MERKEZİYETSİZ TOPLUM

Blok Zinciri Teknolojisi ve Merkeziyetsiz Örgütlenme Biçimleri

Halit GÜRLEYİK - Sinan YILMAZ

Karabük Üniversitesi Yayınları
2025

MERKEZİYETSİZ TOPLUM

Blokzinciri Teknolojisi ve Merkeziyetsiz Örgütlenme Biçimleri

Yazarlar

Halit Gürleyik - Prof. Dr. Sinan Yılmaz

Editör

Doç. Dr. Selman Yılmaz

Dizgi ve tasarım

Halit Gürleyik

ISBN: 978-625-93475-7-8

Karabük Üniversitesi Yayınları - 149

İÇİNDEKİLER

Giriş

90'lı yıllarda ortaya çıkan internet ve bu dönemde hızla gelişen bilgisayar teknolojileri, beraberinde yeni tür iletişim, iş yapma biçimleri ve toplumsal organizasyon becerileri getirdiği gibi, özellikle insanların birbirleriyle hızlı ve kolay iletişime geçebilme imkânları bulmaları nedeniyle mesafeleri ortadan kaldırmış ve her alanda yeni fırsatların ortaya çıkmasını sağlamıştır.

Teknoloji, uzak mesafelerdeki insanların birbirleriyle etkileşime girmelerini kolaylaştırırken yeni güvenlik sorunlarını da beraberinde getirmiştir. Aslında insanlar arasındaki güven sorunu sadece bu zamanın sorunu olmayıp çok daha eski zamanlardan beri var olan bir sorundur. "İnsanların birbirlerinden emin olarak iletişime geçebilmeleri veya birlikte iş yapıp, birlikte yaşayabilmelerini sağlayan şey nedir?" sorusu Toplumsal Sözleşme teorisyenlerinin de uzun süredir cevabını aradığı soruların başında gelmektedir.

Toplum sözleşmecileri, insanların bazı doğal özgürlüklerini devlet otoritesine devrederek bir tür toplumsal düzen kurmaya çalıştıklarını söylemektedir. Bu araştırmada, toplum sözleşmecilerinin "insanların birbirlerine güvenebilmek ve beraber yaşayabilmek adına devlete devrettikleri bazı özgürlüklerini, gelişen yeni teknolojiler

sayesinde yeniden kendi ellerine alabilme imkânları var mıdır?" ve "bu teknolojiler farklı türde toplumsal organizasyonlar kurmamıza yardımcı olabilir mi?" Vb. sorularına cevap aranmaya çalışılmıştır.

Bitcoin, 2009 yılında ilk defa çalışmaya başladığında, sadece bir grup geliştirici tarafından bilinen deneysel bir çalışmaydı. Üreticisi olan Satoshi Nakamoto'nun ortaya koyduğu vizyon ve bunu gerçekleştirmedeki başarısı sayesinde kısa sürede geniş kitleler tarafından bilinir hale gelen Bitcoin, özellikle değerindeki hızlı artış sayesinde bu bilinirliliğini de hızlı bir şekilde artırmıştır. Ancak Bitcoin'i asıl değerli kılan şey, ilk defa onunla birlikte anılmaya başlayan Blokzinciri Teknolojisi kavramı olmuştur.

Alternatif deneysel bir para birimi olarak çalışmaya başlayan Bitcoin, aslında Blokzinciri teknolojisinin nasıl bir potansiyel sunduğu ile ilgili olarak geliştiricilere ilham vermiştir. Özellikle Blokzinciri üzerinde akıllı sözleşmelerin de çalışmasıyla birlikte, kripto para çalışmaları bambaşka bir mecraya doğru yönelmeye başlamıştır.

Kripto para sektörü geniş kitleler tarafından alternatif bir kazanç kapısı olarak görülse de Blokzinciri teknolojisinin sunduğu teknolojinin merkeziyetsiz organisasyon ve toplum yapılarının önünü açmış olması onu bir gelir kapısı olmaktan çok daha öte bir konuma taşımaktadır. Dolayısıyla bu teknolojinin sahip olduğu potansiyelin günümüz ve gelecekte toplumlar üzerinde ne gibi değişimlere yol açma potansiyeli taşıdığı da araştırılmaya muhtaç olduğundan bu çalışmanın ortaya çıkmasına vesile olmuştur.

Toplumun farklı katmanlarında işlev gören bazı organizasyonlara ve geleneksel merkezi yönetim biçimlerine alternatif olarak, bu organizasyonların merkeziyetsiz bir şekilde çalışabilmelerine imkân tanıyan Blokzinciri teknolojisi, yeni bir toplumsal yapı modeli oluşturması nedeniyle Teknolojinin Sosyolojisi bağlamında bu çalışmada ele alınmıştır. Konunun Örgüt sosyolojisi ve Sosyal ağlar ile de yakın bir ilişkisi bulunmaktadır.

Aslında daha eski olmakla birlikte, özellikle 2008 yılında manifestosu yayınlanan ve 2009 yılında çalışmaya başlayan Bitcoin ile birlikte dünyada ismi yaygın bir şekilde duyulmaya başlayan Blokzinciri teknolojisinin bilinen üç temel ayağı vardır. Matematik – kriptografi, bilgisayar bilimleri ve finans.

Bu teknolojinin toplumsal etkileri göz önüne alındığında sosyolojinin de dördüncü bir ayak olarak tanımlamaya dâhil edilmesi son derece faydalı olacaktır.

Blokzinciri teknolojisinin sadece bir iki alanı, dolayısıyla sadece bu alanlarla ilgilenen bir grup insanı kapsadığı söylenemez. Barındırdığı potansiyel sayesinde ve günümüzde geldiği noktayı dikkate alarak değerlendirdiğimizde, çok daha geniş toplum kitlelerini ilgilendirdiğini söyleyebiliriz. Bu çalışmanın amacı, bu teknolojinin toplum üzerinde genel olarak ne gibi etkilerinin olabileceğini incelemektir.

Özelde Bitcoin, genelde kripto para olarak isimlendirilen bu ekosistemin ve bunların temelinde bulunan Blokzinciri teknolojisinin sadece bir değer transfer aracı olmayıp, aynı zamanda bazı toplumsal

organizasyon (örgütlenme) biçimlerini de değiştirebilecek bir potansiyele sahip olduğuna dikkat edilmelidir.

Bitcoin ile adı duyulan, sonrasında gelen Akıllı Sözleşmeler ile kullanım alanı genişleyen Blokzinciri teknolojisinin bu gün itibariyle çok fazla kullanım alanı vardır. Henüz çok yeni olması ve kullanım alanlarının birçoğunun deneysel aşamada olmasına rağmen bu teknolojinin on beş yıl gibi bir sürede dünya çapında ciddi bir şekilde rağbet gören ürünlere dönüşmesi, birçok akademik disiplin tarafından da incelenmesine neden olmuştur.

Başta bilgisayar bilimleri, finans ve kriptografi alanlarında olmak üzere daha birçok alanda Blokzinciri teknolojileri üzerine çalışmalar yapılmıştır. Ancak yeni bir konu olması nedeniyle konuyu toplumsal bağlamda ele alan sosyolojik çalışmaların sayısı oldukça kısıtlıdır.

Bu araştırmada, teknolojinin yeni sunduğu imkânlardan da faydalanarak Toplumsal Sözleşme teorisini yeniden ele almayı, Blokzinciri teknolojisinin toplumsal organizasyon (örgütlenme) biçimlerini ne şekilde etkileyebileceği tartışılmaktadır.

Çalışmada öncelikle Blokzinciri teknolojisinin temelleri üzerinde durulmuştur. Devam eden bölümlerde de, bu teknolojinin hali hazırda kullanım alanları incelenmiş, devamında ise bu hizmet alanlarının ne gibi toplumsal yansımaları olduğu incelenmiştir.

Blokzinciri teknolojisinin temelleri ve uygulama alanlarının toplumsal yansımalarının incelendiği bölümlerde doküman taraması yöntemi kullanılmıştır. Bu bölümlerde kaynak olarak kitap, süreli yayınlar, bu alanlarda yazılmış tezler ve internette yayınlanmış yazılardan faydalanılmıştır.

Blokzinciri teknolojisinin kullanım alanlarıyla ilgili yapılan araştırmada ise genellikle bu alanda sunulan hizmet ve ürünlerin bizzat kullanılmasıyla elde edilen deneyimlerden ve internette yayınlanan kullanıcı deneyimlerinden istifade edilmiştir.

Araştırmada aşağıdaki hipotezler tartışılmıştır:

1. Blokzinciri teknolojisi ve bu teknoloji üzerine üretilen tüm ürün ve hizmetler geniş toplumsal kesimleri etkilemektedir.
2. Bu etkilenme sadece bir veya birkaç yönde olmayıp, çok yönlü bir etki üretmektedir.
3. Blokzinciri teknolojileri, Toplumsal Sözleşme gereği bireyin kurum ve kuruluşlara devrettiği bazı özgürlükleri bireye geri verilebilme potansiyeline sahiptir.
4. Blokzinciri teknolojileri yeni tür toplumsal örgütlenme ve iş yapma biçimleri sunmaktadır.

Blokzinciri teknolojisinin toplumsal yapıyı nasıl etkilediğini doğru bir şekilde anlayabilmek için öncelikle bu teknolojinin yapısı ve toplumsal organizasyonlar üzerinde ne gibi etkilerinin olabileceği tartışılacaktır. Yapılan literatür taramalarında bu teknolojinin doğru bir şekilde tanımlanmasında eksiklerin olduğu dikkat çekmektedir. Multidisipliner bir alan olması nedeniyle bu teknolojinin doğru bir şekilde tanımlanıp anlatılması da araştırmanın güçlükleri arasındadır.

Yukarıda da ifade edildiği üzere Blokzinciri teknolojisi, kriptoloji, bilgisayar bilimleri ve finans alanlarının kapsamında değerlendirilmektedir. Bu alanlardan sadece biri veya ikisi ele alınarak yapılan tanımlamaların eksik kalacağı literatür taramalarından anlaşılmaktadır. Bu sebeple, Blokzinciri teknolojisinin toplumsal etkilerini incelemeye geçmeden önce henüz yeni sayılan bu teknolojinin tüm ilgi alanlarını da kapsayacak bir şekilde tanımlanması son derece mühimdir.

Doğru şekilde tanımlanamayan, kapsam alanı, yeterlilikleri, eksik veya üstün yönleri doğru tespit edilmemiş bir sistemin analizinin de sorunlu olacağı bir gerçektir. Özellikle bilgisayar bilimleri alanında oldukça geniş bir teknik literatüre sahip olması, bilgisayar bilimleri ile doğrudan ilişkisi bulunmayan kişiler tarafından Blokzinciri kavramının anlaşılmasını zorlaştırmaktadır.

Çalışmanın ilk bölümünde Blokzinciri'nin temelleri, temel kavramları, nasıl çalıştığı ve hali hazırdaki kullanım alanları, çok fazla teknik detaya girmeden incelenmiştir. Ayrıca bu bölümde

Blokzinciri'nin kullanım alanları incelenirken aynı zamanda bu alanlarda ne tür toplumsal organizasyonlara imkânlar tanıdığını da ifade edilmiştir. Son olarak bu teknolojinin toplumsal sözleşme ve para kavramları üzerinden ele alınarak değerlendirmesi yapılmıştır.

1. Blokzinciri Teknolojisinin Ortaya Çıkışı ve Toplumsal Dönüşüm Üzerine Etkileri

Her canlının temel ihtiyaçlarını karşılayabilmek için farklı yetenekleri veya bedensel özellikleri vardır. Tüm canlılar bu özelliklerini veya becerilerini kullanarak hayatta kalmak, beslenmek ve türünü devam ettirebilmek için mücadele verirler.

İnsanoğlunun da bu mücadelede var olabilmesini sağlayan temel yeterliliği, düşünce gücünü el becerisiyle birleştirip alet, araç-gereç üretebilme yeteneğidir. İnsan, çevresini yani bulunduğu ortamı değiştirebilme, yeniden düzenleyebilme, doğal ortamı dönüştürebilme yeteneğine sahiptir.

Bu sayede insan eski çağlardan itibaren avlanabilmek için aletler geliştirmiş, yırtıcı hayvanlardan ve doğa şartlarından korunabilmek için barınaklar inşa etmiş ve daha sonraları toprağı işleyip ondan ürünler çıkarabilmek için tarım aletleri üretmiş ve kullanmıştır. Böylece teknoloji adı verilen belli amaçlara ulaşmada gözleme dayalı kanıtlanmış bilgi birikimi oluşmuştur.

Türk Dil Kurumu'nun web sitesinde teknoloji şu şekilde tanımlanır:

"İnsanın maddi çevresini denetlemek ve değiştirmek amacıyla geliştirdiği araç gereçlerle bunlara ilişkin bilgilerin tümü."[1]

[1] https://sozluk.gov.tr/ erişim tarihi: 05.11.2022

Sanayi devrimi ise insanoğlunun bir üst aşamaya geçerek, kendi yapabildiği işleri makinelere yaptırdığı dönemin başlangıcıdır. Daha öncesinde insan yaptığı işi kolaylaştırmak için alet kullanırken, bu dönemle birlikte işlerini artık makinelere yaptırmaya başlamıştır. Bu sayede insan, gücünün yetmeyeceği işleri makinelere yaptırmaya başlamış ve makinelere de insan yerine iş yapma becerisi kazandırmıştır.

İnsan yerine çalışan makineler, zamanla insanın yapamayacağı işleri yapmakta kullanılmaya başlanmıştır. Ayrıca makineler için yorulma, sıkılma, uykusu gelme, hastalanma veya acıkma gibi insani zaafiyetlerin bulunmaması da onlar için bir avantaj teşkil etmiştir. Doğru şekilde tasarlanmış, ayarlanmış ve bakımları yapılmış makineler sürekli çalışarak daha fazla üretim yapabilme kapasitesine sahiptir. Bu nedenle, üretimin birçok yerinde makine kullanmak insan çalıştırmaktan daha verimli olmuştur.

İnsan, hayatını kolaylaştırmak için zamanla bazı teknikler geliştirmiş, o teknikleri kullanmış ve eğer işe yarıyorsa teknikleri geliştirmenin yollarını aramıştır. Bu sürecin işlemesi sonucu zaman içerisinde buhar gücünün yerini petrol, elektrik veya nükleer gibi farklı enerji kaynakları almıştır. Yeni enerji kaynakları daha verimli ve daha küçük makinelerin de üretilebilmesinin yolunu açmıştır. Üretimde ve günlük hayatta makinelerin kullanılması, zamanla tüm dünyaya yayılmış ve küresel çapta geri dönülemez toplumsal dönüşümlere yol açmıştır.

Nasıl ki tarım teknolojileri ile birlikte yerleşik hayata geçen insanlar zamanla devletler ve imparatorluklar kurduysa, benzer şekilde sanayi toplumları da kendi toplumsal organizasyonlarını ihtiyaçlarına göre yeniden yapılandırmıştır. Sanayi toplumu imparatorlukların veya krallıkların değil, ideolojilerin, ulus devletlerin, diktatörlüklerin, demokrasilerin ve cumhuriyetlerin dönemi olmuştur.

Yerleşik hayata geçtikten sonra toplumsal yapı ve organizasyon (örgütlenme) biçimleri de değişmiştir. Dağınık küçük kabileler halinde yaşayan insan topluluklarından büyük imparatorluklara giden süreçte şüphesiz tarım teknolojilerinin katkısı yadsınamaz. Tarımsal üretimdeki artış sayesinde insan nesli de çoğalmıştır. Yaşam süresi uzamış ve yarın ne yiyeceğinin derdinde olmayan insanlar farklı işlere yoğunlaşarak değişik zanaatlarda uzmanlaşmıştır (UYANIK & BERK, 2016).

Benzer bir toplumsal değişim de Sanayi Devrimi'nden sonra Avrupa'da olmuştur. Üretimde insan ve hayvan gücü yerine makinelerin kullanılmasıyla birlikte, bu değişimi ilk yaşayan Avrupalı toplumlarda toplumsal yapı ve organizasyon (örgütlenme) biçimleri de zamanla değişmiştir (GÜZEL, 2005).

İmparatorlukların ulus devletlere, seçkinlerin ve soyluların iş adamlarına, kölelerin işçilere, servetin sermayeye dönüştüğü bu sürecin en büyük tetikleyicisi şüphesiz üretim teknolojilerindeki gelişmeler olmuştur (KARA, 2017).

Teknolojik gelişmeler toplumsal değişimlerin en önemli tetikleyicilerinden birisidir. Tarım teknolojilerindeki gelişmeler

imparatorluklar çağını açarken, makinelerin yükselişiyle başlayan sanayi çağında ise ulus devletler, sivil toplum ve demokrasi gibi kavramlar yeni toplumsal düzeni tanımlamaya başlamıştır.

Teknolojik gelişmeler öncelikle iş yapma biçimlerimizi, değişen iş yapma biçimlerimiz ise ekonomik organizasyonlarımızı değiştirmiştir. Değişen ekonomik yapı, yaşama biçimlerimizi, değişen yaşam biçimlerimiz ise düşünce kalıplarımızı değiştirmiştir. Tarım toplumundaki değişen düşünce kalıpları ise yeni meslek gruplarını ve devlet yapılanmalarını ortaya çıkarmıştır. Sanayi toplumunda yaşayan bireyin değişen düşünce biçimi de demokrasi, insan hakları, kapitalizm, sosyalizm, cumhuriyet gibi kavramları ortaya çıkarmıştır.

Günümüzdeyse bilgisayar teknolojilerindeki gelişmelerin sağladığı imkânlar, toplumsal yapılarımızı ve organizasyon (örgütlenme) biçimlerimizi yeniden gözden geçirip köklü değişiklikler yapmamızın önünü açmıştır.

Bu bakış açısıyla dikkate alındığında, Blokzinciri teknolojisinin yeni tür merkeziyetsiz organizasyon (örgütlenme) biçimleri oluşturma imkânının ve potansiyelinin var olduğu açıkça ortadadır. Ayrıca devletlere veya kimi kurum ve kuruluşlara devretmiş olduğumuz ve Hobbes, Locke, Rousseau gibi düşünürlerin Toplumsal Sözleşme vb. kavramlarla ifade ettikleri bazı özgürlüklerimizi geri alabilmemiz mümkün olacaktır (Fabre, 2018). Merkeziyetsiz çalışabilen ve bunu herhangi bir otoriteye güven duyma zorunluluğunda olmadan yapabilen sistemler sayesinde bu değişimin gerçekleşmesi mümkündür.

2. Blokzinciri Teknolojisinin Kavramsal Gelişimi

2.1. Blokzinciri Teknolojisinin Fikri Temelleri

2.1.1. Bilgisayar Teknolojilerinin Gelişimi

Yerleşik hayata geçen toplumlar göçebe toplumlara göre yerleşik hayatta farklı sorunlarla karşılaşmıştır. Bu sorunlardan birisi de hesaplama yapma gereksinimidir. Nitekim, tarım yapılan arazilerin boyutlarının ölçülmesi, bu arazilerden elde edilecek ürünlerin miktarının hesaplanması, bu ürünlerin saklanması için gerekli olan depoların oluşturulması ve bu ürünlerin değiş tokuşu (mübadelesi) için ürünlere değer biçilmesi gibi sorunlar göçebe toplumların karşılaştığı sorunlar değildir. Hayvanların evcilleştirilmesinde ve yetiştirilmesinde, çoğaltılıp mübadele edilmesinde de benzer bir şekilde hesaplama ihtiyacı ortaya çıkmıştır (Ülger, 2022).

Toplumların hesaplama ihtiyacına paralel olarak Matematik bilimi de zamanla gelişim göstermiştir. Hesaplamalar iyice karmaşık hale geldiğinde ve daha fazla kişi bu hesaplama işleriyle uğraşmaya başladığında ise işlemleri kolaylaştırmak için araçlar geliştirilmiştir (KESER, 2019).

Uzun süre basit araçlar kullanılmış olsa da zamanla hesaplama amacıyla kullanılan araçlar geliştirilmiştir. Bugün kullandığımız bilgisayarlar da bu hesaplama ihtiyacını gidermek amacıyla geliştirilen teknolojilerin son versiyonudur denilebilir. Bilgisayarlar artık sadece

hesaplama yapmak için değil, hayatın her alanında kullanılan ve değişik işleri yapmamıza yardımcı araçlar durumuna gelmişlerdir.

Makinelerin icat edilmesi insanın işlerini kolaylaştırmak ve bazı işleri insan yerine makinelerin yapması içindir. Bu makineler, kimi zaman insanın bedensel kabiliyetlerinin üzerinde olan işleri yapmak için kullanılırken kimi zaman da tekrar eden rutin işlerin insan hatasından arındırılması için de kullanılmaktadır. Bazen de insanların kasıtlı olarak yaptıkları insani yanlış ve suistimallerin de önüne geçilmesi için makinelerin istihdam edildiği bilinmektedir. Sonuçta makineler insanlar gibi duygulara sahip değildir. Yorulmaz, zaaf göstermez, görev alanının dışına çıkmaz ya da kasıtlı olarak hatalı işlem yapmazlar. Aksine, ne için tasarlanmışlarsa, enerjisi sağlandığı ve bakımları yapıldığı sürece o işi yapmaya devam ederler. İyi tasarlanmış bir makine tüm insani zaaflardan arınmış bir şekilde kullanım ömrü süresince çalışmasını sürdürür.

Günümüzde makine ve teknolojik aletlerin pek çoğu artık bilgisayarlar ile kontrol edilmeye başlanmıştır. Bilgisayar teknolojilerinin bu denli hayatın içerisine girmesine neden olan etmenlerden biri de şüphesiz bilgisayarların birbiriyle iletişime geçebilme becerilerini kazanmış olmalarıdır. Basit bilgisayar ağları olarak geliştirilen bu teknoloji günümüzde tüm dünyayı kapsayan ve adına internet dediğimiz küresel bilgisayar ağına dönüşmüştür.

2.1.2. İnternet ve Blokzinciri

Farklı kurumların geliştirdikleri bilgisayarlar arasında sorunsuz bir bağlantı oluşturulması amacıyla ISO (International Organization for Standardization) tarafından ilki 1978 yılında sonuncusu da 1984 yılında OSI (Open Systems Interconnection) modeli yayımlanmıştır.[2]

Bu modellerde ağ iletişimi katmanlara ayrılmıştır. En altta fiziksel katmandan en üstte uygulama katmanına kadar yedi katmana bölünen ağ iletişimi terminolojisinin, en üst katmanı olan ve kullanıcıların gereksinimlerini karşılayan uygulama katmanında protokoller bulunur. Bu protokoller sayesinde kullanıcılar ağı amaçlarına göre kullanabilirler. Uygulama yazılımları bu protokolleri kullanarak ağ üzerinde işlemleri gerçekleştirir.

Örneğin bu protokollerden biri olan HTTP (Hyper Text Transfer Protokol) web sayfalarını görüntüleme hizmeti vermektedir. Internet tarayıcısı uygulamaları (Chrome, Opera, Safari vd.) bu protokolü kullanarak aynı protokolü kullanan web sunucusuna bağlanmakta ve bu sunucuda tutulan web sayfasının içeriğini kullanıcıya görüntülemektedir.

SMTP ve POP3 protokolleri mail alma gönderme hizmetlerini organize eder. Protokoller bir program değil bir kurallar dizesidir. Programlar bu kurallar dizesine göre ağı kullanırlar. Mail alma ve göndermek amacıyla kullandığımız mail istemci programları, SMPT ve

[2] https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/osi-katmanlar%C4%B1 erişim tarihi: 01.12.2022

POP3 protokollerini kullanarak posta sunucusuna erişir ve posta alma gönderme işlemlerini gerçekleştirir.

Henüz bir isimlendirmesi veya tanımlaması yapılmamış olsa da Blokzinciri mimarisi protokol katmanında çalışan bir servistir (TÜRÜN, Ethereum Platformu Nedir, Ne İşe Yarar?, 2022). Farklı Blokzinciri modelleri ise kendi içyapılarında birer ekosistem oluştururlar.

Örneğin Ethereum ekosisteminde Ethereum, altyapıyı oluşturan Blokzinciri mimarisinin adıdır. Bir nevi protokoldür. Bu ekosistemde uygulama geliştirenler, tıpkı HTTP protokolü örneğindeki gibi, Ethereum altyapısını kullanarak eşler arasında iletişim kurarlar. Uygulamalar protokolün altyapısını kullanarak çeşitli ihtiyaçları karşılamak için farklı çözümler sunar. HTTP, bir web sayfası görüntüleme hizmeti sunarken, bu servisi kullanan web sitesi geliştiricileri çok değişik amaçlara hizmet eden web siteleri geliştirerek kullanıcılarla etkileşime girerler. Ethereum gibi Blokzinciri ekosistemleri de (protokoller) üzerlerinde çalışan farklı uygulamalarla kullanıcılara merkeziyetsiz bir şekilde bu işlemlerini gerçekleştirme imkânı sunar.

Kısacası Blokzinciri, merkeziyetsiz bir şekilde çalışan bir bilgisayar ağı servisidir. Klasik bilgisayar ağlarında hizmetler, sunuculardan istemcilere doğru akar. Örneğin web siteleri sunucularda tutulur. Aynı şekilde mailler de eposta sunucularda kayıtlı tutulur. İstemci yani kullanıcı, web tarayıcı uygulamasını kullanarak veya eposta uygulamasını kullanarak bu sunucularla iletişime girer ve o

sunucudan hizmet alır. Blokzinciri ağında ise merkezi sunucular yerine, dağıtık halde bulunan düğümler (node) vardır. Veri, merkezi sunucular yerine dağıtık düğümler üzerinde kayıtlı tutulur. Dolayısıyla verinin sahibi yoktur. Bu ağda çalışan uygulamalar da, merkeziyetsiz veri kayıt yapısını kullanarak işlemlerini gerçekleştirirler. Kısacası Blokzinciri, uygulamaların merkezi sunucular olmadan birbirleriyle güvenli bir şekilde iletişim kurup işlemlerini gerçekleştirmelerini sağlan bir bilgisayar ağı servisidir.

2.1.3. Büyük Veri Yığınları ve Tekelleşme

"*Modern dünyaya musallat olan bir hayalet, kripto anarşisinin hayaleti.*"[3]

Günümüzde dijitale kayan ürün ve hizmetlerin birçoğunda veriler merkezi sistemlerde tutulmaktadır. E-posta hizmetinde postalar, hizmeti veren firmanın merkezi sunucularında tutulur. Banka hesap bilgileri bankanın merkezi sunucularında kayıtlıdır. Sosyal medya hesaplarından yapılan bütün işlemler, sosyal medya şirketinin veri tabanlarında tutulur. Anlık mesajlaşma yazılımlarında mesajlar, şirketin merkezi sunucularından doğru eşten eşe aktarılır ve bazı şirketler mesajları analiz etmek amacıyla depolarlar.

[3] Timoty C. Mayis, Cypherpunks hareketi kurucularından. Kripto Anarşist Manifestosu konuşmasından bir alıntı.

Burada saymış olduğumuz örneklere ilave olarak daha pek çok örnek vardır. Günlük hayatta kullandığımız neredeyse bütün internet ürün ve servislerinde sistem hemen hemen bu şekilde çalışmaktadır. Kullanıcının, verisinin kaybolmayacağı, yetkisiz ellere geçmeyeceği, istediği zaman ulaşabileceği veya mahremiyetinin ihlale uğramayacağı konusunda, hizmet aldığı kuruma güven duyduğu sürece bu karşılıklı etkileşim devam eder.

Hizmet veren firmalar ise, hizmet alan kişilere bu hizmeti ücretli sunmaktan, verdiği hizmetin yanında reklam servis etmeye, müşteri verilerini analiz etmek amacıyla üçüncü kişi veya firmalara kategorize edilmiş verilerin satışına kadar bir dizi iş modeliyle kazanç elde etmenin yollarını aramaktadırlar.

2.1.4. Cypherpunks Hareketi

Marks, üretim araçlarının sahipliği, kullanımı, kontrolleri gibi birçok konuya değinirken, üretim yapabilme kabiliyeti ile sosyal ilişkiler arasındaki çelişkiye de değinmiştir (TÜRÜN, NFT'ler ve Yeni Üretim Biçimleri, 2022). Acaba Marks, klasik üretim araçları dışında, günümüz veri üreten devasa bilgisayar sistemlerinin ürettiği verilerle ilgili ne düşünürdü? Veriyi de bir çeşit meta sayar mıydı?

Marks ne düşünürdü bilinmez ama günümüzde bu devasa veri yığınlarının sahipliğiyle ve bunun sonucu oluşan veri tekelleriyle ilgili aykırı düşünenlerin erken örneklerinden birisi Cypherpunks

Hareketi'dir. Bu hareket, insanların internette rahatça gezinebilmeleri ve herhangi bir gözetime, takibe veya suiistimale uğramadan faaliyetlerini icra edebilmelerinin gerekliliğini savunmaktadır. Küresel bilgisayar ağına katılıp bu nimetten faydalanmak isteyen herhangi biri yine bir başkası, bir şirket veya bir devlet kurumu tarafından takip edilebilir, gözetlenip mahremiyeti ihlal edilebilir veya farklı şekillerde kişisel verileri suiistimal edilebilir. Cypherpunks üyeleri insanları bu olası tehditlere karşı korumanın mümkün olduğunu düşünmüş ve bu konuda çalışmalar yapmışlardır.

Cypherpunks hareketi kurucularından olan Timoty C. Mayis, 1992 yılı Kasım ayından Silikon Vadisi'nde yapılan "Fiziksel Cypherpunks" toplantısında yaptığı Kripto Anarşist Manifestosu konuşmasına şu cümlelerle başlamıştır:

> Bilgisayar teknolojisi, bireylere ve gruplara tamamen anonim bir şekilde birbirleriyle iletişim kurma ve etkileşim kurma yeteneği sağlamanın eşiğindedir. İki kişi, diğerinin gerçek adını veya yasal kimliğini bilmeden mesaj alışverişinde bulunabilir, iş yapabilir ve elektronik sözleşmeler müzakere edebilir. Ağlar üzerindeki etkileşimler, herhangi bir kurcalamaya karşı neredeyse mükemmel bir güvence ile kriptografik protokolleri uygulayan şifreli paketlerin ve kurcalamaya karşı korumalı kutuların kapsamlı bir şekilde yeniden yönlendirilmesi yoluyla izlenemez olacaktır.[4]

[4] https://www.activism.net/cypherpunk/crypto-anarchy.html Erişim Tarihi: 20.10.22

Bilgisayar teknolojilerinin gelişimine en ön cepheden tanık olan Şifreci Anarşistler, gelişimin ne yöne doğru ilerleyeceğini elbette görebiliyorlardı. Bu teknolojinin insanlara büyük bir iletişim kurma kolaylığı sağlayacağını ama bu özgürlük alanının başta devletler tarafından engellenmek isteneceğinin de farkındaydılar. Her şeyi kontrol altında tutmak isteyen büyük otoriteler buna izin vermeyeceklerdi ya da kontrol edebilecekleri ölçüde gelişmesine izin vereceklerdi.

"Biz Cypherpunklar, kendimizi anonim sistemler oluşturmaya adadık. Gizliliğimizi kriptografi, anonim posta yönlendirme sistemleri, dijital imzalar ve elektronik para ile koruyoruz."[5] (Eric Hugles)

Bir başka Şifreci Anarşist olan Eric Hugles, 1993 yılında yazdığı "Bir Cypherpunk'ın Manifestosu" yazısında bu konuya değinmişti. Anonim kalmanın, mahremiyetin, özel hayatın gizliliğinin ve ifade özgürlüğünün öneminden bahsettiği manifestosunda, dijital ortamda bunları sağlamanın yolunun mümkün olduğunu da vurgulamaktaydı. Açık bir toplumda mahremiyetin ve anonimliğin özünün kriptolamadan geçtiğini söylediği yazısında, eğer mahremiyet isteniyorsa, bunu birinin bize vermesini beklemeden bir araya gelerek, anonim iletişime izin veren sistemler geliştirerek bu özgürlüğe kavuşulabileceğini ifade etmekteydi.

[5] https://www.activism.net/cypherpunk/manifesto.html Erişim Tarihi: 20.10.22

Erken internet döneminde benzer kaygıları taşıyan ve internetin özgür bir mecra olması gerekliliğine inanıp bu amaçla çözümler üreten çok sayıda insan vardır. 1983 yılında yayınladığı makalesiyle David Chaum, dijital para fikrinin öncülerinden sayılmaktadır. 1989 yılında kurduğu DigiCash adlı firmanın geliştirdiği eCash adlı kripto para, kriptografik anahtar teknolojisini kullanan bir öncüydü ama bazı yetersizliklerden dolayı başarısız olmuştur. Stuart Haber ve W. Scot Stornetta 1991 de yayınladıkları makalelerinde Blokzinciri teknolojisini tanımlamışlardı. Ross Anderson 1996'da merkezi olmayan ve geriye dönük değiştirilemeyen bir veri tabanı fikrini geliştirmiştir. Hashcash ve Bitgold gibi kripto para girişimleri d olmuştur (DURSUN, 2020).

Kısacası, 2008 yılına kadar aslında adım adım Bitcoin ve Blokzinciri teknolojisi için önemli olan bütün teknolojiler hem teorik hem de teknolojik olarak geliştirilmiştir. Satoshi Nakamoto bu süreçten süzülen bilgileri iyi bir şekilde derleyerek ve bazı teknik sorunları çözerek 2008'de Bitcoin'i geliştirmiştir.

2.2. Blokzinciri'nin Teknolojik Temelleri

Merkezi kayıt sistemlerinde verinin işlenmesi ve yönetilmesi kolaydır. Bu nedenle genel yöntem olarak merkezi veri kayıt sistemleri tercih edilir. Buradaki kolaylık kullanıcı için olsa da aslında daha çok veriyi yönetenler içindir.

Mesela para transferleri için bankaların kullanılması, kullanıcılar açısından işleri çok büyük oranda kolaylaştırır. Tüm para transferlerinin ve diğer bankacılık işlemlerinin verilerinin merkezi bir kayıt sisteminde tutulması da bankacıların işlerini kolaylaştırır. Ancak bu müşteriler için bir dezavantajdır. Müşteri yani kullanıcı burada tüm her şey için bankaya güvenmek zorundadır.

Benzer şekilde insanlar günlük işlerini yaparken birçok merkezi sisteme güvenmek zorundadır. Yatırımcı yatırım yaptığı şirketin yönetimine, üretici hammadde veya malzeme aldığı tedarikçiye, satıcı üreticiye, müşteri satıcıya, notere, tapu dairesine, belediyeye, devlet kurumlarına, mahkemeye vs. güvenmek zorunda kalır. Tüm bu kurum, kuruluş veya sisteme olan güven aslında bu yapıları işleten insana duyulan güvendir. Her alanda olmasa da insana güven duyma zorunluluğunu ortadan kaldırmanın teknolojik çözümü olarak Blokzinciri teknolojileri geliştirilmektedir.

Merkezi olmayan bir veri kayıt sistemi tasarlamak ve bunun işlevselliği yanında güvenliğini de sağlamak haliyle diğer merkezi sistemlere göre çok daha zordur ama imkânsız değildir. Blokzinciri'nin ne gibi imkânlar sunduğunu anlamak için nasıl çalıştığını bilmek gerekir. Bunun için ise ağı oluşturan bazı temel yapıların bilinmesi gerekmektedir.

Yaptığımız literatür çalışmasında ve genel gözlemlerimizde, ağın temel işleyiş sisteminin doğru olarak anlaşılamamasının, yanlış

yorumlara neden olduğunu tespit etmemiz nedeniyle çalışmada bu konuya da değinilmektedir.

2.2.1. P2P (Peer to Peer) – Eşten Eşe Ağlar

Blokzinciri'nin en önemli özelliği merkeziyetsiz bir sistem olmasıdır. Bunu sağlayan teknoloji de P2P (Peer to Peer) yani eşten eşe kurulan doğrudan ağ bağlantısıdır. Bu ağın ilk örneği 1999 yılında piyasaya çıkan Napster'dır. Bu ağ bağlantısı sayesinde insanlar herhangi bir aracı olmadan doğrudan birbirleriyle dosya paylaşımı yapabilme imkanına kavuşmuştur. Bu şekilde film, müzik ve dosya arşivleri paylaşıma açılabilmiş ve dünyanın herhangi bir yerindeki bir bilgisayar kullanıcısı bir diğerinin arşivinden izin verdiği dosyaları kopyalayabilir hale gelmiştir. Bu şekilde arama kutucuğuna yazılan dosya adı üzerinden ağa bağlı bütün kullanıcı arşivlerinde tarama yapmak ve bulunan sonuçları anında yerel bilgisayara indirmek sıradan hale gelmiştir.

Film, müzik, e-kitap veya bilgisayar yazılımı vb. yasal lisanslarla korunan bütün dijital içerikler bir anda patlayan bu akımla küresel bir "bedava indirme havuzu" içerisinde erişime açılmıştır.

Bütün bu gelişmelere paralel olarak kişisel bilgisayarlar da Moore Kanunu[6] uyarınca gelişmeye devam etmekteydi. Donanımlar

[6] Intel şirketinin kurucularından Gordon Moore'un 19 Nisan 1965 yılında Electronics Magazine dergisinde yayınlanan makalesi ile teknoloji tarihine kendi adıyla geçen yasa.

hızlanıyor, yazılımlar da bu hıza ayak uydurarak sürekli güncelleniyor ve internet de bu kervana eklemlenerek büyük bir hızda yayılım gösteriyordu. Bu dönem, Dot-com balonunun[7] şiştiği dönemler olarak da ifade edilmektedir.

Yaşanan bu gelişmelere ilk tepki gösteren müzik endüstrisi olmuş ve sonrasında telif davaları birbirini kovalamıştır. Napster sunucularının mahkeme kararıyla kapatılmasıyla son bulduğu sanılan bu serüven aslında günümüze kadar gelen bir dizi değişimin de başlangıcı olmuştur.

Sonraki dönemde Napster'ı daha bir sürü P2P (Peer to Peer – Eşten Eşe Bilgisayar Ağı) uygulaması takip etmiştir. Aslında bu takipçiler de bir şekilde tam olarak merkeziyetsiz sistemler değillerdi ve zamanla yasal engellemelerle karşılaşıp sonlandırıldılar. Daha sonra ise Torrent ağları ortaya çıktı. Gerçek manada P2P altyapısı ile çalışan ve bir merkezi olmayan ağlar bugün de çalışmalarına devam etmektedir.

Blokzinciri teknolojisinin temelini P2P ağları yani eşten eşe ağlar oluşturmaktadır. Kendilerine "Merkeziyetsiz" denmesinin sebebi

---

Her 18 ayda bir tümleşik devre üzerine yerleştirilebilecek bileşen sayısının iki katına çıkacağını, bunun bilgisayarların işlem kapasitelerinde büyük artışlar yaratacağını, üretim maliyetlerinin ise aynı kalacağını, hatta düşme eğilimi göstereceğini öngören deneysel (ampirik) gözlem. https://tr.wikipedia.org/wiki/Moore_yasas%C4%B1 erişim tarihi: 06.12.2022

[7] Dot-com balonu 2000 yılının Mart ayında teknoloji firmalarını yer aldığı borsa endeksi olan NASDAQ'daki senetlerin büyük değer kaybı yaşamasıyla sönen ekonomik balon. Söz konusu kriz, gelişen bilgisayar ve Internet teknolojilerine yatırım yapan risk sermayesi şirketlerinin yatırımlarının geri dönüşünü sağlayamamaları sonucunda bu sektörlerden çekilmeleri sonucu yaşanmıştır. https://tr.wikipedia.org/wiki/Dot-com_balonu erişim tarihi: 06.12.22

de budur. Napster ile başlayıp günümüzde de devam eden Torrent, eşten eşe dosya paylaşım sisteminin geliştirilmesinden edinilen deneyimler sayesinde, Blokzinciri sistemi geliştirilmiştir. Eşten eşe ağ topolojisi ve açık anahtar şifreleme sistemi Blokzinciri'nin temelini oluşturmaktadır.

> Bu devrimin teknolojisi -ve kesinlikle hem sosyal hem de ekonomik bir devrim olacak- teoride son on yıldır var olmuştur. Yöntemler, açık anahtarlı şifrelemeye, sıfır bilgili etkileşimli kanıt sistemlerine ve etkileşim, kimlik doğrulama ve doğrulama için çeşitli yazılım protokollerine dayanmaktadır. (Timoty C. Mayis)

Kripto Anarşist Manifesto'nun bu cümlesindeki idealin gerçekleşmesi 2008 yılında mümkün olmuştur. Gerçekte kimliği bilinmeyen bir başka Şifreci Anarşist Satoshi Nakamoto adıyla yayınladığı Bitcoin manifestosunda[8], 2008 mali krizini eleştirmiş, sınırsız basılan ve belli merkezler (Merkez Bankaları) tarafından sürekli kontrol altında tutulan para sisteminin insanlığı sömürdüğünü belirtmiştir.

Buna karşılık da ortaya merkezi olmayan, dağıtık defter yapısı mimarisinde, P2P ağlar üzerinde çalışan, yüksek seviyeli şifreleme algoritmalarıyla oluşturulan ve korunan, sayısal ve sınırlı bir para biriminin pek âlâ mümkün olduğunu da söylemiş, böyle bir para

[8] https://bctr.org/ingilizce-turkce-cevirisi-ile-bitcoin-makalesi-8202/ adresinden hem Türkçe hem de İngilizce metnine ulaşılabilir. Erişim tarihi: 06.12.2022

sisteminin ön hazırlığını yaptığını, kodlarını yazdığını ve deneme amacıyla yayınladığını da manifestosunda ilan etmiştir.

Bir başka Anarşist Şifreci Julian Assange 2010 yılında The Guardian, The New York Times ve Der Spiegel gazetelerinde yayınlanan 92.000 belgeyle tarihe geçen Wikileaks belgelerinde, devletlerin halklarından neler gizleyebileceklerine dikkat çekmiş ve dünyada ses getirmiştir. Sonrasında yayımladığı kitabında da hem büyük teknoloji firmalarının hem de devlet otoritelerinin internet servisleri üzerinden nasıl bir bilgi toplama yarışına girdikleri üzerinde durmuştur. Assange, devletlerin ve şirketlerin gözetleme ve sansür konusunda büyük imkânlara ve araçlara sahip olduklarını belirtirken, bunlardan korunmak içinse kriptografi yardımıyla korunan merkeziyetsiz sistemlerin kurulmasının gerekliliği üzerinde durmuştur (Assange, 2013).

2.2.2. Şifreleme (Kriptografi)

Kriptoloji, Yunanca bir türetilmiş kelime olup "Gizlilik Bilimi" anlamına gelir. Teknik terim olarak da, bir mesajın üçüncü şahıslar tarafından anlaşılamayacak biçimde belirli teknikler kullanılarak dönüştürülmesi şeklinde tanımlanır. Mesajın orijinal haline açık metin, dönüştürülmüş haline şifrelenmiş, gizlenmiş metin denir ve bu dönüştürme işlemine de kriptolama denir (YERLİKAYA, 2006).

İki kişi arasında gizli kalması istenen iletişimin bir üçüncü kişi tarafından öğrenilmemesi amacıyla şifrelenmesi ihtiyacı M.Ö. 2000'li yıllara, Antik Mısır'a kadar dayanır. Günümüz arkeolojik araştırmalarında hiyeroglif şekillerinin arasında şifrelenmiş mesajların bulunduğu keşfedilmiştir. Aynı şekilde, M.Ö. 1500'lü yıllarda Mezopotamya'da çivi yazısı ile bazı tabletlerde şifreleme yapıldığı tespit edilmiştir. Sparta ve Roma'da da kullanıldığı bilinen farklı şifreleme yöntemleri mevcuttur. Bilinen ilk şifreleme ile ilgili kitabı Arap Filozof Al-Kindî (Doğum: 801 – Ölüm: 873) yazmıştır. Sonraki zamanlarda da özellikle askeri alanda sıklıkla değişik türde şifreleme yöntemleri geliştirilmiştir (ÇEŞMECİ, 2009).

Şifrelenmiş mesaj alıcısına ulaştığında alıcı tarafından bilinen şifre çözme yöntemi ile tersine bir işlem yapılarak şifreli metin çözümlenir ve orijinal mesaja ulaşılır. Bu noktada gönderici ve alıcı tarafından ortak bir şifreleme yöntemi kullanılması gerekmektedir ve bu yöntemi diğer kişilerin bilmemesi önemlidir. Ayrıca şifreleme yönteminin üçüncü şahıslar tarafından tahmin edilerek veya deneme yanılma yöntemleriyle çözülemeyecek kadar da güvenli olması beklenir. Bu nedenle değişik şifreleme yöntemleri geliştirilmiştir.

Mesela Romalı General Sezar'ın kullandığı bilinen şifreleme yöntemi oldukça basittir. Yazılan mesaj, her bir harfin alfabedeki belli bir sayı sonrasında gelen harfle değiştirilmesi şeklindedir. Anahtar sayı 5 ise, mesajdaki her harfin yerine 5 sonraki harf yazılarak metin şifrelenir. Mesajın alıcısı anahtar değeri biliyorsa kolayca şifreli

mesajdaki her harfi, alfabede 5 öncesinde yer alan harf ile değiştirerek şifreyi çözer. O zaman için oldukça etkili ama kırılması da bir o kadar kolay bir şifreleme yöntemidir. (ÇEŞMECİ, 2009)

Özellikle 2. Dünya Savaşı sırasında Almanların geliştirdiği Enigma makinesi çok etkili bir şekilde kullanılmıştır. Bu şifreleme yönteminin kırılması savaşın gidişatını değiştirmiştir. Hatta bu çalışmaların savaş sonrasında bilgisayar teknolojisinin gelişmesinde önemli katkıları olmuştur.

Şifreleme ve şifre çözme işlemleri için kullanılan yöntemlere Şifreleme Algoritmaları denir. Günümüzde iki çeşit şifreleme algoritması vardır.

Simetrik şifreleme algoritmasında şifreleme için bir gizli anahtar vardır. Bu anahtar yardımıyla mesaj şifrelenir. Mesajın çözümü için de yine aynı anahtara ihtiyaç duyulur. Anahtar burada karmaşık matematiksel işlemlerdir. Anahtarı bilen biri hem şifreleme hem de şifreyi çözümleme işlemi yapabilir (BEKİRLİ, ÖZDEMİR, & BEŞKİRLİ, 2019).

Asimetrik şifrelemede ise bir açık anahtar (public key) ve bir de özel anahtar (private key) vardır. Açık anahtar ile şifreleme yapılır. Şifrenin çözümü ise özel anahtar ile yapılır. İki anahtar da birbiriyle ilişkilidir. Açık anahtarı herkes bilebilir ama özel anahtarı kimsenin bilmemesi gerekir. Kişi göndereceği mesajı karşıdaki kişinin açık anahtarı ve kendi özel anahtarını kullanarak şifreler. Karşıdaki kişi mesajı aldığında kendi özel anahtarı ve gönderenin açık anahtarını

kullanarak mesajı çözer. Böylece simetrik şifrelemede olduğu gibi şifre anahtarının taşınması da gerekmez. Blokzinciri'nde de bu şifreleme algoritması kullanılır.

Kriptografi, günümüzde internet ve bilgisayar ağları gibi birçok alanda etkili bir şekilde kullanılmaktadır. Web sitelerini ziyaret ederken, mail alıp gönderirken, alışveriş yaparken vs. birçok alanda biz farkında bile olmadan arka planda çalışan kriptografik algoritmalar tarafından işlemlerimizin güvenliği sağlanır.

Şifreleme, üçüncü tarafların işleme müdahalesini engeller ama sonuçta internet üzerinden bir hizmet alıyorsak, hizmeti almamızı sağlayan merkezi sunucu sistemine güvenmek zorunluluğumuzu ortadan kaldırmaz. Blokzinciri ağında şifreleme en temel unsurdur. Kullanıcının kimliğinin gizli kalmasını sağlayan şey, asimetrik şifreleme yöntemiyle üretilen kripto cüzdan uygulamasıdır.

2.2.3. Dağıtık Defter Teknolojisi

Genel kullanım olarak dijital ortamda veriler merkezi veri tabanlarında tutulur. Bu şekilde verinin kaydedilmesi, düzenlenmesi, değerlendirilmesi ve işlenmesi oldukça kolay ve az masraflı bir şekilde gerçekleşir. Ancak verilerin merkezi bir sistemde toplanması beraberinde saldırıya ve suiistimale açık olması gibi sorunlar da getirir.

Bu soruna çözüm olarak da Dağıtık Defter Teknolojisi (Distributed Ledger Technology - DLT) geliştirilmiştir. Bu sistemde

veri tek bir merkezde tutulmaz. Birbiriyle bağlantılı dağınık halde farklı yerlerde bulunan ortamlarda depolanır. Kaydedilecek veri birbirinden farklı bölgelerde bulunan bu birimlere aktarılarak kaydı yapılır. Dağıtık Defter Teknolojisinde verinin birçok kopyası birbirinden uzak konumlarda bulunan sistemlerde eş zamanlı olarak kaydedilir yani aynı verinin bir sürü kopyası üretilir. Böylece bir sistem zarar görse bile diğerleri çalışmaya devam eder. (ŞAFAK, ARSLAN, GÖZÜTOK, & KÖPRÜLÜ, 2021). Bir sistemdeki veride bir bozulma veya değişiklik gerçekleşirse, eş zamanlı olarak çalışan zincir, diğer kayıt ortamlarında tutulan verilerle karşılaştırma yapar ve değişen sistemdeki verinin güvenilmez olduğunu ya da veride bir sorun olduğunu kolayca tespit eder.

Bu sistem her iş için uygun değildir. Veriler bu yapıda sadece kaydedilir. Geriye dönük silme veya düzenleme yapılamaz. Veri tek yönlü olarak kaydedilir. Bu yüzden tam bir veri tabanı olarak tanımlanması doğru değildir. Çünkü üzerinde düzenleme, değişiklik, geriye yönelik herhangi bir müdahalede bulunulamaz. Bu yüzden sadece işlem kaydının tutulması gereken durumlarda kullanılabilecek bir çözümdür.

Bu sistem bir nevi hesap defteri, muhasebe defteri gibi de düşünülebilir. Eğer kayıt bir defterde tutulursa, o defterin kaybolması, tahrip olması veya üzerinde değişiklik yapılması sonucu mağduriyetler oluşabilir. Ancak deftere kaydedilecek veri aynı zamanda farklı

noktalardaki başka defterlere de kaydedilirse, veri güvenliği açısından çok daha kesin bir sonuca ulaşılabilir.

Bu yapı aynı zamanda şeffaflığı da sağlar. İşlemler herkese açık defterlere kaydedilir. İsteyen herkes geriye dönük olarak ağ üzerinde yapılan bütün işlemleri kontrol edebilir. Açık anahtar şifreleme sayesinde işlemleri yapanların kimlikleri gizlidir ama yapılan işlemler açık bir şekilde görülebilir.

Dağıtık defter teknolojisinin farklı çözümler sunan ve farklı mimarilere sahip birçok türü bulunmaktadır. Kullanım alanlarına göre Blokzincirleri bu türlerden biri üzerine inşa edilir.

Burada deftere hangi verinin kaydedileceğine ise eşler (düğüm, node) arasında varılan mutabakat (konsensüs) sonucu karar verilir.

2.2.4. Düğüm (Node)

Açık Blokzinciri sistemlerinde isteyen herkes sistemin bir parçası olabilir. Blokzinciri'nin bel kemiğini kayıtların tutulduğu Düğüm (Node) denilen bu yapılar oluşturur. Sistemin güvenilirliğini sağlamak adına Düğüm (Node) olmak isteyen herkes bazı gereklilikleri yerine getirmesi gerekir. Bu gereklilikler mutabakat protokollerine göre değişebilir. Mesela Bitcoin ağında Düğüm olmak isteyen kişinin yüksek işlem gücüne sahip bir bilgisayarı olması gerekirken, Ethereum ağında Düğüm olmak isteyen kişinin belirli bir miktar Ether'i (Ethereum ağında kullanılan kripto para) sisteme yatırıp kilitlemesi (stake etmesi) gerekir.

Bu gereklilikler değişebilmektedir ama en büyük özellik üğümlerin tamamen anonim olmasıdır.

Bir Blokzinciri ağındaki Düğümler, birbirinden bağımsız bir şekilde, ağı işleten yazılım üzerinden haberleşerek çalışırlar. Bitcoin ağına katılmak isteyen bir Düğüm, gerekli donanıma sahip bir bilgisayar sistemini hazırlayıp, o sisteme Bitcoin yazılımını yükler ve bu yazılım sayesinde ağın bir parçası olur. Sonrasında Düğüm üzerinde çalışan Bitcoin yazılımı Bitcoin ağı ile haberleşerek, ağ üzerinde gerçekleşen işlemlerde o sistemin de bir payının olmasını sağlar. Daha önceden yapılmış olan bütün işlemlerin bir kopyasını da o sisteme yükler. Bitcoin ağına katılan bütün Düğümlerde, Bitcoin ağında başlangıcından beri yapılmış olan bütün işlemlerin bir kopyası vardır. Dağıtık defter teknolojisi, Düğümler üzerinde çalışır ve yapılan işlemlerin kayıtlarının Düğümlere yayılarak eş zamanlı olarak kaydedilmesini sağlar.

Bir Bitcoin Düğümü, yapılan işlemlerin doğruluğunun kontrol edilmesi için gerekli olan işlem gücüne katkıda bulunurken aynı zamanda onaylanan işlemlerin de yaparak kaydını tutar. Bitcoin Düğümleri hem Bitcoin üretimi yapar hem eşler arasındaki Bitcoin transferlerin geçerliliğini kontrol edip onaylar hem de bu işlemlerin kaydını tutarken aynı zamanda da kullanıcıların cüzdanlarındaki kripto para miktarının da verisi Düğümlerde tutulur.

Düğümler, Blokzinciri ağının bel kemiğini oluşturan yapılardır. Dağıtık olmalarından dolayı saldırılara karşı korunaklıdırlar. Dağıtık defter mimarisinden dolayı da şeffaftırlar. Kriptografik algoritmalar

sayesinde de kullanıcıların anonim kalmasını sağlarlar. Gerekli şartları yerine getiren herkesin katılabileceği bir yapıda olduklarından dolayı da merkeziyetsizdirler.

2.2.5. Kripto Para Cüzdanı

Kripto para, Blokzinciri üzerinde üretilir ve düğümler üzerinde saklanır. Blokzinciri ağının bütün verileri her bir düğümde kayıtlıdır. Kendi kripto varlığına sahip olmak isteyen biri, o Blokzinciri ağının bütün verilerini bilgisayarına indirmek ve tam bir düğüm çalıştırmak zorundadır. Bunu yapmak zor ve kullanışlı değildir. Kullanıcılar zincir üzerinde cüzdanlar oluşturarak kendilerine ait kripto varlıklara ulaşabilirler.

Aslında kripto para cüzdanı, kullanıcının zincir üzerindeki varlıklarına erişebilmesi için kullandığı bir anahtardır. Kripto varlık zincir üzerinde kayıtlı tutulur. Kullanıcı cüzdanla (anahtarla) o hesabına erişerek kripto varlıklarını görebilir veya başka bir hesaba transfer yapabilir. Aslında kripto varlığın transferi diye de bir şey söz konusu değildir. Kripto varlık zincir üzerinde sabit durur ama sadece sahipliği el değiştirir (TÜRÜN, Token'larımızı Artık Bankalarda Saklayacağız!, 2022).

Bir kullanıcı diğer bir kullanıcıya bir kripto varlık transfer ettiğinde, aslında o kripto varlığın sahipliğini devretmiş olur. Kripto cüzdanlar, sadece bu varlık sahipliğinin el değiştirmesine aracılık eden,

kullanıcının o kripto varlığa sahipliğini kesinleştiren birer eşleştirme mekanizmalarıdır.

Kripto para cüzdanı iki bölümden oluşur, gizli anahtar ve açık anahtar. Bu iki anahtar da aslında kriptografik algoritmalar tarafından üretilen rastgele sayılardır ve birbirleriyle bağlantılıdırlar yani birbirlerinden türetildikleri için bir nevi ikiz olarak çalışırlar. Açık anahtar, adı üzerinde kullanıcının cüzdan adresidir ve herkes tarafından bilinir. Gizli anahtar ise o cüzdanın sahipliğinin kime ait olduğunu belirleyen gizli bir koddur. Eğer gizli anahtar bir başkasının eline geçerse, o cüzdanın sahibi o kişi olur. O yüzden iyi saklanmalıdır. Ayrıca kaybedilirse de cüzdana erişim sağlanamayacağından dolayı o cüzdandaki kripto varlıklar sonsuza kadar zincir üzerinde sahipsiz bir şekilde kalır. Bitcoin ağı üzerinde tahminlere göre 3 milyon civarı Bitcoin'in[9] bu şekilde sahipliğinin kaybedildiği düşünülmektedir.

Bir kripto varlığın sahipliği el değiştireceği zaman gönderici, alıcının cüzdan adresine (açık anahtarına) ihtiyaç duyar. Alıcının açık anahtarı ve gönderenin gizli anahtarı ile imzalanan varlık transferi işlemi zincire gönderilir. İşlem isteğini alan düğüm (madenci, node) bu işlem isteğini ağdaki diğer düğümlere iletir. Düğümler işlem isteğinde bulunan adreslerin gerçekliğini ve göndericinin hesabında gerçekten o gönderilmek istenen miktarda kripto varlığın olup olmadığını bu anahtarlar sayesinde doğrular. Aynı zamanda alıcı adres de kendisine gönderilen kripto varlık verisinin doğru kişiden gelip gelmediğini,

[9] https://www.bbc.com/turkce/articles/cld4w3dqz9lo erişim tarihi: 18.04.2024

gönderenin açık anahtarı ile yine gönderen tarafından gizli anahtarı ile imzaladığı işlemi eşleştirerek doğrulama yapar. Eğer işlemde bir sorun yoksa onaylanır ve bloğa eklenmek üzere sıraya alınır. Blok zamanı dolduğunda diğer işlemlerle birlikte işlem onaylanıp bloğa eklenir ve transfer işlemi tamamlanmış olur yani kripto varlığın sahipliği el değiştirmiş olur.

Kısaca gönderici, alıcının açık anahtarı ve kendi gizli anahtarı ile işlemi imzalar. Alıcı da kendi gizli anahtarı ve göndericinin açık anahtarı ile gönderinin gerçekten o kişiden gelip gelmediğini doğrular ve işlem tamamlanır.

Açık anahtar ve gizli anahtar birbirlerinin çiftidir ve birbirlerinden üretilirler. Bu sayede alıcı ve gönderici birbirlerinin gizli anahtarlarını bilmezler ama karşının gizli anahtarı ile damgaladığı transfer işlemini, yine karşı tarafın açık anahtarı ile doğrulayabilirler. Bir açık anahtardan yola çıkarak gizli anahtarı bulmak, şuanki bilgisayarların işlem güçleriyle neredeyse imkansızdır. Çünkü $1\text{-}2^{256}$ gibi bir aralıkta ikili sayı sisteminde üretilen anahtarların deneme yanılma yöntemiyle bulunması çok çok zordur (TANRIKULU, YÜCE, & ÖLÇER, 2021).

Cüzdanlar sıcak cüzdan ve soğuk cüzdan olarak genelde iki guruba ayrılabilir. Sıcak cüzdanlar masaüstü, web ve mobil cüzdanlar olarak üçe ayrılır. Kullanım açısından pratiktir ama güvenlik açısından zayıftırlar. Kaybedilmeleri veya çalınmaları daha kolaydır. Soğuk cüzdanlarda ise anahtarlar çevrim dışı olarak saklanır yani internete

bağlantısı yoktur. Donanım cüzdanlar ve kâğıt cüzdanlar buna örnek gösterilebilir. Daha güvenilirdirler ama kullanım açısından pratik sayılmazlar (DURMUŞ, 2018). Karipto varlıkların saklanmasında ve transferinde sorumluluk tamamen kullanıcıya aittir. Gizli anahtarın kaybedilmesi, unutulması veya çaldırılması, yanlış adrese transfer gibi durumlarda işlemler geriye döndürülemez.

2.2.6. Konsensüs (Mutabakat) Protokolleri

Peki, veriler tek bir merkezde tutulmuyorsa, dağıtık bir kayıt sistemi kullanılıyorsa ve isteyen (şartları karşılaması koşuluyla) herkes bu sisteme dâhil olabiliyorsa, bu kadar çok paydaşı olan bir sistemde hangi verinin kaydedilip hangisinin reddedileceğine kim karar verecektir? Art niyetli kişilerin sistemi manipüle etmesine, yanlış verilerin kaydedilmesine kim nasıl engel olacaktır?

Burada devreye Mutabakat (Konsensüs) protokolleri girmektedir. Kullanıcıların Dağıtık Defter'e kaydedilmesi için gönderdikleri istekler (mesela bir para transferi), Düğümlere iletilir ve Düğümler kendi aralarında bu isteğin doğruluğunu ve geçerliliğini, önceden belirlenmiş bir dizi kurallar manzumesine uygunluğuna göre analiz eder ve işlemin doğru/güvenilir/geçerli olduğuna mutabık olduklarında da deftere kaydederler (yani zincire işlemi/bloğu eklerler).

Burada iki temel sorun ortaya çıkmaktadır;

Bunlardan birincisi, işlem isteğini gönderen kişinin doğru işlem yapıp yapmadığıdır. Para transferi örneğinden yola çıkarak devam edecek olursak, kişi aynı para ile iki transfer yapmak isteyebilir veya hesabında olmayan parayla işlem yapmak isteyebilir.

İkinci sorun ise, Düğümlerden biri veya birkaçının işlemleri suiistimal etmek istemesi ihtimalidir. Düğümler, işlemlerin arasına fazladan işlem ekleyebilir veya işlemlerin yapısını bozarak manipüle edebilir. Mesela para transferinde transfer miktarlarının değiştirilmesi gibi ihtimaller ortaya çıkabilir.

Bu ve bunun gibi birçok sorunu çözebilmek ve sistemin hem merkeziyetsiz hem de anonim kalabilmesinin yanı sıra güvenliğinin de sağlanabilmesi için kriptografi, mutabakat ve ödül-ceza gibi bir dizi araçlar kullanılarak tedbir alınmaktadır. Bu nokta oldukça önemlidir. Çünkü güvenmek yerine somut geçerliliği ve kanıtı olan bir sistem çalışmaktadır.

Düğümlerin, kullanıcılardan gelen işlem istekleri üzerinde mutabakata varmak için kullandıkları bazı Mutabakat (Konsensüs) protokolleri vardır. Burada hepsine değinmeye gerek görmüyoruz. Sadece iki tanesini çok fazla teknik detaya girmeden izah etmemiz meselenin anlaşılmasına yardımcı olacaktır.

Bitcoin ağında kullanılan Mutabakat protokolüne İşlem Kanıtı (Proof of Work – POW) denilmektedir. En basit haliyle burada Düğümler, gerçek birer katılımcı olduklarını işlem güçleriyle kanıtlamak zorundadırlar. Biriktirilen işlemlerin bloğa eklenmesi için

sistem ortaya bir bulmaca atar. Yüksek matematiksel hesaplama gücüyle çözülebilecek olan bu bulmacayı ağdaki tüm Düğümler çözmeye çalışır. Bu sayede bir nevi Düğüm'ün donanımsal yeterliliği test edilir. Böylece yeterince gücü olmayan kimse sistemi manipüle etmek için girişimde bulunamaz.

Bulmacayı ilk çözen Düğüm'ün biriktirdiği işlemler Defter'e (Bloğa) kaydedilir ve bu Düğüm'e bunun karşılığında ödül verilir (DURSUN, 2020). Dolayısıyla işlem gücü zayıf kalanın ağda hiçbir etkisi yoktur. Yüksek işlem gücü yüksek elektrik tüketimi demektir. Düğümler kendilerinin gerçek birer ağ elemanı olduklarını ispatlamak, art niyetli olmadıklarını kanıtlamak ve çifte ödemeleri engellemek için güçlü dolanımlar ve yüksek elektrik faturalarını ödemeye mecburdurlar. Karşılığında da işlemlerden komisyon alırlar.

Bir Düğüm'ün bu sistemde Bitcoin ağını manipüle edebilmesi için, ağdaki toplam işlem gücünün %51'inden daha fazla bir işlem gücüne sahip bir bilgisayar sistemi kurması gerekir ki bu da oldukça pahalı bir yatırım olur. Buna %51 saldırısı denir ve bu mutabakat protokolünü kullanan, düğüm sayısı az bazı kripto para ağlarında ara sıra görülür. Bu saldırı sayesinde geriye dönük değişikler yapılabilir, cüzdanlardaki varlıklar değiştirilebilir veya çifte harcamalar yapılabilir.

Ancak, böyle bir girişimde bulunulsa ve yapılan işlemler o anlık manipüle edilse bile ağın diğer Düğümleri bunu fark edeceklerdir. O andan itibaren ağda bir çatallanma (fork) olur ve ağ ikiye bölünür. Manipüle edilen işlemlerin devam ettirildiği Bitcoin ağı bir taraftan, o

işlemin kaydını onaylamayan diğer Düğümlerin çalıştırdığı Bitcoin ağı diğer taraftan çalışmaya devam eder. Burada Bitcoin topluluğu hangi ağı tercih ederse o ağ rağbet görür ve çalışmaya devam eder. Diğer ağ rağbet görmeyeceği için o ağın değeri düşecektir.

İşlemlerin onaylanması için ortaya atılan bulmacayı çözmek için gerekli olan işlem gücü de zamanla artmaktadır. Bitcoin ağında ortalama dört senede bir otomatik olarak Bitcoin yazılımı, Düğümlere çözmeleri için gönderdiği bulmacanın zorluk derecesini iki katına çıkarır. Yüksek işlem gücü olan Düğümler daha fazla ödül kazanır. Bu da Düğümleri sürekli olarak sistemlerini daha hızlı hale getirmek için donanımsal olarak güncelleme yapma zorunluluğu getirir. Aynı zamanda daha fazla elektrik tüketmelerine de neden olur.

İşlem Kanıtı Mutabakat Protokolü'nde yüksek işlem gücü büyük maliyetlere neden olur ayrıca bu sistemlerin çalışması büyük miktarda elektrik enerjisine bağlıdır. Bu nedenle daha çevre dostu bir sistem olarak Hisse Kanıtı (Proof of Stake) Protokolü geliştirilmiştir. Ethereum gibi ağların kullandığı bu sistemde Düğümler, belirli miktarlarda para birimini (Ethereum ağında 32 adet Ether, Avalunch ağında 2000 adet Avax gibi) sisteme yatırırlar. Belirli miktarda kripto varlığa sahip olduğunu ispat eden herkes sistemde söz sahibi olur. Ancak bu paydaşlardan biri yani bir Düğüm yanlış bir iş yapmaya kalkarsa sistemde kilitli tutulan kripto varlığı sistem tarafından yakılır. Eğer doğru bir şekilde çalışmaya devam ederse de sistemde gerçekleşen işlemlerden komisyon ücreti alır (DURSUN, 2020).

Hisse Kanıtı (POS) protokolü ile çalışan Blokzinciri ağlarında işlem gücü önemli değildir. Böylelikle yüksek işlem gücüne sahip bilgisayar sistemlerinin kurulması, sonrasında artan işlem gücü ihtiyacı için sistemlerin güncellenmesi, bu sistemlerin bakım ve elektrik maliyetlerine katlanılması gerekmez. Herkesin ulaşabileceği seviyede bir işlem gücüne sahip bir bilgisayarla yeterli miktarda kripto parası olan herkes Hisse Kanıtı (POS) ağına dahil olarak o ağın çalışmasına katkıda bulunabilir ve ağdan ödül kazanabilir.

Konsensüs protokolü bir yazılımdır. Bütün düğümler aynı yazılımı kullanırlar. Genelde de açık kaynak kodlu yazılımlardır. Böylece sistemin nasıl çalıştığı herkes tarafından bilinebilmektedir. Dağıtık bir şekilde bulunan Düğümlerin birbirleriyle doğru bir şekilde haberleşebilmeleri, eş zamanlı ve kurallara uygun bir şekilde çalışabilmeleri için bu yazılımlar önemlidir.

Konsensüs protokolü yazılımı hazırlanırken şarlar baştan yazılıma tanımlanır. Sistem dağıtık bir şekilde çalıştığı için ve belirli bir yöneteni olmadığı için kimse söz sahibi değildir. Dolayısı ile Konsensüs protokolleri üzerinde sonradan bir değişiklik yapılabilmesi için katılımcıların ortak onayının olması gerekir. Bazı Blokzinciri ağlarında ara sıra güncellemeler yapılmaktadır. Bu güncellemelerin Düğümler tarafından onaylanarak sistemlerine yüklenmesi gerekir ki, ancak bu şekilde çalışabilirler.

Mesela Bitcoin ağında ilk zamanlarda birkaç güvenlik güncellemesi yapılmış olup onun dışında yıllardır aynı yazılım üzerinden Düğümler çalışmaya devam etmektedir.

2.3. Blokzinciri Nasıl Çalışır?

Blokzinciri en temelde halka açık bir muhasebe defteridir. Modern muhasebe çift taraflı kayıt tutma prensibine dayanır. Alacaklı alacağı tutarı muhasebe defterine yazarken, borçlu da borcunu muhasebe defterine yazar ve bu defterlerin birbiriyle tutarlılık göstermesi beklenir.

Blokzinciri'nde tarafların birbirleri arasındaki işlemler çok sayıda ve herkesin istediği zaman okuyabileceği bir defterde kayıtlı tutulur. İşlemi yapan taraflar gizlidir ama işlemler herkese açıktır. Bu sisteme şeffaflık getirir. Gizli kapaklı işlerin yapılmasının önüne geçer. Kullanıcıları gizlediği için de aynı zamanda bir anonimlik sağlar. Kayıtlar kriptografik yöntemlerle birbirlerine bağlanarak zincirin bir halkası olacak biçimde uç uca eklendiklerinde, geriye dönük olarak değiştirilmeleri de neredeyse imkânsızdır.

İşlemlerin gerçekleştirilerek kayıt altına alınması (blokların oluşturulması) çok sayıda düğüm (Node) üzerinden gerçekleştiğinden ve bu düğümlerin birbirleri ile önceden belirlenmiş kurallar çerçevesinde, (her biri üzerinde çalışan aynı programlar sayesinde) bir

mutabakat üzerine bu işlemleri gerçekleştirdiklerinden dolayı da, taraflardan birinin sahtekârlık yapması imkânsız hale gelir.

Biraz daha yakından inceleyecek olursak Blokzinciri yapısı temelde beş katmandan oluşur (DURSUN, 2020).

1. Altyapı katmanı; Blokzinciri'nin temeli olan dağıtık düğümleri (Node) yani birbirine bağlı bilgisayarları ifade eder. Mutabakat (konsensüs) protolokülünün biçimine göre değişik yapıda olabilirler.

2. Ağ Katmanı; İşlemlerin düğümler (Node) arasında yayılması, zincir verilerinin indirilmesi ve blokların ağda yayımlanması gibi işlemlerin yürütüldüğü işlem katmanıdır.

3. Mutabakat Katmanı; Mutabakat protokollerinin işletildiği işlem katmanıdır. Burada düğümlerin (Node) aralarında uzlaşmaya vararak hangi işlemlerin bloğa ekleneceğine karar verdikleri alandır. Birçok mutabakat (Konsensüs) protokolü bulunmaktadır. Bunlardan en çok bilinen ve kullanılanları İşlem Kanıtı (POW) ve Hisse Kanıtı (POS) mutabakat (konsensüs) protokolleridir.

Mesela Bitcoin ağı için ilk zamanlarda bilgisayarlar yeterliyken, İş İspatı (POW) konsensüs protokolü gereği artan işlem gücünü karşılamada bilgisayarlar yetersiz kalmıştır. Bu sebeple özel işlemciler geliştirilmiştir. Sadece bu amaçla üretilen ASIC cihazlar şuan Bitcoin ağının altyapısını oluşturmaktadır.

Ethereum ağı için de İş İspatı (POW) algoritması kullanılırken işlemci yerine bilgisayarların ekran kartları kullanılmıştır. Ethereum ağının Hisse İspatı (POS) algoritmasına geçmesiyle birlikte işlem gücü yerine sıradan bilgisayarların da kullanılabildiği bir modele geçilmiştir. Şuan ki birçok Blokzinciri sistemi bu yöntemi kullanmaktadır.

4. İşlem Katmanı; Veri katmanı olarak da bilinir. Zincir üzerinde yapılan işlemlerin verilerinin zincire kaydedildiği işlem katmanıdır. İşlemler biriktirilerek, zincirin yapısına göre belirlenen zamanlarda, mutabık kalınan koşullar çerçevesinde onaylanan işlemler blok haline getirilir ve zincire yazılır. Bitcoin ağında bu süre yaklaşık on dakikadır. Bu süre içerisinde işlemler biriktirilir. İşlemlerin geçerliliği İş Kanıtı (POW) konsensüs (mutabakat) protokolüne göre düğümler (Node) arasında doğrulanır ve süre sonunda işlemler blok haline getirilerek zincire kaydedilir.

Bitcoin gibi sadece para transferi için oluşturulmuş ağlarda işlem denilen şey paranın aktarılması iken, Ethereum gibi para transferini şarta bağlan yani bir akıllı sözleşme ile bağlayan ağlarda akıllı sözleşmeler de bu katmanda değerlendirilir.

5. Uygulama Katmanı; Zincir üzerinde verinin üretilmesi, depolanması ve daha sonraları sorgulanabilmesini sağlayan uygulamaların çalıştığı işlem katmanıdır. Kripto para cüzdanları, borsalar, dağıtık defterlerin izlenmesini ve incelenmesini sağlayan uygulamalar ve geliştirilen akıllı kontratların tüm işlem ve sonuçlarının takip edilebilmesini sağlayan uygulamalar bu katmanda yer alır.

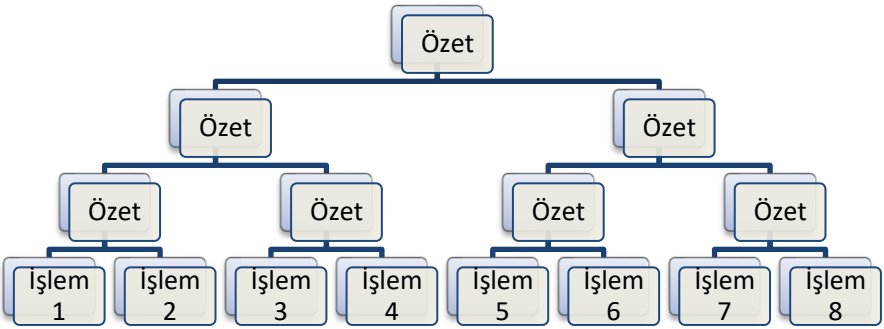
Özellikle akıllı sözleşmelerin kullanım alanlarını yaygınlaşmasıyla birlikte uygulama katmanında geliştirilen uygulamalar çoğalmıştır. Blokzinciri hizmetlerini kullanan kullanıcılar bu katmandaki uygulamaları kullanarak zincire erişim sağlarlar.

Örnek olarak, bir kullanıcının bir işlem yapmak istediğini farz edelim. Bu bir dijital varlık (kripto para, NFT veya başka bir dijital varlık olabilir) transfer isteği olsun. Kullanıcı uygulama katmanındaki uygulamayı kullanarak (kripto para cüzdanı mesela) bu isteğini işlem katmanına iletir. Kullanıcı kendine ait olan şifreli anahtarla bu işlemi damgalar ve transfer isteği işlem katmanına iletilir.

Dijital varlığın transferi isteği işlem katmanı tarafından düğümlere iletilir. Bu isteğin düğümler tarafından doğrulanması gerekir. Bunun için işlemin kendisine iletildiği düğüm bu işlemi komşu düğümlere iletir ve düğümler kendilerine iletilen işlem isteğinin doğruluğunu ve ağa uygunluğunu kontrol ederler. Gönderilmek istenen dijital varlığın gerçekte olup olmadığı, şifre anahtarının doğruluğu, deftere uygunluğu gibi bir dizi kontrolden geçer.

Bu esnada her bir düğüm kendi doğrulama ve onaylama işlemini yapar. Ardından düğümlerin arasında bu işlemin doğruluğunun ve geçerliliğinin onaylanması için mutabakat (konsensüs) protokolleri çalışır. Biriktirilen işlemlerin doğruluğunun ve geçerliliğinin düğümler arasında varılan mutabakat sonucu onaylanmasıyla birlikte işlemler birleştirilerek blok haline getirilir ve zincire kaydedilir.

İşlemlerin blok haline getirilmesi esnasında her iki işlemin, Hash algoritması tarafından özeti alınır. Bu özetler başka bir ikili işlemin özeti ile tekrar özeti alınacak şekilde işleme sokulur. Sonra bu işlem tekrarlanır. Bu işlem bir ağaç şeklinde aşağıdan yukarıya doğru hiyerarşik bir şekilde ilerler. Sonuçta en tepede tek bir özet sonucu oluşur. İşte bu özet sonuç sonraki bloğa girdi olarak kaydedilir. Bu sayede zincir ağı kurcalamaya karşı korunmuş olur. Bu yapıya Merkle Ağacı denilmektedir.



Şekil 1: Merkle Ağacı

Blokzinciri teknolojisini güvenli kılan en önemli unsurlardan birisi de bu Özet Fonksiyonu (Hash Algoritması) dur. Özet Fonksiyonu; girdisi ne olursa olsun sabit uzunlukta bir sonuç üreten algoritmadır (TAŞ & KİANİ, 2018). Özet Fonksiyonu tek yönlü bir fonksiyondur. Sonuçtan girdiye ulaşılamaz. Girdinin büyüklüğünün de bir önemi

yoktur. Genel olarak kullanılan SHA-256 fonksiyonunda bu sonucun uzunluğu 64 karakterdir. Girdideki en ufak bir değişiklik bile sonucu değiştirir.

"Merkeziyetsiz Toplum" girdisinin özeti (hash) şu şekildedir;

85dfe050a8de58e2d50a3eeaa05ee81dece5e0dc845ae1171bfbed4934fdf7f0

Sadece bir harfini değiştirelim "Merkeziyetsiz toplum" ;

180f3bfd04029b1e7160a5311779f9d57f76e6d5ca4576dcb2cbbe24ac31fa7d

"T" harfini "t" harfiyle bile değiştirdiğimizde sonuç tamamen değişti. Bu girdi çok büyük bir metin de olabilir. Yüzlerce sayfalık bir metinden tek bir harf bile değiştirsek sonuç farklı olacaktır. Özet Fonksiyonu'nun (Hash Algoritması) farklı türleri vardır ve dijital güvenlik alanında birçok yerde kullanılır. Bu sayede verinin gerçekliği kontrol edilebilir.

Blokzinciri üzerindeki bloklarda yer alan işlemlerin birindeki en ufak bir değişiklik bile bu özet alma işlemi sayesinde hemen fark edilir. Sonuçta oluşturulan blokların her biri bütün düğümlerde kayıtlıdır. Düğümün biri kayıtlı bloklardan birindeki bir işlemi değiştirmek istese bile diğer düğümlerde işlemin doğru şekli kayıtlı olduğundan sistem tarafından bu değişiklik reddedilir ve değişikliği yapan düğüm cezalandırılır.

İş Kanıtı (POW) ağında bu cezalandırma, o manipülasyonu yapan Düğüm'ün ağdan atılması şeklinde olur. Hisse Kanıtı (POS) protokolü ile çalışan ağlarda ise Düğüm'ün ağa katılmak için sisteme

yatırıp kilitlediği (stake ettiği) kripto parası yakılır. Her iki durumda da ağda manipülasyon yapmaya çalışan Düğüm, maddi olarak zarara girecek şekilde cezalandırılır. Büyük Blokzinciri ağlarında bu cezaların karşılıkları ciddi paralara ulaşabildiği için ve yukarıda da bahsettiğimiz gibi bir sonuca ulaşılamayacak olduğundan dolayı kimse böyle bir girişimde bulunmaz.

Blokzinciri henüz çok yeni bir teknolojidir. Ancak barındırdığı potansiyele bakıldığında, kamu veya özel sektör tarafında sunulan birçok ürün ve hizmetin bu teknoloji sayesinden çok daha güvenli bir şekilde sağlanabilmesi mümkündür.

2.4. Blokzinciri'nin Kullanım Alanları

Blokzinciri teknolojisi şüphesiz devrimsel özellikler sunmaktadır. Ancak bu teknolojinin her ortamda ve her koşulda kullanılması gerektiği anlamına da gelmemektedir. Blokzinciri'nin en büyük özelliği tarafların birbirine güven duyması gerekliliğini ortadan kaldırmasıdır. Bu nedenle böyle bir ihtiyacın olmadığı durumlarda bu teknolojinin kullanılmasının bir anlamı yoktur. Tarafların hali hazırda işleyen bir sistemleri varsa ve bu durum, birbirlerine güvene dayalı değilse o zaman bu teknolojinin o sistemde kullanılmasına da gerek yoktur. Blokzinciri, güven mekanizmasının taraflar arasında ciddi bir sorun teşkil edebileceği senaryolar için geliştirilmiş bir teknolojidir.

Satoshi Nakamoto Bitcoin manifestosunda bu duruma dikkat çekmektedir. İnsanlar merkez bankalarına güvenir. Paranın değerinin merkez bankaları tarafından korunacağına dair bir güvendir bu. Ancak merkez bankalarının doğru yönetilememelerinin neticesinden paranın değeri düşer ve bu da insanlara enflasyon olarak yansır. Sonuçta taraflar arası güvene dayalı kurulan mekanizmanın suiistimali neticesinde taraflardan birinin elindeki varlık değerini kaybeder ve zarara uğrayan taraf diğerine karşı olan güvenini kaybeder. Bir ülkede yaşayan bütün insanları ilgilendiren böylesi durumlar toplumsal huzursuzluklara ve hareketlenmelere neden olur. Satoshi, Bitcoin ile paranın arzını sınırlamış ve değiştirilmesini de neredeyse imkânız hale getirmiştir. Ayrıca para transferlerinin de bir merkeze güvenmeden yapılabilmesinin de önünü açmıştır. Böylece hem paranın üretiminde hem de transferinde tarafların birilerine güvenme gereksinimini ortadan kaldırmış, keyfiliğin veya doğru yönetememenin doğuracağı olumsuz sonuçların da önüne geçmenin yolunu bulmuştur.

Eğer veri, birden fazla aktör tarafından üretilmiyorsa veya okunmuyorsa da Blokzinciri'ne ihtiyaç yoktur. Mesela tedarik zincirlerinde Blokzinciri'nin kullanılmasında taraflar önemli faydalar sağlar ve bunun için çalışmalar yapılmaktadır. Özellikle uluslararası ticarette bir ürünün kaynaktan çıkıp hedefe ulaşana kadar birçok tarafın sürece dâhil olduğu bir mekanizma işlemektedir. Taşıma sürecindeki her bir aşamanın Blokzinciri'ne kaydedilmesi, tarafların bu kayıtları görüntüleyebiliyor olmaları ve bu süreçlerin tamamının makineler tarafından manipülasyona kapalı bir şekilde işletiliyor olması hem

güven hem de çoklu veri oluşturma/yazma/okuma gereksinimini karşılamaktadır. Eğer veri, tek bir kaynak tarafından üretiliyor ve başkasının da bu veriye erişime ihtiyacı yoksa Blokzinciri'nin kullanılmasına gerek yoktur.

Tarafların ürettikleri verilerin geriye dönük bir şekilde değiştirilmemesi veya silinmemesi gerekli durumlarda da Blokzinciri kullanılır. Bir önceki örnekteki gibi, hedeften kaynağa giden ürünün geçtiği her bir süreç sisteme kaydedilir ve bunun taraflardan biri tarafından değiştirilememesi gerekir. Mesela bir para transferinden transfer yapıldıktan sonra geri alınamaması veya miktarın sonradan değiştirilememesi gerekir. Blokzinciri bunu sağlar. Eğer sonradan değiştirilebilecek verilerin olduğu bir senaryo işleyecekse Blokzinciri bunun için uygun değildir.

Özetleyecek olursak Blokzinciri;

- Verinin birden fazla ortak tarafından üretildiği,
- Üretilen verinin değiştirilmemesinin gerektiği,
- Veri kayıt ortamının tek bir yerde bulunmasının sakıncalı olduğu,
- Üretilen ve kaydedilen veri ile ilgili taraflar arasında güven sorununun yaşandığı,
- Kaydedilen verinin bütün taraflar veya herkes için açık bir şekilde görüntülenmesinin gerektiği,

durumlar için uygundur diyebiliriz. Bu temel prensipler çerçevesinde bakıldığında Blokzinciri teknolojisinin kullanım alanlar her geçen gün yaygınlaşmaktadır.

Temelde üç çeşit Blokzinciri türü vardır. Açık Blokzinciri ağı herkese açık bir şekilde çalışır. Bağımsız ve merkezi otorite gerektirmeyen, isteyen herkesin ağa dâhil olabildiği ve ağ bilgilerine erişebildiği sistemlerdir. Yaygın şekilde kullanılan ve bilinen türü budur. Özel Blokzinciri sistemleri ise sadece izin verilen düğümlerin çalıştığı ve yine sadece izin verilen kullanıcıların verilere erişebildiği kapalı devre çalışan yapılardır. Merkezi bir otorite etrafında planlanır ve işletilir. Konsorsiyum Blokzinciri'nde ise her iki ağın karması olacak bir mimaride inşa edilir. Verinin açık olup olmadığı veya mutabakat mekanizmalarının nasıl düzenleneceği yine bir otorite tarafında belirlendiği sistemlerdir (ÜNAL & ULUYOL, 2020).

Bu çalışmada Açık Blokzinciri ağı üzerinde durulacaktır. Diğer iki kullanım alanı her ne kadar yenilikler getiriyor olsa da aslında var olan iş yapma yöntemlerine eklemlenerek mevcut sistemlerin daha güvenli hale getirilmesini sağlayan teknolojik gelişmelerdir ve bizim çalışma alanımız dışında yer almaktadır.

Açık Blokzinciri mimarisinin en önemli özelliği merkeziyetsiz bir yapıda olmasıdır. Bu şekilde birbirini hiç tanımayan insanlar bir araya gelir, güven mekanizmasını makinelere bırakarak iş yapabilme imkânına kavuşurlar. Bu güne kadar insanlar arasındaki güven mekanizmasını sağlama konusunda ya merkezi otoritelere veya üçüncü

şahıslara ihtiyaç duyuluyordu. Bu da insanlar arasında ciddi sorunların çıkmasına neden olabiliyordu. Ancak güven konusunda kaygısı kalmayan insanların çok daha verimli bir şekilde etkileşime girerek daha üretken sonuçlar çıkarabileceği dikkate alındığında bu yeni teknolojinin önemi daha da artmaktadır.

2.4.1. Bitcoin ve Diğer Kripto Paralar

Önceki bölümlerde de değindiğimiz gibi aslında dijital paralar üzerinde çalışmalar çok daha eskilere gitmektedir. Ancak, o zamanki teknoloji ve tecrübe birikiminin yetersiz olması nedeniyle bu tür girişimler başarısız olmuştur. Ancak bu girişimlerden elde edilen tecrübe ile 2008'de Satoshi tarafından Bitcoin'in geliştirilmesi mümkün hale gelmiştir. Satoshi'nin Bitcoin ile çözüm bulduğu en önemli sorunlardan birisi, sistemde çalışan düğümlerden birinin sistemi manipüle etmesinin önüne geçecek bir yöntem keşfetmiş olmasıdır. Çünkü Bitcoin, Açık Blozinciri yapısında olduğu için isteyen herkes sisteme dâhil olabilir ve bir düğüm çalıştırabilir. Ancak bu düğümlerden birisinin yapılan işlemleri manipüle ederek çifte harcama yapması, olmayan para ile harcama yapması, ya da yapılan bazı para transferlerinin içeriğini değiştirmesi mümkün olabilirdi. Ancak İşlem Kanıtı (POW) mutabakat protokolü ile bunun önüne geçilmiştir.

İşlem Kanıtı (POW) sisteminde böyle bir manipülasyon yapmak isteyen düğümün çok büyük harcamalar yaparak sistemdeki diğer düğümlerden çok daha fazla işlem gücüne sahip bir bilgisayar sistemi

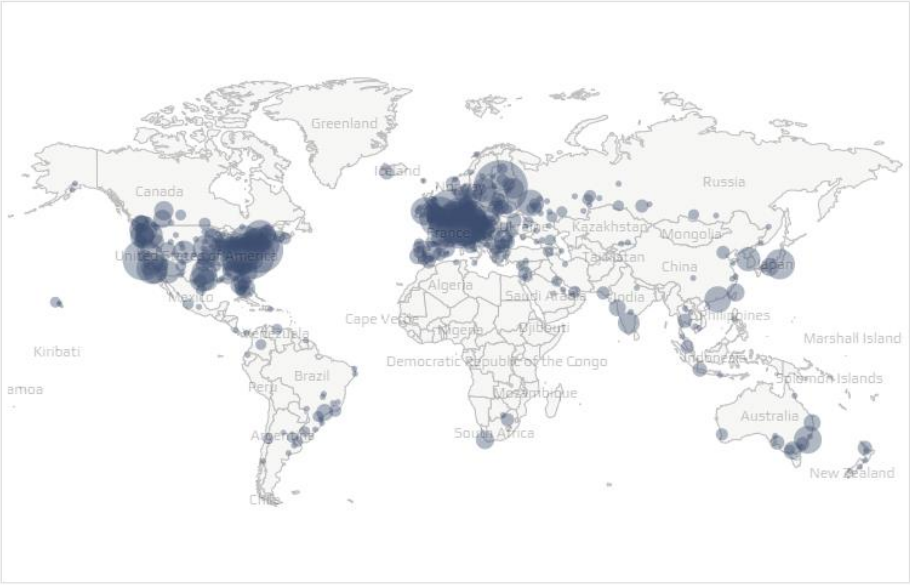
kurması gerekir (TAŞ & KİANİ, 2018). Bitcoin üreten, işlemleri onaylayan ve blok üreten düğümlerin bu işlemleri gerçekleştirmek için aralarında kurdukları mutabakatın temel argümanı işlem gücüdür. İşlem gücü yüksek olanın sözü daha çok geçer ama sisteme hükmedebilmesi için mevcut düğümlerin işlem güçlerinin toplamının yarısından bir fazla işlem gücüne ihtiyaç duyulur ki, bu da çok çok büyük bir bilgisayar sisteminin kurulması gerektiği anlamına gelir. Böyle bir işe kalkışmanın da bir anlamı yoktur. Kaldı ki böyle bir girişimde bulunulsa bile bu hilenin yapıldığı herkes tarafından görülecek ve Bitcoin'nin değeri hızlı bir şekilde düşecek, manipülasyonu yapan yine zarara uğrayacaktır. Düğümlerin dağıtık olması ve aralarında uzlaşma için işlem güçlerini kullanmaları sorunların çoğunun çözülmesine neden olmuştur.

Ayrıca böyle bir girişimde bulunulsa ve başarılı olunsa bile, o andan sonra Bitcoin ağında bir çatallanma olacaktır. Sistemdeki bütün düğümler, manipülasyonu yapan düğümden ayrılarak kendileri ikinci çatal olarak ağlarını manipülasyonun yapıldığı anın öncesinden devam ettireceklerdir. Manipülasyonu yapan düğüm veya düğümler kendi ağlarını işletirken, ayrılan diğer düğümler ise bozulan bloğu dışlayarak sistemlerini işletmeye devam edeceklerdir. Bu noktadan sonra da söz Bitcoin topluluğunda olur. Geniş kesim, birbirinden ayrılan ağlardan hangisini tercih ederse o ağ güçlenerek yoluna devam eder, diğer ağ ise zamanla kullanıcı ve değer kaybeder.

Bitcoin tarihinde farklı nedenlerle bazı çatallanmalar yaşanmıştır ama Bitcoin topluluğu, ağ üzerinde yapılmaya çalışılan değişikliklere

veya müdahalelere fazla teveccüh göstermemiş, değişiklik yapılmamış haliyle devam eden çatalı kullanmayı tercih etmişlerdir.

Benzer girişimler diğer Blokzinciri ağlarında da ara sıra görülmektedir. Ağın büyüklüğüne ve kullanıcı sayısına göre bu girişimler farklı sonuçlar doğurmuştur. Kısacası bir Blokzinciri ağının gücü, o ağı kullanan kullanıcıların yani ağ topluluğunun iradesine göre şekillenmektedir.



Şekil 2: Bitcoin düğümlerinin dünya haritası üzerinde konumlarının dağılımı

Bitcoin'nin çalışan düğümleri ile ilgili istatistikler yayınlayan bitnodes.io sitesinin verilerine göre Nisan 2024 tarihi itibariyle toplam 64014 düğüm bulunmaktadır.[10] Görselde bu düğümlerin dünya haritası üzerindeki konumlarının bir özeti gösterilmektedir. 143 ülkede 6990 şehirde dağıtık bir şekilde farklı kişiler tarafından işletilen bu düğümler, Bitcoin ağının güvenliğini sağlamaktadır.

Aynı zamanda madenci olarak da adlandırılan bu düğümler, hem işlemlerin onaylanmasını hem de blok kayıtlarının tutulması yanında Bitcoin üretimi de yapmaktadırlar. Bu nedenden dolayı madenci denilmektedir. Bitcoin üretimi de işlem gücüyle ilişkilidir. Bitcoin İş Kanıtı (POW) mutabakat protokolünde ağa gönderilen işlemler biriktirilir. Ortalama her on dakikada bir bu işlemler onaylanarak bloğun son zinciri olarak halkaya eklenir. Bu işlem esnasında düğümlere o anki zorluk seviyesine göre bir bulmaca verilir. Düğümler saf işlem gücü gerektiren bu bulmacayı çözebilmek için yüksek miktarda işlem gücü gerektiren hesaplamalar yaparlar. Bu bulmacayı ilk çözen düğüm cevabı yayınlar, diğer düğümler tarafından da bu cevap doğrulandığında bloğu zincire kaydetme hakkını o düğüm alır ve bunun karşılığında da Bitcoin kazanır (MENDİ & ÇABUK, 2018).

Bu şekilde ortalama her on dakikada bir Bitcoin üretilir. Bitcoin'in ilk zamanlarında her blokta 50 Bitcoin üretiliyordu yani düğümler (madenciler) her on dakikada bir 50 Bitcoin kazanmak için rekabete giriyorlardı. Bu miktar ortalama dört senede bir yarıya

[10] https://bitnodes.io/ erişim tarihi: 18.04.2024

düşürülür. Buna yarılanma (halving) denir. Mayıs 2020 deki son yarılanmada madenci ödülleri yani her on dakikada bir kazılan Bitcoin miktarı 6,5 Bitcoin'e düştü ve problemi çözme zorluğu iki katına çıkarıldı. Böylece düğümler arasında rekabetin artırılması ve Bitcoin arzının zaman yayılması planlamıştır. Bitcoin'in toplam arzı 21 milyondur. Nisan 2024 itibariyle üretilen toplam Bitcoin miktarı 19 milyonu geçmiştir.[11] Yarılanmalar neticesinde son Bitcoin'in en erken yüz yıl sonra kazılması beklenmektedir (FIRAT & DAŞDEMİR, 2021).

Zincire eklenen blok bütün düğümlerde aynı şekilde zincire eklenir ve bu şekilde bütün düğümler Bitcoin ağındaki bütün işlemlerin kayıtlarını tutarlar. Böylece çifte harcamanın da önüne geçilir. Yani biri bir para transferi yaptığında aynı para ile başka bir transfer yapamaz. İşlemler onaylanıp bloğa eklendiğinde artık o kişinin cüzdanında ne kadar Bitcoin'in kaldığını bütün düğümler bilmektedir. Bu nedenle cüzdan bakiyesini değiştiremez.

Düğümler hem madencilik yaparak yani blok üreterek (kazarak) hem de yapılan transfer işlemlerin komisyon alarak para kazanmaktadır. İşlem Kanıtı (POW) mekanizması, düğümleri dürüst çalışmaya teşvik eder. Burada Oyun Teorisi devreye girer ve sistemdeki düğümler maksimum rasyonel faydaya erişebilmek için sistemle uyumlu çalışmak zorundadır.

Oyun Teorisi ilk olarak John von Neumann ve Oskar Morgenstern tarafından ortaya atılmıştır ve John Nash tarafından

[11] https://coinmarketcap.com/tr/currencies/bitcoin/ erişim tarihi: 18.04.2024

geliştirilmiştir. Çok taraflı bir oyunda tarafların her birinin kendi kazançlarını maksimuma çıkaracak rasyonel kararlar verecekleri üzerine kutulu olan teori, düğümler arasındaki mutabakat ilişkilerini tarifte kullanılır. Eğer oyunculardan biri için geçerli olan en mantıklı oyun stratejisi diğer oyuncular için de en karlı oyun stratejisi ise buna Nash dengesi denir (METİN, 2014). Her bir düğüm için işlemlerden komisyon kazanmak ve ortaya atılan bulmacayı çözüp Bitcoin üretmek (kazmak, kazanmak) en mantıklı strateji olduğu için bütün düğümler bu amaç için çalışır. Aksi bir durum yani sistemi manipüle etmek veya işlemleri bozmaya çalışmak çok yüksek işlem gücü gerektirdiği ve bunu sağlamanın da çok maliyetli olduğu için mantıksızdır. Üstelik burada başarılı olunsa bile elde edilecek kazanç, harcanandan fazla olmayacaktır. Böylece Nash dengesi, Bitcoin ağını güvende tutmaktadır.

Bitcoin bir yazılımdır ve açık kaynak kodludur. Yani isteyen herkes bu yazılımı indirerek çalıştırabilir, Bitcoin ağında bir düğüm (Node) oluşturarak Bitcoin transferlerine ve üretimine katkıda bulunabilir. Ancak kazanç elde edebilmesi için bilgisayarının hesaplama gücünün yüksek olması gerekmektedir.

Bunun yanında yazılımın açık kaynak kodlu olması da bir başka güven artırıcı etkendir. Yani çalışan programın ne türde işlemler yaptığı herkes tarafından bilinebilmektedir. Günümüzde kullandığımız neredeyse bütün yazılımlar kapalı kaynak kodludur yani kullanıcı, uygulamanın geliştiricisine güvenmek zorundadır. Kullanıcı

uygulamayı kullanırken uygulamanın arka planda başka ne işler yaptığını bilemez. Bu durum uygulama geliştiricisinin kullanıcının aleyhine çalışabilecek kod parçacıklarını uygulamaya ekleyebilmesinin de önünü açar. Geliştirici böyle bir art niyet sergilemese bile uygulamayı geliştirirken yaptığı bazı kodlama hataları kullanıcı için bir güvenlik zafiyeti oluşturma potansiyeli barındırmaktadır. Bilgisayar virüsleri gibi zararlı yazılımların çoğu bu uygulamalardaki kodlama hatalarını suiistimal ederek yayılmaktadır.

Kontrolü, merkezi yapılardan veya kişilerden alıp dağıtık bir yönetişim biçimi oluşturmayı hedefleyen Blokzinciri'nde, kullanılan uygulamaların kapalı kaynak kodlu olması da beklenemez. Halka Açık Blokzinciri ağlarındaki uygulamalar açık kaynak kodludur. Bu sayede kullanıcılar uygulama geliştiriciye güvenmek zorunda kalmazlar. Aynı zamanda uygulamanın kodlarındaki hatalar da çok daha hızlı bir şekilde tespit edilip düzeltilir.

Kısacası Bitcoin, ilk halka açık Blokzinciri ağında çalışan ilk kripto para birimidir. Bitcoin, internet üzerinden insanların birbirlerine değer aktarmalarını kolaylaştırır. Dünyanın herhangi bir yerinde internete bağlı olan biri, kendi para birimini kullanarak Bitcoin alır, sonra onu alternatif yöntemlere nazaran oldukça ucuz ve hızlı bir şekilde yine dünyanın başka bir yerindeki birine gönderir. Sonra Bitcoin'i alan kişi de onu kendi para birimi üzerinden bozdurabilir. Böylece bir değer transferi gerçekleşmiş olur.

Yerel para birimlerine dönüştürülmeden de Bitcoin ile alışveriş yapmak mümkündür. Zaman içerisinde Bitcoin ile alışverişi mümkün kılacak uygulamalar yapılmıştır. Ancak Bitcoin'in günlük alışverişlerde kullanılması konusunda bazı eksiklileri vardır. Anlık para transferi yapılması gereken bir alışveriş için Bitcoin uygun değildir. Çünkü blokların oluşturulması ve onaylanması ortalama on dakika almaktadır. Bu da anlık transferi zorlaştırır. Mesela bir market alışverişinde bu durum oldukça kısıtlayıcıdır. Ayrıca her transfer için komisyon ödenmesi gerekmektedir. Ağdaki yoğunluğa göre bu transfer ücreti değişiklik göstermektedir. Bu nedenlerden dolayı Bitcoin'in her alışverişte kullanılması pek mümkün olmamaktadır. Bu eksikliklerin giderilmesi üzerine çalışmalar yapılmaktadır. Hali hazırda Bitcoin, daha çok uzak mesafelere para gönderimi veya bir değer saklama ve yatırım aracı olarak kullanılmaktadır.

Klasik bir para transferinde bankadan yapılacak işlem için defter açması istenir. Eğer bu işlem iki banka arasında yapılacaksa, her iki banka yapılacak işlem için defter açar ve işlemleri kendi defterlerine kaydederler. Bu defterler kapalıdır ve bankaların kontrolündedir. Yapılacak transferin banka tarafından onaylanması beklenir. Bitcoin'de ise işlemler halka açık bir defter üzerinde kayıtlıdır. Bankalarda hesap isimleri belli ama transferler gizli iken, Blokzinciri'nde isimler gizli, transferler açıktır. Yapılacak olan işlemlerin onaylanmasını ise dünyada dağıtık bir şekilde bulundan Düğümler (Node) yapar. Burada Düğümler kimden kime neyin gittiğine bakmaz. İşlemler kurallara uygun ise onaylarlar. Engelleme veya keyfe göre işlem kararı verme durumları

yoktur. Dine, dile, ırka, bölgeye, statüye bakılmadan işlemler gerçekleştirilir. İsteyen herkes bu ağda işlem yapabilir ve yine isteyen herkes bu ağda çalışan bir Düğüm (Node) işletebilir.

Bitcoin kamusaldır ve merkeziyetsizdir. İster işletilmesi olsun ister üzerinde gerçekleşen işlemler olsun, herkesin katılımına açıktır ve belirli bir kesim tarafından yönetilip yönlendirilemez. Dünyada farklı bölgelerde dağıtık şekilde bulunan Düğümler sayesinde de sistemin engellenmesi neredeyse imkânsızdır. Bitcoin ağına erişim zorlaştırılabilir ama engellenemez.

Bitcoin'in merkeziyetsiz ve kimsenin kontrolünden olmaması, Bitcoin'in fiyatı ile karıştırılmaması gerekir. Değişik zamanlarda Bitcoin fiyatları dünyadaki siyasi veya ekonomik durumlara göre değişiklik göstermektedir. Bitcoin fiyat bakımından manipülasyonlara açıktır. Ancak çalışma sistemi dışarıdan müdahalelere kapalıdır ve 2009 yılından beri kesintisiz çalışmaya devam etmektedir. Güncel para birimlerinde bir Bitcoin'in değeri sürekli değişiklik göstermektedir. Bu, Bitcoin'in bir değer saklama aracı olarak da kullanılmasından kaynaklanmaktadır. Bu sebeple "Dijital Altın" olarak da isimlendirilmektedir.

Bitcoin elbette mükemmel değildir. Teknik açıdan eksikleri vardır. Küresel bir para birimi olarak bakılacak olursa ihtiyacı tam olarak karşılayamaz. Fiyatı ise aşırı dalgalı bir seyir izlemektedir. Zaten Satoshi Nakamoto'da bunu vurgulamıştır. Bu bir denemedir. Ancak Bitcoin çok önemli bir şey yapmıştır. Kimsenin kimseye güvenmek

zorunda olmadığı, halka açık, sahibi olmayan, kendiliğinden çalışan bir para sisteminin mümkün olabileceğini göstermiştir. Aynı zamanda 2009 yılından beri böyle bir sistemin sorunsuz bir şekilde çalışabileceğini de ispat emiştir.

2.4.1.1. Alternatif Kripto Paralar

Bitcoin yazılımının açık kaynak kodlu olmasından dolayı birtakım geliştiriciler bu yazılım üzerinde bazı değişiklikler yaparak veya bu yazılımdan esinlenerek başka kripto para yazılımları kodlamışlardır. Böylece alternatif kripto paralar yani altkoinler ortaya çıkmıştır. İlk zamanlarda bu Bitcoin alternatifi kripto paralar aynı Bitcoin'de olduğu gibi kripto para oluşturma, saklama ve transfer işlemlerini farklı yöntemler ve teknikler kullanarak yapmaya çalıştılar. Mutabakat protokollerini, blok büyüklüklerini, blok oluşturma zamanını değiştirmek gibi değişiklikler yaparak alternatif çözümler ürettiler. Bunlardan bir kısmı halen çalışmakta olup bir kısmı da yeteri kadar kullanıcı bulamadığından dolayı uygulamaya son vermek zorunda kalmıştır.

2009 yılından itibaren birçok alternatif kripto para birimi ortaya çıkmıştır. Merkeziyetsiz bir şekilde para oluşturma, saklama ve transfer etmek için çok değişik teknikler kullanılmıştır. Ancak yine de Bitcoin bu alanda ezici bir üstünlüğe sahip durumdadır ve ilk çalışmaya başladığı günden itibaren neredeyse sorunsuz bir şekilde çalışarak gücünü ispat etmiştir. Hâlbuki Satoshi, Bitcoin'i duyurduğu

makalesinde Bitcoin'in bir test uygulaması olduğunu söylemiştir. Bu uygulamayı geliştirmek ve daha iyi hale getirmek için topluluktan yardım istemiştir. Satoshi'nin test aşamasında olduğunu söylediği Bitcoin, ilk zamanlar kaynak kodlarında yapılan bazı düzeltmeler sonrası hiç durmadan ve ciddi bir sorun yaşamadan günümüze kadar gelmiştir.

Alternatif kripto paralar, ilk etapta Bitcoin'deki eksikleri gidermek üzere çalışmışlardır. Blok büyüklükleri ve süreleri üzerinde değişiklikler yaparak daha hızlı para transferi yapmaktan, farklı mutabakat protokolleri üzerinde çalışan sistemler geliştirmeye kadar çok farklı denemeler yapılmıştır. Sonuçta değişik sorunlara değişik çözümler üreten binlerce alternatif kripto para projesi ortaya çıkmıştır. Özellikle de akıllı sözleşmelerin Blokzinciri üzerinde çalışmasını mümkün kılan uygulamalardan sonra işin rengi değişmiş, mesele sadece para transferi olmaktan çıkmıştır.

Bugüne kadar on binden fazla kripto para projesi piyasaya sunulmuştur. Akıllı sözleşmelerin bu sayının çokluğunda önemli katkısı vardır. Sonraki bölümlerde genel hatlarıyla inceleyeceğimiz, kripto paraların kullanım alanları sürekli olarak çoğalırken, her geçen gün yeni projeler piyasaya sürülmektedir.

Sayının bu kadar çok olması, haliyle de sorunları beraberinde getirmektedir. Suiistimaller, dolandırıcılıklar, siber saldırılar gibi birçok olumsuzluk yanında, kripto paraların değerleri üzerinde yapılan spekülasyon ve manipülasyonlar, bu alana yatırım yapıp destekleyen,

gelir beklentisinde olan kullanıcı ve yatırımcıları da zor durumda bırakmaktadır.

Kripto paraların merkeziyetsiz yapısı, bu alana devletlerin veya düzenleyici kurumların da müdahalesini zorlaştırmaktadır. Klasik finansal piyasalar için geliştirilmiş olan birçok düzenleyici ve denetleyici mekanizmalar, kripto para evreninde pek bir karşılık bulamamaktadır. Yine de devletler ve düzenleyici kurumlar, insanların bu alanlarda daha az zarar görmeleri için çalışmalar yapmaktadır.

2.4.1.2. Kripto Para ve Kripto Varlık Kavramı

Bitcoin ve diğer kripto paraların zamanla bir değeri oluşmuştur. Bu noktada ortaya çıkan şeyin bir para olup olmadığı iktisatçılar arasında tartışma konusu olmuştur. Paranın bir değişim aracı, tasarruf aracı ve aynı zamanda hesap birimi olduğunu vurgulayan bazı iktisatçılar, paranın bu özelliklerinden bazılarının kripto paralarda olmadığını vurgulayarak, başta Bitcoin olmak üzere diğer alternatif projeleri para olarak tanımlamazlar. Bir kısmı da kripto para olarak isimlendirilen bu enstrümanların değerlerindeki aşırı oynaklıktan dolayı bunları şans oyunu veya kumar olarak tanımlamaktadırlar (ATİK, KÖSE, & YILMAZ, 2021).

Kripto paralar, itibari paralarda olduğu gibi arkasında bir devlet erki ve desteği olmadığı için klasik para kavramına uymamaktadır. Ancak sosyolojik açıdan değerlendirdiğimizde “paranın arkasında bir

devlet desteği olmalı mıdır?" sorusunu sormamız gerekir ki, bu noktada paranın iktisadi bir olgu olmasının yanı sıra aynı zamanda sosyolojik bir olgu olarak da değerlendirilmesi gerektiği gerçeğiyle karşılaşırız. Bu konu ile ilgili değerlendirmeler çalışmanın ilerleyen bölümlerinde daha detaylı bir şekilde incelenecektir.

Kripto paraların bu isimle anılmasının nedeni oluşturulmasından transferine kadar her aşamasında kriptografik algoritmalar kullanılmasından dolayıdır. Satoshi'nin Bitcoin'i geliştirmesindeki temel güdü, paranın kontrolünün kurumlardan ve kuruluşlardan alıp halka devretmekti. Bu sebeple tüm para süreçlerini halka mal edecek bir sistem geliştirmiştir. Sonuçta para denilen şeyin her ne kadar iktisadi tanımları olsa da asıl olan şey insanların ona yükledikleri anlamdır.

Günümüzde kullandığımız itibari para birimlerinin değerleri yani alım güçleri, iktisadi veya siyasi birçok değişkenle belirlenmektedir. Birçok ülke tarafından benimsenen serbest piyasa sisteminin dengeleri, ülkelerde kullanılan para birimlerinin birbirlerine göre değerlemelerini de belirler. Burada devletlerin ve para politikalarını belirlemek üzere yetkilendirilmiş kurumların politikaları, para birimlerinin değerlerini etkileyen başat faktörlerdir. Hâlihazırdaki para sisteminin yapısı ciddi ulusal ve uluslararası hukuki düzenlemelerle belirlenmiştir. Kriptografik paralarda ise belirli bir kontrol mekanizması olmadığından dolayı, devletlerde ve para politikalarının yönlendirilmesinde yetkili kurumlarda bu konuda bir kafa karışıklığı devam etmektedir.

Hal böyle iken, Blokzinciri'nde para transferini belli şartlara bağlı olarak tanımlamaya çalışan akıllı sözleşmelerin ortaya çıkması ve bu alanda her geçen gün farklı çözümlerin piyasaya sunulmasıyla birlikte mesele sadece "para" olmaktan çıkmıştır. Bu noktada yine bazı otoriteler bu yeni olguya da "kripto varlık" demeyi daha uygun bulmaktadırlar.

Kripto paralar Blokzinciri ağları üzerinde hem para yani ödeme aracı hem bir değer saklama aracı hem de yatırım aracı olarak kullanılmaktadır. Kripto paraların bir varlık mı, menkul değer mi yoksa emtia mı olduğu ile ilgili tartışmalar ise halen devam etmektedir. Bu çalışmada ise, ödeme aracı olarak kullanıldığı durumlarda kripto para, ödeme aracı haricinde yatırım amaçlı kullanıldığı durumlarda ise kripto varlık kavramının daha uygun olması nedeniyle bu şekilde bir kullanım tercih edilmiştir.

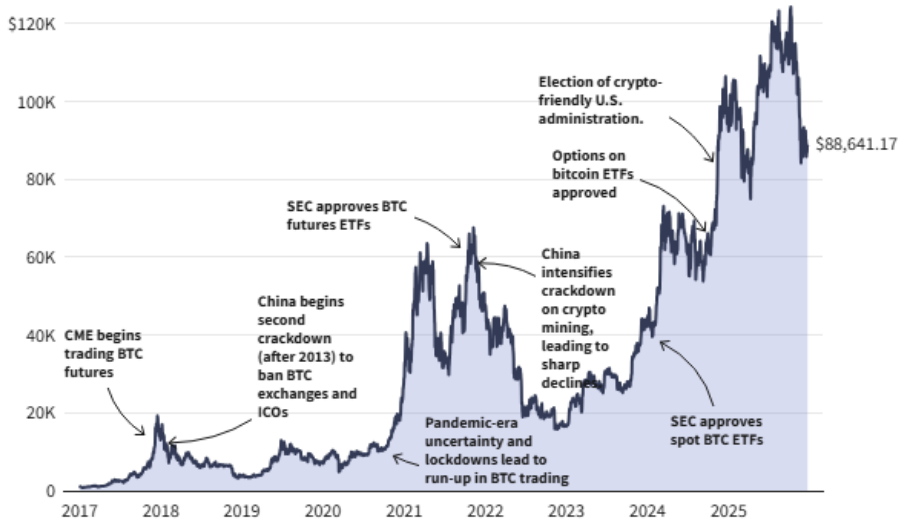
İster bir Blokzinciri ağı olsun ister herhangi bir ağ üzerinde çalışan bir uygulama olsun, yatırımcılar bir projenin kripto para ekosistemine katkı sağlayacak bir teknolojisinin olduğuna inanırlarsa, bu projenin kripto parasını satın alarak yatırım yapmaktadır. Böylece o kripto para değer kazanmakta ve aynı zamanda bir kripto varlığa da dönüşmüş olmaktadır. Durum karışık gibi görünse de yeri geldiğinde para, yeri geldiğinde bir menkul değer, yeri geldiğinde de emtia gibi davranan bir olgu ile karşı karşıya olduğumuzu söylemek daha doğru olacaktır.

Bütün bu gelişmelere rağmen kripto paraların günlük hayatta henüz çok fazla kullanım alanı olduğu söylenemez. Örneğin, günlük hayatın kaçınılmaz bir parçası olan market alışverişlerinde kripto paralar kullanılmamaktadır. Kripto paralar, şu an için büyük oranda Blokzinciri ağlarında yapılan işlemlerde kullanılmaktadır. Kripto paraların gündelik hayatta kullanılmasıyla ilgili çalışmalar ve denemeler elbette olmuştur ama bu konuda tam bir başarı sağlanamamıştır. Bunun en önemli sebebi ise kripto paraların değerlerinin çok değişken olmasıdır. Kripto paraların aynı zamanda bir yatırım aracı olarak da kullanılması fiyatlarının da değişken olmasına yol açmıştır. Çünkü, kısa zamanda fiyatı ciddi değişiklere uğrayabilen bir varlıkla alışveriş yapmak pratikte çok verimli olma şansına sahip değildir. Yoksa teknolojisi bakımından kripto paraların alışverişlerde kullanılmasına sorun teşkil edecek büyük eksiklikleri yoktur.

Bitcoin'e para değeri kazandıran ilk işlem Ekim 2009 da Hall Finly'in Martti Malmi'ye 5050 Bitcoin'i 5 Dolar karşılığı satması olmuştur. Bu satışta 1 Bitcoin 0,0009 Amerikan Doları'na karşılık gelmiştir. Bitcoin'in ilk defa bir alışverişte kullanılması da 2010 yılının Mayıs ayında gerçekleşmiştir. ABD 'de yaşayan Laszlo Hanyecz adında bir kişi o dönem değeri 41 dolar olan iki büyük boy pizza siparişi vermiş ve ödemeyi Bitcoin olarak yapmıştır. İki pizzaya toplamda 10.00 Bitcoin ödenmiştir. Buradan yola çıkarak o dönem için Bitcoin'in değerinin 0,0041 Dolar olduğunu söylemek mümkündür (Ashmore & Powell, 2023).

İlk zamanlar Bitcoin madenciliğinin hobi olarak yapılması nedeniyle Bitcoinler çok kolay bir şekilde üretiliyor ve elden ele dolaşıyordu. Bu nedenle de pek bir değeri yoktu. İlk dönemlerde ortalama on dakika içerisinde bir blok üretiliyor ve karşılığında 50 Bitcoin madencilere dağıtılıyordu. İlk zamanlar işlem zorluğu seviyesi düşüktü ve sıradan bilgisayarlarla bile Bitcoin madenciliği yapılabiliyordu. Arzı çok fazlaydı ve kullanım alanları oldukça sınırlıydı. Bu nedenle belirli bir fiyatının olmaması da doğaldı. Ancak sunmuş olduğu alternatif imkanlar nedeniyle tanınması kısa sürdü ve geniş kitleler tarafından kabul görmeye başladı.

İlk Bitcoin borsası olan bitcoinmarket.com 2010 Mart ayında açıldı ve sonrasında diğer borsalar sırasıyla açılmaya devam etti. Bitcoin'in alınıp satılmaya başladığı bir borsanın oluşmasıyla birlikte değeri de artmaya başlamış ve 2011 yılı sona ermeden değeri 1 Dolar'ın üzerine çıkmıştır. Aşağıdaki grafikte de görüldüğü gibi Dolar karşısında Bitcoin'in değeri çok dalgalı bir seyir takip etmiştir (EDWARDS, 2025). Ekim 2025'te tarihi zirvesi olan 126.200 Dolar'a ulaşmıştır. Böylece Bitcoin, Amerikan Dolar'ı karşısında muazzam bir değer artışı göstermiştir.



Şekil 3: Bitcoin'in Amerikan Doları karşısındaki fiyat grafiği

Bitcoin fiyatının 69bin Dolar seviyesine ulaştığı günde, bütün kripto varlıkların piyasada dolaşımda olan miktarlarının toplam değerini belirleyen Kripto Toplam Piyasa Değeri (Coin Market Cap) verisi, dolaşımda olan kripto varlıkların toplam değerini 3 trilyon Dolar'ın üzerine çıktığını göstermiştir (OSSINGER, 2021).

Kripto varlık ekosisteminin değerinin bu derece artmasına rağmen diğer para piyasalarının yanında market hacminin düşük kalması, çok sayıda kripto projesinin olması ve bu alandaki kanuni düzenlemelerin yetersiz olmasından dolayı fiyat oynaklıkları fazlaca görülmektedir.

Blokzinciri teknolojisi, kripto varlıklara devletlerin müdahalesini zorlaştırmaktadır. Bu sebeple oluşan kanuni boşluklar da bazı zamanlar kripto varlık yatırımcılarının ve kullanıcılarının mağdur olmalarına neden olmaktadır. Siber saldırılar ve dolandırıcılık olayları kripto varlık piyasasında sıkça görülen durumlardır. Bu tarz olumsuzluklar da insanların bu alana yönelmesini engelleyen durumlar olarak karşımıza çıkmaktadır. Her şeye rağmen hem dünyada hem de ülkemizde bu alana yönelik kanuni düzenlemeler yapılmaya çalışılmaktadır.

Avrupa Birliği Parlamentosu tarafından 20 Nisan 2023 tarihinde onaylanan ve 2024 yılında yürürlüğe giren MiCA (Kripto Varlık Piyasalarının Düzenlenmesi) kanununda, Blokzinciri üzerinde üretilen değerler "kripto varlık" olarak tanımlanmaktadır. Bu düzenleme ile Avrupa Birliği kripto varlıkları üç ana guruba ayırmış ve kripto varlık hizmet sağlayıcıları ile ilgili düzenlemeler yapmıştır.

Ayrıca ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) Ocak 2024 tarihinde spot Bitcoin Borsa Yatırım Fonu (ETF) başvurularını onaylama açıklamasında da yine "kripto varlık" kavramını kullanmış ama bu konuda tam bir tanımlama bu tarih itibariyle halen yapılamamıştır. Kripto varlıkların menkul kıymet mi, emtia mı yoksa başka bir finansal olgu mu olduğu henüz netleşmemiştir.

Ülkemizde de "Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik" başlıklı bir düzenleme, 16 Nisan

2021 tarihinde 31456 Sayılı Resmi Gazete'de yayımlanmıştır. Yönetmelikte kripto varlık şu şekilde tanımlanmaktadır;

> Dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydî para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder.[12]

Bu yönetmelik uyarınca kripto varlıkların doğrudan veya dolaylı olarak ödeme aracı gibi kullanılması yasaklanmıştır.

Kripto varlıklar üzerinde tartışmalar ve düzenlemelerle ilgili çalışmalar devam ederken 2021 yılında El Salvador, Bitcoin'i resmi para birimi olarak tanıyarak, bir ilke imza atmıştır. Böylece Bitcoin ilk defa bir ülkede resmi para birimi statüsü kazanmıştır.

2.4.1.3. Koin (Coin) ve Token (Jeton) Kavramları

Bir Blokzinciri ağından, kullanılmak üzere oluşturulan kripto paraya Koin denir. Bir kripto paranın Koin olarak adlandırılabilmesi için kendine ait bir Blokzinciri ağının olması gerekir. Bir de var olan bir Blokzincir ağı üzerinde inşa edilen yan uygulamalarda kullanılmak

[12] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik - https://www.resmigazete.gov.tr/eskiler/2021/04/20210416-4.htm erişim tarihi: 11.01.2024

üzere üretilen kripto paralar vardı ki bunlara da Token denir.[13] Koin'in kendine ait bir Blokzinciri ağı varken Token, bu Blokzinciri üzerinde çalışan uygulamanın para birimini tanımlar.

Yekpare bir Blokzinciri ağı kurmak, topluluğunu oluşturmak ve düğümleri çoğaltıp güvenliği/güvenilirliği sağlamak zor bir iştir. Yeniden bir ağ kurmak yerine var olan bir ağın alt yapısını kullanarak uygulama geliştirmek daha pratik ve verimli olabilir. Böylece koskoca bir ağı kurmak ve işletmek gibi sorunlarla uğraşılmamış olur. Bu sebeple Blokzinciri ekosistemi, kendi ağına sahip olanlar veya bir ağın altında çalışanlar olarak ikiye ayrılmıştır.

Bitcoin'in kendi Blokzinciri ağı vardır ama bu ağ üzerinde başka bir uygulamanın çalışmasını desteklemez. Bunun yanında Ethereum da bir Blokzinciri ağıdır ama bu ağda başka uygulamaların tasarlanıp çalışmasına izin verir. Ethereum ağının Koin'i yani para birimi Ether'dir. Bu ağda çalışan uygulamalar, ağda yaptıkları tüm işlemler için Ethereum düğümlerine yani madencilere, Ether cinsinden komisyon ödemesi yapmaktadır. Bunun yanında da kendi çalışma alanlarında kendi Tokenlarını kullanarak işlemlerini gerçekleştirektedirler.

Örnek verecek olursak, Uniswap, Ethereum ağında çalışan merkeziyetsiz bir kripto varlık takas borsasıdır. Burada kullanıcılar Ethereum ağında çalışan uygulamaların Tokenlarını takas edebilirler. Bu takas işlemi için cüzdanlarında takas etmek istedikleri varlıkları

[13] https://www.btcturk.com/bilgi-platformu/kriptopara-cryptocurrency-jeton-token-ve-koin-coin-nedir-aralarindaki-farklar-nelerdir/ erişim tarihi: 16.02.2023

bulundururlar. Anlaşılan fiyat üzerinden takas gerçekleşir ve işlem komisyonu da Ether cinsinden ödenir.

Avalaunch, Polkadot, Solana gibi daha birçok Blokzinciri ağı varken, bu ağların altında çalışan binlerce alt uygulama ve bu uygulamaların Tokenları vardır.

2.4.2. Akıllı Sözleşmeler (Smart Contracts)

Şimdiye kadar ele aldığımız konu ve açıklamalar, Satoshi'nin finansal sistemdeki yozlaşmaya tepki olarak ortaya koyduğu Bitcoin'in, deneme aşamasında olan bir prototip olsa bile dünya çapında büyük ilgi gördüğünü ortaya koymuştur. Satoshi'nin çözdüğü sorunlar sayesinde Blokzinciri sistemi, bu konu üzerine ilgi duyan kişileri cezbetmiştir. 2013 yılında henüz 19 yaşında olan Vitalik Butarin isimli genç bir bilgisayar programcısı, Ethereum adını verdiği Blokzinciri projesini duyurmuştur. O zamana kadar Bitcoin kopyası birçok kripto para ortaya çıkmıştı ancak Buterin, Blokzinciri ağı üzerinde akıllı sözleşmeler yazarak, bunların dağıtık bir şekilde çalıştırılabileceği fikrini ortaya atmıştır. Ethereum 2014 yılında kitle fonlaması yoluyla fon toplamış ve 2015 Temmuz ayında İş Kanıtı (POW) mutabakat protokolüyle çalışan kendi Blokzinciri ağını işletmeye başlamıştır.

Kâğıt üzerindeki sözleşmelerin bilgisayar kodlarına dönüştürülerek saklanması ve işletilmesini öngören akıllı sözleşme (smart contrats) kavramı ilk olarak 1994 yılında Nick Szabo tarafından

ortaya atılmıştır. Bu sayede kâğıt üzerinde kayıtlı sözleşmelerin işlemesi sırasında insanlardan kaynaklanan hataların ortada kaldırılması hedeflenmekteydi. Ancak akıllı sözleşmelerin kayıtlı olduğu bilgisayarlar da merkezi bir sisteme bağlı oldukları için, programlara müdahale edilmesi mümkün olacağından çok bir fark yaratmayacaktı (DURSUN, 2020).

Blokzinciri bu noktada sunduğu dağıtık işlem platformu hizmeti sayesinde, merkezi sunucularda çalışan programlara müdahale dilmesi gibi durumların önüne geçebilmektedir. Bitcoin de aslında bir akıllı sözleşmedir ama işlevleri kısıtlı ve ek işlevlerin tanımlanması imkânsızdır. Başta nasıl tasarlandıysa o şekilde çalışmaktadır. Akıllı sözleşmeleri destekleyen Blokzinciri ağlarında ise ağ sadece bir kayıt mekanizması olarak çalışmaz. Aynı zamanda bir nevi dağıtık bilgisayar gibi çalışır. Yani kodlanıp ağda çalıştırılan bir akıllı kontrat, tek bir bilgisayarda değil, dağıtık bir şekilde birçok düğüm (madenci, node) üzerine çalışır. Bu yüzden nasıl kodlanmışsa o şekilde çalışır ve sonradan müdahale edilemez, durdurulamaz. Kodlama aşamasında ne şekilde tasarlandıysa o şekilde işlemeye devam eder. Eğer koduna sonradan müdahaleye imkân veren bir tanımlama eklenmemişse, o uygulamanın tasarlandığı şeyi yapması ancak bütün Blokzinciri ağı kapatılarak engellenebilir.

Akıllı kontrat çalıştırma özelliği bulunan Blokzinciri ağları, Bitcoin gibi ağlara nazaran çok daha karmaşık ve katmanlıdır. Bu sebeple hatalar ve sorunlar daha çoktur denilebilir. Ethereum ağı

2015'ten bu yana geliştirilmeye devam edilmektedir. Ethereum Vakfı koordinasyonunda yapılan bu geliştirme ve güncelleştirme işlemleri, Ethereum topluluğu tarafından desteklenirse ağa uygulanabilir. Bu noktada bütün düğümlerin yani madencilerin, yapılan değişiklikleri desteklemeleri ve çalıştırdıkları düğümlerde bu güncellemeleri yapmaları gerekir.

Ethereum ağındaki en radikal güncelleme 2022 Eylül ayında gerçekleşmiştir. Merge adı verilen bu güncelleme sayesinde Ethereum ağı, İş İspatı (POW) mutabakat protokolünden Hisse Kanıtı (POS) mutabakat protokolüne geçiş yaptı. Yani madenci olarak tanımlanan Ethereum düğümü çalıştıranlar, işlem gücü sağlamak için pahalı donanımlar kullanmak yerine, belirli bir miktar Ether kripto parasını sisteme yatırarak (stake ederek) madencilik yapmaya devam edebilmektedir. Böylece Donanım maliyetlerinden ve elektrik faturalarından da tasarruf edilmiş olacaktır. Bu güncellemeyi ağın çok büyük bir kısmı desteklediği için Ethereum ağı artık bu sistem üzerinde çalışacaktır. Sistemin bu şekilde çalışabilmesinin nedeni ise çoğunluk tarafından desteklenmesidir.

Akıllı sözleşmeler, Blokzinciri ağı üzerinde çalışan programlardır. Taraflar arasında kararlaştırılan şartlar, programcılar tarafından kodlanarak Blokzinciri ağına eklenmektedir. Akıllı sözleşmelerin de kripto para cüzdanları vardır. Bu cüzdana aktarılan kripto para, sözleşmenin işleyişine göre bir hesaba aktarılabilir. Akıllı sözleşmeler sayesinde taraflar arsında yapılan anlaşmaların, tarafların

birbirine veya üçüncü bir tarafa güven duymak zorunda kalmadan işletilmelerini sağlamaktadır (TEVETOĞLU, 2021).

Mesela bir yardım organizasyonu için oluşturulan bir akıllı sözleşme uygulaması tasarladığımızı varsayalım. Yardımlar akıllı sözleşmenin cüzdan adresine gönderilecektir. Sözleşmenin koduna yardımların belirli bir tarihe kadar kabul edileceği, bu tarihte belirlenen bir miktarın üzerinde yardım toplanmışsa, toplanan tüm paranın yine önceden belirlenmiş olan ihtiyaç sahiplerinin hesaplarına transfer edileceği eğer belirlenen miktar toplanmazsa da yardım hesabına para gönderen hesaplara, gönderdikleri miktarın geri transfer edileceği kodlanmış olsun. Akıllı sözleşmeler açık kaynak kodlu olduğu için herhangi bir gizli işlem yapılması mümkün olmayacaktır. Sözleşme Blokzinciri ağına aktarılıp çalıştırıldığında, müdahaleye kapalı bir şekilde kodlanmışsa çalışması, belirlenen tarihe kadar engellenemeyecek veya yönlendirilemeyecektir. Böylece yapılacak olan yardım faaliyeti kimseye güven duymaya gerek kalmadan, makineler üzerinden kendiliğinden çalışacak ve tamamen şeffaf bir şekilde, dış müdahaleye kapalı bir biçimde işleyecektir.

Özetle akıllı sözleşmeler sayesinde, kripto varlıkların bir hesapta tutulması veya transfer edilmesi sonradan müdahale edilemeyecek ve şeffaf olarak tasarlanan iş yapma biçimleri üretilebilmesinin önünü açmaktadır. Akıllı sözleşmeler sayesinde kripto paralar, oldukça geniş bir uygulama alanı kazanmaktadır. Akıllı sözleşmelere, programlanabilen para demek de doğru bir tanımlama olacaktır. Sadece

bir hesaptan bir hesaba transfer edilen para olgusu, transfer şartlarını belirli koşullara bağlayan ve insan müdahalesine kapalı otonom uygulamalarla zenginleştirilmektedir.

Burada mevzuyu sadece para transferine bağlamak da biraz sınırlayıcı bir bakış açısına neden olabilir. Akıllı sözleşme teknolojisi, merkeziyetsiz uygulamaların da üretilebilmesinin önünü açması açısından önemlidir. Akıllı sözleşmeler keyfi uygulamaların önüne geçme konusunda etkili bir çözümdür. Bu açıdan, akıllı sözleşmelerin merkeziyetsiz, otonom ve sonradan müdahaleye kapalı yapısı, bu çalışmanın son bölümünde ele alacağımız toplumsal sözleşme teorisine de yeni bir yorum getirmemizi mümkün kılacaktır.

2.4.3. Merkeziyetsiz Uygulamalar (DAPPS)

Bilgisayar programları, programlama dilleri ile kodlanarak üretilmektedir. Programlama, yapılmak istenen işin niteliğine bağlı olarak oldukça karmaşık süreçler ve kodlamalar içerebilir. Bunun için de ticari işletmeler kurulur ve çalışanlar istihdam edilerek finansal kaynaklar temin edilir. Bilgisayar programı sektörü, zamanla bilgisayarların da gelişmesiyle birlikte ciddi bir iş alanı haline gelmiştir.

Firmalar ürettikleri programlardan gelir elde etmek için, yasalarla belirlenen lisanslama ilkeleri çerçevesinde, ürünlerini lisanslayarak pazarlamakta ve buradan gelir elde etmektedirler. Bu noktada firmaların ürettikleri programların kodlarını ticari bir sır olarak

saklamaları, rakiplerinden korumaları doğaldır. Bu sebeple üretilen programlar, satış aşamasına geldiğinde programlama dilleri editörleri tarafından derlenerek çalışan bir uygulamaya dönüştürülmektedir. Son müşteriye satılan uygulama budur. Yani müşteri, programın derlenmiş ve paketlenmiş çalışan halini kullanır. Ticari kaygılardan dolayı son kullanıcı kullandığı programın kaynak kodlarını göremez.

Bu durum ticari firmaların haklarını koruyan bir yöntem olsa da son tahlilde kullanıcının para verip aldığı ürünün içeriğine tam olarak hâkimiyet kurmasını engellemektedir. Kullanıcı, kullandığı programın kodlarında ne olduğunu bilemez, sadece programın çalıştığında ortaya çıkarttığı sonucu görebilir. Eğer programcı tarafından programın kodlarına art niyetli bazı eklemeler yapılmışsa, kullanıcının bunu bilmesi neredeyse imkânsızdır yani programcıya (firmaya) tam olarak güvenmesi gerekir.

Kaynak kodların kullanıcılar tarafından görülememesi durumu güvenlik, şeffaflık, birlikte çalışabilirlik, esneklik ve yerelleşme gibi sorunları da beraberinde getirmiştir (CASSON & RYAN, 2006). Kullanıcıyı edilgen bir durumda tanımlayan bu yaklaşıma karşılık 1980-1990'lı yıllarda Özgür Yazılım ve Açık Kaynak Kodlu Yazılım kavramları geliştirildi. Açık Kaynak Kod Lisansı kapsamında yazılımın telif hakkı sahibi, yazılımın kaynak kodlarını da programla birlikte sunmaktadır. Böylece isteyen kişi programın kodları üzerinde izleme ve değiştirme hakkına sahip olmaktadır (LAURENT, 2004).

Blokzinciri teknolojisinin temel kavramlarından birinin güven olmasından dolayı, bu ekosistemde faaliyet gösteren neredeyse bütün uygulamalar Açık Kaynak Kod ilkesini temel almaktadır. Amaç kimseye güvenmek zorunda olmamak olduğu için, geliştiriciler projelerinin kaynak kodlarını da halka açarlar. Böylece kullanıcı kullandığı uygulamanın tam olarak ne yaptığından haberdardır. Blokzinciri projelerinde geliştiriciler klasik yöntemle yani program satarak değil, projelerinin kalitesinin yarattığı katma değer üzerinden kazanç elde ederler. Var olan bir soruna doğru çözümler üreten iyi tasarlanmış bir proje, insanlar tarafından kabul görür, kendi topluluğunu oluşturur ve bu topluluk zamanla büyür. Düzgün çalıştığı zamanla tescillenirse hem geliştirici hem kullanıcı hem de yatırımcı toplar. Böylece projenin Koin'i veya Token'ı değerlenmiş olur.

Proje geliştiricileri, henüz tasarım aşamasındayken bütün sürecin nasıl işleyeceğini ve aşama aşama neler yapılacağını White Paper denilen bir yol haritasında detaylıca anlatırlar. Bitcoin ile başlayan bu uygulama, kripto para sektöründe bir nevi temayül haline gelmiştir. Böylece geliştiriciler, projelerinin ne amaca hizmet edeceğini, ne gibi hedeflerinin olduğunu, süreç içerisinde nelerin ne zaman yapılmasının planlandığı gibi detaylı bilgileri diğer kullanıcılarla paylaşmaktadır. Bu ön bilgilendirme taslağını okuyan insanlar da uygun buldukları projelere yatırım yaparak destek olmakta ve süreç içerisinde o projenin başarılı olup yatırımlarının değerlenmesini beklemektedirler.

White Paper denilen bu taslak içerisinde o projede üretilecek toplam kripto para miktarı da belirtilmektedir. Hatta belki de en önemli kısımlarından birisi budur. Bu kısımda zamanla üretilecek olan kripto paranın ne amaçlarla kullanılacağı da ayrıca belirtilmektedir. Toplamda üretilecek kripto para miktarının bir kısmını da çalışmalarını finanse etmek için kendi hesaplarına ayırarak bunu da projenin kaynak koduna eklemektedirler. Klasik yazılım satma yönteminden farklı şekilde işleyen bu mekanizmada, proje çalışmaya başlayıp değerlendikçe, geliştiricilerin kendileri için ayırdıkları kripto paranın da değeri artmakta ve geliştiriciler buradan gelir elde etmektedirler. Bu durum, bir şirketin kendi çalışanlarına şirketin hisse senetleriyle ödeme yapması gibi düşünülebilir.

Programların kaynak kodlarının halka açılmasının bir başka faydası da, diğer programcıların o kodları geliştirerek farklı uygulamaları kısa zamanda üretebilmelerinin yolunu açmasıdır. Bu sebepledir ki Bitcoin'in yayınlanmasından hemen sonra, Bitcoin kodları üzerinde çalışan yazılımcılar birçok benzeri proje ortaya koymuşlardır. Blokzinciri ekosisteminin bu denli hızlı büyümesinin en büyük etkenlerinden birisi de projelerin kaynak kodlarının açık olmasıdır.

Sadece bir değer transfer aracı olarak çalışan Blokzinciri ağları, akıllı sözleşmelerin geliştirilmesiyle birlikte çok değişik işlevler kazanmışlardır. Akıllı sözleşmelerle birlikte varlık transferleri şartlara bağlanabilir hale gelmiştir. Bu şartları kontrol eden şey ise dağıtık

bilgisayarlar üzerinde çalışan Merkeziyetsiz Dağıtık Uygulamalar (DAPPS)' dır.

Klasik bir yazılım, bir bilgisayar üzerinde çalışır. Bu yerel bir bilgisayar olabileceği gibi bir sunucu bilgisayar sistemi de olabilir. Her halükarda merkezi bir sistemde çalışır. Merkeziyetsiz uygulamalar ise üzerinde çalıştıkları Blokzinciri ağının düğümlerinde çalışırlar. Bir diğer ifadeyle, belirli bir bilgisayarda değil, birçok bilgisayar üzerinde çalışırlar. Bu sayede programın çalıştıktan sonra durdurulması söz konusu değildir.

Merkeziyetsiz uygulamaların bu mimarisi, kullanıcıların akıllı sözleşmelere güvenmesini sağlar. Çünkü, sözleşme işlemeye başladığında eğer uygulamaya bu yönde kodlar eklenmemişse, insan müdahalesine kapalıdır. Uygulamayı durdurmak için Blokzinciri ağındaki çok sayıdaki bilgisayarı durdurmak gerekmektedir. Şayet kaynak kodlarında bir hata yapılmamışsa dağıtık yapısından dolayı siber saldırılara karşı da oldukça güvenlidir.

Merkeziyetsiz uygulamaların dağıtık yapısı, bu uygulamaları siber saldırılara karşı koruduğu gibi sansüre karşı da korur. Değişik coğrafyalarda çok sayıda bilgisayar üzerinde dağıtık bir şekilde çalıştığı için merkezi otoriteler tarafından engellenmesi de neredeyse imkânsızdır.

Merkeziyetsiz uygulamalar, akıllı sözleşmelerin kullanım alanlarının çeşitlenmesine de katkı sağlar. Front-End denilen uygulamanın kullanıcı ile etkileşime girdiği kısmı, herhangi bir

programlama dili ile kodlanırken, Back-End denilen uygulamanın arka planında çalışan kısmı, bir Blokzinciri ağı yazılımı ile kodlanmaktadır. Bu sayede kullanıcı, normal şekilde tasarlanmış bir program kullanıyormuş hissi ile çalışırken, aslında arka planda Blokzinciri altyapısı üzerinde, akıllı sözleşmeler dağıtık bir şekilde işlem yapmaktadır. Front-End uygulamalarının sağladığı kolaylık sayesinde kullanıcılar, aracıya ihtiyaç duymadan doğrudan birbirleriyle bağlantıya geçebilmektedir.

Ayrıca Merkeziyetsiz uygulamalar, her ne kadar bir programcı ekip tarafından yazılsa da çalışmaya başladıktan sonraki süreçler o uygulamanın topluluğu tarafından yönetilmektedir. Yazılımcı ekip, merkeziyetsiz uygulamayı kodlarken grup ilkelerini de göz önünde bulundururlar. Çünkü uygulama çalışmaya başladığında eğer kodlarında bir güncelleme yapılacaksa, bu değişiklik o projeye yatırım yapan topluluğun değişikliği oylayıp onaylamasıyla mümkün olmaktadır. Merkeziyetsiz uygulamalarda kodların açık olması kadar, topluluğun ne kadar söz sahibi olduğu da bir o kadar önemlidir. Çünkü, topluluğu önceleyen projeler daha fazla rağbet görmektedir.

Merkeziyetsiz kavramının geçtiği hemen her yerde, “topluluk” kavramı da karşımıza çıkmaktadır. Her ne kadar proje bir grup tarafından geliştirilse de, o projenin değerlenmesi için bir topluluğa ihtiyacı vardır. Bu topluluk o projeye inanıp, proje ürünü olan uygulamayı kullananlardan ve projeye yatırım yaparak gelir elde etmeyi amaçlayanlardan oluşmaktadır. Bir Blokzinciri projesini ayakta tutanlar,

geliştiriciler ve onu kullanan topluluktur. Geliştiriciler ve topluluk arasındaki etkileşim, karşılıklı fayda çerçevesinde ilerlemektedir. Katılımcı sayısı arttıkça topluluk genişlemekte ve dolayısıyla proje değerlenmektedir. Böylece hem geliştirici hem yatırımcı olanlar bu gelişmeden kazanç sağlamaktadır.

Blokzinciri projeleri kendi topluluklarını oluşturmak için değişik stratejiler geliştirebilirler. Bu sayede uygulamanın kullanıcıları ve yatırımcıları edilgen taraf olmaktan çıkıp, projenin gelişim yönünü de etkileyebilen konumuna gelmektedirler. Bu durum, merkeziyetsizliğin getirdiği bir sonuçtur. Merkeziyetsizlik, topluluğun fikrinin değerli olmasını, topluluğun görüşünün de alınmasını beraberinde getirmekte, kullanıcıyı edilgen durumdan etken duruma taşımaktadır.

Merkeziyetsiz uygulamalar, Blokzinciri ağlarının kabiliyetlerini ve kullanım alanlarını genişletmektedir. Bunun, merkeziyetsiz oyunlardan sosyal medya uygulamalarına, merkeziyetsiz finansa kadar birçok alanda halihazırda çalışan örnekleri vardır ve geliştirilmeye de devam edilmektedir. Henüz çok yeni bir alan olması sebebiyle, zamanla farklı uygulamaların merkeziyetsiz alternatiflerini görmemiz de mümkün olacaktır. Bu alanda çalışan geliştiricilerin ortak amacı, merkezi bilgisayarlarda çalışan uygulama ve hizmetlerin, merkeziyetsiz alternatiflerini üretmektir.

Merkeziyetsiz uygulamaların sağladığı avantajlar yanında dezavantajları da vardır. Henüz yeni bir teknoloji üzerine kurulu olduklarından dolayı zamana ihtiyaçları vardır. Kaynak kodların açık

olması, kodlamada yapılan hataların da art niyetli kişiler tarafından görülmesine neden olur. Bu da gerekli kontroller yapılmadan hizmete sunulan uygulamaların, siber saldırılara uğramalarına neden olabilmektedir. Ayrıca üzerinde çalıştıkları Blokzinciri ağlarının da olumsuzluklarından etkilenmektedirler. Topluluk yönetimlerinde yaşanan anlaşmazlıklar da bazen sorunlara neden olmaktadır.

Merkeziyetsiz uygulamaların, geleneksel iş yapma, organizasyon kurma ve örgütlenme biçimlerimizi değiştirme potansiyeline sahip oldukları söylenebilir. Son yıllarda gelişen bilgisayar teknolojileri sektörü bile, geleneksel iş yapma biçimlerimizle organize edilmektedirler. Diğer bir ifadeyle, Merkeziyetsiz uygulamalar, merkezi belirli bir grup tarafından yönetilen, yönlendirilen ve işletilen kurum/kuruluş ve organizasyon biçimlerine alternatif bir organize biçimidir. Başta Blokzinciri'nin kendisi olmak üzere, bu teknoloji ile geliştirilen merkeziyetsiz uygulamalar, klasik yönetişim biçimini değiştirme potansiyeline sahiptir. Blokzinciri teknolojilerinin sağladığı imkânlar sayesinde, yeterli yetkinliğe sahip herkes, kendi organizasyonunu kurup işletebilir ve mekândan bağımsız bir şekilde kurduğu bu organizasyona topluluk oluşturabilir. Ayrıca, kitle fonlaması yöntemleri sayesinde de projesine dünyanın dört bir yanından kolayca kaynak bulabilir.

Devam eden bölümlerde de ele alacağımız gibi burada sadece ticari değil, herhangi bir toplumsal organizasyondan bahsedilmektedir. Önemli olan, kurulacak organizasyonun yönetişim biçiminin,

katılımcıların da dâhil olacağı etkileşimli bir model olmasıdır. Merkeziyetsiz uygulamaların, sivil toplum kuruluşlar, siyasi partiler, finansal ürünler veya ticari girişimler gibi çok fazla alanda kullanılabilme potansiyeli vardır. İlerleyen dönemlerde, iş yapma, organizasyon kurma ve toplumsal örgütlenme biçimlerinin, merkeziyetsiz uygulamalar sayesinde farklı bir boyuta taşınabilme potansiyeli oldukça yüksektir.

2.4.4. Merkeziyetsiz Finans (DEFI)

Her ne kadar Bitcoin ile birlikte alternatif merkeziyetsiz bir para sisteminin mümkün olduğu kanıtlanmış olsa da Bitcoin sadece para üretimi, saklanması ve transferini mümkün kılacak bir teknolojidir. Aslında bu bile başlı başına bir finansal sistemdir ancak günümüz finansal sistemi her ne kadar para üzerine kurulu olsa da buna ek olarak parayla ilgili daha birçok araç ve hizmet içermektedir.

Merkez bankaları ve ticari bankalar, sigorta ve aracı kurumlar, borsalar, finansal kiralama şirketleri, varlık yönetim şirketleri, yatırım ortaklıkları, yatırım fonları ve risk sermayesi şirketleri, ilk etapta sayabileceğimiz finansal hizmet veren bazı yapılardır. Özellikle son bir yüzyılda, sadece bankalardan bu derece geniş ve karmaşık bir iş alanı haline gelen finansal hizmetler, merkezi yapıların kontrolünde işleyen bir yapıya sahiptirler Merkezi kurum ve kuruluşların, bazen daha fazla kâr amaçlı, bazen de siyasal kaygılarla yaptıkları hatalar bu sektörün hizmet verdiği bütün iş alanlarında ekonomik sorunlara yol açmaktadır.

ABD'de konut kredilerinin fazla şişmesi nedeniyle başlayan ve dünyaya yayılan 2008 Dünya Ekonomik Krizi bunun en bariz örneklerden biridir. Merkez bankasının piyasadaki likiditeyi bollaştıran para politikası ve konut kredisi veren finansal kuruluşların daha fazla kar beklentisiyle özensiz davranmaları gibi birçok etken bir araya gelerek, dünyayı etkileyecek ve etkisini halen hissetmeye devam ettiğimiz bir ekonomik krize neden olmuştur (AKBULUT, 2010).

Taraflar arasındaki finansal sözleşmelerin yapılması ve işletilmesinde geleneksel finansal yapılar yüzyıllardır aracılık faaliyeti yürütmektedir. Bu finansal kurumların güçlenmesi ve merkezileşmesi, gelişen dijital sistemlerin de etkisiyle artık sorgulanmaya başlamıştır. Özellikle de Blokzinciri teknolojisinin gelişmesi ve bilhassa akıllı sözleşmelerin kabiliyetlerini artması, bu geleneksel finans sistemlerine alternatif bir merkeziyetsiz finansın mümkün olabilirliği üzerine tartışmaları başlatmıştır (PARLAR, 2022).

DEFI, finansal işlemlerin merkeziyetsiz Blokzinciri ağları üzerinden yapılabilmesini sağlayan, belirli bir otoritenin güvencesi altında sunulmayan ürün ve hizmetleri tanımlamaktadır (MERAKLI, 2021). Burada merkeziyetsiz uygulamalar ve akıllı sözleşmeler ana uygulayıcı unsurlardır. Bir aracıya ihtiyaç duyulmaz ve işlemler eşten eşe doğrudan yapılabilmektedir. Henüz çok daha yeni olan bu alanda her geçen gün yeni ürünler ve hizmetler ortaya çıkmaktadır. Geleneksel finansal kurumlara tam bir rakip olması henüz mümkün olmasa da hızla büyüyen bir ekosisteme sahiptir. Bu hızlı büyümenin en büyük

tetikleyicisi ise uygulamaların açık kaynak kodlu olarak geliştirilmesidir. Ayrıca internetin fiziki sınırları ortadan kaldırma gücüyle birlikte insanların mesafelerden bağımsız şekilde bir araya gelerek iş yapabilme kabiliyetlerini geliştirmeleri, merkeziyetsiz finans ürünlerinin hızla çoğalmasına katkı sağlamaktadır.

Bununla birlikte DEFI'nin geleneksel finansal sisteme alternatif olması da gerekli değildir. Özellikle internetin hızlanması ve yaygınlaşmasıyla birlikte, bir internet ekonomisinden söz edilebilir. İnternet ekosistemindeki ekonomik faaliyetlerin finansmanında, geleneksel finansal kuruluşlar yetersiz kalmaktadır. Geleneksel finansın yetersiz kaldığı bu alanlarda da DEFI, alternatif bir finansal unsur olarak kendini konumlandırabilme potansiyeline sahiptir.

DEFI ürünlerinin sunduğu hizmetlerin bazı önemli avantajları vardır;

Erişilebilirlik: DEFI platformları, internet sayesinden dünyanın her yanından kolayca ulaşılabilir konumdadırlar. Blokzinciri teknolojisinin dağıtık yapısı sayesinde, erişilebilirlik kabiliyetleri daha da artmaktadır. Tam merkeziyetsiz çalışan bir Blokzinciri ağının, kural koyucu merkezi otoriteler tarafından engellenmesi neredeyse imkânsızdır. Merkeziyetsizlik idealinin temel amaçlarından biri de zaten budur. Ancak halihazırdaki birçok Blokzinciri ağı, daha fazla kitleye daha kolay ulaşabilmek için, merkezi otoritelerle anlaşmalar yaparak, merkeziyetsizliklerinden tavizler vermektedir.

Bu merkezi otoriteler, bazen regülasyonlar (yasal düzenlemeler) uygulayan hükümetler, bazen de büyük bilişim şirketleri olabilmektedir. Erişilebilirlik kabiliyetlerini artırmaya çalışan Blokzinciri ağlarının, bu amaçla merkezi otoritelerle girdikleri uzlaşmacı yaklaşımlar, hem bu ağların hem de bu ağlar üzerinde çalışan uygulamaların merkeziyetsizlik özelliklerini sekteye uğratmaktadır.

Merkezi finansal yapıların sundukları ürün ve hizmetlere ulaşım, bağlı oldukları ülkelerin uyguladıkları regülasyonlar nedeniyle zordur. Mesela Türk bir yatırımcı, Amerikan borsasında yatırım yapmak istediğinde, bir sürü yasal engeli aşmak zorunda kalır. Ancak DEFI ürün ve hizmetlerine ulaşmak için sadece internet bağlantısının olması ve bir kripto para cüzdanı edinmek yeterli olmaktadır. Erişilebilirlik, DEFI ürün ve hizmetlerinin hızlı bir şekilde değerlenip büyümelerini de tetiklemektedir.

Şeffaflık: Blokzinciri teknolojisinin, önceki bölümlerde de bahsettiğimiz gibi en önemli özelliği şeffaf olmasıdır yani ağ üzerinde yapılan işlemlerin herkes tarafından görülebilmesidir. Hem açık kaynak kod ilkesiyle geliştirilen uygulamalar hem de zincir üstü verilerin herkese açık olması, sistemi şeffaf ve güvenli kılmaktadır.

Blokzinciri ağı üzerinde işlem yapacak herkesin mutlaka bir kripto cüzdanı olması gerekmektedir. Cüzdanların sahiplikleri gizlidir ama cüzdanlar arası yapılan transferler şeffaftır. Böylece gizli işlemlerin yapılması engellenmektedir. Üstelik zincir üzerinde geriye dönük olarak

da bütün işlemler açık bir şekilde incelenebilmektedir. Sistem üzerinde geriye dönük değişiklik yapılması da mümkün değildir.

Ancak önceki başlıkta da bahsettiğimiz gibi, kimi Blokzinciri ağlarının merkezi otoritelerle yaptıkları bazı işbirlikleri, Blokzinciri ağlarının şeffaflık ilkesine de zarar vermektedir. Terörün finansmanı veya kara para ile mücadele gibi gerekçelerle, hükümetlerin uyguladıkları regülasyonlara, bazı Blokzinciri ağları uyum sağlamaktadır.

Bu ağlar, zincir üzerinde yapılan kimi transferleri engellemekte, yapılan transferleri durdurmakta, geri almakta veya cüzdan sahiplerinin kişisel bilgilerini merkezi otoritelerle paylaşmaktadırlar.

Güvenlik: Mevzubahis finansal işlemler olunca, en önemli önceliklerden birini de güvenlik oluşturmaktadır. DEFI ürünlerinin, hem açık kaynak kodlu olması hem de Blokzinciri ağının sağladığı sağlamlık sayesinde, güvenlik seviyeleri oldukça yüksektir. Bu özellikler sayesinde, merkezi bir finansal ürünün karşılaşabileceği güvenlik sorunları, DEFI ürünleri için çok daha az tehdit oluşturmaktadır. Tabi ki hiçbir dijital ürün için tam bir güvenlikten bahsedilemez. Sadece güvenliği en üst seviyeye çıkarmak için sürekli bir çalışma yapılabilir.

Dijital verilerin güvenliği, dijital ürün ve hizmetlerin yaygınlaşmasıyla paralel bir şekilde, her geçen gün daha da fazla önem arz etmektedir. Dijital güvenlik, bilişim sektöründe önemli ve büyük bir

yer tutmaktadır. Özellikle finansal ürün ve hizmetlerin güvenliğini üst seviyeye çıkarmak için çok fazla emek ve para harcanmaktadır.

Merkezi finansal yapıların güvenliğinin sağlanması, merkeziyetsiz finansal yapılara göre çok daha zordur. Verilerin merkezi sistemlerde tutulması, o merkezleri ulaşılması kolay hedefler haline getirmektedir. Bu merkezlerin güvenliğini sağlamak da haliyle oldukça maliyetli olacaktır. Blokzinciri ağlarının dağıtık yapısı, verilerin güçlü şifreleme yöntemleriyle farklı noktalarda depolanması, siber saldırılara karşı verileri korunaklı tutmaktadır.

Bununla birlikte, merkezi sistemlerde çalışan uygulamalar kapalı kaynak kodludur. Kapalı kaynak kodlu yazılımlarda ki güvenlik açıklarının tespiti zordur ancak böyle bir zafiyetin art niyetli kişiler tarafından tespit edilmesi, o sistemin uzun süre fark edilmeden istismar edilmesinin önünü açar. Açık kaynak kodlu uygulamalarda ise güvenlik zafiyetlerinin tespiti daha kısa sürede gerçekleşir.

Ancak günümüzde bazı DEFI ürünleri, gerekli güvenlik taramaları yapılmadan çalıştırılmaktadır. Açık kaynak kodlu bu ürünlerdeki güvenlik zafiyetleri kolayca tespit edilip istismar edilmektedir. Kripto para sektöründe bu şekilde çok fazla istismar gerçekleşmekte ve insanlar mağdur olmaktadır. Burada sorun sistemde değil, gerekli tedbirleri almayan geliştiricilerdedir.

Bunların dışında, DEFI alanında dolandırıcılık olayları da sık sık görülmektedir. Bu alanda yasal düzenlemelerin tam olarak yapılamamış olması ve düzenlemeler yapılsa bile, erişilebilirliğin kolay olmasından

dolayı dolandırıcılıkların önü kolay kolay alınamamaktadır. Bu alanda yatırım yapan insanların kolay yoldan zengin olma arzusuyla hareket etmeleri, onları dolandırıcıların tuzaklarına kolayca düşmelerindeki en önemli etkendir. Ayrıca DEFI ürünlerinin sıradan kullanıcılar için karmaşık denebilecek kullanım deneyimi, kullanıcıların hatalar yapmalarının da en önemli sebeplerinden biridir.

Çok hızlı gelişen, rekabetin üst seviyede olduğu bir ortamda güvenliği sağlamak, hem üretici hem de kullanıcı açısından zorluklara neden olmaktadır.

Verimlilik: DEFI ürün ve hizmetlerinden en büyük beklenti, işlemlerin hızlı ve ucuz bir şekilde yapılmasıdır. Geleneksel finans sisteminde sınır ötesi bir para transferi günler sürerken, Blokzinciri üzerinde birkaç saniye veya birkaç dakikada bitmektedir.

DEFI ürün ve hizmetleri, üzerinde çalıştıkları Blokzinciri ağının verimlilik kabiliyetine bağlıdır. Mesela Ethereum ağındaki transferler, Solana ağına göre daha yavaş ve daha pahalıdır. Ancak Solana ağındaki bu verimlilik artışı, ağda bazı güvenlik sorunlarına da neden olmaktadır. Verimlilik meselesi, Blokzinciri ağlarının üzerinde çalıştıkları en büyük sorunlardan biridir.

Erişilebilirlik, şeffaflık, güvenlik ve verimlilik başlıklarında DEFI ürün ve hizmetlerinin önemli avantajları vardır. Bu avantajlar, insanların merkezi finansal yapılara olan bağımlılıklarını önemli ölçüde azaltma potansiyeli içermektedir. Günümüzde, hem bireysel hem de toplumsal açıdan değerlendirildiğinde, merkezi finansal yapılara büyük

bir bağımlığımızın olduğu görmekteyiz. Merkez bankalarından, özel finans kurumlarına kadar uzanan bu bağımlılık düzeyi, her geçen gün de genişlemektedir. Merkez bankalarının uyguladıkları para politikaları, tüm ülkenin hatta bazen de dünyanın ekonomik düzenini etilerken, özel finansal kurumlardan bağımsız bir şekilde yaşam sürdürmek veya ticaret yapmak neredeyse imkânsız bir hal almıştır.

Bu açıdan DEFI ürün ve hizmetleri, şuan için tam bir alternatif olmasa bile, merkezi finansal sisteme karşı, hem bireylerin hem de toplumların elinde alternatif bir imkân olarak kendini göstermektedir. Borç alma ve verme, takas alım ve satım, türev ürünler, varlık yönetimi, sigorta ve ödeme gibi birçok alanda DEFI çözümleri mevcuttur. Henüz çok yeni olan DEFI'nin, bazı hizmet alanları aşağıda ele alınacaktır.

2.4.4.1. Kripto Para Borsaları

Kripto paraların en büyük özelliklerinden biri eşten eşe aracısız bir şekilde transfer edilebilmesidir. Ancak akıllı sözleşmelerin kullanım alanları genişledikçe alternatif kripto para birimleri de çoğalmıştır ve şu an sayıları binlerle ifade edilmektedir. Bu alternatif kripto paralara yatırım yapmak isteyen veya kimi servislerin sunduğu hizmetlerden yararlanmak için o servisin kripto parasına sahip olmak isteyen kişilerin doğrudan birbirlerine ulaşıp ellerindeki kripto paraları değiş tokuş etmeleri oldukça zordur. Dolayısıyla bu ihtiyacı karşılamak ve takası kolaylaştırmak için kripto para ürünlerinin takas edildiği borsalar kurulmuştur.

İlk kripto para borsaları merkezi yapıda kurulmuştur. Bu borsalarda elindeki Koin veya Token'ı takas etmek isteyen kişiler hesap açmak zorundadır. Çoğu merkezi kripto para borsasında işlem yapmak isteyen kullanıcılar, gerçek kişi olduklarını doğrulamak için kimlik doğrulama işlemleri yapmak zorundadır. Bu zorunluluğun sebebi, borsaların devletlerin kara paranın aklanması ve terörün finansmanı ile ilgili düzenlemelerine takılıp engellenmek istememeleridir.

Kimlik doğrulaması yapan kişi, bankadaki hesabından kripto para borsasındaki hesabına geleneksel para birimlerinden birini transfer edebilir, borsadaki hesabında bu para ile istediği bir kripto parayı takas edebilir. Borsadaki cüzdanında tuttuğu bu kripto parayı başka kripto paralarla takas edebilir, başka bir kripto para cüzdanına transfer edebilir ve burada herhangi bir DEFI ürününde harcayabilir. Genel prosedür bu şekilde işlemektedir.

Bu takas ve alışverişlerden dolayı kripto paraların değerleri de piyasa koşullarına göre değişmektedir. Kripto ekosistemindeki sorunlara iyi çözümler sunan kaliteli projelerin Koin veya Tokenları değerlenirken, gözden düşen projelerin Koin ve Tokenları yani kripto paraları değer kaybetmektedir. Bu değer değişimlerinden para kazanmak isteyenler de bir yatırım aracı olarak kripto paralara rağbet etmektedir. Kripto paralar hem bir yatırım aracı hem de o Blokzinciri uygulamasında kullanılan bir enstrüman olarak değerlendirilmektedir.

Merkezi kripto para borsalarında kullanıcıların ayrı ayrı cüzdanları vardır ama o cüzdanların özel (gizli) anahtarları borsanın

elindedir. Yani kullanıcı borsaya güvenmek zorundadır. Geçmişte birçok örnekte olduğu gibi o borsa siber saldırıya uğrayabilir veya borsanın yöneticileri tarafından kullanıcıların hesaplarındaki kripto paralar amacı dışında kullanılabilir hatta çalınabilir. Merkezi borsaların böylesi büyük riskleri vardır ama kullanım kolaylığı nedeniyle oldukça rağbet görmektedir.

Bugün itibariyle dünyanın en büyük merkezi kripto para borsası olan Binance'ın spot işlemlerde günlük hacmi 30 milyar dolar, türev ürünlerde ise 70 milyar dolar civarındadır. Ağustos 2022 itibari ile spot işlemlerde en yüksek seviye olan günlük 70 milyar dolar ve 90 milyon kullanıcıya ulaşılmıştır. Bu borsada şimdilik 350'den fazla Koin ve Token listelenirken haftalık ziyaretçi sayısı da 16 milyon civarındadır.[14]

Merkezi borsalardaki güvenlik endişelerinden dolayı merkeziyetsiz kripto para borsaları kurulmuştur. Bu borsalar tamamen Blokzinciri üzerinde çalışan merkeziyetsiz uygulamalar olarak hizmet vermektedir. Kullanıcı kişisel kripto para cüzdanını bu borsaya bağlayarak yapmak istediği takas işlemini borsaya bildirir ve uygun fiyat üzerinden anlaştığı başka bir kullanıcı ile takası gerçekleştirir. Merkeziyetsiz borsalar sadece aracılık hizmeti sunmaktadır. Kullanıcının kripto parası kendi cüzdanında durmaktadır. Dolayısıyla borsanın kullanıcının kripto parası üzerinde herhangi bir tasarruf yetkisi yoktur. Ayrıca merkeziyetsiz borsaların yazılımları da açık kaynak kodlu olduğu için işlemler şeffaf bir şekilde yürür. Borsa, kullanıcının

[14] https://coinmarketcap.com/tr/rankings/exchanges/ erişim tarihi: 26.04.2024

kendisine herhangi bir güven duyma zorunluluğu hissetmeden takas işlemini gerçekleştirmesine aracılık eder. Karşılığında da komisyon alır.

Merkeziyetsiz borsalar merkezi borsalara nazaran işlemlerin gerçekleşme süreleri ve işlem emirlerinin sisteme iletilme süreleri gibi bazı teknik konularda biraz zayıf kalmaktadır. Ayrıca kullanıcı yapılan takas işleminde borsaya verdiği komisyonun yanında bir de kullandığı Blokzinciri ağına da transfer ücreti verdiği için takas işlemi merkezi borsalara göre daha pahalı gerçekleşebilir. Ayrıca işlemin gerçekleşebilmesi için cüzdanın borsaya o anda bağlı olması gerekir. Yani bir kullanıcı o anlık fiyat üzerinden değil de eğer bekleyen bir fiyat emri verdiyse o emrin gerçekleştiğinde transferin yapılabilmesi için bilgisayarın açık durumda olması gerekmektedir. Bu nedenlerden dolayı sıklıkla takas işlemi yapan kullanıcılar güvenlikten taviz vererek merkezi borsaları tercih etmektedirler.

Merkezi borsalar hem yazılım hem donanıma büyük yatırımlar yapmak zorundadır. Bu nedenle klasik finansal kurumlara benzerler. Bir saklama hizmeti verdiklerinden dolayı bu yatırımları yapmak zorundadırlar. Ayrıca iş yüklerinin fazla olmasından dolayı çok sayıda kişiyi de çalıştırmak zorundadırlar. Ancak merkeziyetsiz borsalarda durum çok daha farklıdır. Ortada çalışan sadece bir yazılım olduğu için geliştiriciler bütün enerjilerini bu yazılımın geliştirilmesi üzerine odaklayabilirler. Dolayısıyla merkezi borsalara göre daha az sayıda personelle işlerini sürdürebilirler.

Bugün itibariyle en büyük merkeziyetsiz kripto para borsası olan Uniswap'ın günlük işlem hacmi 2 milyar dolar civarındadır.[15]

Borsaların kripto para piyasasının gelişmesine katkıları çok büyüktür. Bu aracı kurumlar sayesinde kripto para piyasası ihtiyacı olan likiditeye ulaşır ve böylelikle projelerin finansmanı sağlanmış olur. Geleneksel finansal araçlara (borsalar, tahvil, bono, emtiya ve forex piyasaları vb.) nazaran oldukça sığ bir piyasa olsa da kripto paraların popülaritesi her geçen gün artmakta ve dünyada sadık bir kullanıcı kitlesi edinme konusunda emin adımlarla ilerlemektedir. Kripto para borsaları ise Kripto para ekosisteminin tanınırlığın artması konusunda önemli roller üstlenmektedir.

2.4.4.2. Likidite Madenciliği (Yield Farming)

Likidite Madenciliği, elinde kripto para bulunduran kişilerin bu varlıkları başkalarına kredi olarak vermesine, piyasaya likidite sağlamasına denir (MERAKLI, 2021). Bu işlem bankaların kredi vermesine benzer ancak burada eşten eşe doğrudan çalışan bir sistem vardır. Bu işleme Blokzinciri üzerinde çalışan borsalar aracılık etmekte ve işleyiş akıllı sözleşmeler üzerinden yürütülmektedir.

Kullanıcı merkezi veya merkezi olmayan borsalardaki likidite havuzlarına likidite ekleyerek bu havuzlardaki takas ücretlerinden ve

[15] https://coinmarketcap.com/tr/rankings/exchanges/dex/ erişim tarihi: 26.04.2024

ikincil piyasalarda gerçekleşen işlem ücretlerinden para kazanır.[16] Kullanıcıların asıl amacı pasif gelir elde etmektir. Gelirler günlük veya belirli periyotlarda hesaplarına yatmaktadır.

Kullanıcı bu havuzlara yatırdığı kripto parası karşılığı bir Token alır. Belirli bir süreliğine bu yatırılan kripto para kilitlenir. Bu süre içerisinde faiz geliri elde ederken aynı zamanda sistem tarafından verilen Token'ın değeri artarsa buradan da gelir elde edebilir.

Bir kullanıcının elindeki kripto parayı bir başka kullanıcıya faiz karşılığı vermesi olarak özetleyebileceğimiz likidite madenciliği, akıllı sözleşmeler üzerinden yürüdüğü için sisteme müdahale edilmesi imkansızdır. Ancak merkezi borsaların güvenlik sorunları veya merkeziyetsiz borsa da olsa kodlamada yapılan hatalardan dolayı saldırıya uğraması gibi durumlardan dolayı kullanıcılar zarar görebilmektedir. Ayrıca kullanıcının sisteme yatırdığı kripto paranın zaman içerisinde değerinin düşmesi veya likidite sağlama karşılığı aldığı Token'ın değerinin düşmesi gibi durumlarda da kullanıcının zarara uğraması mümkündür.

2.4.4.3. Kitle Fonlaması (ICO – Initial Coin Offering)

Geleneksel finansta, girişimciler veya hali hazırda bir girişimi bulunan firmalar projelerine ek kaynak sağlamak adına kitle fonlaması

[16] https://www.bybit.com/tr-TR/earn/liquidity-mining#mining erişim tarihi: 17.02.2023

yöntemlerini kullanırlar. Bu şekilde ya girişimlerini hayata geçirmek veya büyütmek için ihtiyaç duydukları likiditeye ulaşmayı amaçlarlar. Geleneksel kitle fonlamasının birçok yolu ve yöntemi vardır ve hukuki birçok bağlayıcılığı mevcuttur (YAVUZ & SUYADAL, 2020).

Blokzincir tabanlı kitle fonlamasında ise Blokzinciri ağında proje geliştiren girişimcilerin, projelerine kaynak sağlamak amacıyla fon toplamasına ICO denir (MERAKLI, 2021). Fonlama amacıyla duyuruya çıkan proje sahipleri, çalışmalarını ve yol haritalarını açıklayan detaylı bir kaynak hazırlarlar. Genellikle web siteleri üzerinden yayınladıkları bu kaynaklarla yatırımcıları bilgilendirirler. Yatırımcılar projeleri değerlendirip yatırım yapmaya değer gördüklerinde, ellerindeki kripto parayı o projenin cüzdanına gönderir ve karşılığında o projenin Koin veya Token'ından alırlar.

Bu şekilde girişimciler kaynak edinmek karşılığında projelerinin bir kısım hissesini yatırımcılara devretmiş olur. Bu işlem, bir nevi geleneksel şirket ortaklığı gibi düşünülebilir. Proje hayata geçip çalışmaya başladığında eğer rağbet görürse projenin değeri artar. Bu da o projeye yatırım yapıp karşılığında Koin veya Token alan yatırımcının elindeki varlıkların değerlenmesine yani para kazanmasına neden olur. Bu şekilde halka arz edilen Koin veya Tokenları hisse senedi gibi değerlendirmek mümkündür (YAVUZ & SUYADAL, 2020).

Bu yöntemle girişimciler çok daha geniş bir kitleden çok daha kısa bir sürede fon toplayabilirler. Girişimci dünyanın dört bir yanından fon toplayabileceği gibi yatırımcı da herhangi bir yasal engele

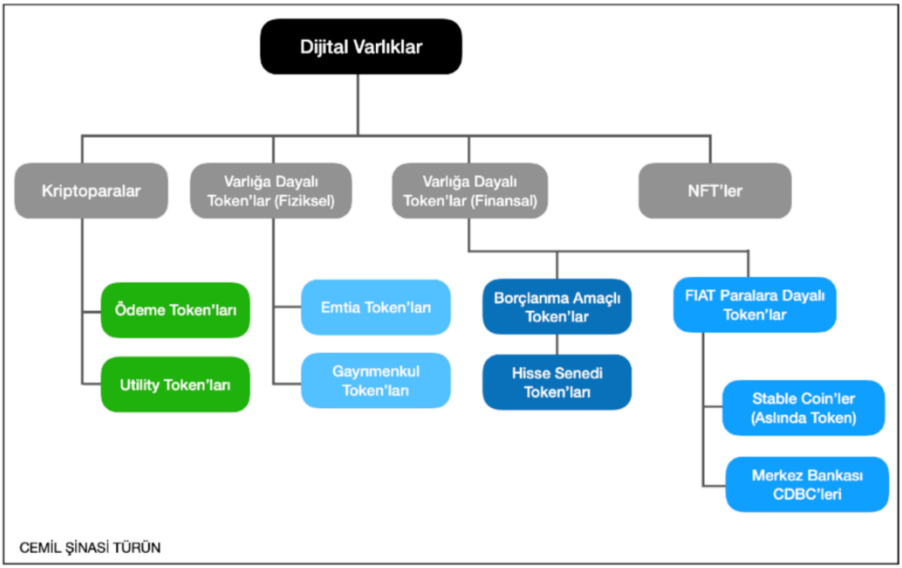
takılmadan dünyanın istediği bölgesindeki projelere yatırım yapabilir. Bu şekilde arz edilen Koin ve Tokenlar yatırımcılar arasında takas edilerek de gelir elde edilmesi mümkündür. Ayrıca bu hisse dağılımları akıllı sözleşmeler üzerinden yapıldığı için şeffaf bir şekilde gerçekleştirilir. Bu yöntemle 2017 yılında 913 projenin topladığı toplam fon miktarı 5,6 milyar dolar civarındadır. Bunlardan sadece 435'inin başarılı olduğu tespit edilmiştir (Williams, 2018).

İyi projelere ICO aşamasında yatırım yapan yatırımcılar sonraki dönemlerde çok yüksek getiri elde etmişlerdir. Ama yukarıdaki veride de görüldüğü üzere ICO yapan projelerin yarısı başarısız olmuştur. Sonraki senelerde de bu halka arzlar devam etmiştir. Ancak bazı dolandırıcılar, herhangi bir denetimden muaf olarak geniş kitlelere ulaşmanın verdiği fırsatı kötü niyetlerine alet ederek teknik konularda yeterince bilgisi olmayan birçok yatırımcının ICO süreçlerinde ciddi zararlara uğramasına neden olmuşlardır.

2.4.4.4. Varlıkların Tokenlaştırılması

Akıllı sözleşmeler Blokzinciri ağının yapısını ve işlevselliğini önemli ölçüde geliştirmiştir. Bu sayede geleneksel birçok finansal aracın, ürünün ve hizmetin merkeziyetsiz Blokzinciri ağı üzerinden sunulmasının da önü açılmıştır. ICO'larla birlikte kitle fonlamasının ne kadar kolay ve zahmetsiz olduğunun görülmesi, bu yöntemin daha başka alanlara da uygulanabilmesinin önünü açmıştır.

Blokzinciri'nde farklı çözümler için üretilen farklı uygulamaların birbirinden farklı türde Tokenları vardır. Aşağıdaki grafikte bu ayrım genel bir şekilde görülmektedir (TÜRÜN, Asset-Backed Token'lar Gümbür Gümbür Geliyor!, 2022).



Şekil 4: Dijital varlıkların gruplandırılması

Bu yöntemle bir şirketin borsada işlem gören hisse senedinin, tahvil veya bonosunun, bir altın madeni veya petrol kuyusunun, bir arazi veya evin tokenlaştırılarak sahipliğinin tamamının veya bir kısmının Blokzinciri üzerinden satılması mümkündür. Henüz çok yeni olan bu teknolojinin geliştirme çalışmaları girişimciler tarafından sürdürülmektedir. 2022 yılında Orta Afrika Cumhuriyeti'nden gelen bir

haberde, bu ülkenin altın madenlerini tokenlaştırma kararı aldığı duyurulmuştur.[17] El Salvador'dan sonra Bitcoin'i resmi para birimi olarak tanıyan ikinci ülke olan Orta Afrika Cumhuriyeti bu şekilde doğal kaynaklarını daha verimli kullanmayı düşündüklerini bildirmiştir.

Bu başlık altında, henüz daha yeni yeni gelişmeye başlayan Gerçek Dünya Varlıkları'nın tokenlaştırılmasına (RAW – Real World Assets) da değinebiliriz. Gerçek dünya varlığı olarak, fiziksel veya finansal varlıkların yanı sıra hizmetleri de saymamız mümkündür.

Fiziksel varlıklar sınıfında gayrimenkul, sanat eseri, altın, petrol veya tarımsal ürünler sayılabilir. Finansal varlıklar ise hisse senetleri, tahviller, bonolar, krediler veya diğer finansal araçlar bulunabilir. Bunların yanı sıra bazı hizmet alanlarının da tokanlaştırılarak satılması mümkündür.

Türkiye'de bir firma, dünyada öncü sayılabilecek bir girişimde bulunarak şu an için buğday, arpa, mısır ve fındık olmak üzere dört tarım ürününde tokanlaştırma yapmış ve bu ürünlerin kripto tokenlarını çıkartmıştır. Firma, yasal düzenlemelere uygun olarak bu dört tarımsal ürünü, hasat zamanı toplamış ve depolamıştır. Bağımsız bir denetleme kurumuyla da düzenli aralıklarla depoların denetlenmesi ve raporlanması için anlaşmalar yapılmıştı. Böylece ürünlerin gerçekte var olduğu yasal olarak da kanıtlanmıştır.

[17] https://www.reuters.com/world/africa/central-african-republic-launches-sango-coin-cryptocurrency-amid-industry-rout-2022-07-15/ erişim tarihi: 17.02.2023

Firma, elinde tuttuğu ürünlerin karşılığında kripto token üreterek yerel kripto para borsaları üzerinden satışa çıkarmıştır. Böylece dünyanın herhangi bir yerindeki bir yatırımcının, Türkiye'de üretilen bu dört ürüne yatırım yapmasının yolu açılmıştır. Firma, daha fazla tarımsal emtianın bu şekilde tokenlaştırılması için çalışmalarına devam etmektedir. Bu yöntemin dünyada benzerlerinin çıkmasının sadece zaman meselesi olduğu kanaatindeyiz. Böylece ev, arazi, değerli metal veya taşlar, tarımsal emtia gibi herhangi fiziksel bir değer, kolayca geniş kitlelere arz edilebilecek bir duruma gelmektedir.

2023 yılı, geleneksel büyük finansal kurumların Blokzinciri sektörüyle yakından ilgilenmeye başladığı bir sene olmuştur. Bu kurumlardan bazılarının, geleneksel finansal ürünlerin tokanlaştırılması üzerine çalışmalar yaptıkları ile ilgili haberler bulunmaktadır. Bu büyük finans devleri, geleneksel finansal varlıklarını, Blokzinciri teknolojisinin sağladığı imkânlardan faydalanarak daha geniş kitleler, daha hızlı, daha ucuz ve daha erişilebilir bir şekilde sunmaya hazırlanmaktadır.

Bu yöntemle yatırımcıların sadece dijital varlıklara değil aynı zamanda fiziksel varlıklara da yatırım yapmasının önü açılacaktır. Ancak bunun yapılabilmesi için Blokzinciri teknolojisinin daha çok gelişmesine ihtiyaç duyulduğunu da belirtmemiz gerekmektedir.

Merkeziyetsiz finans alanındaki uygulamaları genel anlamda bu başlıklar altında sayabiliriz. Tabi ki ilerleyen zamanda çok daha farklı

ürün ve hizmetler de ortaya çıkacaktır. Merkeziyetsiz finansın insanlara ve toplumlara sağlayacağı çeşitli faydalar bulunmaktadır.

Öncelikle merkeziyetsiz finans, geleneksel finansal ürünlere erişimi olmayan insanlara daha kolay ve ucuz çözümler sunma potansiyeline sahiptir. Ayrıca Blokzinciri teknolojisi çok daha güvenli ve şeffaf ürünler geliştirilmesini mümkün kılmaktadır. Merkeziyetsiz yapısı sayesinde erişimi ve geliştirilmesi kolay ürünler geliştirmek mümkündür. Girişimciler çok büyük yatırımlar yapmadan da bu alandaki girişimlerini hayata geçirebilme imkânına sahiptir. Ayrıca bu teknolojinin yenilikçi ürünler geliştirmeye imkân tanıyan yapısı sayesinde daha inovatif çözümler sunması da imkân dâhilindedir.

2.4.5. Merkeziyetsiz Otonom Organizasyonlar (DAO)

Burada Organizasyon kavramı, belirli bir amaç için bir araya gelmiş ve organize olmuş insan topluluğunu ifade etmektedir. Bu bir şirket, bir sivil toplum örgütü veya bir devlet kurumu da olabilir. Sonuçta ortak bir amaç için bir araya gelen insanlar bir organizasyon kurarlar. Kurdukları bu organizasyonun amaçları doğrultusunda da çeşitli eylemler icra ederler.

Modern dönemde hem ticaretin gelişmesi hem de kentleşmenin etkisiyle toplumsal organizasyonların sayıları, çeşitlilikleri ve işlevleri de gelişmiş ve çoğalmıştır. Devlet, özel sektör veya sivil toplum gibi alanlarda çok katmanlı hiyerarşik yapılar kurulmuştur. Bu yapıların

idaresi genellikler merkezi bir sistem üzerinden kurgulanmıştır. Bir başkan, müdür, patron veya idareci ile onun yönettiği, etki alanında olan bir çeşit yönetim kurulu vb. yapılarla yukarıdan aşağıya dikey bir yönetim biçimi, merkezi yönetim sistemlerinin ana kurgusunu oluşturmaktadır.

Merkezi yönetim biçiminin modern dönem kurum ve kuruluşlarının idaresinde yetersiz kalmasından dolayı yönetişim gibi kavramlarla yönetim faaliyetlerinin etki alanının genişletilmesi için çalışmalar yapılmıştır. Birlikte yapma, sinerji, ortak akıl gibi kavramlar etrafından yönetimin yetki alanlarının belirli paydaşlarla paylaştırılmaya yönetişim denilmiştir (FİDAN Y. , 2013).

Yönetimden kaynaklanan sorunların önüne geçebilmek için de çeşitli toplumsal organizasyonları ilgilendiren farklı yasal düzenlemeler ve denetleme mekanizmaları kurulmuştur. Ancak belirli kişiler tarafından alınan kararlarla yönetilen yapıların güvenilirliği günümüzde daha da fazla sorgulanmaktadır (ORHAN Z. Y., 2022).

Blokzinciri Teknolojisi'nin sunduğu imkânlarla yönetişimin sınırları daha da genişletilmekte ve akıllı sözleşmelerin de yardımıyla söz hakkının bütün bir toplulukta olduğu şeffaf organizasyonlar kurulabilmektedir. Dağıtık ağ yapısının sağladığı güvenlik, açık kaynak kodun sağladığı şeffaflık, akıllı sözleşmelerin geri döndürülemez ve müdahale edilemez yapısı sayesinde, merkeziyetsiz organizasyonlar kurmak mümkün hale gelmiştir.

Merkeziyetsiz Otonom Organizasyonlar, adı üzerinde merkezi bir yapı tarafından yönetilmeyen, Blokzinciri teknolojisinin sağladığı alt yapı ve imkanlar üzerinde, akıllı sözleşmeler tarafından şeffaf ve otonom bir şekilde yürütülen sistemlerdir.

Bu organizasyon bir ticari kuruluş, bir sivil toplum örgütü veya bir devlet organı olabilir. Organizasyonun amaçları ve ilkeleri belirlendikten sonra bu doğrultuda sistemin kodlaması yapılır. Üyeler için Yönetişim Token'ı üretilir. Bu Token'lara sahip olanlar, organizasyonun işleyişi ile ilgili değişiklik teklifinde bulunarak bunun oylanmasını sağlamada ve yapılan oylamalarda oy kullanmada hakka sahip olurlar. Topluluğun kararları, kodlama aşamasında belirlendiği ölçüde bağlayıcıdır ve çoğunluğun verdiği karara kimsenin müdahale etme yetkisi yoktur (METJAHIC, 2018).

Organizasyon, kuruluş aşamasında belirlenen ilkeler çerçevesinde kodlanmış akıllı sözleşmeler üzerinde çalışır. Organizasyonda yapılacak işler veya değişiklikler, topluluğun oylamasına sunulur. Elinde o organizasyonun Token'ı bulunan üyelerin yaptıkları oylama sonucuna göre, akıllı sözleşme çalışarak işlevini yerine getirir. Dağıtık Defter Mimarisi sayesinde iş ve işlemler şeffaf bir şekilde yürür.

Merkeziyetsiz Organizasyonların kullanıldıkları veya kullanılması muhtemel alanları şu şekilde özetleyebiliriz;

Hali hazırda UNISWAP veya SUSHISWAP gibi merkeziyetsiz borsa örnekleri vardır. Compound ise kullanıcıların varlıklarını borç

vererek faiz geliri elde ettikleri bir başka örnektir. Merkeziyetsiz Finans'ın diğer alanlarında da kullanılması için çalışmalar yapılmaktadır.

Bu sistem, sivil toplum kuruluşları için de ideal bir yönetişim sistemidir. Yardım kuruluşları, topluluklar hatta sosyal medya uygulamalarının bile bu sistemle geliştirilmesi mümkündür. Yardım kuruluşları alanında en güzel örneğinin 6 Şubat 2023 tarihli Kahraman Maraş merkezli yaşanan deprem sonrasında görüldüğünü söyleyebiliriz. Deprem sonrası kurulan yardım organizasyonları sayesinde dünya çapında kripto para topluluklarından da yardımlar toplanmıştır. Bu tür durumlarda yardım organizasyonlarının şeffaflığı ve güvenliğinin Blokzinciri sayesinde nasıl sağlandığı da kanıtlanmıştır.

Geleneksel hiyerarşik şirketlerde alternatif bir yönetim modeli olarak da kullanılabilir. Ayrıca girişimcilerin proje geliştirme süreçlerinde hem finansal kaynak sağlamada hem de teknik yapının işletilmesinde kullanılabilir. Mesela GITCOIN, açık kaynak kodlu projelere kaynak sağlamak üzere kurulmuş bir DAO'dur. Token sahipleri, hangi projenin fonlanacağına dair oylama yaparak karar vermektedir.

Bunların dışında sanal oyunlarda da kullanılan örnekleri vardır. Oyuncular, oyunun geleceği hakkında karar verme hakkına sahip olurlarken, oyun içinde kazandıkları varlıkların da sahipliğini yönetme konusunda söz sahibi olmaktadırlar.

Daha birçok örneğini sayabileceğimiz Merkeziyetsiz Organizasyonlarda topluluk kavramı ön plana çıkmaktadır. Topluluk kavramı, Blokzinciri alanında önemli bir yer tutar. Sonuçta merkeziyetsizlik yani sınırlı sayıda bir idareci ekibin olmayışı, idarenin kimsenin kontrolünde olmadığı anlamına da gelmemektedir. Burada amaç, işleyişin ve süreçlerin mümkün olduğu kadar şeffaf ve geniş bir katılımcı ağıyla yürütülmesidir.

Haliyle bunun da kendi içinde zorlukları, işleyişte kendine has aksaklıkları olacaktır. Ancak, kripto para sektöründe ağırlıklı olarak yer alan genç kuşakların, Merkeziyetsiz Organizasyonlara büyük önem verdikleri de bu alanda inceleme yapan herkesin dikkatini çeken bir durumdur.

2.4.6. Merkeziyetsiz Kimlik (DID)

Merkeziyetsiz kimlik, gerek devlet hizmetlerinden gerekse de şirketlerin ürettikleri ürün ve hizmetlerden kolay bir şekilde yararlanmak isteyen insanlara büyük kolaylıklar sağlamaktadır. Kimlikler sayesinde doğru hizmetin doğru kişiye iletilmesi daha da kolay hale gelmektedir (KAVUT, 2020).

Modern dönemde devletler, her yeni doğan vatandaşına resmi bir kimlik belgesi verir. Hayatı boyunca insanlar, devletin verdiği kimlikle tanımlanırlar ve birbirlerinden ayırt edilirler. Bu konuda bir karmaşa yaşanmaması için kimlik belgesi vermeyi devletlet üstlenmiştir.

Ancak ulaşım ve iletişim alanındaki gelişmelerle birlikte küreselleşen dünyada fiziki sınırların da ötesinde ürün ve hizmetlere ulaşmak isteyen insanlar için yerel kimlikler, işlev açısından yetersiz kalmaya başlamıştır. Pasaportların kimliklere ek olarak kullanılması da özellikle internetin bu derece geliştiği ve yaygınlaştığı bu dönemde yeni çözümlere ihtiyaç olduğunu ortaya koymaktadır (DOĞAN & KARACAN, 2022).

Devletler vatandaşlarına verdikleri fiziki kimliklerin yanı sıra artık dijital kimlik çözümleri üretmeye çalışmaktadır (KAVUT, 2020). Bu sayede dijital ortamdaki ürün ve hizmetlere de daha kolay erişmek ve kişinin dijital ortamlarda tanımlanması amaçlanmaktadır.

Ne var ki dijital ortamdaki ürün ve hizmetlerin çeşitliliği ve küresel yapısı, bu kimliklerin ve kişisel verilerin güvenliğini ön plana çıkarmaktadır. Bir web sitesinden bir hizmet almak isteyen kişi o siteye birçok kişisel verisini vermek zorunda kalabilmektedir. Bu kişisel verilerin merkezi sunucularda depolanması, sistemlerdeki güvenlik zafiyetlerinden dolayı art niyetli kişilerin eline geçme riskini de beraberinde getirmektedir. İster dijital ortamda olsun ister gündelik hayatta olsun birçok kurum, kuruluş veya firmaya kimlik bilgileriyle birlikte kişisel verilerini emanet eden günümüz insanı için bu durum bazı tehlikeleri de içinde barındırmaktadır. Art niyetli kişiler tarafından çalınan kimlik bilgilerinin veya kişisel verilerin insanlara karşı kullanılması önemli bir sorundur. Her ne kadar devletler hukuki ve idari düzenlemelerle bu sorunları aşmaya çalışsalar da özellikle dijital

ortamda devletlerin yetkilerinin erişemeyeceği alanlarda, kişisel verilerin korunmasının zafiyete uğraması, insanları tehdit etmeye devam etmektedir (TAKAOĞLU, ÖZER, & PARLAK, 2019).

İnternetin yeni yeni gelişmeye başladığı dönemlerde internette veri akışı tek taraflı bir yapıya sahipti. Sunucu sistemlerdeki hizmetlere erişen kullanıcılar, o ortamdaki hizmetlerden faydalanabilmekteydi. Özel hizmetlerden faydalanabilmek için ise sisteme üye olunuyor, kullanıcı adı şifre gibi basit tanımlamalar kullanılıyordu. Web 2.0 teknolojileri sayesinde tek taraflı bu iletişim, karşılıklı etkileşimi artıracak ürün ve hizmetlerin yolunu açmıştır. Bu dönemde de yine kullanıcı adı ve şifre yöntemi kullanılmaya devam etmiş, ancak bunun yanında farklı kimlik tanımlama yöntemleri de kullanılmaya başlamıştır. Mesela "Google ile bağlan", "Facebook ile bağlan", "Twitter ile bağlan" gibi seçenekler sunularak, bu merkezi yapılar üzerinden üyelik işlemleri yapılabilir hale gelmiştir. Diyelim ki Google hesabı olan birisi bir başka sitedeki hizmetten faydalanmak istediğinde, o siteye üyelik işlemleri ile uğraşmamakta, "Google ile bağlan" diyerek kimlik tanımlamasını Google üzerinden yapabilmektedir (KAVUT, 2020).

Bu tür kimlik tanımlamaları bir kolaylıktır ama kullanıcı açısından sakıncaları da bulunmaktadır. Google örneğinden ilerlersek, kullanıcının Google ile bağlandığı bir servisten hizmet aldığında, aslında o alanda yaptığı her şey aslında Google'ın gözetimi altında

yapılmaktadır. Her ne kadar kullanım kolaylığı sağlansa da, kullanıcı verileri büyük firmalarca izlenmekte ve kaydedilmektedir.

Merkezi onaylayıcı bir kurum tarafından verilen kimliklerde tüm tanımlamalar kimliği veren kurum tarafından yapılır. Kimlik sahibinin kimlik üzerinde hiçbir tasarrufu bulunmaz. Ayrıca kimlik bilgilerinin tutulduğu neredeyse bütün ortamlar yine merkezi sistemler tarafından yönetildiğinden dolayı kimlik bilgilerinin kimler tarafından ve ne amaçlarla kullanıldığıyla ilgili de bir bilgiye sahip değildir. Mesela sürekli alışveriş yaptığı bir sitenin siber saldırıya uğraması sonucu kimlik bilgilerinin ve kişisel verilerini çalınması ile mağduriyet yaşayan birinin muhatabının kim olacağı meselesi önemli bir sorundur.

Dijital kimlik bilgisi, sadece birkaç tanımlayıcı ile belirlenen kısıtlı bir bilgiyi ifade etmeyip çok daha geniş bir tanımlama alanına sahiptir. Klasik kimlik bilgilerinin yanı sıra, kişinin dijital ortamda yaptığı bütün işlemler, bu işlemlerde bıraktığı ayak izleri, kişisel beğeni ve eğilimleri, görüş ve fikirleri, sosyal, finansal, ailevi, siyasi, iş alanları gibi birçok alanla ilgili verileri içermektedir.

Blokzinciri teknolojisi, merkeziyetsiz dağıtık yapısı ve kriptografik çözümleri sayesinde, dijital ortamda kimliklerin tanımlanması, bu dijital kimliklerin yetkisiz ellere geçse bile kullanılamaması ve kimliklerin yönetiminin tamamen kullanıcıların hâkimiyetinde kalmasını sağlayan çözümler sunmaktadır. Bu amaçla Blokzinciri ekosisteminde merkeziyetsiz kimlikler üretilebilmektedir. Birçok kaynakta bu kimlik türüne dijital kimlik denilse de merkeziyetsiz

kimlik (DID – Decentralized Identity) olarak tanımlamanın daha uygun olacağı söylenebilir.[18] Çünkü bu teknolojinin yapısını en iyi tarif eden tanımlama budur ve devletlerin ürettiği dijital kimliklerle de karıştırılmasının önüne geçecektir.

Blokzinciri ağları üzerinde inşa edilen merkeziyetsiz kimlikler, bireylerin kimlik bilgilerini yönetebilmelerini sağlar. Kişi, bir Blokzinciri ağı üzerindeki merkeziyetsiz kimlik uygulamasıyla tanımlayacağı, devredilemez benzersiz bir Token (Soulbound Token) ile merkeziyetsiz kimliğini oluşturabilir. Bu kimlik Token'ı kripto para cüzdanında tutulur. Bu Token devredilemez ve parasal bir değeri yoktur. Kullanıcı herhangi bir uygulamada kimlik tanımlamak durumunda kalırsa, o uygulamaya giriş yaparken kripto para cüzdanı ile oturum açarak onay verir ve uygulamayı kullanmaya başlar. Kullanıcı adı ve şifre yerine kripto para cüzdanı ile onay vererek kimliğini onaylar.[19]

Merkeziyetsiz kimlik ile girilen uygulamalarda kullanıcı verileri ifşa edilemez. Çünkü kullanıcı uygulamaya herhangi bir bilgi vermez. Kimlik Token'ı sayesinde sadece kimliğini onaylar. Burada kullanılan Sıfır Bilgi Kanıtı (Zero-Knowledge Proof) teknolojisi sayesinde kullanıcı, gerçek kimlik bilgilerini vermeden kendisinin gerçek bir kişi olduğunu ispat eder. Bu sayede kişisel bilgilerini vermeden o uygulamayı kullanma hakkı kazanmış olur (TANRIVERDİ, UYSAL, & ÜSTÜNDAĞ, 2019).

[18] https://ethereum.org/tr/decentralized-identity/ erişim tarihi: 17.03.2023
[19] https://www.binance.com/en/BABT?source=header erişim tarihi: 17.03.2023

Merkeziyetsiz kimlikle kullanıcı, sadece kimlik bilgilerinin kontrolünü elinde tutmaz. Aynı zamanda bu kimlik ile kullandığı tüm uygulamalardaki kullanıcı deneyimleri ile ilgili verileri ve bu ortamlarda elde ettiği kazanımların da kontrolünü eline alır. Günümüzde kullanıcı verilerini sağarak, bu verileri reklam ajanslarına pazarlayan dijital mecraların daha fazla kullanıcı mahremiyetini ihlal etmelerin de böylece önüne geçilmesi planlanmaktadır.

Ayrıca kullanıcının kimlik bilgileri, merkezi bir sunucuda değil, kullanıcının kendi cihazında tutulur. Bu da merkezi sunucuların siber saldırıya uğrayıp, kullanıcı bilgilerinin çalınmasının önüne geçer. Hizmeti sağlayan site, kullanıcının kimlik bilgilerini göremez. Merkeziyetsiz Kimlik sistemi, kullanıcının kimliğinin doğrulanmasını sağlar. Kimlik bilgileri karşı tarafa iletilmez. Kullanıcının kendisinde kalır.

Bunun yanı sıra kullanıcı, hangi bilgilerini paylaşacağını da kendisi belirler ve bu paylaştığı bilgilerin nasıl ve nerelerde kullanıldığını da ağ üzerinden izleyebilir. Paylaştığı veriler üzerinden gelir elde edebilir.

Merkeziyetsiz kimlikler sayesinde kullanıcının bir uygulamada elde ettiği tüm deneyim ve birikimlerini, başka bir uygulamaya taşıması mümkün olmaktadır. Kısaca merkeziyetsiz kimlik sadece kimlik bilgilerinin korunmasına yardımcı olmakla kalmamakta, dijital ortamdaki tüm ayak izlerinin ve bilgi kırıntılarının da kontrolünü kullanıcıya vermektedir.

2.4.7. Nitelikli Fikri Tapu (NFT)

Sanat eserlerinin ticareti uzun zamandır yapılagelen bir ticaret faaliyetidir. Değişik türdeki sanat eserlerinin farklı şekillerde yapılan ticaret usulleri vardır. O eseri üreten, ticaretini yapan ve esere sahip olanın hakları zaman içerisinde değişik yasal düzenlemelerle korunmaya çalışılmıştır. Burada en büyük sorun, bu tarafların haklarının doğru şekilde korunmasında yaşanan olumsuzluklardır. Eserin kopyalanması, çoğaltılması veya çalınması gibi olumsuzluklardan bahsedilebilir.

Dijital teknolojilerin de gelişmesiyle birlikte geleneksel yöntemlerle üretilen sanat eserleri, dijital ortamlarda da üretilmeye başlamıştır. Bu eserler geleneksel yöntemlerle üretilmiş olsalar bile bir şekilde dijital ortamda yeniden üretilebilmektedir. Dijital aygıtların sağladığı kolaylıklardan birisi de bu ortamdaki verilerin çok rahat bir şekilde kopyalanabilmesidir (SOYUER, 2023). Bu kolaylık, sanat eserleri için aslında bir tehdit oluşturmaktadır. Çünkü, dijital ortamlarda sanat eserlerinin haklarının korunması oldukça zordur.

Bir sanat eserinin değerini belirleyen en büyük özelliği onun benzersiz olmasıdır. Dijital teknolojiler sanat eserlerinin bu benzersiz olma özelliğini tehlikeye atmış olsa bile Blokzinciri teknolojileri sayesinde yine sanat eserlerinin benzersiz özelliği tescillenebilir. Bu o sanat eserine verilecek olan benzersiz bir Token (Non-Fungible Token – NFT) ile mümkün olmaktadır. Akıllı sözleşmelerin dağıtık

merkeziyetsiz Blokzinciri ağı üzerinde çalışması ile birlikte bir sanat eserine verilen benzersiz Token, o eserin sahibinin ve üreticisinin bilgilerini değiştirilemez hale getirir (ARAPOĞLU, 2021).

NFT Token, bir sanat eseri ne kadar kopyalanırsa kopyalansın, ilk üretenin ve o ilk üretilen orijinal eserin o anki gerçek sahipliğinin kimde olduğunun tescilini sağlar. Bu sayede sanat eserinin orijinalinin sahipliği rahatlıkla el değiştirebilir. Böylece el değiştiren sanat eserinin bu ticareti sonucunda orijinalliği korunur ve bu ticaretten de her seferinde üreticisi de kazanç elde edebilir (TÜRÜN, Tekil Tokınlar: Tek-Tok (Non-fungible tokens), 2021).

Türkçe'ye Nitelikli Fikri Tapu olarak çevrilen Non-Fungible Token kavramındaki Non-Fungible tanımı, bölünemez anlamına gelir. Fungible bölünebilir, takas edilebilir değerleri tanımlamak için kullanılır. Fungible olan bir değerin birçok benzeri olabilir. Para veya kripto para bir fungible değerdir. Birçok benzeri vardır ve birbiri ile takas edilebilir. Non-Fungible ise benzeri olmayan tek bir varlığı ifade eder. Benzeri olmadığı için de takas edilemez. Bir başka benzeri üretilemez. Sanat eserleri veya tapu gibi. Bir tapunun bir sahibi olabilir. Devredilebilir ama bir benzeri daha olmadığı için takas edilemez (USTAOĞLU, KIRAN, BAĞCI, & EMRE, 2022).

NFT üretmek (mint etmek) için hali hazırda değişik platformalar vardır. Üretilen sanat eseri bu platformlara yüklenerek karşılığında eserin sahipliğinin tescili olan Token yani NFT alınır, sanatçı tarafında bu Token kripto para cüzdanına aktarılır. Böylece o eserin sanatçı adına

tescili merkeziyetsiz dağıtık Blokzincir ağı üzerinde sağlanmış olur (USTAOĞLU, KIRAN, BAĞCI, & EMRE, 2022). Bundan sonra NFT sahibi elindeki benzersiz Token'ı kendi cüzdanından isterse başka bir cüzdana transfer edebilir.

Benzersiz veya Tekillik Token'ı olarak da isimlendirilen NFT'ler ressam, müzisyen, çizer, yazar, heykeltıraş gibi birçok değişik sanat alanında ürün ortaya koyanlara hitap etmektedir (TÜRÜN, Sanat Eserlerinin Blokzinciri Üzerinden Takibi, 2022). NFT sayesinde sanat üreticisinin sanat tüccarlarına da bağımlılığı sona ermektedir. Müzayede evi, ajans, yayıncı vb. gibi birçok aracı merkezi yapıya da ihtiyaç duyulmamaktadır. Bu da sanatçının daha özgür hareket etmesinin ve ticari olarak da daha fazla gelir elde edebilmesinin önünü açmaktadır (TÜRÜN, Karikatürler İçin NFT'li Yeni İş Modeli Önerisi, 2021).

Her ne kadar sanat alanında kullanılıyor gibi görünse de henüz yeni sayılan bu teknolojinin şimdilik otuzdan fazla kullanım alanı olduğu bilinmektedir. Dijital oyunlardan elde edilen kazanımların ticaretinde, sertifikalandırma, bilet satışı, kitlesel fonlama, lojistik vb. gibi birçok alanda kullanım imkânı bulunmaktadır (AYAN, 2022).

2.4.8. Yeni Nesil İnternet (WEB 3.0)

Bir belge içerisindeki bir metne tıklandığında kullanıcıyı başka bir belgeye yönlendiren sisteme Hiper Metin (Hyper-Text) denir. Sunucu görevi gören bir bilgisayardaki belgeye, istemci rolündeki bir

başka bilgisayarın erişmesi ve köprü metne tıklayarak başka bir belgeye ulaşması şeklinde tanımlanan sistemin genel kurgusuna da Hiper Metin Transfer Protokolü (HTTP – Hyper Text Transfer Protokol) denilmektedir (Berners-Lee, Fielding, & Frystyk, 2023).

HTTP, Tim Berners-Lee ve ekibi tarafından 1989 yılında CERN Laboratuvarları'ndaki araştırmacıların kullandıkları kaynakları daha verimli bir şekilde organize edebilmek amacıyla geliştirilen bir bilgisayarlar arası iletişim standardıdır. Bu iletişim yöntemi ile kurgulanan sisteme de örümcek ağından esinlenerek World Wide Web – WWW denilmiştir (BAYTER, 2009). Sunucu bilgisayarlarda yayınlanan sayfalara, istemci bilgisayarlardan tarayıcı denilen yazılımlarla erişilmekte ve görüntülenen sayfadaki bağlantılara/köprülere tıklanarak başka bir sayfaya ulaşılabilmektedir.

İlk zamanlarında çoğunlukla metin tabanlı çalışan internet, HTTP protokolü sayesinde komutlar yazmadan sadece fare tıklamalarıyla işletilebilen, metnin yanı sıra görsellerle de zenginleştirilmiş içerikler sunana bir yapıya dönüşmüştür. 90'lı yıllarda bilgisayar sektöründe hem donanım hem de yazılım alanlarında yaşanan gelişmelerle birlikte internet de rağbet görmeye başlamış ve bu sayede gelişimi hızlanmıştı. Masaüstü bilgisayar/kişisel bilgisayar üzerinden insanların bütün dünyadaki diğer insanlarla iletişime geçebilmesi ve kaynaklara erişebilmesi fikri büyük rağbet görmüş ve hızla yayılmıştır. İlk internet sitesi 1991 yılında yayınlandıktan sonra o kadar hızlı

yayılmıştır ki, 1999 yılına gelindiğinde 14 milyondan fazla internet sitesi aktif bir şekilde çalışır hale gelmiştir (BAYTER, 2009).

Bu hızlı büyüme beraberinde internet siteleri üzerinden sunulan ürün ve hizmetlerin de çeşitlenmesine neden olmuştur. Kısa zamanda internet bir kaynak üzerindeki bir veriye ulaşmanın çok ötesine geçerek, ticaretten eğlenceye kadar çok çeşitli alanda seçeneklerin sunulduğu bir yapıya dönüşmüştür. İstemci konumundaki kullanıcıya, tek taraflı veri aktarımının yerine iki taraflı etkileşime geçebilme imkânı sunulması ile birlikte internet dünyası yeni bir seviyeye geçiş yapmıştır. Tek taraflı veri aktarımı dönemine WEB 1.0 denilirken çift taraflı etkileşimin olduğu yani kullanıcının kullandığı internet hizmetine de katkıda bulunduğu yeni yapıya WEB 2.0 denilmiştir (ARVAS, Gutenberg Galaksisinden Meta Evrenine: Üçüncü Kuşak İnternet, Web 3.0, 2022).

Yeni nesil internet sayesinde kullanıcı, internet üzerinde bir yer edinebilmiş ve edilgen durumdan etken duruma geçiş yapmıştır. Sosyal medya siteleri ikinci nesil internetin başat örnekleridir. Kullanıcı buralarda içerik üreterek diğer kullanıcılarla etkileşime geçmektedir. İkinci nesil internet ürün ve hizmetleri aynı zamanda kullanıcıların dijital bir şekilde sosyalleşebilmelerinin de yolunu açmıştır.

Tek taraflı bir veri akışının olduğu ve kullanıcının bir tüketici konumunda bulunduğu internetin birinci nesli ile kullanıcının da içerik üreterek çift taraflı etkileşim içerisinde olduğu ikinci nesil internetin ortak noktaları merkezi olmalarıdır (ARVAS, Gutenberg Galaksisinden Meta Evrenine: Üçüncü Kuşak İnternet, Web 3.0, 2022). Her iki

sistemde de merkezi sunucular üzerinde yayınlanan internet ürün ve hizmetlerine erişen kullanıcının tüm aktiviteleri ile ilgili veriler bu merkezi sunucularda tutulmaktadır. İkinci nesil internette kullanıcı her ne kadar bir etkiye sahipse de sistemin kendisine bir müdahalede bulunamaz. Mesela bir sosyal medya uygulamasında içerik yazabilir ama o sosyal medya sitesinin çalışma biçimine müdahale edemez. Bu açıdan bakıldığında da aslında kullanıcı halen edilgen bir konumdadır. Kendine sunulanı kullanır. Sınırlı oranda etkileşime girebilir ama hiçbir şekilde sistemin yürütülmesi ile ilgili söz sahibi değildir. Kullandığı ürün veya hizmeti geliştiren ve hizmete sunanların koyduğu kurallar çerçevesinde bir etkileşime girebilir. Kısacası kullanıcı internet hizmetinin tasarlanması, geliştirilmesi ve çalışması sürecinde tamamen edilgen bir konumdadır.

Merkezi sunucular üzerinden hizmetlerin sunulması, şüphesiz çok daha kolay ve daha az masraflıdır. Yönetmesi de bir o kadar kolaydır. Ancak güvenlik ve mahremiyet konusunda da kafalarda soru işaretleri bırakmaktadır. Sınırlı bir ekip tarafından, genelde kapalı kaynak kodlu olarak geliştirilen ürün veya hizmetin, çalışmaya başladığında ortaya çıkabilecek muhtemel güvenlik açıklarından dolayı kullanıcılar her zaman bir güvenlik tehdidiyle karşı karşıyadır. Ayrıca merkezi sunucuların güvenliğinin sağlanması da bir başka potansiyel güvenlik riskidir. Kullanıcı verilerinin yetkisiz kişilerin eline geçmesi ihtimali her ne kadar kullanıcı açısından bir potansiyel risk ise de, kullanıcı verilerinin bizzat sistemi yürütenler eliyle, kullanıcının bilgisi

ve rızası olmadan kullanılması da bir o kadar önemli güvenlik riskidir ve mahremiyetin ihlalidir.

İnsanların her geçen gün daha fazla bir şekilde internet ürün ve hizmetlerini kullanıyor olmaları, bu ürün ve hizmetleri kullanmalarından kaynaklanan ürettikleri her türlü verinin de doğal bir şekilde çoğalmasını beraberinde getirmektedir. En basit haliyle bir kullanıcı, telefonundan sosyal medya hesabına girdiğinde iletilere bakmak için sayfayı aşağıya doğru kaydırması esnasında hangi iletiye ne kadar süre ile baktığı bile o sosyal medya şirketi açısından önemli bir veridir. Kullanıcıya daha iyi bir internet deneyimi sunma gerekçesiyle buna benzer birçok kullanıcı verisi, firmalarca kaydedilmektedir. Ancak bu uygulamaların, kapalı ve merkezi sistemler olmalarından dolayı topladıkları bu bilgileri gerçekte ne amaçlarla kullandıkları kullanıcı tarafından tam olarak bilinememektedir.

2015 yılında İngiliz The Guardian gazetesinde çıkan bir haberle patlak veren Facebook–Cambridge Analytica veri skandalı ile birlikte, sosyal medyadaki kullanıcı veri mahremiyetinin ne derece önemli olduğu ortaya çıkmıştır. İngiltere merkezli Cambridge Analytica firması tarafından, 2014 yılı boyunca Facebook'dan toplanan 50 milyondan fazla kullanıcı verisinin, Amerika'daki başkanlık seçimlerinde kullanıldığı anlaşılmıştır (Davies, 2015). Devamında 2018 yılında Amerikalı Newyork Times gazetesi meseleyi daha derinlemesine araştırmıştır. Gazetenin yayınlanan haberinde, Facebook kullanıcı verileri üzerinden seçmenlerin fikirlerinin değiştirilmesiyle ilgili

yapılan çalışmalarla ilgili olarak çalışan uzmanlarla yapılan mülakatlara yer verilmiştir (ROSENBERG, CONFESSORE, & CADWALLADR, 2018).

Facebook'tan sızdırılan bu verilerde sadece kullanıcı paylaşımları değil, konum ve beğeni bilgisine kadar her türlü verinin bulunduğu belirtilmiştir. Hatta bir firma yetkilisinin verdiği bilgiye göre, sadece beğeni bilgileriyle bile kullanıcının hangi ırktan olduğu %95 doğrulukta, hangi partiye oy vereceği de %85 doğrulukta tahmin edilebilmektedir (SCHWARTZ, 2017).

The Guardian gazetesinde 2018 yılında yayınlanan bir başka haberde, Cambridge Analytica firmasının Facebook kullanıcı verilerini, İngiltere'nin Avrupa Birliği'nden çıkma sürecinde yapılan Brexit seçimlerinde de kullandığı bilgisine yer verilmiştir (CADWALLADR & TOWNSEND, 2018).

Benzer bir olay da bir diğer sosyal medya şirketi olan Twitter'da yaşanmıştır. Twitter'ın Elon Musk tarafından satın alınmasında sonra bizzat Musk tarafından 2022 Aralık ayında bazı gazetecilere peyderpey verilen dosyalarda, şirketin geçmiş dönemlerde başta Amerikan hükümeti olmak üzere bir dizi başka ülke yönetimleri ve istihbarat servisleriyle nasıl çalıştığı anlatılmıştır (FRANKEL, 2022).

Kullanıcıların veri mahremiyetinin ne denli önemli bir mesele olduğu sadece bu iki örnekten bile yola çıkarak kolayca anlaşılmaktadır. Sanıldığının aksine sıradan hayatlar yaşayan insanların eğlence amacıyla vakit geçirdikleri internet hizmetlerindeki faaliyetleri, bu

ortamlardaki her türlü aktiviteleri, Büyük Veri (Big Data) kapsamında ele alındığında çok ciddi değer taşımaktadır. Kaldı ki yapa zekâ ve derin öğrenme algoritmalarının gelişmesiyle birlikte, bilgisayarların verileri yorumlama kabiliyeti kazanmaları, büyük veri yığınlarının çok daha etkili bir şekilde analiz edilerek daha net çıkarımlar yapılabilmesinin önünü açmaktadır.

Hali hazırda kullandığımız internet yapısında, kullanıcı verileri ve mahremiyeti, kimi zaman bizzat ürün veya hizmeti veren firmalar tarafından, kimi zaman da üçüncü taraflar eliyle ihlal edilmektedir. Bu durumlarda kullanıcıların yapabilecekleri pek bir şeyleri de yoktur.

Web 3.0 bu tarz kaygılardan dolayı geliştirilen bir sistemdir. Blokzinciri ağları üzerinde merkeziyetsiz, açık kaynak kodlu ve daha güvenli bir internet vizyonu çerçevesinde geliştirilmektedir. (ARVAS & ZAMUR TUNCER, 2023)

Blokzinciri teknolojisinin sağladığı eşten eşe ağ yapısı sayesinde merkeziyetsiz, dağıtık defter teknolojisi ve açık kaynak kodlu geliştirilmesi sayesinde de şeffaf bir yapı sunmaktadır. Aslında Web 3.0, bütün Blokzinciri ürün ve hizmetlerinin genelini kapsayan bir tanımlamadır. Bu sebepten dolayı Yeni Nesil İnternet olarak tanımlanması daha uygundur. Çünkü var olan hali hazırdaki internet sisteminden tamamen farklı bir şekilde çalışmaktadır. Önceki bölümlerde anlattığımız bütün Blokzinciri ürün ve hizmetlerini, Web 3.0 çatısı altında toplamak mümkündür.

Web 3.0 tek bir ürün değildir. Blokzinciri teknolojisi ile geliştirilen her türlü ürün ve hizmet, bu Yeni Nesil İnternet'in bir parçasıdır. Kullanım olarak bakıldığında mevcut internete benzeyen ama çalışma prensibine ve altında yatan teknolojiye bakıldığında ise farklı bir şekilde işleyen yeni bir tür iletişim ve etkileşim ağıdır. Eşten eşe ağ yapısı ve akıllı kontratların bu ağ üzerinde etkili ve esnek bir şekilde çalışmasını sağlayan merkeziyetsiz uygulamalar, Web 3.0'ın en temel unsurlarıdır. Bir başka bakış açısıyla, kendisine Merkeziyetsiz İnternet de denilebilir.

Halihazırda kullandığımız internet, teknik altyapısı ve sunduğu hizmetlerle birlikte bakıldığında muazzam bir büyüklüğe sahiptir. Ancak değindiğimiz gibi merkezi yapısından dolayı hemen her kesim için farklı şekillerde sorunlara yol açma potansiyeli mevcuttur. Merkezi yapısı aynı zamanda internet tekellerinin de oluşmasının önünü açmaktadır.

Merkezi sistemler he zaman için belirli bir kesime ayrıcalık tanınmasına yol açar. Büyük veri tekelleri, medya, sosyal medya, alışveriş, eğlence veya teknik hizmetler gibi birçok alanda tekellerin ortaya çıkması merkezi sistemlerin kontrolü ile mümkün olmuştur.

Yönetici elit veya tekel haline gelmiş büyük bir ürün/hizmet sağlayıcısı, toplumlar için sağlıklı yapılar değillerdir. Yukarıda vermiş olduğumuz birkaç örnekte de görüleceği üzere, bir ürün/hizmet sağlayıcısının büyük bir tekel haline gelmesi, kimi zaman kişisel verileri

kimi zaman da ülkelerin milli güvenliklerini tehdit eder hale dönüşme potansiyeli barındırabilmektedir.

Bu sebepten dolayı, “Blokzinciri’nin Kullanım Alanları” başlığı altında ele aldığımız, genel olarak da Web 3.0 ekosisteminin genelini kapsayan uygulamalar, merkeziyetsiz yapıların da bir alternatif olarak oluşturulup kullanılabileceğinin ispatları olarak durmaktadır.

3. BİR TÜR TOPLUMSAL ORGANİZASYON (ÖRGÜTLENME) BİÇİMİ OLARAK BLOKZİNCİRİ

Arkeolojik bulgular, en eski çağlardan bu yana insanın topluluk halinde yaşamaya eğilimli bir varlık olduğunu göstermektedir. Topluluk halinde yaşam, iş bölümü ve iş birliği sayesinde sorunlarla baş etme kapasitesini artırmaktadır. Birey, toplumsal yaşam içinde şahsi kapasitesinin çok ötesinde bir fayda oluşturabilmektedir. Bireyin tek başına üstesinden gelemeyeceği zorluklar da toplumsal iş bölümü sayesinde yönetilebilir hale gelmektedir. Tabi ki toplumsal iş birliği oluşturmanın, devam ettirmenin ve yönetmenin de birçok zor tarafı bulunmaktadır. Toplumu doğru ve verimli bir şekilde organize edebilmek, iş süreçlerinin aksamaya uğramadan ilerleyebilmesini sağlayabilmek için de etkili örgütlenme biçimlerine ihtiyaç duyuldu. Toplumlar zaman içerisinde ihtiyaçlarına göre organizasyonlar kurma, bu organizasyonları verimli bir şekilde işletmenin yollarını aradılar.

Toplum–devlet ilişkisine dair klasik tartışmaları Antik Yunan düşüncesine kadar geri götürmek mümkündür. Platon, *Devlet* adlı eserinde, Aristoteles ise *Politika* adlı eserinde devlete ve topluma dair fikirlerini açıklamışlardır. İkisi de insanın sosyal bir canlı olduğunu ve kendi başına yaşayamayacağını, ancak birlikte iş bölümü yaparak hayatta kalabileceğini eserlerinde dile getirmişlerdir. Ayrıca, toplumsal düzenin sağlanabilmesi ve toplumsal örgütlenmenin doğru bir şekilde

organize edilmesinin de önemine vurgu yapmışlardır. Buna ilaveten toplumların sağlıklı bir şekilde yaşayabilmeleri için eğitim ve adaletin önemi üzerinde de durmuşlardır. Benzer şekilde İbni Haldun da *Mukaddime* adlı eserinde, insanların topluluk halinde yaşamalarının gerekliliğine vurgu yaparken, toplumsal örgütlenmelerin önemi ve iş bölümü yapmanın sağlayacağı faydalar üzerinde durmuştur (İÇLİ, 1987). Hatta İbn Haldun iş bölümünü bedevi bir toplumdan medeni bir topluma geçişin bir ön koşulu olarak değerlendirmektedir (YILMAZ, 2019).

Sanayi Devrimi ile birlikte daha da karmaşık hale gelen toplumsal sorunların çözümü, toplumsal düzenin nasıl sağlanabileceği, ideal toplumsal yapıların nasıl kurulabileceği ile ilgili olarak da Aydınlanma Dönemi düşünürleri değişik görüşler ortaya koymuşlardır. Toplumları doğru ve sağlıklı bir şekilde organize etmek, bu organizasyonların verimli bir şekilde işlevlerini yerine getirebilmelerini sağlamak, gerektiğinde güncellemek veya yenisi ile değiştirmek, toplumsal organizasyonlarla ilgili karşılaşılan temel sorunlardır.

Toplumsal organizasyon bireylerin, grupların veya kurumların belirli amaca veya hedefe yönelik bir araya gelip örgütlenerek oluşturdukları yapıdır. Bu tür organizasyonlar siyasal, ekonomik, kültürel ve sivil alanlar da dâhil olmak üzere toplumun farklı düzlemlerinde ortaya çıkabilir. İnsanlar, bir ihtiyacı karşılamak, belirli bir hizmeti üretmek ya da ortak bir problemi çözmek amacıyla örgütlenerek çeşitli organizasyonlar kurarlar. Kamu kurumları, sivil

toplum örgütleri ve özel teşebbüsler bu bağlamda örnek olarak verilebilir. Burada amaç, insanların bir araya gelerek iş birliği içerisinde hedeflerine ulaşmak için organize bir şekilde çalışmalarıdır. Ortak bir hedef, amaç, ihtiyaç, vizyon söz konusudur.

Toplumsal organizasyonların kurulması, işletilmesi ve değişen durumlara göre yeniden yapılandırılması gibi süreçlerin iyi bir şekilde yönetilebilmesi de hayati önem taşımaktadır. Organizasyonlar çoğu zaman belirli bir lider ya da liderlik ekibi etrafında biçimlenmekte, yönetsel kararlar ve yönlendirme faaliyetleri de bu aktörler tarafından yürütülmektedir. Ancak Blokzinciri teknolojisi, bu alanda alışılagelmiş yönetim biçimlerine alternatif çözümler getirmektedir. Teknolojinin gereksinimlerden ortaya çıkması olgusu burada da kendini göstermektedir. Blokzinciri teknolojisinin ilk ve en görünür uygulamalarından biri olan Bitcoin, para yönetimine ilişkin tartışmaların ve özellikle merkezî finansal yapılardan kaynaklandığı ileri sürülen sorunlara yönelik alternatif arayışların bir ürünü olarak ortaya çıkmıştır.

Blokzinciri teknolojisin kullanım alanlarını anlattığımız önceki bölümlerde sürekli olarak dikkat çektiğimiz nokta, bu teknoloji üzerine kurgulanan organizasyonların merkeziyetsiz yapısıydı. Toplumsal organizasyonların merkezi yapılar tarafında kontrol edilmesi her ne kadar alışılagelmiş bir uygulama olsa da, günümüzde alternatif bir yönetişim biçimi olarak Blokzinciri teknolojisinin sunduğu çözümlerin de değerlendirilmesi gerektiğini düşünüyoruz.

İnsanlar ihtiyaçlarını gidermek için teknoloji üretir ve o teknolojiden fayda sağladıkları takdirde onu geliştirerek daha verimli hale getirmeye çalışırlar. Blokzincir teknolojisi de belirli sorun alanlarına çözüm üretme arayışının bir sonucu olarak ortaya çıkmıştır. Gelinen aşamada, bu teknolojinin sunduğu imkânların kayda değer bir kullanıcı ve paydaş kitlesi tarafından benimsendiği görülmektedir. Buna bağlı olarak uygulama alanlarının hızla genişlediği ve teknolojinin geliştirilme sürecinin devam ettiği anlaşılmaktadır.

Bitcoin ile birlikte, parasal sistemlerde merkezî aracılara duyulan ihtiyaç ve paranın üretimi/dağıtımı üzerindeki merkezî düzenleme biçimleri daha yoğun biçimde tartışılmaya başlanmıştır. Ayrıca merkeziyetsizliğin mümkün olabileceğinin pratik olarak gösterilmiş olması beraberinde merkezi kurumların işlevi ve meşruiyeti üzerine yürütülen tartışmaları—özellikle devletin konumu bağlamında—yeniden gündeme taşımıştır.

Çalışmamızın bu aşamasında, öncelikle para olgusu ele alınacak, ardından da devletin yapısı ve meşruiyetine ilişkin olarak "Toplumsal Sözleşme" yaklaşımı blokzincir bağlamında tartışılacaktır.

3.1. Paranın Toplumsal Rolü ve Kripto Paraların Konumu

İnsanlık tarihine bakıldığında, insan topluluklarının farklı coğrafyalara yayılmış biçimde, irili ufaklı gruplar hâlinde yaşamlarını

sürdürdükleri görülmektedir. Zaman içerisinde nüfusun artması, toplumsal yapıların gelişip çeşitlenmesi ve yeni teknolojilerin ortaya çıkması gibi çok sayıda değişkenin etkisiyle, başlangıçta birbirinden görece uzak olan toplumlar giderek artan ölçüde etkileşime girmiştir.

Toplumsal yapıları, örgütlenme biçimleri ve iş yapma şekilleriyle tarihsel süreçte kendi deneyimlerini ve pratiklerini oluşturan görece izole toplumlar birbirleriyle bağlantı kurduklarında, geçmiş tecrübeleriyle elde ettikleri deneyimleri ve pratikleri birbirlerine aktardılar. Bu şekilde birçok bireysel ve toplumsal tecrübe birikimi toplumlardan toplumlara aktarıldı. Bu aktarımlardan birisi de, bir iş yapma biçimi olarak ticaret olgusuydu. İlk insan topluluklarında mübadele (değiş-tokuş) olarak gerçekleşen bu iş yapma biçimi zamanla gelişip yaygınlaşarak farklı boyutları, katmanları ve tarzlarıyla toplumların gelişmesine ve ilerlemesine fayda sağladı.

3.1.1. Paranın Tanımı, Tarihi ve Toplumdaki Rolü

Ticaretin yaygınlaşması ve mübadelede paranın bir araç olarak kullanılmasıyla birlikte ticaret ve para kavramları üzerine düşünceler de ortaya çıkmaya başlamıştır. Antik Yunan'da Platon, Aristoteles ve Xenophon'un ticaret ve para üzerine değerlendirmeler yaptıkları bilinmektedir. Platon, ticaretle uğraşanları daha düşük saygınlığa sahip bir meslek grubu olarak konumlandırırken; Aristoteles, parayı mübadeleyi kolaylaştıran, ticaretin ölçeğini genişleten ve değer saklama işlevi gören bir araç olarak ele almıştır. Xenophon ise tarımı en saygın

uğraş alanı olarak görmüş, özellikle gümüş dışındaki araçların "para" olarak kullanılmasını, arzlarının artırılabilir olması nedeniyle eleştirmiştir. Dinî metinlerde de para ve ticaretle ilişkilendirilen bazı uygulamalara temkinli yaklaşımlar bulunmaktadır. Özellikle faiz, "haksız kazanç" olarak değerlendirilerek üç semavî dinde de yasaklanmaktadır (DOĞRUYOL & AYDINLAR, 2017).

Coğrafi keşiflerle birlikte mal ve hizmetlerin mübadelesi küresel çapta bir eylem haline dönüşmeye başlamıştır. Doğudan Batı'ya doğru akan mal ve hizmet ticaretinin güzergâhları olan Bahar Yolu ile İpek Yolu'na birçok alternatifin çıkması ticareti, dolayısıyla parayı küreselleştirmiştir. Bu süreçte, paraya ve ticarete yönelik hem dini hem de felsefi söylemlerde bir yumuşama başlamıştır. Nitekim Avrupa'da Yahudi tüccarlar ve bankerlerin iktisadî faaliyetlerinin genişlemesi, modern ekonomik yapının dönüşüm dinamikleri içinde sıklıkla tartışılan örnekler arasındadır. Ayrıca Weber'in Protestan Ahlakı ile kapitalizmin gelişimi arasındaki ilişkiyi açıklamaya yönelen yaklaşımı, Hristiyanlığın ticaret ve dolayısıyla parayla kurduğu ilişkinin modern dönemde geçirdiği değişimi anlamada önemli bir analitik çerçeve sunmaktadır.

Avrupa merkezli bir toplumsal değişim olgusu olan modernizmin, gelişen ulaşım ve iletişim araçlarının da etkisiyle dünyanın geri kalanına yayılması, önceki dönemlerin toplumsal değişim süreçlerine bakıldığında son derece hızlı olmuştur. Bu hızın da etkisiyle toplumsal yaşamda, örgütlenme ve iş yapma biçimlerinde yaşanan bu

değişimin yoğunluğu da yayılma süreci kadar etkilidir. Modernlik, on yedinci yüzyılda Avrupa'da başlayıp sonraları bütün dünyaya farklı şekillerde yayılan, toplumsal yaşamda ve örgütlenme biçimlerindeki değişimlerin toplamını tanımlarken kullanılan bir kavramdır (GIDDENS, 2012). Modernizmin getirdiği değişimin yoğunluğunu, insanların bireysel yaşamlarındaki alışkanlıklarını, geçmişten gelen geleneklerinin bir kısmını değiştirmeye veya dönüştürmeye mecbur kalmalarıyla da ölçümleyebiliriz.

Aydınlanma dönemiyle birlikte iktisat alanında uzmanlaşmanın artması ve akademik çalışmaların çoğalması, para üzerine yapılan tanımlamalarda da çeşitlenmeye yol açmıştır. Adam Smith'in ve diğer başka iktisatçıların ifade ettiği gibi para, iktisadi hayattaki değişimler ve uzmanlaşmalar sonucu ortaya çıkması kaçınılmaz bir araçtı (DOĞRUYOL & AYDINLAR, 2017). Anthony Giddens'in parayı "mübadeleyi erteleme aracı" olarak tanımlaması ise paranın toplumsal işlevine ilişkin açıklayıcı bir çerçeve sunmaktadır (GIDDENS, 2012). Buna göre para, bir ürün veya hizmetin başka bir ürün ya da hizmetle doğrudan değişiminin zaman ve mekân koşulları bakımından mümkün olmadığı durumlarda, mübadelenin ileri bir tarihe ötelenmesini sağlayan bir araç işlevi görür.

İki kişi arasında gerçekleşen doğrudan mübadelede, tarafların karşılıklı olarak birbirlerinin sunduğu mal veya hizmete ihtiyaç duyması gerekir. Ancak taraflardan biri, karşı tarafın ihtiyacını karşılayacak mal veya hizmeti sunamıyorsa, doğrudan mübadele mekanizması

işlemeyebilir. Ticaretin görece basit düzeylerde kaldığı dönemlerde değiş-tokuş pratikleri işlevsel bir çözüm sunabilse de ticaret yaygınlaşıp karmaşıklaştıkça doğrudan mübadele birçok durumda yetersiz kalmıştır. Ayrıca çok sayıda mal ve hizmet için ortak bir değer ölçüsünün belirlenmesi de giderek güçleşmiştir. Bu noktada, toplumun geniş kesimlerince ortak değer atfedilen araçların mübadelede aracı rol üstlenmeye başladığı görülmektedir (AYSAN, 2018).

Paranın ortaya çıkışı, mübadele süreçlerinde herkesçe kabul gören ortak bir araca duyulan ihtiyacın belirginleşmesiyle ilişkilendirilebilir. Bu bağlamda para, bir tarafın mevcut ihtiyacını karşılamasına imkân tanırken, diğer tarafın gelecekteki ihtiyacını giderebilmesi için mübadelenin bir kısmını zamansal olarak ileriye taşıyan bir mekanizma üretir. Böylece bir değişim işlemi anlık olarak tamamlanırken, karşılık ilişkisi belirli koşullar altında ileri bir zamana ertelenmiş olur.

Paranın tanımının yanında bazı özelliklerinden ve birtakım işlevlerinden de söz etmek gerekir. Bir aracın para olabilmesi için şu özellikleri taşıması beklenmektedir (ORHAN & ERDOĞAN, 2003);

- Taşınabilirlik: Para olarak kullanılacak aracın kolayca taşınabilmesi beklenir.
- Dayanıklılık: Paranın el değiştirdikçe yıpranıp hasar görmemesi gerekir.

- Bölünebilirlik: Alışverişte değişik miktarlarda ölçeklenebilmeli ve bölünerek her türlü alışverişte kullanılabilir olmalıdır.
- Standardizasyon: Paranın her yerde aynı değerde olması gerekir. Kullanıldığı her bölgede insanların paraya aynı alım gücünü atfetmeleri beklenir.
- Taklit edilememe: Sahtesinin üretilemeyecek derecede güvenli olması gerekir.

Ayrıca paranın bir değer ölçüsü ve fiyatlama aracı olma, tasarruf ve servet saklama, değerli taşınmazların taşınması gibi işlevleri de vardır (AYSAN, 2018).

Önceleri mal veya hizmet değiş-tokuşu (mübadele, trampa, takas, barter) olarak başlayan ticari ilişkiler, sonraları değerli olan şeyler üzerinden mübadeleye dönüştü. Deniz kabukları, tahıl, kumaş, büyük ve küçükbaş hayvanlar gibi çok çeşitli para yerine geçebilecek şeyler kullanıldı (ŞENBAYRAM, 2019).

Paranın ticarette ilk kullanımı günümüzden 5000 yıl öncesine kadar gidiyor. MÖ 3000'li yıllarda Mezopotamya bölgesinde yaşayan Sümerlerin ilk parayı kullanan toplum olduğu, yapılan Arkeolojik kazılarda ortaya konuldu. Arpa para sistemi olarak isimlendirilen bu yöntemde para ölçüsü olarak arpa kullanılıyordu. Sila adı verilen ve yaklaşık bir litreye karşılık gelen bir ölçü birimi vardı. Ancak arpanın bir gıda maddesi olması, kolay bozulabilmesi ve taşınıp depolanmasının zor olması sorunlar çıkarıyordu (AYSAN, 2018).

Tarihsel süreçte farklı nesnelerin mübadele aracı olarak kullanımı çeşitli biçimlerde denenmiş; ancak altın ve gümüş, dayanıklılıkları ve görece taşınabilirlikleri nedeniyle daha "pratik" görülerek yaygınlaşmıştır. Buna rağmen bu metallerin özellikle yüksek miktarlarda taşınması ve saklanması önemli güçlükler doğurabilmekteydi. Bu dönemde ticari işlemler çoğunlukla metalin ağırlığı üzerinden değerlenmekte, dolayısıyla ölçüm, standardizasyon ve bölünebilirlik gibi teknik sorunlar gündeme gelmekteydi.

Paranın icadının Lidyalılara atfedilmesi yaygın bir kabuldür; bununla birlikte bazı çalışmalarda Lidyalıların asıl katkısının, madenî paranın belirli bir standart ve işaretleme sistemiyle dolaşıma sokulması, yani metalin yalnızca ağırlığıyla değil, üzerinde yer alan nominal değer üzerinden işlem görmesi yönünde olduğu belirtilmektedir (FİDAN, DİLEK, & ESEV, 2019). Bu yenilik, ölçüm birimi seçimi, külçenin pratik biçimde bölünebilmesi ve değer tespiti gibi problemlerin önemli bir kısmını azaltmış; ayrıca saklama ve transfer süreçlerini görece kolaylaştırmıştır. Böylece altının yalnızca fiziksel ağırlığına dayalı değişim yerine, sikke üzerindeki değer üzerinden işlem yapılması, mübadele sürecinde standardizasyonun ve güvenin güçlenmesine katkı sağlamıştır.

M.Ö. 6. yüzyılda Lidyalılar altının taşınmasındaki ve bölümlenmesindeki zorluklar nedeniyle altını ve gümüşü ağırlıklarıyla değil, üzerlerinde yazan değerlerle değerlemeye başladılar. Böylece sikke (coin) kullanılmaya başlandı. Aynı ağırlıktaki iki altın sikkenin

birinin alım değeri diğerinden daha fazla olmasının tek nedeni, üzerinde yazan değerin fazla olmasıydı. Bu değer farkının herkes tarafından kabul görmesini sağlayan şey de devlet otoritesi idi. Sonrasında kullanılmaya başlanan kâğıt paralarda aynı şekilde değerlenmektedir ve buna itibari para denir. İtibari para değerini devletin hukuki gücünden alır (FİDAN, DİLEK, & ESEV, 2019).

Çin'de 10. ve 11. yüzyıllarda altın ve gümüş sikke yerine bunlara endeksli ilk kâğıt paraların kullanıldığı bilinmektedir. Özellikle Moğol Hükümdarı Kubilay Han'ın Çin'i yönetimi altına aldıktan sonra bastırdığı kâğıt paraların geniş bir kullanım alanı bulunduğu bilinmektedir. Hatta Marko Polo şahit olduğu kâğıt para basım ve kullanımını "simyacılık" olarak seyahatnamesinde yazmıştır (ERCAN, 2021). Kâğıt parayı ilk kullanan Çinliler aynı zamanda enflasyonla ilk karşılaşan millet de olmuşlardır.

Türk Dil Kurumu enflasyonu şu şekilde tanımlamıştır;

"*Dolaşımdaki para miktarıyla, malların ve satın alınabilir hizmetlerin toplamı arasındaki açığın büyümesinden ortaya çıkan ve fiyatların toptan yükselmesi, para değerinin düşmesi biçiminde kendini gösteren ekonomik parasal süreç; para şişkinliği"* (Türk Dil Kurumu, 1988).

İlk önce altın ve gümüş miktarına endeksli bir şekilde basılan kâğıt paranın sonraları karşılıksız basılması, dolaşımdaki kâğıt paranın miktarını artırmış, bu da mal ve hizmetlerin fiyatlarının para basımıyla aynı oranda artmasına neden olmuştur. Tarihsel örnekler, para arzındaki

genişlemenin denetim dışına çıkması hâlinde kâğıt paranın değerinde aşınma, güven kaybı ve fiyat istikrarsızlığı gibi sonuçların ortaya çıkabildiğini göstermektedir.

Osmanlı'da ilk enflasyonun 1585-1586 yılları arasında madeni paralardaki tağşişler (paradaki değerli maden oranının azaltılması) ile birlikte ortaya çıktığı bilinmektedir. Bu dolaylı para arzının artırımı kolaycılığı üç sene içerisinde fiyatların iki katına çıkmasına neden olmuştur (AYSAN, 2018).

İngiltere de 1717'de sabit kurlu, altına dayalı ilk para tedavüle girmiş, savaş dönemlerinde askıya alınsa da 1931'e kadar varlığını sürdürmüştür. 1818 yılında Hollanda, 1832'de ABD, 1871'de Almanya ve Japonya, 1876 yılında Fransa ve İspanya, 1879'da Avusturya, 1881'de Arjantin, 1893'de Rusya ve 1898'de Hindistan altın standardına geçerek kâğıt para birimlerini altına endeksleştiler. Kabaca 1870-1914 arası klasik altın standardı dönemi olarak isimlendirilir ve bu dönemde neredeyse hiç enflasyon olmamıştır. Hatta bu dönem önemli bilimsel, finansal, teknolojik gelişmelerin olduğu dönem olarak da bilinir (RICARDS, 2017).

3.1.2. Merkez Bankaları ve Bankalar

İnsanlar arasındaki erken dönem ticari ilişkiler, büyük ölçüde doğrudan değiş-tokuş (mübadele) mantığıyla ve aracıya ihtiyaç duyulmadan yürütülmekteydi. Bir kişi elindeki mal veya hizmeti, başka

bir kişiyle karşılıklı ihtiyaç temelinde başka bir mal ya da hizmetle değiştirebilmekteydi. Ancak paranın mübadelede yaygın bir araca dönüşmesiyle birlikte, bu aracın üretilmesi, dolaşıma sokulması, saklanması ve değerinin korunmasına ilişkin süreçler ortaya çıkmış; böylece mübadele ilişkilerine belirli ölçülerde üçüncü tarafların dâhil olması giderek yaygınlaşmıştır. Bu üçüncü taraf kimi dönemlerde bireysel aktörler (ör. tefeciler), kimi dönemlerde kurumsal yapılar (ör. Sümerlerde tapınak ekonomisi bağlamında zigguratlar) ya da siyasal otoriteler biçiminde ortaya çıkabilmiştir. Bu gelişmeler, paranın basımı ve dolaşımı üzerindeki kontrolün siyasal meşruiyet ve egemenlik göstergeleriyle ilişkilendirilmesi sürecini de güçlendirmiştir.

Sanayi Devrimi'nin etkileri ve sömürge imparatorluklarının genişlemesiyle birlikte, söz konusu aktörler ve kurumsal yapılar tarihsel süreç içinde ölçek ve etki bakımından büyümüştür. Devletlerin para basma yetkisini giderek merkezîleştirmesi ve bu yetkiyi tekel niteliğinde kurumsallaştırması, paranın saklanması, transferi ve değerlendirilmesi alanlarında bankacılık kurumlarının gelişimini hızlandırmıştır. Bu bağlamda Amsterdam'da 1609 yılında kurulan Amsterdam Bankası (Wisselbank), modern bankacılık tarihinin erken örnekleri arasında yer almaktadır. Banka, tüccarların yatırdıkları mevduatı belirli koşullar altında geri çekebilmelerine imkân tanımış; farklı para birimleri arasında dönüştürme işlemlerini kolaylaştırmış ve ticari işlemlerde güveni artıran bir altyapı işlevi görmüştür. Hollanda örneğinin ardından İngiltere'de de bankacılık faaliyetleri kurumsallaşmaya başlamış;

böylece Avrupa'da bankacılık pratikleri zamanla yaygınlaşmıştır (DOĞRUYOL & AYDINLAR, 2017).

Ancak devletlerin madeni paralarda tağşiş yapmaları, kâğıt paralarda da sınırsız kâğıt para basmaları bu dönemde ciddi enflasyon ve ekonomik krizlere neden oluyordu. Bunun en yıkıcı örneğin 1921'de Weimar Almanya'sında görüldü. Alman merkez bankası Reichsbank Alman ürünlerinin ihracatını kolaylaştırmak, yabancı yatırım çekmek ve turist gelmesini sağlamak amacıyla Alman Markı'nın değerini düşürerek devalüasyon yapmaya başladı. Devalüasyon öyle çığırından çıktı ki 1922'de Reichsbank durumu kontrol etmeyi bıraktı. 1923'e gelindiğinde ise mürekkepten tasarruf etmek için paraların sadece bir yüzü basılıyordu. Bu süreç Nazi Partisi'nin güçlenmesi gibi birçok ilginç sonuca neden oldu (RICARDS, 2017).

1944 yılında ABD'nin New Hampshire eyaletindeki Carroll kasabasının bir bölgesi olan Bretton Woods'da toplanan Birleşmiş Milletler Para ve Finans Konferansı'nın ardından bir anlaşma imzalandı. Konferans, savaş nedeniyle bozulan uluslararası ticaretin yeniden düzene sokulmasını hedefliyordu. Konferans sonunda tarihe toplantının yapıldığı bölgenin adıyla geçen Bretton Woods Anlaşması imzalandı. Buna göre uluslararası ticarette ortak para birimi olarak Amerikan Doları kullanılacaktı. Ülkelerin para birimleri Amerikan Doları'na endekslenecek ve Amerikan Doları'nın da altın ile konvertibilitesi sağlanacaktı. Bir ons altın 35 Dolar'a sabitlendi. Ülkeler Amerikan Merkez Bankası'na koydukları altın karşılığında Dolar alacaklar ve

ticaretlerinde bu Dolar'ı kullanacaklardı. İsteyen ülke de elindeki Dolar'ı Amerikan Merkez Bankası'na getirdiğinde karşılığı olan altını alacaktı. Ancak işler uzun süre bu şekilde yürümeyecekti. Özellikle Vietnam Savaşı'nın maliyetlerini karşılamakta zorlanan Amerikan yönetimi, karşılıksız para basmaya başladı. Altın karşılığı basılması gereken Dolar'ın karşılıksız basılması, Bretton Woods Anlaşması'na taraf ülkelerde huzursuzluğa neden oldu. Sabit kalan altın rezervine karşılık Dolar'ın arzı sürekli artıyordu. Vietnam Savaşı, Soğuk Savaş giderleri ve ekonomik vaatlerinin yerine getirilmesi gibi birçok gider kalemini karşılamak için para basıldı. İlk başta Fransa, Amerikan Merkez Bankası'na teminat olarak bıraktığı altını geri istedi. Sonra diğer ülkeler de sıraya girince 1971 yılında ABD Başkan Richard Nixon, Amerikan Dolarının altın ile olan bağının koparıldığını açıkladı (RICARDS, 2017).

Birinci Dünya Savaşı, Britanya İmparatorluğu'nun küresel güç kapasitesini önemli ölçüde zayıflatmış; bu zayıflama, uluslararası finans ve ticaret düzeninde İngiltere'nin belirleyici rolünün aşınmasına zemin hazırlamıştır. Bu sürecin bir yansıması olarak İngiltere, 1931 yılında altın standardını terk ederek sterlinin altınla olan bağını sonlandırmıştır. Uluslararası ticarette yaygın biçimde kullanılan sterlin, savaş sonrası dönemde ekonomik kapasitedeki gerileme ve artan kırılganlıklar nedeniyle değer kaybı yaşamıştır (KURUÇ, 2016). İkinci Dünya Savaşı sonrasında küresel güç dengelerinin ABD lehine değişmesi, doların uluslararası sistemde merkezî bir konum edinmesini kolaylaştırmış;

ancak altına dönüştürülebilirlik taahhüdünün sürdürülebilirliği zaman içinde tartışmalı hâle gelmiştir.

Paranın karşılıksız ve sınırsız basılabilmesi, teminat veya güven açısından sadece parayı basan ülkenin itibarının tek gerçeklik olması, Fiat Para denilen günümüz para sistemini ortaya çıkardı. Günümüzde para birimlerinin değeri, parayı basan ülkenin ekonomik, siyasal, sosyal, askeri ve daha birçok açıdan ortaya koyduğu itibar ile ölçülüyor. Bu noktada yöneticilerin kararları ve uygulamaları, ülkelerin para birimlerinin diğer ülkelerin para birimleri karşısında nasıl değerleneceğini belirleyen en büyük etmen durumunda. Halklar, yöneticilerine her zamankinden daha fazla güvenmek zorundalar. Bu güvenin kaybolduğu durumlarda da başta enflasyon olmak üzere ekonomik, siyasi ve sosyolojik sorunlar baş gösteriyor.

Ticaretin, toplumsal düzenin kurulmasında ve doğru bir şekilde işleyebilmesinde hayati bir önemi vardır. Sağlam bir zeminde işleyen ticaret, toplumların ekonomik olarak refaha kavuşmalarına katkı sağlar. Ancak ticaretin rahat bir şekilde yapılabilmesi için kullanılan paranın değerinin korunması gerekiyor. Paranın değerinin korunması üzerine kurgulanan sistem kırılgan dengeler üzerinde kurulmuşsa, bu kırılgan dengelerin her bozulduğu durum önce ekonomiyi sonra da toplumsal düzeni olumsuz etkileyecektir.

Altın, gümüş gibi kıymetli metaller herkes tarafından ortak bir değer olarak göründüğü için ve arzlarının sınırlı olmasından dolayı ticarette ortak bir mübadele aracı olarak kullanıldı. Ancak metallerin

taşınması ve saklanması zor olduğundan, altın yerine geçebilecek kâğıt banknotların kullanılması pratikte büyük kolaylık getirmiş olsa da, değerli metallerin sınırlı olan arzlarının kâğıt muadillerinde olmaması işleri zorlaştıran en önemli unsurdu. Hem küresel ticarette hem de halk arasındaki kısa mesafeli ve düşük yoğunluktaki ticarette kâğıt paranın büyük kolaylıklar sağladığı tartışılmaz bir gerçektir. Ancak gelişen teknolojilerle birlikte kâğıt para da yeni ihtiyaçları tam olarak karşılayamamaktadır.

Zaman içerisinde ödeme yöntemlerinde yeni araçlar devreye girmiştir. Kredi kartları ile havale/EFT gibi bankacılık temelli çözümler, internetin yaygınlaşmasıyla birlikte gündelik ekonomik ilişkilerde daha geniş ölçekte kullanılmaya başlanmıştır. Benzer biçimde PayPal gibi çevrimiçi ödeme hizmetleri ile Google Pay/Google Wallet, Apple Pay, WeChat Pay ve Alipay gibi dijital cüzdan uygulamaları, mobil cihazların bir ödeme aracı olarak kullanılmasını mümkün kılan altyapılar sunmuştur. Dijital (e-) cüzdan olarak adlandırılan bu uygulamalar, nakitsiz ticareti kolaylaştırdığı gibi hem çevrimiçi hem de fiziksel alışverişlerde ödeme süreçlerini hızlandırarak işlem maliyetlerini azaltabilmektedir.

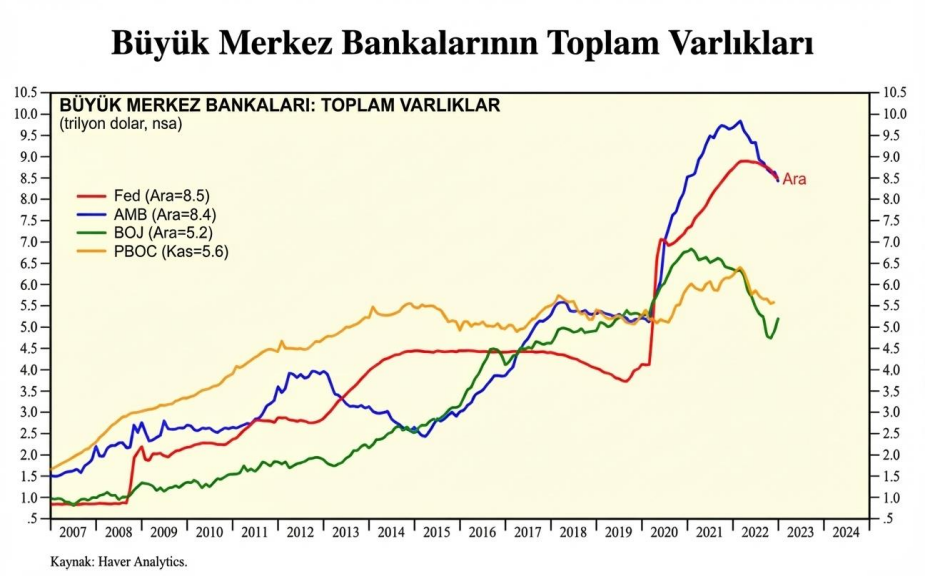
Bu ödeme biçimlerinin ortak özelliklerinden biri, belirli kurumsal aktörler tarafından işletilen merkezî altyapılara dayanmasıdır. Merkez bankaları, bankalar veya ödeme kuruluşları tarafından organize edilen bu sistemlerde, işlemlerin doğrulanması, takası ve mutabakatı belirli kurumların kurallarına ve teknik kapasitesine bağlıdır. Bu durum,

ödeme ekosisteminin işleyişinde kurumsal güvenin önemini artırırken, aynı zamanda kullanıcıların belirli altyapılara bağımlılık geliştirmesi sonucunu doğurabilmektedir. Örneğin kredi kartı kullanımı, hem ilgili bankaya ve ödeme ağına duyulan güveni hem de daha geniş ölçekte para politikasını belirleyen kurumsal çerçeveye yönelik güveni gerektirmektedir.

Bu güven ve merkezileşme aynı zamanda bağımlılığı da beraberinde getirmektedir. Merkezî ödeme altyapılarına bağımlılığın sonuçları, uluslararası kriz ve yaptırım süreçlerinde daha görünür hâle gelebilmektedir. Nitekim Rusya–Ukrayna savaşının başlamasının ardından bazı Batılı ülkelerin Rusya'ya uyguladığı yaptırımlar kapsamında, belirli kişi ve kurumlara yönelik varlık dondurma uygulamaları gündeme gelmiş; ayrıca bazı Rus bankalarının SWIFT sisteminden çıkarılması ve Visa ile Mastercard'ın Rusya'daki faaliyetlerini askıya alması gibi gelişmeler ödeme sistemlerine erişim üzerinde doğrudan etkiler üretmiştir. Milyonlarca Rus vatandaşının bireysel sesi ve mağduriyeti bu süreçte göz ardı edilmiştir. Bu örnek, ödeme ve finansal altyapıların merkezî aktörler tarafından yönetilmesinin, ülkeleri ve bireyleri ekonomik ve toplumsal açıdan nasıl etkileyebileceğini gösteren güncel bir vaka olarak değerlendirilebilir.

Bir diğer güncel örnek ise 2020 yılının başlarında yaşamaya başladığımız pandemi sürecinde küresel çapta yaşandı. Pandemi tedbirleri nedeniyle uygulanan sokağa çıkma yasaklarından dolayı arzda ve talepte büyük düşüşler yaşandı. Bu nedenle ülkelerin ekonomileri bu

süreçten büyük zarar gördü. Yönetimler de çalışamayan ve gelir elde edemeyen vatandaşlarının mağduriyetlerini gidermek amacıyla devlet hazinelerinden yardımlar yapmak zorunda kaldılar ancak bu yeterli olmadığında dolayı merkez bankaları büyük miktarlarda para basmak zorunda kaldı (CİNEL, 2021).



Şekil 5: Dört büyük merkez bankasının para basma grafiği

Şekil 5 deki grafikte de görüldüğü gibi dört büyük merkez bankası (FED – Amerikan Merkez Bankası, ECB – Avrupa Merkez Bankası, BOJ – Japon Merkez Bankası, PBOC – Çin Merkez Bankası) özellikle 2008 Küresel Ekonomik Krizi'nden sonra hızlı bir şekilde para basmaya başladılar. Covid-19 tedbirleriyle birlikte para basma hızı ciddi

miktarlarda arttı ve Ocak 2023 itibariyle bu parasal genişlemenin etkilerini azaltmak ve artan enflasyonu dizginleyebilmek için merkez bankaları ciddi faiz artırımlarına gitmeye başladılar. Bu da ekonomilerin resesyon denilen durağanlaşma sürecine girmesine ve işsizliğin artmasına neden oldu (KÜÇÜKBAY, UYSAL, & ÇIRAK, 2022).

Bu örnekler, paranın üretimi ve dolaşımının merkezî aktörler tarafından belirlenmesinin, kriz ve olağanüstü dönemlerde ekonomik ve toplumsal etkiler üretebildiğini göstermesi bakımından dikkate değerdir. 2008 yılında ABD'de konut finansmanı piyasalarında başlayıp küresel ölçekte genişleyen finansal krizin ardından, Satoshi Nakamoto tarafından dolaşıma sokulan Bitcoin tasarımı, para arzının sınırlandırılması ve işlemlerin merkezî aracılara ihtiyaç duymadan doğrulanabilmesi fikrini gündeme taşımıştır. Bu çerçevede Nakamoto, tarafların birbirine güven duymasını zorunlu kılmayan, doğrulama ve kayıt süreçlerinin dağıtık bir ağ üzerinde yürütüldüğü bir dijital para sistemi önermiş; sistemi "Bitcoin" adıyla tanımlamış ve çalışmanın erken bir sürüm olduğunu belirterek geliştirme sürecine katkı çağrısında bulunmuştur.

Günümüzde kullanılan fiat para, fiziksel taşıyıcısı (kâğıt banknot) bakımından sınırlı bir maddî değere sahip olmakla birlikte, değerini büyük ölçüde toplumsal kabule ve onu ihraç eden otoritenin kurumsal güvencesine dayalı olarak sürdürmektedir. Benzer şekilde Bitcoin ve diğer kripto varlıklar da fiziksel bir emtiaya karşılık gelmeyen, dijital ortamda üretilen ve saklanan kayıtlardan oluşur.

Bununla birlikte Bitcoin'i ayırt eden özellik, işlemlerin doğrulanması ve kayıt altına alınması süreçlerinin, merkezî bir otoriteye başvurmaksızın, ağ katılımcılarının uzlaşması yoluyla yürütülmesidir. Bu işleyişin temelinde, İş Kanıtı (Proof of Work, PoW) olarak adlandırılan uzlaşma mekanizması yer almaktadır. PoW modelinde ağın güvenliği ve işlemlerin doğrulanması, yüksek hesaplama gücüne dayalı rekabetçi bir süreç üzerinden sağlanmakta; bu durum, sistemin çalışması için donanım yatırımı ve enerji tüketimi gibi maliyet kalemlerini beraberinde getirmektedir.

Bu noktada Bitcoin'in enerji tüketimi, literatürde ve kamuoyunda önemli bir tartışma başlığıdır. Eleştiriler, PoW mekanizmasının yüksek enerji kullanımına yol açtığını ve bunun çevresel maliyetler ürettiğini vurgularken; savunular ise ağ güvenliğinin ve değiştirilemez kayıt yapısının belli bir maliyetle tesis edildiğini ileri sürmektedir. Ayrıca geleneksel finansal altyapıların da (banka şubeleri, veri merkezleri, ödeme ağları, personel ve operasyonel giderler gibi) önemli kaynak kullanımını gerektirdiği; dolayısıyla maliyet kıyaslamalarının farklı boyutları dikkate alarak yapılması gerektiği ifade edilmektedir.

Blokzinciri teknolojisinin toplumsal açıdan gerçekleştirdiği en büyük devrim, paranın üretilmesi, saklanması, transferi ve tüm bu işlemlerin kayıt altına alınmasını merkeziyetsiz bir hale getirmiş olmasındır. Bu haliyle aslında paranın aracılık ettiği ticaretin, aracılardan kurtularak ve bu aracıların neden olduğu hatalardan,

suiistimal veya manipülasyonlardan arınarak ilk zamanlardaki statüsüne kavuşmasını sağlayacaktır. Blokzinciri teknolojisi sayesinde para, toplum tarafından üretilen, arzı toplum tarafından kontrol edilen yani tüm parasal organizasyonun toplum tarafından yapıldığı ilk haline, ilk işlevine geri dönebilme ihtimaline sahip olmuştur.

Günümüzde insan, tükettiği ürünlerin neredeyse hiçbirini kendi üretmiyor. Bu sebepten dolayı da ihtiyaç duyduğu şeyi alabilmek için paraya sahip olması gerekiyor. Modern hayatın her geçen gün artarak sunduğu imkânlardan faydalanmak isteyen insan için para, her zamankinden daha değerli oldu. Bu şekilde modern insan, paraya bağımlı hale geldi. Dünyanın her yerinde insanlar bir şekilde para ulaşmak için verdikleri mücadelelerle ve uğraşlarla günlerini geçiyorlar.

Paranın tüm insanlar için bu denli önemli olduğu günümüzde, bu alanda çalışan gerek kamu gerekse özel sektör kurum ve kuruluşlarının yaptıkları hatalar, suiistimaller, manipülasyonlar küresel etkileri olan olaylara dönüşebiliyor. Finansal ürün ve hizmetlerin merkezi tekellerin kontrolünde ve güdümünde olmasının (hem geçmişte hem de özellikle pandemi sonrası dönemde şahit olduğumuz haliyle değerlendirdiğimizde) küresel huzur ve refah açısından olumsuz sonuçlar doğurduğunu düşünüyoruz. Merkez bankalarının yürüttükleri yanlış para politikaları, ülke para birimlerinin değerlerinin düşmesi sonucu, halkların emeklerinin karşılığını yeterince alamamalarına, dolayısıyla toplumların fakirleşmelerine neden oluyor.

Her geçen gün daha fazla dijitalleşen dünyada geleneksel finansal sistemin güncel sorunlara gerekli ve yeterli çözümler üretemediği görülmektedir. Her ne kadar dijital dönüşüme ayak uydurmak için sürekli olarak bu alanlarda çalışmalar yapsalar da, asıl sorunları merkezi yapılarından kaynaklanmaktadır. Para politikalarının belirlenmesinde merkez bankaları, bu politikaların işletilmesinde de özel veya kamuya ait finansal kurumlar, hızla değişen toplumsal sisteme ayak uyduramamaktadırlar. Web 2.0 ekosisteminin yaygınlaşması, kullanıcıların yalnızca hizmet tüketicisi olmanın ötesinde, süreçlere katılım ve söz sahibi olma talebinin güçlendiğini göstermiştir. Bununla birlikte mevcut siyasal ve kurumsal mekanizmaların, bu katılım beklentilerini her durumda karşılayabildiği söylenemez.

Blokzinciri teknolojisinin, bir taraftan insanların kendilerini ilgilendiren (mesela para ile ilgili) meselelere daha demokratik bir şekilde katılımlarını sağlarken, diğer taraftan da merkezi yapıların sistemlerini daha şeffaf ve katılımcı olacak şekilde düzenlemelerini sağlayacak fırsatlar sunduğunu düşünüyoruz.

3.2. Toplumsal Sözleşme'nin Yeniden Yorumlanması

İnsanların neden bir siyasal otoriteye ve devlet idaresine ihtiyaç duyduğu; hangi gerekçelerle ve hangi karşılıklar üzerinden birtakım özgürlüklerinden feragat ederek otoriteye yetki devrettiği sorusu, siyaset felsefesinin en köklü tartışma alanlarından biridir. Antik dönemden itibaren birey–toplum–devlet ilişkisini tanımlama ve açıklama

girişimleri bulunsa da modern dönemde bu ilişkiyi sistematik bir çerçevede ele alan yaklaşımların başında Thomas Hobbes gelir. Hobbes, ilk modern dönem siyaset felsefecisi olarak kabul edilir. Devletin temel dayanağını akılcı nedenlere bağlayarak, bireysel özgürlükleri ve siyasal otoriteyi birleştirmeye çalışmıştır. Hobbes'a göre devlet, otoritesinin meşruiyetini ilahi bir zeminden değil, bireylerin özgür rızaları ve kabulleriyle birlikte gelen rasyonel bir zeminden yani "toplumsal sözleşme" den almaktadır (AYDIN, 2022).

Hobbes'un hemen ardından Jean-Jacques Rousseau ve John Locke da toplumsal sözleşme konusu üzerinde durmuşlardır. "Doğa Durumu" (the state of nature) olarak kavramsallaştırdıkları, insanın tüm otoritelerden bağımsız, birbirine karşı eşit bir ilişki içerisinde oldukları ve böylece özgürlük içerisinde yaşadıkları bir konumdan yola çıkarlar. Böylesi bir tasarımda birey, haklarını korumak amacıyla bir diğerini öldürme hakkına bile sahiptir (FABRE, 2018). Toplumsal sözleşme, bireyin doğa durumundan sıyrılarak uygar insan konumuna geçişini anlatır (AYDIN, 2022).

Doğa durumunda kimse kimseye hükmetmediği için herkes birbiriyle eşit seviyededir. Bireyler arasında herhangi bir bağımlılık olmadığından dolayı da herkes özgürdür. Asıl sorun insanların birbirleriyle iş yapmaya başladıklarında veya karşılıklı iletişime geçmeye başladıklarında ortaya çıkmaktadır (FABRE, 2018).

Bireyin doğa durumu gereği kendi çıkarlarını korumaya hakkı vardır. Birey bu haklarını kendi iradesiyle devlet otoritesine devrederek

ve kendisi gibi aynı taahhütte bulunan insanlarla beraber devletin yaptırım gücünü kabullenerek bir sosyal sözleşme imzalamış olur. Klasik dönem teorisyenlerine göre insan aklını kullanarak bu seçimi yapar. Rasyonel düşünce gereği bireyin en yüksek faydayı sağlayacağı seçenek budur. Doğa durumunda her konuda özgür olan birey, kendi rızası ile bir devlet otoritesinin altına girdiğinde, hem bazı özgürlüklerinden feragat eder hem de bazı yaptırımlara uyacağını taahhüt eder. Bu kısıtlamalara rıza göstermesinin nedeni, diğerlerinin de aynı şartlarda bu sözleşmeyi kabul ettiklerini ve aynı yükümlülükler altına girdiklerini bilmesidir.

Buradaki rıza meselesi de tartışmalıdır. Devletin otoritesini kabul etmeyen, bu sözleşmenin bağlayıcı sınırlarına girmek istemeyen kişilerin durumları, teorisyenler tarafından değişik şekillerde ele alınmıştır. Asıl soru şudur; insanlar gerçekten bir sözleşmeye rızaları ile taraf olduklarından dolayı mı yoksa yaptırımlardan ve alacakları cezalardan dolayı mı devlet otoritesine itaat ederler? İnsanlar bilinçli ve rasyonel tercihlerinin sonucu mu yoksa zorlandıkları ve korktukları için mi devlet otoritesini kabul ederler?

20. yüzyılın önemli siyaset felsefecilerinden olan John Rawls'da, Kant gibi bireysel hakların dokunulmazlığına dikkat çeker. İki düşünür de bireylerin birer araç olarak görülemeyeceğini, çoğunluğun iyiliği için bireyin hak ve özgürlüklerinin yok sayılamayacağını, kısıtlanamayacağını savunurlar. Rawls, toplumsal sözleşme kuramını yeniden gündeme getirmiş ve ele almıştır. Rousseau,

Locke, Hobes ve Kant gibi düşünürlerin gelişiminde katkıda bulundukları toplumsal sözleşme anlayışını yeniden ele alarak bu amaca uygun bir adalet anlayışı geliştirmeye çalışmıştır. Amacı her bir bireyin özgürce seçimini yapabileceği, bireysel farklılıkları kabul eden, adalet temelli bir toplum teorisi ortaya koymaktır. Doğa durumu kavramı yerine koyduğu başlangıç durumu tanımlamasında, insanlar başlangıçta her konuda eşittirler. Başlangıç durumunda insanlar kendilerini yönetecek olan adalet ilkelerini belirlemek için bir araya gelirler. Başlangıç durumu, kimsenin birbirine herhangi bir üstünlüğünün olmadığı bir noktadır. Rawls'a göre eğer adil bir toplumsal düzen kurulacaksa böylesi bir başlangıç durumunun kurgulanması gerekmektedir (AYDIN, 2022).

İnsanları temelde bencil ve kötücül gören Hobbes'un aksine Rawls, insanların birbirlerine zarar vermelerini engelleyen ahlaki değerlere sahip olduklarını düşünür. Rawls'un toplumsal sözleşme yorumunun temelinde ahlaki yaklaşım yer almaktadır. Ona göre toplumsal sözleşme, ahlaki kaygılarla yola çıkılarak rasyonel bireyler tarafından adalet ilkesine göre tanımlanmalıdır. Hobbes'un aksine insanlar bir çatışma durumunu sona erdirmek için veya korkularından dolayı değil ahlaki kaygılardan dolayı toplumsal sözleşmeyi ortaya koyarlar ve ona uyarlar (AYDIN, 2022).

İnsan doğasının tanımlanması, insanların birbirleriyle olan münasebetlerinin hangi temelde şekilleneceği, bu münasebetleri düzenlemek için ortaya konulacak olan ilkeleri, devletin varlığını,

sorumluluk alanını ve birey devlet ilişkilerini tanımlamaya çalışan toplumsal sözleşme teorisi, zaman içerisinde farklı açılardan ele alınmış olsa da günümüzde tartışılmaya devam edilmektedir.

Devlet-birey-toplum ilişkisinin doğru şekilde düzenlenmesinde gösterilen çabalar, sonucunu Sanayi Devrimi sürecinde kendini göstermiş ve bu organizasyonu doğru şekilde kurup işleten toplumların, süreç içerisinde belirgin bir şekilde diğerlerinden ayrışmasına ön ayak olmuştur.

İki bireyin arasına bir üçüncü düzenleyici otorite olarak devletin girmesindeki asıl neden, bireylerin birbirine karşı olan güvensizlikleridir. İster ahlaki nedenlerle olsun ister korku ve kaygı temelli olsun sonuçta insanların birbirlerine güven duymaya gerek olmadan iş yapabilmelerini sağlamaya yöneliktir bütün bu uğraşlar. Basit bir ticarette bile tarafların birbirlerine güven duymalarını gerektiren birçok durum vardır. Dolayısıyla güven duyulması gereken noktada mutlaka şüphe de kendini göstermektedir. Bu sebepledir ki insanlar, bir üst otoritenin kararlarına itaat etmeyi kabul ederek, gerektiğinde yaptırıma bile uğrayabileceğini bilerek ve kabullenerek, diğerine karşı güven duymak zorunda olmadan, onunla irtibata geçebilme özgürlüğüne kavuşmayı amaçlamaktadırlar.

Sonuçta güven her şeyin temelinde yatan olgudur. Üçüncü taraf olarak devletin konumlandırılmasında da güven yine başat aktördür. Taraflar, devlet mekanizmasının herkese aynı şekilde yaklaşacağı

varsayımı üzerinden yola çıkarak hareket ederler ve bu konfor alanı içerisinde faaliyetlerini gerçekleştirirler.

Bu nokta da devlet mekanizmasının iyi organize edilmiş olması, en çetrefilli konularda bile tarafların rızasını kazanacak şekilde, zararı en aza indirip faydayı en yukarıya çekecek sistematiği doğru biçimde işletebilmesi beklenir. Bu sanıldığı kadar da kolay bir şey değildir. Doğru kanunların çıkarılması, bu kanunların yürütme erki elinde doğru şekilde işletilmesi ve anlaşmazlık durumlarında da yargının kendisinden beklenen şekilde adaletli davranabilmesi gibi eş güdüm halinde çalışması gereken büyük bir mekanizmadan bahsediyoruz.

Her ne kadar iyi bir sistem kurulsa da sonuçta her şey gelip güven mevzuuna dayanmaktadır. Siyasetçinin doğru kanunları çıkaracağına, bürokratın bu kanunları doğru bir şekilde işleteceğine, yargının da bunu en ideal şekilde denetleyeceğine olan güven. Aslında burada duyulan güven hissi, sistemden çok o sistemi işletecek olan insanadır. İşini doğru bildiğine, bu konuda yetkinliğinin tam olduğuna, doğru ve dürüst bir şekilde işini yapacağına, kimseyi kayırmayacağına, toplumun ve sistemin menfaatini üstün tutarak işini yapacağına karşı duyulan güven.

Ne yazık ki insan faktörü devreye girdiğinde sonuçlar her zaman beklendiği gibi gerçekleşmeyebiliyor. İnsani birçok etken (liyakatsizlik, adam kayırma, kişisel menfaat vb.) kurulan sistemden istenen verimin alınamamasına neden olabiliyor.

Peki, güven gerektiren bazı durumlarda insan faktörünü devreden çıkarabilseydik nasıl olurdu? Öyle ya, Sanayi Devrimi boyunca insani zayıflıklarımızı bertaraf edecek makineler geliştirmeyi öğrendik ve bu çok da işimize yaradı. İnsanın yapamayacağı hızda, yoğunlukta ve güçte işleri yapmak için makineler geliştirdik. İşlerimizi onlara yaptırdık. Yük taşımak için gemiler, trenler, büyük kamyonlar ürettik. Daha hızlı gidebilmek için uçaklar, otomobiller icat ettik. Fabrikalarda daha hızlı üretebilmek için otomasyon sistemleri geliştirdik.

Makinaları bedensel işlerimizi yapmaya yardımcı olarak kullandık. Elektronik Biliminin gelişmesiyle de bunu bir üst aşamaya taşıdık. Zihinsel olarak yaptığımız işlerde bize yardımcı olmaları için bilgisayarları tasarladık. Bilgisayar teknolojileri artık karar vermek mekanizmalarında da bize yardımcı olabilecek seviyeye gelmiş durumdadır. Donanım ve yazılım alanındaki gelişmeler sayesinde bunu yapmak mümkün artık.

Bireylerin Toplumsal Sözleşme'nin gereği olarak devlet erkine verdikleri bazı yetkileri, şeffaf bir şekilde tasarlanmış, titizlikle kurgulanmış, büyük bir gizlilikle de çalışabilen, en önemlisi de merkeziyetsiz bir şekilde çalışmaya başladığında kimse tarafında yönetilemeyen/yönlendirilemeyen/kontrol edilemeyen, insani zaaflardan berî bir şekilde çalışabilen, üzerinde sadece (toplumsal sözleşmeye de atıfla) bir konsensüsle düzenlemenin yapılabildiği bir sisteme devretmekten bahsediyoruz.

Önümüzde 2009'dan bu yana kesintisiz bir şekilde çalışan, bir para sistemi olarak tasarlanmış Bitcoin örneği var. Üstelik Bitcoin, tasarımcısının da belirttiği gibi bir deneme sürümüdür. En başta belirlenen kurallar çerçevesinde çalışmaya devam ediyor. Herhangi bir yöneteni, düzenleyicisi, sahibi yok. Eğer Bitcoin yazılımı üzerinde bir düzenleme yapılmak isteniyorsa, dünyanın dört bir yanına yayılmış binlerce, on binlerce düğüm sahibinin rızasının alınması gerekiyor. Üstelik isteyen herkes bu sistemde söz sahibi olabiliyor.

Bir önceki başlıkta ele aldığımız para meselesinde de görüldüğü üzere, ülkelerde para politikalarını düzenlemek amacıyla çalışan kurumaların yaptıkları hatalar ve yanlışlar toplumlara ekonomik ve toplumsal açıdan zarar vermektedir. Özellikle pandemi sonrasında yanlış para politikalarının sonucu olarak bütün dünyada yaşanan enflasyon sorunu küresel çapta birçok sıkıntıya neden olmuştur. Geçmişte de birçok kez aynı hataların tekrarlandığını görülmektedir.

Sadece para örneğinden bile yola çıkarak diyebiliriz ki, toplumsal sözleşme gereği bazı kurumlara devrettiğimiz bazı özgürlüklerimizi, yeniden kurgulanmış bir toplumsal sözleşme düzleminde ele alarak, makinelerin işletebileceği, kimseye güven duymak zorunda kalınmayacağı, çalışmasına dışarıdan müdahale edilemeyecek güvenli mekanizmalara devredebileceğimiz kanaatindeyiz.

SONUÇ

Toplumsal sözleşme, insanların ister korku ve kaygıları, isterse ahlaki gerekçelerle olsun bir araya gelip rasyonel bir zeminde birbirleriyle olan münasebetlerini düzenledikleri, adalet temelli, bireyi önceleyen bir toplumsal düzen arayışıdır.

Toplumsal düzeni sağlama arayışında, birçok teorinin ve hatta ideolojinin zaman içerisinde ortaya çıktığını ve dünyanın farklı bölgelerinde bunlardan bazılarının uygulama alanları bulduklarını görmekteyiz. Sonuçta insanlar ister kendi iradeleri, isterse bir başkasının zoruyla olsun bir çeşit toplumsal sözleşmeye uymak zorundadır.

Günümüzde de farklı ülkelerde birbirinden çok farklı yönetim biçimleri altında insanlar hayatlarını sürdürmeye devam etmektedir. Geçmişte olduğu gibi günümüzde de (ve muhtemelen gelecekte de) insanlar daha adil bir toplumsal düzen arayışı içerisinde olmuştur/olacaklardır. Gelişen teknoloji sayesinde bu arayışa yeni bir yorum getirmenin de mümkün olduğu söylenebilir.

Tıpkı makine ve alet kullanarak bedensel manadaki zayıflıklarımızı aşmaya çalıştığımız gibi benzer şekilde modern toplumun ihtiyaçları ve geleceğin toplumsal düzenini oluşturmak üzere teknolojiye ve Bitcoin örneğinde olduğu gibi Blokzinciri teknolojisini kullanmamız mümkündür.

Burada kastedilen, devlete devredilen bütün özgürlüklerin bir çırpıda merkeziyetsiz organizasyonlara dönüştürülmesi değildir. En

azından Toplumsal Sözleşme'nin bu bağlamda ele alınarak yeniden değerlendirilmesi bile iyi bir başlangıç olabilir. Merkeziyetsiz organizasyonların hayata geçmesi ne şekilde adlandırılırsa adlandırılsın, insanın insan olmasından kaynaklı doğal özgürlüklerini bağımsız olarak kullanabilmesinin yolunu açması nedeniyle son derece önemli bir adımdır. İnsan, bu özgürlüklerden vazgeçecekse veya devredecekse bile çok daha sağlıklı şekilde işleyen bir mekanizmaya bu görevi devretmesi elzemdir. Blokzinciri teknolojisi kişi ve kurumlardan bağımsız olarak insana bu özgürlüğünü bağımsız bir şekilde kullanabilme imkânı vermesi nedeniyle son derece avantajlı bir konumdadır.

Nitekim, Blokzinciri teknolojisi, insanların birbirlerine veya bir üst otoriteye güvenmek zorunda kalmadan merkeziyetsiz organizasyonlar kurmalarına olanak vermektedir. Çünkü bu teknoloji yapısı gereği merkezi organizasyonlara olan ihtiyacı gereksiz kılmaktadır. Toplumsal bir mutabakata ihtiyaç duymadığı gibi, kişi ya da kurumlara güvenmek zorunluluğunu da ortadan kaldırmaktadır. Henüz daha emekleme aşamasında olan bu teknolojinin, zamanla çok daha güvenli bir hale geleceğini tahmin etmek zor değildir. İlk Blokzinciri örneği olan Bitcoin'in ortaya çıktığı 2009 yılından beri, bu alanda yapılan çalışmalara ve ortaya çıkan yeni teknolojilere bakıldığında denilebilir ki; Blokzinciri teknolojisi sadece teknolojik veya finansal çözümler sunmamakta, bunun yanında hukuktan ahlaka birçok alanda yeni toplumsal çözümler üretmemize de imkân tanımaktadır.

Böylece karar verme veya uygulama aşamalarında, geniş katılımla varılan toplumsal uzlaşmaya aykırı hareket etme gibi bir durum da ortadan kalkmaktadır. Üzerinde uzlaşmaya varılan ortak amaca zarar verecek, kişisel hatalardan, zaaflardan, eksikliklerden ve art niyetlerden korunmuş bir toplumsal düzen inşa etmenin teorik imkânı dikkate alındığında bunun sadece Blokzinciri teknolojisi ile mümkün olabileceği anlaşılmaktadır.

İnsanların, alışılagelmiş merkezi yönetim biçimlerinden vazgeçmesi elbette kolay olmayacaktır. Zaten bu dönüşüm sürecinin de kısa zamanda tamamlanabilmesi mümkün değildir. Toplumların merkezi yapılardan merkeziyetsiz organizasyonlara geçmeleri elbette zaman alacaktır. Ancak bu süreç Bitcoin'in hızlı bir şekilde hayatımıza girmesi ile birlikte çoktan başlamıştır. Sürecin henüz daha çok başında olsak bile özellikle genç neslin Blokzinciri teknolojilerine büyük ilgi gösterdiği gözlemlenmektedir. Blokzinciri alanında ortaya konulacak yeni çözümler ve bu çözümlerin toplumlar tarafından ne şekillerde sahiplenileceği, sürecin de nasıl ilerleyeceğini belirleyecektir.

Aldous Huxley'in "Cesur Yeni Dünya"sı veya George Orwell'in "1984" romanındaki gibi distopik bir geleceği teknoloji ile inşa etmek pekâlâ mümkündür. Ancak tam tersi, özgürlüklerin çok daha geniş ve rahatça uygulanabildiği bir ütopyayı da teknolojik imkânları kullanarak inşa etmek olasıdır. Merkeziyetsiz toplum idealinin bir ütopya mı yoksa mümkün bir ideal mi olduğunu, bu alanda mesai harcayan insanların gayretleri ve toplumların iradesi belirleyecektir.

Bilgi Notu

Bu çalışma 2024 yılında Prof. Dr. Sinan Yılmaz danışmanlığında Halit Gürleyik tarafından hazırlanan "Merkeziyetsiz Toplum: Blokzinciri teknolojisinin toplumsal yansımaları" başlıklı Yüksek Lisans tezinin incelenip yeniden gözden geçirilmiş ve kitap formatına çevrilmiş baskısıdır.

KAYNAKÇA

Akbulut, R. (2010). Son Yaşanan Küresel Finansal Kriz ve Türk Finans Sektörü Üzerine Etkileri. *Akademik Araştırmalar ve Çalışmalar Dergisi*, 45-68.

Arapoğlu, F. (2021, 06 30). Sanatta Aktüel Gündem: Kripto Sanat (NFT). *Sosyal Bilimler Dergisi*, s. 91-93.

Arvas, İ. S. (2022, 02 28). Gutenberg Galaksisinden Meta Evrenine: Üçüncü Kuşak İnternet, Web 3.0. *AJIT-e: Academic Journal of Information Technology*, s. 53-71.

Arvas, İ. S., & Zamur Tuncer, R. (2023, 07 01). Kavram Karmaşasının Gölgesinde Blokzincirinin Matruşkası: Bitcoin, Blokzinciri, Web 3.0 ve Metaverse. *İnsan Ve İnsan*, s. 71-87.

Ashmore, D., & Powell, F. (2023, 06 14). *Bitcoin Price History 2009 to 2022.* Forbes: https://www.forbes.com/advisor/in/investing/cryptocurrency/bitcoin-price-history-chart/ adresinden alındı

Assange, J. (2013). *Cypherpunks Freedom and the Future of the Internet - Şifrepunk Özgürlük ve İnternetin Geleceği Üzerine bir Tartışma (Çev. Ayşe Deniz).* İstanbul: Metis Yayıncılık.

Atik, M., Köse, Y., & Yılmaz, B. (2021, 5 31). Kripto Para, Para mıdır Döngüsünde Kabul Edilebilirlik Üzerine Ampirik Bir Uygulama. *Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, s. 155-172.

Ayan, B. (2022, 12 24). *NFT Balonu Patladı mı?* BTCHaber: https://www.btchaber.com/nft-balonu-patladi-mi/ adresinden alındı

Aydın, Y. (2022, 04 01). Thomas Hobbes ve John Rawls'da Doğal Durum ve Toplumsal Sözleşme. *Uluslararası Sosyal Bilimler Ve Eğitim Dergisi*, s. 437-458.

Aysan, M. (2018, 1). Dünya ve Osmanlı Devleti'nde Enflasyon. *Muhasebe ve Finans Tarihi Araştırmaları Dergisi*, s. 92-123.

Bayter, M. (2009, 07 01). Türkçe Web Sitelerinin Kataloglanmasının Önemi. *Türk Kütüphaneciliği*, s. 563-585.

Bekirli, A., Özdemir, D., & Beşkirli, M. (2019). Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme. *Avrupa Bilim ve Teknoloji Dergisi*, 284-291.

Berners-Lee, T., Fielding, R., & Frystyk, H. (2023, 04 07). *RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0.* RFC Editor: https://www.rfc-editor.org/info/rfc1945 adresinden alındı

Cadwalladr, C., & Townsend, M. (2018, 03 24). *Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica*. The Guardian: https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions adresinden alındı

Casson, T., & Ryan, P. S. (2006). Open Standards, Open Source Adoption in the Public Sector, and Their Relationship to Microsoft’s Market Dominance. S. Bolin içinde, *Tandards Edge: Unıfıer Or Dıvıder* (s. 87). California: Bolin Group.

Cinel, E. A. (2021, 03). Pandeminin Parasal ve Finansal Boyutları. *Sosyal Bilimler Araştırma Dergisi*, s. 90-101.

Çeşmeci, M. Ü. (2009). Elektronik Çağ Öncesi Dönem Kriptoloji Tarihi. *Tübitak UEKAE Dergisi*, 12-31.

Davies, H. (2015, 12 11). *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*. The Guardian: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data adresinden alındı

Doğan, Ö., & Karacak, H. (2022, 12 30). Türkiye'deki e-Ticarete Özgü Blokzincir Tabanlı Dijital Kimlik Güven Çerçevesi Önerisi. *Bilgi Yönetimi Dergisi*, s. 256-279.

Doğruyol, A., & Aydınlar, K. (2017, 1). Değerden İllüzyona: Para, Kredi, Banka. *Trakya Üniversitesi Edebiyat Fakültesi Dergisi*, s. 160-187.

Durmuş, S. (2018). Sanal Para Bitcoin. *Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 18.

Dursun, T. (2020). Blok Zinciri Teknolojisi. *BİLGEM Teknoloji Dergisi*, 10-15.

Edwards, J. (2023, 11 27). *Bitcoin's Price History.* Investopedia: https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp adresinden alındı

Ercan, A. B. (2021, 7). Yuan Hanedanlığı'nda Bilim ve Kültür. *Alınteri Sosyal Bilimler Dergisi*, s. 97-110.

Fabre, C. (2018). Toplumsal Sözleşme. *Felsefe Arkivi*, 123-135.

Fidan, M., Dilek, S., & Esev, A. (2019, 12). Dünden Bugüne Paranın Tarihi ve Türkiye'de Kâğıt Para Kullanımı. *Sosyal Bilimler Dergisi*, s. 141-162.

Fidan, Y. (2013, 12 26). Yönetimden Yönetişime: Kavramsal Bir Bakış. *Yalova Sosyal Bilimler Dergisi*, s. 5-10.

Fırat, S., & Daşdemir, E. (2021, 1). Kripto Paralarda Miktar Teorisi Uygulaması: Bitcoin Örneği ve Covid-19 Salgının Etkisi. *İstanbul İktisat Dergisi*, s. 81-102.

Frankel, A. (2022, 12 06). *Musk is entitled to order disclosures like 'The Twitter Files.' Are states?* Reuters: https://www.reuters.com/legal/transactional/musk-is-entitled-order-disclosures-like-the-twitter-files-are-states-2022-12-05/ adresinden alındı

Giddens, A. (2012). *Modernliğin Sonuçları.* İstanbul: Ayrıntı Yayınları.

Güzel, S. (2005). Bir Sosyal Değişme Süreci: Sosyolojik Bakış Açısından Sanayi Devrimi. *Muhafazakar Düşünce*, 189-198.

İçli, G. T. (1987, 12 15). Tarihi Perspektif İçinde Sosyal Düzen, Sosyal Organizasyon, İş Bölümü Kavramları. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, s. 58-68.

International Bank for Reconstruction and Development / The World Bank. (2024). *Digital Progress and Trends Report 2023.* Washington DC: World Bank Publications.

Kara, S. (2017). Teknoloji ve Toplumsal Değişim İlişkisinin Sosyal İnşa Kuramı Bağlamında İncelenmesi. *Dört Öğe*, 117-131.

Kavut, S. (2020, 07 01). Kimliğin Dönüşümü: Dijital Kimlikler. *Selçuk İletişim Dergisi*, s. 987-1008.

Keser, H. (2019). Bilgisayarın Evrimi. *Ankara University Journal of Faculty of Educational Sciences*, 411-422.

Kurt, G., & Yavuzarslan, T. (2021, 6 31). Kripto Varlık Arzıyla (Ico) İşletme Finansmanı Ve Risklerinin Değerlendirilmesi. *Muhasebe Bilim Dünyası Dergisi*, s. 222-253.

Kuruç, B. (2016, 03 31). Bretton Woods Anlaşması'nın 70. Yılı. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, s. 7-26.

Küçükbay, F., Uysal, D., & Çırak, A. N. (2022, 04). Dünya'da ve Türkiye'de Covid-19 Pandemisinin Ekonomik Etkileri. *Selçuk Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi*, s. 124-140.

Laurent, A. M. (2004). *Understanding Open Source and Free Software Licensing.* Sebastopol: O'Reilly Media Inc.

Mendi, A. F., & Çabuk, A. (2018, 7). Bitcoin'in Arkasındaki Güç: Blockchain. *GSI Journals Serie C: Advancements in Information Sciences and Technologies*, s. 12-23.

Meraklı, S. (2021, 3 12). Merkeziyetsiz Finans (Defi) Faaliyetlerinin İzinsiz Bankacılık Faaliyetinde Bulunma Suçu Bakımından Değerlendirilmesi. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, s. 1156-1190.

Metin, S. (2014, 6). Oyun Teorileri Işığında Thomas Hobbes'un Sosyal Sözleşme Kuramının Analiz Ve Yorumu. *Journal of Istanbul University Law Faculty*, s. 235-264.

Metjahic, L. (2018, 4). Deconstructing the Dao: the Need for Legal Recognition and the Application of. *Cardozo Law Review*, s. 1533-1567.

Orhan, O. Z., & Erdoğan, S. (2003). *Para Politikası.* İstanbul: Avcı Ofset.

Orhan, Z. Y. (2022, 12 27). Merkeziyetsiz Otonom Organizasyonlar, Kurumsal Yönetim ve Blokzincir. *Maltepe Üniversitesi Hukuk Fakültesi Dergisi*, s. 153-164.

Ossinger, J. (2021, 11 08). *The World's Cryptocurrency Is Now Worth More Than $3 Trillion.* Time: https://time.com/6115300/cryptocurrency-value-3-trillion/ adresinden alındı

Parlar, T. (2022, 12 31). Blokzincir Teknolojisi ve Merkeziyetsiz Finans Uygulamaları. *Journal of Politics Economy and Management*, s. 165-174.

Rickards, J. (2017). *Kur Savaşları.* İstanbul: Scala Yayınları.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, 03 17). *How Trump Consultants Exploited the Facebook Data of Millions*. The Newyork Times: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html adresinden alındı

Schwartz, M. (2017, 03 30). *Facebook Failed to Protect 30 Million Users From Havıng Their Data Harvested By Trump Campaign Affiliate*. The Intercept: https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/ adresinden alındı

Soyuer, B. (2023, 02 01). Dijital Değiştirilemezlik Çağında Sanat Eseri. *Bodrum Journal of Art and Design*, s. 15-27.

Şafak, E., Arslan, Ç., Gözütok, M., & Köprülü, T. (2021). Dağıtık Defter Teknolojileri ve Uygulama Alanları Üzerine Bir İnceleme. *Avrupa Bilim ve Teknoloji Dergisi*, 36-45.

Şenbayram, E. A. (2019, 4). Paranın Geldiği Uç Nokta: Bitcoin. *Econharran Harran Üniversitesi İİBF Dergisi*, s. 72-92.

Takaoğlu, M., Özer, Ç., & Parlak, E. (2019, 12 19). Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulanma Alanları. *Uluslararası Doğu Anadolu Fen Mühendislik ve Tasarım Dergisi*, s. 260-295.

Tanrıkulu, A., Yüce, H., & Ölçer, E. (2021, 6 21). Blokzincir Tabanlı Donanımsal Cüzdan ve Akıllı Kartlar. *Afyon Kocatepe Üniversitesi Uluslararası Mühendislik Teknolojileri ve Uygulamalı Bilimler Dergisi*, 37-48.

Tanrıverdi, M., Uysal, M., & Üstündağ, M. T. (2019, 07). Blokzinciri Teknolojisi Nedir ? Ne Değildir ?: AlanyazınİncelemesiBilişim Teknolojileri Dergisi, s. 203-217.

Taş, O., & Kiani, F. (2018, 10 4). Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine Bir İnceleme. *BİLİŞİM TEKNOLOJİLERİ DERGİSİ*, s. 369-382.

Tevetoğlu, M. (2021, 6 30). Ethereum ve Akıllı Sözleşmeler. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, s. 193-202.

Türk Dil Kurumu. (1988). *Türkçe Sözlük.* Ankara: TDK-Yayınları.

Türün, C. Ş. (2021, 08 03). *Karikatürler İçin NFT'li Yeni İş Modeli Önerisi*. BTCHaber: https://www.btchaber.com/karikaturler-icin-nftli-yeni-is-modeli-onerisi/ adresinden alındı

Türün, C. Ş. (2021, 03 27). *Tekil Tokınlar: Tek-Tok (Non-fungible tokens)*. BTCHaber: https://www.btchaber.com/tekil-tokinlar-tek-tok-non-fungible-tokens/ adresinden alındı

Türün, C. Ş. (2022, 3 22). *Asset-Backed Token'lar Gümbür Gümbür Geliyor!* BTCHaber: https://www.btchaber.com/asset-backed-tokenlar-gumbur-gumbur-geliyor/ adresinden alındı

Türün, C. Ş. (2022, 10 08). *Ethereum Platformu Nedir, Ne İşe Yarar?* BTCHaber: https://www.btchaber.com/ethereum-platformu-nedir-ne-ise-yarar/ adresinden alındı

Türün, C. Ş. (2022, 10 05). *Finansal Piyasalarda Neler Oluyor, Anlama Kılavuzu.* BTCHaber: https://www.btchaber.com/finansal-piyasalarda-neler-oluyor-anlama-kilavuzu/ adresinden alındı

Türün, C. Ş. (2022, 10 10). *NFT'ler ve Yeni Üretim Biçimleri.* BTCHaber: https://www.btchaber.com/nftler-ve-yeni-uretim-bicimleri/ adresinden alındı

Türün, C. Ş. (2022, 03 04). *Sanat Eserlerinin Blokzinciri Üzerinden Takibi*. BTCHaber: https://www.btchaber.com/sanat-eserlerinin-blokzinciri-uzerinden-takibi/ adresinden alındı

Türün, C. Ş. (2022, 10 13). *Token'larımızı Artık Bankalarda Saklayacağız!* BTCHaber: https://www.btchaber.com/tokenlarimizi-artik-bankalarda-saklayacagiz/ adresinden alındı

Ustaoğlu, E., Kıran, S., Bağcı, M., & Emre, İ. E. (2022, 12 26). NFT (Non-Fungible Token) ve Uygulama Alanları. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, s. 1801-1821.

Uyanık, N., & Berk, F. M. (2016). Mekân - Şehir Ve Medeniyet Bağlamında ÇatalhöyüK. *ÇATALHÖYÜK Uluslararası Turizm ve Sosyal Araştırmalar Dergisi*, 1-16.

Ülger, P. D. (2022, 12 05). *Matematiğin Kısa bir Tarihi.* Koç Üniversitesi: http://portal.ku.edu.tr/~aulger/histofmathematics.html adresinden alındı

Ünal, G., & Uluyol, Ç. (2020, 4). Blok Zinciri Teknolojisi. *Bilişim Teknolojileri Dergisi*, s. 167-175.

Williams, O. (2018, 6 31). *Only 48% of ICOs were successful last year — but startups still managed to raise $5.6 billion*. www.businessinsider.com: https://www.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1 adresinden alındı

Yavuz, M. S., & Suyadal, M. (2020, 9 30). Girişimciliğin Finansmanında Initial Coin Offering (ICO) Yöntemi ve Alternatif Finansman Yöntemleriyle Karşılaştırılması. *Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, s. 63-84.

Yerlikaya, T. (2006). Yeni şifreleme algoritmalarının analizi. . *(Doktora Tezi)*. Trakya Üniversitesi Fen Bilimleri Enstitüsü.

YILMAZ, S. (2016). Türkiye'de Toplumsal ve Dini Değişimin İzleri: AK Parti İktidarında Nereden Nereye. Ankara: Grafiker.

ŞEKİLLER LİSTESİ