GSI JOURNALS SERIE C: ADVANCEMENTS IN INFORMATION SCIENCES AND TECHNOLOGIES

Number: 1,Issue: 1, p. 12-23, 2018

BITCOIN'İN ARKASINDAKİ GÜÇ: BLOCKCHAIN

POWER BEHIND BITCOIN: BLOCKCHAIN

Arif Furkan MENDİ[1]
Prof. Alper ÇABUK[2]
(Received 01.07.2018 Published 25.07.2018)

Özet

Son yıllarda finans piyasasında "Kripto Para" kavramı gittikçe popülerlik kazanmış, borsa gibi günlük işlem hacimleri takip edilir duruma gelmiştir. Kripto para denilince birçok insanın aklına ilk olarak Bitcoin gelmektedir. Bitcoin piyasaya çıkan ilk kripto paradır. Bitcoin'den sonra benzer nitelikte birçok kripto para birimi ortaya çıkmıştır. Bitcoin gibi bu para birimleri de işlem görmekte ve çeşitleri gün geçtikçe artmaktadır. Bitcoin ve ardından diğer kripto para birimlerinin bu denli bir popülariteye ulaşması, arkasındaki teknolojik altyapı olan "Blockchain" sayesindedir. Blockchain'in getirmiş olduğu avantajlar devrim niteliğinde gelişmelere sebep olmuş ve insanlar kripto paralar ile sanal ortamda güvenli bir şekilde işlem yapabilme imkânı elde etmiştir. Blockchain teknolojisi Bitcoin ile birlikte duyulmaya başlamış olsa da icadı Bitcoin'in ortaya çıkmasından çok daha önceye dayanmaktadır. 1991 yılında bulunan Blockchain'in tanımını yapmadan önce toplumda genel kanı olan; Bitcoin ile Blockchain'in aynı kavramlar olduğu yanılgısına düşmemek faydalı olacaktır. Blockchain teknolojisi, Bitcoin uygulamasının temelinde yer alan teknolojidir, iki kavram aynı anlama gelmemektedir. 2008 yılında ortaya çıkan Bitcoin'in popülerliğinin artması ile birlikte Blockchain teknolojisi çalışılmaya başlanmış ve yapabilecekleri ortaya kondukça ilgi odağı olmaya başlamıştır. Blockchain teknolojisinin dağıtık veri tabanı yaklaşımı, sunmuş olduğu; aracısız, şeffaf, güvenli işlem gibi avantajları sayesinde birçok firma tarafından tercih edilmeye başlanmış, firmalar yeni projelerini Blockchain teknolojisi ile geliştirmeye başlarken aynı zaman mevcut sistemlerini taşıma yönünde eğilim göstermeye başlamıştır. Bu makalede, Blockchain'in temel yapısı, sunmuş olduğu avantajları ve tüm avantajlarının yanında uygulamaya geçişteki yaşanan tereddütlerin sebebi anlatılmaktadır.

Anahtar Sözcükler: Blockchain, Bitcoin, Dağıtık Veri Tabanı Mimarisi, Açık Muhasebe Defteri

[1] Havelsan AŞ, ARGE, Teknoloji ve Ürün Yönetimi Direktörlüğü, afmendi@havelsan.com.tr
[2] Phd, Eskişehir Technical University, Faculty of Architecture and Design, acabuk@anadolu.edu.tr

Abstract

In recent years, the concept of "Crypto Money" has become increasingly popular in the financial market, where daily trading volumes such as the stock market have been tracked. Bitcoin is the most known crypto currency. Bitcoin is the first crypto currency on the market. After Bitcoin, many crypto currencies appeared in similar qualification. These currencies, such as Bitcoin, are also traded and their varieties are increasing day by day. Bitcoin and other crypto currencies have reached such a popular level by the "Blockchain", which is the technology behind it. With the revolutionary advantages that Blockchain brings, people have been able to operate securely in cyberspace with crypto money. Blockchain technology has begun to be heard with Bitcoin, but found long before the invention of the Bitcoin. Before introducing Blockchain which was found in 1991, it would be useful to point out that Bitcoin and Blockchain are not the same concepts. Blockchain technology is the technology that is the basis of Bitcoin application, the two concepts do not mean the same. With the rise of the popularity of Bitcoin in 2008, Blockchain technology became more popular and lots of application appeared. With the Blockchain distributed database approach; transparent, safe and no-intermediary processing capability are obtained. Thanks to these advantages, Blockchain has begun to be preferred by many companies, companies have begun to develop their new projects with Blockchain technology and at the same time have started to tend to move their existing systems. In this article the basic concept of Blockchain, the advantages that Blockchain serves, and the hesitations to move to Blockchain will be explained.

Keywords: Blockchain, Bitcoin, Distributed Database Structure, Open Ledger

1. GİRİŞ

Blockchain, sürekli büyüyen işlem kayıtlarının listesini çalınma veya değiştirilme gibi tehlikelerden koruyarak tutan dağıtık veri tabanı olarak tanımlanmaktadır. Bireysel işlemlerin yığınlarını tutan bloklardan oluşur. Her blok bir zaman damgası ve bir önceki bloğa bir bağlantı içerir (Nakamoto, 2008). Toplumda genel kanı olan; Bitcoin ile Blockchain'in aynı veya benzer kavramlar olduğu yanılgısını düzelterek, Blockchain teknolojisinin Bitcoin uygulamasının temelinde yer alan teknoloji olduğunu belirtmekte fayda vardır. Günümüz İnternet dünyasında pek çok alanda (multimedya, haberleşme, web ara yüzü gibi) veri transferi yapılmaktadır. Blockchain teknolojisi ise, bu verilerin haricinde değer atfettiğimiz varlıkları da transfer etmemizi sağlayan dağıtık bir veri tabanıdır. "Satoshi Nakamoto" lakaplı gizli bir yazarın 2008 yılında önerdiği Bitcoin dijital parası ile birlikte dünyada yeni bir uluslararası para biriminin varlığından bahsedilmeye başlanmıştır. Bitcoin, başlangıçta sadece para olarak düşünülürken, sonradan Bitcoin'in temelinde yer alan Blockchain teknolojisinin daha genel kullanım alanları olabileceği fark edilmiştir.

Blockchain teknolojisi birbirini tanımayan veya güvenmeyen taraflara, sistemdeki tüm katılımcıların ortak kararı ile onaylanacak ve herkesi ilgilendirecek bir kayıt oluşturulmasının yolunu hazırlar. Blockchain, gerçekleri yaratmanın ve korumanın bir yoludur (The Economist, 2015). En genel ifadeyle, merkezi bir sunucunun veya güvenilir bir otoritenin kaldırılmasına olanak sağlayarak, merkezi güvenin yerine dağıtık bir veri tabanı yapısında ağdaki tüm katılımcılara şifrelenmiş şekilde verinin yayılmasını sağlar. Blockchain teknolojisi yaygın olarak Bitcoin ve Ethereum gibi sanal paraların altındaki teknoloji olarak bilinmektedir. Fakat bu teknoloji, sağladığı olanaklar ve çeşitlendirilebilir uygulamaları ile çok daha geniş bir yelpazeye sahiptir. 1991 yılın bulunmasına rağmen İlk olarak Bitcoin kripto parası için 2008 yılında kullanılmıştır. Blockchain teknolojisine olan ilgi, Bitcoin'in kullanımının yaygınlaşmasıyla birlikte giderek artmaktadır. Blockchain'e olan ilginin nedeni herhangi bir merkeze ihtiyaç duymadan güvenli işlem yapmaya izin vermesindendir. Bu makalede Blockchain'in temel yapısı, sunmuş olduğu avantajları ve tüm avantajlarının yanında uygulamaya geçişteki yaşanan tereddütlerin sebebi anlatılacaktır.

2. ÇALIŞMA PRENSİBİ

Blockchain sistemi; herhangi bir üçüncü taraf ihtiyacı olmaksızın; dağıtık veri yapısında, katılımcılar tarafından doğrulanan blokların sistematik bir biçimde uç uca eklenmesiyle zincirlerin oluşması prensibiyle çalışmaktadır (Swan, 2015). Bu mekanizmadaki bileşenleri üç sınıfta incelememiz mümkündür. Bunlar Blockchain veri tabanı mimarisi, blok yapısı ile birlikte zincir oluşma mantığı ve doğrulama mekanizması olarak sıralanmaktadır.

Veri Tabanı Mimarisi

Blockchain, tüm işlemlerin bloklar üzerinde şifrelenmiş olarak tutulduğu dağıtılmış bir işlem veri tabanı teknolojisi olup, alıcı ve satıcının, herhangi bir üçüncü

tarafın onaylaması gerekmeden doğrudan kendi aralarında güvenli bir alışveriş yapmasına olanak tanır. Bu işlemsel veri tabanı teknolojisinde kayıtlar; işlemlerin yapıldığı ve tüm kullanıcılara açık olan Dağıtık (Açık) Muhasebe Defterinde kaydedilir (Xu et al., 2016). Geleneksel yaklaşımda (merkezi veri tabanı), veri tabanı bir üçüncü tarafça kontrol edilirken, Blockchain yaklaşımında veri tabanının kopyası tüm katılımcılara açıktır. Blockchain teknolojisinde her bir katılımcı, başlangıçtan itibaren tüm kayıtların bir kopyasını tutar. Bu kayıtların değiştirilmesi özetlerin değişmesine yol açacağından dolayı, kayıtlar değiştirildiğinde bu durum fark edilir. Bu yüzden güvenilir ortamda merkezi bir veri tabanı ihtiyacı ortadan kalkar. Herkesin doğrulama yapabildiği dağıtık bir veri tabanı sistemi ile kimseye güvenmeye gerek kalmadan doğru bilginin tutulduğu ispatlanabilir. Dağıtık veri tabanı mimarisi ve getirmiş olduğu merkezi olmayan yaklaşım Blockchain'i diğer teknolojilerden öne çıkarmaktadır.

Blok Yapısı ve Zincir Oluşumu

Blockchain'de birçok kişisel bilgisayar, birbiriyle ilişki içerisinde bulunan bir ağda yer almaktadır. Her bilgisayarın blok adı verilen kendi veri kümesi vardır. Her blok, kriptografi kullanılarak ağa eklenir ve güvenli hale getirilir. Her blok, bir "hash kodu" ile önceki bloğa bağlanır. Ayrıca kaydın tam yaratılma zamanını tutmak için zaman damgası mevcuttur (Verma & Garg, 2010). Başka bir deyişle; bloklar ağ üzerinde güvenilmeyen işlemlerin devre dışı bırakılması adına uygulanan mantıklı bir yöntemdir. Bu noktada işleyiş oldukça basittir. Bloklar üzerinde yapılan işlemler gruplandırılır ve tüm ağ için görüntülenebilen tek bir zincir bulunur. Zincirde yer alan her bir blok bir sonraki bloğa referans olur.

Merkezi otoritenin olmadığı ve P2P (kullanıcıdan kullanıcıya) işlemlerin gerçekleştiği bu sistemde güven nosyonu bir otoriteye değil, tarafların birbirine güvenmesine ihtiyaç duymayan sistem tasarımına ve çalışma mantığına adreslenmiştir. İletişimin güvenliği, kayıtların tutarlılığı ve değiştirilemezliği başta olmak üzere tüm güvenlik konuları da genelde kriptolama algoritmaları ile sağlanmaktadır. Bu sistemde alım, gönderim yapmak isteyen kullanıcı bir "private key" ve ona bağlı bir "public key"e sahip olmalıdır. Private key, sahip olduğumuz varlığı başkasına gönderebilmek için uygulamamız gereken dijital imzalama işleminde ihtiyaç duyduğumuz anahtardır. Onunla ilişkili olan public key de hem bize başkalarının bitcoin gönderebilmesi için adres görevi görür, hem de bizim başkasına bitcoin gönderme sürecimizde gerek alıcının gerekse sistemdeki tüm aktörlerin söz konusu işlemin geçerliliğini denetlerken private key'imizle şifrelediğimiz mesajı açabilmelerini ve içeriğini kontrol edebilmelerini sağlar. Eğer bizim imzalayarak şifrelediğimizi iddia ettiğimiz mesaj bizim public key'imizle açılamıyorsa biz doğru bir iddiada bulunmuyoruz demektir ve transfer işlemi geçersiz kılınır.

Private key'le imzalanan transfer işlemi P2P network'e yayınlanır. Yani mesaj sadece alıcıya değil tüm ağa duyurulmak üzere bizim bağlantıda olduğumuz tüm düğümlere gönderilir. Mesajı ilk kez alan düğümler de işlemin kurallara uygun ve geçerli olduğunu denetledikten sonra onu bağlı oldukları düğümlere yayımlar. Böylece

kısa sürede işlem, bizim alıcımız da dâhil tüm ağa yayılır. Mesajı alan düğümler bizim public key'imizi kullanıp, mesaj içeriğini açmaya yani "decrypt" etmeye ve içeriği kontrol etmeye çalışır. İşlem başarılı bir şekilde onaylanınca uygun zincirin son bloğuna eklenir. Eğer doğrulama işlemi başarısız olursa mesaj reddedilir ve işlem başarısız sayılır.

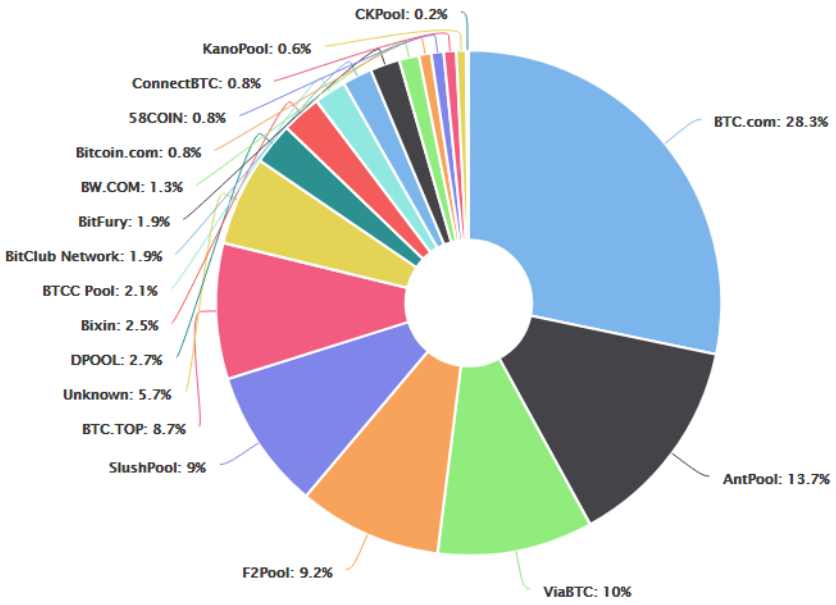
Ağ Üzerinde Doğrulama

Başarılı transaction'lar "Madenci" adı verilen düğümlerde "Teyit Edilmemiş İşlem Havuzu" olarak tanımlanan bir listeye alınır. Burada geçerliliği kontrol edilmiş, kurallara uygun bulunmuş bloklar zincire eklenmek için bekletilmektedir. Madenciler bu teyit edilmemiş işlemlerden "blok" adı verilen belirli bir büyüklüğü aşmayan bir liste oluşturmak için yarışırlar. Her blok için o bloğun içine konulan tüm "transactionlara" bağlı olarak değişen ve bir önceki geçerli bloğa da referans veren, standart bir formülle hesaplanamayan ancak çok fazla sayıda deneme ile bulunabilecek özel bir koşulu ""Hash" kodunu bulmaya çalışır. Bu değeri ilk bulan madenci yeni bloğunu, blok için bulduğu hash değerini ve bu hash'e ulaşmak için yaptığı deneme yanılmalar sonunda o hash'e ulaşmasını sağlayan "Nonce" adı verilen bir başka sayısal değeri ağa yayımlar. Bu işlemi ilk bitirip işlem kuyruğundaki ilk bloğu zincire ekleyen madenci fikir birliği işlemini tamamlamış olur ve işlemin ödülünü alır. Madencilerin gerçekleştirmiş olduğu bu hesaplama yoğun işleme "Madencilik" adı verilir. Bu işlem çok fazla işlemci gücü gerektirdiği ve geçerli bir hash ve nonce bulunması yapılan doğrulama çalışmasının ispatı niteliğinde olduğu için "Proof of Work(PoW)" olarak nitelenir (Tasca & Tessone, 2017).

Fikir birliği, farklı Blockchain teknolojilerine ve ihtiyaçlarına göre değişmektedir, her fikir birliği mekanizması, farklı özelliklere dayalı avantajlar ve dezavantajlar getirmektedir. Bu sebeple Blockchain sistem ihtiyaçlarına göre çeşitli fikir birliği yöntemleri mevcuttur (Mattila, 2016). En revaçta olan fikir birliği yöntemlerine baktığımızda karşımıza Proof of Work ve Proof of Stake(PoS) metotları çıkmaktadır. PoS metodu ağdaki işlemleri doğrulamanın bir diğer türüdür. Bu yöntem aslında madencilik bile değildir çünkü kullanıcıların yeni para üretmeleri için herhangi bir işlem yapmalarına gerek yoktur. Bu nedenle madencilik olarak değil para basmak olarak nitelendirilmektedir. Bu yöntemde para kazanmak için elektronik cüzdanınızda para bulundurmalısınız. Kazanacağınız ödül cüzdanınızda tuttuğunuz para miktarı ile doğru orantılıdır. Cüzdanınızda ne kadar çok paranız varsa o kadar çok ödül kazanırsınız yani yeni para üretirsiniz.

Proof of Work(PoW) metodunda kazdığınız blok kadar ödül kazanırsınız. Ayrıca bu doğrulama yönteminde bloğun zincire eklenmesi için gerekli algoritmayı çözen ilk kişi ödülü alır. Bu tarz madencilik, yatırımcıların veri bloklarını doğrulamada aktif bir rol almasını gerektirir bu da işlemlerin doğrulanmasını ve yeni paraların üretilmesini sağlar. Bu madencilik türünde blok doğrulaması için aktif olarak çalışmazsanız hiçbir ödül almazsınız. Ödül, yeni bloğu çözen ilk kişiye verildiği için ve blok algoritmasını çözmek için işlemci gücü gerektiğinden dolayı, en yüksek işlemci gücüne sahip kişilerin

ödülü alma ihtimali en yüksektir. Bu da madencilik işleminin kurumsallaşmasına ve milyonlarca yüksek kapasiteli işlemcinin çalıştığı büyük madencilik çiftliklerinin kurulmasına yol açmıştır (Resim 1). Kullanıcıların artık evlerindeki masaüstü bilgisayar ile bitcoin madenciliği yapması imkânsız hale gelmiştir. Bu da Bitcoin gibi birçok kripto paranın ilk çıkış fikri olan bir merkeze bağlı olmama düşüncesini günden güne zedelemektedir.



Resim 1: Bitcoin Madenci Havuzunun Dağılımı ("Bitcoin Hashrate," 2018)

PoS yöntemi ise PoW'a göre binlerce kez daha çok maliyetten tasarruf sağlar. Elektrik tüketim maliyeti nerdeyse sıfırdır. Ayrıca yatırımcıları ödül cüzdan bakiyesi bazlı olduğu için yatırımcıları daha fazla yatırım yapmaya teşvik eder. PoS metodu ilk olarak 2012 yılında bazı alternatif kripto paralar tarafından kullanılmaya başlandı. Şuanda popüler kripto paralardan olan Ethereum PoW'dan PoS'a geçme hazırlıkları yapmaktadır (Steven Buchko, 2018). Benzer şekilde birçok kripto para PoS metoduna geçiş yönünde çalışmalar yapmakta, ayrıca piyasaya çıkan yeni kripto paraların bir kısmı bu yöntemi seçmektedir.

3. AVANTAJLAR VE UYGULAMADA YAŞANAN ZORLUKLAR

Blockchain teknolojisinin özellikle Dağıtık Muhasebe defter veri yapısı sayesinde popüler teknolojiler arasına girdiğini ve birçok firma tarafından kullanılmaya başlandığını görmekteyiz. Güncel çalışmalardan bazı popüler olan örnekleri incelediğimiz zaman:

- Hollanda Bankaları (ABN Amoro, ING, RaboBank) 2014 sonunda Blockchain konusuna çalışmaya başlamıştır (Petkovic & Arnab, 2018).
- Master Card, Blockchain üzerine çalışmalarının devam ettiğini açıkladı. Hatta anlık Blockchain ödeme işlemleri için patent başvurusunda bulundular (Zhao, 2018).

- Hindistan'ın en büyük bankası olan Hindistan Merkez Bankası(SBI) önümüzdeki dönemde Blockchain teknolojisine yatırım yaptıklarını ve kullanıma alacaklarını açıkladı (Agarwal, 2018).
- AKBANK Türkiye'de bir ilk olarak Ripple firması yardımıyla Blockchain teknolojisini kullanarak para transfer işlemini gerçekleştireceğini duyurdu. Blockchain teknolojisinin Bitcoin'den ibaret olmadığını vurgulayarak, sağlamış olduğu avantajların farkında olduklarını ve kullanmayı hedeflediklerini açıkladılar ("Akbank Blockchain," 2018).
- Türkiye'de ise Merkez Bankası Blockchain için çalışma grubu kurulacağını duyurdu. Bankacılık Düzenleme Denetleme Kurumu, Sermaye Piyasası Kurulu ve Hazine Bakanlığı'nın dâhil olacağı çalışma grubuna Maliye Bakanlığı'nın da katılmasının beklendiği açıklandı (Papuççiyan, 2017).
- Kanada yeni dijital kimlik sisteminde Blockchain teknolojisine geçileceğini açıkladı. IBM desteği ile SecureKey Technologies Inc. tarafından geliştirilen sistem ile 2018'in ilk yarısında tüketicilerin bu yeni dijital kimlik sistemine kaydolabileceği duyuruldu. Bu sayede kullanıcıların bankalara, telekom hizmet sağlayıcılarına ve hatta resmi makamlara karşı kimliklerini anında doğrulayabilmeleri sağlanacaktır (Alexander, 2018).

Tüm bu örnekler Blockchain teknolojisine olan ilginin artmakta olduğuna işaret etmektedir. Bunun yanında, Blockchain teknolojisinin neden tercih edilmekte olduğuna baktığımızda karşımıza çıkacak avantajları 5 başlık altında toplayabiliriz. Bunlar; Dağıtık Veri Tabanı Mimarisi, Şeffaflık, Otomatikleşmiş Algoritma Yapısı, Güvenlik, Uçlar arası iletişimdir. (Mooney, 2011).

Dağıtık Veri Tabanı Mimarisi

Blockchain sistemi dağıtık veri tabanı mimarisinin sağlamış olduğu avantajlar ile herhangi bir üçüncü taraf ihtiyacı olmaksızın; dağıtık veri yapısında, ağdaki katılımcıların onaylaması ile birlikte zincirler oluşturulmakta, bu şekilde sistemin merkezi bir otorite ihtiyacı olmaksızın sağlıklı bir şekilde çalışması sağlanmaktadır (Swan, 2015). Sistemde tüm işlemler, işlemlerin yapıldığı ve tüm kullanıcılara açık olan dağıtık muhasebe defterinde kaydedilir. Geleneksel yaklaşımda (merkezi veri tabanı), veri tabanı bir üçüncü tarafça kontrol edilirken, Blockchain yaklaşımında veri tabanının kopyası tüm katılımcılara açıktır. Bu sayede verinin değiştirilmesi, tahrip edilmesi, manipüle edilmesi engellenir. Böylelikle güvenilir, merkezi bir otorite ihtiyacı ortadan kalkar. Herkesin doğrulama yapabildiği dağıtık veri tabanı sisteminde kimseye güvenmeye gerek kalmadan bilgi muhafaza edilir.

Şeffaflık

Tüm etkinlik kayıtları açık muhasebe defterinde tutulduğu için, ağdaki tüm katılımcıların sistemdeki tüm verileri görüntülemesi mümkündür, böylelikle şeffaflık bir sistem elde edilmiş olur (Xu et al., 2017). Bir zincirdeki her düğümün veya kullanıcının, onu tanımlayan benzersiz bir kriptografik şifreli adresi vardır. Ağ üzerindeki tüm işlemler şeffaf bir şekilde takip edilebilir, böylece veri manipülasyonu

engellenir. Sistemdeki varlığın hangi kaynaktan çıktığı ve hangi kullanıcıların kullanımına geçtiğini ve nerede olduğunu takip etmek için ideal bir platformdur.

Otomatikleşmiş Algoritma Yapısı

Açık muhasebe defteri ile Blockchain işlemlerinin sayısallaştırılmış mantığı sayesinde kullanıcılar düğümler arası işlemleri otomatik olarak tetikleyen algoritmalar ve kurallar oluşturabilmektedir (Mooney, 2011). Böylelikle işlem adımları esnek ve otomatik olarak gerçekleştirilebilmektedir.

Güvenlik

Güvenlik konusu Blockchain'in popüler olmasındaki en önemli avantajlardan biridir. Açık muhasebe defterine bir işlem eklendikten ve tüm ağda yayınlandıktan sonra kayıtlar değiştirilemez. Bunun sebebi, her bir bloğun kendinden önce gelen blok ile bağlantısının kuruluyor olmasıdır. Zincirde yer alan herhangi bir blokta yapılacak bir değişikliğe veya tahribata karşı korumalıdır. Değişikliğe uğrayan bloğun şifre kodu değişeceği için, zincirdeki bütünlük kaybolacak yani bir sonraki blok, değişikliğe uğramış olan bloğu adreslemiyor olacaktır. Zincirdeki bütünlük kaybolduğu için zincir geçerli olmayacak, ağdaki diğer kullanıcılar tarafından onaylanmayacaktır(Mooney, 2011).

Blockchain, kayıtların geri döndürülemez olduğu ve tek yönlü kriptografik karma işlevleri sayesinde taklit edilemediği, manipülasyona karşı güvenli bir sistemdir. Güvenlik göreceli bir kavram olsa da, kullanıcıların yalnızca özel bir anahtarı varsa verileri aktarabilmeleri nedeniyle blokların nispeten güvenli olduğunu söyleyebiliriz. Özel anahtarlar, bir kullanıcının gönderdiği her bir işlem için bir imza oluşturmak için kullanılır. Bu imza, işlemin kullanıcıdan geldiğini doğrulamak için kullanılır ve ayrıca, işlem yapıldıktan sonra diğer kullanıcılar tarafından değiştirilmesini de engeller (Tasca & Tessone, 2017).

Yapılacak bir siber saldırı da saldırganların sistemi ele geçirmesi için, ağdaki düğümlerin çoğunluğunu ele geçirmesi gerekmektedir ki düğümlerin dağıtık yapıda olması, bu olasılığı da oldukça düşürmektedir. (Mugla et al., 2017). PoW fikir birliği metodunda, her değiştirilecek blok için zincirdeki tüm blokların değiştirilmesi gerekmektedir. Aksi durumda işlem doğrulanmayacak ve diğer katılımcılar tarafından reddedilecektir. Yalnızca ağdaki düğümlerin çoğunluğunun ele geçirilmesi durumunda kural dışı onaylamalar ile veri manipülasyonu yapılabilmektedir. Bu saldırıya %51 saldırısı adı verilmektedir. Bu tip bir saldırı teorik olarak mümkün olsa da pratikte olası olmayacağı ve olsa bile etkisinin kısa süreli olacağı belirtilmektedir (Learn Cryptography, 2018). PoS fikir birliği metodu kullanıldığında ise ilgili saldırıyı gerçekleştirecek olanın sistemdeki tüm varlık miktarının(Ethereum vb. kripto paralar gibi) %50'sinden fazlasına sahip olması gerekmektedir (Steven Buchko, 2018). Her ne kadar bu ihtimal teorikte mümkün olsa da kripto para konsorsiyumlarının, sağlıklı bir şekilde çalışan sistemlerinin bu tür bir manipülasyona uğramasına izin vermeyeceğini,

dolayısıyla sistemin çoğunluğunu tek bir kullanıcıya vermeyeceğini düşünerek bu ihtimalin pratikte pek mümkün olmadığını söyleyebiliriz.

Uçlar Arası İletişim

İletişim, merkezi bir düğüm yerine doğrudan eşler arasında gerçekleşir. Her düğüm diğer tüm düğümlere bilgi depolar ve iletir. Özel anahtarla imzalanan aktarım işlemi P2P ağına yayınlanır. Yani, mesaj sadece alıcıya değil, ağ üzerinde bağlı olunan tüm düğümlere gönderilir. Mesajı ilk kez alan düğümler ayrıca işlemin meşru ve geçerli olduğunu kontrol eder ve ardından bağlı oldukları düğümlere serbest bırakır. Yani kısa bir süre içerisinde, alıcı da dahil olmak üzere, tüm ağda işlem yayılır. Mesajı alan düğümler, içeriğin şifresini çözme ve kontrol etme ile mesaj içeriğini açmaya çalışmak için ortak anahtarımızı kullanır. Bu doğrulama başarısız olursa, mesaj reddedilir ve işlem başarısız sayılır (Mooney, 2011).

Listelemiş olduğumuz avantajların yanında, Blockchain teknolojisini uygulama noktasında henüz standartların oluşmamış olmasının sorun teşkil etmekte olduğunu görmekteyiz. Açık kaynaklı sistem; pek çok farklı yazılım grubu tarafından, farklı idealler doğrultusunda, farklı şekilde kurgulanması bir standart oluşturulmasını engellemektedir. Tüm firmalar kendi altyapılarını ve kurdukları sistemi kullanmakta, standart bir altyapı bulunmamaktadır. Bu problemi çözmek için LINUX Açık Kaynak Kod topluluğunun koordinesinde; aralarında IBM, Cisco, Fujitsu gibi büyük teknoloji firmalarının ve J.P. Morgan, Accenture gibi finans kuruluşlarının bulunduğu 54 şirketten oluşan bir grup, "Hyperledger" adlı bir açık kaynak kod topluluğunu kurmuştur (Hyperledger, 2018a). Topluluk, yapmış olduğu çalışmalar sonrası Temmuz 2017'de "Fabric 1.0" versiyonunu piyasaya sürdüler. Şubat 2018'de ise Sawtooth 1.0 versiyonunu piyasaya sürdüler. Bu versiyonların dışında Iroha, Indy, Burrow gibi sürümleri de mevcuttur. Kullanıma sundukları farklı versiyonlar ile geliştiricilerin kullanımlarının ardından verdikleri geri bildirimlerin değerlendirilmesinin ardından olgun bir sürüm ortaya çıkarmayı hedeflemektedirler (Hyperledger, 2018b). Olgun seviyeye getirilmesi çalışmaları devam eden bu şirketler birliği faaliyetleri ile şirketler, sektörler arası para aktarımını sağlayacak dev bir altyapı oluşturulması isteniyor. Bu altyapı ile internet dünyasında, finans alanında farkındalık yaratılabileceği düşünülüyor.

4. SONUÇ

Bitcoin'in öncülüğünde kripto paraların yakalamış olduğu popülerlik ile birlikte finans alanına yeni bir kavram daha eklenmiş ve kripto para borsası oluşmuştur. Kripto paraların yakalamış olduğu bu popülerliğin temelinde Blockchain sistemi ve getirmiş olduğu göz kamaştırıcı avantajlar yer almaktadır. Günümüz İnternet dünyasında pek çok alanda (multimedya, haberleşme, web ara yüzü gibi) veri transferi yapılmaktadır. Blockchain teknolojisi ise, bu verilerin haricinde değer atfettiğimiz varlıkları da transfer etmemizi sağlayan dağıtık bir veri tabanıdır. "Satoshi Nakamoto" lakaplı gizli bir yazarın 2008 yılında önerdiği Bitcoin dijital parası ile birlikte dünyada yeni bir uluslararası para biriminin varlığından bahsedilmeye başlanmıştır. Her ne kadar

başlangıçta yalnızca Bitcoin'in temelindeki teknoloji olarak bilinse de, teknolojinin incelenmesi ile birlikte çok daha fazla kullanım alanları olabileceği fark edilmiştir. Blockchain, sürekli büyüyen işlem kayıtlarının listesini çalınma veya değiştirilme gibi tehlikelerden koruyarak tutan dağıtık veri tabanı olarak tanımlanmaktadır. Bireysel işlemlerin yığınlarını tutan bloklardan oluşur. Her blok bir zaman damgası ve bir önceki bloğa bir bağlantı içerir. Sistem herhangi bir üçüncü taraf ihtiyacı olmaksızın; dağıtık veri yapısında, katılımcılar tarafından doğrulanan blokların uç uca eklenmesiyle zincirlerin oluşması prensibiyle çalışmaktadır. Dağıtık veri tabanı mimarisi sayesinde kullanıcılar üçüncü bir taraf ihtiyacı olmaksızın, işlemlerin tüm katılımcılara açık olduğu dağıtık muhasebe defteri ile verinin kontrolünü ve doğruluğunu sağlamaktadır. Tüm katılımcıların doğrulama yapabildiği dağıtık bir veri tabanı sistemi ile kimseye güvenmeye gerek kalmadan doğru bilginin tutulduğu ispatlanabilir. Blockchain ağ yapısında her katılımcının blok adı verilen kendi veri kümesi vardır. Verilerin tutulduğu her blok, kriptografi kullanılarak paketlenir ve ağa eklenmek üzere hazır hale getirilir. Uygunluğu kontrol edilmiş bloklar zincire eklenmek üzere havuzda bekletilir. Bu blokların sistem üzerinde doğrulanması için çeşitli fikir birliği metotları vardır. Uygulanan popüler yöntemlere baktığımız zaman PoW ve PoS metotları en popüler olanlarıdır. PoW metodunda madenciler blokları ağ üzerinde doğrulayabilmek için matematiksel doğrulama problemi çözmek için çalışırken, PoS metodunda ise madenci kavramı yoktur ve herhangi bir matematiksel doğrulama problemi çözülmez. Burada kullanıcının cüzdanında ne kadar çok para var ise o kadar fazla doğrulama yapma yetkisine sahiptir. PoW metodu Bitcoin başta olmak üzere birçok kripto para birimi için kullanılıyor olsa da PoS metodu yeni çıkan ve hesaplama gücü gerektirmemesi sebebiyle popülerliği gittikçe artan bir fikir birliği metodudur. Blockchain teknolojisi, sağlam bir şekilde kurgulanmış çalışma prensibi ile birçok avantaj barındırmakta ve firmaların ilgi duymasına sebep olmaktadır. Dağıtık veri tabanı mimarisinin sağlamış olduğu; merkezi olmayan sistem, işlemlerin şeffaf bir şekilde takip edilebilmesi, otomatikleşmiş algoritma yapısı ile kullanıcı dahlinin minimum seviye indirilmiş olması, sistemin yüksek seviyede korunaklı olması sebebiyle veri tahribatının çok zor olması, merkezi doğrulama yerine uçlar arası iletişim imkânı sağlayarak fikir demokrasisi getirmesi gibi avantajlar Blockchain'i cazibe odağı haline getirmiştir. Bu ilgi çekici avantajları sayesinde birçok büyük firma Blockchain teknolojisine karşı kayıtsız kalamamış ve geçiş çalışmaları başlatmıştır. Tüm bu avantajlarının yanında, firmaların farklı idealler doğrultusunda sistemi farklı şekillerde kurgulaması henüz bir standardın oluşturulamamasına sebep olmaktır. Bu sorunun çözümü için; LINUX Açık Kaynak Kod topluluğunun koordinesinde; aralarında IBM, Cisco, Fujitsu gibi büyük teknoloji firmalarının ve J.P. Morgan, Accenture gibi finans kuruluşlarının bulunduğu 54 şirketten oluşan bir grup, "Hyperledger" adlı bir açık kaynak kod topluluğunu kurmuştur. Bu topluluk, yürütmekte olduğu çalışmalar neticesinde piyasaya çeşitli sürümler çıkartmaktadır. Bu sürümlerin kullanımı sonrası alınacak geri bildirimler neticesinde daha olgun bir sürümün elde edilmesi hedeflenmektedir. Blockchain sisteminin mükemmel kurgulanmış çalışma prensibi ile sağladığı avantajlar değerlendirildiğinde standartlaşmanın da sağlanması durumunda başarılı uygulama

sayılarının artacağını, kripto para alanının dışında başka faaliyet alanlarında da Blockchain'in yaygın bir şekilde kullanılacağını öngörebiliriz.

KAYNAKÇA

Agarwal, M. (2018). SBI to create blockchain-based exchange for recovering NPA's. Retrieved June 04, 2018 from https://inc42.com/buzz/sbi-to-create-blockchain-based-exchange-for-recovering-npas

Akbank Blockchain. (2018). Retrieved June 14, 2018 from 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. Retrieved June 14, 2018 from https://www.bloomberg.com/news/articles/2017-11-14/forget-iris-scans-canadians-to-use-blockchain-for-digital-ids

Bitcoin Hashrate. (2018). Retrieved June 14, 2018 from https://blockchain.info/tr/pools

Hyperledger. (2018a). Hyperledger Community. Retrieved June 14, 2018 from https://www.hyperledger.org/announcements/2017/07/25/hyperledger-adds-cisco-as-a-premier-member

Hyperledger. (2018b). Hyperledger Projects - Hyperledger. Retrieved June 18 , 2018from https://www.hyperledger.org/projects

Learn Cryptography. (2018). Learn Cryptography - 51% Attack. Retrieved June 18, 2018 from https://learncryptography.com/cryptocurrency/51-attack

Mattila, J. (2016). The blockchain phenomenon the disruptive potential of distributed consensus a rchitectures. *ETLA Working Papers*, *38*(38), 26. https://doi.org/10.1098/rsnr.2016.0036

Mooney, C. (2011). The truth about. *Scientific American*, (August), 80–85. https://doi.org/10.1016/j.annals.2005.11.001

Mugla, E. K.; Akba, M. F.; Katip, I.;& Karaarslan, E. (2017). Blok Zinciri Tabanlı Siber Güvenlik Sistemleri (Blockchain Based Cyber Security Systems), (October). https://doi.org/10.13140/RG.2.2.25889.71529

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, https://doi.org/10.1007/s10838-008-9062-0

Papuççiyan, A. (2017). Türkiye Cumhuriyet Merkez Bankası Blockchain Calısşma Grubu. Retrieved June 18, 2018 from 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. Retrieved June 10, 2018 from https://www.coindesk.com/ideation-realization-dutch-bank-harness-blockchain/

Steven B. (2018). Ethereum PoS movement. Retrieved June 18, 2018 from

https://coincentral.com/when-will-ethereum-mining-end/

Swan, M. (2015). *Blueprint for a new economy*. *O'Reilly Media, Inc.* https://doi.org/10.1017/CBO9781107415324.004

Tasca, P., & Tessone, C. J. (2017). *Taxonomy of blockchain technologies*. Principles of Identification and Classification. https://doi.org/10.2139/ssrn.2977811

The Economist. (2015). The great chain of being sure about things - Blockchains. Retrieved June 14, 2018 from https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things

Verma, A. K. & Garg, M. A. (2010). Blockchain: An analysis on next-generation internet. *International Journal of Advanced Research in Computer Science*, *8*(8), 429–432. Retrieved June 10, 2018from http://ijarcs.info/index.php/Ijarcs/article/view/4769/4195,

Xu, X.; Pautasso, C.; Zhu, L.; Gramoli, V.; Ponomarev, A.; Tran, A. B. & Chen, S. (2016). The blockchain as a software connector. *Proceedings - 2016 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016*, 182–191. https://doi.org/10.1109/WICSA.2016.21

Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L. &Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. *Proceedings - 2017 IEEE International Conference on Software Architecture, ICSA 2017*, 243–252. https://doi.org/10.1109/ICSA.2017.33

Zhao, W. (2018). Mastercard patent would put credit cards on a public blockchain. Retrieved June 10, 2018 from https://www.coindesk.com/mastercard-patent-would-put-credit-cards-on-a-public-blockchain/