Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 29, S. 181-186, Aralık 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 29, pp. 181-186, December 2021

Research Article

Blokzincir Mimarisi ve Getirdiği Fırsatlar

Arif Furkan Mendi[1*]

[1*] HAVELSAN, Ankara, Türkiye (ORCID: 0000-0002-0750-4012), afmendi@havelsan.com.tr

(International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) 2021 – 21-23 October 2021)

(**DOI:** 10.31590/ejosat.1009655)

ATIF/REFERENCE: Mendi, A. F. (2021). Blokzincir Mimarisi ve Getirdiği Fırsatlar. *Avrupa Bilim ve Teknoloji Dergisi*, (29), 181-186.

Öz

Son yıllarda özellikle Bitcoin kripto parasının finansal alanda yapmış olduğu sansasyonel çıkış ile birlikte, Bitcoin'in altyapısındaki teknoloji olmasının da etkisiyle blokzincir teknolojisi giderek popüler hale gelmiştir. Blokzincir, tüm işlemlerin bloklar üzerinde şifrelenerek tutulduğu, alıcı ve satıcı tarafların herhangi bir üçüncü tarafın onaylamasına gerek olmaksızın kendi aralarında güvenli bir şekilde alışveriş yapmasına olanak tanıyan merkezi olmayan işlemsel veritabanı teknolojisidir. Bu işlemsel veri tabanı teknolojisinde tüm işlemler, sistemdeki kullanıcılara açık olan "Dağıtık (Açık) Defter" adı verilen bir yapıda kayıt altına alınır. Geleneksel yaklaşımda (merkezi veritabanı), veritabanı üçüncü bir tarafça kontrol edilirken, Blokzincir yaklaşımında veri tabanının birer kopyası tüm katılımcılarda bulunur. Böylelikle, verilerin bozulması ve tahrip edilmesi önlenir. Güvenlik, aracısız işlem, şeffaflık gibi avantajlar Blokzincir teknolojisini çekici kılmakta, birçok teknoloji şirketinin yatırım yapmasına ve mevcut sistemlerini blokzincir teknolojisi ile değiştirme eğilimi göstermesine sebep olmaktadır. Tüm bu avantajların temelinde ise blokzincir teknolojisinin sahip olduğu mimari yapısı yer almaktadır. Bu çalışmada blokzincir ağ mimarisi, kriptografik blok anahtarı yapısı ve fikir birliği yapısının bütüncül olarak blokzincir yapısı olarak ele alınması; bu yapının sağladığı avantajları ve ortaya çıkarttığı fırsatlar değerlendirilecektir.

Anahtar Kelimeler: Blokzincir, Blokzincir Mimarisi, Dağıtık Defter

Blockchain Architecture and Opportunities

Abstract

In recent years, especially with the sensational breakthrough of Bitcoin cryptocurrency in the financial field, blockchain technology has become increasingly popular with the effect of being the technology in the infrastructure of this cryptocurrency. Blockchain is a decentralized transactional database technology where all transactions are kept encrypted on blocks, allowing buyers and sellers to securely exchange transactions between themselves without the need for any third-party approval. In this transactional database technology, all transactions are recorded in a structure called "Distributed (Open) Ledger" that is open to users in the system. In the traditional approach (central database), the database is controlled by a third party, while in the Blockchain approach, all participants have a copy of the database. Thus, data corruption and destruction are prevented. Advantages such as security, agentless processing, and transparency make Blockchain technology attractive, causing many technology companies to invest and tend to replace their existing systems with blockchain technology. On the basis of all these advantages, there is the architectural structure of blockchain technology. In this study, the blockchain network architecture, cryptographic block key structure, and consensus structure will be considered as a blockchain structure, the advantages and opportunities of this structure will be evaluated.

Keywords: Blockchain, Blockchain Architecture, Distributed Ledger

[*] Sorumlu Yazar: HAVELSAN, Simülasyon Otonom ve Platform Yönetim Teknolojileri, Ankara, Türkiye, ORCID: 0000-0002-0750-4012, afmendi@havelsan.com.tr

1. Giriş

Blokzincir teknolojisi 1992'de geliştirilmiş, 2008 yılında Bitcoin kripto parasının temeli olarak kullanılmıştır. Bitcoin en popüler ve yaygın olarak tanınan kripto para birimi olsa da blokzincir teknolojisinin kökleri çok daha eskiye dayanmakta ve çok daha fazlasını vadetmektedir. Yalnızca finansal işlemleri değil aynı zamanda değer atfettiğimiz hemen hemen her şeyi kaydetmek için programlanabilen, işlemlerin bozulmaz bir dijital defterini sağlamaktadır. Mülk sahipliği, eğitim bilgileri, finansal hesaplar, oy sistemleri, sağlık raporları gibi kodla ifade edilebilecek birçok alanda uygulanabilmektedir. Hatta evlilik ve doğum gibi kayıtların bile blokzincir teknolojisi ile takip edilebileceği değerlendirilmektedir. Akıllı mülkiyet alışverişi, blokzincir teknolojisinin kullanılabildiği bir diğer önemli alandır. Bu geniş ürün yelpazesi ve uygulama alanlarının çeşitliliği sebebiyle blokzincir teknolojisinin popülerliği gittikçe artmaktadır. Hatta bazı teknoloji uzmanları daha da iddialı bir yaklaşımda bulunarak, blokzincir teknolojisinin "Yeni İnternet" etkisi yapabileceğini savunmaktadır. Bu iddialı yaklaşımın temelinde blokzincir teknolojisinin devrimsel özellikleri yatmaktadır. Dağıtık muhasebe defteri, bu devrimsel özelliğin sebebidir. Dağıtık muhasebe defteri, ağdaki tüm katılımcılarla paylaşılır, gerçekleşen her işlemi, katılan her bilgisayarda kaydeder ve depolar. Böylelikle banka gibi güvenilir üçüncü taraflara olan ihtiyacı ortadan kaldırır. Nispeten yeni bir teknoloji olmasına rağmen, yapılan çalışmaların sayısı çarpıcı bir şekilde artmakta, büyük şirketlerin saha çalışmaları yapma eğiliminde olduğu görülmektedir.

"Harward Business Review" çalışması ile blokzincir teknolojisini konu alan bir araştırma gerçekleştirmiştir. Bu çalışmada blokzincir teknolojisi, anlaşmaların dijital ortamda koda gömülü olarak tarafların erişimine şeffaf bir şekilde sunulduğu; silinme, değiştirilme, tahrip edilme gibi dış müdahalelere karşı korunaklı bir veritabanı olarak tanıtılmıştır. Bu dijitalleşme ile sistem üzerindeki her anlaşma, süreç, görev ve ödemenin tanımlanmasına, doğrulanmasına, saklanmasına ve paylaşılmasına olanak tanıyan dijital bir kayıt ve imzaya sahip olacaktır. Dolayısıyla bankalar, avukatlar, noterler gibi güvenilir üçüncü taraf onaylayıcılara olan zorunlu ihtiyaç ortadan kalkacak; insanlar, organizasyonlar, cihazlar birbirleriyle dış dâhillerin en aza indirildiği bir yapıda iletişim kurabilecektir. Blokzincir teknolojisinin göz alıcı potansiyeli buradan gelmektedir (Mooney, 2011). Bu çalışmada, blokzincir teknolojisinin sunmuş olduğu mimarinin avantajları ve ortaya çıkarttığı fırsatlar değerlendirilecektir.

Blokzincir teknolojisinin tercih edilmesindeki avantajlar üzerine kurulmuş olduğu mimariye dayanmaktadır. Veri tabanı yapısı tamamen dağıtıktır. Yani sistemdeki işlemleri kontrol eden herhangi bir merkezi otorite mevcut değildir. Blokzincir, kullandığı ileri kriptografik sayesinde dağıtık defterdeki kayıtların silinmesini veya değiştirilmesini engeller, yapılan işlemlerin kaynağını ve gideceği adresi tanımlayarak verinin doğruluğunu sağlar. Kripto para birimleri tarafından kurulan blokzincir ağları, sisteme dâhil olan herkesin okuyup yazabilmesi için halka açıktır. Ancak, erişimin yalnızca belli taraflarca sağlanabileceği özel, izinli blokzincir ağları oluşturmak da mümkündür. Verilerin hassas olduğu durumlarda, verinin tamamının tutulması yerine verileri açığa çıkarmayan kriptografik özetler blokzincir ağı üzerinde taşınabilir. Böylelikle, gizli verilerin açık bir şekilde tutulması yerine, karma kodu sistem üzerinde tutularak verinin güvenliği sağlamlaştırılır. Bu ve bunun gibi esnek çözümler ve alternatifler sayesinde blokzincir teknolojisi ihtiyaca göre farklı çözümler sunmaktadır.

Blokzincir ağında gerçekleşen tüm hareketler, işlemlerin tutulduğu ve tüm kullanıcılara açık olan "Dağıtık Defter" adlı bir yapıda kayıt altına alınır. Geleneksel yaklaşımda (merkezi veritabanı), veritabanı üçüncü bir taraf tarafından kontrol edilirken, blokzincir yaklaşımında veri tabanının kopyası tüm katılımcılarda mevcuttur, böylece verilerin bozulması ve yok edilmesi önlenir. Bu dağıtık yapıda, verinin değiştirilebilmesi için ilgili değişikliklerin sistemdeki tüm bilgisayarlara kaydedilmesi gerekir. Bunun için de veri ağın çoğunluğunun değişikliği onaylaması ve doğrulaması gerekir ki bu da yapılacak her türlü siber saldırının başarılı olmasını neredeyse imkânsız hale getirmektedir. Güvenlik, aracısız işlem, şeffaflık gibi avantajlar Blokzincir teknolojisini çekici kılmakta, birçok teknoloji şirketinin yatırım yapmasına ve mevcut sistemlerini blokzincir teknolojisi ile değiştirme eğilimi göstermesine sebep olmaktadır. Bu teknolojik yeniliğin temelinde üç anlayış yer almaktadır. Bunlar, merkezi olmayan ağ mimarisi, kriptografik anahtarlama yapısı ve dağıtık fikir birliği kavramlarıdır. Hiçbiri yeni olmayan bu üç kavram bir araya getirilerek yeni bir yapı, yani blokzincir teknolojisi ortaya çıkmıştır. Bu çalışmada, blokzincir teknolojisinin sunmuş olduğu mimarinin avantajları ve ortaya çıkarttığı fırsatlar değerlendirilecektir.

2. Materyal ve Metot

2.1. Materyal

Çalışma kapsamında önemli bilimsel veri tabanları taranmış, buradaki kaynaklar birincil veri kaynağı olarak kullanılmıştır. Ayrıca blokzincir teknolojisinin son dönemlerde popülerliğinin artması, dolayısıyla eski çalışma sayısının sınırlı olması sebebiyle güncel veriye erişim ihtiyacı sebebiyle teknolojik gelişmelerin incelendiği internet sayfaları ve yazılar da veri kaynağı olarak kullanılmıştır.

2.2. Metot

Çalışma öncelikle blokzincir yapısının araştırılması adımı ile başlamıştır. Blokzincir yapısının derinlemesine incelemesi; ağ mimarisi, kriptografik anahtar yapısı ve fikir birliği mekanizmasının irdelenmesi ile gerçekleştirilmiştir. Ardından blokzincir teknolojisinin getirdiği avantajlar ve kullanım örnekleri incelenmiş, araştırma sonuçlarının tartışılması ve sonuç ile çalışma tamamlanmaktadır. Çalışma yöntemleri adımları Görsel 1'de yer almaktadır.

Görsel 1: Çalışma Yöntem Adımları

2.3. Gerçekleştirilen Çalışma

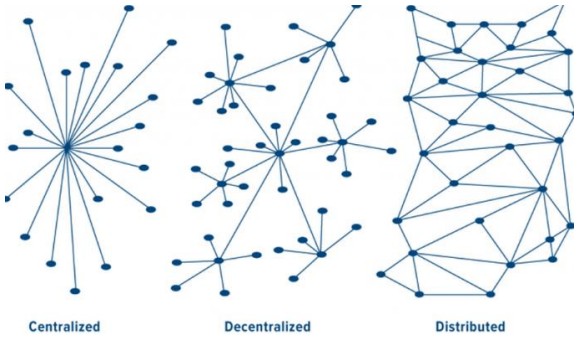
2.3.1. Blokzincir Yapısının Araştırılması

Blokzincir teknolojisi devrimsel nitelikte çözümler sunmakta, teknoloji firmalarının bu teknolojiye yatırım

yapmasına sebep olmaktadır. Bu teknolojik yeniliğin temelinde üç temel unsur yer almaktadır. Bunlar, merkezi olmayan ağ mimarisi, kriptografik anahtarlama yapısı ve dağıtık fikir birliği kavramlarıdır. Hiçbiri yeni olmayan bu üç kavram bir araya getirilerek yeni bir yapı, yani blokzincir teknolojisi ortaya çıkmıştır. Bu bölümde bu üç yapı ele alınacaktır.

2.3.1.1. Blokzincir Yapısının Araştırılması

Günümüzde yaygın olarak birçok alanda kullanılan bilgi sistemleri, bilgisayarların birbirlerine bağlanması sonucu oluşmaktadır. Ağ üzerinde bilgisayarlar farklı görevleri yerine getirmekte ve oluşan veri/bilgi ağ üzerinde yayılmaktadır. Her bir bilgisayarın veya kullanıcının farklı rolleri ve sorumlulukları olmakta, verinin işlenmesi için farkı yöntemler benimseyebilmektedirler. Temelde, verinin depolanması, işlenmesi ve yönetilmesi için ağ tipleri farklılık göstermekte, kurulacak sistemin ihtiyacına göre uygun tipin belirlenmesi gerekmektedir. Ağ tiplerini incelediğimizde karşımıza üç temel seçenek çıkmaktadır. Bunlar, merkezi, merkezi olmayan ve dağıtık ağ tipleridir. (Bkz. Görsel 2).



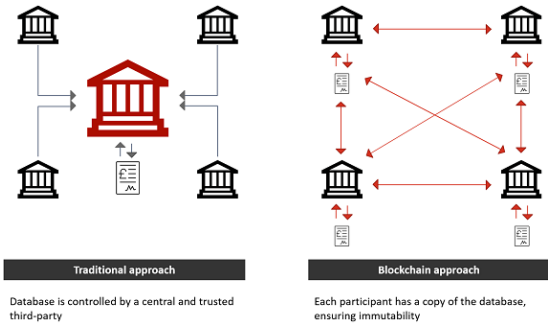
Görsel 2: Ağ Tipleri (Frank Holmes, 2018)

i. **Merkezi:** Ağ, tek bir otorite tarafından kontrol edilir, yönlendirilir ve kararlar alınır (Tasca & Tessone, 2018). Bu ağ tipi için verilebilecek en iyi örnek bankalardır. Bankanız, merkezi bir ağdaki işlemlerin tekilliğini doğrulama nosyonunu sahiptir. Ayrıca çift harcama gibi hatalı durumların kontrolü ve yönetimi de bankanızın sorumluğundadır. Örneğin hesabında 50TL olan bir müşteri düşünün. Banka, bir manipülasyon veya bir sorun nedeniyle bu kişinin iki kez 50TL (çift harcama sorunu) para transferi yapmasını engelleyecektir. Böylelikle, müşterinin para kaybı yaşamayacağını garanti etmek bankanın sorumluluğundadır. Bu tür yapılarda merkezi kontrol noktası tüm taraflarca yetkilendirilmiş ve güvenilen bir yapıdır. Twitter uygulaması bir diğer önemli merkezi ağ uygulama örneği olarak verilebilir. Taraflar paylaşacakları bilgiyi merkezi yapıya verir, ağ üzerinde paylaşılma kuralları belirlenir ve bu kurallar doğrultusunda merkezi noktadan bilginin paylaşımı gerçekleştirilir.

ii. **Merkezi olmayan:** Hiçbir kişinin, kurumun veya makinenin başkalarına ne yapacaklarını söylemediği bir yapıdır. Örneğin Ethereum, paranın bir kurum tarafından basılmaması ve değer atfedilmemesi, bunun yerine onu kullanan topluluk tarafından yaratılması ve değer atfedilmesi ilkesiyle oluşturulmuş, merkezi olmayan bir para birimidir. Bilişim teknolojileri terminolojisi ile açıklamak gerekirse, bu tür bir ağın çalıştırılıp, yaşamaya devam ettirilebilmesi için özel bir tekil makineye/otoriteye ihtiyaç duyulmamaktadır.

iii. **Dağıtık:** Dağıtık ağ mimarisi, ağa bağlı bilgisayarlarda bulunan bileşenlerin mesajlar ileterek iletişim kurduğu ve eylemlerini koordine ettiği bir modeldir (Coulouris et al., 2011). Bu tanımdan yola çıkarak, merkezi olmayan bir sistemin aynı zamanda dağıtık bir sistem olduğu söylenebilir. Temelde merkezi olmayan veri tabanları ile benzer şekilde tanımlansa da burada sistem birden fazla makineye yayılmış durumdadır. Bu, bir makinenin servis dışı kalması durumunda sistemin çalışmayı bırakmaması anlamına gelir. Yine önemli bir diğer konu, merkezi bir kontrol noktasının olmamasıdır. Büyük boyuttaki internet uygulamalarının ve hizmetlerinin dağıtık olarak sunulduğunu görsek de internet uygulamalarının büyük çoğunluğu merkezi yapıdadır. Bunun sebebi, uygulama sahibi şirketlerin istedikleri zaman uygulamaları güncelleme, değiştirme veya kullanıma kapatma gibi işlemleri tek yetkili olarak yapmak istemesidir. Ethereum merkezi olmayan bir mimari sunmasının yanından aynı zamanda dağıtık yapıdadır. Kullanıcılarına dağıtık uygulamalar geliştirmek için altyapı sağlar.

Bir önceki bölümde açıklandığı gibi, blokzincir teknolojisinin en önemli özelliklerinden biri, dağıtık defter olarak adlandırılan geleneksel olmayan ağ yaklaşımının sebebidir. Dağıtık defter teknolojileri (DLT); kullanıcıların, kendi standartlarını ve süreçlerini dayatan merkezi bir doğrulama sistemi kullanmaya gerek kalmadan, katılımcılarla paylaşılan ortak bir defterdeki kayıtları değiştirmelerine olanak tanıyan teknolojidir (Pinna & Ruttenberg, 2016). Bu iddialı yaklaşımın nedeni, yenilikçi özellikleriyle ilgilidir. Dağıtık defter kurulmuş ve dağıtılmış bir bilgisayar ağına katılan tüm taraflarca paylaşılır. Ağda gerçekleşen her işlemi, katılan her bilgisayarda kaydeder ve depolar. Özellikle, ödeme işlemlerindeki gibi güvenilir üçüncü taraflara(banka) olan ihtiyacı ortadan kaldırır. Sisteme dâhil olan tüm düğümlerin bu dağıtık deftere erişimi vardır. Sistemdeki tüm katılımcılara bunun birer kopyası sağlanmaktadır. Geleneksel yaklaşımla karşılaştırırsak; veri tabanı (merkezi olan) geleneksel yaklaşımda üçüncü bir taraf tarafından kontrol edilirken, blokzincir yaklaşımında veri tabanının kopyası tüm katılımcılara açıktır. Böylelikle, verilerin bozulması ve yok edilmesi önlenir (Bkz. Görsel 3).



Görsel 3: Geleneksel ve Blokzincir Yaklaşımlarının Karşılaştırılması (Technology, 2018)

Ağ mimarisini ve veri tabanı yapısını özetlersek; geleneksel yaklaşımda (blokzincir öncesi) merkezi onay ve hesaplama mekanizması ile oluşturulan "Merkezi Veri Tabanı" varken; blokzincir yaklaşımı sonrası, merkezi olmayan onay ve hesaplama mekanizması ile oluşturulan "Dağıtık Defter" kavramı bulunmaktadır.

2.3.1.2. Kriptografik Blok Anahtarı Yapısı

Dağıtık defter konseptiyle sağlanan merkezi olmayan ağda süreçler, bu blokların birbiri ardına yerleştirilmesiyle zincirlerin oluşturulduğu "Bloklar" üzerinde tutulur. Bloklar üzerindeki işlemler gruplanmıştır ve tüm ağ için görüntülenebilen tek bir zincir vardır. Kriptografi, blokların manipülasyonunu önlemek ve bunları zincirin sonuna eklemek için kullanılır. Kullanılan kriptografik şifreleme mekanizması sayesinde her bir kullanıcının açık ve kapalı olmak üzere iki tür anahtarı vardır. Alıcı tarafın, kendi açık adresini satıcı taraf ile paylaşması sonrası el değişim süreci başlar. Değişime konu değerin transferi için karma(hash) kodu adı verilen blok imzası ile gerçekleştirilir. Açık adresleri kriptografi kullanılarak oluşturulur, değerin transferi bu adresler ile sağlanır (Pilkington, 2016). Açık anahtarlar asla gerçek dünya kimlikleri ile eşleşmemekte ve böylelikle blokzincir teknolojisinin sunduğu anonimlik özelliği sağlanabilmektedir. Gönderen taraf kapalı anahtarını kullanarak değeri imzalar ve transfer sürecini başlatır. Kapalı anahtarlar asla bir başka kullanıcı ile paylaşılmaz. Bu kişiye özgü bir bilgidir.

Blokzincir ağı şeffaftır; zincirdeki her blok bir öncekine referanstır. Blok üzerinde saklanacak veriler, eklenecek zincir bloğun link bilgisi ile kriptografik şifreleme ile paketlenir. Bloktaki veri veya önceki blok bağlantısının adresi değiştirilirse, bu şifreleme kodu yani karma kodu tamamen değişir ve bu da sistemde tanınmayan bir bloğa neden olur. Böylelikle, verideki manipülasyon kolaylıkla tespit edilir. Bu mekanizma sayesinde sistemin güvenliği ve veri bütünlüğü sağlanır.

2.3.1.3. Fikir Birliği Mekanizması

Blokzincir, tüm işlemleri içeren ve ağ üzerinde uçtan uca tutulan birleştirilip katılımcılar arasında kopyalanan bir defterdir. Bu işlemler parasal işlemlerden mülk transferine kadar her şey olabilir. Ağdaki üyeler, düğüm adı verilen anonim kişilerdir. Ağda kurulan tüm iletişimlerde, gönderen ve alıcıyı güvenli bir şekilde tanımlamak için kriptografi kullanılır. Bir düğüm deftere bir kayıt eklemek istediğinde, bu kaydın nerede olması gerektiğine fikir birliği karar verir. Fikir birliğine blok da denir. Fikir birliği, yönetim organı ve karar alıcıdır. Yeni bir bloğun meşru olup olmadığını ve zincire eklenmesi gerekip gerekmediğini onaylamak için dağıtılmış fikir birliği yöntemi uygulanır (Charleer et al., 2016). Sistem üzerinden bir değer gönderip almak isteyen kullanıcının bir kapalı anahtara ve ona bağlı bir açık anahtara sahip olması gerekir. Kapalı anahtar, dijital imzalama sürecinde sahip olduğumuz nesneyi birisine göndermemiz için ihtiyacımız olan anahtardır. Bununla ilişkili olan açık anahtar ise hem başkalarının nesneler gönderebileceği bir adres görevi görür hem de şifrelenmiş mesajı açmamıza ve özel anahtarımızla içeriğini kontrol etmemize olanak sağlar. Ayrıca açık anahtar sayesinde sistemdeki diğer tüm taraflar işlemin geçerliliğini kontrol eder. İmzalayarak şifrelediğimizi iddia ettiğimiz mesaj genel anahtarımızla açılmıyorsa, geçerli bir talebimiz olmadığı ve transfer işleminin geçersiz olduğu anlamına gelir.

Özel anahtarla imzalanan transfer işlemi P2P(Uçlar Arası) ağında yayınlanır. Yani mesaj, yalnızca alıcıya değil, ağda bağlı olduğumuz tüm düğümlere gönderilir. Mesajı ilk kez alan düğümler ayrıca sürecin meşru ve geçerli olup olmadığını kontrol eder ve ardından bunu bağlı oldukları düğümlere dağıtır. Böylece kısa sürede işlem, alıcımız da dâhil olmak üzere tüm ağa yayılır. Mesajı alan düğümler, içeriğin şifresini çözmek ve kontrol ederek mesaj içeriğini açmak için açık anahtarımızı kullanır. Bu doğrulama başarısız olursa, mesaj reddedilir ve işlem başarısız sayılır.

Başarılı işlemler, madenci olarak adlandırılan bir düğüm tarafından "Onaylanmamış İşlem Havuzu" olarak tanımlanan bir listeye alınır. Buradaki "Onaylanmamış" ifadesi, kurallara uygun ve geçerli olmadığı şeklinde yorumlanmamalıdır. Kurallara uygun bulunmayan bir mesaj bu listeye eklenmez. Bu işlem havuzu, bekleme listesi gibi düşünülebilir. Konu, işlemin henüz blok zincirine bir blok halinde eklenmemiş olmasıdır. Zincire bloklar eklemek ve süreci tamamlamak için bu işlemlerin onaylanması gerekir. Bu onay “Madencilik” ile gerçekleştirilir. Madenciler temel olarak yeni işlemleri onaylar ve bunları dağıtık deftere kaydeder. Bir işlemin, bir bloğun parçası haline geldiği ve blokzincir ağına eklendiğinde onaylandığı söylenir. Ancak madencilik işlemi, önemli bilgisayar hesaplama gücü gerektirir. Öne çıkan iki madencilik yöntemi vardır: "Proof of Work" ve "Proof of Stake".

Proof of Work (PoW)

Yeni bir bloğun usule uygunluğu ve zincire eklenmesi gerekliliği konusunda mutabakata varmak için dağıtık fikir birliği sağlanmalıdır. Bu, bir katılımcının bilgisayarının, blokzincir ağına yeni bir öğe eklemeyi denemeden önce önemli miktarda hesaplama çalışması gerçekleştirmesini gerektirir. Ağa uygun olmayan bir blok eklemek ve bunu fikir birliği ile kabul ettirmek çok zordur. Bu noktada fikir birliği yöntemlerinden Proof of Work(PoW) madencilik yöntemi ilk ve en yaygın kullanılan doğrulama yöntemi olarak karşımıza çıkmaktadır (Charleer et al., 2016).

Madenciler, "blok" adı verilen belirli bir boyutu aşmayan bir listeyi oluşturmak için onaylanmamış işlemler üzerinde rekabete girerler. Her blok için yüksek bir hesaplama çabasına girerek, o bloğa yerleştirilen tüm işlemlere bağlı olarak değişen özel bir koşul sağlayan ve standart bir formülle hesaplanamayan ancak bir önceki geçerli bloğa referans veren bir kriptografik şifre (karma) bulmaya çalışırlar. Bu değeri bulan madenci ilk önce yeni bloğu, blok için bulduğu hash değerini ve deneme yanılma sonunda bu hash'e ulaşmasını sağlayan "nonce" adlı başka bir sayısal değeri ağa yayınlar. Bu işlemi ilk tamamlayan ve uygun zincirin sonuna bloğu ekleyen madenci, işlem ödülünü ve o blok üzerindeki işlemlerde göndericiler tarafından belirtilen "işlem ücreti" adı verilen transfer ücretlerini alır.

Hash ve nonce değerlerini bulma sürecinde; işlemlerin geçerliliği kontrol edilir ve geçerli işlemlerden geçerli blokların oluşturulması sağlanır. Bu işleme "Proof of Work" yani iş kanıtı adı verilir çünkü çok fazla CPU gücü gerektirir ve geçerli bir hash ve nonce bularak kanıtlanması gerekir.

Bir bloğun doğru hash değerini bulmak için trilyonlarca "nonce" değeri denemek gerekli olabilirken, bunları bir adımda bulmak mümkün değildir, böyle bir iddiada bulunuluyor ise doğru olma ihtimali imkânsıza yakındır. Blok, hash ve nonce değerleri tutarlıysa, madenciler bu bloğu doğru bir şekilde kabul edecek ve bir sonraki bloğu bu bloğun sonuna eklemek için havuzdan bir dizi doğrulanmamış işlem emri üzerinde çalışmaya başlayacaktır.

Proof of Stake (PoS)

Blokzincir ağında işlemlerin doğrulanması için bir başka kimlik doğrulama türü Proof of Stake(PoS)'dir. Aslında bu yöntem tam olarak bir madencilik değildir, çünkü kullanıcıların yeni para kazanmak için hiçbir karmaşık hesaplama yapmalarına

gerek yoktur. Bu nedenle adı madencilik olarak değil "Minting" yani para basımı olarak da geçmektedir. Bu yöntemde, işlemleri basmak için elektronik cüzdanınızda değer bulundurmanız gerekir. Doğrulama işlemi sonucu elde edeceğiniz kazançlar, cüzdanınızda tuttuğunuz değerlerin miktarı ile doğru orantılı olacaktır.

PoW yöntemine kıyasla binlerce kat daha fazla maliyet tasarrufu sağlar. Yüksek hesaplama gerektirmediği için elektrik tüketim maliyeti neredeyse sıfırdır. Ek olarak, yatırımcılar daha fazla yatırım yapmaya teşvik edilir çünkü ödüller cüzdanlarındaki değer miktarına bağlıdır.

PoS yöntemi ilk olarak 2012 yılında bazı alternatif kripto paralar tarafından kullanılmaya başlanmıştır. Ethereum şu anda PoW yönteminden PoS yöntemine geçiş yapmaktadır. Peercoin, Ohm coin, MorningStar, OkCash gibi yeni çıkan kripto para birimlerinin birçoğu PoS yöntemini kullanmaktadır.

PoW ve PoS yöntemlerine ek olarak farklı konsensüs modelleri de mevcuttur. Doğrulama yöntemleri, kurulacak Blockchain sisteminin ihtiyaçlarına göre değişiklik gösterir. PoW ve PoS yöntemleri ağırlıklı olarak kripto para birimlerine sahip bir sistem söz konusu olduğunda tercih edilirken, farklı türde bir uygulama yapılandırıldığında uygulamanın ihtiyaçlarını karşılayacak uygun doğrulama yöntemi kullanılmalıdır.

2.3.2. Avantajları ve Kullanım Örnekleri

Blokzincir teknolojisinin merkezi olmayan veritabanı yapısı sayesinde ortaya çıkan avantajları temel olarak dört başlık altında özetleyebiliriz:

i. **Aracısız işlem:** Merkezi olmayan veri yapısı sayesinde, güvenilir bir merkezi otoriteye ihtiyaç yoktur. Bu sayede hem operasyonel hem de bakım maliyetlerinde ciddi tasarruflar el edilir.

ii. **Şeffaflık:** Ağdaki tüm faaliyet kayıtları dağıtık defterde tutulduğundan, ağdaki katılımcıların sistemdeki tüm verileri görüntülemesi mümkündür. Ağ üzerindeki tüm işlemler şeffaf bir şekilde takip edilebilir, böylece veri manipülasyonu önlenir. Sistemdeki varlığın hangi kaynaktan nereye gittiğini ve hangi kişilerin elinden geçtiğini takip etmek için ideal bir platformdur.

iii. **Gizlilik:** Sistemdeki katılımcılar, tüm işlemleri görebilmekle birlikte işlemi kimliklerle ilişkilendiren bilgileri göremezler. Bir yandan işlemler şeffaf bir şekilde görüntülenirken diğer yandan kullanıcıların kişisel bilgileri gizlidir ve şifresi çözülemez.

iv. **Güvenlik:** Sistem saldırılara dayanıklıdır. Blokzincir ağında merkezi bir kontrol noktası olmadığı için siber saldırının tüm uçlara yapılması gerekir ki bu da yüksek efor gerektirecek ve ekonomik olarak çok mantıklı olmayacaktır. Bir siber saldırı neticesinde blokzincir ağının %51'inin saldırgan tarafından kontrol edildiğini varsayalım. Ağ içindeki değer düşeceğinden saldırganın ağa zarar vermesi ekonomik açıdan faydalı olmayacaktır. Ayrıca, blokzincir ağlarının hata toleransı oldukça yüksektir. Merkezi olmayan ağları oluşturan çok sayıda farklı makine olması nedeniyle sistemin çökme ihtimali daha düşüktür. Tüm bir ağı çökertmek için her ucun tek tek hedeflenip düşürülmesi gerekir ki sistem çöksün. Bu da ihtimali oldukça zayıflatmaktadır. Ağın siber saldırı neticesinde ikiye ayrılması durumunda bile, ağın yarısı diğer kısım olmadan çalışabilir. Hatta saldırgan ağın %51'lik kısmının kontrolüne sahip olsa da saldırı direnci yine de koruyucu bir faktör olacaktır.

Tüm bu avantajları ile blokzincir, son yıllarda popüler hale gelmiştir. Birçok şirket ve kuruluş, blokzincir tabanlı sistemler geliştirmeye veya mevcut sistemlerini blokzincir teknolojisine taşımaya başlamıştır. Blokzincir teknolojisinin yaygınlaşması konusundaki gelişmelere baktığımızda aşağıda sıralanan bazı örnekleri görebiliriz:

- ABN Amro, ING Bank, RaboBank gibi büyük Hollanda bankaları, 2014'ün sonunda blokzincir konusunda çalışmalara başlamıştır (Petkovic & Arnab, 2018).
- Deutsche Bank ve Golden Sachs gibi önemli bankalar, blokzincir teknolojisinin önemini vurgulayarak bu teknolojiye geçme yönünde çalışmalarının olduğunu belirtmişlerdir (GoldmanSachs, 2018).
- MasterCard, blokzincir teknolojisi üzerinde çalışma gerçekleştirmektedir. Bunun en önemli kanıtlarından biri, anlık ödeme işlemlerinin blokzincir teknolojisi üzerinden yapılması konusunda patent başvurusu yapmış olmalarıdır (Zhao, 2018).
- Hindistan'ın en büyük bankası olan State Bank of India (SBI), blokzincir akıllı sözleşmelerinin kullanımına ilişkin çalışmalar gerçekleştirdiklerini ve bunları önümüzdeki dönemde kullanacaklarını duyurmuştur (Agarwal, 2018).
- Akbank, uluslararası para transferlerinde blokzincir teknolojisini kullanarak şeffaflığı artıran, işlemleri hızlandıran ve maliyetleri düşüren, blokzincir tabanlı çözümler sunan bir teknoloji firması olan Ripple ile anlaşma yapan ilk Türk bankası olmuştur (Akbank, 2018).
- Türkiye Cumhuriyet Merkez Bankası, Bankacılık Düzenleme ve Denetleme Kurumu, Sermaye Piyasası Kurulu ve Hazine Bakanlığı'ndan oluşan "Blokzincir Çalışma Grubu" kurulmuştur (Papuççiyan, 2017). Bu önemli gelişme, Türkiye Merkez Bankasının blokzincir teknolojisi konusunda çalışmalar gerçekleştirdiğini ve önümüzdeki dönemler için de planlamalarının olacağını göstermektedir.
- Kanada'da, blokzincir teknolojisini dijital kimlikler için kullanacağını duyurmuştur. Yeni dijital kimlik, SecureKey Technologies tarafından geliştirilmiş ve IBM tarafından desteklenmiştir. 2018 yılının ilk yarısı itibariyle tüketicilerin bu yeni dijital kimlik sistemine kaydolabilecekleri açıklanmıştır. Bu sayede kullanıcıların bankacılara, iletişim servis sağlayıcılarına ve hatta resmi makamlara karşı kimliklerini anında doğrulayabilmeleri hedeflenmiştir. Kullanıcı bilgileri tek bir noktada toplanmadığı için bu yeni dijital kimlik sisteminin, siber saldırılar sonucu ele geçirilme olasılığının büyük ölçüde azalacağı öngörülmektedir (Alexander, 2018).

Blokzincir teknolojisinin bu göz alıcı avantajlarını fark eden şirketler, bu yönde çalışmaya ve sistemlerini blokzincir teknolojisine taşıma eğiliminde bulunmaya başlamıştır. Ancak, durum değerlendirmesi yapılmadan mevcut bir sistemin

3. Araştırma Sonuçları ve Tartışma

Tüm bu örnek çalışmalardan da görülebileceği üzere, blokzincir teknolojisi giderek yaygınlaşmaya başlamıştır.

blokzincir teknolojisine geçirilmesi şirketler için genellikle olumsuz sonuçlar doğurmaktadır. Mevcut bir uygulamayı blokzincir teknolojisine geçirmeden önce bu teknolojinin sisteme uygunluğu mutlaka göz önünde bulundurulmalıdır. GARTNER firması bu konuda bir çalışma yayınlamış; söz konusu uygulamanın ihtiyaçlarının iyi analiz edilmesi gerektiği, blokzincir teknolojisinin buna uygun olması durumunda kullanılması önerilmektedir. Mevcut bir uygulama yenilenmek istendiğinde blokzincir teknolojisinin popülerliğinden etkilenerek otomatik olarak bu teknolojiyi seçmenin uygun olmayacağı vurgulanmaktadır. Riskler iyi analiz edilmeli, risk azaltma planları hazırlanmalıdır. Ardından yapılacak değerlendirmenin neticesinde blokzincir teknolojisini kullanmayı seçme, daha uygun olabileceği değerlendirilen farklı teknolojilere yönelme, blokzincir teknolojisini kullanmak üzere kapsamın daraltılması veya fazlara bölünmesi kararlarından biri alınmalıdır. Fayda maliyet analizi gerçekleştirilip, blokzincir teknolojisinin kullanılmasının getirileri maliyetlerden ağır basıyorsa ve risklerin yönetilebileceğine inanılıyorsa, projeye blokzincir teknolojisi ile başlamak iyi bir seçim olacaktır. Bunun yanı sıra, blokzincir teknolojisi o dönemde proje için uygun olmayabilir, bu nedenle teknolojinin olgunluğa ulaşması için beklemeye kararı alınabilir veya blokzincir teknolojisini kullanma kararı geri çekilebilir. Diğer taraftan, maliyetler çok yüksekse veya risklerin yönetilmesinde sorun olabileceği değerlendiriliyorsa; kapsamı daraltmak veya fazlara bölüp blokzincir teknolojini aşamalı olarak kullanmak yönünde karar da alınabilir (Panetta, 2017).

Mevcutta çalışan ve yenilemek istediğimiz bir sistemde veya yeni geliştirmek istediğimiz bir sistemde; farklı paydaşlar varsa, bu paydaşlar arası mutabakat gerekiyorsa, proje ve teknoloji ile ilgili riskler de göz önünde bulundurularak blokzincir teknolojisini kullanma yönünde tasarrufta bulunmak mantıklı olacaktır. Aksi takdirde blokzincir teknolojisini bu ön koşulları yerine getirmeden, körü körüne kullanma kararı almak projeye fayda sağlamayacak, aksine başarısızlık getirecektir.

4. Sonuç

Dijitalleşme ile birlikte, teknolojik gelişim hızlanmış, günlük hayat da dâhil olmak üzere pek çok alanda önemli değişiklikler görülmeye başlanmıştır. Özellikle COVID-19 dönemindeki fiziki kısıtlamalar, dijitalleşmenin önemini somut olarak ortaya çıkartmıştır. Blokzincir teknolojisi, dijitalleşme çağının en önde gelen teknolojilerinden biridir. Sunmuş olduğu aracısız işlem, şeffaflık ve yüksek güvenlik avantajları diğer teknolojilerden bir adım öne çıkmasına sebep olmaktadır. Bu avantajların sağlanmasındaki temel unsur blokzincir teknolojisinin mimari yapısından kaynaklanmaktadır. Uçtan uca dağıtık ağ mimarisi, fikir birliği mekanizması ve kriptografik anahtar yapısı bu avantajları ortaya çıkaran unsurlardır. Fakat blokzincir teknolojisi yeni yaygınlaşmaya başlayan bir teknoloji olması sebebiyle doğal olarak yüksek olgunluk seviyesine sahip değildir. Mevcut bir sistemimizi blokzincir teknolojine geçirmek veya blokzincir teknolojisi ile bir sistem geliştirmek için ihtiyaçları ve riskleri detaylı incelemek başarı için kritiktir. Teknolojinin popülerliğinden etkilenerek, körü körüne kullanma kararı almak projeye fayda sağlamayacak, aksine başarısızlık ortaya çıkacaktır. Her ne kadar blokzincir teknolojisi şu an olgunluk dönemini yaşamıyor olsa da başarılı uygulama sayısının artması ile birlikte daha fazla tecrübe edinilecek, eksikler giderilecek ve teknolojik olgunluğa ulaşılacaktır.

Kaynakça

Agarwal, M. (2018). *SBI To Create Blockchain-Based Exchange For Recovering NPA's*. Inc42. https://inc42.com/buzz/sbi-to-create-blockchain-based-exchange-for-recovering-npas/

Akbank. (2018). *Blockchain Teknolojisi Türkiye'de İlk Kez Akbank'ta*. Akbank. https://www.akbanklab.com/tr/guncel/basinda-biz/blockchain-teknolojisi-Turkiyede-ilk-kez-akbankta

Alexander, D. (2018). *Canadians to Use Blockchain for Digital IDs - Bloomberg*. https://www.bloomberg.com/news/articles/2017-11-14/forget-iris-scans-canadians-to-use-blockchain-for-digital-ids

Charleer, S., Klerkx, J., Duval, E., De Laet, T., & Verbert, K. (2016). Creating Effective Learning Analytics Dashboards: Lessons Learnt. In *Adaptive and Adaptable Learning*. Springer. https://doi.org/10.1007/978-3-319-45153-4_4

Coulouris, G., Dollimore, J., Kindberg, T., & Blair, G. (2011). *DISTRIBUTED OPERATING SYSTEMS: CONCEPTS AND DESIGN* (5th ed.).

Frank Holmes. (2018). *Bitcoin is Just the Latest in the Trend Toward Decentralization*. Forbes. https://www.forbes.com/sites/greatspeculations/2018/01/31/bitcoin-is-just-the-latest-in-the-trend-toward-decentralization-infographic/#78a89ac048ac

GoldmanSachs. (2018). *Blockchain the New Technology of Trust*. GoldmanSachs. http://www.goldmansachs.com/our-thinking/pages/blockchain/

Panetta, K. (2017). *Are You Ready for Blockchain?* Gartner. https://www.gartner.com/smarterwithgartner/are-you-ready-for-blockchain-infographic/

Papuççiyan, A. (2017). *Türkiye Cumhuriyet Merkez Bankası Blockchain Calisma Grubu*. https://webrazzi.com/2017/10/02/turkiye-cumhuriyet-merkez-bankasi-blockchain-icin-calisma-grubu-olusturuyor/

Petkovic, S., & Arnab, S. (2018). *Ideation to Realization: How Dutch Banks Are Harnessing Blockchain*. Coindesk. https://www.coindesk.com/ideation-realization-dutch-bank-harness-blockchain/

Pilkington, M. (2016). *Research Handbook on Digital Transformations* (M. Z. F. Xavier Olleros (ed.)). https://books.google.com.tr/books?hl=tr&lr=&id=1_QCDQAAQBAJ&oi=fnd&pg=PA225&dq=blockchain+public+key+cryptography&ots=s-41GDMFQ-&sig=usfePRUz2Uuj9bIMurTQfZpLk1c&redir_esc=y#v=onepage&q=blockchain public key cryptography&f=false

Pinna, A., & Ruttenberg, W. (2016). Distributed ledger technologies in securites post-trading. *European Central Bank: Occasional Paper Series*, *172*, 1–35. https://doi.org/10.2866/270533

Tasca, P., & Tessone, C. J. (2018). Taxonomy of Blockchain Technologies. Principles of Identification and Classification. *ArXiv*. https://doi.org/10.2139/ssrn.2977811

Technology, O. W. (2018). *Can digital leaders still ignore Blockchain technology?* Openwt. https://openwt.com/en/trends/blockchain

Zhao, W. (2018). *Mastercard Patent Would Put Credit Cards on a Public Blockchain*. Coindesk. https://www.coindesk.com/mastercard-patent-would-put-credit-cards-on-a-public-blockchain/