BLOKZİNCİR (KRİPTOPARA) TEKNOLOJİSİ VE FİNANSAL SİSTEMLERE KAÇINILMAZ ETKİLERİ

Dr. Murad KAYACAN (SMMM) (SPK Düzey III./KY)

(www.muradhoca.com)

Oğuzhan ÇELİK (THY Muhasebe Uzmanı)

Giriş

Ekonominin bir parçası olan ödeme sistemleri zaman içerisinde sürekli değişime uğramış ve gelişen teknolojilere uyum sağlamıştır. Çok kısa zamanda nakit paradan günümüzdeki ödeme sistemlerine gelene kadar bile onlarca gelişime uğramıştır. 2000'lerden sonra ise artık tamamen dijitalleşen Dünya'da paranın, ödeme sistemlerinin yapısı ve işlem hacmi ciddi bir şekilde ve hızla değişmiştir. Bugünlerde ise çokça konuşulan kripto paralar ve ardından gelen altyapı teknolojisi olan blok zinciri yapısı ise gelecek dönemde bildiğimiz ödeme sistemlerini daha da değiştireceğe benziyor ancak bu yenilik elbette riskleri de beraberinde getiriyor. Artık yatırım araçları arasında da kabul edilen Bitcoin son bir yılda Amerikan doları karşısında on kat değer kazanmış ve yatırımcıların ilgisini de bu alana çekmeyi başarmıştır fakat hala sahip olduğu belirsizlikler yüzünden ne devletler ne de kurumlar tarafından net bir şekilde onaylanmayı başaramamıştır. Bu çalışmada blok zinciri teknolojisinin ve sağladığı yan ürünlerin finansal piyasalara etkisi tartışılacak aynı zamanda gerekli hukuki altyapı için önerilerde bulunulacaktır.

Ödeme Sistemlerinin Tarihçesi

Ekonominin ve hayatın vazgeçilmez aracı olan para, yüzyıllardır bir değişim aracı ve ölçüm birimi olma özelliğini devam ettirmektedir. Bu süre zarfında takas sistemindeki mal paradan maden paraya geçilmiş ardından madenlere dayalı kâğıt paralar ortaya çıkmış böylece ticari hayatta bire bir mal ya da maden değişimi olmadan temsili kâğıtlarla işlemler yapılması sağlanmıştır. Madene dayalı kâğıt para önceleri çift metal sistemini(gümüş ve altına dayalı sistem) 1817 yılına gelindiğinde ise İngiltere öncülüğünde tek metal sistemini(altın) benimsemiştir. Bunun sebebi gümüşteki aşırı değer kaybının çift metal sistemini çalışamaz hale getirmesi olmuştur. Altın standartlarıyla birlikte paranın çevrilgenlik(convertibility) özelliği doğmuştur.

I. Dünya Savaşıyla birlikte hükümetlerin para ihtiyacı artmış, dünya ekonomik krizi ve II. Dünya Savaşı'nın patlak vermesiyle de bu ihtiyaç somutlaşmıştır. Öyle ki çoğu ülke altın standardını kaldırmış ve altın külçe standardına geçmiştir yani banknotların direkt olarak altınla takası da böylece son bulmuştur.(Davies,2002) Bu süreçte kâğıt para dediğimiz her ülkenin kendi yetkili bankası(Merkez Bankası) tarafından basılan para egemen olmuştur. İtibari ya da kâğıt para olarak adlandırılan bu para 1971 yılında ABD dolarının altın karşılığının kaldırılmasıyla birlikte modern siyasi iktisatta yerini almaya başlamıştır. Kâğıt paranın gücü ağırlıklı olarak ülke içi istikrara ve dış ilişkilerdeki başarıya bağlıdır. Bunlar dışında birçok değişkene de bağlı olmakla birlikte ülkenin ekonomik durumu etkin belirleyici konumdadır. Kâğıt para kavramı zaman içerisinde kaydı paranın daha çok kullanılmasına sebebiyet vermiştir. Son aşamada ise bankalar arası yeni değişim araçları ve ödeme sistemleri oluşmaya başlamıştır.

Ödeme sistemleri para dışında ödeme aracı olarak kullanılan ve günümüzde çoğunlukla banka, kredi kartı ve dijital sistemler olarak adlandırılan değişim araçlarıdır. Bu yöntemler arasında EFT, havale, virman, swift, mobil cüzdanlar ve ön ödemeli kartlar(sanal kart)

bulunmaktadır. Yakın zamanda ise ortaya çıkan blok zinciri teknolojisi ile de gelecek dönemde "bitcoin ve alt coinler" gibi daha farklı ödeme yöntemleri de geliştirilebilir.

Ödeme araçları tarihte oldukça büyük öneme sahiptirler çünkü bu sistemlerin bilinçli kullanılmaması sonucunda finansal balonlar ve krizler yaşanmıştır. Nakit para yerine, kartla ödeme yapılması fikri ilk kez Amerikalı yazar Edward Bellamy' in "Looking Backward or Life in the Year 2000" adlı romanında 1887 tarihinde kaleme alınmıştır. 1914 yılında Western Union Bank "şimdi al, sonra öde" sloganı ile dünyanın ilk kredi kartlı ödeme sistemini müşterilerine tanıtmıştır. Bugün kullandığımız kredi kartlarının ilk örneği ise 1950 yılında Frank McNamara tarafından "Diners Club Card" olarak sunulmuştur. 1956 yılında kredi kartları Amerika'da yaygınlaşmaya başlarken Türkiye de ilk defa 1968 yılında "American Express" sayesinde kredi kartıyla tanışmıştır. Türkiye'de kartların yaygınlaşması ilk olarak 1975 yılında Mastercard ve Eurocard sistemlerinin girmesiyle başlamış, 1983 yılında VISA kartında sektöre girmesiyle büyümeye devam etmiştir. Kredi kartları dışında, 1990 yılında Bankalar arası Kart Merkezinin(BKM) kurulmasıyla ilk elektronik POS terminali 1991 yılında kullanıma sunulmuştur. 2000 yılına gelindiğinde güvenlik önlemi gereği BKM ve üye kuruluşları chip&PIN uygulamasına geçmişlerdir. 2005 yılında ise ilk ön ödemeli akıllı kartlar TSK tarafından kullanılmaya ve aynı dönem temassız otoban ödeme sistemi olan kartsız geçiş sistemi(KGS) uygulanmaya başlanmıştır. Teknolojinin ve imkanların gelişmesi yeniliklerle beraber riskleri de arttırdığından güvenlik amaçlı olarak BKM ve TURKCELL dünyada bir ilki gerçekleştirerek, "3D Secure" ve "Turkcell Mobil İmzayı" entegre etmeyi başarmıştır. 2000'lerde oluşturulmaya başlanan sanal cüzdanlar Türkiye'de ilk defa 2012 yılında uygulamaya konulmaya başlanmıştır. (URL 1)

2009 yılı küresel krizin ardından adına "Bitcoin" denilen yeni bir dijital kripto para ortaya sunulmuştur. Bu ödeme sistemi ilk başlarda para olarak kabul edilmese de artık günümüzde kripto para ve yatırım aracı olarak yerini almış bulunmakta. Satoshi Nakamoto tarafından yayınlanan "Bitcoin: Eşten Eşe Elektronik Nakit Sistemi" yazısı ile tanılan bu kripto para, blok zinciri teknoloji alt yapısını kullanmakta ve hiçbir merkezi otoriteye bağlı kalmadan çalışmaktadır. Aynı zamanda bu varlık altın, gümüş gibi herhangi bir madene ya da devlet gücüne dayanmadan piyasadaki arz-talep şartlarında değerlenmektedir.

Gelişen Teknolojilerin Finansal Piyasalara Etkileri

Ekonominin en temel tanımı olarak "kaynakların kıtlığı ve buna nazaran ihtiyaçların sınırsızlığı" verilebilir. Bu bağlamda insanoğlu yıllar boyu kendi var olan ihtiyaçlarını karşılamak için hem elindeki kaynakları kullanmaya çalışmış hem de yeni kaynaklar bulmaya başlamıştır. Yeni kaynak arayışı ise beraberinde yeni ihtiyaçları da doğurmuş ve genel anlamda bu süreç devam edegelmiştir. Eski çağlarda tekerleğin icadıyla taşımanın kolaylaşması, kıtalar arası yolculuğu kolaylaştıran gemiler sayesinde coğrafi keşifler ve ortaya çıkan yeni kaynaklar, buharlı makinelerle birlikte ortaya çıkan sanayi devrimi neticesinde yeni ekonomi anlayışları, elektriğin ve elektrikli motorun icadıyla verimliliğin arttırılması, seri üretim bandının oluşturulması ve yakın dönemde ortaya çıkan bilgisayar temelli sistemler ile dijital dünya, internet ve otomasyon teknolojileri var olan yaşam biçiminin ve ekonominin ne yönde değiştiğini herkese göstermektedir.

Uzun yıllar teknoloji ekonomik hayat içerisinde "tarafsız" bir değişken olarak kabul edilmiş ve sadece ülkelerin ekonomik gelişmesine etkileri üzerinde durulmuştur. Teknolojinin geliştirildiği toplumdan bağımsız, alınır satılır bir meta gibi görülmesinde ve ekonomik gelişmenin tarafsız bir etkeni olarak algılanmasında neo-klasik iktisadın teknoloji seçim modelinin büyük rolü olmuştur. Bu iktisadi okul üretimi çeşitli girdilerin(emek, sermaye, hammadde vb.) çıktılara dönüştürülmesi olarak anlatmakta ve bu dönüşümün kullanılan teknoloji tarafından şekillendireceğini varsaymaktadır. En temel manada emek ve sermaye girdisinin hangi oranda

ve nasıl kullanılacağını teknoloji seçimi olarak adlandırmaktadır aynı zamanda teknolojiyi dışsal kabul etmekte ve verimlilik ölçütü olarak ele almaktadır. Tam rekabet ortamında varsayılan ekonomide sayısız teknik birleşimi oluşmakta böylece firmalar kendilerine uygun teknik ve emek-sermaye bileşimlerini seçebilmektedirler. Bu yüzden teknoloji bağımsız ve alınıp satılabilen meta gibi kabul edilmiştir.(Ansal,2004) Teknolojik gelişme ise bir malı aynı ölçekte daha az girdi kullanarak üretmek olarak kabul edilmekte ve bu da teknolojinin ekonomi dışı bir etken olduğu varsayımıyla açıklanmaktadır. (Elster,1983) Ekonomide statik ve kararlı bir denge varsayımı bulunduğundan, tam rekabet piyasasında, firmalar elinde bulundurdukları teknolojileri geliştirme yoluna gitmezler hâlihazırda farklı bir tekniği alıp satabilmektedirler. Teknoloji seçimi varsayımı dışsal etken olarak gördüğü teknolojiyi, ekonomik çerçevede sadece üretkenlik bağlamında ele almış ve niçin geliştirilmesi gerektiğini açıklamamıştır. (Ansal,2004)

Teknolojik yeniliği ekonomik büyüme açısından ilk irdeleyen Schumpeter olmuştur. Bu varsayım teknolojik yeniliğin ekonomik gelişme ve dalgalanmaların temel sebebi olduğuna dayanmaktadır. Girişimcilik, yaratıcılık ve tahmin edilmezlik oluşturulan varsayımın en önemli unsurlarıdır. Schumpeter' e göre teknolojik yenilik devamlılık arz etmeyen ve cari durumdan, teknolojiden ayrılış ifade eden radikal ve nitel bir değişikliktir. Bu açıdan sadece üretimi arttırmaz aynı zamanda yeni bir malın, pazarın, üretim metodunun sunulması, yeni hammadde kaynaklarının bulunması ya da piyasa yeni örgütlenmeleri de kapsar. Böylece neo-klasik anlayışın üretkenlik bağlamından daha geniş anlam ifade eder. Varsayımda girişimci çıkardığı teknolojik yenilik sayesinde piyasa ortalamasının üstünde kar eder ve tekel konuma gelir ardından diğer firmalar da yeniliğe adapte oldukça kar normal seviyesine iner ve bu durum başka bir girişimci tarafından yeni bir teknolojik gelişim yaratılana kadar devam eder. Dolayısıyla teknoloji ekonominin gelişmesindeki en önemli ve içsel bir faktör olarak ele alınmıştır.(Ansal,2004)

Neo-klasik iktisadın sunduğu teknoloji teorisi ve Schumpeter'in ortaya koyduğu teknolojik yenilik teorisi sadece ekonominin üretim kalemi üzerinde ele alınmıştır. Evrimci kuram teknolojiyi fiziksel bir dönüşüm süreci olarak görmektense teknolojik bilgi ve bunun organizasyonda nasıl kullanıldığı üzerinde durmaktadır. Yenilik kavramını da sadece üretim süreçleriyle kısıtlamamış aynı zamanda yönetim, organizasyon, finans gibi konulardaki yeni gelişmeleri de kapsamaktadır. Neo-klasik iktisadın cevaplayamadığı firmaların teknoloji seçim sorusunu Ar-Ge bağlamında ele almıştır. Teknolojik değişim firmaların Ar-Ge yatırımları ve çabalarıyla sağlanmaktadır. Ancak, firmalar organizasyonel zayıflıklar nedeniyle girdilerin verimli ya da verimsiz kullanılabileceği sosyal sistemlerdir. Aynı piyasa koşullarıyla karşılaştıklarında bile firmalar aynı yönlü hareket etmeyebilir ve aynı kararları vermeyebilirler. Belirli sektörler için ise yaparak öğrenme önemli bir faktör olabilir ve Ar-Ge faaliyetlerinin yerine geçebilir. Ekonomik büyümenin sağlanması ve refahın arttırılması ülke içerisindeki firmaların Ar-Ge çalışmalarıyla yarattıkları teknolojik yenilikler sonucu elde ettikleri ticari başarılara bağlıdır.(Ansal,2004)

Görüldüğü üzere teknoloji kavramı ve teknoloji alanındaki gelişmeler sürekli olarak ekonomi içerisinde ele alınmış bu süreçte farklı yaklaşımların ortaya çıkmasına sebep olmuştur. Sadece üretim yöntemleri değil, aynı zamanda bilginin elde edilmesi, kullanılması, organizasyonu, paylaşılması ve tekrardan geliştirilmesi üzerine kurulu bir iş çevrimleri oluşturmaktadır.

Literatürde teknoloji üzerine birçok çalışma olmasının sebebini yine bu gelişme döngüsüne bağlamak mümkündür. 2008 krizi öncesi ABD ekonomisinin durumu bilişim teknolojileri açısından ele alınması bu konuda daha çok çalışma yapılmasını sağlamıştır. Bakıldığında 1990'larda Asya başta olmak üzere dünyanın diğer ülkelerinde yaşanan durgunluğa rağmen ABD ekonomik anlamda gücünü korumayı başarabilmiş hatta enflasyonu düşürebilmiş ve istihdam seviyesini arttırmıştır. ABD Merkez Bankası Başkanı Alan Greenspan'in bu ivmeyi

bilişim teknolojilerinin verimlilik düzeyini arttırmasıyla bağdaştırması ilgiyi daha da arttırmıştır.(Karaata,2012) Günümüzde dünyanın en büyük şirketleri olarak adlandırılabilecek şirketlerin bahsedilen bu firmalardan oluştuğu görülebilir.

Teknolojik gelişmeyi birçok alanda ele almak mümkündür. Bunlar arasında üretim yöntemleri, lojistik, arşivleme, finansal işlemler, iletişim, satış pazarlama en önemlileri olarak ele alınabilir. Dijital yeniliklerin sağladığı blok zinciri teknolojisi ise bahsedilen alanların birçoğunda aynı anda ve bütünleşmiş şekilde değişime sebebiyet verebilecek potansiyele sahip olduğu düşünülmektedir. İlk olarak ileriki bölümlerde de ele alınacak olan blok zinciri yapısı ve ortaya koyduğu ilk örnekler olan kripto paraların finans sektöründe mevcut ve muhtemel etkileri yadsınamayacak ölçüde büyüktür. Teknolojinin sağladığı yenilikler farklı bağlamlarda hem avantaj hem de dezavantaj olarak ele alınabilir.

Blok Zinciri Teknolojisi ve Kripto Paralar

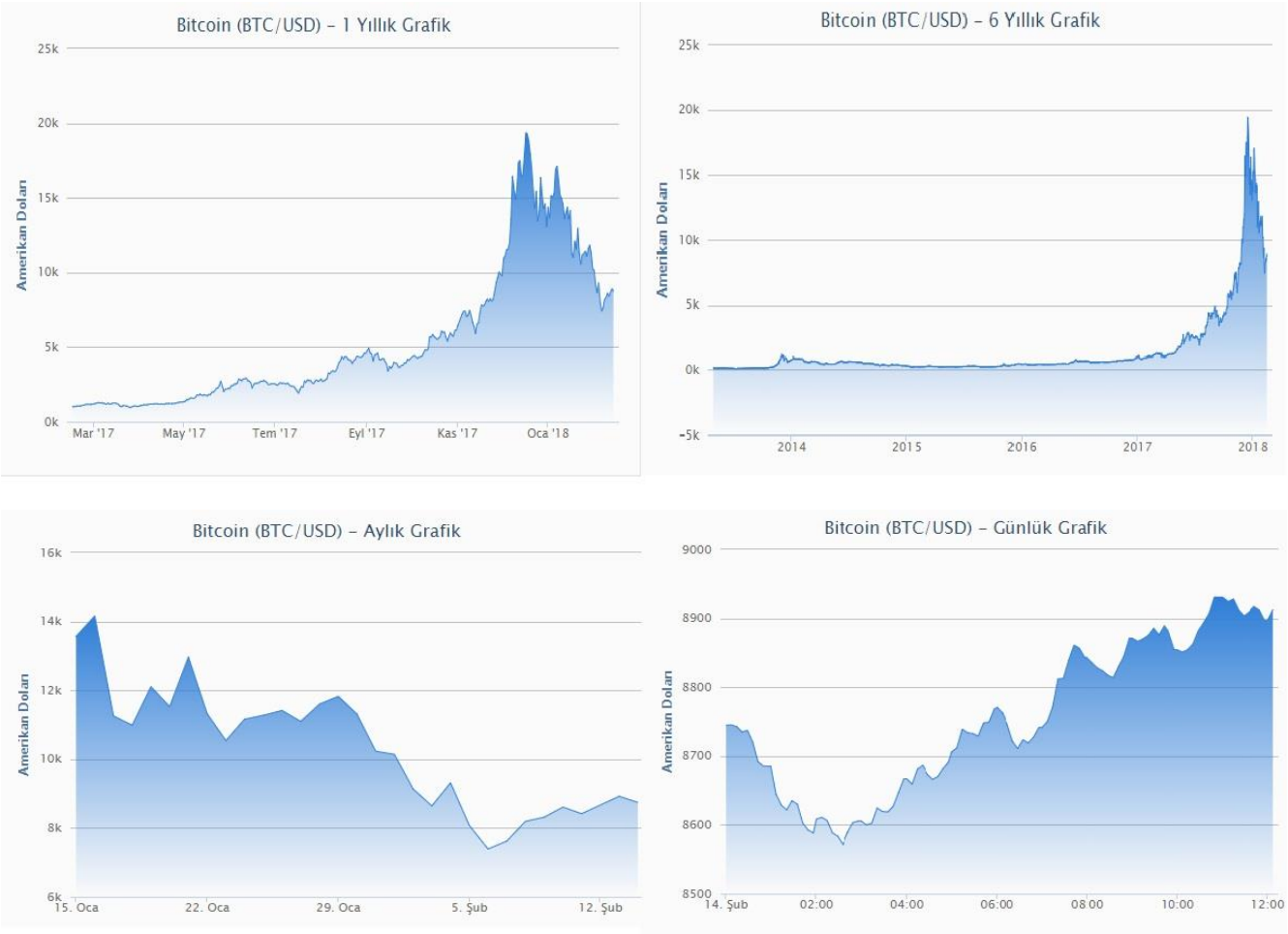
İnternet üzerinde yapılan ticaret yönteminde ve günlük hayatta kullandığımız elektronik ödeme sistemleri temel anlamda güvenli üçüncü tarafların bulunmasına dayanmaktadır. Karşılıklı tarafların yaptığı ödeme işlemlerinde banka ve kart merkezlerinin sunduğu hizmetler kullanılmaktadır. Bu işlem ise alacaklı ve borçlu taraf için işlem ve diğer maliyetleri oluşturmaktadır. Ayrıca güvene dayalı bir sistem olduğu için yüzde yüz anlamda işlemler açısından herhangi bir garanti verilememektedir. Blok zinciri(Blockchain) teknolojisi ilk olarak 2009 yılında Satoshi Nakamoto adlı kimliği kesin olarak bilinmeyen şahıs tarafından yayınlanan “Bitcoin: Eşten Eşe Elektronik Nakit Sistemi” adlı manifesto ile tanınmaya başlanmıştır. Aracılık faaliyetlerinin getirdiği maliyetler, işlem sınırları vb. gibi nedenler Bitcoin ve türevlerinin kullanımını çekici hale getirmektedir.

Bitcoin kişiden kişiye(Peer to Peer/P2P), dağınık veri tabanı sistemini kullanan şifrelenmiş elektronik para ve ödeme sistemidir. P2P sistemi ilk olarak 1999 yılında dosya paylaşım sistemi olan “Napster” ile ortaya çıkmıştı. Bu sistemle birlikte müzik dinlemek için CD yerine bir ağ üzerinde P2P işlemlerle müzik paylaşımı yapılmaya başlandı. Ardından tüm müzik endüstrisi değişmeye başladı diyebiliriz (ITunes, YouTube, Spotify vs. gibi). Bu işlem aracıları ortadan kaldıran bir sisteme sahip, parasal olarak aracı finans kuruluşlarını hatta merkez bankalarını dahi anlamsızlaştırabilecek belki de kaldırabilecek güce sahip diyebiliriz. Bu sistemde merkezi bir yapı yerine açık kaynak kodlu yazılım kullanılmaktadır. Açık kaynak kodlu yazılım olması, istenildiği zaman incelenebilir ve geliştirilebilir olması anlamına gelmektedir. Bu sistem sayesinde hâlihazırda 1400’den fazla Bitcoin benzeri altcoin bulunmaktadır. Bu sisteme blok zinciri (blockchain) denmektedir. Blok zinciri sistemi Bitcoin ile yapılan tüm parasal işlemleri o anda bir bloğa kaydederek işlemekte ve bunu ağdaki diğer tüm işlemlerle senkronize şekilde yapmaktadır. Sistem dijital cüzdan diye adlandırılan hesaplarla yönetilmektedir. Birey kendisine ait cüzdan üzerinden transfer yapmak için eşler arası kendine has özel anahtarı (private key) kullanmakta ardından ağdaki diğer kullanıcılar tarafından da açık anahtarlar (public key) kullanılarak doğrulanmaktadır. İşlem bir bloğa kayıt edilirken aynı anda başka bir işlem daha gerçekleştiriliyor olabilir ve bunun tüm ağ içerisinde doğrulanması ve senkronize edilmesi oldukça karmaşık ve zaman alan bir işlem haline gelmesini sağlayabilir. Bu karmaşık yapı içerisinde çift kullanım ya da harcama diye adlandırılan hata ve gecikme problemlerini çözmek için matematiksel olarak geliştirilen “hash fonksiyonları” yani özet fonksiyonlar kullanılır. Hash fonksiyonu karmaşık işlemleri hızlandırmak ve daha sade şekilde tanımlamak için kullanılan bir özet anlamına gelmektedir. Birçok değişken uzunluğa ve farklı yapıya sahip verileri sabit uzunlukta ve yapıdaki verilere dönüştürmek için kullanılır. Ancak kullanılan verinin türüne göre algoritma yapısı değişmektedir. Bitcoin gibi güvenlik unsurunun en temel sorun olduğu sistemde ise SHA-256 bit (Secure Hash Algoritma) yapısı kullanılmaktadır. Bu işlemin yapılabilmesi için yani SHA-256 çözülmesi için iyi bir donanım ve enerji gücüne sahip bir bilgisayarın yaklaşık 10 dakika boyunca çalışması gerekiyor. Bitcoin ağı üzerinde bu 10 dakika

içerisinde milyonlarca işlem yapıldığını düşündüğümüzde ciddi derecede zor ve zaman alan bir yapı haline geliyor. Bu yüzden on binlerce mükemmel derecede bilgisayar bu fonksiyonları çözmek için saatlerce çalışıyor. Bu problem çözme işlemine ise madencilik denmektedir. Madenciler önce de bahsedildiği gibi transferlerin güvenliğini kontrol etmek için çözdükleri bu problemler sonucunda yeni Bitcoinleri elde ediyor ve oluşan bu Bitcoinler madencilerin hesaplarına aktarılıyor. Yani bir ödül sistemi ile çalışmakta diyebiliriz. (URL 2,2017)

Bitcoin'in ise altında herhangi bir dayanak varlık, emtia vb. olmadığı halde değerlenmesi nasıl açıklanabilir sorusu tabiki akıllara gelmektedir. Piyasa içerisinde sadece arz ve talep unsurlarının etkili olduğu Bitcoin pazarı için arz miktarı ise sınırlıdır, tam olarak 21 milyon adet olduğu bilinmekte ve şuan dolanımda yaklaşık 16 milyon adet bitcoin kullanılmaktadır. Bitcoin madenciliğinin ve doğrulanmasının bu kadar zor olması onu değerli yapan etkenlerin başında geliyor denebilir ancak piyasa şartlarında talep unsuru en etkili faktör olarak göze çarpmaktadır. 2015 yılında kendi piyasasını oluşturmuş olan bu kripto paranın değeri yıllar içerisinde oldukça dalgalı bir seyir izlemiştir. Dalgalanmanın sebepleri arasında en temel göstergeler talep artışları ve hakkında yapılan olumlu ve olumsuz açıklamalar olmaktadır.

Grafik 1: BTC/ USD Farklı Dönem Fiyatları



(URL 3,2017)

Ekonomik olarak gelişmiş olan ülkelerin yaptığı açıklamalar kısa vadeli iniş ve çıkışların yaşanmasında etkili olmuştur. 21 milyon adet ile sınırlı olan arz miktarı için yapılan projeksiyonlarda son adet Bitcoin çıkarılması 2140 yılı olarak öngörülmektedir. Böylelikle daha zor çıkarılabilen ve daha da azalan Bitcoinin değerleneceği düşünülmektedir. Yakın zamanda

NYSE ve CME(CIBOT) yaptığı açıklamalar üzerine son bir ayda fiyat noktasında hızlı bir yükselişle 3 kat civarında bir artış olmuştur. CBOE Bitcoin işlemleri 10 Aralık itibariyle gerçekleşmeye başlarken 17 Aralıkta ise CME grubun sunduğu Bitcoin vadeli işlemleri başlamıştır. Bu haberlerin önceki aylarda ortaya çıkmasıyla beklentiyi satın almak isteyen yatırımcılar talebi arttırmış ve ardından NYSE de benzer açıklamalarda bulunmasıyla birlikte değeri 3 katına yani yaklaşık 19.000$ civarına çıkmıştır. Son bir yıldır kendi rekorunu kırmaya devam eden bu kripto para gelecek günlerde yaygın olarak kullanılmaya başlanabilecektir ancak halen daha hiçbir merkezi otorite veya devlet tarafından resmi bir altyapıya sokulmadığı ve tanınmadığı için uzun vadede nasıl bir süreç geçireceği öngörülememektedir. 2017 yılının son ayında kendi rekorunu kıran Bitcoin yine aynı ay içerisinde ciddi değer kayıpları yaşamaya başlamıştır. Farklı ülkelerde önümüzdeki yıllarda tanınmaya başlanacağı duyurulsa da bazı ülkeler de zaman zaman bu teknolojinin bir finansal balon, spekülasyon için kullanılan bir araç olduğu yönünde açıklamalar yapmaktadır. 13 Aralık tarihi itibariyle ise ülkemizde Sayın Mehmet Şimşek'in yaptığı açıklamaya göre "Dünya tarihinin en büyük finansal balonu ve ilki olan lale çılgınlığını aşmış bulunmaktadır, uzak durulması gerekir" söylemleri yer almaktadır(URL 4,2017). 2016 Aralık ayında ise Dr. Abdurrahman Çarkacıoğlu tarafından hazırlanan "Kripto Para-Bitcoin" SPK araştırma raporunda güvenilir bir yatırım aracı olduğu bununla birlikte kaldıraç etkisiyle işlem görmediğinden, fiyatı tamamen piyasa şartlarında belirlendiğinden ve kar-zararı önceden tahmin edilemediğinden finansal balon ya da saadet zinciri olmadığı ifade edilmiştir. (Çarkacıoğlu, 2016)

Kripto Paraların Tarihçesi

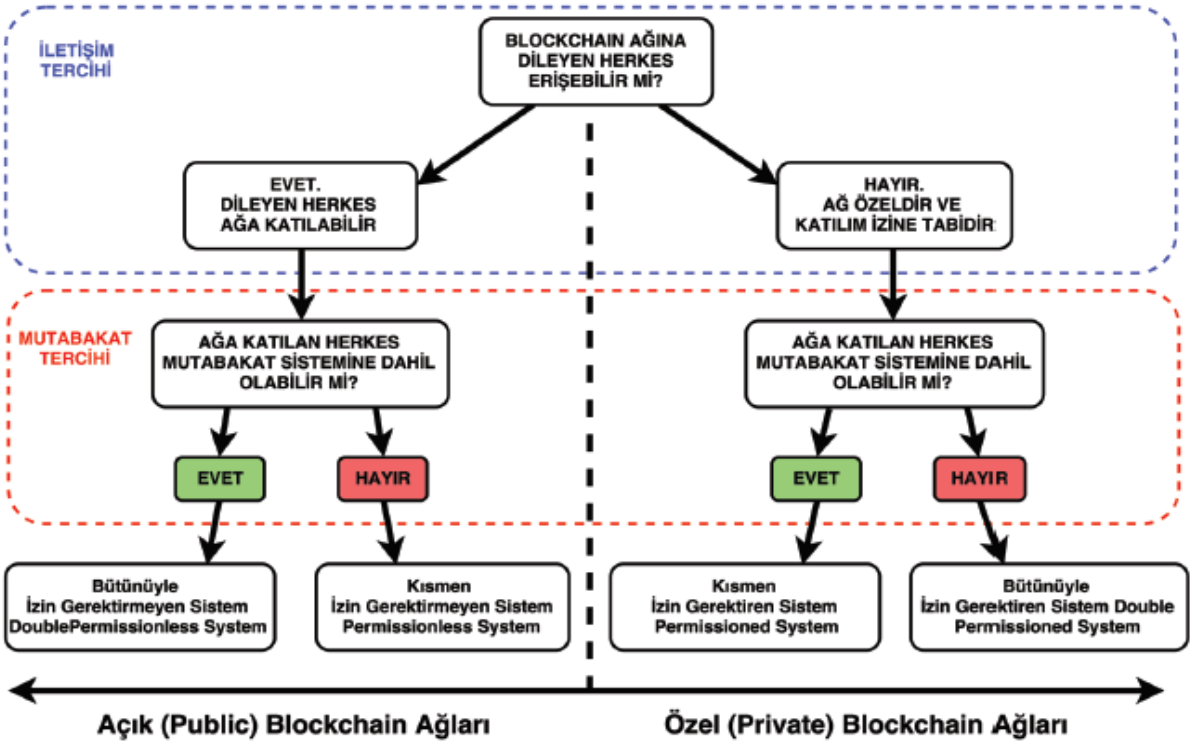
Verinin kaydedilmesi, sistemin işleyişi ve yönetilmesi açısından büyük miktarda önem arz etmektedir. Zaman içerisinde gelişen teknolojiler bu durumun sürekli iyileşmesine olanak tanımıştır. Günümüzde verileri tek bir sistemde kaydetmek zorunda değiliz bunun yerine birçok bilgisayarda ya da bulut sistemlerde saklamamız veya bu verileri P2P yapılarla dağıtarak saklamamız da mümkün hale gelmiştir. Verinin sahip olduğu yapı ve büyüklük ise sahip olduğumuz hızlı kablolu veyahut kablosuz iletişim ağları sayesinde artık önem arz etmemektedir. Görüldüğü üzere gelişen teknoloji hem veri tabanlarının düzenlenme, saklanma yöntemlerini iyileştirirken hem de bunları sağlayacak diğer araçların da gelişmesine yardımcı olmaktadır. Böylece maliyet yükü ve harcanan zaman azaltılabilir.

Verinin, önceki dönemlerde tek bilgisayarda saklandığı ardından birçok bilgisayarda saklanabildiği ve sonrasında ise verinin birçok kopyasının birçok bilgisayarda saklanabildiği bir gelişme süreci söz konusudur. Yeni sistemler sayesinde artık tüm veri tüm bilgisayarlarda saklanabilir hale gelmiştir. Verinin tüm bilgisayarlara dağıtılmasını sağlayan bu yapıya dağıtık kayıt defteri (distributed ledger) denmektedir. Bu kavram önceki yıllarda "eDonkey ve Bittorrent" gibi ağlarda da kullanılmıştır. Verilerin bu şekilde daha az maliyetle ve çoklu halde bulunması beraberinde farklı sorunları da getirmişti. Dağıtık halde bulunan verilerin güven içerisinde devamlılığının sağlanması, bozulmaması ya da değiştirilmemesi ve yeri geldiğinde doğru şekilde güncellenebilmesi için bir güven unsuru gerekliydi. Bu noktada blok zinciri teknolojisi hakkında sorunlara problem üretebileceği hatta fazlasını sunabileceği iddia edilmiştir. Verilerin kullanıcılar tarafından doğrulanmasını sağlayan ve değiştirilmesini engelleyen bu sisteme mutabakat denmektedir. "Mutabakat işlemi sistem tarafından güvenilen dış kaynaklar tarafından yapılabileceği gibi bu işlemi sistem içerisinden de yapmak mümkündür." (Usta&Doğantekin;2017)

Blok zinciri her kullanıcıya kendi şifresini de tanımlayarak, isteyen kişilerin şifreyi sadece kendisinin kullanmasına olanak tanımaktadır. Ayrıca mutabakat sisteminin sağlanması için farklı platform imkânı sunabilmektedir. Blok zinciri izin yapısına göre iki ayrı kategoride sınıflandırılabilir. Bunlar açık ağ sistemi(public ledger) ve özel ağ(private ledger) sistemleridir, dahası bunlar da kendi aralarında ağa katılma izinlerine ve katılan herkesin mutabakat

sistemine dâhil olup olmamasına göre ikiye ayrılırlar. Şekil 1'de görüldüğü üzere farklı izin yapılarında farklı mutabakat sistemleri bulunmaktadır.

Şekil 1: Blok Zinciri Ağlarının Yapısı



Kaynak: (Usta&Doğantekin;2017)

Bütünüyle izin gerektirmeyen sistem (Double Permissionless System) açık blok zinciri ağında yani dileyen herkesin girebildiği blok zincirinde, mutabakat sistemine dâhil olmak için izin gerektirmeyen yapı olarak tanımlanabilir. Bu yapıda, sisteme dâhil olan kullanıcıların ve sistemin kendisi de fayda sağlamalıdır. Böylece sistemin kendisi bir değer ifade edebilmektedir. Bitcoin blok zinciri yapısı bu sistemin en meşhur örneğidir. Bu örnekte bilindiği gibi doğrulama işlemleri yapılıp hash fonksiyonları çözüldükçe sistem kullanıcıya daha doğrusu "miner" a hediye olarak Bitcoin vermektedir. Aynı zamanda kazanılan Bitcoinlerin finansal değeri de olduğu için kullanıcıya fayda sağlamaktadır. (Usta&Doğantekin;2017) Bitcoin blok zincir sisteminin kullandığı uzlaşma yöntemi ise emek ispatı(proof of work) diye adlandırılan yöntemdir.

Açık ağlar içerisinde mutabakat sistemine dahil olmak için izin gerektiren yapılara ise kısmen izin gerektirmeyen sistem denmektedir. Burada verilere herkes erişebilirken doğrulama işlemi sadece izinli kullanıcılar tarafından yapılabilmektedir. (Usta&Doğantekin;2017) Bu bağlamda bağımsız denetim firmalarının sunduğu raporlar, bu sistem içerisinde örnek verilebilir. Günümüzde şirketlerin kendi kaynaklarında ve KAP gibi ortamlarda yayınlanan bu belgeler herkes tarafından erişilebilse bile düzenlenme, değiştirilme veya kaldırabilme gibi işlemler sadece yayın merkezleri ve bağımsız denetim firmaları tarafından onaylanabilmektedir. Böyle bir durumda blok zinciri yapısı sistemin daha etkin kullanılmasını sağlayabilmektedir. Düşünüldüğünde kısmen izin gerektirmeyen blok zinciri yapısı cari sisteme en uygun çözüm olabilecektir. Bu sayede daha hızlı ve herkesin kolayca erişebildiği, daha güvenilir ve kopyasının birçok sistem dâhilinde olduğu birçok avantajı sağlayabilir.

Ethereum blok zinciri yapısı da bu sisteme örnek verilebilir. Akıllı sözleşmeler gibi pek çok farklı amaca hizmet edebilen bu yapı sözleşme sürecini bir üst seviyeye çıkarmakta ve güvenli

işlemler için aracıları ortadan kaldırmak adına yeni imkânlar sunabilmektedir. Görüldüğü üzere ağın çıktısına bağlı bir çıkar söz konusu olmaktadır. (Lauslahti, Mattila&Seppälä,2017) Ethereum da aynı şekilde emek ispatı(proof of work) mutabakat sistemini kullanmaktadır.

Kısmen izin gerektiren sistemlere ise bankaların havale sistemi örnek verilebilir. Havale işlemi sadece bir banka içerisinde olabileceği için diğer bankalar bu ağa giremezken onay mekanizmasında tüm şubeler bu ağ içerisinde mutabakat yetkisine sahiptir yani özel bir yetkilendirme gerekmemektedir. (Usta&Doğantekin;2017) Farklı olarak bağımsız denetim firmalarının kendi içlerinde kullandığı hizmetler çerçevesinde raporların ve çalışma kâğıtlarının daha efektif bir şekilde kullanılabilmesi, aynı zamanda firma içindeki tüm kullanıcılar tarafından anında ve kolayca erişilebilir olan bir blok zinciri yapısı da bu sisteme örnek verilebilir.

Son sistem ise bütünüyle izin gerektiren sistemlerdir. Bu yapıda özel ağ olması sebebiyle sisteme giriş ve mutabakat işlemleri izinli kişilerce yapılabilmektedir. Bankalar arası EFT işlemleri bu bağlamda ele alınabilir. Her bankanın EFT sistemi için kendi blok zinciri yapısının olduğunu varsaydığımızda işlem gerçekleştirilirken mutabakat işlemi için sadece sürece dâhil bankalar bulunabilmektedir. Yani sadece bankaların girebildiği bir ağda yine sadece yetkili bankaların birbirleri arasındaki işlemleri onaylayabildiği bir sistem düşünülebilir. (Usta&Doğantekin;2017) Bağımsız denetim firmalarının verdiği raporları düşündüğümüzde bu raporları hazırlama aşamasında birçok farklı kademede insan çalışırken raporun onay aşamasında sadece o veriye yetkili kişilerce imza atılabilmektedir. Aynı zamanda bu raporun oluşturulma aşamasına kadar birçok çalışma kağıdı sistem içerisinde kullanılmaktadır. Bu noktada rapor onay aşaması için oluşturulabilecek şirketlere özgü, özel blok zinciri ağı bu sisteme örnek gösterilebilir.

Blok zinciri yapısı dağıtık sistem ve kriptolama özellikleri ile kullanıcılara anonim olabilme imkânı da sağlamaktadır. Özellikle Bitcoin için kullanılan blok zinciri yapısı kullanıcılardan gerçek kimlik bilgilerini de istemediğinden doğrudan yollarla kullanıcı bilgisine erişmeyi imkânsız hale getirmektedir. Ancak dolaylı olarak farklı yöntemlerle bu yapılar için bile gerçek kişiye ulaşmak mümkün olabilmektedir. Özellikle devletler anonim olan bu işlemlerin, kendi bilgisi dâhilinde yapılmadığı için, takibine ve kullanıcı bilgilerine ulaşmaya çalışmaktadır. Anonim olma özelliğini güçlendirebilecek farklı sistemler de bulunmaktadır. Bu noktada dış kaynaklı servisler olduğu gibi, örneğin karıştırma servisleri (mixing), blok zinciri seviyesinde Monero, Zcash ve Dash gibi kriptografik yöntemler de bulunmaktadır. Devletlerin bu işlemleri çözmek ya da imkanları ortadan kaldırarak yapacağı yaklaşımlar doğru sonuç vermeyebilecektir. Bunun yerine verilerin korunması için bu teknolojilerin kullanılarak daha güvenilir yeni sistemeler oluşturabilmesi mümkündür. (Usta&Doğantekin;2017)

Uygulama Alanları

Günümüz teknolojileri sayesinde kullanıcıların gerçek hayattaki kimlikleri dışında dijital kimliklerinin de olması vazgeçilmez hale gelmiştir ancak bu dijital kimlikler sadece belli bir merkezin kontrolünde ve yine buradan dışarıya aktarılması şeklinde oluşmaktadır. Bu durum sürecin kısıtlanmasına ve yavaş ilerlemesine sebebiyet vermektedir. Öte yandan blok zinciri yapısı sayesinde merkezi olmayan kullanıcın onay yetkisine dayalı, gerektiğinde farklı alt kimlikler oluşturulabilecek herkese açık veya kısmen açık şekilde bulunan dijital kimlikler sunmak mümkün hale gelebilmektedir. Ayrıca bu sistemle diğer alanlarda da daha verimli çalışmalar elde etmek mümkündür. Örneğin, kişilerin bilgilerinde var olan değişiklikler kısa zaman içinde dağıtık şekilde tek bir ağ üzerinde bulunabilir ve kontrol edilebilir. Böylece kullanıcının yapacağı işlemler için her yaptığı değişiklikte ayrı ayrı arşivleme ve tanımlama süreçlerine gerek kalınmamış olur. (Usta&Doğantekin;2017)

Bunlara ilaveten bu teknoloji fon ihtiyacını karşılamak isteyen firmalar içinde kullanılabilir. Kitlesel fonlama olarak adlandırılan sistemler de aracı kurum işlemlerini gerektirmekte bu da maliyetleri ve harcanan zamanı arttırmaktadır. Halbuki firmalar fon ihtiyacını karşılamak için kendisine ait bir alt coin çıkartarak bunu piyasada satabilir ve böylece kripto paranın menkul kıymetleştirilmesinde önemli adımlar da atılabilir. Dahası bu yapıyı bir borçlanma aracı veyahut ortaklık aracı olarak kullanmak da mümkündür. Böylece hisse senetlerini daha güvenilir şekilde muhafaza etmek ve kripto paralara da dayanak varlık oluşturmak mümkün hale gelebilecektir.

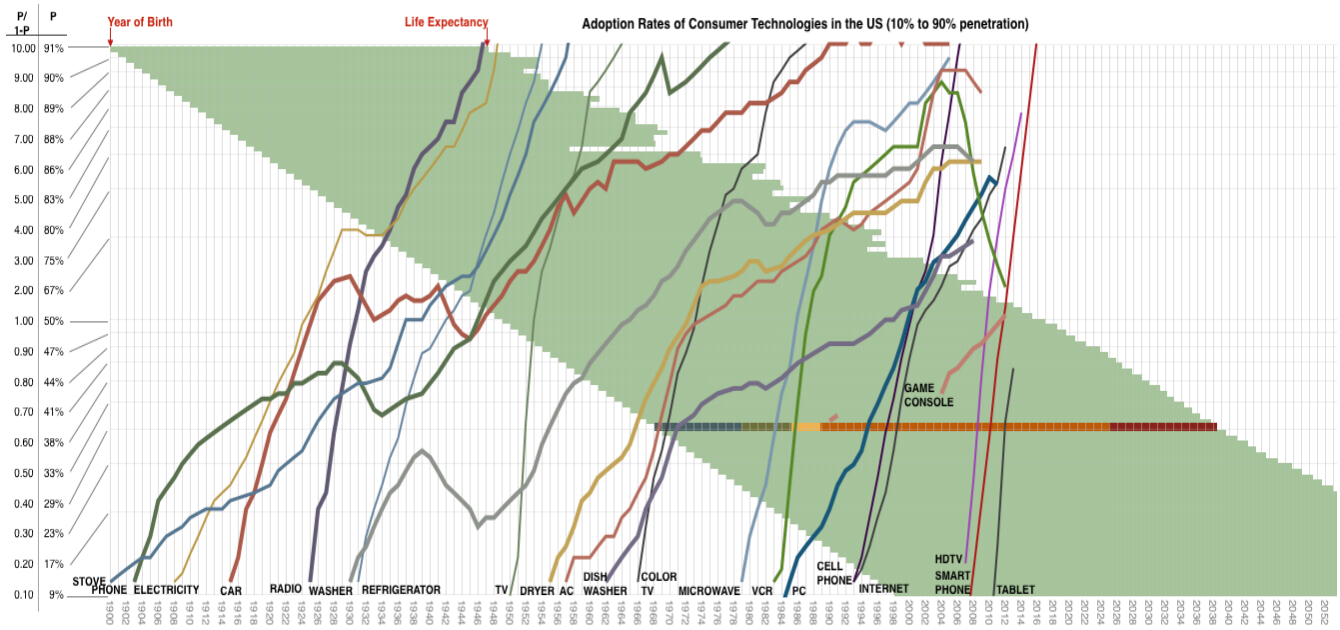
Bilindiği üzere bağış işlemleri dünya üzerinde ciddi rakamlara ulaşmış bulunmaktadır. Fakat bu yapının en önemli unsuru güven olduğundan kapalı şekilde çalışan bağış sisteminin daha şeffaf ve verimli olması gerekmektedir. Aracı kurumların varlığı ise bu bağışların aktarımı sırasında kesintilere sebep olmakta bu yüzden etkin bir şekilde tüm bağış ihtiyaç sahiplerine aktarılamamaktadır. Bu bağlamda blok zinciri alt yapısına sahip bir bağış sistemi hem daha şeffaf, güvenilir hem de daha az kesintilerle gerçekleşebilir. Oluşturulan dijital kimlikler sayesinde hangi kurumun kime ne kadar ve ne zaman bağış yaptığını görmek mümkün hale gelecek ve mevzuat gereği yapılan denetimler de daha etkili bir şekilde gerçekleştirilebilecektir. (Usta&Doğantekin;2017)

Bunlarla birlikte genel olarak aracılık işlemlerinin faaliyet gösterdiği çoğu alanda, örneğin sigortalama süreçleri, Sendikasyon kredileri, vekâleten oy kullanma işlemleri, tapu ve telif kayıt sistemleri ve kamusal diğer kayıt sistemleri, ihaleler, askeri emir komuta zinciri gibi mühim alanlarda bu teknoloji sayesinde merkezi bir yapı olmadan ya da aracıyı ortadan kaldırarak işlemleri daha güvenilir ve daha az maliyetle yapmak mümkün hale gelebilir. (Usta&Doğantekin;2017)

Kripto Paraların Değerlendirilmesi ve Geleceği

Kripto paraların fiyatını etkileyen başlıca faktörler arz ve talep unsurları olsa da talep unsurunu etkileyen farklı değişkenler de bulunmaktadır. Oldukça oynak fiyat hareketlerine sahip bu piyasada temel olarak arz ve talep, kullanım kolaylığı, altında yatan teknoloji ve getirdiği yenilikler, kullanım kolaylığı, eğer madencilik ile elde ediliyorsa harcadığı enerji miktarı ve diğer maliyetler, Bitcoin fiyatı, hukuki düzenlemeler, medyada yapılan haberler ve piyasa manipülasyonu, geleneksel sistemdeki problemler gibi değişkenlere bağlı fiyat belirlendiği söylenebilir. Talep unsuru fiyatın belirlenmesinde en önemli değişken olmaktadır. Birçok kripto paranın arz miktarı sınırlı olduğu içi talep arttıkça fiyatlar da doğrudan yükselmeye başlıyor lakin burada asıl önemli olan ise talep faktörünü etkileyen alt değişkenlerin farklılık göstermesi ve bunların birbiriyle olan ilişkileridir. Bu bağlamda ilk olarak, sunulan teknolojinin adaptasyon süreci ve araçların günlük ticari işlemlerde ne kadar kullanıldığı talep unsurunun belirlenmesinde önemli rol oynamaktadır. Eğer bu araçlar ticari işlemler için yakın zamanda kullanılmaya başlanırsa hem vatandaşlar hem de hükümetler tarafından benimsenmesi daha hızlı olacaktır. Bu noktada uyum süreci ön plana çıkmaktadır. Grafik 2 incelendiğinde ortaya çıkan yeni teknolojilerin ve sunduğu araçların benimsenmesi yaklaşık 10 ile 20 yıl arası bir süre zarfında mümkün olmaktadır.

Grafik 2: Teknolojilerin Benimsenme Süreleri



Kaynak: URL 6,2017

Hukuki zemin ve hükümetlerin yaklaşımı olarak değerlendirilebilir. Yakın zamanda farklı ülkelerin yaptığı açıklamalar günlük ya da haftalık olarak kripto para fiyatlarını etkilemiştir. Ülkelerin hukuki olarak bu varlıkları tanımlamaları vergi elde etmek amaçlı olabildiği gibi yenilikleri destekleme ve kendi teknolojilerini geliştirme amaçlı da olabilmektedir. Bu araçlara vergi koyma fikri her ne kadar ana fikir ile uyuşmasa da hukuki olarak kripto paraların tanınması veyahut tanınacağının bildirilmesi fiyat değişimleri üzerinde olumlu etkilere sebep olmuştur. Öte yandan belirli yasaklamaların getirileceği söylendiğinde ise fiyatlarda ani olumsuz değişmeler gözlemlenmiştir. Son olarak geleneksel sisteme olan güvenin kripto paraların fiyatları üzerinde etkisi olduğunu söyleyebiliriz. Eğer insanlar tasarruflarını ve yatırım tercihlerini geleneksel yöntemlerle yapmak isterlerse kripto paralara olan talep azalacak bu da fiyatlarında olumsuz değişmelere sebebiyet verecektir fakat insanlar tercihlerini bu alanda değerlendirmek isterlerse geleneksel sitemde oluşan olumsuz durumlara karşı tasarruflarını bu alana yönlendirecek ve talebin artmasını sağlayacaklardır. (URL 8,2017;URL 9,2017&URL 10,2017)

Blok Zincirinin Getirdiği Yenilikler

Blok Zinciri Teknolojisi (Blockchain)

Kripto para olarak adlandırılan Bitcoin ve alt yapısını oluşturan teknoloji sistemi blok zinciri teknolojisi sadece piyasada süregelen borsa işlemleri için değil aynı zamanda çok daha farklı alanlarda da yenilik olarak kabul edilmektedir. Bu konuda hem finansal sistem ve kuruluşlar açısından hem üretim firmaları açısından birçok yenilik bahis mevzu iken çok daha geniş çapta olan yenilikler merkezi olmayan internet ağları, akıllı kontratlar, blok zinciri tabanlı oylama ve kimlik verme, doğrulama sistemleri yenilikler olarak adlandırılabilir.

Ağ sistemleri alanında ortaya atılan ilk proje, Kim Dotcom tarafından sunulan merkezi olmayan küresel bir internet ağı sistemi kurma üzerinedir. Adı “MegaNet” olan bu proje Edward Snowden tarafından sunulan “NSA internet aracılığıyla herkesi izliyor” tezine karşı oluşturulmuş bir koruma alt yapısı sunmayı planlamıştır. Hiçbir kullanıcının IP adresi sahibi olmadığı sistem, Bitcoin için kullanılan dağıtılmış defterler ve blok zinciri teknolojisini

barındırarak daha hızlı erişilebilir ve hiçbir ağın, sunucunun hacklenmediği yapı olarak sunuluyor. Ancak hala proje aşamasında olan bu sistem için oldukça sağlam güvenlik altyapısı gerekiyor.

Farklı bir alan olarak sunulabilecek diğer bir yenilik ise yan zincirler ve akıllı kontratlar teknolojisidir. Yan zincir, ana blok zinciri kullanıcısı tarafından özel olarak belirlenmiş operasyonlara karar vermek için kullanılan, akıllı sözleşmeler aracılığıyla elden ele iletilen defterlerdir. Bu defter, aynı zamanda daha esnek bir yazılım platformundan yararlanırken, ana blok zincirin altında yatan doğrulama gücünü dolaylı olarak etkiler. Yan zincir yapısı, yeni kripto paralar üretmeden çoklu ağın kullanılmasına esneklik ve çeviklik kazandırır. Bu sayede bir ithalatçı yapacağı sözleşmeyi tamamen bu zeminde hazırlayıp riskli taşıma işlemlerinde kendini koruma altına alabilir. Örneğin, yurt dışından Türkiye'ye getirilmek istenen bir meyve türü olduğunu varsayalım ve 1 haftalık yolculuk sonrasında hedefine ulaşacak bu sipariş için uygun sıcaklık, depolama ve zaman şartları gerekebilir. Bu bağlamda belirli şartları olan bu operasyona ana blok zinciri sahibi kendi şartlarını sözleşme şeklinde işler ve karşı tarafın da kabulünü alıp olması gereken doğrulama sistemini açmış olur. Ürün yoldayken belirlenen şartlara uyulmayan bir durum ya da aksilik olması halinde akıllı sözleşmeler, yan zincirler aracılığıyla sisteme müdahale şartlarını yükler alacaklı tarafın riskini sözleşme gereği yerine getirir.

Bir başka yenilik ise dijital kimlik sağlayıcılardır. Çevrimiçi dijital kimlik sorunu, birbiriyle ilişkili iki sorunu, yani erişim kontrolü ve kişisel olarak tanımlanabilen bilgileri içermektedir. Blok zinciri teknolojisi, dijital çağda yeni ve potansiyel olarak devrimci, merkeziyetçi olmayan karakterini dijital kimlik haline getirmeye başlamıştır. Bu büyüyen dijital doğrulama alanındaki yenilikçi "OneName" adlı firma şirket binalarına giriş iznini blok zinciri ile kontrol eden geçiş kartı yapmıştır. Böylece güvene ve merkeziyetçiliğe dayalı olmayan dijital kimlik hizmeti sunmuştur.

Oy kullanma ve sayım yöntemleri uzun dönemdir insanlar tarafından tartışılan bir durum olmuştur. Bu konuda en güvenilir yolu sunmaya çalışan blok zinciri alt yapısı verilen oyların, hash fonksiyonları içeren bloklar içerisinde şifrelenmiş şekilde ağda bulunmasını sağlamaktadır. Böylece özel anahtarlar ile oy veren şahıslar takip edilememekte ya da belirlenmemekte iken genel oy miktarı ve durumu açık anahtarlar sayesinde tüm sistem kullanıcıları tarafından doğrulanabilmektedir.

Son olarak öngörülen yenilik ise "Ripple Labs" olarak adlandırılan deneysel yapıya sahip küresel dağıtık finansal varlık transferi sistemidir. Bu sayede dünya çapında eş anlı, eşten eşe sistemi kullanılarak şifrelenmiş şekilde tüm ödeme protokolleri sağlanabilmekte yani döviz, altın, kripto para vb. gibi tüm varlıklar daha hızlı, daha geniş, daha güvenilir ve çok daha az maliyetli olarak tüm finansal kuruluşlar arası transfer edilebilmektedir. Kullandığı alt yapı olarak kendi protokollerinde yeni bir Pazar oluşturduğu için blok zincirinden çok defterler zinciri olarak adlandırılmaktadır. Benzer bir gelişme ise son zamanlarda ortaya çıkan Bitcoin ve diğer altcoinlerin kullanıldığı borsa işlemleridir. En son CME, CBOE ve NASDAQ kendi piyasalarında vadeli işlemler için Bitcoin kullanacaklarını duyurmuş oldular. Bu haber ile birlikte Bitcoin'e karşı talep artış göstererek değerini 3'e katlamasını sağlamıştır. (Pilkington, 2015)

Blok Zinciri Teknolojisinin Finans Piyasasına Etkileri

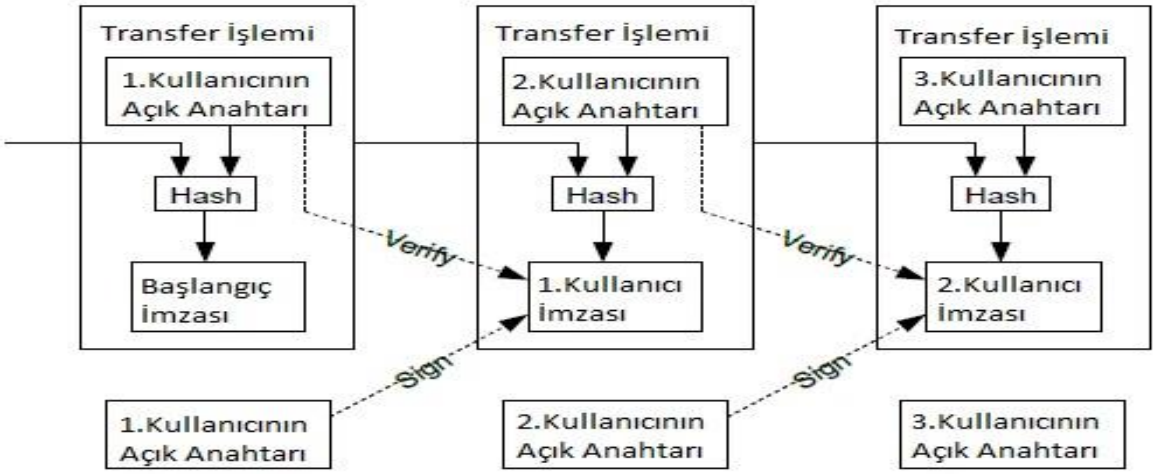
E-ticaret finansal kurumların güvenilir üçüncü parti olarak elektronik ödeme süreçlerinde hizmet vermesiyle sağlanmaktadır. Sistem yeteri derecede iyi işlese de hala güven temelli modelin içsel sıkıntılarını ortaya koymaktadır. Finansal kurumlar arabuluculuk görevi gördüğü için tek taraflı ticari işlemler mümkün olamamaktadır. Arabuluculuk faaliyetleri işlem maliyetlerini arttırdığı gibi, minimum ölçekli pratik işlemleri de sınırlar ve günlük ufak işlemlerin oluşma ihtimalini en aza indirir. Bu faaliyetin temel sebebi ise güven mekanizmasını

sağlamaktır. Elektronik ödemelerin ihtiyacı ise güven yerine şifrelenmiş kanıtlardır. Bu sayede karşılıklı iki taraf, üçüncü tarafa ihtiyaç duymadan direkt olarak ticari işlemlerini gerçekleştirebilirler.(Nakamoto,2008) Geri döndürülmeye elverişsiz olan bu ticari işlemler hem satıcıyı dolandırıcılıktan koruyabilir hem de emanet sistemiyle alıcıyı koruyabilir. Blok zinciri, ticari işlemleri kronolojik sırasıyla sayısal ispat olarak oluşturan bireyden bireye dağıtılmış zaman damgasını kullanarak çifte harcama sorununa çözüm sağlıyor. (Guo&Liang, 2016)

Ticari İşlemler

Elektronik parayı dijital imza zinciri olarak tanımlayabiliriz. Her para transferi önceki işlemin "hash" fonksiyonunu ve sonraki işlem sahibinin açık anahtarını dijital şekilde imzalar ve bunları paranın sonuna ekler. Alacaklı mülkiyetin zincirini doğrulamak için imzaları doğrulayabilir.

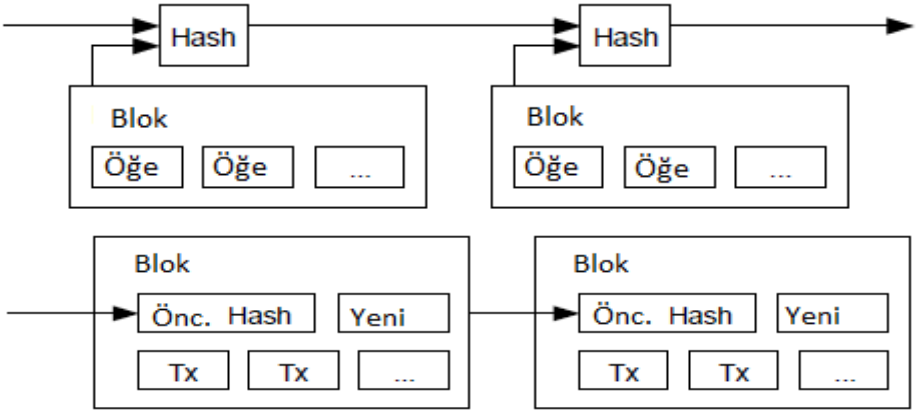
Şekil 2: Bitcoin Blok Zinciri Yapısı



(Nakamoto: 2008)

Dağıtılmış zaman damgası ağını eşten eşe sisteminde uygulayabilmek için gösterge(proof-of-work) olarak daha kapsamlı bir "hash" kullanılmalıdır, SHA-256 bit gibi.

Şekil 3: Blokların Oluşumu



(Nakamoto: 2008)

Blok zinciri ağ katılımcılarının(madenciler) oldukça zor matematiksel problemleri çözerek oluşturduğu ticari işlemin kayıtlarının zinciridir. Madenciler bu matematiksel problemleri en etkin şekilde çözmek için ağda rekabet ederler ve böylece blok zincirine bir sonraki bloğu eklerler. Her blok çözme işlemi ödül getirmektedir ki buna coin, en bilinen örneğiyle Bitcoin, diyoruz. Eğer madenci bu paraları harcamak isterse, açık anahtarla uyumlu olarak imzalamak zorundadır. Madencilik sistemi genişledikçe yeni blok madenciliği için gereken sayısal problemler zorlaşması gerekmektedir. Yaklaşık olarak 10 dakikada bir bu problemler zorlaşmaktadır. Madencilik işleminin başlarında bireysel olarak evdeki bilgisayarın işlemci gücüyle bunu yapmak kolayken zamanla daha karmaşık hale gelen bu algoritmaları çözmek için ASIC(özel bütünleşmiş çevrim uygulaması) gibi yeni madencilik teknikleri gerekti. Ardından yeni paralar çıkarmak için bu teknik milyonlarca internet cihazına bütünleştirerek BitShare adlı madencilik çipi oluşturuldu. Bu yeni kripto para akışı, mikro ödemelerin maliyet sorununu çözmekte ve fişlerin kendilerinin finanse edilmesine yardımcı olarak yeni bir kripto-iş modeli ön plana çıkarmaktadır.

Blok zincirinin asıl önemi parasal ya da ekonomik olmasından önce bilgisel olması ve gelişmekte olan ve artan birçok popüler ücretsiz jetona olanak sağlamasıdır. Bu durum yoğun bir şekilde “hash fonksiyonuna” bağlıdır. Hash fonksiyonu girdiği yeni bir çıktıya dönüştüren matematiksel algoritmadır.

Gösterge olarak kullanılan “iş/emek ispatı”(proof-of-work) fonksiyonu Bitcoin protokolündeki blokların en önemli kısmı olarak adlandırılabilir. Bu uzlaşma modeli adını kendi sürecinden almaktadır. Uzlaşma modelleri blok zinciri ağında mimarinin önemli bir parçasıdır. İş ispatı diye adlandırılan bu yöntem doğrulama işlemlerinde gerçekten bir iş ya da emek ortaya konularak yapılmaktadır. Burada bahsedilen durum madencilerin yaptığı Bitcoin çıkarma sürecidir. Bahsedildiği üzere bu süreçte madenci sistemin verdiği problemi çözmeli bunun için de ciddi miktarda enerji ve donanım gücüne ayrıca bilgi alt yapısına sahip olmalıdır. Bu işlem yeni blokların kabul görmesi için gereklidir. Bunun hesaplanması ve işlemlerin doğrulanması için Bitcoin şifrelenmiş hash fonksiyonuna bağlanmıştır ki bu fonksiyon “SHA-256 hashing” algoritma diye adlandırılır.

Diğer bir gösterge ise “hisse ispatı”(proof-of-stake) şuanda altcoin diye tabir edilen bitcoincash, litecoin gibi diğer kripto para birimleri için kullanılmaktadır. Literatürde hisse ispatının farklı avantajları olduğundan da bahsedilmektedir. Bu sistem yapısında herhangi bir madencilik süreci gerekmediğinden sadece işlemlerin büyüklüğüne, hissenin boyutuna bakılır. Bu sayede de gerekli olan enerji düzeyi makul seviyelere düşürülürken aynı zamanda gerekli olan donanım ihtiyacı da uygun seviyelere çekilebilmektedir. Bunlar daha hızlı blok zinciri kurma potansiyelinin olması, gereken protokollerin azlığı, saldırıların %51’ ine kadar

düşürülebileceği şeklinde bahsedilmektedir. Bu iki uzlaşma yönteminin dışında farklı uzlaşma yöntemleri de bulunmaktadır. Uzlaşma yöntemlerinin farklılık göstermesi blok zinciri ağlarının yapısı ve kullanım alanlarıyla ilgili olmaktadır. Burada uzlaşma yapılarının türüne göre ölçeklendirme, sonuçlandırma ve hız gibi mühim göstergelerde farklılık gösterebilir.

Bitcoin bakıldığında merkezi olmayan ilk kamuya açık defter-i kebir şeklinde tanımlanabilir ve 2013 yılında küresel anlamda statüsünü elde etmiştir. Ancak genel ilgi Bitcoin'in sahip olduğu özelliklerden ve ortaya çıkarabileceği yeniliklerden ziyade piyasadaki değerine odaklanmış durumdadır. Bu kripto para mantığının altında yatan asıl teknoloji altyapısı ise beklenen ilgiyi yeterince kazanamamıştır ya da Bitcoin kadar çok ilgi görmediği söylenebilir. Blok zinciri teknolojisi sadece ödeme sistemlerinde değil birçok alanda yenilik yapacak güce sahip bir sistem. Hâlihazırda farklı alanlarda uygulamalarını görmek de mümkün;

Yan Zincirler ve Akıllı Sözleşmeler

Bir yan zincir, ana bilgi bankası defterine "kilitlenmiş" kendi yazılım koduyla ayrı olarak yönetilen bir defter olarak işlev görür ve böylece anahtar bilgilerin bir zincirden diğerine aktarılmasına izin verir. Yan zincir, ana blok zinciri kullanıcısı tarafından özel olarak belirlenmiş operasyonlara karar vermek için kullanılan akıllı sözleşmeler aracılığıyla elden ele iletilir. Bu defter, aynı zamanda daha esnek bir yazılım platformundan yararlanırken, ana blok zincirin altında yatan doğrulama gücünü dolaylı olarak etkiler. Yan zincir yapısı yeni kripto paralar üretmeden çoklu ağın kullanılmasına esneklik ve çeviklik kazandırır. (Pilkington, 2015)

Blok Zinciri Temelli Dijital Kimlik Sağlayıcıları

Çevrimiçi dijital kimlik sorunu, birbiriyle ilişkili iki sorunu, yani erişim kontrolü ve kişisel olarak tanımlanabilen bilgileri içermektedir. Blok zinciri teknolojisi, dijital çağda yeni ve potansiyel olarak devrimci merkeziyetçi olmayan karakterini dijital kimlik haline getirmeye başlamıştır. Bu büyüyen dijital doğrulama alanındaki yenilikçi "OneName" adlı firma şirket binalarına giriş iznini blok zinciri ile kontrol eden geçiş kartı yapmıştır. Böylece güvene ve merkeziyetçiliğe dayalı olmayan dijital kimlik hizmeti sunmuştur. (Pilkington, 2015)

Blok Zinciri Temelli Oy Sistemi

2015 Şubat ayında "Bitcoin Foundation" tüm oyların blok zincirinde kaydedilmesini ve oylama sürecine daha fazla şeffaflık sağlayacağı blok zincir temelli oylama sistemi projesini ortaya çıkardı. Bu sayede "hash"lenmiş bilgiler bloklar içerisinde daha güvenli ve oyların gizlice verilebildiği, herkes tarafından kontrol edilebilir yapıda olması blok zincirinin içsel bir etkisi olarak düşünülebilirdi. İlk uygulamayı Danimarka partisi kendi iç seçimleri için kullanarak gerçekleştirdi. (Pilkington, 2015)

Ripple Labs

Kripto paralar anlamı itibariyle asıl önemini ödeme sistemleri bağlamında kazanabilmektedir bu noktada ilk olarak 2012 yılında ripple teknolojisi dünya genelinde kurulan bir ödeme protokolü, sistemi üretemeye katkı sağlamıştır. (Cawrey,2014) Günümüzde finansal kuruluşların ödeme araçlarının, altın, döviz, emtia vs. gibi varlıkların transferinde yeterince bütünleşebilmiş değilken ripple bunu tüm dünya genelinde tek bir protokol ile sağlamaya çalışıyor. Yapısı itibariyle açık protokol mantığı ile çalışan ve eşten eşe hareket mimarisine olanak sağlayan bu teknoloji finansal kuruluşların kendi ağlarına, bulunduğu bölgelere ve döviz cinsine bakmadan global olarak transfer işlemini gerçekleştirmesini sağlamaktadır. Bu sistem her defter kapanışında defterler arasında mutabakat da sağlayabilmektedir. Tam anlamıyla gerçek zamanlı brüt hesap kapatma sisteminden oluşmaktadır. Aynı zamanda oldukça hızlı ve güvenilir, çok cüzi miktarda maliyeti olan ve işlem miktarı açısından da sıkıntı yaratmayan bir sistemdir. Bu sayede token, kağıt para ya da kaydi para, kripto para, mülk gibi değer birimi

olan her şeyi transfer edebilmektedir. Ripple algoritması kendi protokolü içinde merkezi olmayan pazarını oluşturmaktadır bu nedenle blok zincirinden daha ziyade defter zincirine daha çok benzemektedir.

Banka/Finansal Kuruluşlar için Blok Zinciri Teknolojisi

Ödeme protokolleri dışında bu teknolojinin banka ve diğer finansal kuruluşlar için birçok avantajı söz konusudur. Bitcoin ve kripto paralar hakkında şüpheler artmış olsa da 21. Yüzyıl da bankacılık sektörünün ana faktörünün blok zinciri teknolojisi olduğu da çok fazla konuşulmaktadır. Bu belirsiz ve çalkantılı süreçten sonra bankalar bireylerin ve kurumların ihtiyaçlarına göre yeniden şekillenmek durumunda kalacaklar. Örneğin 24 Mart 2015'te NASDAQ, "Noble Markets" adlı start-up firması ile yeni bir anlaşma imzaladı. Ardından bu firmanın teknolojik altyapısını kullanarak kripto paralar için yeni piyasa oluşturmaya çalıştı. 11 Mayıs 2015'te ise açık varlık protokolü aracılığıyla kaldıraçlı blok zinciri teknolojisini kullanacağını duyurdu. (Pilkington, 2015) Bu bağlamda NASDAQ 2018 yılının ilk çeyreğinde Bitcoin vadeli işlemlerini başlatmak istiyor, hâlihazırda 2017 Aralık ayı itibariyle CME Grup ve CBOE ise bu yarışa katılmış durumdalar.

Blok Zinciri Yapısının Risk ve Avantajları

Görüldüğü üzere blok zinciri yapısı ve dağınık defter sistemi sayesinde merkezi olmayan ve aracıları ortadan kaldırabilecek bu teknoloji birçok yenilik sağlamaktadır. Bu gelişmeler yanında birçok avantajı barındırırken birçok dezavantajı da beraberinde getirmektedir.

Avantajları ya da sağladığı faydaları incelediğimizde en önemlisi aracı işlemleri ortadan kaldırması olacaktır. Buna ilaveten, kullanıcıların kendilerine ait ticari işlemler ve bilgiler üzerinde kontrol yetkisi tam olarak sağlanmaktadır. Yetkilendirilmiş bu kullanıcılar blok zinciri yapısı sayesinde daha şeffaf bir ortamda bilgi edinebilmektedir ve bunu yaparken veriler tehlike altına sokulmamaktadır. Barındırdığı veriler tam, kesin, anlık ve geniş çapta kullanılabilirdir. Tek bir merkezden idare edilmediği için kötücül amaçlı yazılımların tek seferde saldırısıyla zarar görme ihtimali yoktur. Ancak tüm makinelere aynı anda müdahale edilmelidir ki bu neredeyse imkânsızdır. Aracılık faaliyetlerinin ortadan kaldırılmasını sağlayan bu yapı güvenlik için açık anahtarlar sayesinde çoklu olarak kontrol edilip onaylanmaktadır böylece bilgi korunması daha adil ve kolay şekilde yapılabilmektedir. Tüm bu yapı maliyetlerin azalmasını da sağlamaktadır.

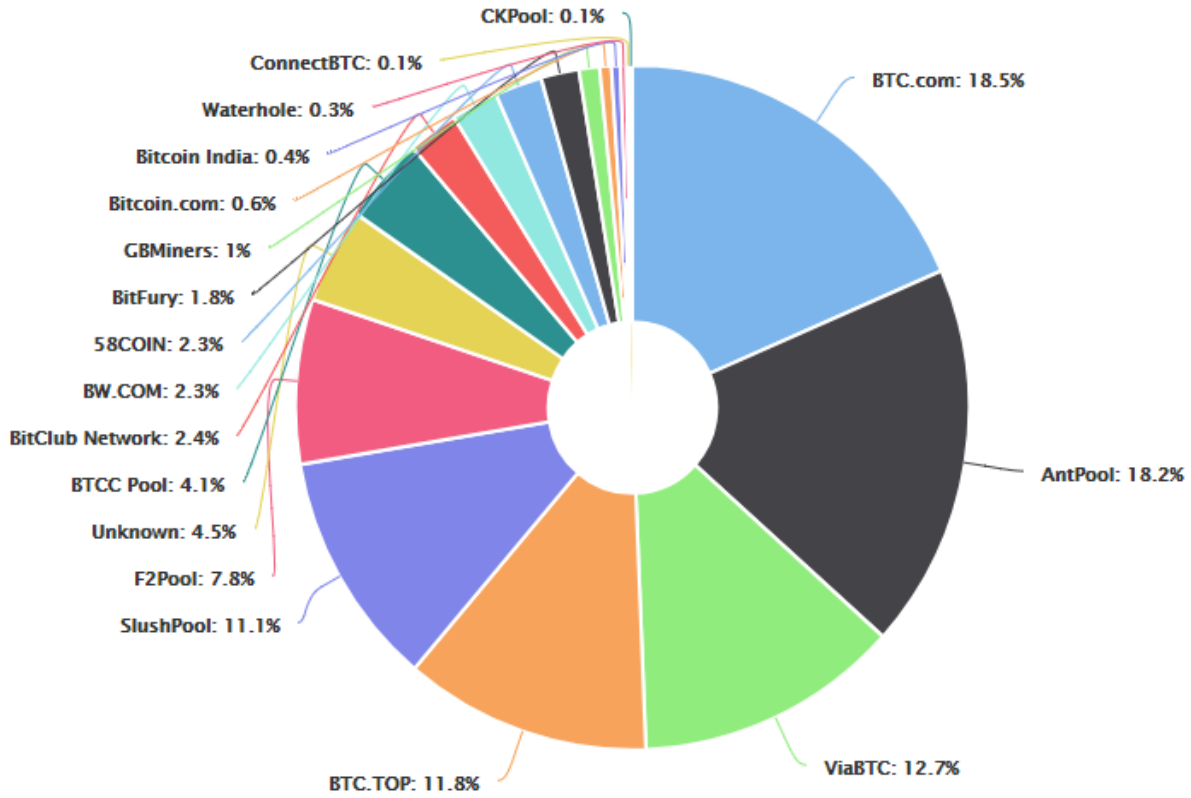
Dezavantajları göz önüne alındığında ise performans bağlamında merkezi sistemlere nazaran yetersiz kaldığı söylenebilir. Eşten eşe yapılan işlemlerin kontrolü için imzaların ve işlemlerin doğrulanması hesaplama olarak oldukça karmaşık ve her seferinde yapılması gerekmektedir. Bir güvenlik unsuru olan bu durum merkezi sistemlerde her işlem için gerekmemekte olduğu için daha hızlı olmalarını sağlamaktadır. Gelişen teknoloji olmasıyla işlem hızı, doğrulama süreci ve veri limitleri blok zincirinin karşılaştığı diğer zorluklar olarak söylenebilir.(URL 14,2016) Sürekli işleyen bu sistem veri kaydetmeye devam etmekte böylece çok daha fazla yer kaplamaktadır. Bu verilerin saklanması bir yana indirilmesi ve işlenmesi gerektiğinde ise zaman kayıpları ortaya çıkmakta, doğrulama işlemleri birkaç saati ya da günü alabilmektedir. Harcanan zamanı arttıran bir diğer etken ise içsel bir problem olan güvenlik aşamalarıdır.

Bir diğer risk unsuru ise bitcoin ile yapılan ödemeler geri alınamaz şekilde yapılmaktadır. Günümüzde bir kredi kartı vb. ödeme araçlarıyla yapılan işlemler yanlışlık olması durumunda geri ödeme, düzeltme gibi yolları ile telafi edilebilirken bitcoin için bu mümkün değildir. Kullanıcının insan olduğunu varsaydığımızda sürekli olarak bu risk göz önünde olacaktır. Böyle bir süreçte bitcoin kabul eden dolandırıcı internet siteleri çoğalacak ve başvurulabilecek hukuki bir alan olmadığı için geri dönüşler alınamayacaktır.(URL 17,2017)

Bu kripto paranın ya da ödeme aracının sahip olduğu en önemli dezavantajlardan biri ise çok dalgalı ve spekülatif hareketlere açık olmasıdır. Bu yüzden tüketim amaçlı kullanımı neredeyse imkânsız hale gelmektedir. Düşünüldüğünde tüketim aracı olarak kullanılacak paranın en önemli unsuru fiyat istikrarı iken bitcoin için anlık ve ciddi miktarlarda fiyat oynaklığı yaşanmaktadır. Günlük alışverişlerde kullanacağımız aracın sürekli fiyat değişikliğine uğradığı bir alanda onu kullanmak çok kullanışsız olurdu. Bu yüzden belli bir fiyat dengesine ulaşamadan kripto paraların tüketim amacıyla kullanılması mümkün olamamaktadır.

Blok zinciri yapısı her ne kadar kendi içerisinde şeffaflık ve güven unsurlarını sağlasa da bitcoin ve benzeri kripto paraların çalınması hala daha mümkün. Bu dijital paraların saklandığı dijital cüzdanlar bireylere özel zorlu şifrelerle korunmakta ancak bu cüzdan yapısı dağıtılmış defter sistemi gibi çalışmadığı için sadece kişiye özel anahtarlar ile kullanılmaktadır yani her ne kadar yapılan işlemler sistem içerisinde herkes tarafında doğrulansa da cüzdan içindeki saklama fonksiyonu şahısların bilgisi dâhilindedir. Bu durum cüzdanların internet üzerinden çalınmasına yol açabilmektedir diğer bir deyiş ile tam anlamıyla güvenlik sağlanamamaktadır. Yakın zamanda gerçekleşen vaka bize durumun ne kadar büyük derecede tehlikeli olduğunu gösteriyor. The Guardian gazetesinin yaptığı habere göre dünyanın en bilinen bitcoin ticaret firmalarından biri olan “NiceHash” aralık ayında sistemlerinden 4.700 adet bitcoin’ in çalındığını bildirdi ve yapılan saldırının sosyal mühendislik içeren profesyonellikte olduğu aktarıldı. Çalınan paranın o günkü değeri itibariyle 64 milyon Amerikan doları civarında olması yaşanan değer kaybını bir kez daha ortaya koymaktadır.(URL 18,2017)

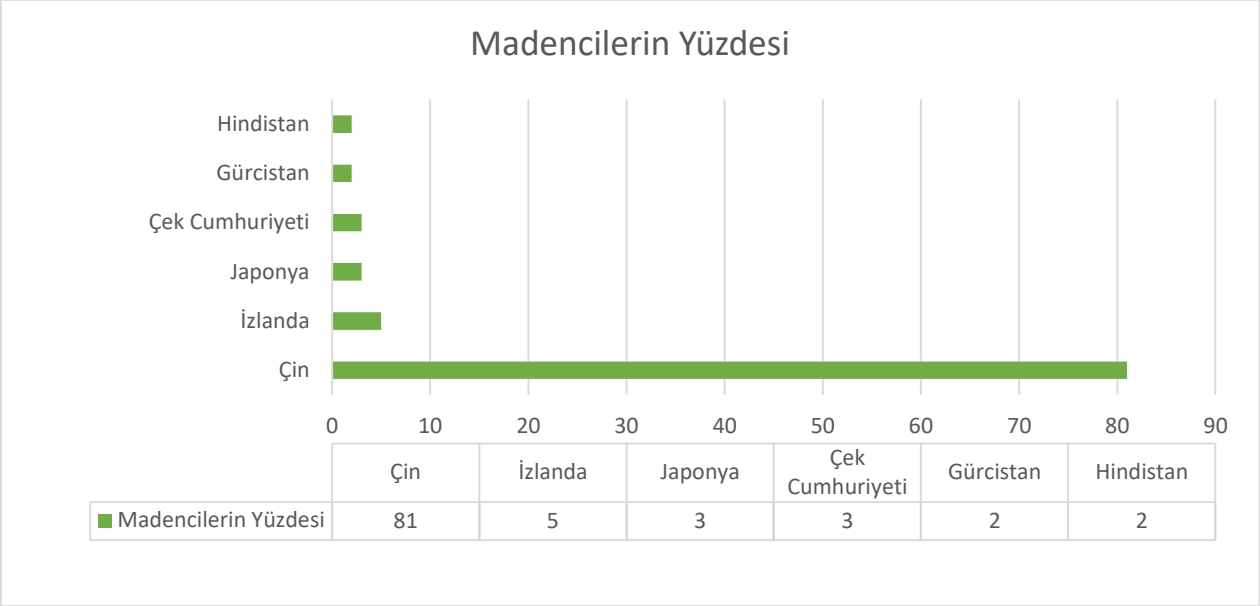
Grafik 4: BTC Madencilerinin Sistemde Sahip Olduğu Ağırlıklar



Kaynak: URL 19, 2016

Üstteki daire grafiği Dünya’nın en büyük bitcoin madencilerini göstermektedir. Buradan da anlaşılacağı üzere en büyük 4 madenci, sistemin sahip olduğu işlem gücünün %50’ sinden fazladır. Burada bu 4 büyük madencinin ise tek ülkede olması tehlikenin boyutunu gözler önüne sermektedir. Grafik 5 bize bu madencilerin ülke temelli dağılımını vermektedir.

Grafik 5: Ülkelere Göre BTC Madencilerinin Yüzdesi



	Çin	İzlanda	Japonya	Çek Cumhuriyeti	Gürcistan	Hindistan
Madencilerin Yüzdesi	81	5	3	3	2	2

Kaynak: URL 20,2017&URL 21, 2017

Bu bağlamda güvenlik sorunlarının yaşanıyor olması hukuki alt yapının önemini daha çok ön plana çıkarmaktadır. Hem kripto paraları hem blok zinciri alt yapısını kullanan sistemlerin hukuki zemine sahip olmaması insanların işlem ve uygulamalara daha az ilgi duymasını sağlamaktadır. Devletlerin bu konuda çalışmaları olsa da hukuki alt yapının bölgesel, ulusal ya da geleneksel bağlamın dışında uluslararası kapsamda sağlanması daha önemlidir. Çünkü sunulan hizmet küresel çapta işlem faaliyetleri sunmakta ve bunun için küresel ağı kullanmaktadır. Öte yandan devlet tarafından kontrole alınacak olması sistemin içsel ideolojisi olan adem-i merkeziyetçilik ve özgürlük unsurlarıyla çelişebilmektedir. Yapılacak çalışmaların buna uygun seviyede olması ilk basamak olacağı söylenebilir. Bununla birlikte kripto paralar için Türkiye ve diğer ülkelerin vergilendirme stratejileri, sermaye piyasalarına entegre etmek istemeleri de hukuki alt yapının gerekliliğini ortaya koymaktadır. Örneğin; bitcoin ve benzeri kripto paraların vergilendirilmesi için menkul kıymet, para ya da farklı bir isim verilmesi Türkiye mali yasal çerçevesi için şart olduğundan tanım verilmesi gerekmektedir. Burada bazı sorunlar ortaya çıkmakta, bu varlıkların altında dayanak varlık olmadığından Sermaye Piyasası mevzuatı açısından menkul kıymet sayılamamakta aynı zamanda, devlet destekli bir araç olmadığı için TCMB tarafından para olarak adlandırılamamaktadır.(URL 22,2017)

Konu üzerinde düşünüldüğünde kripto paraların oluşturulduğu bir dayanak varlık olmadığı ve bir göstergeye(finansal tablo veyahut faaliyet raporu vb. gibi) bağlı değerlenmediği söylenebilir fakat açıklamaya çalıştığımız gibi bu araçlar ne tam olarak bir para ne de tam olarak bir yatırım aracı olarak görülmemelidir. Bu araçların sağladığı en büyük avantaj bir yenilik ortaya koymaları ve sistemsel olarak değişiklik getirmeleridir. Bu yüzden altında yatan bir dayanak varlık olmasa bile bu araçları bir fikir, bir yenilik olarak görmek hatta yakın zamanda başlayacak olan somut adımlarla birlikte bir hizmet ürünü olarak varsaymak daha doğru olacaktır. Ripple veyahut IOTA gibi güçlü altyapısı olan ve belirli sektörler için çığır açabilecek bu araçlar bir hizmet olarak adlandırılabilir ve bu ölçüde mevzuat bağlamında daha kolay zemine oturtulabilir. Öte yandan blok zinciri sisteminin ve oluşturduğu araçların ortaya çıkış amacı bir merkezi sisteme bağlı kalmadan ve doğrudan şahsi bilgileri sunmadan aracılık gibi hizmetleri ve maliyetleri ortadan kaldırmak olduğu için “Bitcoin” ya da diğer altcoinleri vergilendirmeye tabi tutmak sistemin temel anlayışına ters düşecektir. Vergilendirme sürecinin başlamasıyla yatırımcılar oluşacak bu yeni masraftan kaçacak ve daha düşük maliyetli işlemlere ya da

araçlara yönelecektir. Bu yüzden bu araçların piyasa üzerinde gerçek bir değer edinebilmesi mümkün olmayacaktır. Aslında devletlerin bu bağlamda vergilendirme süreci bir noktada direk ortadan kaldıramadığı bir yeniliği dolaylı olarak sistemde kaybetme çabasının bir yolu olarak görülebilir. Halbuki ülkeler kripto paraların sağladığı yenilikleri kullanarak çok kısa zamanda rekabetçi bir ortam olan finans sektöründe kendi büyümesini katlayabilir ve bu alanda öncü olabilir. Türkiye'nin sahip olduğu bankacılık sisteminin gelişmiş olduğu göz önüne alındığında aslında bu bulunmaz bir fırsat olarak değerlendirilebilir. (Kayacan&Tüzünalper,2003) Buna ilaveten sadece bankacılık sektöründe değil aynı zamanda borsadaki faaliyetler çerçevesinde de bu teknolojileri kullanarak daha fazla yatırımcıyı kendine çekebilir. Blok zinciri teknolojisinin sağlamış olduğu diğer yenilikler sayesinde ise bürokratik olarak ciddi zaman harcayan işlemler daha hızlı ve güvenilir bir şekilde yürütülebilir. Yasakçı anlayıştan ziyade daha çok bu gelişmeyi sahiplenebilen ve geliştirebilen bir Türkiye kazanamadığı rekabet üstünlüğünü bu alanda elde edebilme şansına sahip olabilecektir.

"Mikro elektroniğin ve genetik mühendisliğinin dünyasında, bilim ve teknolojinin iktisadi açıdan önemini anlatmaya çalışmak gerçekten gereksizdir. Teknolojiyi, ister sosyolog Marcuse ya da romancı Simone de Beauvoir gibi, insanoğlunun esaretinin ve yıkılışının aracı, istersek Adam Smith ya da Marx gibi öncelikle özgürlüğü sağlayacak bir güç olarak görelim, hepimiz onun gelişimi ile yakından ilgiliyiz. Ne kadar istersek isteyelim, onun günlük hayatımız üzerindeki etkisinden, önümüze çıkardığı ahlaki, toplumsal ve ekonomik ikilemlerden kaçamayız. Onu lanetleyebilir, ya da yüceltebiliriz ama yok sayamayız."
(Freeman,1974;15)