"Blokzincir (Blockchain)'in Kamu İdaresine Olası Etkileri Üzerine"

Article *in* Amme Idaresi Dergisi · December 2019

CITATIONS
22

READS
1,731

1 author:

Nur Şat
Hitit University
32 PUBLICATIONS **72** CITATIONS

SEE PROFILE

Blokzincir (Blockchain)'in Kamu İdaresine Olası Etkileri Üzerine

*Nur ŞAT**

Öz: *Kamu yönetimi, kendi dışındaki yapıların kullandıkları veri protokolü Blokzincir mimarisine uyum sağlamalıdır. Bu uyumla birlikte Blokzincir, demokratik uzlaşmayı gözetmek şartıyla kamu yönetiminin kuralları uygulatma sürecini açık ve meşru kılabilecektir. Kamu yönetimi Blokzincir teknolojisinin hizmet süreçlerine nasıl dahil edebileceğine hızlıca odaklanmalıdır. Devletin daha etkin işleyişi amacına yönelik olarak, bu uyum süreciyse yalnızca nitelikli, iyi hazırlanmış bir kamu teşkilatıyla inşa edilebilecektir. Bu açıdan teşkilatlar yeni vizyonlarla kendilerini geliştirmeli, kamusal değer üretecek kamu yönetici ve memurları yetiştirmelidirler. Makale bu sava Blokzincirin nitelikleri, işleyişi, farklılıkları, avantajları, dezavantajları, akıllı sözleşmeleri, özel sektörde ve kamu idaresindeki kullanımının literatür araştırmasıyla birlikte Dünya örneklerini de değerlendirerek varmaktadır.*

Anahtar Kelimeler: *Blokzincir, kamu yönetimi, kamu hizmeti, bürokrasi, veri*

Blockchain's Potential Impact on Public Administration

Abstract: *Public administration should adjust to the architecture of the Blockchain data convention, in which non governmental collective structures practice. With this adjustment, Blockchain would be able to render the process of enforcing the rules of public administration open and legitimate, provided that it observes democratic consensus. Public administration should focus swiftly on how to incorporate the Blockchain technology into service processes. The overall goal being to make government more efficient, this adaptation process need to be addressed with only a competent and well-prepared public structure. In this respect, organizations should equip themselves with new visions; they should train and educate public administrators and civil servants who will create public value. The article approaches to this argument by evaluating the quality, functioning, dissimilarities, advantages, disadvantages, smart contracts, and usage of the Blockchain in the private sector and public administration both literatür works and World wide cases.*

Keywords*: Blockchain, public administration, public service, bureaucracy, data*

* Dr. Öğr. Üyesi, Hitit Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü.

Makale gönderim tarihi: 02.09.2019
Makale kabul tarihi: 03.12.2019

Amme İdaresi Dergisi, Cilt 52, Sayı 4, Aralık 2019, s. 117-147

Giriş

Modern insanın yazı merkezli uygarlığında hayat; hukuk, haberleşme, para, hisse senedi, sanatsal-akademik fikri mülkiyet hakları, tarım, ithalat-ihracat, gibi konularda devlet, banka, sosyal medya ağları, kredi kartları, sigorta firmaları, noterlikler, akreditasyon şirketleri, para transfer operatörleri, insan kaynakları şirketlerini vb. gerekli, kaçınılmaz ve vazgeçilmez kılmaktadır. Veri görünürlük kazanmış, daha hızlı ulaşılabilir, değiş-tokuş edilebilir olmuştur. Bu değişimde taraflara doğru işlem için referans sağlama işlevini de artık kurumsallaşmış olan aracılar yürütür. Aracılık, iktisadi ve sosyal sistemde karşı tarafa güvenerek kayıt tutma ve işlem yapabilmenin genel geçer yolu olmuştur. Kayıtlarda karışıklık, hata, kötü niyetli kullanım, dolandırıcılık, haksız kazancın önüne aracılık düzeniyle gelişmekte, ancak o da sorunlar çıkarmaktadır: Hayatta her şey bir seferliğine tek bir zaman, mekân ve kişi ile yapılır. Sehven yapılan işlemin düzeltilmesi ikinci bir işlemle yeni bir zaman, mekân ve kişi ile mümkün olur. Kayıtlar değiştirilerek birbirinin yerine de gösterilebilmektedir. Ayrıca, aracılık sistemini kullanmaya, ulaşmaya gücü olmayanlar, küresel ekonominin dışında bırakılmaktadır. Bu kesimler merkezin etki alanı dışında kaldıkça seçenekleri azalmakta, işleri yavaşlamakta, zorlaşmakta, mali yükleri artmaktadır.

İnsanoğlu yakın çevresi dışında güven duygusuyla hareket edemeyeceğinden devletin aracılığına iki anlamda muhtaçtır: vatandaşla vatandaş arasındaki ve kamu hizmeti sunumunda devletle vatandaş arasındaki işlemlerde kamu teşkilatı kayıtları esas alınmaktadır, çünkü devlet en rağbet gören garantördür. Bir başka deyişle en geniş çaplı aracılık faaliyetini kamu bürokrasisi yapmaktadır. Devlet bu güveni bürokratik işleyişiyle sağlamaktadır. Bürokrasi, verinin işlenmesine, dağıtımına ve yeniden üretilmesine adanmıştır. Bürokrasi modeliyse merkezileşmiş dikey hiyerarşiye dayalı otoritedir. Temel örgüt modeli haline gelmiş, şu ana kadar bir alternatifi bulunmamıştır. Ancak 'vazgeçilmez' olsa da sıkça eleştirilmektedir. Eleştirinin temel sebebiyse suistimale açık boşluklardır: işleyiş, yetkililerin istedikleri şekilde yönlendirebilecekleri arka kapılara sahiptir.

Blokzincir Teknolojisi 'hantal, gizli, yolsuzluklara açık' olarak algılanan geleneksel bürokrasi mekanizmasına ciddi bir alternatif olma potansiyeline sahiptir. Gerçek zamanın ve eylemliliğin akışı tekrar edilemez, hiçbir eylem bir ikincisiyle yok edilemez; ilk ve aslî zaman, eylem, işlem yerine geçemez. Düzeltilen şey 'düzeltilmiş' olarak kalacaktır. Bir özne bir işlemi sadece bir seferliğine, geri dönülemez ve inkâr edilemez şekilde yapmaktadır. Büyük bir yenilik olarak gerçeği takip etmek, gerçek akışı manipüle etmeden normal olanı yakalamak, mümkün hale gelmektedir. Bilgi teknolojisinin hızlanan evrimi, yönetişim için de yepyeni bir alan açmaktadır. Yeni çevrimiçi araçlar ortaya çıktıkça, yönetişim

yenilikçi yöntemlerle kullanılmaya başlanmaktadır (Bruns, 2008; Malone, 2004; Tapscott ve Williams, 2006).

Müesses Nizamın Dört Sorunu

Güven Sağlayamama

Teknolojik imkânlar veri üretmeyi, saklamayı, aktarmayı, sonradan düzenlemeyi kolaylaşmıştır. Böylece sehven yapılacak bir işlemin telafisi kolayca sağlanabilmektedir. Ancak, temelinde 'insana güven' olan bu işleyişin kötü niyetlilere haksız çıkar sağlaması da mümkündür. Hiç var olmayan bir işlemin gerçekmiş gibi gösterilmesini veya var olan bir işlemin de gerçekliğinin inkârını engelleyebilecek herhangi bir özellik bulunmamaktadır. Elbette bir ağ modelinde hareket eden toplumda bunu önleyecek bir mutabakatın sağlanması kolay değildir. Mutabakatın önünde uzlaşmazlıklar, ihanet sorunları söz konusu olabilir. Bu zafiyet 'Bizans Generalleri Sorunu' olarak bilinir. Sadece 'insana güvenmeye' dayandırıldığında ağ tipi ilişkilerin her zaman suistimale açık olduğunu, sadakatsizliği engellemeyeceğini açıklayan bir canlandırmadır. Ağ iletişimindeki zıtlık hakkındaki bu sorunu önce Akkoyunlu, Ekanadham ve Hubert (1975) makalelerinde tarif etmişler, daha sonra da Lamport, Shostak ve Pease (1982) makalelerinde 'Bizans Generalleri Sorunu' adıyla ele almışlardır.

Aracıların Ekonominin Merkezinde Yoğunlaşmaları

Çağın iktisadi yapısı merkezi niteliklidir. Temelde hepsi birer para aktarımı işlemi olarak alışveriş, telif hakkı dağıtımı, havale, tasarruf, yatırım vb. işlemlerin her biri merkezi haldeki farklı sistemlerce işlenmektedir. Aracılık sistemi kendini farklılaştırma üzerinden güçlendirmektedir. Tüm işlem koşul ve süreçleri aracıların sağladığı güvenle sınırlıdır. Aracıların ağları ne kadar yaygın olursa olsun iç işleyişleri kendi merkezlerine bağlanmaktadır. Merkezileşmenin sinerjisini kullanabilmek için farklı sektörlerin merkezdeki yapıları da birbirleriyle derin bağlar içinde bulunmaktadır. Bu da ekonominin katı bir çekirdek oluşturmasına ve kötü amaçlı saldırılara açık hale gelmesine neden olmaktadır. Çünkü merkezi yapıların karşılaşacağı zarar riski yaygın (dağıtık) yapılara göre daha yüksektir. Özellikle bilişim dünyasında bu merkeze ulaşıldığında bir saldırıyla bile ciddi hasarlarla yüzleşme ihtimali yüksektir. Bu hasarlar da verinin yetkisiz kişilerin eline geçmesi, mahremiyetin ihlâli anlamına gelmektedir.

Görüldüğü gibi merkezi yapı farklı kurallarla katı olmasının yanında karmaşıktır ve bu nitelikler hizmet alanların aleyhine işlemektedir.

Aracılık Sistemindeki Kişisel Veri Güvenliği

İktisadi yapı genel olarak aracılık üzerine kuruludur. Aracı olmadıkça sosyal ve iktisadî faaliyetleri yapmanın imkânsız olacağı varsayılmaktadır. Aracılar, tarafların kimliklerini saptamak, kayıtları tutmak, anlaşmazlık ve yanlışlıkları gidermek gibi işlemleri yürütmektedirler. Güven temin edecek farklı bir model düşünülemez olmuştur.

Bu model içinde pek çok veri el değiştirmektedir. Mâlûmdur ki, elektronik ortamda yapılan her işlem bir iz bırakır. Büyük bir veri havuzu sistemin bir çıktısı olarak doğmuştur. İlgili kurum ve kuruluşlar dışında, anlaşmalı üçüncü taraflar da kişisel veriye ulaşabilmektedir. Bu halkalar da giderek genişlemektedir. Hiç işlem yapılmamış bir şirkete veya kuruluşa veri akmaya başlamaktadır. Üstelik bu veri, kişilerin bir şirket veya kuruma verdikleri şekliyle de korunmamaktadır. Veri, sahibinin daha önce onay vermediği hatta tahayyül bile etmediği şekilde farklı birleşimlerle farklı bir alanda, farklı bir amaç için bir araya getirilebilmektedir. Islak İmza taklidinden bir farkı olmayan bu veri birleştirmesi bireylerin dijital izlerini tekrarlayarak gerçekte yapılmamış işlemleri veri sahibinin bilgisi olmadan yapılmış gibi gösteren, gerçek kişilerin dijital âlemdeki gerçekliğine münhasır varlıkları kopyalayan bir 'dijital gölge' elde edilebilmektedir. Gözlemlenmektedir ki izinsiz olarak farklı amaçlarla paylaşılan veri, bireylerin paylaşım amacıyla şirket veya kurumların kullanım amaçları arasındaki orantısızlık nedeniyle şirket veya kurumlara asimetrik avantajlar sağlamakta, veri güvenliği sözleşmelerine rağmen demokratik toplumun temeli olan veri mahremiyeti sıkça ihlâl edilmektedir.

Aracılıktaki Yüksek Kâr Oranları

Aracı kurumlara başvuran kişiler için ödedikleri aracılık kârı ciddi bir yüktür. Bunlara iyi bir örnek yurtdışındaki bir alıcıya para gönderimlerinde gözlemlenmektedir. Banka yoluyla veya para transfer operatörleri aracılığıyla havale göndermek pahalı olduğu kadar yavaş da olabilmektedir. Çünkü (Safahi, 2018: 4):

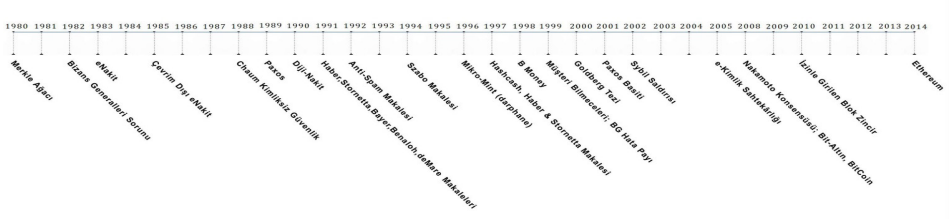
- Aracılık işlemi için işlem tutarının ortalama %8'i kârdır,
- Transfer işlemleri genellikle [gönderici veya alıcıların veri mahremiyeti açısından] şeffaflık olmadan 24 ilâ 72 saat sürmektedir,
- İlgili bankalardaki uyumsuz sistemler uzlaşmayı zorlaştırmaktadır,
- [Transfer sahiplerini önceden bilgilendirmeksizin] gönderici veya alıcı operatörler ek veya yepyeni teminat talep edebilmekte, beklenmeyen masraflara sebep olabilmektedirler.

Merkezi Yapıdaki Aracılık Sistemlerine Bir Alternatifin Doğuşu: Blokzincir

Aracılık sistemlerinin baskın varlığı olmaksızın gerek gerçek gerek sanal varlıklar aynı hız ve kolaylıkta yönetilemez mi, sorusuna bir cevap bulma arayışı 20 yıl kadar geriye dayanmaktadır. Pek çok bilimsel eserin teorileriyle uygulamayı tuğla tuğla ördükleri anlaşılmaktadır. Blokzincir bu arayışın ürünüdür. Blokzincirin amacı dijital verinin kaydedilirken, dağıtılırken sonradan düzenlenmemesini, değiştirilememesini sağlamaktır. Blokzincir belirli bir zaman aralığında tamamlanmış işlemleri kronolojik olarak kaydeden bir 'veri blokları zinciri' olarak tarif edilir. Bir blok, madenciler tarafından bir kez doğrulandığında bir daha değiştirilemez. Çünkü değiştirilmemesi için tüm hareketler herkese veya sadece ilgililerine açık olan ve paylaşılan bir kayıt veri tabanının kullanıcıları tarafından kolayca takip edilmektedir. Üstelik karmaşık iş şartnamelerini kodlanarak değişen şartlara uyarlayan akıllı sözleşmeler yapısını da kullanıma açmaktadır.

Blokzincir, Bitcoin platformuyla adını duyurmuşsa da farklı platformlarda (Ethereum, Hyperledger, Ripple, Tendermint, Corda, vb.) uygulamaları gösterilebilir. Her platform kendine özgü niteliklerine göre birbirinden ayrılmakta, amaçlarına göre şekillenmektedirler. Bu çalışmada Blokzincir platformların farklılıkları üzerinden değil, genel nitelikleriyle aktarılacaktır.

Blok zincir teknolojisini kullanarak Bitcoin'in çıkışını hazırlayan teoriler Çizelge 1'de incelenebilir.



Kaynak: *Narayanan ve Clark, 2017: 3'ten çevrilmiş, uyarlanmıştır.*

Yukarıdaki çizelgede özetlenen gelişmelerin ışığında 2008'de yazılan makalede Satoshi Nakamoto, şifrelenmiş (kripto) bir dijital nakit protokolü önermekteydi: Eşten Eşe bir ağ, zaman damgalarını karma iş kanıtı zincirine sokarak işlemleri gerçekleştirir ve iş kanıtını yinelemeden değiştirilemeyecek bir kayıt oluşturur (Nakamoto, 2008: 1). İşlemler Blokzincir üzerinde kısa zamanda doğrulanmakta, onaylanmaktadır. İşlemin doğruluğu için gereken iş kanıtı topluluk tarafından sağlanmaktadır. Bu işi yapan madenciler de ellerindeki işlemcilerin gücüne göre mecbur oldukları zaman sınırı içinde en hızlı

doğrulamayı yaparak çalışmaları, masrafları karşılığı kazandıkları parayla güdülenmektedirler.

'Nakamoto Konsensüsü', Blokzincirin gerçek hayatta uygulanabileceğini Bitcoin ile göstermektedir. İlginçtir, Nakamoto makalesinde hiç 'Blokzincir ifadesini kullanmamış veya onu açıklamamıştır. Ancak elektronik para sistemi 'Üçüncü bir tarafa güvenmeye gerek olmadan tamamen eşler arası bir sistem' şeklinde tanıtılıp doğal olarak Blokzincir tarifini yapmıştır.

Zaman ve mekândan bağımsız yapılan işlemler standartlaşmış örneğin e-devlet üzerinden resmi başvuru yapmak normalleşmiştir. 'Nakamoto Konsensü' ile bir boyut daha eklemektedir: İki muhatabın üçüncü bir tarafın güvence vermesi gerekmeden karşılıklı, birebir işlem yapabilmesi… Bu fikir, kayıp -kazancın riske atılamayacağı para konusunda sınanmaktadır. Giderek büyüyen bir kesim bu para birimiyle ilgilenmektedir. Kişiler birden fazla cüzdan sahibi olabildiklerinden kullanıcılarla cüzdanları, hesapları eşleştirmek henüz tam olarak mümkün olmamakta, işlem hacmine veya kullanıcı sayısına kesin olarak ulaşılamamaktadır. 40 milyon adetten fazla cüzdanın/hesabın olduğu ve 200 milyar ABD doları tutarında işlem yapıldığı ve Bitcoin için kullanılan adres sayısı Temmuz 2019'da 486.890'dır (Blockchain.com, 2019). Teklif, ekonomideki güveni artık aracı kurumlarla değil; ilgililerin sayısına göre genişleyen bir topluluğun fikir birliğiyle gerçekleştirilebileceğidir.

Bu şifrelenmiş dijital nakit protokolü, insanların üçüncü bir tarafa, yani aracılara gerek olmadan kendi aralarında güvenli işlem yapılabileceği iddiasındadır. Bu iddia insana güvenden 'bilgi işlem (işlemci) hesaplamalarına' güvene geçişi temsil eder (Antonopoulos, 2014: 1). Bitcoin'in varlığını sağlayan teknolojik alt yapı da Blokzincirdir.

Blokzincir Teknolojisi

Blokzincirin Nitelikleri ve Teknolojisi

Sony'nin, ses kalitesi çok iyi olan transistörlü radyodan kalitesi düşük, taşınabilir radyo üretimine geçmesini; IBM'nin piyasadaki baskınlığına rağmen Macintosh kişisel bilgisayarı üreten Apple'ı örnek gösteren Bower ve Christensen yalnızca küçük, yükselen piyasalara hitap eden ve başlangıçta müşteriler tarafından değer verilmeyen özelliklerinin sonradan keşfedilmesiyle pazarı işgal eden teknolojileri 'yıkıcı' olarak nitelendirmişlerdir (1995: 46). Bu yönden Blokzincir de yıkıcı bir teknolojidir: Var olan teknolojinin yerine yenisini koymakla kalmamakta; üretim ve tüketimde süregelen düşünme sistematiğini değiştirmektedir. Konuyla yeni tanışanların teknik olarak olasılıkları anlasalar da merkezi olmayan bir yapıyı veya geri dönüşü olmayan işlemleri pratiğe dökmekte zorlanmaları böyle açıklanabilir.

Blokzincir siber uzamda bir elektronik veri transferi olanağıdır. Blokzincir, kayıtların zincirleme olarak tutulduğu bir yapıdadır. İşlemlerin aralıksız takibini sağlamaktadır. İşlemler şifreli kimliklerle anonim şekilde yapılır, sonradan değiştirilemez bir ağ üzerine kaydedilir (Güven ve Şahinöz 2018:44). Mutabakat denilen üzerinde uzlaşılmış kural kitabı ilgililerce oluşturulur, değiştirilir, kaldırılır. Başka bir kural düzenine geçmek isteyen gruplar yeni kurallarla şekillenen çatallaşma' (*forking*) olarak adlandırılan bir zincir düzenine geçilebilir. Bu transfer yönteminde güvence için aracı gerekmez; işlem hızla yapılabildiği gibi, akışın tüm işlem ve ilgilileri (Bazen herkes, bazen sadece belli şartları taşıyanlar) gerektiğinde denetlenmek üzere takip edilebilecektir.

Blokzincirin birçok tipi vardır:

1. Açık Blokzincirde, herhangi bir (merkezî) kuruluş tarafından önceden onaylanmak zorunda kalmadan bir kişi ağa istediği zaman katılabilir veya ayrılabilir. Ağa katılmak, defteri işlemek için, ilgili yazılımın olduğu bir bilgisayar yeterlidir. Ağ ve yazılımın merkezî bir sahibi yoktur. Defterin özdeşleri ağdaki tüm düğümlerde (*node*) bulunur (örneğin Bitcoin, Litecoin). İşlemler üçüncü tarafın aracılığı olmadan doğrulanabilir.
2. Belli kişilere özel veya izin gerektiren Blokzincirdeyse düğümler, ağa katılabilmek ve kimliklerini doğrulatmak için bir yönetici tarafından önceden seçilmelidir. Mutabakat kurallarını yöneticiler belirler. İzin gerektiren Blokzincirler iki alt kategoriye ayrılabilir (Houben ve Snyers, 2018: 15):
    a) Herhangi biri tarafından erişilebilen, görüntülenebilen, ancak işlem üretebilmek ve/veya defteri güncelleme yetkisinin yalnızca belirli ağ katılımcılarına açık olduğu, Ripple ve NEO örnekleri. İşlemler bir üçüncü taraf olmadan gerçekleştirilebilir.
    b) Erişimin sınırlandırıldığı, yalnızca ağ yöneticisinin işlem ve güncelleme yapabileceği kapalı veya kurumsal izine tabi olanlar. Burada üçüncü taraflara ihtiyaç doğabilir.

Blokzincirin İşleyişi

Kişiler Blokzincir teknolojisini kullanarak işlem yaparlar.

1. Tarafların benzersiz iki şifreleme anahtarı olmalıdır. Bu şifreleme tekniği asimetrik şifreleme olarak bilinmektedir: bir anahtarla diğeri elde edilemez; anahtarlar birbiri yerine geçemez. Şifrenin çözümü ancak ikisinin bir araya gelmesiyle sağlanır. Şifreyi kuran anahtar 'açık anahtar', şifreyi tekrar çözen anahtar 'özel anahtar'dır Anahtarlar arasındaki ilişki tek yönlüdür. Açık anahtar, kullanıcının

kayıt defterindeki dijital imzasıdır. Anonim olmasında, bir başkasına verilmesinde sakınca yoktur. Çünkü bir açık anahtardan özel anahtarı üretmek neredeyse imkânsızdır. İmza taklit edilse bile özel anahtar elde edilemez dolayısıyla da işlem üzerinde değişiklik yapılamaz. Özel anahtarsa paylaşılmaması gereken, ancak açık anahtarla birleştiğinde işlemde değişiklik yapma gücüne sahip anahtardır.

2. İşlem bu haliyle Blokzincirde beklemeye başlar. Blokzincir, koordineli, uzlaştırılmış bir grup bilgisayarlar ağı anlamındaki 'BotAğ' (*BotNet*) üstündedir. Bot Ağlarında, ağ sahiplerinin kararıyla farklı makinelerin gerektiğinde aynı anda, gerektiğinde ayrı ayrı çalışması sağlanabilir. Birlikte çalışmadaki iyi veya kötü amaç ağ sahibine bağlı olarak değişecektir (Tecnopedia 2019b: 1).

3. Blokzincir ağındaki bilgisayarlar, işlemin zamanı, boyutu, katılımcıları vb. tüm unsurlarıyla doğrulama yarışındadırlar. Bunu yapmak için de kullanıcılar özet değeri (*Hash*) denilen karmaşık bir matematik problemini çözmeye çalışmaktadırlar. Bu değerin doğruluğu da herhangi bir değişikliğin var olup olmadığını karşılaştırılabilen 'Merkle kökü' ve devamında 'Merkle ağacı' yoluyla sağlanır. Bilgisayar problemi çözdüğünde, algoritmanın çalışması bloğun işlem değerini doğrular. Yeni blok eklemek ve/veya komisyonla ödüllendirilir.

4. İşlem, kendisi gibi doğrulanmış diğerleriyle birlikte kayıtları oluşturur. Bu kayıtlar başka unsurlarla da desteklenir: Sihirli sayı (daima 0xd9b4bef9 şeklinde, blok başlangıcını ifade eder), blok boyutu (büyüklük), kayıt sayacı (işlem sayısı), blok başlığı , işlemler (Güven ve Şahinöz 2018: 54-55)

5. Böylece yeni bir Blokzinciri oluşmuştur. Bu aşama, bloğun değiştirilemez oluşunu ifade eder. Böylece zincire dâhil olan işlem herkese veya sadece ilgililerine açık olarak kaydedilmektedir. İşlemler mutabakatın öngördüğü şeklide halka veya ilgilerine açık olsa da kullanıcı verisi gizlidir. Veriyi, ancak işlemin tarafları açıklayabilir.

Blokzincirin İşlevsel Öğesi: Blok

Sistemin temelinde yaygın kayıt defterine belirli koşulları sağlayarak girebilecek ve zincirleme depolanacak dijital veri seti şeklinde bir Blok vardır. Bir blok şu amaçlarla oluşturulmaktadır:

1. Bir bloğu diğerlerinden ayıran özel bilgilerin depolanması,
2. Tüm işlem hareketlerinin takibi,
3. Kimin hangi işleme, ne zaman katıldığının takibi…

Blokzincir teknolojisi sadece bir ekleme sistemidir: Veriyi zincire yalnızca ekleyebilir fakat geri alamazsınız (Accenture, 2016: 3). Her bir blok doğrusal ve kronolojik şeklide kayıt defterinde tutulur. Eklenen her veri her

zaman Blokzincirin sonuna eklenir. Veriler özel bir matematik formülü üretilerek kayıt defterine girer, oluşturulduğu zaman verisi de blok üzerine yazılır. Bu şekilde blok, zaman verisinin sağladığı eşsiz bir imzaya sahip olur . Her biri ayrı bir zamanda kayıt altına alınmış bloklar sırayla dizilerek bir 'bloklar zinciri' oluştururlar.

Blokzincirin Araçsallaştırdığı Fikirler

Blokzincir, öncelikle Paul Baran'ın (1964) yaygın iletişim fikrini dayandırdığı ağ modellemesine dayalıdır. Baran'ın ağı, merkezi, dolayısıyla kırılgan bir denetim noktasına ihtiyaç duymadan, öğrenebilme yeteneğinde, düğümlerle değişen çevre koşullarına göre tüm akışı yönlendirilebilen bir ağdır. Baran çalışmasında bu ağın kafes (*grid)* veya örgü (*mesh*) olarak da adlandırılabileceğini belirtmektedir.

Blokzincir de şifrelenmiş işlem takibini sağlayan, yaygınlaştırılmış, yerinden yönetilen, genel muhasebe içerikli bir veri tabanı şeklinde bir 'yaygın kayıt defteri' olarak tanımlanabilmektedir. Defter teknolojisi, düğüm adı verilen istasyonlara sahiptir. Yaygın bir sunucu ağında düğümlerin her biri aynı veri kayıtlarını içerecek şekilde bir arada tutulur, denetlenen veri depolarında (defterler) veri kaydedilir ve paylaşılır. Bir işlemin yapılmasıyla beraber işlemin birer kopyası değil aslı, üstelik de küresel çaptaki her bir bilgisayarda aynı anda meydana gelmektedir. Bu nedenle, bugünkü tüm sistemlerinden çok daha güvenli olma iddiasındadır. Blokzincir teknolojisi de yaygın defter teknolojisinin özel bir türüdür. Çünkü tüm bir Blokzincir yaygın ağ temelli bir kayıt defteri üzerindeyse de bu onun yaygın ağ temelli kayıt defterlerini tümünü ifade ettiğini göstermez (Belin, 2018).

Yaygın ağa ek olarak Blokzincir, Şifreleme (Kriptoloji), Mutabakat fikirlerini de araçsallaştırarak birleştirmektedir. Her türlü varlığı, kuralları mutabakatla oluşturulmuş, eşzamanlı işleyen, küresel ölçekteki 'yaygın ağ temelli bir kayıt defteri' üzerinde şifrelemek, yönetmek mümkündür. Bu iki unsura sırayla bakı-

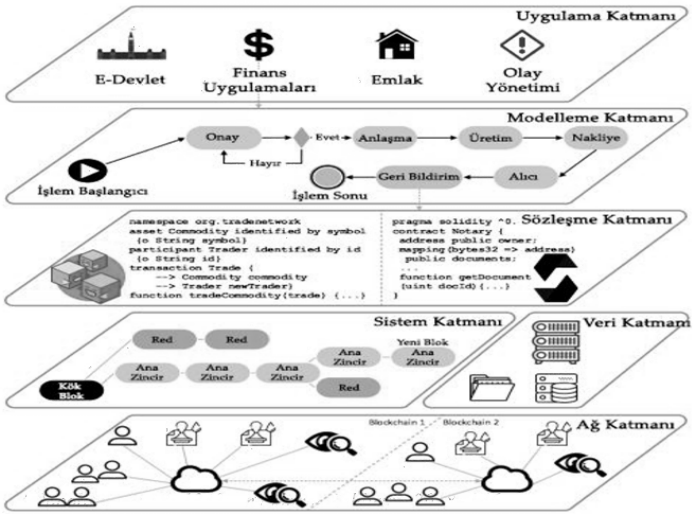
lırsa:

Verinin iletişim ağları sayesinde çok sayıdaki bilgisayara dağıtılması ancak şifresiz olmasıyla mümkündür. Ancak ağ üzerinde tutulan veri şifrelenmediğinde herkesin veriye erişebilmesi, mahremiyet kaybı, veride tahrifat ve mükerrerlik gibi istenmeyen sonuçlar doğmaktadır. Bu çelişkiyi giderecek başka bir ihtiyaç doğmuştur. Veriyi farklı veri tabanlarında saklamak ve her seferinde tutarlılık sağlanması için şifrelemeye duyulan ihtiyaç… Bu ihtiyaç özellikle *asimetrik şifreleme tekniği, dijital imza, özet değeri algoritması, Merkle ağacı* gibi araçlarla karşılanmaktadır.

Şifreleme imkânı önemli bir ilerleme sağlamışsa da bu kez veriyi paylaşmama ve tekrar kullanımdaki tutarlılık için hep ilk kaynağa başvurulması mecburiyetini doğurmuştur. Veri şifrelendiğinde şifreleyen kişi dışında kimseyle paylaşılamaz; veri bütünlüğünü, tutarlılığını da ancak kaynak kişi ya da taraf sağlayabilir. Bu aşamada verinin dağıtılarak paylaşılması ancak aynı zamanda değiştirilmemesini mümkün kılan bir sistem gerekmektedir. Bu da tüm kullanıcıların mutabakata uygun davrandıklarının teyit edilmesiyle sağlanmaktadır.

Blokzincirde, merkezî veri tabanları veya yetkilileri olmadığından Blokzinciri ayakta tutan sadece Topluluk Mutabakatına uygun işlemlerin meşru kılınmasıdır. Mutabakat, verinin doğruluğu, tutarlılığı için gereklidir. Mutabakat hem seviye (örneğin ya tüm işlem süreci ya da sadece işlemin doğruluğu) hakkında hem kapsam (tamamen açık ve sadece belirlenmiş ilgilerine açık olması) açısından çeşitli durumlarda sağlanabilir (Beck vd., 2018: 8).

Şekil 2. Blokzincir Katmanları



***Kaynak**: Zhan,*

Blokzincirde Özel Bir Beceri: Akıllı Sözleşmeler

Blokzincir bir başka bir yenilik daha getirmektedir. O da kendi kendini düzenleyebildiği için akıllı olarak sıfatlandırılan sözleşmelerdir. Akıllı sözleşmeler fikri Nick Szabo tarafından önerilmiştir (1994). Burada icra, performans takibi, ödeme, sadece muhataplar arasında kalan bir sözleşme yönteminden bahsedilmektedir. Akıllı sözleşme, istendiğinde Blokzincir içine yerleştirilebilen bir koddur. Bloklardaki verinin, öngörülen durumlarda, bir otorite onayı olmadan, şartlar oluştukça belirli seçenekler arasında karar verme yeteneğiyle; istenen görevleri kendiliğinden hayata geçirir, gerektiğinde yepyeni bir sözleşme yapılabilmesini sağlar. Örneğin kamuda bir doğal afetten etkilenenlere ödenme yapılması veya ihtiyaç dağıtımının doğrulanmasını otomatikleştirmek için kullanılabilirler. Ethereum bu alanda en çok tercih edilen platformdur.

Akıllı sözleşmeler, muhatapların önceden üzerinde anlaştıkları şartlarda iş görürler. Şartlar oluştuğunda, sözleşme kendiliğinden yerine getirilir. Örneğin, bir mülkün akıllı sözleşme kullanarak kiralandığını varsayalım. Mal sahibi depozito ödendiği an kiracıya daire kapısının giriş kodunu göndermeyi kabul etmiştir. Kiracı kodu kullanmayarak mülkten vazgeçerse akıllı sözleşme güvenlik depozitosunu mal sahibine otomatik olarak iade eder. Bu işleyişte, üçüncü taraflara verilecek ücretleri ortadan kaldırılmıştır.

Yine özellikle sanatçılar, icracılar, kâşifler, akademisyenler, gazeteciler gibi fikrî üretim yapanların telif haklarından geçinmeleri çok güçtür. Fikrî ürünlerde kazanç zincirinde en az pay eser sahiplerine düşmekte, ücretsiz, izinsiz yayım ve dağıtımındaysa haksız kazanç elde edilebilmektedir. Hak sahipleri aynı eserleri Blokzincir ekosisteminde değerlendirdiklerinde, haklarını koruyan 'akıllı sözleşme' yapısıyla korunmaktadırlar. Bu yöntemde ürünün getirileri eser sahibine ulaşmaktadır. Otomatik güncelleme gereği akıllı sözleşmelerle hak kayıpları da önlenmektedir. Fikrî ürün sahipleri aracı kurumların piyasayı manipüle etme güçlerine dayanmak yerine süreci bizzat yönetebilmektedirler.

Blokzincirin Avantajları

Blokzincirin geleneksel IP mimarisine göre avantajlarına yakından bakılırsa:

Değişmezlik: Herhangi bir veri tabanıyla Blokzincir veri tabanının işleyişi farklıdır. Blokzincirin genel finansal endüstrisiyle uyumlu olmasına, onunla benzeşmesine gerek yoktur, çünkü ödeme ve teyit aynı anda gerçekleşebilmekte, aracılara gerek kalmamaktadır. Geleneksel yapıda yetkilendirilmiş bir kullanıcı, merkezi bir sunucuda yani ana kopyada depolanan girişleri değiştirerek, veri tabanı girişinin güncellenmiş sürümünü alır. Sıradan bir veri tabanının kontrolü, erişim izini merkezi bir otorite tarafından sürdürülür. Oysa Blokzincir için her

katılımcının veri tabanına yeni girişlerini saklar, hesaplar, günceller. Hiçbir giriş silinmez. İstenirse geriye dönük tüm işlemlere bakılabilir. Tüm düğümler, birden çok veri tabanının aynı sonuca gelmesini sağlamak için birlikte çalışırlar ve ağ için yerleşik güvenliği beraber sağlarlar (Bauerle, 2018).

Potansiyel: Çok merkezli, eşzamanlı kayıt tutma imkânı neredeyse sınırsızdır. Çok taraflı hemen her konuda da bir Blokzincir oluşturmak mümkündür. Blokzincir, kimlik yönetimi, tapu kayıtları, seçimler, bankacılık, sağlık yönetimi, fikrî ürünler telifi, siber güvenlik, tedarik zinciri yönetimi, nesnelerin interneti (IoT), tahmin ve öngörü araştırmaları, taşıt paylaşımı, bulut depolama, şaibesiz bağış toplama, sigortacılık, enerji yönetimi, emlak-mülk alışverişi, perakende satış gibi pek çok alanda kullanılabilmektedir (Future Thinkers: 2017).

Güvenlik: Müesses nizamın en temel sorunu olan güvene dayanan ilişkilerde sonuçların belirsiz olacağını mantık ilkeleri üzerinden açıklayan 'Bizans Generalleri Sorunu' sadece 'insana güvenmeye' dayandırıldığında ağ tipi ilişkilerin suistimale açık olduğunu, sadakatsizliği engellemeyeceğini tespit etmekteydi. Blokzincirden önce çok ortaya konmuş olan ağ iletişimindeki bu zıtlık hakkındaki Bizans Generalleri Sorununun çözümü 'Hata Payı (Toleransı)'ndadır. Bu pay olan veri tabanının tasarımı aşamasından iyi hesaplanmazsa ciddi kayıplar, haksız kazançlar söz konusu olabilir. Blokzincirde bu hata payı tasarımda göz önüne alınmaktadır. Blokzincir teorisyenleri böylece 'insana güvenin' yerini 'bilgi işlem hesaplama gücünün' aldığını, her bir blokta olması gerekeceklerin tespiti içinse bir mutabakat yapısı oluşturduklarını belirtmektedirler. İlgili topluluğun niceliği, niteliği mutabakata özel olarak sağlanabilecektir.

Çökertilmesinin Anlamsızlığı: Blokzincire kötü niyetli bir blok eklenirse, küresel ağdaki düğümler mutabakatı yenileyerek ağı güven altına alırlar.

Bir korsanının müdahalesi ağın tamamını değil ancak Blokzincirin tek bir kopyasını tehlikeye sokabilecektir. Bir korsanlar topluluğunun saldırısında ise bir merkez olmadığından Blokzincirin çökertilmesi ihtimali azdır. Nakamoto, matematiksel olarak %51'i ele geçirecek saldırgan düğümlerin olabileceğini ancak saldırganların tüm blokları baştan tekrar etmelerinin ve dürüst düğümlerin iş hacmini yakalayıp geçmelerinin imkansızlığını açıklayabilmektedir (2008: 3, 7-8). Üstelik donanım hız, düğüm sayısı gibi değişkenlere göre iş kanıtının zorluk seviyesi tekrar ayarlanır. Ele geçirilip yönetilecek bir Blokzincirde nihai olarak daha çok kazanmak diye bir durum yoktur. Kullanıcılar Blokzincire olan inançlarını kaybederlerse, ağ değersizleşecektir. O halde kullanıcılar için de herkesin kazanç sahibi olacağı, topluluğu yok etmeyecek bir noktaya kadar güçlenmeleri seçeneği rağbet görecektir.

Daha düşük işlem ücretleri: Geleneksel yaşamdaki gibi kişiler aracılık için ödeme yapmaz, komisyon vermezler. Blokzincirde muhataplar işlemlerini kendi başlarına endişe etmeden yaparlar. Aracılık olmadığından yüksek kâr içeren komisyonlar oluşmaz. Dolayısıyla üçüncü tarafların doğrulamalarını ve ilgili maliyetleri ortadan kaldırılmıştır.

Doğru Kayıt Tutma: Buradaki etken Blokzincirdeki işlemlerin milyonlarca bilgisayardan oluşan bir ağ tarafından onaylanmasındaki zorunluluktur. Bağlantılı olma durumu, işlemin inkâr edilememesini, yapılanı geri alamamayı sağlar. Her bir işlemin zaman damgası vardır. İşlem bloğa bir kereliğine dâhil olmakta ve tüm ağ üzerindeki tüm düğümlerde aynı şekilde durmaktadır. Tanımda kullanılan zincir metaforuyla bu kopmamazlık hali simgelenmektedir.

Yerinden Yönetilme: Blokzincir, veriyi tek bir yerde saklamaz. Blokzincirde tüm veri aynı anda üretilir ve küresel ağda oluşur. Yaygın Defter Teknolojisi sayesinde karar alıcılar ağ üzerinde yaygın halde, birbirlerine eşit düğümler üzerindedirler. Bu da karar alma yapısına yerinden ve demokratik olma potansiyelini kazandırmaktadır.

Zamandan Tasarruf: Blokzincir yedi gün yirmi dört hizmet verebilmektedir. Yaklaşık on dakikada işlemler tamamlanabilir ve birkaç saatte de güvenli sayılacak halde olurlar. Özellikle de bu, uluslararası işlemlerin sürelerini kısaltmaktadır.

Saydamlık ve Mahremiyet: Blokzincir veri tabanları genellikle kamuya açıktır. Bir işlem yapıldığında kamuya açık olan, kişisel bilgiler değil, genel anahtarlı bir bloktur. Mutabakat imkân veriyorsa ağın işlem geçmişini internete bağlı herkes görüntüleyebilir. Ancak görüntüleyenler işlemler hakkındaki ayrıntılara erişebilseler de bu işlemleri yapanlar hakkında betimleyici veriye erişemezler. Kişisel bilgiler Blokzincir adresleriyle bağlantılı olmasına rağmen, muhatabı dışında kimsede bulunamaz. Olası bir saldırıda dahi asimetrik şifreleme ile bilgilerin güvende olduğu öngörülmektedir.

Tutarlılık: Bir işlem kaydedildiğinde, doğruluğu Blokzincirin yaygın ağı tarafından doğrulanmalıdır. Bir bloktaki bilgiler değiştirilir veya düzenlenirse, özet kod da değişir. Tek yönlü işlevi nedeniyle özetten orijinal veriye ulaşılamaz. Bu özellik sıradaki bloğu da eşsiz kılmaktadır. Çünkü ilki olmadan ikincisinin varlığı mümkün olmadığından tutarlılık sağlanmış olur (Güven ve Şahinöz, 2018: 45). Bloklar arasındaki bu tutarlılık teminatı, bloktaki verinin habersiz şekilde değiştirilmesini ciddi anlamda zorlaştırmaktadır.

Doğrudan ve Tam Katılım: Bilgi işlem gücünün çoğunluğu desteklediği sürece, uygun görülürse kod değiştirilebilir. Daha önceki kurallardan vazgeçerek

değişiminde fayda görülen bir düzene geçmeleri mümkündür. Böylece aslî anlamında *paylaşım ekonomisini* ve *tam katılımı* mümkün kılmakta, iktisadi ve idari sisteme daha çok sayıda, nitelikli bireyin katılması sağlanmaktadır.

Blokzincirin Dezavantajları

Blokzincir önemli avantajlara sahip olsa da kabul görmesinin önünde önemli zorluklar vardır. Kullanıcının benimsemesinden, birlikte çalışabilme, ölçeklendirme gibi teknolojik engellere, yasal düzenlemelerdeki zorluklardan, enerji israfına kadar önemli zorluklarla karşı karşıyadır (WEF, 2018: 5).

Doğaya Etkileri: Blokzincirde işlem ücretleri yok denecek kadar azdır. Ancak teknolojik altyapısı maliyetsiz değildir. Mesela, tek bir Bitcoin oluşturulması için iş kanıtı, aşırı karmaşık bir algoritmayı, her on dakikada bir çözmelidir. Bunun madenciliğinin maliyeti, (o ülkedeki elektrik maliyetine göre) 531 ABD dolarından 26.170 ABD dolarına kadar değişebilmektedir (Kerr, 2018: 1). Bu maliyet madenciler için kazanç beklentisiyle karşılanıyor olabilir. Ancak asıl önem arz eden maliyet, enerjinin ana kaynağı olan doğanın ödediğidir. Bitcoin vb. yatırım araçlarından haberi dahi olmayan tüm canlı âlemi Blokzincirin yüksek enerji kullanımı nedeniyle ciddi bir tehditle yüzleşmektedir. Örneğin Bitcoin ağının şu anda 7.67 gigaWatt elektrik harcadığı tahmin edilmektedir. Bu anlamda Bitcoin ağı tüketimi 2018 yılı için 8,2 gigaWatt elektrik tüketimine sahip Avusturya'ya yetişmek üzeredir (De Vries, 2018: 804). Bir tek Bitcoin işlemi 468 kiloWatt/saat enerji kullanırken 100.000 adet VİSA ödeme sistemindeki işlemler sadece 151 kiloWatt/saat enerji kullanmaktadır. Yine bu işlemlerin yıllık karbon ayak izinin 29,678 CO2 kiloton, işlem başına karbon ayak iziyse 222.12 CO2 kiloton olduğu tahmin edilmektedir. Bu miktarlar çok ciddi bir tüketime işaret etmektedir (Digiconomist, 2019). Ağın yükünü azaltmak için iki taraf arasındaki işlemlerin Blokzincir dışında yapılarak Blokzincire sadece kayıtların bırakılması yöntemi olarak bilinen 'Lightning Ağının (Lightning Network, 2019:1) bu enerji tüketimini azaltsa da ağın büyüme hızına yetişilemeyeceği belirtilmektedir (De Vries, 2018: 804).

Verimsizlik: Bitcoin'in iş kanıtına olan ihtiyacı nedeniyle, Blokzincire bir blok eklemek neredeyse 10 dakika sürmektedir. Bu nedenle Bitcoin, saniyede iki ilâ yedi işlemi yönetilebilir. Bitcoin'den daha iyi performans gösteren Ethereum ve Bitcoin Cash bile hâlâ çok yavaştırlar. Zira VISA'daki benzer işlem hızı saniyede 24.000'dir (Güven ve Şahinöz 2018: 40). Elbette işlem sonrasındaki doğrulama süresinin Bitcoin'de sadece birkaç saat, VISA işlemlerinde ise birkaç günü bulduğu da hatırlanmalıdır.

Gizlilik: Blokzincir ağındaki mahremiyet avantajı kişinin malvarlığının devlet otoritesinden de saklı şekilde sadece kendisinin bilgisinde olmasını

getirmektedir. Bu kimlik mahremiyeti Blokzincirle yasadışı işlem ve etkinlik yapılmasında bir avantaj olabilmektedir. İngiltere ve Kanada Merkez Bankaları, A. B.D. Federal Rezerv Bankası Bankası'nın içinde olduğu birçok merkez bankası, bu açıdan kripto paralar için soruşturma başlatmışlardır. Ancak bugünkü sistemde benzer faaliyetlerin çok daha büyük hacimlerde olduğu, kara para hareketlerinin bu gelişmelerden önce de var olduğu; zor olsa da takip olanağıyla ilgililerin kimler olduğu değilse de hesaplarının mutabakatla denetim altına alınabileceği unutulmamalıdır (Güven ve Şahinöz, 2018: 32-33).

'Değiştirilemezlik' Niteliği: 'Unutulma Hakkı'nın veya bu teknolojiyle işlem kayıtlarına gelen azami derecedeki şeffaflığın mahremiyeti tehdit edeceği hakkında endişeler söz konusudur. Örneğin Accenture danışmanlık firması Blokzincirin değiştirilemez nitelikte olmasının, kusurlarla dolu bir dünyada işlemden geri dönebilme hakkını ihlal edeceği için gerekirse Blokzincirin değiştirilebilmesi için 2019'da bir patent almıştır (Accenture, 2016: 5; Ramathal ve Greene, U.S. Patent No: 10291413, 2019). Ancak tersine Blokzincirin tüm farklı niteliklerine rağmen zaten zor bir konu olan veri koruma için tam bir çözüm olamayacağı ama yine de kişisel verinin kullanımını kontrol etmeye yardımcı olan bir mekanizma olduğu da belirtilmektedir (IBM, 2018: 7).

Blokzincirin Özel Sektördeki Örnekleri

Profesyonel bir danışmanlık şirketinin1000 şirketle yaptığı bir araştırma, Blokzincirin özel sektörde kullanım örneklerini iş hacmi ve çeşitliliği açısından ortaya koymaktadır (Deloitte, 2018: 6, 8, 18):

- %34'ünün şimdiden Blokzinciri kullandıkları,
- %41'inin gelecek bir yıl içinde kullanmayı planladıkları,
- Her iki gruptan toplamda %39'ununsa gelecek yıl Blokzincire beş milyon ABD dolarından daha fazla yatırım yapacaklarını aktarılmaktadır.

Dağıtık Uygulamalar (*Distributed Applications (DAPPS)*), işlemlerinde akıllı sözleşmeler kullanan uygulamalardır. Blokzincir kullanımını özel sektörde sıradan insanların da hayatlarına dâhil ederek örneklendirmeye başlamışlardır. Birkaç örneğe bakılırsa:

- 2015 yılından beri *Everledger* şirketi, elmas ticaretindeki işlemlerini Blokzincir sayesinde hızlı ve güvenilir şekilde takip edebilmektedir (Everledger, 2019:1).
- *Ujo Music*, bir akıllı sözleşmeyle şarkıların indirilmesi, yayımlanması için dijital lisansı satın alabilmeyi, ödemelerin de besteci, söz yazarı ve diğer pay-

daşları arasında otomatik şekilde dağıtılmasını mümkün kılmaktadır (Ujo Music, 2018:1).

• *OpenBazaar* Her türlü çevrimiçi alış-verişte alıcı ve satıcıları birbirlerine doğrudan bağlayan bir uygulamadır. Burada bilinen alışveriş sitelerinden farklı olarak platformda bulunma ücreti, aylık ücret veya liste ücreti ödenmemektedir (OpenBazaar, 2016:1).

• *Augur* ise akıllı sözleşmelerle çalışan bir tahmin borsasıdır. Belli bir sürede gerçekleşeceği tahmin edilen bir olay için kayıt açarak hizmet sunmaktadır. (Augur, 2019:1). Örneğin, bağımsız gazetecilerin haber yapmalarına bir para desteği imkânı oluşturmaktadır. Böylece öngörüsü kayıt altında olan ve haklı çıkan bir muhabir güven temin ederek yeni araştırmalarına destek toplayabilir

Blokzincirin Kamu İdaresindeki Örnekleri

Elektronik veri tabanlarıyla birlikte bilgi yönetiminin verimliliği, etkililiği, etkinliği önemli ölçüde artırmıştır. Demokratik devlet yönetimleri verinin erişilebilir ve şeffaf olmasına değer atfetmektedirler. Hatta bu özelliği başarılarının bir ölçüsü olarak ortaya koymaktadırlar. Maaş ödemeleri, vergi tahsilatları, transferler, tedarikler, ihaleler, idari ve para cezalarının takibi, ruhsatlar vb. işlemlerin sayısallaştırılması artık bilgi toplumu için bir lüks değil, bir standart olmuştur.

Devletler uzun süredir hem kamu hizmetlerini sunmak hem de idare becerisini geliştirmek için dijital araçlara yönelmektedirler. Blokzincir de güvenilir bir denetim sağladığından ve veriyi istendiğinde ilgililerleriyle paylaşılabildiğinden dikkat çekmektedir (Lyons vd., 2018: 4). Blokzincir teknolojisi, kamu sektöründe dijitalleşmeyi geliştirmek için potansiyel destek platformu olarak anlaşılmalıdır (Ølnes ve Jansen, 2017: 217). Çünkü devletler her düzeyde, ölçekte bir veri okyanusunun içindedir.

Dünya Ekonomik Forumu Blokzincir ve Yaygın Defter Teknolojisi Komisyonu Başkanı Warren'a göre, bu teknoloji, üçüncü tarafların [işlemlerin yapılışında] olup bitenleri denetlemelerini sağlayacak bilgilere erişim sağlayabilecektir. Bu tür bir denetim zahmetli olsa da kamusal süreçlerin kurallara uygun şekilde işlediğini kanıtlamak için kritik bir önemdedir (Cointelegraph, 2019:1).

Kamu sektörünün bu yeni alanı hızla sahiplendiği görülmektedir. Örneğin adli tıp kayıtları, araç sicil ve tescil işlemleri, asayiş denetimleri, pasaport, doğum ve ölüm belgeleri, dijital ödeme sistemleri, inşaat ve silah ruhsatları, kimlik yönetimi, mevzuat, mahkeme kayıtları, şirket lisansları, sabıka kayıtları, tapu kayıtları, tıbbi kayıtlar, tedarik zinciri takibi, ticari sicil, seçim ve seçmen kayıtları, vergilendirme, vb. alanlarda… aşağıdaki haritada da örneklerin dünya çapında arttığını görülmektedir.

Kaynak: *Berryhill vd., 2018: 21*

ABD Savunma Bakanlığı Blokzincire dayalı bir mesajlaşma uygulamasını denerken, NATO geri hizmet ve tedarik gibi alanlarda sınamaktadır (Kar, 2016: 1). Estonya 2016'nın ilk yarısında hükümet, bir milyondan fazla vatandaşının sağlık kartı veri setinin Blokzincire aktarması için *Guardtime* firmasıyla anlaştı (E-estonia, 2016). BAE, tüm devlet sistemlerini 2020'ye kadar Blokzincirde işletmeyi başlatacağını açıklamıştır (Forbes, 2017) Endonezya *Provenance* şirketiyle anlaşarak kaçak balıkçılığı takip etmek için Blokzinciri kullanmaya başladı (Provenance, 2016).

Blokzincirin kullanımında kamu hizmetine karakter veren belli hizmetlere daha da yakından bakılırsa:

Kimlik Yönetimi

Kamu yönetimi için hizmetin başlangıcı kimliktir. Kimlik her tür hizmetin alınması için bir illiyet bağı kurmakta, hizmeti meşru kılmaktadır. Kimlik tespiti hakkındaki bir araştırmaya göre dünya nüfusunun %20'si resmî bir kimlik olmadan yaşadığından kamu teşkilatları tarafından tanınmamaktadır (World Bank, 2018: 3). Bu bireyler sağlık, eğitim, geçim sağlama hakkındaki hizmetlerin başta olduğu kamu hizmetlerine erişmek için mücadele etmektedirler. Sağlıkla yaşamak, kendilerini geliştirmek, ekonomik faaliyette bulunmak veya istihdama katılmak gibi önemli fırsatları kaçırmaktadırlar. Şimdi Blokzincirle bu bireylerin kısa zamanda, hatta küresel ölçekte tanınabilecek standartta bir kimliğe kavuşabilmesi için bir imkân doğmuştur. Kısa sürede ulaşılabilecek, tahrif edilmeyecek, sahtesi

üretilemeyecek; hizmet almak için kullanılabilecektir. Kimliğin ne zaman ne için kullanıldığı Blokzincirle kesintisiz ve tahrifata uğramadan kayıt altına alınabilecektir. Kamusal hizmetlerde bilgi güvenliğini sağlayabilecek bu teknoloji öne çıkmaktadır (Durukal ve Öztürk, 2019: 540). Devlet kayda değer miktardaki işlemin kaydedilmesini, varlıkların mülkiyetinin izlenmesini hem verimli hem şeffaf şekilde yapılabilir. Böylece kimlik doğrulaması kaynakların etkin kullanımında, vatandaşın [da güvenliği açısından üçüncü taraflarca] takibinin azaltılmasında, devlet yardımı tahsislerinde şeffaflık sağlanmasında faydalar gösterecektir (Gupta, 2017: 28).

Tapu Kayıtları

Tapu kayıtları sadece ekonomik güce sahip olanlar için önemli bir hizmet addedilebilir ancak bunu hak sahiplerinin haklarını kaybetmemeleri; haklarına, hukuka aykırı yollarla el konulmaması açısından değerlendirilmesi daha doğrudur. İster mirasla ister birikimleriyle alınsın, mülk kayıtlarının açık ve değiştirilemez şekilde tutulması sosyal adaleti olduğu kadar ekonomik yaşamı da ilgilendirir.

Tapu kayıtlarının genellikle kâğıt üzerinde olması kırılganlığın ciddi bir sebebidir. Örneğin 2010 yılındaki Haiti depreminin ardından devlet yıkılan kamu binalarıyla birlikte tapu sicil kayıtlarının da tahrip olmasıyla yüzleşmiştir (Usta ve Doğantekin, 2017: 75).

Bir başka kırılganlık sebebi bu hizmet sunumunun yolsuzluğa açık yapısıdır. Tapu kayıt işlemleri evrak ve şahitlik esaslıdır. İşlemler oldukça masraflı ve kötü niyetli kişilerce değiştirilmeye açık bir yapıdadır. Siyasi yolsuzluk için fırsatlar da genellikle toprak reformları, kalkınma projeleri veya tapu işlemlerinde ortaya çıkmaktadır. Bu nedenle arazi yönetimi, devlete ait ve özel sektöre ait arazilerin devir ve tescili işlemlerinin yürütülmesi, kayıt altına alınması için önemlidir (TI, 2011).

Dünyada gayrimenkul kayıtlarını, bir uzlaşmazlık karşısında geriye dönük şekilde ispatlayabilmek için Tapu Sicil/Mülkiyet Sigortası (*Title Insurance*) olarak bilinen güvencelere milyarlarca ABD doları harcanmaktadır.

Öte taraftan Uluslararası Şeffaflık Örgütü'nün bir araştırmasına göre Hindistan genelindeki tapu işlemleri için yetkililere tahmini 700 milyon ABD doları rüşvet ödenmiştir (TI India, 2005). Örgütün başka ülkelerde yaptırdığı araştırmalar da bu konudaki kırılganlığı ortaya koymaktadır. Birkaç örnek birlikte incelendiğinde arazi yönetimi işlemlerinin %60'ının rüşvete konu olduğu, işlem tutarın rüşvetin %60-90'ına ulaştığı, tapu makamlarına yasadışı ödemelerin şikâyet edilen hizmet ve kurumlarda ilk 10 hizmet arasında yer aldığı belirtmektedir (Transparencia Mexicana, 2011; TI Kenya, 2011; TI Bangladeş, 2012).

Tapu kayıtlarının Blokzincirde tutulması veya alım satım yapılması, ilgili her tür işlemi; inkâr edilemez, değiştirilemez, yolsuzluk yapılamaz şekilde koruyacaktır. Özellikle anti demokratik ülkelerde kayıtlarla oynayarak malvarlıklarına hukuksuz olarak el koyan hükümetlerin önüne geçilebilecektir. Bu durum, milyarlarca insan için yaşamı sürdürme güvencesi getiren ve miras bırakılabilen varlık imkânları yaratmaktadır. Bu konuda çare Blokzincirde görülmektedir. Rusya, (Rosreestr, 2018), Birleşik Krallık, (HM Land Registry, 2019), İsveç, (Lantmateriet, 2018), Brezilya, (Lemieux, Flores and Lacombe, 2017), Hindistan, (Oprunenco and Akmeemana, 2019), Gürcistan (Georgian Prime Minister's Press Office, 2019), Japonya (Nomura Research Institute, 2019) tapu kayıtlarını Blokzincirde tutmayı sınayarak devlette sahtekârlık ve yolsuzluk sorunlarıyla mücadele etmektedirler.

Seçimler

Oy kullanma demokratik sistemler için meşruiyet sağlayan kritik bir kamusal işlevdir. Vatandaşlar, oy kullanabilmeli, oy kullandıklarını ve seçim sonuçlarını doğrulayabilmelidirler.

Şu anda dünyada e-oylama sistemleri de uygulanmaktadır ancak hem anonim olma hem de dijital kimlik yönetimindeki eksiklikler nedeniyle kişiye özel oylama süreçleri tam olarak yönetilememektedir. Özellikle seçim düzenlemekle yükümlü kurumların dışarıdan ulaşmaya açık yazılımlar üretmeleri veya satın almaları mümkün olmaktadır ki bu oy kutsallığına gölge düşürmektedir.

Geleneksel merkezî seçim süreci genellikle verimsiz, geç sonuç alınan, maliyetli (listelerin hazırlanması, oy pusulası basımı, seçim görevlilerine ücret ödenmesi için yapılan işlemler, elektronik oylama makinelerinin bakımı vb.), yolsuzluk şaibesinin gölgesinde tam olarak güven duyulmayan bir süreç olagelmiştir. Blokzincir altyapısı ise etkin bir oylamayla maliyet tasarrufu, güvenilirlik, seçim kayıtlarının şeffaflığı, geniş katılım, hızlı sonuç önerilerinde bulunmaktadır. Bunun örnekleri oluşmaya başlamıştır[1]. ABD'deki Batı Virginia eyaletinde ara seçimlerde bazı idari bölge birimlerinde (*county*), Voatz adlı Blokzincir uygulamasıyla bir deneme kapsamında 30 ülkedeki 144 seçmen oy kullandı (Warner, 2018:1; Symantec, 2018: 1). Bu tür yollarla e-oylamalardaki zaaflar azalacak gibi görünmekte, Blokzincirin seçime katılım oranını artırma ve seçim sahtekârlığını önleme potansiyeli sınanmaktadır.

1 Bakınız: Follow My Vote, (2019). "How?", followmyvote.com (11.07.2019)

Değerlendirme

Blokzincir, veriyi geleneksel bürokrasiden daha hızlı, daha güvenli, daha doğru ve verimli bir şekilde işleyebilir. Bu teknolojinin getirdiği etkileyici yenilik, ağın açık olması ve katılımcıların etkileşimde bulunmak için birbirlerini tanımalarına, güvenmelerine gerek duyulmamasıdır. Blokzincir teknolojisinin, '*bürokratik süreçte kamusal süreçlerin kurallara uygun şekilde işlediğini kanıtlamak için kullanılabileceği'* fikri kamu sektörünün yararına sunulmakta, sektör de bazı spekülasyonların farkında olsa da bu yeni protokol yapısının yıkıcı teknolojisine kayıtsız kalmamaktadır. Önceliklerini belirlemeye çalışmaktadır. Blokzincirin bu ilgiyi toplamasının sebepleri özetle veride tahrifata yer vermemesi, zaman damgalarının mükerrerliği engellemesi, akıllı sözleşmelerle idari süreci otomatikleştirebilmesidir. Aracısız, farklı tedbirlerle korunmuş bir ortamda, açık ve kayıt altında kamu faaliyetlerinin varlığı artık düşünülebilmektedir.

Blokzincir bu tür teknik imkânlarının yanı sıra siyasal bir boyuta da sahiptir. Daha önce herhangi bir resmî veya sivil otoritenin kurallarını belirlediği bir ağ mevcuttur. Ancak şirket platformlarıyla (Microsoft, Google vb.) ağa katılmak mümkündü. Şimdi farklı bir yapının olması Blokzincirin siyasal yaşama katkısını oluşturmuştur: Artık ağdaki kişiler Blokzincirde bir düğüme (cihaza) sahip olmakla ağın bir parçasına da sahip olacaklardır. Bugünün internet mimarisinden farklı olarak aslî kişiselleştirme, tam ve doğrudan katılım imkânları kamu hizmetleri için Blokzincirin demokratik katkısını öne çıkarmaktadır. Tüm bunların bürokraside yerleşmesi büyük bir 'yapı bozum', dönüşüm demektir.

Yeni Kamu Yönetimi anlayışı Batı ülkelerinde 1970'lerden bu yana ortaya çıkan yeni merkezi yönetim uygulamalarını tanımlamak için önerilmişti. Bu süreçte önerilen 'etkin devlet'; 'çok paydaşlı', 'yerinden yönetimci', 'yaygınlaştırılmış', 'ortak çalışmaya dayalı' vb. farklı yönetişim modellerinin ortak özellikleri Blokzincir imkânlarıyla örtüşmektedir: Dikey hiyerarşinin terk edilmesi eğilimi, karar vermede duyarlı, şeffaf, hesap verebilir bir yaklaşım, sorunlara mutabakata dayalı çözümler bulmak için bir diyalog platformunun varlığı (Atzori, 2017: 50) Bu kısa listedekiler bile Blokzincir temelli yönetişim, bu anlayışın son aşaması olarak değerlendirilmektedir.

Yine de tüm bu düşünceler, yöntemler, araçlar hâlâ bir 'düşünce deneyi' şeklinde algılanmaktadır. Bu makale yazarının gözlemlerine göre bireyler konuyu bir otoriteye, bir kontrol mekanizmasına bağlama eğilimi göstermektedirler. Platon'un "benzer benzerle bilinir" ifadesi (Guthrie, 2011: 221) burada akla geliyor. İnsanoğlu çok uzun bir süre çoğunlukla aracılık sistemini tercih etmek durumunda kalmıştır. Aksi bir örnek zihinde canlanamamaktadır. İşlemin tarafı olmadığı halde, transfer ortamına bir ara yüz sağladığı için ihtiyaç duyulan

üçüncü taraf olmadan güvencenin nasıl sağlanacağı doğal olarak sorgulanmaktadır. Yapı öylesine yenidir ki referans alınacak 'bir benzer' oluşturmak zaman alabilir. Şimdilik Blokzincir teknolojisi bağlamında, paydaşlar çeşitli yönetişim yapılarını sınamaktadırlar (Narayanan vd., 2016: 173).

Birçok Blokzincir savunucusunun yaygın ağda oybirliğini ve yatay yönetişimi benimsemiş, vatanı, ulusu olmayan, hatta kendilerini sınırları çizilemeyen bir ulus topluluğu addeden[2],[3] idealist, eşitlikçi bir toplumun koşullarının oluşturulabileceği tarihi bir aşamadan bahsettikleri değerlendirilmektedir (Atzori, 2017: 46). Temsili demokrasinin doğrudan sivil katılım biçimleriyle güçlendirilmesi gerektiğine ilişkin temel yargı hep rağbet görmüştür. Blokzincir temelli yönetişim, ileride bunu sağlama becerisine sahip olarak kabul görmekle beraber, şimdiden öngörülebilen sorunlar vardır:

• Kuralların hukukiliğinin, hakkaniyetinin denetiminin nasıl sağlanacağı: Çok amaçlı ve/veya çok değişkenli işlevleri nasıl karşılayacağı belli olmayan Blokzincir alanına özel bir hukuk geliştirip geliştiremeyeceği, bu alanda muhakeme ilkelerinin neler olacağı belirsizliğini korumaktadır. Çözüm her mutabakat grubunun çatallanarak ayrılmasıyla, ayrı hukuk geliştirilmesi olacaksa şu an her işleme ayrı kural uygulayan aracılık sisteminden fark ne olacaktır?

• 'Devletin çıkarları ortadan kalktığında, diğer çıkarlar onların yerini alacak. Bu çıkarların ne olduğunu biliyor muyuz, daha iyi olduklarından emin miyiz?' (Lessig, 2000:1): Büyük tekel sahipleri ve oligopolleri ağ işletim gücünü satın alabilirler. Önceki işleyişlerden, kurumsallaşmalardan farklı olarak tüm bir topluluk işlemleri gözetmekte, işlemleri doğrulamak için de yarışmaktadırlar. Aracılık faaliyeti gerçek bir birey veya tüzel kişiye değil, anonim olarak bütün bir topluluğa aittir. Burada, mesele tüm bir topluluğun kendi üyeleri arasında işlem yapabilmesinde ve doğrulayabilmesinde, devlete ve bürokrasisine ihtiyaç olup olmayacağı tartışmaya açık bir husustur. Çünkü Blokzincirin yönetişimi (*Governance of Blockchain*) veya Blokzincirle yönetişim (*Governance by Blockchain*) konusu halen çok tartışmalıdır (DeFilippi ve Mcmullen, 2018; Beck vd., 2018). Yönetişimin Blokzincirde resmî veya gayri resmî şekilde olması; kurumsal, politik, kültürel, sosyal örgütlenmeler olmalarına göre değişebilmektedir. Hatta yönetişimin Blokzincir üzerinden mi, Blokzincir dışından mı, yoksa her ikisinin de aynı anda sağlanması mı gerektiği bile henüz netleşmemiştir. Her topluluğun geliştiricilerden başlamak üzere kendi amaçları için mutabakata, üzerinde fikir birliğine varılmış bir kurallar bütününe (bazıları meritokratik, bazıları da hiyerarşik olarak yapılandırılmış) bürokratik organizasyonlarla varması mümkündür.

2 Bakınız: BitNation (2019). "WhitePaper", https://tse.bitnation.co (11.07.2019)

3 Bakınız: The Government Network (2019). "Overview", http://thegovernment.network/overview (11.07.2019)

• Ağdaki düğümlerin devletler tarafından ele geçirilebilme olasılıkları: Bu durumda devletlerin kendi aralarında kamuya veya diğer ilgili taraflara yetersiz veya hiç uyarı vermeden birleşebilmeleri mümkündür.

• İş kanıtı yoluyla işlemleri doğrulayacak madencilerin sayısının maliyetler sebebiyle azalması: Ağdaki bilgiişlem gücü merkezîleşecektir. Elektrik sarfiyatı, donanım maliyeti, süreci yönetecek yazılımcının istihdamı üzerine iş kanıtıyla gelen yükler caydırıcı olabilecektir.

• Zincir'de kural kitabının kimlerin yazacağı, onları kim seçeceğinin açıkça belli olmaması: Altyapıdaki teknik unsurlar nedeniyle mevzunun teknik bilgi sahibi elitlerin yönetimine dönüşebilmesi mümkündür. Baskın halde ileri düzeyde teknoloji uzmanları seçkin bir grup yaratmaktadır. Blokzincir kod geliştiriciler fiili bir merkezi otoritedir ve bir Blokzincire kodlanmış eylemlerinin altında yatan kararlar işlemlerin kendisi kadar şeffaf olmayabilir.

Bu minvalde hem kamu teşkilatınca kamuyu ilgilendiren işlerin takibi sağlıklı olarak yapılabilecek, hem de bireylerin kamusal kayıtları kendi başlarına oluşturabilmeleri ve Blokzincire eklemeleri imkânı bireysel hakların kullanımını da destekleyebilecektir ki bu hizmetleri kişiselleştirerek sunmayı da mümkün kılacaktır. Kamu hizmetlerindeki bu dönüşümde "planlı, sistematik ve koordineli bir çalışma, güçlü bir iş birliği ve nitelikli insan kaynağına" gerek vardır (Tüfekçi ve Karahan, 2019: 187). Kamudaki dönüşüm vatandaşların edilgenlikten etkin olmaya geçişlerinde ciddi bir teşvik olacaktır. Ancak bireylerin tek tek bu imkânları kullanmaları bir konuyu kamu hizmeti olarak tespit edebilecekleri, tanımlayabilecekleri anlamına gelmeyecektir. Kamu hizmetinin ölçütlerini belirleme hususu süregelen kamu yönetimi anlayışının ve kamu hukukunun bile en muğlak konularından biridir (Derbil, 1950: 29). Bireylerin tek tek hizmetlere ulaşmaları, onlar baştan oluşturmaları veya birleştirmeleri vb. işlemleri yaparak merkezi siyasal iktidara etki etmesinin, baştan oluşturma manasında, kurucu iktidar düzeyinde olmayacağı, bu gelişmelerin devlet otoritesinin ortadan kalkmasıyla sonuçlanmayacağı değerlendirilmektedir. Özellikle yerinden yönetim ile şekillenmiş dijital platformların, siber-politik araçlar olmakla beraber geleneksel merkezi otoritelerin yerini alabileceği henüz doğrulanmamış olup bu yaygın ağda teknik gücü elde edecek yeni grupların baskın bir pozisyon edinmesiyle devlet toplumda gerekli eşgüdüm merkezi olma rolünü sürdürüleceği düşünülmektedir.

Sonuç

İnternet uzun bir süredir aracıları, komisyoncuları birer birer ortadan kaldırmakta ilk yıkıcılık örneğini vermeye başlamıştır. Örneğin bir mektubu muhatabına ulaştırmak için artık aracılara daha az ihtiyaç var. Bir şirketin sunucusundan ücretsiz edinilen bir posta kutusu, posta teşkilatının gerekliliğini azalttı. Ancak internetle elde edilen kazanımlar daha çok sosyal hayata ve iletişime yoğunlaşmış, ancak ni-

teliklerindeki sınırlılıklardan dolayı hem mali yapıdaki aracı kurumlara bağlılığın sürmesine hem de veri mahremiyetinin ihlaline engel olamamıştır. Buna çözüm getiren mevcut IP mimarisinin sınırlarını aşan bir anlayışla tanışmaya başladık: Blokzincir. Blokzincirle ağa katılmak değil, ağın bir parçasının sahibi olmak söz konusu olduğundan aracı kurumlara alternatifler artmaktadır. Bu, bireyler için önceki deneyimlerden olan katılımcılığın ötesinde bir hak ve aynı anda sorumluluk edinimidir. Yine Blokzincirle kişisel veri, tapulu bir arazini olabileceği kadar şüphesiz bir şekilde kişisel mülkiyettedir. Bu, 'dijital gölgenin' oluşturulmasını engelleyebilme becerisinin kazanımıdır. Bu ve benzeri şekillerde birinci elden yetkili olabilmek vatandaşlık bilincini de değiştirecektir. Daha önce yapıp etme gücünden yoksun kitlelerin doğrudan kamusallığı yapılandırmasında söz sahibi olması artık mümkündür.

Blokzincir, yazılım teknolojilerini belli bir protokolle, bir kural düzeniyle hayata uyarlamaktadır. Bu kural düzeni daha önce uygulamayan imkanları teknolojiyle mümkün kılmaktadır. Blokzincir siber uzamın imkânlarıyla gerçek hayatı zenginleştirecek, kalitesini arttıracak, güveni tesis edecek, demokrasiyi yaygınlaştıracak farklı değerlerin üretilmesi potansiyeli taşımaktadır.

Blokzincirin hayata daha çok dâhil olması; aracıları, örneğin bankaları, daha savunmasız ve daha az kârlı hale getirecek ama yok da etmeyecektir. Aynı durum kamu teşkilatı için de geçerlidir. Kamu yönetimi, kendi dışındaki yapıların kullandıkları veri protokolü Blokzincir mimarisine uyum sağlamalıdır. Bu uyumla birlikte Blokzincir, demokratik uzlaşmayı gözetmek şartıyla kamu yönetiminin kuralları uygulatma sürecini açık ve meşru kılabilecektir. Kamu yönetimi Blokzincir teknolojisinin hizmet süreçlerine nasıl dahil edebileceğine hızlıca odaklanmalıdır. Devletin daha etkin işleyişi amacına yönelik olarak, bu uyum süreciyse yalnızca nitelikli, iyi hazırlanmış bir kamu teşkilatıyla inşa edilebilecektir. Bu açıdan teşkilatlar yeni vizyonlarla kendilerini geliştirmeli, kamusal değer üretecek kamu yönetici ve memurları yetiştirmelidirler.

Örneğin tapu kayıtları Blokzincire bırakıldığında aracıların sayısı azaltılabilir, işlem yapan taraflara güven artabilir, süreci verimli ve daha düşük maliyetli kılabilir. Bu yapıya geçişte yapılacak yasal tespit, malvarlığının nesillerce kalıcılığını belirleyeceğinden çok önemlidir. Blokzincire geçilirken mal varlığının kime ait olduğunun tespiti hakkında itirazlar olacaktır. Anti-demokratik yönetimlerin haksız şekilde el koyduğu varlıklar olabilecektir. Bu sürecin, uluslararası standartlarda ve sürece hazırlıklı bir kamu teşkilatınca yapılması kritik önemdedir.

Blokzincir uygulamalarının ne resmî sorumluluk taşıyan ne de tüzel kişiliğe sahip yazılım geliştiricilerince yönetilen özel işlemlerle yürüdüğü idrak edilmelidir. Kamu düzenleyicilerin yaygın muhasebe sistemlerini yasalar aracılığıyla

düzenlemelerini zorlaştıracağı hesaba katılarak tedbir alınmalıdır. Yukarıda bahsi geçen Accenture gibi kurumsal oyuncular 'kod kitabının' yazılmasında söz sahibi olarak, şimdiden işleyişe dahil olmakta, yeni nesil aracılık yapısını şekillendirmektedirler. Kamu sektörü özellikle hukuk ve etik açısından düzenleyici rolü terk etmemek için mücadele göstermelidir. Tüm bu nedenlerle öncelikle daha fazla yazılımcı, kod geliştirici istidam edilmelidir. Kamu personelini yönetecek kamu yöneticilerine de kamusal değer üreten vizyonuyla eşzamanlı kullanılacak bir veri okuryazarlığı becerisi kazandırılmalıdır. Çünkü özellikle kodlama görevlerinde kaynakların verimli ve güvenli bir şekilde kullanılmasını temin için kamu kurumlarının temel bilgi seviyesini korumaları kritiktir. Her hâlükârda Blokzincirdeki kişisel verinin korunması, mutabakatla kamu yararına uygun kararların alınması devletin sorumluluğundadır. Özellikle bir devletin tüm vatandaşlarının, hatta uluslararası toplumun tüm kayıtlarının dâhil edilmesiyle büyüyen Blokzincirin nasıl yönetileceği sorusunun geleceği beklediği iddia edilirken geç kalınmalıdır. Şimdi kamu teşkilatından beklenti, hazırlıklarını yapıp güncel ve hukuki bir harmanı yakalamak için bir kamusal fayda üretmesidir.

Kaynakça

Akkoyunlu E.A., K. Ekanadham ve R.V. Hubert (1975). Some Constraints and Tradeoffs in The Design of Network Communications, *ACM SIGOPS Operating Systems Review*, 9(5), 67-74, https://dl.acm.org/citation.cfm?id=806523#citedby (17.05.2018)

Antonopoulos, A. (2014). *Bitcoin Security Model: Trust by Computation*, https://medium.com/@aantonop/bitcoin-security-model-trust-by-computation-d5b93a37da6e (14.10.2018)

Atzori M. (2017). Blockchain Technology and Decentralized Governance: is the State Still Necessary?. *Journal of Governance and Regulation,* 6(1), 45-62, http://dx.doi.org/10.22495/jgr_v6_i1_p5 (10.02.2018)

Augur (2019). *Define: Augur Protocol*, https://www.augur.net/faq/#define-augur-protocol (31.08.2018)

Baran, P. (1964). *On Distributed Communications, Memorandum RM-3420-PR*, California: RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf (11.10.2018)

Bauerle, N. (2018). *What is the Difference Between a Blockchain and a Database?*, https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database (13.12.2018)

Beck, R., C. Müller-Bloch ve J.L. King (2018). Governance in the Blockchain Economy, *Journal of the Association for Information Systems*, 19(10), 1020-1034, https://aisel.aisnet.org/jais/vol19/iss10/1/ (03.01.2019)

Belin, O. (2018). *The Difference Between Blockchain & Distributed Ledger Technology*, https://tradeix.com/distributed-ledger-technology/ (10.02.2019)

Berryhill, J., T. Bourgery ve A. Hanson (2018). Blockchains Unchained: Blockchain Technology and its Use in the Public Sector, *OECD Working Papers on Public Governance 28*, https://www.oecd-ilibrary.org/governance/blockchains-unchained_3c32c429-en (23.06.2019)

Blockchain.com (2019). *Charts.* https://www.blockchain.com/charts (21.07.2019)

Blokchain Technology in Publıc Service Presentation Accenture (2016). *Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems*, https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm (10.05.2019)

Bower, J.L. ve C.M. Christensen (1995). Disruptive Technologies: Catching the Wave, *Harvard Business Review*, 73(1): 43–53, https://hbsp.harvard.edu/ (17.12.2018)

Bruns, A. (2008). *Blogs, Wikipedia, Second Life, and Beyond: from Production to Produsage*, New York: Peter Lang Inc.

Cointelegraph (2019). *WEF Head of Blockchain Sheila Warren This Tech Can Solve the Trust Crisis,* https://cointelegraph.com/news/wef-head-of-blockchain-sheila-warren-this-tech-can-solve-the-trust-crisis (01.04.2019)

De Vries, A. (2018). Bitcoin's Growing Energy Problem, *Joule*, 2(5), 801-805, https://www.cell.com/action/showPdf?pii=S2542-4351%2818%2930177-6 (15.05.2019)

DeFilippi, P. ve G. McMullen (2018). Governance of Blockchain Systems. *Blockchain Research Institute and COALA*, https://hal.archives-ouvertes.fr/hal-02046787/document (02.03.2019)

Deloitte (2018). *2018 Global Blockchain Survey*, https://www2.deloitte.com/tr/tr/pages/financial-services/articles/2018-global-blockchain-survey.html (21.02.2019)

Derbil, S. (1950). Kamu Hizmeti Nedir? *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 7(3), 29–36, http://dergiler.ankara.edu.tr/dergiler/38/248/2245.pdf (21.06.2019)

Digiconomist (2019). *Bitcoin Energy Consumption Index*, https://digiconomist.net/bitcoin-energy-consumption (12.01.2019)

Durukal, O. ve N.K. Öztürk (2019). Kamusal Hizmet Sunumunda Blokchain Teknolojisi, *EKEV Akademi Dergisi*, 23(77), 449-456, http://www.ekevakademi.org/DergiDosyalar/332571370_00%20KUNYE%20(77).pdf, (14.11.2019)

Dwork, C. ve M. Naor (1992). *Pricing via processing or combatting junk mail*, *Advances in Cryptology – CRYPTO'92*, 139–147https://dl.acm.org/citation.cfm?id=705669 (21.01.2019)

E-Estonia (2016). *Guardtime Secures Estonian Health Records*, https://e-estonia.com/guardtime-secures-estonian-health-records/ (03.06.2019)

Everledger (2019). *Industry Applications*, https://www.everledger.io/industry-applications (31.08.2019)

Forbes (2017). *Dubai Sets Its Sights on Becoming the World's First Blockchain-Powered Government*. https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#18d9a27a454b (22.12.2018)

Future Thinkers (2017). *19 Industries The Blockchain Will Disrupt*, https://futurethinkers.org/industries-blockchain-disrupt/ (15.05.2019)

Georgian Prime Minister's Press Office (2019). "*Mamuka Bakhtadze: Plots Registered under Land Registration Reform Make up over 300,000 Hectares"*, http://gov.ge/index.php?lang_id=ENG&sec_id=526&info_id=70040 (10.07.2019)

Gupta, M. (2017). *Blockchain-IBM Limited Edition,* New Jersey: John Wiley & Sons, Inc., https://www.ibm.com/tr-tr/blockchain/what-is-blockchain (03.02.2019)

Guthrie, W.K.C. (2011). *Yunan Felsefe Tarihi-I*, İstanbul: Kabalcı

Güven, V. ve E. Şahinöz (2018). *Blokzincir, Kripto Paralar, Bitcoin*, (2. Baskı). İstanbul: Kronik

HM Land Registry (2019). *"HM Land Registry to Explore the Benefits of Blockchain",* https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain, (10.07.2019)

Houben, R. ve A. Snyers (2018). *Cryptocurrencies and Blockchain*, EU Publications, http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (27.02.2019)

IBM (2018). *Blockchain and GDPR (White Paper)*, https://iapp.org/media/pdf/resource_center/blockchain_and_gdpr.pdf (20.04.2019)

Jakobsson, M. ve A. Juels (1999). Proofs of Work and Bread Pudding Protocols (Extended Abstract)*,* Preneel B. (eds) Secure Information Networks. *The International Federation for Information Processing*, Vol: 23. Boston: Springer, 258-272, https://link.springer.com/chapter/10.1007/978-0-387-35568-9_18#citeas (20.10.2018)

Kar, I. (2016). *The Latest Customers for the Technology Behind Bitcoin are NATO and the U.S. Military, Quartz*, https://qz.com/681580/the-latest-customers-for-the-technology-behind-bitcoin-are-nato-and-the-us-military/ (21.03.2018)

Karahan, Ç. ve A. Tüfekçi (2019). Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen

Hizmetlerde Blokzincirin Kullanım Durumu. *Verimlilik Dergisi*, (4), 157-193, https://dergipark.org.tr/tr/pub/verimlilik/issue/49238/444617 (14.11.2019)

Kerr, Z. (2018). *It Only Costs $531 to Mine One BTC if You Live in Venezuela: Bitcoin Mining Around the World*. https://mineable.com/it-only-costs-531-to-mine-one-btc-if-you-live-in-venezuela-bitcoin-mining-around-the-world/ (27.01.2019)

Lamport, L., R. Shostak and M. Pease (1982). The Byzantine Generals Problem, *ACM TOPLAS,* 4(3), 382-401, https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf (12.10. 2018)

Lantmateriet (2018). *"Block chain tested live-can save billions for home buyers and mortgage customers",* https://www.lantmateriet.se/en/nyheter-och-press/nyheter/2018/blockkedjan-testad-live--kan-spara-miljarder-at-bostadskopare-och-bolanekunder/ (10.07.2019)

Lemieux, V., D. Flores, ve C. Lacombe (2017). "*Title and code: Real Estate Transaction Recording in the Blockchain in Brazil",* https://www.researchgate.net/publication/322665512_Title_and_code_Real_Estate_Transaction_Recording_in_the_Blockchain_in_Brazil_RCPLAC-01-Case_Study_1_Document_Control_Version_history_Version_Date_By_Version_notes (10.07.2019)

Lessig, L. (2000). Code is Law: On Liberty in Cyberspace, *Harvard Magazine*, https://harvardmagazine.com/2000/01/code-is-law-html (12.10. 2018)

Lightning Network (2019). *The Bitcoin Lightning Network*, https://lightning.network/lightning-network-summary.pdf (13.02.2019)

Lyons, T., L. Courcelas ve K. Timsit (2018). Blockchain for Government and Public Services, *The EU Blockchain Observatory & Forum Publication*, https://dutchblockchaincoalition.org/uploads/pdf/eu-observatory-blockchain-in-government-services.pdf (24.02.2019)

Malone, T.W. (2004). The Future of Work How the New Order of Business Will Shape Your Organization, *Your Management Style, and Your Life*. Boston: Harvard Business School

Nakamoto, S. (2008). *Bitcoin a Peer-to-Peer Electronic Cash System,* https://bitcoin.org/bitcoin.pdf (10.12.2018)

Narayanan, A. ve J. Clark (2017). Bitcoin's Academic Pedigree, *Queue*, 15(4) 36-45, https://dl.acm.org/citation.cfm?id=3136559 (17.12. 2018)

Narayanan, A., J. Bonneau, E. Felten, A. Miller ve S. Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, New Jersey: Princeton

University

Nomura Research Institute (2019). *"Survey on Blockchain Technologies and Related Services FY2015 Report",* Tokyo: Japan's Ministry of Economy, https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf, (10.07.2019)

Ølnes S. ve A. Jansen (2017). Blockchain Technology as Support Infrastructure in e-Government, *Janssen M. et al. (eds) Electronic Government, EGOV 2017 Lecture Notes in Computer Science*, Vol: 10428, Switzerland: Cham, Springer, 215-227, http://link.springer.com/10.1007/978-3-319-64677-0_18 (07.08.2018)

OpenBazaar (2016). *What is OpenBazaar?* https://openbazaar.zendesk.com/hc/en-us/articles/208020193-What-is-OpenBazaar- (23.12.2018)

Oprunenco A. ve C. Akmeemana (2019). *"Using Blockchain to Make Land Registry More Reliable in India"* https://blogs.lse.ac.uk/businessreview/2018/04/13/using-blockchain-to-make-land-registry-more-reliable-in-india/ (10.07.2019)

Provenance (2016). *From Shore to Plate: Tracking Tuna on the Blockchain*, https://www.provenance.org/tracking-tuna-on-the-blockchain (03.02.2019)

Ramathal, N. V. ve K. B. Greene (2019). *Hardware Blockchain Corrective Consensus Operating Procedure Enforcement, U.S. Patent No: 10291413*, http://patft.uspto.gov/netahtml/PTO/srchnum.htm (20.04.2019)

Rosreestr (2018). "*Pilot Project For Registering D.D.U."*, https://rosreestr.ru/site/press/news/rosreestr-predstavil-na-vsemirnom-sammite-blokcheyna-i-kriptovalyut-pilotnyy-proekt-po-registratsii-/?sphrase_id=15809286 (10.07.2019)

Safahi, A. (2018). *ZED Global Platform for Money Transfer Operators (MTOs)*. Toronto: ZED Network Inc., https://assets.ctfassets.net/xwo28v1qbyr0/1kHadIdBOY6UOSku8Ag80Y/476b77be54b9d28405bf0fadf8ac0a36/ZED_Investor_Presentation_-_Final.pdf (21.09.2018)

Symantec, (2018). *Smartphone, Blockchain Voting Technologies to Get Big Test This Fall*, https://www.symantec.com/blogs/election-security/smartphone-blockchain-voting-technologies-get-big-test-fall (17.12.2018)

Szabo, N. (1994). *Smart Contracts*, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (12.12.2018)

Tapscott, D. ve A.D. Williams (2006). *Wikinomics: How Mass Collaboration Changes Everything*, New York: Portfolio.

Tecnopedia (2019a). *Definition: What Does Node Mean?*, https://www.techopedia.com/definition/5307/node (15.05.2019)

Tecnopedia (2019b). *Definition: What Does BotNet Mean?*, https://www.techopedia.com/definition/384/botnet (11.04.2019)

Transparencia Mexicana (2011). *Indice Nacional deCorrupción y Buen Gobierno 2010, Mexico City*, https://www.tm.org.mx/wp-content/uploads/2013/05/01-INCBG-2010-Informe-Ejecutivo1.pdf (01.05.2019)

Transparency International (TI) (2011). *Corruption in the Land Sector (Working paper 04/2011)*, www.fao.org/docrep/014 /am943e/am943e00.pdf (01.05.2019)

Transparency International (TI) Bangladesh (2012). C*orruption in Service Sectors: National Household Survey 2012*, https://www.ti-bangladesh.org/files/HHSurvey-Exec-Sum-Eng-fin.pdf (01.05.2019)

Transparency International (TI) India (2005). *TII-CMS India Corruption Study 2005: With Focus on BPL Households*, www.transparencyindia.org/resource/survey_study/India%20 Corruption%20Study%202005.pdf (01.05.2019)

Transparency International (TI) Kenya (2011). *East African Bribery Index 2011*, https://tikenya.org/wp-content/uploads/2017/08/TI-Kenya_East-African-Bribery-Index-2011.pdf (01.05.2019)

Ujo Music (2018). *Frequently Asked Questions*, https://www.ujomusic.com/faq (23.12.2018)

Usta A. ve Doğantekin S., (2017). *Blockchain 101*, İstanbul: Kapital Medya

Warner, M. (2018). *General Election: A Huge Success for West Virginia*, https://sos.wv.gov/news/Pages/11-15-2018-A.aspx (17.12.2018)

World Bank (2018). *Identification for Development (ID4D)-2018* (Annual Report), https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018_ID4D_Annual_Report.pdf (30.01.2019)

World Economic Forum (WEF) (2018). *Building Block(chain)s for a Better Planet*, http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf (12.01.2019)

Yıldırım, H. (2018). Açık ve Uzaktan Öğrenmede Blokzincir Teknolojisinin Kullanımı. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi,* 4(3), 142-153

EK: Okuma Listesi (Kronolojik)

Merkle, R. C. (1980). Protocols for public key cryptosystems. *IEEE Symposium on Security and Privacy*, http://www.merkle.com/papers/Protocols.pdf

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* 24(2): 84-90. https://dl.acm.org/citation.cfm?id=358563

Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology*, 199-203. https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF

Chaum, D. (1985). Security without identification: transaction systems to make Big Brother obsolete. *Communications of the ACM* 28(10), 1030-1044. https://dl.acm.org/citation.cfm?id=4373

Lamport, L. (1989). *The part-time parliament*. (Report), Digital Equipment Corporation. https://computerarchive.org/files/mirror/www.bitsavers.org/pdf/dec/tech_reports/SRC-RR-49.pdf

Bayer, D., Haber, S., Stornetta, W. S. (1991). Improving the efficiency and reliability of digital time-stamping. *Proceedings of Sequences*. https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24

Haber, S., Stornetta, W. S. (1991). How to Time-Stamp a Digital Document, *Journal of Cryptology*, 3(2), 99-112. https://www.anf.es/pdf/Haber_Stornetta.pdf

Benaloh, J., De Mare, M. (1991). *Efficient broadcast time-stamping*. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.38.9199

Dwork, C., Naor, M. (1992). *Pricing via processing or combatting junk mail*. https://dl.acm.org/citation.cfm?id=705669

Szabo, N. (1994). *Smart contracts.* http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Rivest, R. L., Shamir, A. (1996). PayWord and MicroMint: Two simple micropayment schemes. *International Workshop on Security Protocols.* https://people.csail.mit.edu/rivest/RivestShamir-mpay.pdf

Back, A. (1997). *Apartial hash collision based postage scheme*. http://www.hashcash.org/papers/announce.txt

Haber, S., Stornetta, W. S. (1997). Secure names for bit-strings. *Proceedings of the 4th ACM Conference on Computer and Communications Security*: 28-35. http://dl.acm.org/citation.cfm?id=266430

Dai, W. (1998). *B-Money.* http://www.weidai.com/bmoney.txt

Castro, M., Liskov, B. (1999). PracticalByzantinefault tolerance. *Proceedings of the Third Symposium on Operating Systems Design and Implementation.* http://pmg.csail.mit.edu/papers/osdi99.pdf

Juels, A., Brainard, J. (1999). Client puzzles: a cryptographic counter measure against

connection completion attacks. *Proceedings of Networks and Distributed Security Systems*: 151-165. https://www.isoc.org/isoc/conferences/dss/99/proceedings/papers/juels.pdf

Goldberg, I. (2000). *A pseudonymous communications infrastructure for the Internet* (Ph.D. Dissertation), University of California Berkeley. http://moria.freehaven.net/anonbib/cache/ian-thesis.pdf

Lamport, L. (2001). Paxos made simple; http://lamport.azurewebsites.net/pubs/paxos-simple.pdf

Douceur, J. R. (2002). *the Sybil attack*. https://dl.acm.org/citation.cfm?id=687813

Aspnes, J., Jackson, C., Krishnamurthy, A. (2005). *Exposing computationally challenged Byzantine imposters* (Report). Yale University, http://cs.yale.edu/publications/techreports/tr1332.pdf

Szabo, N. (2008). Bit gold. https://unenumerated.blogspot.com/2005/12/bit-gold.html

Nakamoto, S. (2008). *Bitcoin: a peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Blankstein, A., Bonneau, J., Felten, E. W., Freedman, M. J. (2015). CONIKS: Bringing key transparency to end users. *Proceedings of the 24th Usenix Security Symposium*. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-melara.pdf