ULUSLARARASI TİCARET VE TAHKİM HUKUKU DERGİSİ

JOURNAL OF INTERNATIONAL TRADE AND ARBITRATION LAW

Bu dergi yılda iki sayı olarak yayımlanan hakemli bir dergidir.
This is a peer-reviewed bi-annual journal.

Cilt: 7 / Sayı: 1
Volume: 7 / Issue: 1
Yıl / *Year*: 2018

LEGAL

ISSN: 2146-9717

BLOCKCHAIN VE FİNANSMAN*

BLOCKCHAIN AND FINANCING

❖ ❖ ❖ ❖ ❖

Abdurrahman ÖZALP
TEB Dış Ticaret Merkezleri Danışmanı
ICC Türkiye Bankacılık Komisyon Başkanı
Counsellor for TEB Foreign Trade Centers
Chair of ICC Turkey Banking Commission

❖ ❖ ❖ ❖ ❖

Öz

Blockchain internet üzerinde merkezi olmayan dağıtık yapıda çalışan hızlı, güvenilir ve güçlü bir teknolojidir. Blockchain, başta finansman olmak üzere farklı alanlarda kullanılabilir. Çalışmamızda Blockchain kavramı açıklandıktan sonra muhtelif alanlarda kullanımının sağlayacağı katkılar incelenecektir.

Anahtar Kelimeler

Dağıtık yapı, açık defter, dijital cüzdan, akıllı sözleşme, açık anahtar, özel anahtar, uçtan uca, kripto, dijital para, Bitcoin, Blockchain

Abstract

Blockchain is a fast, reliable and powerful technology that operates on a decentralized distributed structure on the internet. Blockchain has a wide range of uses, mainly in financing. In this study the benefits of usuing Blockchain in various field will be evaluated.

Keywords

Distributed structure, open ledger, digital wallet, smart contract, public key, private key, peer-to-peer, crypto, digital currency, Bitcoin, Blockchain

***

* Bu makale 20.12.2017 tarihinde Editörler Kurulu'na ulaşmış olup 09.01.2018 tarihinde birinci hakem ve 24.01.2018 tarihinde ikinci hakem incelemesinden geçmiştir (ORCID ID: 0000-0001-9828-1442).

İçindekiler

Kısaltmalar

BFHD	: Banka ve Finans Hukuku Dergisi
Bkz.	: Bakınız
BPO	: Bank Payment Obligation
BTC	: Bitcoin
CEO	: Chief Executive Officer
DNS	: Domain Name System
IBM	: International Business Machines
ISBP	: International Standard Banking Practices
KYC	: Know Your Customer
PBFT	: Practical Byzantine Fault Tolerance
POA	: Proof of Activity
POC	: Proof of Capacity
POS	: Proof of Stake
POW	: Proof of Work
SWIFT	: Society for Worldwide Interbank Financial Telecommunication
TMA	: Transaction Matching Application
UTTDER	: Uluslararası Ticaret ve Tahkim Hukuku Dergisi
WEB	: World Wide Web

I. Blockchain Kavramı ve Benzer Sistemlerden Farkı

Türkçeye "Blok Zinciri", "Bağlı Kayıtlar Dizisi" veya "Bağlı İşlem Öbekleri" şeklinde çevrilebilecek "Blockchain", işlem kayıtlarının bilgisayar ağları üzerinde zaman kaşesiyle tarihlenerek tarihçeleriyle birlikte geriye dönük olarak değiştirilemeyecek ve silinemeyecek biçimde birbirine bağlı bloklar halinde saklayan, istendiğinde ulaşılabilen, denetlenebilen, programlanmış sözleşmeleri (smart contracts)yürütebilen Blockchain web'den (wold wide web) farklı bir teknolojidir. Blockchain, herkese açık, özel veya yarı özel olabilir. Blockchain, web'den farklı olarak merkezi yapıda değil dağıttık yapıda çalışır. Böyle bir yapı bir taraftan hız, güvenlik ve devamlılık sağlarken diğer taraftan bunun doğal sonucu olarak kolaylık ve maliyet avantajları getirmektedir. Blockchain'nin diğer sistemler ile birlikte yani hybrid olarak çalışması da mümkündür, hatta kısmi web veya kısmi Blokchain olabilir.

Blockchain hakkında bazı yanlış bilgileri düzeltmek gerekir. Blockchain hakkındaki yanlış bilgilerden biri, Blockchain'in işlem kayıtlarını elektronik ortamda tutabilen açık küresel bir hesap defteri olduğudur. Ancak Blockchain sadece işlem kayıtlarını elektronik ortamda tutan basit küresel defter değildir. Bunun çok ötesinde bilgileri yüksek derecede şifreleyerek geriye doğru değişmez biçimde saklayabilen, havale, devir, takip, tevsik, doğrulama işlemleri yapabilen, akıllı sözleşmeleri çalıştırabilen, programlanan iş ve işlemleri yürütebilen, yönetim ve devlet işlerinde kullanılabilecek yeni bir teknolojidir. Durum böyle olunca, başta hayatı kolaylaştıran günlük işler olmak üzere tüm devlet, yönetim ve finansman gibi tüm konuları yeniden düşünmek gerekmektedir. Blockchain, bir alet, araç veya makine değildir, Blockchain web gibi internet üzerinde çalışan ancak web'den farklı avantajlar sunan bir altyapıdır. Blockchain'nin üst yapıda verimli olması için akıllı ve profesyonel yazılımlar ile desteklenmesi ve donatılması gerekir. Aksi halde sadece basit havale, saklama ve doğrulama işlerini kullanmaya yarayacak, bunun ötesine geçemeyecektir. Daha ileri düzeyde ileri finansman ve hukuk işleri, devlet, yönetim, sanayi gibi yerlerde kullanmak için daha profesyonel yazılımlarla çalıştırmaya ihtiyacı vardır. Nasıl çalıştırırsanız öyle verim alırsınız, Blockchain de limit sizsiniz. Blockchain ile sadece pizza siparişi vermek, basit iddia veya bahis işine girmek veya akıllı

sözleşmeler ile akreditif[1] açmak, finansman işleri yapmak veya sanayi işlerini yapmak da mümkündür. Daha önce belirttiğimiz gibi Blockchain ile yapılabilecekler konusunda sınır yok gibidir; burada sınır, kişilerin hayal ve yeteneğidir. Bugün internet üzerinde web teknolojisi ile birçok ticaret ve bankacılık işlemi yapılabilmektedir. Blockchain ile bunun çok daha fazlası yapılacaktır, uzmanlara göre web teknolojisi bilgiye ne yaptıysa Blockchain teknolojisi de işlemlere aynı şeyi yapacaktır.[2] Blockchain'i sadece bir teknoloji olarak görmemek gerekir, birçok şeyi değiştirecek ve etkileyecek bir olay olarak görmek gerekir. Kısacası Blockchain, sosyal hayattır, finansmandır, yönetimdir, devlet işleridir, iş dünyasıdır, eskidir, yenidir, her şeydir. Başta finans dünyası olmak üzere pek çok alanda köklü değişikliklere yol açacağı için her yenilikte olduğu gibi başlangıçta dirençle karşılaşacaktır. Bu direnç daha fazla bankalar ve finans kurumları ile bilgi teknolojileri firmalarından gelecektir. Zira bir çok işlemde bu aracıları ortadan kaldıracaktır. En fazla teknoloji firmaları, bilgi güvenliği ve bankalar gibi kurumları tehdit edeceği tahmin edilmektedir. Örneğin, bir havale bir göndericiden bir alıcıya noktadan noktaya aracısız olarak güvenli ve hızlı bir şekilde yapılabiliyorsa bu hizmet için bir bankaya komisyon ödemenin anlamı olmayacaktır: Aynı durum bir akreditif işlemi veya noterlik işlemi için de geçerli olabilecektir. Başta bankalar ve finans kurumları olmak üzere SWIFT gibi önemli mesajlaşma firmaları başlangıçta bu gücü küçümsediler, zamanla bu gücün büyüklüğünün farkına varabildiler ve sonuçta iş birliği yapmak ve kullanma eğilimine girdiler. Bu durum sadece bankalar ve finans kurumları için değil diğer birçok sektör içinde geçerli olacaktır. Bu nedenledir ki IBM, SWIFT, Barclays Bank, HSBC, BNP, Banco Santander, Bank of America, Credit Mutual, Societe Generale, UBS, Westpac, Standard Chartered, LLoyds Bank, Credit Suisse, RSB, ABN AMRO, CBW BANK, BBVA Compass, Citibank, HSBC, JPMorganChase, Morgan Stanley, DBS, USAA, Rabobank, Fidor Bank, Goldman Sacs, Nasdaq, CrossFlayerBank, Deutshe Bank, ANZ Bank, Euro Banking Associa-

---

1 Akreditif ve özellikle işleyişi hakkında bkz. ÖZALP Abdurrahman, Akreditif ve Uygulama Yeni ISBP'ye Göre, İstanbul 2015, s. 13-169.

2 "What internet did to the information, blockchain will do the same to the transactions" Ginni Rometty, CEO, IBM. https: //www.forbes.com/sites/tomgroenfeldt/2016/09/28/ibms-ginni-rometty-tells-bankers-not-to-rest-on-their-digital-laurels/#79ab4ae3604d). Erişim tarihi 08.01.2018.

tion, UHV Bank, Visa, Western Union, Commonwealth Bank gibi kurumlar bu konuda çalışma ve uygulama geliştirmeye başladılar.

II. Blockchain'i Değerli ve Güçlü Yapan Unsurlar

Blockchain'nin en güçlü taraflarından biri merkezi bir sisteme bağlı olmaması, dağıtık yapıda çalışmasıdır. Birbirlerine direkt ve bir şebeke üzerinde bağlı bilgisayarlar aracılığıyla kesintisiz çalışır. Blockchain yapısında bilgisayarlar dağıtık bir yapı ile birbirlerine bağlıdırlar, kompleks bir yapı ile tek bir merkeze bağlı olmadıkları için sistem hatası, elektrik kesintisi veya siber saldırılar sonucu tamamen devre dışı kalmaları pek mümkün değildir.

Internet, yakın tarihte web teknolojisi ile bazı aracıları ortadan kaldırmıştı. Şimdi de Blockchain bir başka grup aracıları ortadan kaldıracaktır. Bir görüşe göre, web, bilgiye ne yaptıysa Blockchain de işlemlere aynısını yapacak, insan aklının sınırlarını zorlayacak ve hayallerin ötesine geçecektir. Zaten Blockchain söz konusu belirtilerinden birçoğunu görmeye başladık bile. Web ve veri tabanları en ileri teknoloji oldukları dönemde nasıl kendi yaklaşımlarını getirdilerse Blockchain de kendi yaklaşımını getirecektir. Bir süre dirençle karşılaşsa bile sonunda bu yaklaşım benimsenecek ve kullanılacaktır. Geçmişte "google" ve "akıllı telefonlar" olmadığı halde işlerimizi yapıyorduk, bugün yine yapıyoruz ancak işerimizi yapmamızda google ve akıllı telefonlar vazgeçilmez olmuştur. Eskiden düşünemediğimiz birçok şeyi bunlar aracılığıyla daha verimli yapmaya başladık, yeni kapılar açtılar, birçok mesleği ve aracıyı ortadan kaldırdılar, ancak yeni meslek ve aracıları da beraberlerinde getirdiler. Blockchain de bugün her ne kadar acil bir ihtiyaç olarak gözükmüyorsa da ileride birçok alanda vazgeçilmez olacaktır. Daha nelere yol açabileceğini şimdiden tam olarak söyleyebilmek mümkün değildir. Belki de verileri verip roman, hikâye, makale ve senaryo yazdırmak bile mümkün olabilecektir. Bugün geleneksel yöntemlerle yaptığımız birçok işlemi Blockchain ile yapabiliyor olacağız. Örneğin; para transferleri, tapu kayıtları, noter işlemleri, kimlik doğrulamaları, işlem takipleri, akıllı sözleşme düzenlemeleri, finansman işleri, patent ve telif hakları korumaları vs. Diğer taraftan mükerrer işlemleri, yasal olmayan işleri ve birçok sahteciliği önlemek gibi olumlu işlerde göreceğiz. Bugün web teknolojisi ile çok fazla bilgiye ulaşabiliyoruz, ancak bilgiye ulaşmak yeterli değildir. Birçok durumda ulaşılan bilgiye güvenmek ve işleme alabilmek için o bilginin orijinal olduğundan ve değişmediğinden emin olma-

mız gerekmektedir. Mevcut durumda bunu sağlayabilmek yani güvenilir bilgileri elde edebilmek için üçüncü tarafların hizmetinden faydalanmamız gerekmektedir, yani bir bakıma üçüncü taraflara güvenmek zorundayız. Blockchain ile bu ihtiyaç karşılanacaktır, bu tür aracılara ihtiyacımız olmayacaktır. Zira Blockchain ile başka kişilerin hizmetine değil sisteme güven vardır. Blockchain de yüksek derecede güvenlik standarttır, zira bir ilk blokun oluşturulması veya yeni bir blokun mevcut blok zincirine eklenebilmesi için yüksek matematiksel algoritmalar ile çok kısa sürede şifrelenmesi şebeke üzerindeki görevli bilgisayarlarda (nodle) doğrulanması ve konsensüsünün sağlanması gerekir. Blockchain üzerinde yapılan işlemler kendi güvenliklerini kendileri sağladıkları için ayrı bir güvenlik sertifikasına ihtiyaçları yoktur, her bir işlem yüksek şifreleme ve doğrulama yöntemleriyle sisteme girer ve aynı şekilde işlem görmeye devam eder. Blockchain de basit şifreleme yöntemleri kullanılmaz, kaynağını yılların birikim ve tecrübesinden alan kriptoloji bilimini en ileri düzeyde kullanan algoritmik şifreleme ve doğrulama yöntemleri kullanılır ki zaten Blockchain'i güvenilir, ilginç ve kullanılabilir kılan da budur. Daha önce belirttiğimiz gibi Blockchain'de sisteme güven duyulur, kişilere değil. Blockchain mekanik açıdan yeni bir teknoloji değildir, ancak mevcut yazılım teknolojisini mevcut uygulamaların yerini alabilecek uygulamaları geliştirmeye zorlayan bir teknolojidir.

Blockchain, başta finans olmak üzere hayatın pek çok alanı için yenilikler getirmektedir. Blockchain teknolojisi gerek noktadan noktaya aracısız çalışma özelliği ile gerekse de kullandığı çok sağlam algoritmik şifreleme ve doğrulama yöntemleri ile web teknolojisine göre çok daha güvenli, kolay ve hızlı bir teknolojidir. Her yeni teknolojide olduğu gibi Blockchain'e de direnç ve zorluklar olacaktır. Bunlar bazıları fikri, bazıları fiziki olacaktır. Fikri olanlar daha çok bilgi eksikliği, endişe ve önyargı kaynaklıyken fiziki olanlar daha çok standartlar ile ilgilidir. Bunlar altyapı ve üst yapı standartlarıdır, alt yapıda standart genelde sağlanırken üst yapıda standardın sağlanması her zaman mümkün olmamaktadır. İş yapmak için geliştirilen ve kullanılan uygulamaların çoğu standart değildir. Geliştirmek için kullanılan yazılımların bile çok farklı özellikleri olabilmektedir, bu nedenle anlaşılmaları, yaygın kullanılmaları pek kolay olmamaktadır, örneğin; IBM, Etherum, Ripple.

Blockchain ile ilgili önemli engellerden bir diğeri yukarıda belirttiğimiz gibi yanlış bilgilerdir. Blockchain'e ilişkin yanlış bilgilerden bazıları şunlardır: yeraltı ve gizli servisler tarafından geliştirilmiştir, suç

ortamlarında kullanılır, derin internettin ürünüdür, kaçakçılık, kara para ve terörizmin finansmanında kullanılır. Blockchain'in yasal olmayan işleri çağrıştırmasının nedeni, başlangıçta yasal görülmeyen işlerde kullanılmasıdır ve bir devlete ait olmayan dijital paraların, örneğin Bitcoin, kullanılması için geliştirilmiş olmasıdır. Bu hususlar, Blockchain'e mesafeli yaklaşmaya neden olmaktadır. Şüphesiz zamanla Blockchain'nin sağlık, eğitim, devlet işleri gibi faydalı işlerde kullanıldığı görüldükçe bu önyargılar ortadan kalkacaktır. Ancak bu önyargıların ortadan kalkması zaman alacaktır. Bu kısma katkı sağlaması bakımından öncellikle yanlış bilinen bazı konuları açıklamakta fayda vardır. Bu konuları iki sorunun cevaplarıyla açıklamaya çalışacağız.

Birinci soru, Blockchain, yeraltı dünyası ve yasadışı işler ile mi ilgilidir? Bu sorunun cevabı hayırdır. Çünkü bu teknoloji sadece yeraltı dünyası ve yasadışı iş yapan kişilerin kullandığı işlemlerle ilgili değildir. Herkes kullanabilir, sonuçta bir teknolojidir, hangi amaçla kullanılırsa o şekilde sonuç doğurur. Devlet ve özel sektör işlerinde rahatlıkla kullanılabilir. Önemli olan yasal ve teknolojik altyapısının kurulmasıdır.

İkinci soru, Blockchain, sadece dijital para (Bitcoin, Litcoin, Ether, Altcoin) ve transferlerinde mi kullanılabilir? Bu sorunun cevabı da hayırdır. Blockchain'nin çok geniş bir kullanım alanı vardır, sadece dijital para transfer işlerinde kullanılmaz. Bu nedenle şimdilik değişik amaçlar için geliştirilmiş birkaç versiyonu mevcuttur. Bunlar; Blockchain 1.0, Blockchain 2.0 ve Blockchain 3.0'dır. Bunlardan sadece Blockchain 1.0 para ve ödeme işlemleri ile ilgiliyken diğerleri sözleşmeler, taahhütler, protokoller, belgeler, teyitler, değerler, uygulama ve yönetim işleriyle ilgilidir. Örneğin; Blokchain 2.0 sözleşmeler ve doğrulama işlemleri ile ilgiliyken Blockchain 3.0 yönetim ve çözüm işleriyle ilgilidir.

III. Blockchain'in Ortaya Çıkışı ve Gelişimi

Blockchain'nin tarihi Bitcoin isimli dijital kripto para ile başlar. Bitcoin, Dijital para birimidir. Altın gümüş vb. gibi maddesel veya fiziki bir karşılığı şimdilik yoktur. Bitcoin bir ağ etkileşimidir. Herhangi bir merkezi yoktur. A'dan B'ye dijital para transferi sağlamaktadır. İnternet olan herhangi bir noktadan internet olan herhangi bir noktaya transferi yapılabilir. Aracısı ve komisyoncusu bulunmamaktadır. Bu nedenle masraflar da oldukça düşüktür. Sadece transfer işlemini onaylayan madencilere çok cüzi miktarlarda ödeme yapılır. Bitcoin, açık kaynak kodla yazılmıştır ve erişim açısından herkese açıktır. Sistemin sahibi onu kulla-

nan herkestir, tüm ülkelerde kullanılır ve offline hesabına kimse müdahale edilemez. Bu bakımdan İsviçre bankalarından daha güvenlidir şeklinde yorumlanabilir. Kullanım koşulu, ön sınırlama sözleşmeleri veya şartları gibi sınırlayıcılar yoktur. Bitcoinler, "madenci" denilen ücretsiz bir program tarafından üretilir, üretilecek bitcoinlerin belli bir sayı sınırı vardır, toplamda 21 milyon adet üretilecektir, üretim hızını ve enflasyonunu kontrol edebilmek için "zorluk seviyesi" her geçen gün belirli protokoller çerçevesinde artmaktadır. Bu seviyeler ağdaki üretim yoğunluğuna göre belirlenir, her kullanıcının dijital bir cüzdanı vardır. Bitcoinlerinizi bu cüzdanlarda tutarsınız, Bitcoin transferleri eşsiz bir imza ile imzalanır ve sırayla madenciler tarafından doğruluğu ve eşsizliği kontrol edilerek onaylanır, böylece aynı bitcoin ikinci kez kullanılamaz. Bitcoin ile ürün satışı yapmak için hiçbir ekstra ödeme yapılmaz. Sizden herhangi bir ön koşul istenmez, Bitcoin, TL, USD, EURO gibi birçok para birimine dönüştürülebilir. Ancak bu işlemi yapan siteler komisyon almaktadır. Qr kodu ile mobil ödemeler yapılabilir, Bitcoin borsaları hafta sonu ya da tatil günleri durmaz, daima çalışırlar[3].

Bitcoin, Satoshi Nakamoto mahlasıyla 2008 yılında yazılan "Bitcoin: Uçtan Uca Elektronik Ödeme Sistemi" isimli makaleyle dünyaya duyurulmuştur. Satoshi'nin getirdiği yenilik, dağıtık işlemci güçlerini kullanarak her on dakikada bir transfer işlemleri onaylayan bir mekanizmayla, çifte harcamayı engellemiş olmasıdır. Satoshi Nakamoto, güvensiz ve potansiyel olarak hileli, dağıtık bir işlemci ağında, bilgi paylaşımının nasıl olacağı problemi olarak bilinen "Bizans Generalleri"[4] problemine, merkezi bir otorite kullanmadan, "iş ispatı" kavramıyla, yeni bir çözüm önermiştir. Satoshi Nakamoto'nun Nisan 2011'de ortalıktan kaybolmasına rağmen, sistem tamamen şeffaf ve matematik prensipleri çerçevesinde çalışmaya devam etmektedir. 2009 yılında çalışmaya başlayan Bitcoin ağının, şu an ki toplam işlemci gücü, dünyanın en hızlı bilgisayarlarının gücünden fazladır. 1 Aralık 2016 itibarıyla, Bitcoin'in toplam pazar değeri yaklaşık 12 milyar Amerikan Doları'dır. Bugüne kadar, transfer yapılan en büyük tutar 194.993 BTC'dir (yaklaşık 147 milyon

[3] Bu paragrafta verilen örnek ve konuyla ilgili ayrıntılı bilgi için bkz. ehttp: //cointurk.com/bitcoin-nedir. Erişim tarihi: 8.1.2018.

[4] Bizans Generalleri örneği konu anlatımında sıklıkla kullanılan ve genel olarak Dünya'da kabul gören bir terimdir. Konuyla ilgili detaylı bilgi için bkz. https: //hipper.club/bitcoinin-tarihcesi. Erişim tarihi: 08.01.2018.

dolar). Bu işlem Kasım 2013'te hiç bir işlem masrafı alınmadan gerçekleştirilmiştir[5].

IV. Blockchain'in İşleyişi ve Kullanılabileceği Alanlar

A. Blockchain'in İşleyişi

Blockchain, ağ üzerinde dağıtık yapı ile birbirine bağlı bilgisayarlar üzerinde yardımcı uygulama programları aracılığı ile çalışan bir sistemdir. Kullanıcılar uygulama programları aracılığıyla işlemi Blockchain'e gönderirler. Blockchain'e gönderilen işlem şifrelenir, analiz edilir, doğrulanır ve en uzun blok zincirine eklenerek tamamlanır. İşlemler Blockchain'de amacına göre işleme tabi tutulurlar, saklanmak amacıyla gönderilen veriler şifreli olarak saklanır, bir işi yapmak (performance) veya bir programı yürütmek üzere programlanan bir akıllı sözleşme (smart contracts) verilen programa göre çalışır. İşlemler internet veya özel ağlar üzerinde herkese açık olarak veya tercihe bağlı olarak bir gruba kapalı olarak bir merkezin veya üçüncü tarafların hizmetine ihtiyaç duyulmadan noktadan noktaya veya uçtan uca (peer-to-peer) eş düzeyli birimler arasında direkt olarak yapılır. Üçüncü kişilerin hesap tutmasına veya servis sağlamasına gerek yoktur. Geliştirilen yeni yazılımlar ile basit bir bilgisayar üzerinde bile blockchain işlemi yapmak mümkündür. Bunun için kullanıcının kendi bilgisayarına yükleyeceği bir yazılımı veya ağ üzerindeki düğümlerde (nodes) çok güçlü bilgisayarlar üzerinde kurulu profesyonel yazılımları o yerlerde kullanmak gerekir. Bu amaçla şu anda kullanılan yazılımlar şimdilik sınırlıdır, ancak bunlar her geçen gün geliştirilmektedir. Bazıları gelişmelere uyum sağlayarak farklı bir yapıya dönerken, bazıları uyum sağlayamadığı için ortadan kalkmakta ve piyasaya yenileri girmektedir. Bütün bu eksiklikleri gidermek için yazılım teknolojisinde yapılacak hamleler sonucunda, gelecekte sayıca çok daha güçlü ve nitelikli yazılımların görüleceği kanaatindeyiz.

Mevcut durumda bir işlemi Blockchain ile kullanmak için o işlemi uygun bir yazılım ile "hashing" ederek göndermek gerekir. Burada "hashing" etmek, bir işlemi içeriği ile birlikte 64 karakterli bir özet haline getirmektir. 64 karakterli bir özet haline getirilen bilgi adres ve açık anahtar (public key) ile kullanılır. Sisteme gönderilen bir işlemin gerçek-

[5] ÇARKACIOĞLU Abdurrahman, Kripto-Para Bitcoin, Araştırma Raporu Aralık 2016, Sermaye Piyasası Kurulu Araştırma Dairesi, s. 14-15.

leşmesi için önce şifrelenmesi, ağ üzerindeki görevli bilgisayarlarda analiz edilmesi, doğrulanması, geriye doğru değişmez şekilde zaman kaşesiyle kapatılması, mevcut ilgili en uzun işlem blok zincirine eklenmesi ve bir kopyasının ağ üzerinde bulunan (kapalı özelde izin verilen) bilgisayarlara dağıtılması gerekir. Bu işlemler "madenci" denilen kişiler tarafından yapılır.

Madenci kişiler bu işi para kazanmak için belirlenen kurallara göre kurulmuş (established) bir yapıya uygun olarak yaparlar. Bu kurulu yapı madencilerin tümünün, bir veya birkaçının veya bir başkasının kötü niyetli girişimlerini kabul etmemek üzere gerek süre gerekse de zorlaştırılmış matematiksel algoritmalarla yapılandırılmıştır. Günümüzdeki mevcut teknoloji ile bu sistemi manipüle etmek neredeyse imkânsızdır. Madenciler bu hizmeti sistemden aldıkları ücret karşılığında hız ve disiplin içerisinde yaparlar. Bunun için yüksek performanslı çok hızlı makine ve özel programlara ihtiyaç duyarlar, yüksek derecede elektrik enerjisi tüketirler, harcanan elektrik ile kazandıkları para arasındaki fark gelirleri olur. Bunun için çok hızlı, organize ve disiplin içerisinde çalışmaları gerekir. Teorik olarak mümkün olmakla birlikte pratikte normal bilgisayarlar ile bu işleri yapmak neredeyse mümkün değildir, çok güçlü ve hızlı özel makinalar kullanmak gerekir. İşlemleri yapmak için madenci olarak tabir edilen kişilerin avcı programlarla girişi yapılan işlemleri bulması ve tamamlaması gerekir. Madencinin yaptığı neticede girilen bir işlemi yakalamak, çözümlemek, doğrulamak, bir önceki işleme bağlamak ve birer kopyasını ağ üzerindeki görevli bilgisayarlara ("nodes") göndermektir. Kopyaların ağ düğümlerinde yani görevli bilgisayarlarda değişmeden muhafaza edilmesi önemlidir. Zira müteakip doğrulamalar bu noktalar kullanılarak yapılacaktır ki bu çift işlem (double spending) oluşmasını ve sahteciliği engellemek bakımından önem taşımaktadır.

Bir işlemin "işlem blok zinciri"ne eklenmesi için mutlaka doğrulanması gerekir. Doğrulama işlemi mutabakat yani konsensüs[6] sağlanarak yapılır. Konsensüs sağlanmadan işlem tamamlanmaz, reddedilir. Örneğin, işlem bir havale veya ödeme ise o ödeme veya havale gerçekleşmez. Konsensüs için farklı yöntemler vardır. Bunların en önemlileri Proof of Work (POW), Proof of Stake (POS) ve Practical Byzantine Fa-

[6] USTA Ahmet/DOĞANTEKİN Serkan, Kapital Medya Hizmetleri A.Ş., 2017 Blockchain 101, s.125,.

ult Tolerance'tır (PBFT)[7]. Bunların dışında Proof of Activity (POA), Proof of Capacity (POC) gibi karma yöntemler de vardır. POW ve POS daha çok herkese açık hesap defterleri işlemleri için uygun olurken PBFT yani "Bizanslı Generaller" problemini esas alan algoritmalı yöntem özel veya kapalı blok zinciri işlemleri için daha uygundur. Bu yöntemin mantığının Bizanslı generallerin kullandıkları bir yönteme dayandığı, sıklıkla uygulamada belirtilmektedir[8]. Bizanslı generaller üstlerinden gelen emirlerin gerçek olup olmadığını anlamak için basit ancak etkili bir yöntem kullanmışlar. Buna göre üstlerinden gelen emir, generallere birden çok haberciler yoluyla gönderiliyormuş. Emri alan generaller de bunu kendi aralarında haberciler yoluyla paylaşıyorlarmış, belirlenen plana göre emir ile ilgili çoğunluk sağlanırsa doğru kabul edilip uygulanıyor, aksi halde uygulamıyormuş. Blockchain de bu yöntemi benzer bir şekilde, ağ üzerindeki bilgisayarlara uygulatmaktadır. Buna göre ağ üzerinde doğrulama yetkisine sahip bilgisayarlar vardır. Bu bilgisayarların her birinde doğrulama yetkisine sahip diğer bilgisayarların açık anahtar (public key) bilgisi bulunmaktadır. Her makine kendisine gelen bir işlem bilgisini kontrol eder, doğruladığı işlemi imzalayarak ağdaki bütün bilgisayarlara birer kopyasını gönderir. İşlem önceden belirlenen plana göre yeterli sayıda bilgisayar tarafından onaylanırsa konsensüs sağlanmış olur ve ağ tarafından geçerli işlem olarak kabul edilir. İşlem zaman kaşesiyle kapatılarak en uzun işlem blok zincirine eklenir. Böylece o işlem bir öncekine geri dönülmez ve değişmez biçimde bağlanmış olur, blok zinciri veya Blockchain budur.

Yukarıda belirtildiği üzere bir kopyası o ağ üzerinde bulunan ilgili bilgisayarlara dağıtılır. Müteakip işlemlerin ağ üzerindeki bu kopyalardan doğrulanması gerekir, aksi halde işlem gerçekleşmez. Kötü amaçlı birinin sistemi manipüle etmesi için başlangıçtan (genesis) beri oluşturulan ilk bloktan itibaren bütün eklenen yeni blokları ve bunların dağıtılan bütün bilgisayarlardaki kopyalarını değiştirmesi gerekmektedir. Ancak kullanılan algoritmanın çalışma şekli ve işlemin tamamlanması için gerekli kısıtlı süre buna imkân vermeyecek biçimde yapılandırılmıştır. Bu nedenle bu günkü mevcut teknoloji ile gerçek olmayan bir işlemin doğrulanması neredeyse imkânsızdır. Mevcut durumda bu yapı kullanılmak-

[7] USTA/DOĞANTEKİN, s. 131.

[8] Bu örnek ve Blockchain ile bağlantısı hakkında detaylı bilgi için bkz. https://teknochain.com/teknik-detaylari-ile-blockchain/. Eişim tarihi: 08.01.2018.

la birlikte ileride bunlara gerek bırakmayan çok daha güçlü ve farklı yapıların kullanılması da mümkün olabilecektir. Sonuçta burada önemli olan konu, bir bilgi veya bir işlemin çok güvenli olarak geriye doğru değiştirilemeyecek biçimde bir işlem blok zincirine eklenmesi ve gerektiğinde aynı güvenlikte elde edilebilir olması, kullanılabilmesi ve işleme alınabilmesidir. Şimdilik Blockchain ile yapılabilenler iş ve işlemler işin çok başında olduğu için sınırlı olsa bile geleceğe yönelik olarak çok büyük imkânların sinyallerini vermektedir. Sadece finansman dünyası için değil hayatın her alanı için çok büyük imkânlar olacaktır. Web teknolojisinin imkân ve sınırları bellidir, birçok yerde merkezi yapıları ve üçüncü tarafların hizmetlerini kullanmak zorundadır. Böyle bir durum kötü amaçlı kişilerin iştahını kabartmakta, ilgilerini çekmekte ve bunlar tarafından ele geçirilmeyi ve siber saldırılara maruz kalmayı olanaklı kılmaktadır, zira her zaman merkezi bir yeri ele geçirmek dağıtık bir yapıyı ele geçirmekten daha cazip ve kolaydır.

Blockchain farklı uygulamalarla farklı alanlarda kullanılabilir. Bazı durumlarda havale ve ödemeler için para transferi yapmaya yarayan basit uygulamalar yeterli olurken, daha ileri finansman işleri için akıllı sözleşmeleri (smart contracts) dikkate alan uygulamaları ve idari işler/devlet işleri için daha çok veri okuma ve doğrulama uygulamalarını kullanmak gerekli olacaktır. Bu birbirinden farklı amaçlar için mevcut durumda üç ayrı Blockchain sürümü vardır. Bunlar; Blockchain 1.0, Blockchain 2.0 ve Blockchain 3.0 şeklinde ayrılmıştır. İleride belki başka sürüm ve ayırımlarda olabilecektir. Blockchain 1.0 basit ödemeler ve havaleler, Blockchain 2.0 interaktif veri ve sözleşmeleri kullanan ticari uygulamalar ve Blockchain 3.0 yönetimsel işler için uygun sistemlerdir.

Yukarıda ki sürümler bazında Blockchain'lerin genel karakteristikleri üzerinde durmak gerekir. Blockchain 1.0[9] Bitcoin ile karıştırılmaktadır, Bitcoin dijital bir paradır, oysa Blockchain yukarıda belirtildiği üzere, bir altyapıdır, para değildir, şeffaf ve küresel açık bir hesap defteridir, üzerinde para göndermeye, işlem yapmaya yarayan uygulamalar (yazılım) ve programlanabilir protokoller çalışır. Blockchain 1.0 üzerinde çalışan uygulamalar Bitcoin gibi dijital paraları havale etme ve ödeme yapma işlerinde kullanılırlar. Blockchain 1.0 üç kademeden oluşur; alt-

[9] SWAN Melanie, Blockchain, Blueprint for a New Economy, Chapter 1. Printed in the United States of America, Published by O'Reilly Media, Inc., Sebastopol, CA 95472. Year: 2015, s. 1.

yapı, yazılım/uygulama/protokol ve dijital para. Dijital para sadece Bitcoin değildir, bunun dışında birçok dijital para vardır, örneğin; Litecoin, Dogecoin, Ripple, NXT ve Peercoin gibi. Bitcoin bunlardan en çok bilineni ve kullanılanıdır. Her bir para cinsinin kendi protokolü ve blok zinciri olabilir. Bir protokol ile başka bir blok zinciri üzerinde çalışmakta mümkündür. Örneğin; Litecoin kendi protokolü ile kendi blok zinciri üzerinde çalışırken Counterparty'nin XCP isimli dijital parası Bitcoin'nin blok zinciri (Blockchain) üzerinde çalışabilir. İleride maliyeti düşürmek, standart ve verimi artırmak için bu tür işbirliği artacaktır, zayıf olanlar piyasadan çekilecek, güçlü olan ve teknolojisini yenileyenler piyasada kalacak ve zaman zaman piyasaya yenileri girecektir.

Blockchain 2.0[10] üzerinde "akıllı sözleşmeler" (smart contracts) kullanılabilir. Akıllı sözleşmeler, duruma göre bir sözleşme veya mutabakatın şartlarını yerine getirmek üzere programlanabilen protokollerdir. Akıllı sözleşmeler ödeme, taahhüde girme, bildirimde bulunma, mahsup işlemi yapmak, yeni bir işlemi başlatma, uyum kontrolleri yapmak, işlem kapatmak, rehin koyma, gizlilik kaydı oluşturma, doğrulama işlemi yapmak gibi finansal alanda yapılabilecek tüm işlemleri yapabilirler. Yapılması gereken tek şey ihtiyacı iyi belirlemek ve üzerinde buna uygun akıllı sözleşmeler oluşturmaktır. Akıllı sözleşme haline getirilen veya akıllı sözleşmeye bağlanan işlemler programlandığı şekilde sırasıyla bütün işlem adımlarını sırasıyla ve zamanında yapacaktır.

Bir akıllı sözleşme nasıl programlanırsa o şekilde iş yapar, hızı, maliyeti ve verimi buna göre değişir. Örneğin, bir akreditif işleminde yüklemeden en az 10 gün önce yükleme tarihinin hatırlatılması ve en uygun navlun fiyatı veren firmaların listelenmesi istenmişse yüklemeden en az 10 gün önce hatırlatma yapılacak ve en uygun fiyatı veren taşıma firmaları listelenecektir. Bir başka örnekte bir akreditif veya benzer bir işlemde ödeme vadesi belirlendikten sonra önceden anlaşılan bir fiyattan iskonto yapılması istenmişse ödeme vadesi belirlendikten sonra önceden mutabık kalınan fiyattan iskonto yapılacak, masraf ve tahsilatlar programlandığı gibi işleme alınacaktır. Akıllı sözleşmeleri birçok yerde kullanmak mümkündür, bir satım sözleşmesinden itibaren başlatılabileceği gibi bir işlemin belli bir aşamasında itibaren başlatmak ta mümkündür. Bir satım sözleşmesini akıllı sözleşme yapmak için bu sözleşmeye adım

[10] SWAN Melanie, Blockchain, Blueprint for a New Economy, Chapter 2, s. 9.

adım yapılması gerekenleri şartlı olarak vermemiz yani programlamamız gerekir ki akıllı sözleşme verilen plana göre zamanı geldiğinde programlanan işlemleri başlatabilsin ve yapabilsin. Örneğin; bir akreditifi açtırmak için teklif formunu bankaya gönderecek, akreditifi açtıracak, tahsil talimatı gönderecek, fiyat alacak, iskonto yaptıracak vs. bazı durumlarda bir olaya bağlı işlemler yaptırılabilecektir. Örneğin, firmanın hesabına bir paranın yatması veya firmaya bir Standby[11] gelmesi ile bir akreditifin açılması işleminin başlatılması gibi.

Bir diğer örnek, bir iddia ile ilgili olabilir. İki kişi hafta sonu oynanacak futbol maçları için kendi aralarında iddia'ya girebilirler. İddiayı kaybeden diğer tarafa ödeme yapacaksa bunun için "iddia" isimli bir akıllı sözleşme yapılabilir, böyle bir durumda hafta sonu maçları buna göre akıllı sözleşme tarafından takibe alınır, kesin sonucu resmi bir siteden tam olarak aldıktan sonra kaybedenin hesabından parayı alır ve kazanan tarafın hesabına yatırır.

Daha kapsamlı bir örnek verecek olursak; tarafların kendi aralarında vadeli bir BPO (Bank Payment Obligation)[12] ile ithalat/ihracat yapmaya karar verdiklerini varsayalım. BPO kâğıt belge gerektirmeyen banka güvenceli bir ödeme yöntemidir. Blockchain üzerinde akıllı sözleşmeler ile BPO işlemi yapmak için Blockchain üzerinde BPO isimli bir akıllı sözleşme (smart contract) programlanır. BPO isimli akıllı sözleşmeye yapılması gereken bütün işlem ve eylemler zaman bilgileriyle birlikte ayrıntılı olarak yazılır. Zamanı geldiğinde ve şartlar gerçekleştiğinde BPO isimli akıllı sözleşme çalışmaya başlar, sırasıyla kendisine verilen iş, işlem ve eylemleri yapar. Şöyle ki; işlem alıcı tarafında başlatılacaksa programlandığı üzere başvuru bilgilerini iç prosedürlere göre kontrol eder, eksikleri tamamladıktan sonra alıcının bankasına yani yükümlü bankaya (obligor bank) gönderir, banka, gelen başvuruyu işleme koyar, önce kredi limitlerini kontrol eder, uyum kontrollerini yapar, BPO met-

[11] Standby için bkz. ÖZALP Abdurrahman, UCP 600'ın Kullanılması ve Akreditif, İstanbul 2007.

[12] ÖZALP Abdurrahman, BPO'nun Kullanılması, İstanbul 2014, s. 19 vd.; ÖZALP Abdurrahman, Uluslararası Ticarette Banka Güvenceli Yeni Bir Ödeme Yöntemi: BPO, (2014)1 UTTDER, s. 247-258; EKŞİ Nuray, Milletlerarası Ticaret Hukuku, İstanbul 2015, s. 284-295; EKŞİ Nuray, Banka Ödeme Yükümlülüğüne İlişkin ICC URBPO 750E Kurallarının Hukuki Niteliği ve Bağlayıcılığı, II(2014)8 BFHD, s. 3-18.

nini oluşturur, TMA (Transaction Matching Application)[13] uygulamasına yükler, TMA, BPO bilgilerini satıcının bankasına gönderir, satıcının bankası satıcıya ihbar eder, satıcı BPO işlemine onay verir, böylece BPO işlemi kurulmuş olur. Satıcı daha sonra malı BPO şartlarına uygun olarak yükledikten sonra BPO'nun gerektirdiği data setlerini (yükleme bilgileri, fatura ve konşimento üzerindeki bilgiler vs.) bankasına sunar, bankası Blockchain üzerinde akıllı sözleşme yoluyla oluşturulan TMA'ya data setlerini yükler, TMA kendisine sunulan dataları daha önce kendisine yüklenen şartlar ile eşleştirmeye tabi tutar, datalar eşleşirse BPO duruma göre görüldüğünde veya vadede ödenebilir hale gelir. Bundan sonrası yine BPO isimli akıllı sözleşme tarafından kendisine verilen programa göre yürütülür. Verilen programda vadeli alacağın belli şartlarda iskonto edilmesi istenmişse o halde BPO isimli akıllı sözleşme vadeyi takibe alır ve diğer taraftan kalan müteakip işlemlere devam eder, yani iskonto yapılacaksa fiyat için belirlenen bankalar ve finans kurumlarından fiyat alır, gelen fiyatları programlanan limitlere göre karşılaştırır, en uygun fiyatı belirledikten sonra en uygun fiyatı veren tarafa işlemi yapması için talimat gönderir, iskonto yapıldıktan sonra gelen parayı yine verilen programa göre havale veya mahsup eder veya en yüksek faize yatırır. Bu ve buna benzer işlemleri ihtiyaca göre artırmak ve çeşitlendirmek mümkündür.

Görüldüğü gibi Blockchain üzerinde smart contract yani akıllı sözleşmeler yolu ile her işlemi programlamak ve yürütmek mümkündür. Akıllı sözleşmelerin geliştirilmesi ve kullanılmaya başlanması Blockchain'e hayat vermiştir. Blockchain'nin başta finans dünyası olmak üzere birçok alana girmesi bakımından önemli bir aşamadır. Geliştirme çalışmaları her geçen gün artarak devam etmektedir. IBM ve Microsoft gibi teknoloji devleri bu çalışmalar için ortam sağlamakta ve kendileri de çalışmalarını devam ettirmektedirler. Özellikle başta bankalar olmak üzere finansman şirketlerinin şimdiden bu tür altyapıları ve geliştirme ortamlarını kurmalarında veya satın almalarında fayda vardır, yoksa geride kalırlar, çünkü bu yeni teknoloji çok hızlı gelmektedir. Mevcut web teknolojisine göre daha hızlı, ucuz ve güvenli olduğu için bu teknolojinin yerini alacak gibi gözükmektedir.

[13] BPO işlemlerinde data setlerini karşılaştırmaya yarayan bir uygulamadır.

Blockchain 3.0[14], Blockchain teknolojisi sadece para ve parasal işlemler dışında hayatın pek çok alanı ile ilgili olabilir. İnsan hayatındaki pek çok faaliyet Blockchain teknolojisi ile kolaylık sağlayabilir, kontrol ve koordinasyon altına alınabilir. Başta e-devlet ve noter işleri olmak üzere pek çok hukuki işler, taşınır taşınmaz kıymetlerin işleri, satış, devir, doğrulama, izleme, kontrol, filtreleme ve uyum işleri Blockchain teknolojisi ile kolaylıkla, hızlı ve güvenli bir şekilde yapılabilir. Böylece Blockchain içsel ve dışsal, nicel ve niteliksel faydaların entegrasyonunu sağlayan bütünsel bir çözüm sunmuş olur.

Blockchain 3.0 ile yapılabilecek bazı işler şunlardır:

–Aktiviteler organize edilebilir.

–Tüm insan ve makine aktiviteleri koordine edilebilir.

–Bazı aktiviteler kontrol altına alınabilir. Örneğin, sansür, Blockchain teorik olarak küresel bir açık hesap defteri olduğu için herhangi bir kimsenin herhangi bir zamanda Blockchain üzerindeki herhangi bir bilgiyi bulabileceği ve kontrol edebileceği unutulmamalıdır. Bu yönüyle Blockchain aynı zamanda küresel bir kontrol sistemidir.

–Ülkeler tarafından kontrol edilemeyen dağınık DNS (domain name system-domain isim sistemi) kullanılabilir, böylece internet üzerinde yapılan yayınlar hiçbir şekilde sansür edilemez ve baskıya maruz kalmaz. Örneğin, bit uzantılı domainler dağınık yapı üzerinde kontrol dışıdır, oysa *com, org, info, gov* gibi uzantılar merkezi olup üst seviyede kontrol edilebilirler. Son zamanlar da *bit* uzantılı adreslerde teknik bazı açıklar nedeniyle *P2P* uzantısı geliştirilmiş ve dağıtık yapıda dijital bir kimlik tanıma sistemi (KeyID) ile birlikte güvenli mesajlaşma ve doğrulama hizmeti verilebilmektedir.

–Etkili ve güvenli dijital kimlik doğrulama sistemleri geliştirilebilir/kullanılabilir. Örneğin, *OneName, BitID, Bithandle gibi.*

–Fikri mülkiyet hakları, tapu ve diğer sahipliklerin saklanmasında ve korunmasında kullanılabilir.

–Hashing ve Timestamping işleri için kullanılabilir. Bu iki özellik zaten Blockchain ile çalışmanın ana fonksiyonlarıdır. Hashing, bilgisayar uygulamasında hesaba dayalı adresleme şeklinde tarif edilebilecek bir terim olarak Blockchain uygulamasında bir dosya üzerinde bir algo-

[14] SWAN, Blockchain, Blueprint for a New Economy, Chapter 3 and 4.

ritmanın çalıştırılması ve geri dönülmez veya geriye doğru değiştirilemez biçimde şifrelenmesi anlamındadır. İçerisinde yazılı, görsel, video, resim, fotoğraf vs. olan her dosya Hashing işlemine tabi tutulabilir. Hashing işlemi ile dosya sayı ve rakamlardan oluşan 64 karakterli bir dizi haline getirilir. Yani bu 64 haneli dosya orijinal dosyanın içeriğini bir dizi karakter halinde saklar. Söz konusu dosyayı kullanmak isteyen veya teyidini almak isteyen kişinin o dosya üzerinde aynı hash algoritmasını çalıştırması ve doğrulama teyidi alması gerekir, bunun içinde anahtarının olması gerekir. Anahtarla doğrulama algoritması çalışacağından dolayı bir kopyasının dahi değiştiğinin tespit edilmesi halinde bilgi alınamayacaktır, zaten blok zincirine de eklenemeyecektir. Söz konusu dosya veya işlemin doğrulanması için o işlem veya dosyanın dağıtıldığı tüm bilgisayarlardan doğrulanması ve hiç biri tarafından reddedilmemiş olması gerekir. Timestamping, Blockchain'e konulan kodlanmış dizinin aynı zamanda tarihlenmesi yani tarih ve saat içermesidir.

Blockchain'nin Hashing-plus-timestamping özelliğiyle tasdik ve doğrulama hizmeti verebilmesi ve bu yöntemle çalışabilmesi Blockchain'nin en önemli özelliğidir denilebilir, zira güvenlik her şeyden önemlidir. Bu özellik sayesinde kıymet, değer, belge ve bilgilere ilişkin tüm hizmetler (dosyalama, saklama, kayıt, noterlik hizmetleri ve fikri hakları koruma şeklinde) verilebilir. Bu fonksiyonlar Blockchain' nin kriptolu dizileri (cryptographic hashes) kullanarak sonsuza kadar değişmeyecek biçimde belgeleri sürekli ve sınırlı veya herkese açık olarak kayıt altına alabilmesine ve bilgileri saklamasına imkân verir. Blockchain de saklanan bu bilgilere gerektiği zaman ulaşılabilir, bunun içinde bu amaç için yazılmış uygun yazılım ve programları kullanmak yeterlidir. Yine özetlemek gerekirse Blockchain herkese açık, dağıtık yapıda çalışan küresel elektronik bir hesap defteridir. Burada işin can damarı herkese açık dağıtık küresel bir hesap defterine dijital bilgilerin şifrelenerek silinemeyecek ve değiştirilmeyecek şekilde girilmesi daha sonra gerektiğinde doğrulanarak işleme alınabilmesidir (özel Blockchain'ler hariç, burada aynı durum izin verilen kişiler için geçerlidir). Bu konuda hizmet veren bazı kurumlar şunlardır: Proof of Existance, Virtual Notary, Bitnotar, Pavilion.io.

Bunlardan birini biraz açmak gerekirse, örneğin, Proof of Existance şu şekilde çalışmaktadır: insanların yaptıkları işleri veya belgelerin içeriğini kriptolu bir metin dizisi haline getirerek yani hashing işlemine tabi tutarak geri dönülmez ve değiştirilemez bir biçimde bir Blockc-

hain'e yerleştirir. Daha sonra bu iş, belge veya bilgilere ihtiyaç duyan kişilerin söz konusu iş, işlem veya bilgilere ulaşabilmesi için o işlemlere özel anahtar (private key) verilir, ihtiyacı olan ve özel anahtara sahip kişi özel anahtar bilgisi ile sisteme erişim sağlayarak teyidini alabilir. Bir dokuman veya bilginin içeriği metin dizisi haline getirilip bir Blockchain'e konulurken o işlem bir işlem bloku işareti alır, işlemde daha sonra aynı dokuman veya bilgi aynı orijinal haliyle teyit veya doğrulama amacıyla girilirse yine bir işlem bloku işareti üretilir, sonuçta içerik bilgileri ve işlem bloku işareti eşleşirse teyit veya doğrulama yapılır, aksi halde yapılmaz. Böyle bir yöntemle Blockchain'e yerleştirilen belgelerin veya dijital değerlerin varlığının ve içeriğinin tarihleriyle birlikte kanıtlanması mümkündür. Avukatlar, müşteriler, bankacılar, yöneticiler, kamu idareleri ve ihtiyaç duyan herkes Blockchain'nin bu özelliğini kullanarak teyit ve doğrulama ihtiyaçlarını karşılayabilirler, örneğin, mahkemeye sunulacak bir belgenin ilk hali veya belli bir tarihteki bilgileri ihtiva ettiği dönemdeki halini veya bir diploma, senet, poliçe, sağlık belgesi gibi belgelerin varlığını kanıtlamak için kullanılabilir. Bir fikri veya buluşu olan bir sanatçı veya bilim adamı fikir veya buluşunu Blockchain'e koyabilir, daha sonra gerektiğinde kendisine ait olduğunu kanıtlayabilir.

Bunlardan bazıları sertifika üretebilmektedir, teyit ve doğrulama almak isteyen kişi ücreti karşılığında bu sertifikaların teyit ve doğruluğunu Blockchain'den alabilirler. Bazıları sadece imzalama hizmeti vermektedir, örneğin, DocuSign. Bazıları eser ve mal mülk sahipliği teyidi verebilmektedir, örneğin, Ascribe, Monegraf.

Devletin Blockchain'i tam kapasite ile kullanması halinde e-devlet uygulamaları ile memurların büyük çoğunluğuna ihtiyaç olmayacaktır. Blockchain'nin yönetim işlerinde kullanılması ile organizasyon, koordinasyon ve bütün personel işlerinde devlet, özel sektör ve iş dünyası büyük verimlilik elde edilebilecektir.

Resmi belgelerin Blockchain'e gömülmesi halinde süreli/süresiz olarak kullanıma hazır olacaktır, isteyen kişiler bu konudaki uygulamalarla bu belgelere ulaşabilecek, gerekli teyitleri alabilecek işlemlerinde kullanabilecektir. Sonuçta sürekli, aranabilir ve değiştirilemez global çaplı bir kayıt deposu söz konusu olacaktır. Son yıllarda Blockchain üzerinde yapılan bir evlilik bu konunun gerçek hayattan uzak olmadığını ve geleceğe ne tür potansiyel taşıdığı konusunda önemlidir. Bu örnekte evlilik dosyası Blockcahain'e gönderiliyor, değiştirilemez biçimde kayde-

diliyor, daha sonraki tüm olaylar (çocuk doğumu, yıldönümü, boşanma vs.) bu kütüğe ekleniyor.

B. Blockchain'in Kullanılabileceği Alanlar

Blockchain ile yapılacak işlemlerin sayısı bir hayli fazladır. Ancak bu işlemlerin Blockchain ile yapılacağı ülkelerin ulusal mevzuatlarında Blockchain ile işlem yapılmasını engelleyen hükümler olabilir. Bu nedenle aşağıda Blockchain ile yapılabilecek işlemler sıralanırken başta banka mevzuatı, ceza mevzuatı, gümrük mevzuatı, tapu mevzuatı ve ihale mevzuatı olmak üzere ulusal mevzuat hükümleriyle getirilen sınırlama ve yasaklamaları da dikkate almak gerekir. Mevcut yapısı itibariyle tüm Blockchain'ler ile yapılabilecek işler özetle şunlardır:

- Cüzdan hesap işlemleri
- Dijital para transferleri (Bitcoin, Litcoin, Ether vs.)
- Dijital kimlik işleri
- Ülke paraları transferleri, ödeme işleri
- Kayıt işlemleri
- Saklama işlemleri
- Dijital dosya işlemleri (kitap, fotoğraf, logo, şarkı, eser, patent)
- Akıllı sözleşme işlemleri
- Kimlik doğrulama işlemleri
- Belge, kıymet, menşe, işlem doğrulama işleri
- Şifreleme işlemleri
- Rehin işlemleri
- Menkul ve gayrı menkul (taşınmaz) işlemleri
- Her türlü belge işlemleri (fatura, konşimento, sertifikalar ve diğer)
- E-devlet işlemleri
- Yönetim işleri
- Noter işleri
- Evlenme/boşanma işleri
- Oylama işleri
- Uyum işleri (müşteri tanıma-know your customer-KYC)
- Devir ve temlik işleri
- Takip işleri
- Kayıt işleri (kamu, sağlık, trafik vs.)

– İhale işlemleri
– Tevsik işleri
– Karşılıklı işlemler
– Denetleme işleri
– İnsan kaynakları işleri
– Referans işleri
– Tedarik zinciri işleri
– İthalat ihracat işlemleri
– Finansman işlemleri (kredi bulma, kullandırma, iskonto)
– Sermaye ihtiyacı karşılama işlemleri, kitle fonlama (crowdfunding)
– Bağış toplama ve yönetimi işleri
– Sendikasyon işleri
– Sigorta takip ve tazminat işleri
– Telif, tapu kayıt ve kopya ürün koruması işlemleri
– Askeri emir komuta işleri.

Ancak bu işlemler zamanla daha da artırılabilir.

V. Blockchain'in Faydaları

Blockchain'in avantaj ve faydaları şu şekilde sıralanabilir:

– Güvenlidir
– Hızlıdır
– Durmadan hizmet verir
– Bozulmaz
– Kaybolmaz
– Erişim sorunu olmaz
– Bir merkeze bağlı değildir
– Her bilgiyi kaynağında doğrular
– Belgeleri kaynağında doğrular
– Her bilgiyi değişmeden kalmak üzer saklar
– İhtiyaç halinde doğrulama yapar
– Şeffaflık sağlar
– Denetime izin verir
– Sahteciliği engeller
– Mükerrerliğe izin vermez

– Sözleşmelerin programlar
– Programlanan sözleşmeleri çalıştırır
– Programlanmış işlemleri yapar
– Siber saldırılara karşı dirençlidir.

Sonuç

Blockchain başta finans olmak üzere birçok alanı etkileyebilecek yeni bir teknolojidir. Mevcut teknolojilere göre hız, emniyet, maliyet, siber saldırılara karşı koymak gibi pozitif özellikleri vardır. Her sektöre veya işe uygun olmayabilir, ancak uygun olabildiği alanlarda zaman kaybetmeden uygulama imkânları profesyonel kurum veya kişilerden hizmet alarak araştırılmalı, altyapılar hazırlanmalı, işlemler akıllı sözleşmeler ile programlanarak çalıştırılmalıdır. İş veya işlemlerin tamamen uygun olmadığı yerlerde karma biçimde (hybrid) uygulama da yapılabilir, yani bir kısmı blockchain diğeri mevcut teknoloji olabilir. Blockchain teknolojisi kendinden önceki teknolojilerin yerini hızlı bir şekilde alan bir teknoloji (disruptive) olduğu için öncü finans ve teknoloji kurumları bunu görerek bu teknoloji ile işbirliği yapmak ve kendileri için kullanmak eğilimine girmişler. Bu amaçla konsorsiyumlar kurmuşlardır. "R3 Consortium" bunlardan biridir. Bu konsorsiyuma 42 banka dahildir. Finans ve banka sektörleri tarafından Blockshian'e yapılan yatırımlar, gelecekte blockchain'i diğer alanlarda da cazip kılacaktır.

Yararlanılan Kaynaklar

ÇARKACIOĞLU Abdurrahman Kripto-Para Bitcoin, Araştırma Raporu, Aralık 2016, Sermaye Piyasası Kurulu, Araştırma Dairesi.

EKŞİ Nuray, Milletlerarası Ticaret Hukuku, İstanbul 2015.

EKŞİ Nuray, Banka Ödeme Yükümlülüğüne İlişkin ICC URBPO 750E Kurallarının Hukuki Niteliği ve Bağlayıcılığı, II(2014)8 BFHD.

FLYNT Oscar, Smart Contracts, 2016.

IBM Financial Market Service, Making Blockchain Real for Banking, 16 February 2017.

RAMSEY Seth, Quick Start Guide to Undertsanding Blockchain, 2016.

NAKAMOTO Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System: www.bitcoin.org (2.1.2018).

ÖZALP Abdurrahman, Akreditif ve Uygulama Yeni ISBP'ye Göre, İstanbul 2015.

ÖZALP Abdurrahman, UCP 600'ın Kullanılması ve Akreditif, İstanbul 2007.

ÖZALP Abdurrahman, BPO'nun Kullanılması, İstanbul 2014.

ÖZALP Abdurrahman, Uluslararası Ticarette Banka Güvenceli Yeni Bir Ödeme Yöntemi: BPO, (2014)1 UTTDER, s. 247-258.

USTA Ahmet/DOĞANTEKİN Serkan, Blockchain 101, Kapital Medya Hizmetleri A.Ş., 2017.

World Economic Forum, the Future of Financial Infrastructure.

The Future of Retail Financial Services © Cognizant, © Marketforce Business Media Ltd, © Pegasystems Inc, January 2016, Research devised and conducted by Marketforce.

The future of financial infrastructure, World Economic Forum, 2016.

The Fintech 2.0 Paper: Rebooting financial services, www.anthemis.com, www.santanderinnoventures.com, www.oliverwyman.com (6.1.2018).

SWAN Melanie Blockchain, Blueprint for a New Economy, O'Reilly Media, Inc. 2015.

Satış : Türkmen Kitabevi, Sahaflar Çarşısı No: 19 Beyazıt/İstanbul, Tel: 0 212 512 27 17 www.turkmenkitabevi.com.tr

Faydalı dokumanlar : www.abdurrahmanozalp.com veya www.ucp600.info