi parasal göstergeler hakkında bilgi vermesi, fakat gerçekte hangi değerin sağlandığı konusuna değinmemesidir. Bu ise dijital paraların, terörist organizasyonlar tarafından uyuşturucu, silah ve insan kaçakçılığı gibi yasa dışı yöntemlerle elde edilen kazançların aklanmasında kullanıldığına yönelik eleştirileri gündeme getirmiştir (Böhme, et.al., 2015: 233-235).

Kripto paralar, arkasında iz bırakmama özelliğine de sahiptirler. Özellikle Rusya ve Çin yönetimlerinin, bu sebeplerle sanal paralara yakın geçmişte sınırlama getirmesi de, kullanımını ve yaygınlaşmasını zorlaştırmaktadır. Bu tür gelişmeler, bitcoin için sistemik bir açık oluşturarak ve geleceğine ilişkin kuşkuları artırarak, finansal sistemin dışına itilmeye çalışılmasına yol açmaktadır (Atik vd, 2015: 250-251).

Japonya uygulaması, diğer ülkeler için bir örnek teşkil edebilir. Japonya, dünyada kripto paraların ticaretine ve sermaye piyasası aracı olarak kullanılmasına yasal olarak ilk izin veren ülkedir. Dünyadaki ilk bitcoin borsası, 2010 yılında Tokyo'da, elektronik ticaret platformu olan MtGox tarafından açılmıştır. Fakat hükümet, bunu yaparken işlem görecek tüm hesaplara doğrulama zorunluluğu getirmiştir. Böylece sanal para işlemlerinin, yasal olmayan faaliyetlerde kullanımını önemli oranda engellemiştir (Atik vd, 2015: 259-260).

MtGox Borsası'ndan, 500 Milyon Dolar'a yakın değerde olan 750.000 bitcoin'in çalınması ve MtGox'un iflasını açıklaması, kripto para borsalarındaki sistemik açıkların her daim mevcut olabileceğini göstermiştir (Atik vd, 2015: 250).

Borsalardan veya hesaplardan çalınan kripto paralar, bitcoin'e karşı duyulan kuşkuları artırmaktadır. Yatırımcılarda, bu tür olumsuz haberlerden etkilenmekte ve ani

fiyat düşüşlerinden zarar etme korkusu sebebiyle, dijital varlıklardan uzak durmaktadırlar.

Blok zinciri sistemleri, protokol yaklaşımları ile bitcoin'in kayıt tutma sürecine farklı bir yaklaşım getirmiştir. Kripto para yazılımlarının korunması, aracı sistemlerle uyumlu kalınması ve anlık işlem onayları sayesinde koordine edilen genel mutabakat prensiplerine bağlı kalınması bu sayede mümkün olmaktadır (Böhme, et.al., 2015: 233-235).

Bitcoin ekonomisi, aslında Milton Friedman'ın tezlerinin bir kopyası niteliğindedir. Şöyle ki Monetarist ekol, bir ekonominin reel büyüme oranını bulabilmek için, nominal para arzı artışlarının yol açtığı büyüme artışlarının, toplam büyüme oranından düşülmesini önermiştir. Kripto paralar da bu kurala uygun biçimde ele alınabilir. Çünkü Klasik iktisatçıların ve Friedman'ın önemle vurguladığı gibi, para arzının aşırı hızlı büyümesi, enflasyonla bağlantılı olduğu gibi bunun tersi de doğrudur. Dijital paralar da sahip olduğu özellikler gereğince, deflasyonist baskılara yol açabilir. Ekonomiler için böyle bir olumsuz sonucun, bitcoin arzı 21 Milyon sınırına ulaştığında ortaya çıkma riski çok büyüktür. Krugman, nakit ve sanal paraya dayalı ekonomilerde, yeni bir altın standardına ihtiyaç olduğunu vurgulamıştır. Kripto paraların değerinde yaşanan oynaklıklarla mücadele edebilmek için, dijital varlıklara altın karşılığı değerler atanmalıdır (Böhme, et.al., 2015: 233-235).

Bitcoin'in finans sistemi için sunmuş olduğu fırsatlar ve oluşturduğu tehditler aşağıdaki gibi toparlanabilir: (Sönmez, 2014: 11-12)

4.1. Fırsatlar

i. Merkez bankasına ihtiyaç duymadan üretilip, piyasaya arz edilebilen ilk dijital para birimi olması.

ii. Güçlü bir algoritmaya dayanan altyapısı sayesinde, tüm işlemlerin aracı kuruluşlara ihtiyaç duymadan yapılmasına imkan vermesi.

iii. Hesapların tamamen gizli oluşu ve üçüncü kişilerin koymuş olduğu kurallara uyulma zorunluluğunun bulunmaması.

iv. Blok zinciri teknolojisine ve özel bir şifreleme yöntemine sahip olması sebebiyle, hesap hırsızlığı olaylarının sınırlı düzeyde yaşanması.

v. Banka hesaplarına el konulması, günlük para çekme miktarına sınırlama getirilmesi gibi uygulamalara karşı, kullanıcılarına hesaplarını güvence altına alma ve başka ülke borsalarına taşıma şansı sağlaması.

4.2. Tehditler

i. Kullanıcıların gerçek kimliklerinin bilinememesi, uyuşturucu ticareti, kaçak silah satışı ve yolsuzluk gibi yasa dışı faaliyetlerde kullanılmasına aracılık etmektedir.

ii. Toplam üretilecek miktarın, sistemin kuruluşunda belirli olması, ekonomik durgunlukla karşılaşma riskini yükseltmektedir.

iii. Somut yani fiziki bir varlık olmayıp, sadece bir bilgisayar yazılımı ve kodu olması, arkasında bir devlet güvencesinin bulunmaması denetlenmesini güçleştirmektedir.

iv. Blok zincirlerinin karmaşık işlemleri, muhasebeleştirilmesini zorlaştırmaktadır.

v. İşlemlerin geri döndürülemez özellikte oluşunun operasyonel hatalara yol açması.

vi. Hacker saldırıları, dolandırma vakaları ile borsa çöküşleri gibi sistemik açıklarının olması.

Bitcoin'in oluşturduğu tehditler sebebiyle yakın bir gelecekte ulusal para sistemlerine alternatif olarak kullanılma olasılığı zayıf gözükmektedir. Bu konuda ülkelerin vergileme ve diğer mali prosedürler ile kripto paraları kontrol altına alma ve sınırlama çabaları dikkat çekmektedir. Özellikle de merkez bankalarının, senyoraj gelirlerinin azalmasına yol açacak ve para politikalarının etkinliğini düşürecek dijital varlıklara sempati ile bakmadığı aşikardır.

Sonuç

Dijital kripto paralar, merkezi otoritelerden bağımsız yapıları nedeniyle, fırsat ve tehditleri içinde barındırmaktadırlar. Kripto para hesaplarının gizli olması ve arkasında iz bırakmaması, manipülasyonlara maruz kalma olasılığını azaltmaktadır.

Bitcoin arzının 21 milyon ile sınırlı olması, paranın özelliklerini ve fonksiyonlarını taşımasını engellemektedir. Bu nedenle klasik para tanımları içerisinde yer almamakta ve basılı kağıt parayı tamamen ikame edememektedir.

Bitcoin üretimi sona erdiğinde, işlemlerin onaylanmasında sıkıntılar çıkabileceği gibi, krediye konu coinlerin faizini ödeyecek bir muhatabın bulunması da güçleşecektir. Bu nedenle kredi aracı olma işlevini üstlenmesi pek mümkün değildir.

Değerindeki dalgalanmalar, ticari hayatta kullanılmasını güçleştirmektedir. Paranın mübadele ve değer saklama aracı olma fonksiyonlarını içerme şansı da düşük görünmektedir. Ulusal para sistemleri için alternatif bir ödeme aracı olarak kullanılma olasılığı da yok denecek kadar azdır.

Buna karşılık blok zinciri teknolojisi, bankacılık faaliyetlerine hız kazandırması, maliyetleri düşürmesi, hatalı işlemleri minimuma indirmesi sebebiyle, ulusal bankacılık ve finans sistemleri tarafından kullanılabilecek etkin ve verimli bir çözüm yöntemi olabilir. Kripto para alım ve satım ile transfer işlemlerinde, aracı kuruluşlara olan bağımlılığı ortadan kaldırmaktadır. Bu da işlemlerin esnekliğini ve güvenilirliğini artırarak, bilgilerin kaybolma olasılığını azaltmaktadır.

Finansal kuruluşların, son yıllarda kripto para altyapısını oluşturan blok zincirlerini kullanmaya başladıkları gözlenmektedir. Bu sayede EFT, Havale, Swift ve Interbank işlemleri, daha güvenli biçimde gerçekleştirilmektedir. Bu durumun finansal sistemin tüm taraflarının lehine olması beklenmektedir.

Kaynakça

Antonopoulos, A., M. (2014). *Mastering Bitcoin: Unlocking Digital Crypto-Currencies*. California: O'Reilly Media.

Atik, M., Köse, Y., Yılmaz, B. ve Sağlam, F. (2015). "Kripto Para: Bitcoin ve Döviz Kurları Üzerine Etkileri". *Bartın Üniversitesi İ.İ.B.F. Dergisi*, 6(11): 247-261.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. And Virza, M. (2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin". *IEEE Symposium on Security and Privacy*. California: IEE Computer Society: 459-474.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. and Felten, E. W. (2015). "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". *IEEE Symposium on Security and Privacy*. California: IEE Computer Society: 104-121.

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015). "Bitcoin: Economics, Technology and Governance". *Journal of Economic Perspectives*, 29(2): 213–238.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016). "BlockChain Technology: Beyond Bitcoin". *Applied Innovation Review*, 1(2): 6-19.

Çarkacıoğlu, A. (2016). Kripto-Para Bitcoin. *https://www.spk.gov.tr/SiteApps/Yayin/ArastirmaRaporlar*i/07.08.2019.

Dimitri, N. (2017). "Bitcoin Mining as a Contest", *Ledger Journal*, 2(1): 31-37.

European Central Bank (2012). "Virtual Currency Schemes". *http://www.ecb. europa.eu/ pub/pdf/other/virtualcurrencyschemes201210en.pdf*/15.09.2018.

Eyal, I., Gencer, A., E., Sirer, E., G. and Renesse, R., V. (2016). "Bitcoin-NG: A Scalable Blockchain Protocol", *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16)*. Santa Clara: Usenix Assocation: 46-59.

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". *https: //bitcoin.org /bitcoin.pdf*/20.10.2018.

Sönmez, A. (2014). "Sanal Para Bitcoin". *The Turkish Online Journal of Design, Art and Communication-TOJDAC*, 4(3): 1-14.

Usta, A. ve Doğantekin, S. (2017). *Blockchain 101*. İstanbul: Kapital Medya Hizmetleri A.Ş.

Yüksel, A., E., B. (2015). "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış". *İstanbul Üniversitesi Hukuk Fakültesi* Mecmuası-*İÜHFM*, 73(2): 173-220.

https:/coinmarketcap.com/30.08.2019.

https://tr.investing.com/crypto/bitcoin/btc-usd-historical-data/08.10.2019.

https://coinmarketcap.com/currencies/bitcoin/historical-data/10.12.2019.

Ek Tablo: Bitcoin Fiyatlarındaki ve İşlem Hacimlerindeki Çeyrek Dönemlik Değişmeler (2012-2019)

Tarih	Bitcoin Fiyatı (BTC/$)	İşlem Hacmi ($)
01,03,2012	4,9	-
01,06,2012	5,3	-
01,09,2012	10,0	-
01,12,2012	12,6	-
01,03,2013	34,5	-
01,06,2013	128,82	1.451.916
01,09,2013	135,14	1.610.215
01,12,2013	1.128,92	11.531.708
01,03,2014	549,92	18.668.100
01,06,2014	623,69	45.259.100
01,09,2014	477,79	20.432.000
01,12,2014	378,25	11.763.000
01,03,2015	254,28	25.213.700
01,06,2015	230,23	26.090.500
01,09,2015	230,26	20.575.200
01,12,2015	377,41	60.452.200
01,03,2016	437,92	74.895.800
01,06,2016	531,11	86.061.800
01,09,2016	575,55	76.923.400
01,12,2016	746,05	80.461.904
01,03,2017	1.180,04	229.056.992
01,06,2017	2.228,33	1.653.180.032
01,09,2017	4.701,76	2.599.079.936
01,12,2017	10.198,60	6.783.119.872
01,03,2018	10.385,0	7.317.279.744
01,06,2018	7.500,70	4.921.460.224
01,09,2018	7.044,81	4.116.050.000
01,12,2018	4.024,46	5.375.314.093
01,03,2019	3.853,76	7.661.247.975
01,06,2019	8.573,84	22.488.303.544
01,09,2019	9.630,59	11.445.355.859
01,12,2019	7.571,62	18.720.708.479

Kaynak: https://coinmarketcap.com/currencies/bitcoin/historical-data/ Erişim Tarihi: 10.12.2019. https://tr.investing.com/crypto/bitcoin/btc-usd-historical-data/ 08.10.2019.