e-Journal of New Media / Yeni Medya Elektronik Dergi - eJNM
ISSN: 2548-0200, May 2019 Volume 3 Issue 2, p.71-83

BLOKZİNCİRİ VE KRİPTO PARALARIN İNSANLIĞA ETKİLERİ

Buket İŞLER
İstanbul Aydın Üniversitesi, Türkiye
bbuketkilic@hotmail.com
https://orcid.org/0000-0002-9393-9564

Mustafa TAKAOĞLU
İstanbul Aydın Üniversitesi, Türkiye
mustafatakaoglu@aydin.edu.tr
https://orcid.org/0000-0002-1634-2705

Ufuk Fatih KÜÇÜKALİ
İstanbul Aydın Üniversitesi, Türkiye
ufkucukali@aydin.edu.tr
https://orcid.org/0000-0002-2715-7046

ÖZ
Günümüzde insanların çokça ilgi gösterdiği konulardan biri de kripto para birimleridir. Bu ilginin sebebi maalesef kripto paraların ortaya çıkma sebebiyle aynı doğrultuda değildir. Çalışmamızda bu amaç farklılığına değinilmiş ve arkasında yatan sebepler üzerinde tartışılmıştır. Bu noktada dogma, değer yargısı ve defaatle tekrar eden alışkanlıklar incelenmiştir. Ayrıca kripto paraların temelinde yatan blokzinciri teknolojisinin hayatlarımıza getirebileceği değişimin ne boyutlarda olabileceği üzerinde durulmuştur. Blokzinciri ve kripto paraların insanlığa etkileri konusu üzerinde yapılacak çalışmanın daha iyi anlaşılabilmesi amacıyla konuyu öğretici bilgiler paylaşılmıştır.

Anahtar Kelimeler: *Dogmatik Bilgi, Değer Yargısı, Bilim Felsefesi, Blokzinciri, Kripto Paralar.*

THE EFFECTS OF BLOCKCHAIN AND CRYPTO COINS ON HUMANITY

ABSTRACT
Cryptocurrencies are one of the issues that people are interested in today. The reason for this interest is unfortunately not in line with the emergence of crypto coins. In our study, this purpose difference was mentioned, and the reasons behind it were discussed. At this point, dogmatism, value judgment, and repetitive habits were examined. Besides, the extent of the change that can be brought to our lives by the blockchain technology underlying the crypto coins is emphasized. To better understand the study on the effects of blockchain and crypto coins on humanity, informative information was shared.

Keywords: *Dogmatic Knowledge, Value Judgment, Philosophy of Science, Blockchain, Crypto Coins.*

GİRİŞ
Büyük dogmalar, yani güvenilirliği büyük teoriler insan zihninin büyük başarılarıdır. Dogmatik düşünce ayrıca, kritik düşüncenin meydana gelebilmesi için bir ön safhadır. Dogmatizm, kritisizm ile birlikte büyük dogmaların yani bilimsel gelişmenin kaynağını meydana getirir (Oeser, 1984). İnsanların hayatlarını sürdürdükleri toplumlardaki sosyal, ekonomik ve kültürel gelişmişlik seviyesine göre sahip oldukları dogmaları vardır. Aynı ortamda etkileşim halinde olduğumuz kişileri göz önüne alarak düşündüğümüzde, karşılaşılan sayısız görüş farklılıkları; aslında sahip olduğumuz dogmaların ve bu dogmaların yorumlanmasının benzer olmamasından kaynaklanmaktadır. Toplumların karşılaştığı her yeni gelişme, dogmaların doğrudan ya da dolaylı etkisiyle, tecrübe olarak hafızalarda

Research Article - Submit Date: 01.11.2018, Acceptance Date: 25.04.2019

DOI NO: 10.17932/IAU.EJNM.25480200.2019.3/2.71-83

kaydedilir. Popper'a göre öğrenme işlemi bir amipten insana kadar bütün canlılarda ortak olup, tecrübe etme ve yanılma sürecine bağlı olarak cereyan eder (Ural, 1985). Sorular sormak, bir problem bulup birtakım cevaplar vermek felsefenin geleneksel tutumudur (Ural, 1994). Peki, Popper'ın bahsettiği bu öğrenme süreci, sürekli benzer sonuçlar tecrübe edilmesine rağmen, temelde aynı olan bir işlemin, önceki testlerden farklı bir sonuç vereceğine inanarak yeniden denenmesinin sebebi ne olabilir? Yukarıda bir cümlede belirttiğimiz gibi, dogmaların doğrudan ya da dolaylı etkileri burada üzerinde durmamız gereken noktadır. Dogmalar aynı zamanda değer yargılarımızın büyük bir kısmını oluşturur. Çünkü gelir geçer fikirler, temeli zayıf ve herkesçe kabul görmemiş görüşler değer yargısı olarak kabul edildiğinde; gelişen zaman ve oluşan yeni akımlar karşısında doğruluğunu yitirir ve anlamsız bir hal alır. Doğruluğu, gelişen bilim ve evreni daha iyi kavrama olanakları ile daha kesin bir şekilde ispatlanabilen dogmalar ve bu dogmalar doğrultusunda oluşturulan değer yargıları; insanın iç dünyasında bir tutarlılık, disiplin ve vicdani rahatlık getirecektir. Ancak tamamı dogmalar etkisiyle oluşmuş değer yargısına sahip bir insanda dahi terbiye edilememiş insani güdüler, sahip olduğu değer yargılarının yüceliğine rağmen, günümüzde birçok problemin temelinde yatmaktadır. İnsanın dâhil olduğu birçok alanda, farklı şekillerde defaatle söylenen; "insanlar değil, dogmalar kusursuzdur" genellemesi bu noktada doğru bir cevap olacaktır. Buna en güzel örnek olarak kolay "para kazanma arzusu" gösterilebilir. İnsanlar modern ekonomi sistemi ile karşılaştığı günden itibaren birçok kez kolay para kazanma arzusunun esiri olmuş ve büyük paralar kaybetmiştir. Büyük mağduriyetler devletlerce engellenmeye çalışılmış ancak temelde aynı fakat farklı formlarda geliştirilen yeni modeller ile insanlar kandırılmış ve dolandırılmıştır.

Kolay para kazanma arzusu en çok Piramit şemaları ile kötüye kullanılmıştır. Çalışmamızın başında dikkat çektiğimiz: "Sürekli benzer sonuçlar tecrübe edilmesine rağmen, temelde aynı olan bir işlemin, önceki testlerden farklı bir sonuç vereceğine inanarak yeniden denenmesinin sebebi ne olabilir?" Sorusuna piramit şemaları çok güzel bir cevaptır. Tarihteki en ünlü piramit şeması, 1920 yılında ABD'de Charles Ponzi tarafından oluşturulmuştur. Bu nedenle piramit satış, literatürde "Ponzi şeması" olarak da adlandırılmaktadır. Ponzi, kendisi ile birlikte on arkadaşının 150 $ katılım ücreti yatırmasını sağlayarak işe başlamış ve arkadaşlarına yatırımlarının %50'sinin 90 gün içinde kendilerine geri döneceğini vaat etmiştir. Daha sonra aynı şekilde bir arkadaş grubuna daha aynı miktarda katılım ücreti yatırtmış ve sözde yatırımcılardan oluşan orijinal grubun da onlara yatırımlarını aynı süre zarfında döndüreceğini anlatarak zinciri başlatmıştır. Piramidin başında yer alan öncü katılımcılar, vaat edilen geri dönüşün 90 günden çok daha kısa sürede gerçekleşmesinden hoşnut kalmış, diğer katılımcıları da bu coşkuyla piramit şemaya dâhil edebilmişlerdir. Ponzi, 9 ayda 9 milyon dolardan fazla kazanmış olup, piramide sonradan katılanlara da bu rakamın yaklaşık on katı borçlanmış ve sahtekârlıktan tutuklanmıştır (Taşoğlu, 2008). Tabii ki tüm dünyada ses getiren bu uygulama farklı form ve şekillerde defaatle tekrar edilmiş ve dolandırıcıları memnun eden sonuçlar alınmıştır. Örneğin en büyük Ponzi oyununa imza atmış olan Bernard Madoff, kurduğu sistem sayesinde 65 milyar dolar para toplamıştır. Ülkemizde 90'lı yıllarda tanınan Titan Saadet Zinciri'nin kurucusu Kenan Şeranoğlu, binlerce kişiden 70 milyon mark toplamıştır. 10 yıl hapis yattıktan sonra serbest bırakılmıştır. Halk arasında saadet zinciri olarak adlandırılan piramit satış sistemlerinden dolayı ülkemizde yaklaşık bir milyon kişi mağdur olmuştur (Sütçü, 2016). Maalesef bu rakamlar 2016 yılında tanıştığımız, Mehmet Aydın'ın Çiftlik Bank isimli Ponzi Şeması mantığıyla tasarlanmış dolandırıcılık çalışması sebebiyle daha da artmıştır. Aynı süreçte birçok benzer internet oyun siteleri açılmış ve binlerce kişi kolay para kazanma arzusunun mağduru olmuştur. Ponzi şemaları dışında dünyada ses getirmiş ve insanları mağdur etmiş bir diğer yöntem de borsa manipülasyonlarıdır. 2000 yılında, Amerika'nın en büyük 500 şirketinden biri olan Enron buna çok güzel bir örnektir. Şirketin hisse fiyatlarının başarılı muhasebe oyunları, para aklama sistemi ve içeriden alınan bilgilerle yükseltilerek halka açılması sonucunda, 40 milyar dolarlık sahteciliğiyle Enron, tarihin en büyük borsa dolandırıcılıklarından biri olmuştur. Keza Jordan Belfort gibi Wall Street borsa dolandırıcısı da insanları 110 milyon dolar dolandırmış ve The Wolf of Wall Street filmine esin kaynağı olmuştur. Birçok benzer dolandırıcılık girişimleri tarihte görülmüş ve önlemler alınmaya çalışılmıştır. Bahsettiğimiz Ponzi ve Borsa dolandırıcılıkları dışında dünyada en çok görülen bir diğer yöntem ise dinlerin ve insanların duygularının kötüye kullanılmasıdır. Bu yöntem aslında direkt olarak dogmaları kullanılarak insanları hedef alan bir yöntemdir. Örneğin Benny Hinn isimli misyoner televizyon şovları ve tutmayan kehanetleri ile insanların duygularını sömürerek 90'lı yıllarda milyonlarca dolar kazanmıştır. Pos makineli dilenciler

ve bankada milyonlarca lirası olan ve okuma yazma bilmeyen büyücüler de unutulmamalıdır. Birçok din ve inanıştan binlerce insan bu şekilde haksız kazançlar elde etmiştir. En önemlisi insanlar bu tarz kişilere maddi bir geri dönüşü olmayacağını bilerek, manevi bir istikbal hayaliyle, para ve değerli gördükleri varlıklarını mutlulukla teslim etmişlerdir. Peki, yukarıda bahsettiğimiz birkaç dolandırma yöntemi düşünüldüğünde, dolandırıcı ile dolandırılan insanlar arasında ortak bir nokta yok mudur? Birçok kabul görmüş dogma insanı çalışmaya, düşünmeye, dürüstlüğe, sabır, kanaat ve olayların arkasındaki manayı anlamayı çalışmaya sürükler. Bu durumda dolandırılan kişilerin değer yargılarını dogmalar etkilememiştir yahut az etkilemiştir demek doğru mudur? Ya da insanın değer yargılarının ulviliğini ölçme imkânımız yahut yetkimiz var mıdır? Varsa ve böyle bir yetkiyi üstleneceksek bunu hangi değer yargısına göre yapacağımız belli midir? Ve en önemlisi, dolandırıcı ile dolandırılan insanların değer yargıları ve etkilendikleri dogmalar benzer midir? Bu sorular üzerinde düşünülmesi gerekmektedir.

Felsefenin bilimlerle ilgisi sadece fizik gibi belirli bilimler ile sınırlı değildir. Mesela "Bir insan annesinin aynı zamanda kardeşi olabilir mi?" sorusu, kelime oyunlarından ibaret olmayıp, hukuki ve sosyal bir probleme işaret etmektedir. Çünkü tıptaki mevcut teknikler sayesinde, bir annenin döllenmiş yumurtası o annenin annesinin rahminde geliştirilebilmekte ve anneanne kızının çocuğunu doğurabilmektedir. Yani tıptaki gelişmeler beraberinde ahlaki, hukuki ve toplumsal birçok problemi de beraberinde getirmektedir (Ural, 1994). Hayatta her şey bir süreçtir. Kimse çok iyi bir bilim insanı, sporcu yahut suçlu olarak doğmaz. Yeni doğan bir bebeğin dünya görüşü, onu yetiştiren kişilerin etkisi doğrultusunda gelişecektir. Bir insanın ailesinden sorgulamadan öğrenmiş olduğu bilgileri düşünüp tekrardan doğruluğuna kanaat getirmesi ve değer yargılarını ve dogmalarını adlandırabilmesi ciddi bir zaman alır. Çoğu örnekte insanlar hayat koşturmacası, eğitim eksikliği ve materyalist değer yargıları gibi çoğaltılabilecek birçok sebeple varoluş gayesini dahi düşünmeye zaman ayıramamaktadır. İnsanın en azından başına gelen felaketten ders çıkarması ve en temel felsefi tutum olan soru sormaya başlaması gerekmektedir. Aksi takdirde insan makineleşir ve en önemli özelliği olan düşünme yetisini önem arz eden birçok konuda kullanmamaya başlar. Bu noktada çalışmamıza dönecek olursak, özellikle finansal açıdan hayatlarımızda karşılaştığımız her yeni "fırsat" aynı zamanda yeni bir "tuzak" olma ihtimalini akıllarımıza getirmektedir. Çünkü birçok yeni fırsat olarak pazarlanan fikir; televizyon, internet ve gazete gibi insanların düzenli takip ettiği mecralarda tanıtılıp, insanların hizmetlerine kusursuz bir projeymiş gibi sunulmakta ve doğruluğu tartışılır sertifikalarla güvenilirliği arttırılmaya çalışılmaktadır. Maalesef dolandırıcı amaçlarla kurulan firmalar, dolandırma işlemi yapıldıktan sonra fark edilmekte ve önlemler alınmaktadır. Dinamik olarak firmaların yaptıkları işler, hukuki açıdan bir sorun teşkil etmediği sürece takip edilmemekte ve kullanıcıların şikâyet etmeleri durumunda takip mekanizmaları çalıştırılmaktadır. Bu sebeple günümüzde, geçmişten ders çıkaran ve düşünen insanların algılarında kolay para kazanma fırsatı olarak sunulan projeler hep büyük soru işaretleriyle karşılanmaktadır. Çalışmamızın da konusu olan bitcoin gibi kripto paralar insanlar nezdinde benzer bir muhakemeden geçmektedir. İlerleyen bölümlerde kripto paraların arkasındaki yaratıcı güç olan blok zinciri teknolojisi, kripto paralar ve bu yeniliklerin hayatlarımızda yarayabileceği değişimlerden ve yukarıda bahsetmeye çalıştığımız insanların mağdur olmalarına sebebiyet veren olaylardan farklarını açıklayacağız. Anlaşılacağı gibi blokzinciri ve kripto paralar konularının üzerinde fikir yürütebilmek için gerekli olan temel bilginin okuyucuya sağlanması gerekmektedir. Bunun sağlanması amacıyla ilerleyen bölümlerde gerekli bilgilerin yer aldığı başlıklar paylaşılmıştır.

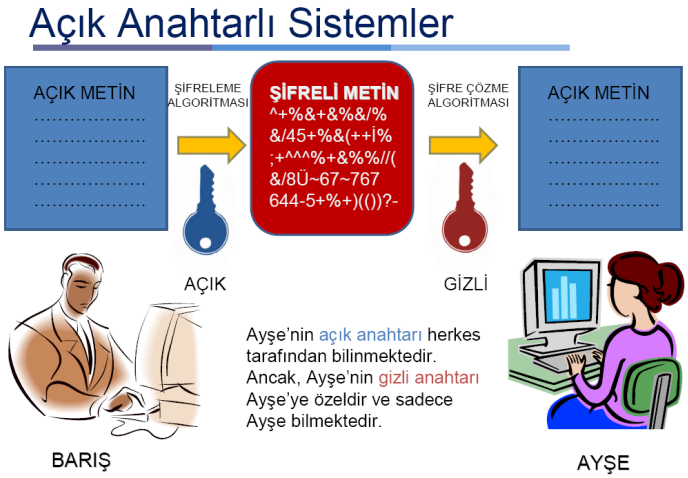
TERMİNOLOJİ

Blokzinciri ve kripto paralar konularına meraklı kişilerin bilmesi gereken temel kavramlar bulunmaktadır. Bu kavramların önceden tanıtılması, okunan çalışmanın daha faydalı olmasını sağlayacaktır. Bu sebeple çalışmamızda kullanılan kavramlar hakkında açıklamalara yer verilmiştir. Bunlardan bahsedecek olursak: Bitcoin; açık kaynaklı bir kod olarak yayınlanan ve blokzinciri teknolojisine dayanan ilk kripto para birimidir (Anavatan ve Kayacan, 2018). Blokzinciri(Blockchain): Kripto para birimlerinin temel teknolojisi olan blokzinciri, dağıtılmış bir defterdir(ledger). Aynı zamanda hataya dayanıklı olan "Eşler Arası (Peer-to-Peer)" ağı kullanan dijital bir ödeme sistemidir (Sakakibara, Nakamura ve Matsutani, 2017). Kripto Para(Cryptocurrency): Günümüzde çokça konuşulan Bitcoin, Ethereum, XRP, EOS, Litecoin gibi kodlarında ve kodlanma şekillerinde

kriptografinin kullanıldığı para birimlerine verilen genel isimdir. Kriptografi: Adını gizli ve yazı kelimelerinin Yunancalarından alan Kriptografi; var olan verinin içeriğinin korunmasını ve başka şahıslarca içeriğinin okunamaması veya çözülememesini amaçlayan bilim alanıdır (Takaoğlu, Sönmez ve Kaynar, 2018). Kripto para birimleri, kriptografiye (şifreleme bilimi) dayanmaktadır (Anavatan ve Kayacan, 2018). Bir iletinin içeriğini saklamak üzere yapılan gizleme işleme şifreleme denir. Bu işlem düz metini anahtar kullanarak şifreli metine dönüştürmektedir (Kodaz ve Botsalı, 2010). Aşağıdaki Şekil 1'de şifreleme ve şifreyi çözme işlemleri gösterilmektedir.

Şekil 1: Basit Şifreleme İşlemleri

Şifreleme algoritmaları anahtar kullanma yöntemlerine göre genel olarak iki kategoriye ayrılmaktadır. Bunlar: Gizli anahtarlı (Simetrik) ve Açık anahtarlı (Asimetrik) şifreleme algoritmalarıdır. Simetrik şifreleme algoritmasını kısaca ifade edecek olursak: Hızlı çalışan, küçük sistemler için yeterli bir şifreleme algoritması olmasına karşın, şifrelemede ve şifre çözme adımlarında aynı anahtar kullanılır. Bu n kullanıcılı bir sistem için [n * (n-1) / 2] anahtar saklanmalıdır anlamına gelir. Kısacası ölçeklendirilebilir değildir. Bizim çalışmamızda önem arz eden ve üzerinde özellikle durmak istediğimiz algoritmalar Asimetrik şifreleme algoritmalarıdır. Simetrik şifrelemenin aksine asimetrik şifrelemede 2 farklı anahtar vardır. Bu anahtarlar public ve private olarak isimlendirilirler. Public anahtarlar networkteki(tüm katılımcıların oluşturduğu ağ) herkese dağıtılırlar, ancak private anahtarlar sadece ve sadece kişinin kendisi tarafından bilinmelidir.



Şekil 2: Açık Anahtarlı Şifreleme Örneği

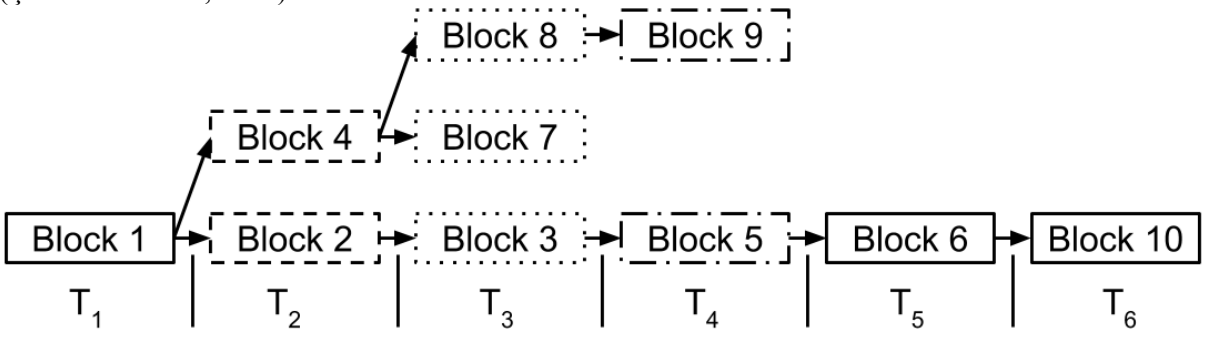
Gizli Anahtarlı Sistemlerde, alıcı ve gönderici aynı anahtarı kullandığından, bu gizli anahtarın paylaşılması bir problemdir. Gizli anahtar öyle bir paylaşılmalıdır ki, sadece alıcı ve gönderici gizli anahtarın ne olduğunu bilsin. Gizli Anahtarlı Sistemlerdeki anahtar paylaşım problemine Açık Anahtarlı Sistemler ile çözüm gelmiştir (Akleylek, Yıldırım ve Tok, 2011). Yukarıdaki Şekil 2'de açık anahtarlı bir şifreleme işleminin nasıl yapıldığı gösterilmiştir. Asimetrik algoritmalar gizlilik, imzalama ve anahtar paylaşımı için kullanılırlar. Asimetrik algoritmalar simetrik algoritmalara göre daha karmaşık bir yapıya sahiptir ve bu sebeple çok daha yavaş çalışırlar. En yaygın kullanılan asimetrik algoritmalar, RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) ve Eliptik eğri algoritmasıdır.

Cüzdan (Wallet): Sanal para internete bağlı ve internete bağlı olmayan cüzdanlar şeklinde saklanır. İnternete bağlı cüzdanlar (Online Wallet); masa üstü cüzdanları, mobil cüzdanlar ve web

DOI NO: 10.17932/IAU.EJNM.25480200.2019.3/2.71-83

cüzdanlarıdır. Masa üstü cüzdanlar: Masa üstü cüzdanların kendine ait web siteleri vardır. Bu siteler yardımıyla yazılımlara erişim ve kurulum süreci tamamlanır. Kurulum işleminden sonra cüzdanın kontrolü kullanıcıya geçer bu cüzdanla blok zincirinin bir parçası olunur (Durmuş ve Polat, 2018). Mobil cüzdanlar: Blok zincirinin telefona yüklenme şansı bulunmamaktadır. Mobil cüzdanlar kriptolu bir cüzdan çeşididir. Telefonun çalınma ve bozulma risklerine karşı güvensizdir. Bu sebeple pek tercih edilen bir cüzdan çeşidi değildir (Durmuş ve Polat, 2018). Web cüzdanları: Kullanıcıları adına gizli/açık anahtar üretir ve onların güvenliğinden sorumlu olurlar. Gizli anahtarı kendisinde saklayan şirketler, geçmişte bilgisayar korsanlarının saldırılarına maruz kalmış ve müşterilerinin Bitcoin'lerini çaldırmışlardır. Bu sebeple ünleri iyi değildir (Çarkacıoğlu, 2016).İnternete bağlı olmayan cüzdanlar(Hardware Wallet); kağıt cüzdanlar, beyin cüzdanlar ve donanım cüzdanlarıdır. Kâğıt Cüzdanlar: Kâğıt cüzdanlarda kriptolu para miktarları, adresleri ve şifreleri kâğıda yazılıdır. En sağlam cüzdan şekillerinden biridir. Oluşabilecek tek sorun hamiline yazılmış çek gibi kimin elindeyse, bu kâğıt cüzdan sahibi de odur. Hacklenme riski yoktur (Antonopoulos, 2014). Beyin Cüzdanlar: Cüzdan tarafından en az sekiz kelimeden oluşan ve ezberlenmesi gereken bir anahtar ile çalışan cüzdanlardır. Donanım Cüzdan: Bir çeşit şifreli USB çeşididir. Şifreli USB cüzdanları sadece kriptolu para saklamak için üretilmiştir, taşınması kolaydır çevirim dışı tutulurlar kullanılmak istendiğinde bilgisayara takılarak çevrimiçi olurlar hem taşınması hem de kullanması kolay oldukları için en çok tercih edilen kriptolu cüzdan çeşididir (Durmuş ve Polat, 2018). Madencilik (Mining): Bitcoin ve altcoin denen bitcoinden sonra üretilmiş tüm kripto para birimleri bir merkezden üretilmezler. Kripto paraların arzı, merkezi olmayan ağdaki bilgisayarların sağladığı işlemci gücüyle yapılır. Açık kaynak kodlu olan madenci yazılımlarını çalıştıran herkes madenci olabilir ve istediği kripto parayı üretebilir. Kripto paralar, madencilik adı verilen, transfer işlemleriyle uğraşırken karmaşık bir matematik problemini birbirleriyle yarışarak çözen, madenciler aracılığıyla arz edilir. Bitcoin örneğinde toplamda yirmi bir milyon adet bitcoin vardır. Bu sebeple madenciler sayısı değişmeyecek olan bu coinlere sahip olmak için yarışırlar. Problemi çözen madenciler belli bir miktarda Bitcoin ile ödüllendirilirler.
Özet (Hash) Fonksiyonu: Simetrik ve asimetrik şifrelemelerin haricinde girdi olarak anahtar kullanmayan Özet (Hash) algoritmaları bulunmaktadır. Özet algoritmaları sistemde tek başına kullanılmazlar; simetrik ve asimetrik diğer algoritmalara yardımcı olmak için yapılmışlardır.

Konsensus Protokolleri, PoW (Proof of Work) ve PoS (Proof of Stake): Konsensus protokolleri; blokzincirinde değişiklikleri kimin yapacağını belirleyen kurallar bütünüdür. PoW metodunda kazdığınız blok kadar ödül kazanırsınız. Ayrıca bu doğrulama yönteminde bloğun zincire eklenmesi için gerekli algoritmayı çözen ilk kişi ödülü alır. Bu tarz madencilik, yatırımcıların veri bloklarını doğrulamada aktif bir rol almasını gerektirir. Bu da işlemlerin doğrulanmasını ve yeni paraların üretilmesini sağlar. Bu madencilik türünde blok doğrulaması için aktif olarak çalışmazsanız hiçbir ödül almazsınız. PoS metodu Pow'a alternatif olarak düşünülmüş ve ağdaki işlemleri doğrulamanın bir diğer türüdür. Bu yöntem aslında madencilik bile değildir çünkü kullanıcıların yeni para üretmeleri için herhangi bir işlem yapmalarına gerek yoktur. Bu nedenle madencilik olarak değil para basmak olarak nitelendirilmektedir. Bu yöntemde para kazanmak için elektronik cüzdanınızda para bulundurmalısınız. Kazanacağınız ödül cüzdanınızda tuttuğunuz para miktarı ile doğru orantılıdır. Cüzdanınızda ne kadar çok paranız varsa o kadar çok ödül kazanırsınız yani yeni para üretirsiniz (Çabuk ve Mendi, 2018).



Şekil 3: Blokzinciri Konsensüs Modeli

DOI NO: 10.17932/IAU.EJNM.25480200.2019.3/2.71-83

Defter(Ledger): Bitcoin ve diğer kripto paraların blokzincirindeki hareketlerinin tutulduğu defterlerdir.

Blokzinciri Teknolojisi

Blokzinciri, sürekli büyüyen işlem kayıtlarının listesini, çalınma veya değiştirilme gibi tehlikelerden koruyarak tutan dağıtık veri tabanı olarak tanımlanmaktadır (Çabuk ve Mendi, 2018). Şekil 4'de blokzincirinin dağıtık ağ mimarisinin görseli paylaşılmıştır.

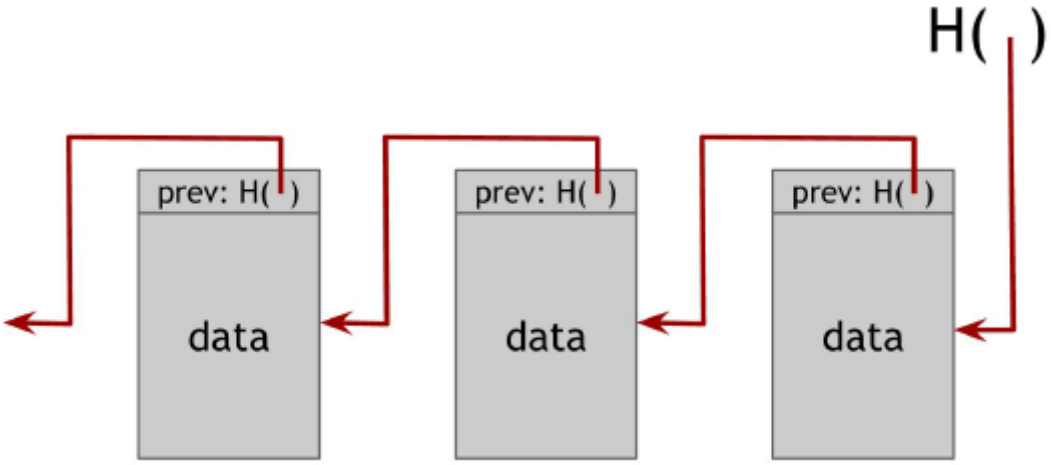
Şekil 4: Merkezi, Merkezi Olmayan ve Dağıtık Ağlar

Yukarıda verdiğimiz tanımdan farklı olarak Nakamoto blokzincirini; ihtiyacımız olan; güven yerine kriptografik kanıta dayalı, iki tarafın üçüncü bir güvenilir kişiye gerek duymadan doğrudan birbirleriyle işlem yapabileceği bir elektronik ödeme sistemi, olarak tanıtmıştır (Nakamoto, 2008). Blokzincirini ilk olarak 1991 yılında, resmi evrakların bilgisayar ortamında geçerliliğinin sağlanabilmesi için bir çözüm yolu arayan Stuart Haber ve W. Scott Stornetta isimli kriptograflar tarafından önerilmiştir. Günümüzde kullanılan hali düşünüldüğünde, Haber ve Stornetta'nın 1991 yılında yaptıkları çalışmaları, blokzincirinin prototipi niteliğindedir. Günümüz blokzinciri sistemi bir muhasebe defteri gibi düşünülebilir. Eşler arası herhangi bir işlem yapıldığında bu işlem şifrelenmiş bir biçimde kayıt altına alınmaktadır. İsteyen herkes bu ağa katılabilmektedir. Bu ağa özgürce katılma, blokzinciri sisteminin açık bir defter olma özelliğinden kaynaklanmaktadır (Şahin, 2018). Kullanılan "Zincir" tabiri aslında bir veri bloğunu ifade eder. Bu veri bloklarına işlemler geldikçe yazılarak kaydedilir. Yazılan bu veriler değiştirilemez ve nihaidir. Bu özellik, blokzincirinin en önemli özelliklerinden birisidir.

İşlemler eşler arası (P2P) ağda tüm düğümlere yayınlanır. Veri blokları sınırlı bir boyuttadır ve dolunca zincirin yanında yeni bir blok oluşturulur. Bir hile yapıp bloktaki veri değiştirilmeye çalışılırsa, sistem bu zinciri sistem dışına iter ve ağın bütünlüğünü korur. Hile yapılan zincir eski haline döndürüldüğünde, yani hileden vazgeçtiğinde, blok zincire yeniden bağlanır. Herkes, tüm işlem geçmişini görebilir. İşlem geçmişinin eksiksiz olması da her sanal paranın geçerliliğini sağlar ve tüm sanal paralar oluştukları andan itibaren izlenebilir. Ayrıca teknolojisi sayesinde çözünürlük sağlayarak geriye dönük şeffaflık sağlar. Geçerli kayıtların değiştirilmesini engeller (Avunduk ve Aşan, 2018). Şekil 5'de blokzinciri ve blokzincirini oluşturan blok yapısını görebilirsiniz (Ünsal ve Kocaoğlu, 2018).

Research Article - Submit Date: 01.11.2018, Acceptance Date: 25.04.2019

DOI NO: 10.17932/IAU.EJNM.25480200.2019.3/2.71-83



Şekil 5: Blokzinciri Veri Yapısı.

Blok içeriği ise aşağıdaki Tablo 1'de görüldüğü gibidir. Bir blok içerisinde birden fazla işlem olabilir. Blok zinciri sisteminde her kullanıcı kendi bilgisayar kaynaklarını kullanır. Ağdaki her bir düğüm tüm defter kaydının tam kopyasına sahiptir (Taş ve Kiani, 2018).

Tablo 1: Blok İçeriği

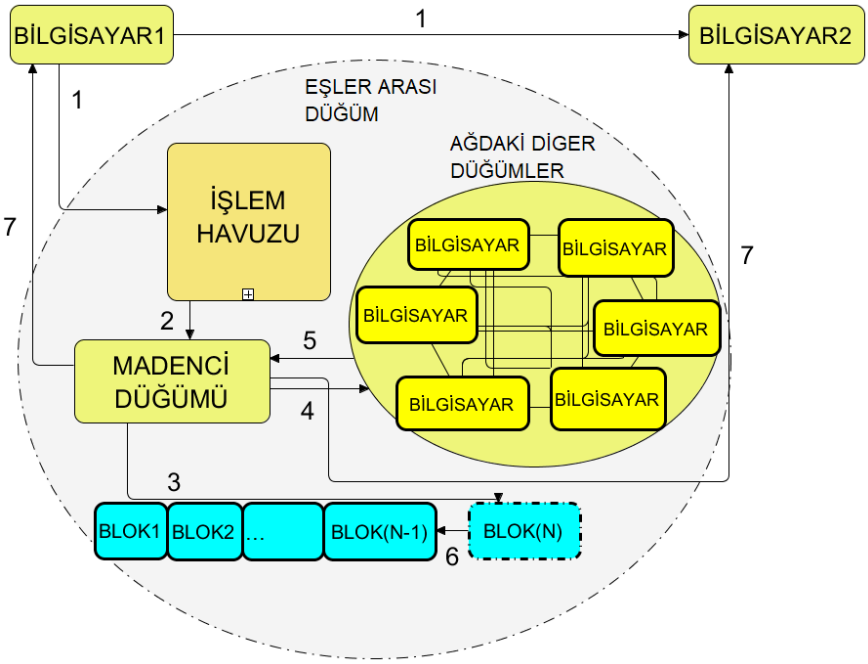
Sihirli Sayı	Blok zincirini tanımlayan eşsiz sayı, sonraki tüm bloklar için sabit kalır.
Blok boyutu	Bloğun sonuna kadar takip eden bayt sayısı
Sürüm Numarası	Blok format biçimi.
Önceki blok bağlantısı	Önceki bloğun özütü
İşlem Özütü	Merkle ağacının kök düğümü, ağaçtaki tüm özüt çiftlerinin bir torunu. Kök düğüm, bloktaki tüm işlemlere bağlı 256 bit özüttür.
Zaman Damgası	Bloğun oluşturulduğu zaman
Kazma Güçlüğü	Yeni blok bulmanın bağıl zorluk ölçüsü. Zorluk, ağdaki madencilerin ne kadar özüt gücü harcadığının bir fonksiyonu olarak periyodik şekilde güncellenir.
Nonce	Bir defa kullanılan sayı, PoW hesaplamasında kullanılır.
İşlem Sayısı	Bu bloktaki işlem sayısı
İşlemler	İşlemler listesi (boş olmaz)

Blokzinciri uygulamasında madenci adı verilen sistemler, şu ana kadarki bütün işlemleri içeren bütün blokzincirini tutarlar. Bloğu oluşturacak düğümün seçimi konsensüs protokolü ile gerçekleştirilir. Blokzinciri yapısı kullanan bir uygulama aracılığı ile Bilgisayar1 ve Bilgisayar2 makineleri arasında bir işlem yapılacağı bir senaryodaki yeni bloğun oluşturulması ve blokzincirine eklenmesi Şekil 6'da gösterilmiştir. İşlem aşamaları şekilde gösterilen numaralarla aşağıdaki gibidir:

1. Bilgisayar1 yapılacak işlemi Bilgisayar2 de dâhil olmak üzere eşler arası ağda yayınlar. 2. Sistemde işlem havuzunun kullanımı seçimli olabilmekte, işlemler yayınla öğrenilebilmektedir. Doğrulanmamış işlemler, düğümler tarafından çağırılır. 3. Ağda kullanılan protokole göre, n adet işlem toplu olarak bir bloğa yazılabilir. Düğümler tarafından yeni blok oluşturulur. 4. Doğrulama için eşler arası ağdaki bilgisayarlara yayın yapılır. 5. Doğrulama bilgisinin tamamlandığı bilgisi ağ içerisinde iletilir. 6. Eşler

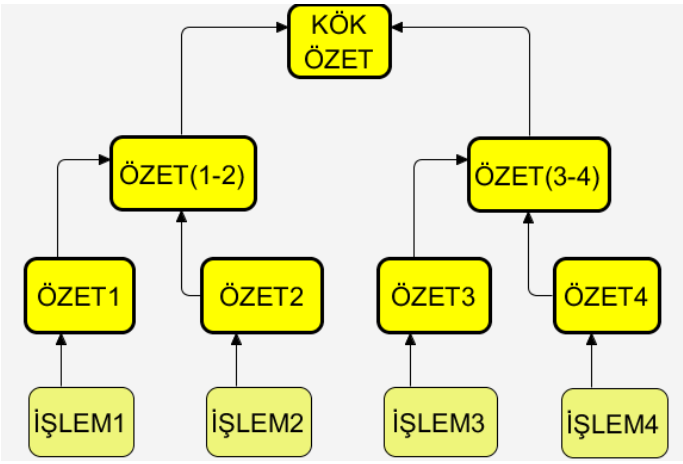
DOI NO: 10.17932/IAU.EJNM.25480200.2019.3/2.71-83

arası ağda konsensüs protokolü ile bir madenci düğümü seçilir. Seçilen madenci düğümü, yeni bloğu blokzincirine ekler. 7. Talep edilen işlemin tamamlandığı bilgisi, işlemi gerçekleştiren makinelere iletilir (Karaarslan ve Akbaş, 2017).



Şekil 3: Blokzinciri Tabanlı Uygulamada Yeni Bloğun Zincire Eklenmesi

Bloklar, hash (özet) değeri ile önceki bloklara bağlanmaktadır. Bu süreçte önceki bloklardaki özet değerinden genel özet değeri oluşturulmaktadır. Aynı zamanda bir önceki bloğun özeti de tutulmaktadır. Blok içerisinde ise; 4 işlemin toplanarak bir bloğa yazılması durumunda alınan özetlerden kök özet (Merkle ağacının) oluşturulması Şekil 7'da gösterilmiştir (Karaarslan ve Akbaş, 2017).



Şekil 4: Merkle Ağacının Oluşturulması

Bir blok içerisinde en az bir işlem yer alır ve bir blok 1 MB boyutundadır. Blok üst bilgisi 80 Byte uzunluğundadır ve bloğa ilişkin bilgileri içermektedir. Her bir transfer işlemi en az 250 Byte uzunluğundadır ve bir blokta ortalama 350-500 arası işlem bilgisi yer alır (Kırbaş, 2018).

Research Article - Submit Date: 01.11.2018, Acceptance Date: 25.04.2019

DOI NO: 10.17932/IAU.EJNM.25480200.2019.3/2.71-83

KRİPTO PARALAR

Kripto paraların günümüzde en yaygın kullanımı Bitcoin'dir (Turan, 2018). Bitcoin, blokzinciri teknolojisinin ilk uygulamasıdır (Iansiti ve Lakhani, 2017). Anlaşılacağı üzere Bitcoin ile blokzinciri aynı şey olmayıp, blokzinciri Bitcoin kripto parasının arkasındaki yaratıcı güçtür. 2009 yılının Ocak ayında ise ilk blok (Genesis blok) Nakamoto tarafından oluşturularak madencilik ve transferler başlamıştır. Bitcoin'i kendisinden önce ortaya çıkan sanal paralara karşı farklı kılan şey kişiden kişiye (P2P) doğrudan transfer yapılabilmesi ve hiçbir aracıya ihtiyaç duyulmaması ve blokzinciri teknolojisi üzerine kurulu olmasıdır (Yıldırım, 2015). Günümüzde takibi zor miktarda yeni kripto paralar oluşturulmaktadır. Özel iştirakler dışında kamu kurumlarının da finans alanındaki çalışmaları, kaçınılmaz olarak yeni finansal ürünleri ortaya çıkarmaktadır. Kabaca günümüzde kullanılan kripto paralara örnek vermek gerekirse: "Bitcoin, Ethereum, XRP, Litecoin, EOS, Bitcoin Cash, Binance Coin, Tether, Stellar, TRON, Bitcon SV, Cardano, Monero, IOTA, Dash, Maker, NEO, Ethereum Classic, NEM, Ontology, Zcash, Waves, VeChain, Tezos, Basic Attention, USD Coin, Dogecoin, Bitcoin Gold, TrueUSD, ABBC Coin, Qtum, Chainlink, OmiseGO, Decred, ICON, List, Holo, Augur, Zilliqa, Steem, 0x, DigiByte, THETA, BitShares, Bytecoin, Nano, Bitcoin Diamond, Enjin Coin, Pundi X, Komodo, Aurora" gösterilebilir.

Şekil 5: Kripto Para Örnekleri

Alışılmış klasik para birimleri ve ödeme şekilleri ile karşılaştırıldığında Bitcoin'i diğer para birimlerinden ayıran temel özellikleri şöyledir: Merkezi bir otoriteye bağlı olmaması. P2P teknolojisi ile işlem yapması. Dijital bir ortamda hazırlanması ve kullanılması. Arzında bir limitin olması. Bilgisayar algoritmaları ile tasarlanan çok karmaşık bir ürün olması. Sınırlı bir kabul ve kullanım alanının bulunması. Bitcoin hesaplarının herhangi bir kamu ya da özel kuruluşu tarafından sigortalanmaması şeklinde sıralanabilir (Sönmez, 2014). Bitcoin'in blokzinciri uygulama tecrübeleri, halen aşılması gereken çok sayıda zorluk olduğunu ortaya koymaktadır. Güvenlik, Ölçeklenebilirlik ve (De-)Merkezileşmenin Sınırları bu zorluklara örnek gösterilebilir (Karame, 2016). Bitcoin'in işleyişi, ağdaki işlemsel güce sahip çoğunluğun dürüst olmasına dayanmaktadır. Her yeni blok, daha önceki bloğun hash (özet) adı verilen bir fonksiyon ile sabit sayıda bit'e sıkıştırılmış diyebileceğimiz bir halini içerir. Böylece blokzinciri üzerinde geriye dönük değişiklik yapılması engellenerek güvenlik açısından bütünlük sağlanmış olur; onaylanmış bir işlem üzerinde değişiklik yapılmak isteniyorsa o işlemi içeren bloğun tamamlanması için çözülmesi gereken algoritmik problem tekrar çözülmelidir. Ayrıca bunun üzerine, her blok önceki blokların yansımasını içerdiği için, değişiklik yapılmak istenen bloktan sonra gelen tüm bloklar için aynı işlem tekrarlanmalı yani alternatif bir blokzinciri üretilmelidir. Blokzincir yapısının tüm Bitcoin kullanıcıları tarafından devamlı üzerinde çalışılan ve büyüyen bir yapıda olması bu güvenlik riskine imkân tanımamaktadır; çünkü "en uzun" blokzincir alternatifi kabul edilmekte ve kullanıcılar bunun üzerinde çalışmaya devam etmektedir. Geçmişe yönelik bir değişikliğin kabulü ancak alternatif blokzincirin daha hızlı üretilmesi ile gerçekleştirebilir ki bu da ağdaki işlemsel gücün çoğunluğuna sahip olmayı gerektirir. Tüm işlemlerin ağdaki kullanıcılar tarafından kolektif halde gerçekleştirilmesi bunu anlaşılır hale getirmektedir. Çoğunluğun dürüst davranmaması halinde normalde onaylanmaması gereken işlemlerin onaylanmış kabul edildiği

blokzinciri alternatifi "gerçek" blokzincirinden daha uzun hale gelerek kabul görebilir. Örneğin 2014 yılında Ghash isimli mining havuzu herhangi kötü bir niyet olmasa da geçici olarak ağdaki işlem gücü çoğunluğunu elde ederek Bitcoin sistemini tehdit edebilecek hale gelmiş, risk kullanıcıların diğer havuzlara yönlendirilmesi gibi çeşitli önlemler ile bertaraf edilmiştir. Verilen blok ödülü işte bu noktada, sistemin işleyişi ve kullanıcıların dürüst davranmaları için bir teşvik olarak davranmaktadır. 21 milyon bitcoin oluşması sonrası blok oluşturma ödülünün verilmemesi ile işleyiş, kullanıcıların işlemlerinin işlenmelerini ve onaylanmalarını sağlamak için işlemlerine işlem ücreti eklemeleri ile devam edecektir; blok oluşturan kullanıcılar ödül olarak blok içerisinde yer alan işlemlerin işlem ücretlerine sahip olacaktır (Khalilov, Gündebahar ve Kurtulmuşlar, 2017). Diğer yeni ödeme yöntemleri gibi, sanal bir para birimi olarak Bitcoin de meşru kullanım alanlarına sahiptir; önde gelen girişim sermayesi firmaları sanal para kurma girişimlerine yatırım yapmaktadır. Sanal para birimleri, ödeme verimliliğini artırma ve ödemeler ve fon transferleri için işlem maliyetlerini azaltma potansiyeline sahiptir. Örneğin, Bitcoin, geleneksel kredi ve bankamatik kartlarından daha düşük ücretlerle işlem yapılmasını sağlayabilecek küresel bir para birimi olarak işlev görmektedir. Sanal para birimi, mikro ödemeleri de kolaylaştırabilir ve işletmelerin bir kerelik oyun veya müzik indirme gibi internette satılan çok düşük fiyatlı mal ya da hizmetlerin alım satımının kolaylıkla yapılmasını sağlayabilir. Hâlihazırda bu tür ürünlerin, örneğin geleneksel kredi ve borç ilişkisi içinde, daha yüksek işlem maliyetlerinden ötürü birim başına uygun fiyatlarla satılabilme kabiliyetleri zayıftır. Sanal para birimleri, uluslararası nakit ödemeleri kolaylaştırabilir ve başka yollarla finansal içermeyi destekleyebilir. Zira potansiyel olarak bankalara hizmet verebilecek yeni sanal para birimlerine dayalı ürün ve hizmetler geliştirilebilir. Sanal para birimleri, özellikle de Bitcoin, yatırım için bir alternatif olabilir. Basılması için herhangi bir merkezi otoriteye ihtiyaç duymamakla birlikte saklanması için ticari bir bankanın varlığına ve transferi için de bir elektronik para transferi şirketine ihtiyaç duymaz (Dulupçu, Yiyit ve Genç, 2017).

TARTIŞMA VE SONUÇ

Bilim sadece bilimsel çalışmalardan ve felsefe de sadece filozofların sistemlerinden ve aynı zamanda felsefe sadece filozofların yorumlarından, bilim de sadece bilimsel çalışmalardan ibaret değildir. Her iki alan, sadece filozofa veya bilim insanına bırakılamayacak kadar önemlidir; çünkü bu iki alanın kesişimi insanlık serüvenini oluşturan temel iki unsurdur[29]. Çalışmamızın konusu olan blokzinciri ve uygulama alanlarından biri olan kripto paralar da yapılan açıklamanın çok güzel bir örneğidir. Çünkü finansal krizler ve bu krizlerin temelinde yer alan merkezi otoritelerin görevlerini layıkıyla yerine getirmemeleri, tarihte birçok kez görüldüğü üzere farklı form ve şekillerde kabul görmüş ekonomik anlaşmaların içlerinin boşaltılması ve manipülasyonların yapılması, 2008 yılında Satoshi'nin önerdiği çözümün karşımıza çıkarmasına sebep olmuştur. Ortada felsefi bir yaklaşımın, yani var olan ekonomik sistemin sorunlarının düşünülmesi ve sonuç olarak da tümden bir reform ihtiyacının olduğu kanısına varılması ve bunu yaparken de bilgisayar bilimleri konularının esas alınarak bir çözüm önerilmesi, tam da bilim ve felsefenin kesişimine verilebilecek uygun bir örnektir. Hatırlanacağı üzere çalışmamızın giriş bölümünde dogmaların insanın değer yargıları üzerindeki etkilerinden bahsetmiştik. Dogmaların da aynı zamanda toplumun geniş bir kısmının onayından geçmiş ve doğruluğunun tartışılma ihtiyacı hissedilmeyen kavramlar olduğunu açıklamış ve "insanlar değil, dogmalar kusursuzdur" genellemesi ile bu açıklamalarımızı tasdik etmiştik. Ancak insanların sahip olduğu, çoğunluğunu dogmaların oluşturduğu değer yargılarının ulviliğine rağmen, bu değerlere ters kalacak şekilde kolay para kazanma arzusuna kapıldıklarından bahsetmiştik. Kolay para kazanma arzusu; üzerinde psikoloji, sosyoloji ve alakalı bilimsel alanlar yardımıyla araştırmalar yapılması gereken ve kati bir cevap verilemeyecek derinlikte bir konudur. Çalışmamızda dikkat çekmek istediğimiz husus; kripto paralar ve arkasındaki yaratıcı güç olan blokzincirine insanların kolay para kazanma arzusu ile rağbet görmesi ve doğal olarak da aşırı talep ile sınırlı sayıdaki Bitcoin kripto parasının değerinin beklenenden çok daha kısa bir sürede, beklenmedik meblağlara yükselmesi ve bu durumun da temelinde yatan kolay para kazanma arzusunun katlanarak ve bir hastalık gibi yayılarak büyümesi durumudur.

Çalışmamızın terminoloji, Blokzinciri Teknolojisi ve Kripto Paralar bölümlerinde açıklanan bilgiler ışığında düşündüğümüzde, 2008'den sonra karşımıza çıkan Bitcoin ve birçok altcoinin ne Ponzi şeması, ne borsa manipülasyonları ne de herhangi bir duygu sömürüsüne dayalı bir aldatma yöntemi

olmadığı çok açık ortadadır. Aksine kripto para teknolojisi çok yeni sayılabilecek bir geçmişe sahip olmasına rağmen, birçok resmi kurum ve kuruluşun dikkatini çekmiş ve "merkezi otoritenin" kendi sistemlerine bu teknolojiyi adapte etme çalışmalarına sahne olmuştur. ABN Amoro, UNG, RaboBank, Master Card, Akbank gibi yerli ve yabancı finans kurumları kripto paralar ve blokzinciri üzerinde çalışmalarına devam etmektedirler. Venezuela kripto para olan Petro-Gold'u çıkarmış ve fiyatını da varil petrolün birim fiyatına göre belirlemiştir. Hindistan Merkez Bankası ve Türkiye Merkezi Bankası blok zinciri ve finansal uygulamaları üzerinde çalışma yaptıklarını duyurmuştur. Kanada kimlik kartlarının, Estonya ise sağlık sisteminin blokzinciri teknolojisinden faydalanarak yeniden oluşturulacağını açıklamıştır. Tüm bu gelişmeler, yaşanacak değişimin beklenenden çok daha kapsamlı ve etkili bir şekilde yaşanacağına işaret etmektedir. Bu bağlamda, blokzinciri ve kripto paralar teknolojisi ile internet teknolojisinin hayatlarımıza etkisi birçok kişi tarafından benzer görülmektedir. Açıkladığımız tüm bu olumlu yanları ile blokzinciri teknolojisi insanların kolay para kazanma arzusunu kötüye kullanma amacıyla geliştirilmemiş olup, yine de üzerinde durulması gereken soru işaretlerini bünyesinde barındırmaktadır.

Newton, bilimin, bilimsel çalışmalardan ibaret olmadığını göstermiştir; çünkü cevaplar ne kadar "bilim" sınırları içinde kalsa da sorunlar felsefi içeriklerle donatılmıştır. Bu durum, felsefe ve bilimin birbirini etkilemesinin de tipik bir örneğidir (Ural, 2015). Öyleyse Bitcoin'e geri dönüp tekrardan bir ilgi göstermekte fayda vardır. Bitcoin kripto para birimini öneren kişinin gerçek bir şahıs olmadığı aşikardır. Önerilen teknolojinin tanıtılması ve yaygınlaşması sürecinden sonra Satoshi'nin ortadan kaybolması ve şahsi hesabından hiç bir işlem yapmaması (BTC 19000 Dolar değerini gördüğünde dahi bir satış görülmemiştir.) üzerinde düşünülmesi gereken bir noktadır. Ya Bitcoin'i öneren kişi ya da kişiler insan-ı kâmil diye sıfatlandırabileceğimiz olgunlukta kişilerdir ya da çok daha farklı beklentiler içerisinde olan, biraz daha ileri gitmek gerekirse, kişilerden ziyade günümüz finans sisteminden hoşlanmayan bir otoritenin uzun soluklu bir değişim planlamasından başka bir şey değildir. Tüm bu soru ve teoriler blokzinciri ile alakalı olmayıp tamamen Bitcoin ve bu fikri ortaya atanların asıl niyetini sorgulamamızı gerektiren nedenlerdir. Amiyane bir şekilde ifade etmek gerekirse; birileri kripto para teknolojisini insanlığın kucağına bırakmış ve çekip gitmiştir. Bu durumda kullanmakta olduğumuz Bitcoin, ethereum gibi finansal enstrümanlara duyulan ihtiyacı mı yoksa tümüyle kripto para fikrinin arkasında yatan asıl niyetin ve güvenilirliğinin mi sorgulanması gerekmektedir? Yoksa üzümü yemek ancak orta ve uzun vadede bu işten kimlerin etkileneceğini düşünmek yeterli midir? Bu arada yenen üzümün blokzinciri olduğunu hatırlatmakta fayda vardır. Günümüzde kullanılan tüm kripto paralar günün birinde bir değer ifade etmeyebilir. Ancak blokzinciri teknolojisi ve uygulama alanları ilerde birçok sektörde olduğu gibi finans sektöründe de; demir paradan kağıt paraya geçilmesi ve son süreçte kağıt paradan da kredi kartlarına geçilmesi gibi benzer bir süreç ile devletlerin kripto paralarına geçişleri ile beklenen konuma gelebilir.

Açıklamalarımızdan blokzincirinin her sorunun çözümünde çare olacağı anlamı da çıkarılmamalıdır. Çünkü blokzinciri teknolojisinin de karşı karşıya olduğu zorluklar vardır. Bu zorlukların nasıl aşılacağı aslında blokzincirinin hayatlarımızı kolaylaştırabilir mi yoksa yeni problemlerin, güvenlik açıklarının ve çok daha yıkıcı sonuçların yaşanmasına sebebiyet verebilecek başlı başına bir sorun olup olmayacağını gösterecektir. Blokzincirinin karşılaştığı zorlukların bir kaçından bahsedecek olursak: Önceki bölümlerde bahsettiğimiz, Ledger denen açık muhasebe defteri sayesinde ağdaki tüm veriler görülmektedir. Bu şeffaflığı %100 sağlar. Peki, şeffaflık ile mahremiyet arasında olması gereken denge nasıl sağlanabilir? Bu dengenin şeffaflıktan ödün vererek sağlanacak bir yol bulunduğunu düşünürsek; getirilen çözümün Satoshi'nin ortaya attığı fikirle çelişmesi bir sorun teşkil eder mi? Ayrıca Blokzincirinin şeffaf olmasından ziyade sistemin gizlilik konusunda da sorunları bulunmaktadır. Çünkü gizlilik kavramı blokzincirinde kati değildir. İşlemlerin analiz edilmesi sonucunda kişilerin IP adreslerine erişilmesi imkânsız değildir. Değinmek istediğimiz bir diğer sorun ise kuantum teknolojisidir. Bilindiği üzere blokzinciri, çok basit bir şekilde ifade etmek gerekirse, kriptoloji biliminin bir çalışmasıdır. Temelinde şifreleme algoritmaları yatmaktadır. Günümüz süper bilgisayarları yardımıyla geliştirilen algoritmalar, kuantum bilgisayarlarının kullanımının pratikleşmesi ve yaygınlaşması sonucu kırılması eskisi kadar zor olmayan algoritmalar durumuna düşecektir. Bahsettiğimiz durum elbette kısa süreli ve bir geçiş aşaması olarak adlandırılabilecek bir süreç olacaktır. Ancak yaşanabilecek aksilikler yıkıcı sonuçlar doğurabilir. Bu yüzden kuantum

teknolojisi ile yeni şifreleme algoritmaları geliştirilmesi için ivedilikle hareket edilmesi gerekmektedir. Kuantum teknolojisinin yardımıyla yeni kriptolojik şifrelemeler geliştirilmesi pahalı bir araştırma süreci olup finansmanının merkezi bir otorite yahut büyük şirketlerce karşılanması ihtiyacına da dikkat çekmek gerekir. Bu da doğal olarak üçüncü şahıs diye adlandırılan ve sistem dışına itilmeye çalışılan kurumların, çalışmaları finanse etmeleri sebebiyle oyunda kalmaya devam edeceğini ve yenilikleri sistemlerine adapte edeceklerinin çok basit bir işaretidir.

Yapılan açıklamalar üzerinde düşünüldüğünde, blokzinciri ve kripto para teknolojisinin hayatlarımıza etkisinin şimdiden görülmeye başlandığı anlaşılmaktadır. Her yeni çalışmada olduğu gibi blok zinciri ve kripto paralar teknolojisinin de kötüye kullanımı görülmüştür. Başını yasadışı narkotik trafiğinin çektiği birçok illegal organizasyon finansal işlemlerini bu teknoloji ile yürütmüş ve belki de halen yürütmeye devam etmektedir. Ayrıca Bitcoin ve diğer kripto paraların takas sitelerinde el değiştirmesi konusunda büyük sorunlar yaşanmıştır. Bu güvenlik sorunları üçüncü şahıs olan takas merkezlerinin çoklu imza teknolojisini yeterli oranda kullanmamasından kaynaklanmaktadır. Günümüzde takas sitelerinde yaşandığı düşünülen toplam kripto para hırsızlığı 650 milyon dolar miktarındadır. Yaşanan tüm bu aksilikler blokzinciri ve uygulama alanlarında geliştirilmesi gereken standartların ihtiyacını ortaya koymaktadır. İeee bu konuda gerekli çalışmaları yaptığını açıklamıştır. Standartların doğru belirlenmesi ve güvenlikten, mahremiyete varıncaya kadar birçok alanda getirilecek sınırlamalar sayesinde kurulacak yahut yenilenecek sistemler; günümüzde yaşandığını ve engellenemediğini bildiğimiz sorunların önüne geçme şansına sahip olmamızı sağlayacaktır.

Sonuç olarak çalışmamızda dogmalar ve değer yargılarının, insanın kolay para kazanma arzusu ile düştüğü tezat dikkate alınarak, blokzinciri ve kripto paralar teknolojisinin, kendisinden önce uygulanmış ve insanların mağdur olmalarına sebebiyet vermiş uygulamalardan farklı olduğunu, bilim ve felsefe ilişkisi bağlamında dikkate alarak bir araştırma yapılmıştır. Blokzinciri ve kripto paraların, söz konusu art niyetli yöntemlerden farklı olduğunu anlatabilmek için, blokzinciri ve kripto paralar birer başlık altında ayrı ayrı incelenmiş ve daha iyi anlaşılabilmesi için terminoloji bölümünde de çokça kullanılan kavramlar açıklanmıştır. Tartışma bölümünde ise blokzinciri ve kripto para teknolojisi hakkındaki görüşlerimiz paylaşılmış ve üzerinde düşünülmesi gereken konular dikkat çekilmiştir. Bu bağlamda blokzinciri ve uygulamalarının insanların hayatlarını nasıl etkileyebileceği üzerinde görüşler paylaşılmıştır.

KAYNAKÇA

Akleylek S., Yıldırım H. M. ve Tok Z. Y. (2011). Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta. Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri 2 - 4 Şubat 2011 İnönü Üniversitesi, Malatya. (Erişim 02.03.2019) link: https://ab.org.tr/ab11/kitap/akleylek_yildirim_AB11.pdf

Anavatan A. ve Kayacan E. Y. (2018). Bitcoin Getirilerinin Kaotik Yapısının İncelenmesi. Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi CİLT 5 SAYI 7 Yıl 2018, S 135-142, ISSN:2148-9963.

Antonopoulos A. M. (2014). Mastering Bitcoin. Tokyo: O'Reilly Media, Inc.

Avunduk H. ve Aşan H. (2018). Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme. Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Cilt:33, Sayı:1, Yıl:2018, ss.369-384.

Çabuk M. ve Mendi A. F. (2018). Bıtcoın'in Arkasındaki Güç: Blockchaın. Gsı Journals Serie C: Advancements in Information Sciences and Technologies, 1 (1): 12-23.

Çarkacıoğlu A. (2016). Kripto-Para BITCOIN. Sermaye Piyasası Kurulu, Araştırma Dairesi, Araştırma Raporu. (Erişim 03.03.2019) link: http://www.spk.gov.tr/siteapps/yayin/yayingoster/1130

Dulupçu M. A., Yiyit M. ve Genç A. G. (2017). Dijital Ekonominin Yükselen Yüzü: Bitcoin'in Değeri İle Bilinirliği Arasındaki İlişkinin Analizi. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Y.2017, C.22, Kayfor15 Özel Sayısı, s.2241-2258.

Durmuş S. ve Polat M. Ş. (2018). Sanal Para Bitcoin. KAUJEASF, 9(18), 659-673. ISSN:1309–4289.

Iansiti, M., Lakhani, K., (2017), The Truth About Blockchain, Harvard Business Reveiw, Vol. 95, No. 1, pp. 118-127.

Karaarslan E. ve Akbaş M. F.(2017). Blokzinciri Tabanlı Siber Güvenlik Sistemleri. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, S:16-21, 2017.

Karame G. O. (2016). On the Security and Scalability of Bitcoin's Blockchain. CCS'16 October 24-28, 2016, Vienna, Austria. ISBN: 978-1-4503-4139-4.
Khalilov M. C. K., Gündebahar M. ve Kurtulmuşlar İ. (2017). Bitcoin ile Dünya ve Türkiye'deki Dijital Para Çalışmaları Üzerine Bir İnceleme. 19. Akademik Bilişim Konferansı -- AB 2017 Aksaray Üniversitesi
Kırbaş İ. (2018). Blokzinciri Teknolojisi ve Yakın Gelecekteki Uygulama Alanları. Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi 9(1): 75-82 (2018). DOI: 10.29048/makufebed.365066.
Kodaz H. ve Botsalı F. M. (2010). Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması. Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Teknik-Online Dergi Cilt 9, Sayı:1-2010, Sayfa:10-23. ISSN 1302/6178.
Nakamoto S. (2008). Bitcoin: A Peer to Peer Electronic Cash System. (Erişim Tarihi: 04.03.2019) link:https://bitcoin.org/bitcoin.pdf
Oeser, E. (1984). The Evolution of Scientific Method, in F. M. Wuketits (ed.), Concepts and Approaches in Evolutionry Epistemology: Towards an Evolutionary Theory of Knowledge, D. Reidel, Dordrecht, Boston, Lancaster, pp. 149–184.
Sakakibara Y., Nakamura K. ve Matsutani H.(2017). An FPGA NIC Based Hardware Caching for Blockchain. In Proceedings of HEART2017, Bochum, Germany, June 7–9, 2017, 6 pages. https://doi.org/10.1145/3120895.3120897
Taşoğlu N. P. (2008). Çok Katlı Pazarlama Şirketleri İle Piramit Şema Organizasyonlarının Yapısal Farklılıkları Üzerine Bir İnceleme. Sosyal Bilimler Dergisi / Journal of Social Sciences 2(1),2008, 25-39.
Sütçü S. S. (2016). "6502 Sayılı Tüketicinin Korunması Hakkında Kanun M.80 Hükmüne Göre Piramit Satışlar", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, cilt.22, ss.2505-2521, 2016.
Sönmez A. (2014). Sanal Para Bitcoin. The Turkish Online Journal of Design, Art and Communication - TOJDAC July 2014 Volume 4 Issue 3.
Şahin E. E. (2018). Kripto Para Bitcoin: ARIMA ve Yapay Sinir Ağları İle Fiyat Tahmini. Fiscaoeconomia 2018, Vol.2(2) 74-92. DOI: 10.25295/fsecon.2018.02.005.
Takaoğlu F., Sönmez F. ve Kaynar O. (2018). İdeal Steganografi Senaryosu: Taşıyıcı Resimlerin Kapasitelerinin Hesaplanması, Frekans Tabanlı Steganografide OPA Yöntemi. Acta Infologıca, 2018; 2(1): 12-21 Research Article ISSN: 2602-3563.
Taş O. ve Kiani F. (2018). Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme. Bilişim Teknolojileri Dergisi, CİLT: 11, SAYI: 4, EKİM 2018. DOI: 10.17671/gazibtd.451695.
Turan, Z. (2018). Kripto Paralar, Bitcoin, Blockchain, Petro Gold, Dijital Para ve Kullanım Alanları, Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 11(3), 1-5.
Ural Ş. (2015). Newtoncu Bilim Anlayışı. Kilikya Felsefe Dergisi. Issue 1, Pagination 11 - 22, Date Published 2015. ISSN: 2148-7898 E-ISSN: 2148-9327.
Ural Ş. (1994). Bilim Felsefesinin Amacı veya Bilim Felsefesinin Felsefesi, Felsefe Arkivi, Sayı: 29, 1994. İnternet Kaynağı, (Erişim 29.02.2019) link: https://www.safakural.com/makaleler/bilim-felsefesinin-amaci-veya-bilim-felsefesinin-felsefesi
Ural Ş. (1985). Karl Raimund Popper. Popper'in "Tarihselciliğin Sefaleti adlı eserinin çevirisine (İstanbul, 1985) yazılan sunuş. İnternet Kaynağı, (Erişim 28.02.2019) link: https://www.safakural.com/makaleler/karl-raimund-popper
Ünsal E. ve Kocaoğlu Ö. (2018). Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri. Avrupa Bilim ve Teknoloji Dergisi Sayı 13, S. 54-64, Ağustos 2018.
Yıldırım F. (2015). Kripto Paralar, Blok Zinciri Teknolojisi ve Uluslararası İlişkilere Muhtemel Etkileri. Medeniyet Araştırmaları Dergisi, Cilt: 2 Sayı: 4 Yıl: 2015.