

Kamu Mali Denetiminin Dijitalleşmesi: Blokzincir Teknolojisinin İncelenmesi

(Araştırma Makalesi)

Digitalization of Public Financial Audit: A Review of Blockchain Technology

Doi: 10.29023/alanyaakademik.1095833

Abdulkerim EROĞLU

Dr., Recep Tayyip Erdoğan Üniversitesi İ.İ.B.F. Maliye Bölümü

kerym.eroglu@gmail.com

Orcid No: 0000-0003-2680-8844

Bu makaleye atıfta bulunmak için: Eroğlu, A. (2023). Kamu Mali Denetiminin Dijitalleşmesi: Blokzincir Teknolojisinin İncelenmesi. Alanya Akademik Bakış, 7(1), Sayfa No.187-207.

ÖZET

Anahtar kelimeler:
Mali Denetim,
Blokzincir Teknolojisi,
Akıllı Sözleşmeler,
Hesap Verilebilirlik

Makale Geliş Tarihi:
30.03.2022
Kabul Tarihi:
23.11.2022

Mevcut internet teknolojisinin kullanım yöntemi birtakım riskler barındırmaktadır. Merkezi bir yapıda yapılandırılan uygulamalar siber saldırılara karşı savunmasız kalabilmektedir. Benzer şekilde bireysel hatalar da önemli veri sorunlarına yol açabilmektedir. Bu bağlamda blokzincir teknolojisi, merkezi olmayan dağıtık kayıt yöntemi ve kendine özgü işleyen süreci ile oldukça yenilikçi bir gelişme olarak kabul edilmektedir. Barındırdığı potansiyel, devlet kurumlarının da dikkatini çekmiş ve sınırlı düzeyde bazı girişimler yapılmıştır. Çalışmanın amacı bu kapsamda blokzincir teknolojisinin kamu mali denetiminde nasıl ele alınabileceğinin araştırılmasıdır. Zira yolsuzluk, kamu gücünün kötüye kullanımı, kamu hesaplarının şeffaf olmaması ve denetimde meydana gelen aksaklıklar konunun yenilikçi teknolojilerle çözümünü gündeme getirmektedir. Birçok ülkede görülen bu tür sorunların çözümü ile kamu kaynakların tahsisatında etkinliğin sağlanması, yolsuzlukların önlenmesi, yetki ve takdir sınırlarını belirleyen hesap verilebilirliğin güçlendirilmesi gibi olumlu sonuçların doğumuna katkı sağlanacaktır.

Keywords:

Public Financial Audit,
Blockchain Technology,
Smart Contracts,
Accountability

ABSTRACT

The way of using the current internet technology has some risks. Applications configured in a centralized structure can be vulnerable to cyber attacks, and personal errors can cause data significant problems. In this context, blockchain technology is considered to be a highly innovative development with its decentralized distributed registration method and its unique functioning process. The potential it holds that attracted the attention of government agencies, and some attempts have been made at limited level. In this context, the aim of the study is to explore how blockchain technology can be handled in public financial audit. Because corruption, abuse of public power, the lack of transparency of public accounts, and the administrative disruptions in the audit bring the solution of the issue to the agenda with innovative technologies. The solution of such problems seen in many countries will contribute to the realization of positive results such as ensuring efficiency in the allocation of public resources, preventing corruption, strengthening accountability that determines the limits of authority and discretion.

1. GİRİŞ

Blokzincir teknolojisinin genel anlamda öne çıkan özelliği merkezi olmayan dağıtık kayıt yöntemidir. Adem-i merkezilik olarak da ifade edilebilecek bu özellik, merkezi otoritelere güvenin olmadığı veya güvenin olmasıyla birlikte denetim mekanizmasının politik etkilerden korunmasını gerektirdiği durumlarda ön plana çıkmaktadır. Nitekim kamu kurumları geleneksel yöntemlerle birlikte bilgisayar ve internet imkanlarından faydalanmaya başlamışsa da bu süreçte farklı riskler ortaya çıkmıştır. Örneğin tüm kamu harcamalarının denetiminin tek bir sunucuda kayıt altında tutulması veya bunların tek taraflı müdahalelere açık olması, kamusal hesap verilebilirliğin ve mali denetimin zedelenmesine yol açacaktır. Diğer taraftan bazı hukuki düzenlemeler başkaca sorunlara yol açabilmektedir. Örneğin, hukuki bir düzenleme ile raporların elektronik ortamda belli bir süre müddetince saklanması zorunlu kılınsa bile, bu sürenin sonunda ne olacağının belirsiz bırakılması sorun teşkil edebilir. Benzer bir başka sorun ise kamu hesap denetimlerinin devam ederken hukuki mecburiyet olarak raporların hazırlanması gereğidir. Bu tür zamansal sorunlarda, rapor hazırlandıktan sonra denetim devam etmekte ve ancak bulgular hazırlanan rapora eklenemebilmektedir. Raporun tamamlanmasıyla birlikte rapor bulgularından hareketle sürdürülen soruşturmalar ve bunların sonuçları raporlardan izlenememektedir. Dolayısıyla mutlak manada bir denetim raporu hazırlansa dahi bunun öncesinin izlenmesi veya daha sonrasında ortaya çıkan gelişmelerin takibi zor olmaktadır. Blokzincirin kendisine has dağıtık yapısı ve blokların değiştirilemez bir şekilde* birbirlerine eklenmesi anılan birçok soruna yönelik önemli çözümler getirebilmektedir.

Yakın tarihteki gelişmeler kapsamında blokzincir teknolojisinin kullanımı incelendiğinde, yasama, yürütme ve yargıyı (hesap yargısı olarak yüksek denetim kurumları dahil) kapsayacak şekilde devlet aygıtının bütünüyle güven yitirmesi veya mevcut geleneksel sistemlerin pahalılığı ve düşük verimliliği bu teknolojinin kullanımında etkin faktörler olarak dikkat çekmektedir. Dolayısıyla neden olan faktörler göz ardı edilerek blokzincir teknolojisinin yadsınması olumlu sonuçlar doğurmayacaktır. Zira piyasa işleyişi etkin, güvenilir ve düşük maliyetli olana yönelme eğilimi gösterir.

Devletlerin blokzincir konusunda bir uyum sürecine girmesi hem kamusal işlerde etkinliğin sağlanması hem de piyasada oluşabilecek sorunlarda veya standartların takibinde/belirlenmesinde (Hagan, 2019: 101) düzenleyici rolünü alması bakımından önem taşımaktadır. Zira merkezi bir otorite (ve bu otoriteden alınacak bir izin) olmaksızın blokzincir teknolojisi üzerinden sürdürülecek faaliyetlerin ihtilaflara yol açması söz konusu olabilecektir. Örneğin, akıllı sözleşmeye bağlı bir işlemin sonucunda, asimetrik bilgi sorunu nedeniyle bir tarafın “sözleşme protokolü” tamamlandıktan sonra mağdur olması söz konusu olduğunda, sorunun yasal mahkemelerde çözülmesi gerekecektir. Böyle bir sorun hem piyasa ekonomisindeki aktörler (alıcı-satıcı) arasında hem de kamusal mal ve hizmet temini sırasında ortaya çıkabilir.

Blokzincir teknolojisi bir vergi güvenlik müessesesi olarak da kullanılabilir. Mükelleflere ait geçmişe dönük vergisel işlemlerin kaynağına kadar takip edilebilmesi ile bu teknoloji hem mükellef için vergi planlama aracı olarak hem de vergi dairesi için inceleme aracı olarak kullanılabilir. Böylelikle kamusal yetkinin suiistimal edilmesinin ve mükelleflerin vergi

* Bir işlemin gerçekleştiği bloktan sonra işlem itibarıyla değiştirilemez. Örneğin bir işlem 10. blokta gerçekleşirse ve ardından 6 işlem daha yapılırsa (16. bloğa gelindiğinde) 10. blokta yer alan işlemler değiştirilemez. Bu durum 1 blok öncesindeki tüm işlemler için geçerlidir (Gates, 2017: 7).

ziyana yol açabilecek davranışlarının kısmen engellenmesi mümkün hale getirilebilir. Burada, akıllı sözleşmelerden yararlanılarak “*akıllı beyanname*” uygulaması geliştirilebilir. Blokzincir teknolojisinin bu alanda kullanılmasının bir diğer avantajı adil vergileme anlayışına yapacağı katkıdır. Zira hazırlanacak protokolün herkes tarafından okunabilir olması ve şartların tüm mükellefler için eşit sonuç doğurması şeklinde kurgulanmasıyla, belli çıkar grupları lehine vergisel imtiyazların sağlanmasının önüne geçilebilecektir.

Blokzincir teknolojisinin kullanımında sağlanabilecek bir diğer kazanım uluslararası vergilemede etkinliktir. Özellikle işletmeler arası yurtdışı ticarete, varış ülkesi prensibinin benimsendiği satış vergilerinde, vergi kaçakçılığına yol açacak çok sayıda yöntemin varlığı vergi gelirlerinin tahminin altında olmasına yol açmaktadır (Allessie, Sobolewski ve Vaccari, 2019: 78). Böyle bir sorunla mücadelede blokzincir teknolojisinin kullanılması *ülkelerarası blokzincir* uygulamalarının benimsenmesini gerektirebilir.

Teknoloji araç kılına olarak regülasyonların getirilmesi veya akıllı sözleşmelerde olduğu gibi, hukuki/iktisadi sürecin işletilmesi fikri blokzincir teknolojisinin ortaya çıkmasından öncesine dayanmaktadır. Örneğin, Lessig “Code: Version 2.0” isimli çalışmasında, kodu kanun olarak tanımlar (*code is law*). Çalışmasında vurguladığı husus, siber alemin (cyberspace) anarşi değil düzen sağlamak amacıyla kullanılabileceğidir. Anayasalar, kanunlar ve daha alttaki normlar aslında gerçek dünyadaki hukuki kodlardır (Lessig, 2006: 5). Yasa düzenleyici olan kodun[†] dolaylı etkisi, kanun yaptırımını güçlendirmek ve böylelikle kanunun yaptırımını konusunda kod tabanlı sınırlamalar getirmektir (Lessig, 2006: 64). Bu yönüyle değerlendirildiğinde, blokzincir tabanlı uygulamaların herhangi bir aracıya ihtiyaç olmadan gerçek dünyadaki işlemlerin yürütülebilmesine imkan sağlaması, bunları hukuki kodlar olarak tanımlamayı mümkün kılar.

Blokzincir teknolojisi piyasa ve kamu sektörü geleneksel iş modelleri için yıkıcı değil, kurucu niteliği olan bir teknolojidir. Ekonomik ve sosyal sistemler için temeller oluşturması dolayısıyla etkisi büyük olacağı gibi mevcut yapının içine girmesi de uzun vadede gerçekleşecektir (Iansiti ve Lakhani, 2017: 122). Bununla birlikte, blokzincir teknolojisi resmi devlet kurumları, sivil örgütler, medya veya özel girişimler düzeyinde çeşitli vesilelerle kullanılmaya başlanmıştır. Hükümetler para arzı, oylama, devlet yardımlarının dağıtılması ve vergi toplama gibi merkezi devlet fonksiyonları konusunda bu teknolojinin nasıl kullanılabileceğini araştırmaktadır (Shrier, 2020: 98).

Çalışmanın birinci kısmında blokzincir teknolojisi tanıtılmakta ve teknik yapısı ile kamusal karar verme süreci arasındaki ilişkisi incelenmektedir. İkinci kısımda blokzincirin önemli bir ürünü olan akıllı sözleşmeler ele alınmakta ve bunların kamusal niteliği tartışılmaktadır. Üçüncü kısımda blokzincir teknolojisinin kamusal örnekleri incelenmektedir. Son kısımda ise mali denetim kapsamında blokzincir teknolojisinin kullanılabilirliği değerlendirilmektedir.

2. BLOKZİNCİR TEKNOLOJİSİ

2.1. Kavramsal Boyut

Blokzincir; bilgisayarlar tarafından meydana getirilen bir ağla kaydedilen işlemlerin yer aldığı defter-i kebir (ledger) veya kronolojik veri tabanı olarak tanımlanabilir. Blokzincir terimi, bu işlemlerin bloklar halinde gruplandırılmasını ifade eder ve bu blok zinciri; blok zincirinin başlangıcından bu yana kabul edilen [onaylanan] işlem geçmişini oluşturur. Böyle bir blok

[†] Yazar burada bilişim/internet alanındaki gelişmeleri düzenleyecek bir kodun, düzen sağlamaya yönelik getirilen bir yasa gibi işlevsel olacağına göndermek yapmaktadır.

zincirinde herkes kendi özel şifreleme anahtarı ile imzaladığı yeni bir kayıt veya değişiklikle blok zinciri defterine güncelleme sağlayabilir (Peters ve Panayi, 2016: 241).

Blokszincir kavramı ilk olarak Satoshi Nakamoto tarafından kaleme alınan “Bitcoin: A Peer-to-Peer Electronic Cash System” isimli çalışmada kullanılmıştır. Nakamoto, blokszinciri; yapılan her işleme ait bilginin ağdaki katılımcılar tarafından kaydedildiği ve paylaşıldığı dağıtılmış bir veri yapısı olarak tanımlamaktadır[‡] (Tanrıverdi, Uysal ve Üstündağ, 2019: 204). Geleneksel veri tabanları ile blokszincir arasındaki temel fark; blokszincirin yeni kayıt ekleme, bilgilerin doğrulanması ve dağıtılması işlemleri için (peer-to-peer) P2P ağı üzerinde mutabakat kurallarına dayalı çözümler sunan geliştirilmiş bir veri tabanı olması olarak gösterilmesidir (Tanrıverdi, Uysal ve Üstündağ, 2019: 204).

Blokszincir teknolojisine benzer fikirlere dayanan ve sanal paraların oluşturulmasına yönelik olan girişimler 1980’ler, 1990’lar ve 2000’li yıllarında başında denenmiş veya bir fikir olarak ileri sürülmüştür. Ancak fikirler güçlü bilgisayar desteğinden ve güvenlikten mahrum olmaları dolayısıyla başarısızlıkla sonuçlanmıştır. Nakamoto’nun getirdiği fikir ise işlemleri her on dakikada bir blok halinde birleştiren düğümlerle[§] (node) sürekli büyüyen blokszincir ile düğümlerin sisteme katılım hakkını elde ettiği iş kanıtı mekanizmasını (proof of work) merkezi olmayan bir protokolle birleştirmek olmuştur. Böylelikle bilgisayar gücü artırılarak oransal olarak daha büyük etki meydana getirilmiştir. Bu da daha önceki fikirlerde meydana gelebilen, örneğin bir saldırganın bir sunuda veya botnet ile binlerce simüle edilmiş düğüm oluşturabilmesi^{**} gibi güvenlik sorunlarına çözüm getirmiştir (Buterin, 2014: 3).

İş kanıtı ilk defa 1996 yılında kriptograf Adam Back tarafından test edilmiştir. Back, istenmeyen elektronik postalara (junk e-mail) karşı iş kanıtı mekanizmasını oluşturmuştur. Böylelikle bir elektronik postanın üzerinde ne kadar uğraşıldığı ve ne kadar sürede hazırlandığına göre gelen kutusuna girmesi öngörülmüştü. Dolayısıyla spam posta gönderenler, bu postaların ulaşılabilmesi için normal bir posta şeklinde zaman harcayarak hazırlamaları gerekmiştir. Ancak bu dönemde spam posta sayısının ve genel olarak elektronik posta kullananların görece az olması bu sistemin yaygınlaşmasına engel olmuştur (Wang, 2018:17).

Blokszincir temelde izinsiz/izin gerektirmeyen (permissionless) blokszincir ve izinli/izin gerektiren (permissioned) blokszincir olarak iki kategoriye; izinli blokszincir de kendi içinde herkese açık (public) blokszincir ve özel (private) blokszincir olarak iki alt kategoriye ayrılmaktadır. Herkese açık blokszincirde herkes blokszincir işlemlerine başvurabilir ve bunları okuyabilirken özel blokszincirde bu izin kuruluş veya kuruluş grubu içindeki kullanıcılarla sınırlıdır (Peters ve Panayi, 2016: 243).

Sınıflandırmada karma bir yöntem olarak konsorsiyum blokszincir kategorisi de bulunmaktadır. Bu kategoride doğrulama ve uzlaşma işlemlerinde karar vericiler önceden belirlenmiş bir gruptur. Blok doğrulaması bir bloğun sadece yetkili düğümler tarafından imzalanması (çoklu

[‡] Bu bakımdan blokszincir teknolojisinin ilk uygulaması Bitcoin’dir (Chai ve Zhu, 2016: 4).

[§] Düğüm, ağı (network) oluşturmak için diğer düğümlerle etkileşime giren ağın ayrı üyesidir. Bir düğüm, blokszincir uygulamasını çalıştıran ve bütün blokszinciri depolayan herhangi bir bilgisayardır. Düğümler ağdaki eşler (peer) arasında yeni bloklar talep eder, bunları doğrular ve yayınlara. Düğümlerin uyumlu yazılımı çalıştırmaları durumunda konsensüs sağlanmış olur. Bu sebeple düğüm sayısının çok olması, ağın kötü niyetli veya rastgele kaynak kodu değişikliklerinden, tekrarlayan düzenlemelerden ve diğer protokol değişikliklerinden korunması bakımından çok önemlidir (River Financial, 2021).

^{**} Blokszincirin uzunluğu en geniş işlemci (CPU) havuzundan gelir. Dolayısıyla düğümler tarafından kontrol edilen işlemci gücünün büyük kısmı ağa saldırmak üzere işbirliği yapmadıkları müddetçe zincir uzayacak ve saldırganlara engel olunacaktır (Mougayar, 2016: 3).

imza şeması) ile geçerli olabilmektedir. Ağın herkese açık mı olacağı veya sınırlı mı olacağına; ağda kimlerin veri okuma ve yazma işlemi yapabileceğine konsorsiyum tarafından karar verilir. Blokzincirler herkes tarafından okumaya açık olabileceği gibi sınırlandırılmış da olabilir. Ancak konsensüs işleminin tamamlanması için salt çoğunluğu oluşturan düğümlerin onayı aranabildiği gibi önceden belirlenen çoğunluk şartı getirilebilir. Örneğin 10 katılımcı/düğüm varsa bunların 7'sinin veya 6'sının onayını gerektiren bir kural getirilebilir (Bambara ve Allen, 2018: 14, 174).

İzinli blokzincirde katkı sağlayanlar izne bağlı olanlar iken kayıtların izlenebilmesi herkese açık hale getirilebilir. Burada genellikle “*yetki kanıtı*” (Proof of Authority - PoA) yöntemi kullanılmaktadır. PoA yönteminde kullanıcı kimliklerinin bilinmesi ve onaylanması gerekmektedir. Ayrıca yeni bloklar kullanıcı izni ile dikte edilerek yayımlanabilmektedir (OECD, 2018). Bu bağlamda blokzincirin yapısı ve türleri göz önüne alındığında, kamu sektörü için kullanışlı olanın izinli blokzincir olacağı ifade edilebilir.

Çalışmanın konusu itibarıyla önem taşıdığı düşünülen izinli-özel blokzincirin faydaları ise şunlardır (Bambara ve Allen, 2018: 175):

- Okuma izni sağlanması durumunda özel (private) bir blokzincir gizliliği sağlar. Bu husus okuma iznine sahip olanlar ile hem okuma hem doğrulama/onaylama yetkisine sahip olanların farklı kişiler/düğümler olabileceği anlamına gelir.
- Konsorsiyum veya özel kuruluş, bir blokzincirin kurallarını değiştirerek işlemleri geri almalarına, bakiyelerini değiştirmelerine (düzeltmelerine) vb. izin verebilir. Bu daha ziyade kusurlu işlevselliği düzeltmek için hazırlanan yamalar (patches) kapsamında olur.
- Madencilerin veya doğrulayıcıların kimlikleri bilinir, tanımlanır ve tanınırlar. Bu nedenle kötü aktörlerin gizli anlaşmalarından kaynaklanan yüzde 51'lik saldırı riski bulunmaz veya olsa dahi kolaylıkla tanımlanarak bunlara müdahale edilir.
- H herkese açık (public) ağdaki her düğüm yerine yalnızca sınırlı sayıda güvenilir ve tanımlanmış düğüm tarafından doğrulanmaları gerektiğinden işlemler daha ucuzdur. Herhangi bir işlem ücreti olması gerekmez. Doğrulayıcı bir düğüm çalıştırmak gerekli olsa bile halka açık ağlara kıyasla düşük bir işlem ücreti yeterli olacaktır. Doğrulayıcı düğüm, dağıtık hizmet reddi (Distributed Denial of Service – DDoS) saldırılarına karşı koruma sağlayabilir.
- Konsensüs daha küçük bir grup arasında çok daha hızlı elde edilebilir.

2.2. Teknik Boyut ve Kamusal Karar Verme Süreci

Oyun teorisi kapsamında değerlendirilen Bizanslı Generaller Problemi^{††} (Byzantine Generals Problem) blokzincir teknolojisinin getirdiği çözümle “güven” çerçevesinde ele alınmaktadır. Tarihte kullanılagelen “para” Bizanslı Generaller Probleminin en önemli örneğini oluşturmaktadır. İşlevini yitirdiği döneme kadar altın gibi uluslararası ticarete kabul gören metallere sonra devletler tarafından basılan kağıt paralar tamamen o devletin [merkezi hükümet veya merkez bankasının] otoritesine dayanmıştır. Ancak burada önemli sorun bu otoriteye neden güvenileceği konusundadır. Çünkü bu otoriteler paranın değerini düşürebilme veya sınır olmadan ihraç edebilme gibi yetkilerle bu güveni boşa çıkarabilmektedir. Dolayısıyla

^{††} Bizanslı Generaller Probleminde bir şehre saldırmak isteyen ve ancak birbirleri arasında güvenli haber kanalı olmayan generaller tasvir edilmektedir. Çünkü birbirlerine gönderdikleri bilgiler düşmanlar tarafından ele geçirilmiş veya değiştirilmiş olabilir. Generaller aynı anda saldırırlarsa şehri ele geçirecekler ancak farklı zamanlarda saldırırlarında ise bozguna uğrayacaklardır. Eğer merkezi bir otorite olsa ve tüm generallerin saldırı zamanını belirlese sorun çözülecektir. Bu durumda tesis edilen “güven” sadece bir mecburiyete dayalı olacaktır.

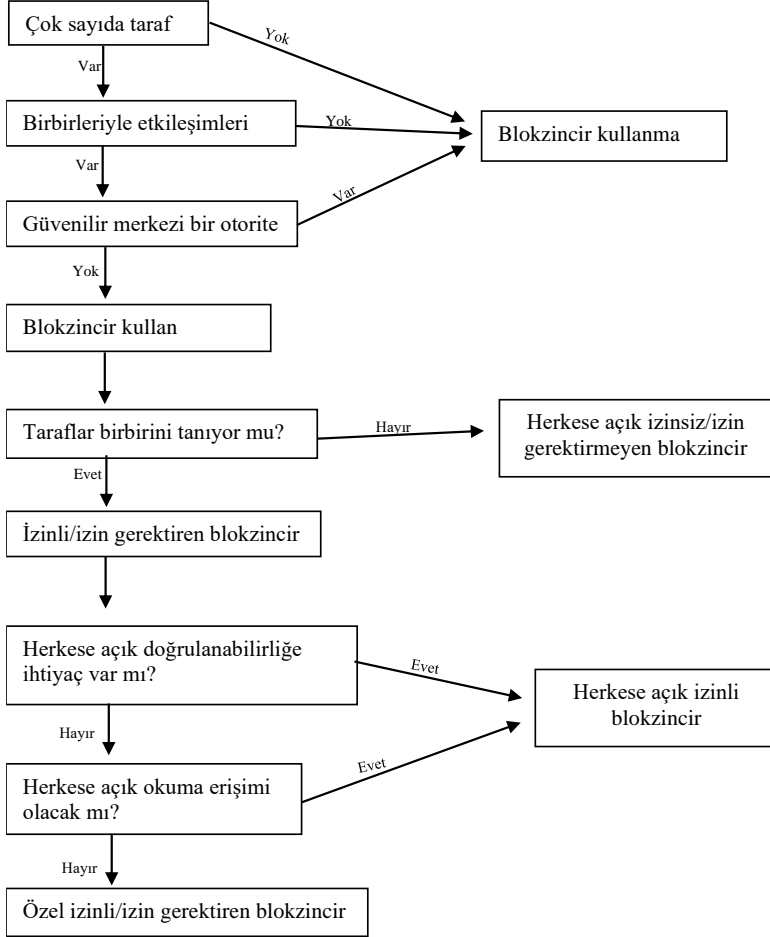
tesis edilen bu ilişki güven üzerine değil, güvensiz ancak zorunlu bir kabul olarak değerlendirilmektedir (Mougayar, 2016: 33-34).

Dağıtık defterler temel açıdan bilgilerin/verilerin birden fazla düğüm arasında kaydedilmesini sağlamak ve bunların merkezi bir birim veya otorite tarafından değiştirilmesini veya silinmesini engellemeyi tasarlamaktadır. Zira mevcut yöntemler merkezîyetçi olmakla birlikte yoğun siber saldırılar karşısında korunmasız kalabilmekte veya sisteme erişimi olanlar tarafından suiistimal edilerek yasadışı işlemler yapılabilmektedir.

Blokszincir teknolojisinde *güvenirlilik* önemli bir kazanımdır. Her bir blok içinde önceki blokların dönüştürülerek (hashing) yer alması ilk bloktan itibaren tüm işlemlerin izlenebilmesine imkan verir. Önceki blok işlemleri “hash” özetini değiştirdiğinden (Lee, 2019: 11) ara işlemler yoluyla sistemi aldatmak mümkün değildir. Örneğin yirmi bloktan oluşan zincirin beşinci bloğuna gidilerek orada veri veya işlem değiştirilmesi durumunda altıncı bloktan itibaren tüm zincirde değişiklik meydana gelecektir. Ancak bu değişikliğin dahi düğümler tarafından onaylanması ve doğrulanarak uygun bulunması gerekecektir.

Kodların oluşturulması sürecine ve test uygulamalarına yeteri kadar önemin verilmesi gerekmektedir. Zira kodlardan bir tanesinde dahi bir hatanın olması fark edilemeyen veya istenmeyen sonuçlara yol açabilir. Bir hatanın baştan yapılmaması ile sonradan fark edilmesi arasında fark vardır. Nitekim sonradan fark edilen bir hatanın düzeltilmesi sırasında diğer düğümlerin bunun bir hata olduğunun kabulü sorunu ortaya çıkabilir. Başka bir deyişle, bunun bir hata olduğuna düğümlerin ikna edilmesi gerekir. Bu bakımdan blokszincir teknolojisinin mahiyeti itibarıyla, sorunu çözmeye yönelik değişikliğin diğer düğümler tarafından onaylanması gerekir (Park vd., 2021: 3).

Blokszincir teknolojisinin kullanımına karar vermek için uygulanması istenen alanda gerekli olup olmadığı konusunda karar vermek gerekmektedir. Nitekim bazı alanlarda veya şartlarda blokszincir teknolojisinden faydalanmak rasyonel veya etkin sonuçlar doğurmayabilir. Bu bağlamda aşağıdaki grafikte karar verme süreci değerlendirilmektedir.



Grafik 1. Blokzincir Platformu Karar Verme Süreci

Kaynak: El Ioini ve Pahl, 2018: 281.

Kamusal düzeyde, blokzincir teknolojisi oylama sistemleri, vergi toplama, pasaport verme, tapu kayıtlarını kaydetme, hibe veya diğer yardımların izlenmesi ve kontrolünde kullanılabilir. Ancak henüz yeni olması dolayısıyla birçok kamusal sektörde uygulanması vakit alacağı düşünülmektedir (Corrales, Fenwick ve Haapio, 2019: 3, 6). Dolayısıyla blokzincir teknolojisinin kullanım alanlarından birinin kamu harcamalarında hesap verilebilirliğin olması söz konusu olabilir. Bu bağlamda yukarıdaki karar verme süreci şu şekilde ele alınabilir:

- Yasama, yürütme, yargı ve bürokrasi bir bütün olarak kamu harcamalarının belirlenmesinde ve gerçekleşmesinde etkili olmaktadır. Genel yönetimin “birçok farklı idareden” oluşması da bu anlamda değerlendirilir. Harcama yetkisi veren parlamento ve yerel idare meclisleri, harcama yetkisini kullanan harcamacı birimler ve bunu denetleyenler çok sayıda tarafın olduğunu ve bunların bütçeleme süreci boyunca “birbirleriyle etkileşim içinde” olduklarını gösterir.

- Yukarıdaki karar verme süreci dikkate alındığında temel sorunlardan birinin hükümetlerin “güvenilir bir merkezi otorite” olup olmadıklarıdır. Ancak bize göre bunun bir önemi yoktur. Zira güvenilir bir otoritenin varlığı, denetim kurumlarının etkin çalışması ve hesap verilebilirliğin şeffaf bir zeminde gerçekleşmesine bağlıdır. Blokzincir teknolojisi bu alanda yapacağı (belgelerin ve raporların geri döndürülmez şekilde kayıt altına alınması ve bu kayıtların dağıtık birimlerde depolanması, işlemlerin anlık izlenebilmesi, hata düzeltme geçmişlerinin görülebilmesi, tüm paydaşların süreç hakkında bilgi edinebilmesi gibi) potansiyel katkılar ile merkezi otoritenin güvenilirliğini arttıracaktır. Diğer taraftan güvenilir bir otoritenin varlığı ancak şeffaf bir mali denetim ile mümkün hale getirilebilir.

- Blokzincirin kullanılmasına karar verilmesinden sonra kamu kurumları arasındaki ilişki göz önünde bulundurularak hangi yöntemin benimseneceğine ve protokolün nasıl izlenebileceğine karar vermek gerekmektedir. Yukarıdan aşağıya doğru ve en az yüzde 51 oranında doğrulanabilirliğe ihtiyaç duyulan, tüm düğümlerin okumaya izni olduğu, herkese açık olmayan ve katılım için izin gerektiren bir protokolün kamusal mali denetim için uygun olacağı düşünülmektedir.

Blokzincir platformunda oluşturulan defterlere erişim sadece güvenilir taraflara sağlanabilir. Böylelikle bürokratlara, dikkate aldıkları verilerin güncel, kesin ve manipüle edilmesi neredeyse imkansız olduğuna dair güvence verilebilir (Arun, Cuomo ve Gaur, 2019: 30). Resmi verilere, evraklara erişim hakkı olanların bunları değiştirerek kamu zararına yol açmaları, kişisel çıkar sağlamaları geleneksel yöntemlerle mümkün olabilmektedir. Blokzincir teknolojisinin çalışma (kayıt ve onay süreci) yöntemi ve verilerin ortadan kaldırılamaması gibi özellikleri kamusal sahtekarlıkların önüne geçmeye imkan sağlayabilir.

3. BLOKZİNCİRİN DEVRİMSSEL ÜRÜNÜ: AKILLI SÖZLEŞMELER

3.1. Ortaya Çıkışı ve Özellikleri

Satoshi Nakamoto *Bitcoin blokzincirini* ilk defa oluşturduğunda aynı anda radikal ve test edilmemiş iki konsepti tanıtmıştır. Birincisi Bitcoin’in kendisinin meydana getirdiği parasal değer ve bunun ihtiva ettiği özelliklerdir. İkinci önemli konsept ise işlemlerin sırasına ilişkin halka açık anlaşmaya imkan veren iş kanıtı (proof of work – PoW) tabanlı blokzinciridir. Yaygın olarak atıfta bulunulan varlıklar arasında özel para birimleri ve finansal araçların (colored coins), fiziksel bir ürünün mülkiyeti (smart property), alan adları (domain) gibi değiştirilemez varlıklar (namecoin) ile merkezi olmayan takas, finansal türevler ve kimlik kartları gibi daha da gelişmiş uygulamalar yer almaktadır. Ancak bir diğer önemli araştırma alanı da dijital varlıkları önceden belirlenen kurallara göre otomatik olarak harekete geçiren/taşıyan akıllı sözleşmelerdir (Buterin, 2014: 1). Bitcoin tek yönlü bir blokzincir teknolojisi kullanırken blokzincir sadece finansal işlemlerin değil, değeri olan herhangi bir şeyi transfer etmek ve kaydetmek için kullanılabilir (Gates, 2017: 3).

Ethereum ilk olarak 2013 yılında çıkmıştır. Bitcoin’den daha esnek ve farklı olsa da blok ve madencilik konusunda aynıydı. Ancak en büyük farklılık akıllı sözleşmelerin ortaya çıkmasıydı. Akıllı sözleşmelerin arkasındaki fikir birçok farklı program veya uygulama çalıştırılmasına imkan veren daha fazla dağıtık işletim sistemi yapmaktı. İlk olarak para birimi şeklinde optimize edilen Bitcoin blokzinciri yerine Ethereum blokzinciri çok amaçlı şekilde inşa edildi (Shrier, 2020: 23). Akıllı sözleşmeler başta olmak üzere çok çeşitli merkezi olmayan uygulamaların (decentralized application – DApp) hazırlanmaya başlamasına olanak vermesi ile bu dönem Blokzincir 2.0 olarak adlandırıldı. Bu dönem aynı zamanda geleneksel finansal sisteme önemli alternatifleri içeren “merkezi olmayan finans” (decentralized finance – DeFi) kapsamında çok sayıda ürünün çıkmaya başladığı dönem olmuştur.

Ethereum merkezi olmayan uygulamaların devreye sokulabileceği *merkezi olmayan bir platformdur*. Ethereum’da Solidity, LLL ve Serpent programlama dilleri kullanılarak akıllı sözleşmeler oluşturulmaktadır. Akıllı sözleşmeleri devreye sokmak veya yöntemlerini talep etmek için Ethereum’um iç para birimi olan *ethere* ihtiyaç duyulmaktadır. DApp’ler bir veya daha fazla akıllı sözleşme kullanılarak oluşturulur. Akıllı sözleşmeler, herhangi bir kesinti, sansür, dolandırıcılık veya üçüncü taraf ara yüzü gibi olasılıklar olmadan tam olarak programlandıkları şekilde çalışırlar (Prusty, 2017: 25).

Akıllı sözleşme, Ethereum Sanal Makinesi’nin (Ethereum Virtual Machine - EVM) blokzincirde yürütülmesini sağlayan bir koddur. Programlama dilini kullanması bakımından diğer sanal makinelerle aynı olan EVM; “*hesaplar*” olarak adlandırılan milyonlarca nesneyi içeren büyük ve merkezi olmayan bir bilgisayar olarak tanımlanabilir. Bu hesaplar dahili veri tabanları ve yürütme kodları içerebilir ve diğer hesaplarla konuşabilir [iletişime geçebilir]. Akıllı sözleşmenin kendisi de bir hesaptır. EVM, harici olarak sahip olunan (externally owned accounts – EOA) ve bir kullanıcı aracılığıyla özel anahtarla kontrol edilen hesapların diğer bir hesaba ether ya da mesaj göndermesine imkan verir (Beck, 2018: 56).

Akıllı sözleşmelerin özellikleriyle ilgili olarak şunlar ifade edilebilir (Mougayar, 2016: 61-62):

- Akıllı sözleşmeler *Ricardian Sözleşmeden* farklıdır. Ricardian Sözleşme benzer dijital işlemlere sahip olsa da beklenti sözleşme devreye girmeden taraflarca sözleşmenin amacının anlaşılmasıdır. Akıllı sözleşmelerde ise karşılıklı yükümlülüklerin yerine getirilmesi sağlanır.
- Akıllı sözleşmeler hukuki bir metin değil ancak bilgisayar programıdır. Bununla birlikte sözleşme faaliyetlerinin sonuçları yasal düzenlemenin bir parçası haline getirilebilir.
- Akıllı sözleşmelerde yapay zeka (Artificial Intelligence – AI) yoktur. Akıllı sözleşmeler blokzinciri çalıştıran iş mantığını temsil eden yazılım kodudur. Bunlar diğer verileri değiştirmelerine izin veren bazı harici veriler tarafından tetiklenirler. Bu bakımdan AI’dan ziyade *olay odaklı bir yapıya* daha yakındırlar.
- Akıllı sözleşmeler blokzincir uygulamaları ile aynı değildir. Genellikle bir blokzincir uygulamasının parçasıdır. Belli bir uygulamaya yönelik birkaç sözleşme olabilir. Örneğin, akıllı sözleşmede yer alan belli şartlar yerine getirildiğinde program veri tabanının güncellenmesine izin verebilir.
- Akıllı sözleşmelerin hazırlanması özel akıllı sözleşme dili (Ethereum’s Solidity gibi) ile yapılmaktadır. Ancak “*oracle*”^{**} adı verilen yapı ile ileri derece akıllı sözleşme uygulamalarının hazırlanması mümkündür.
- Akıllı sözleşmeler birçok alanda kullanılabilir. Bunun en çarpıcı alanı DeFi ürünleridir.

Akıllı sözleşmelerin önemli bir özelliği ve avantajı geleneksel yöntemlere göre daha az maliyetli olmasıdır. Geleneksel bir sözleşmenin hazırlanması ve yürütülmesinin maliyeti son altı yılda yüzde 38 oranında artış gösterdi. 2025 yılında hukuk hizmetleri piyasasının 900 milyar doları geçeceği öngörüldüğü (Statista, 2020) dikkate alındığında akıllı sözleşmelerin toplam tasarruflar üzerindeki etkisi daha iyi anlaşılır (Arun, Cuomo ve Gaur, 2019: 21).

3.2. Kamusal Niteliği

Akıllı sözleşme modeli temel bilgiler, kayıt türü, temel ve gelişmiş işlemler olmak üzere dörde ayrılır. Erişim kontrolü ve çoklu imza işlemleri gelişmiş işlemler arasında yer almaktadır. Erişim kontrolü ile kullanıcıların bazı işlemleri sınırlandırılmaktadır. Örneğin kamusal siciller

** Oracle, akıllı sözleşmelere eyleme geçirilebilir bilgiler gönderen veri kaynağıdır.

herkes tarafından okunabilir olsa da sadece yetkili devlet kurumlarına bu sicillerin eklenmesi veya güncellenmesi konusunda izin verilir. Çoklu imza ise akıllı sözleşme işleminin başlaması için çok sayıda tarafın ortak imza vermesini gerektirmektedir. Kamusal sicil örneğinde olduğu gibi, bir kaydın silinmesi veya güncellenmesi için yetkilendirilen tüm otoritelerden izin almak gerekmektedir (Xu, Weber ve Staples, 2019: 166).

Politik hesap verilebilirlik de akıllı sözleşmeler kapsamında değerlendirilmektedir. Seçilen temsilcilerin akıllı sözleşmeler yoluyla seçmenlerine karşı sorumlulukları otomatik ve şeffaf hale gelebilir (Tapscott ve Tapscott, 2018: 383). Akıllı sözleşmelerin, belirli şartların yerine gelmesi ile kendiliğinden işlemeye başlaması, bunların kalıcı olması, şartların geri alınmaması (değiştirilse dahi önceki şartlar ortadan kaybolmaz) ve sürecin (okuma izni kapsamında) tüm düşümler (vatandaşlar) tarafından takip edilebilmesi politik hesap verilebilirliği destekleyen başlıca hususlar olarak ileri sürülebilir.

Akıllı sözleşmelere ilişkin kod bir kez oluşturulduktan sonra artık değiştirilemez. Bu bağlamda kamusal hesap verilebilirlikte kullanılacak verilerin öncelikle standartlaştırılması gerekmektedir. Standardizasyon; uyumluluğu, birlikte çalışabilirliği, güvenliği, tekrarlanabilirliği ve kaliteyi artırır (Antipova, 2018: 4). Kodun yazılması ve belirlenen şartların tanımlanması sonrasında şartların yerine getirilmesine göre sözleşme kendiliğinden sürdürülecektir. Örneğin bir kamu kurumu, ihalenin nasıl sonuçlanacağı kanuni düzenlemeler çerçevesinde önceden belirlenen bir ihaleye çıkacaktır. Kanuni düzenlemelerin bu süreçte değiştirilmediği varsayıldığında, hazırlanacak akıllı sözleşme ile ihalenin hazırlanmasından ve sonuçlanmasına, işin tamamlanmasından ve ödemenin yapılmasına kadar tüm süreçte kurallar belirlenir. İhalenin, kanuni düzenlemelere göre belirlenen şartlarını sağlayan istekliye verileceği akıllı sözleşmede belirtilirse bu şartları sağlayan kişi ihaleyi almış olacaktır. İhalenin verilmesinden sonra yapılacak iş ve ödeme de şartların yerine getirilmesine göre kendiliğinden yapılacaktır. Dolayısıyla süreç değiştirilemez şekilde kaydedileceğinden ve ihale şartlarının yerine getirilmeden ödemelerin yapılamayacağından hesap verilebilirlik, kamu kaynağının etkin kullanımı ve şeffaflık sağlanmış olacaktır.

Sözleşmelere bağlı düzenlemelerin meydana getirebileceği ahlaki (moral) veya operasyonel olumsuzluklar temelde asimetrik enformasyondan kaynaklanır. Asimetrik enformasyon kaynaklı bu sorunlar blokzincir teknolojisi ile çözülebilir. Zira akıllı sözleşmelerin daha açık ve kendiliğinden yürürlüğe girme (self-executed) özelliğinde olması tüm tarafların enformasyona ulaşmalarını mümkün hale getirmektedir. Kamusal fonların kamu kurumları arasında veya kamudan özel kuruluşlara aktarılması işlemlerinde akıllı sözleşmelerin kullanılabilir olması, anılan olumsuzlukların giderilmesi ve şeffaflığın sağlanmasına yardımcı olacaktır (Souza, Luciano ve Wiedenhöft, 2018: 2).

4. BLOKZİNCİR UYGULAMALARI

Blokzincir teknolojisi ile kamusal birçok alan geliştirilebilir. Sağlık, savunma, eğitim ve maliye gibi alanlar buna örnek olarak verilebilir. Sorumluluk ve hesap verilebilirlik düzeyinde dikkate alınacak en önemli husus geriye dönük yapılacak değişikliklerin veya belge kayıplarının önüne geçmek olacaktır. Zira yapılacak tüm değişiklikler ancak (izinli blokzincirde) yetkilendirilmiş organizasyon/birim veya kişi tarafından yapılabilecektir. Yapılan bu değişiklikler varlığını daha önceki bloklarda devam ettirecektir. Dolayısıyla gerçekleşen iş ve eylemler itibarıyla yetki ve sorumluluğun açık olduğu, sürecin tüm aktörler tarafından izlenebildiği bir süreç gerçekleştirilebilecektir.

Blokszincir teknolojisi ele alınırken çoğunlukla kripto paraya atfı yapılmaktadır. Kamu kesimi kapsamında merkez bankaları, bütçe açıkları ve siyasi güven konuları kapsamında dahi bir takım senaryolar kripto paralar üzerinden ele alınmaktadır (Wang, 2018: 90). Ancak blokszincir teknolojisi ağırlıklı olarak özel sektörle ilgili olmakla birlikte çok sayıda kamusal alanda da kullanım imkanı barındırmaktadır (OECD, 2018):

Kimlik: Yerleşimciler ve vatandaşlar için kimliklerin çıkarılması ve bunlarla ilgili gelişmelerin izlenmesi (doğum sertifikaları, evlilik cüzdanları, vizeler, ölüm kayıtları).

Kişisel kayıtlar: Sağlık veya sigorta raporları.

Tapu sicili: Gayrimenkulle ilgili detaylar ve tarihi dokümanlar ile mülklerle ilgili işlemler.

Tedarik zinciri yönetimi ve envanter oluşturma: Bir varlığın yapılışından itibaren, transferinin, satın alınmasının ve envantere girmesi sürecinin izlenmesi.

Sosyal yardımlar: Sosyal güvenlik, tıbbi yardım ödemeleri, ulusal ve uluslararası yardımlar. İleriye dönük/otomatik ödemeler akıllı sözleşmelerle otomatikleştirilebilir.

Sözleşme ve tedarik yönetimi: Tedarikçilere ödemenin yapılması ve bunun izlenmesi, satın alma taahhütlerinin ve işlemlerin yönetimi, takvim performansının izlenmesi. Bu kamu harcamalarının şeffaf olmasına imkan verir.

Oylama: Yeni dijital oylama yöntemlerinin etkinleştirilmesi, uygunluğu sağlama, doğru sayım ve denetim (sandık hilelerinden sakınmak gibi).

Kurumlar arası sürecin düzene girmesi: Blokszincir ve akıllı sözleşmeler işlemleri otomatikleştirebilir ve bilgi alışverişini geliştirebilir. Böylece her birime kendi misyonuna daha fazla odaklanma imkanı tanır.

Blokszincir teknolojisinin uygulama alanları ABD, AB, Japonya, Çin, Dubai, Gürcistan, İsveç, Meksika, Estonya, Singapur, Papua Yeni Gine, Afganistan ve Lüksemburg'da denenmeye başlamıştır. Uluslararası düzeyde ise IMF, Dünya Bankası ve Birleşmiş Milletler'de blokszincir teknolojisine yönelik araştırmalar devam etmektedir. Blokszincir teknolojisinin farklı ülkelerdeki kamusal sektörlerde başlanan pilot uygulamaları şunlardır:

- Papua Yeni Gine ve Afganistan (Taliban hükümetinden önce başlatılan bir girişim olarak) kamu harcamalarında şeffaflık sağlamak adına (amaç yabancı ve dondurulan yardımları elde etmektir) blokszincir teknolojisinden faydalanmak üzere blokszincir girişimi olan Neocapita ile çalışmaya başlamıştır (Casey ve Vigna, 2018: 210).

- Arizona Eyaleti, üniversite öğrencilerinin kayıtlarının kurumlar arasında paylaşılması için blokszincir tabanlı platform kullanmaya başladı (McKenzie, 2019). HB 2417 numaralı düzenleme kapsamında blokszincir teknolojiyle güvenli hale getirilen imzalar ve akıllı sözleşmeler, elektronik form ve elektronik kayıt olarak kabul edilerek yasal hale getirildi^{§§} (HB 2417, 2017).

- Singapur'da kamusal destekle oluşturulan Singapur Blokszincir Yenilik Programı (Singapore Blockchain Innovation Programme) kapsamında özel sektör odaklı çözümler getirilmektedir^{***} (sbip.sg).

^{§§} Benzer bir uygulama özel bir üniversite olan Lefkoşa Üniversitesinde yapılmıştır. Akademik sertifikalara erişim ve bunların onaylanması işlemleri için -Bitcoin tabanlı- blokszinciri kullanılmaktadır (Olmes, 2016: 261).

^{***} Girişimin kamusal destekli olması dolayısıyla çok sayıda yatırımcı Singapur'u tercih etmektedir. Ayrıntılı bilgi için bkz. Ruehl, 2021.

- Malta hükümeti akıllı sözleşmeler dahil her türlü blokzincir girişiminin desteklenmesi için yasal (Yenilikçi Teknoloji Düzenlemeleri ve Hizmetleri Kanunu - Innovation Technology Arrangements and Services Act) ve kurumsal (Malta Dijital Yenilik Dairesi – The Malta Digital Innovation Authority) düzenlemeler yapmıştır (International Trade Administration, 2021).
- İsviçre'nin Zug kentinde yerel seçimler blokzincir teknolojisi kullanılarak başarılı şekilde gerçekleştirmiştir (test düzeyinde) (Wey, 2018). Benzer girişimler Rusya ve Japonya'da da yapılmıştır (Park vd., 2021: 2).
- Brezilya'da geliştirilen Mudamos+ blokzincir platformu ile vatandaşların onaylanmış doğrulukla oy vermeleri mümkün hale getirilmiştir (Megchelen, 2021: 27).
- Almanya'nın Kuzey Rhein-Westphalia Eyaleti, vatandaşların eyalet tarafından NRW-Portal aracılığıyla yayınlanan tüm verileri doğrulamak için blokzincir teknolojisini kullanmalarını sağlamaktadır. Thüringen Eyaleti Maliye Bakanlığı ise Bundesdruckerei (kimlik kartları ve pasaport gibi yasal belgeleri hazırlayan daire) ile birlikte insanların kişisel verilerine erişmesine izin verecek bir kimlik doğrulama konsepti üzerinde çalışmaktadır (Megchelen, 2021: 39).
- Hollanda'da Ekonomik İşler ve İklim Politikası Bakanlığı, blokzincir teknolojisinin güvenilirliğini, enerji tüketimi açısından sürdürülebilirliğini belirlemek ve en iyi kullanım alanlarını keşfetmek için özel bir blokzincir birimi oluşturmuştur (Vilner, 2018). Bu çerçevede sosyal güvenlik, inşaat izinleri gibi çevresel kanunlar ve diğer birçok yasal kamu hizmeti başarılı şekilde dijitalleştirilmiş ve otomatikleştirilmiştir. Devlet, yasal süreçler ve prosedürleri iyileştirmek için blokzincir teknolojisi denemelerinde oldukça aktif bir tutum sergilemeye devam etmektedir (Timmer, 2019: 158).
- Çin'in Chancheng bölgesinde^{†††} 2016 yılında itibaren çeşitli blokzincir uygulamaları denenmektedir. Bunlardan birincisi dijital kimlik sisteminin kurularak bireysel kredi sistemi (Individual Credit System^{†††}) sorununun çözülmesine, ikincisi de (Akıllı Çiftçiler Pazarı – Smart Farmers Market) tarımsal ürünlerin (üretim, nakliye ve market süreçleri boyunca) yapılan test verilerinin yüklenerek (uploading) ve açıklanarak yenilebilir ürünlerin kalitesinin ve güvenliğinin sağlanmasına yöneliktir (Hou, 2017: 2).
- Gürcistan'da Ulusal Kamu Kayıt Kurumu (National Agency of Public Registry) tapu kayıtları ve bunlarla ilgili işlemlerin –Bitcoin tabanlı- izinli blokzincir teknolojisi üzerinden takip edilmesi amacıyla 2016 yılında Bitfury Group ile anlaşmıştır. Sürecin akıllı sözleşme ile geliştirilmesi planlanmaktadır (Bitfury, 2016). Finansmanın bir kısmının Dünya Bankası tarafından sağlandığı benzer bir proje Factom işbirliği ile Honduras'ta yapılmaktadır (Underwood, 2016: 17).

5. KAMUSAL HESAP VERİLEBİLİRLİĞİN SAĞLANMASINDA BLOKZİNCİR TEKNOLOJİSİ KULLANIMININ DEĞERLENDİRİLMESİ

Blokzincir teknolojisi ile oluşturulan protokoller açık kaynak kodlu olmak zorunda değildir. Belli bir grup arasında da merkezi olmayan uygulamalar geliştirilebilir. Böylece sadece ilgili olanların işlem yapabildiği ve onay mekanizmasının bunlar arasında gerçekleşebildiği platformlar kurulabilir. Açık kaynaklarda olduğu gibi burada da üçüncü kişilerin müdahalesi engellenebilmekte, onaylanan veri değiştirilememekte, işlemler konsensüsle onaylanmakta ve geçmişe doğru izlenebilmekte, gruptaki her düğüm tüm verilere ulaşabilmekte ve salt çoğunluğun onayı olmadan işlem tesis edilememektedir. Ethereum platformunda oluşturulan

^{†††} Guangdong Eyaleti'nin Foshan şehrine bağlı bir bölge.

^{†††} Bireysel kredi sistemi kişilerin okul, çalışma, kamusal cezaları vb. konulardaki kayıt ve puanlamalarını gösterir.

akıllı sözleşmeler ise açık kaynak kodlu olmasının yanında sahip olunan açık ve gizli anahtarlar ile önceden tanımlanan şartların dağıtık kaydı sayesinde çok daha kullanışlı olabilmektedir.

Blokzincir teknolojisi devletin maliyetlerini ve büyüklüğünü azaltabilir (Tapscott ve Tapscott, 2018: 377). Diğer taraftan kamu güvenini kötüye kullanan hükümetler de inceleme ve sorumluluk altında tutulabilir (Tapscott ve Tapscott, 2018: 372). Özel sektör şirketlerinin şeffaf olmadıkları durumda güven sorunu yaşamaları gibi kamu sektörünün de aynı sorunla karşılaşması olasıdır. Şirketlerin ticari sırları olabilir ancak bu sırların müşterilerine ve yatırımcılarına zarar verecek şekilde olmaması gerektiği gibi devletin de (milli güvenlik gibi çok sınırlı bir alan hariç) vatandaşlarına yarar getirmeyecek şekilde kamu harcamasında bulunması güven sorunlarına yol açabilir.

Kamusal hesap verilebilirlik kapsamında blokzincir teknolojisinin kullanımı şu faydaları sağlayabilir (Allessie, Sobolewski ve Vaccari, 2019: 10, 45):

- Devletin idari fonksiyonlarını geliştiren kamu birimlerinin kendi arasındaki ve kamu-özel birimler arasındaki bilgi alışverişine yönelik maliyetlerin, zaman ve karmaşıklığın azaltılmasına katkı sağlar.
- Dağıtık defterlerin ve akıllı sözleşmelerin yapısı bürokrasinin, takdir yetkisinin ve yolsuzluğun azaltılmasına katkı sağlar.
- Vatandaşlar yararına devlet kayıtlarındaki enformasyonun hesap verilebilirliği, denetlenebilirliği, şeffaflığı ve otomasyonu artar. Vatandaşların ve şirketlerin bu kayıtlara ve idari süreçlere olan güveni artar.
- Kamu harcama tahsisatında etkinlik sağlar. Belirlenen amaca tahsis edilen fonun uygun olarak harcanmasına imkan verir. Süreçteki hiç kimseye kendi menfaatlerine uygun alan bırakılmaz. Ayrıca yapılan harcamaların dağıtık defterlerde kaydedilmesi kamu harcamalarının hesap verilebilirliğini arttıran denetim amaçlarına hizmet eder^{§§§}.
- Birçok yeni *merkezi olmayan kamu hizmeti ve yönetim modeli*, hükümetlerin gözetimi olmadan uygulanabilir. Dağıtık konsensüs ve işlemlerin denetlenebilirliği merkezi karar alma süreçlerinde ortaya çıkan (şeffaflık eksikliği, yolsuzluk, tehdit/baskı gibi) sorunların azalmasına veya bertaraf edilmesine katkı sağlayabilir (Atzori, 2015: 7).
- Birçok kamu kuruluşu güven oluşturmak için açık, şeffaf ve işbirlikçi olmaya çalışır. Dağıtık defterlerin altında yatan blokzincir teknolojisi şeffaflık ve işbirliğine yönelik yeni bir yaklaşım sunmaktadır. Zaman damgalı işlemler (time-stamped) işlemden sonra değil, gerçek zamana yakın bir zamanda doğrulanabilir. Bu da dolandırıcılık davranışlarını caydırmada yardımcı olur. Şeffaflık arttıkça güven daha olası hale gelir (IBM, 2017: 7).
- Kamusal fonların sorumlu bir şekilde harcandığına dair vatandaşlara (veya bu konuda diğer departmanlara) güvence verilmesi, hükümete olan güveni ve hesap verebilirliği tesis etmede yardımcı olur (IBM, 2017: 12).
- Çok sayıda tarafın sürece dahil edilmesi katılımcılığın güçlendirilmesi anlamına gelmektedir. Katılımcılığın güçlendirilmesi ile hesap verebilirlik sağlanır ve bu bağlamda hükümet daha açık ve şeffaf hale getirilir (OECD, 2022: 13).
- Blokzincir, devletin enformasyon alışverişini, doğrulama ve güven gerektiren işlemleri desteklemesi potansiyel bir teknolojidir (Olness, Ubacht ve Janssen, 2017: 355).

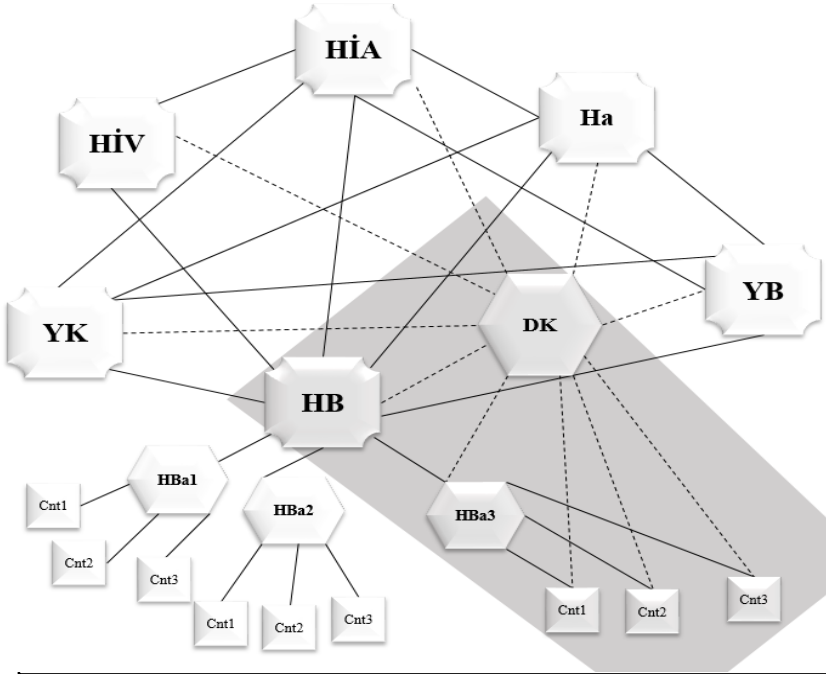
^{§§§} Bu paragraftaki yarar, düşük gelirliilere yapılacak yardımlarda kullanılacak “akıllı kuponlar” a (smart voucher) yönelik ele alınmıştır (Allessie, Sobolewski ve Vaccari, 2019: 62).

- Blokzincir içinde tamamlanan her bir işlem hakkındaki enformasyon herkesle paylaşılabilir ve herkes tarafından elde edilebilir. Teknolojinin bu özelliği onu üçüncü tarafların dahil olduğu merkezi işlemlerden daha şeffaf kılmaktadır (Yli-Huumo vd., 2016: 2).
- Dağıtık defterlere kayıt özelliği, kamu sektörü hizmetlerine daha hızlı ve şeffaf erişim, dolandırıcılığı önleme ve güven oluşturma gibi toplumsal, ticari veya mali konularda hükümetlere yeni yaklaşımlar sunar (Alexopoulos vd., 2019: 3378).
- Blokzincirin (özellikle akıllı sözleşmelerin) kullanılması hukuki güvenliği de teminat altına almaya yardımcı olur. Öngörülebilir usulle ve rasyonel açıdan kabul edilebilir, şeffaf, hukuki değerlere dayanan bir hukuk düzeninin sağlanması ile (Çaptuğ, 2021: 140) kuralları önceden - blokzincir kapsamında- belirlenmiş ve herkes için geçerli olan hususların yürütülmesi güvence altına alınabilir.

Geleneksel yöntemlerde mali işlemlerin sonucu işlem tamamlandıktan sonra öğrenilmektedir. Örneğin bütçe kesin hesap teklifi veya denetim raporları hazırlanırken henüz tamamlanmamış ve bu sebeple hazırlanan belgelerde/raporlarda yer almayan işlemler olabilmektedir. Bunlar hakkında ancak işlemler tamamlandığında bilgi sahibi olunabilir. Ancak blokzincir teknolojisi ile devam eden ve belgelere geçmeyen işlemleri izlemek mümkündür. Bununla birlikte tamamlanan işlemler de geriye doğru izlenebilmektedir. Süreç boyunca işlemlerde meydana gelen değişikliklerin nasıl, ne zaman ve kim tarafından yapıldığı da görülebilmektedir. Yapılan işlemlerin saklanması, işlemler üzerinden yolsuzluk yapılması veya bunların tahrip edilmesinin geleneksel yöntemlere göre daha zor olması hesap verebilirlik açısından önem taşır. İşlemlerin onaylanması mekanizmasına göre en az yüzde 50'den fazla düğüm onayı gerektirmesi dikkate alındığında, işlemlerde görevli olan herkesin işlem bilgilerini onaylayabilme ve bu bilgileri kaydetme hakkı olması anlamına gelir. Blokzincir işlemlerinin geleneksel yöntemlere göre çok daha hızlı olması işlemlerin sonuçlanmasındaki gecikmeleri önleyebilmektedir.

İşlemler tamamlandıktan sonra ortaya çıkan bir hatanın -hukuki açıdan- geri alınması da ülkelerin mevzuatlarına göre belirli sürelerle kısıtlanabilmektedir. Dolayısıyla bir hatanın (açık hata ve hile olmasa dahi) saptanması gecikmeli olduğunda bunun geri alınması mümkün olmayabilmektedir. Hukuki güvenlik ilkesinin bir gereği olan bu husus (Altundiş, 2008: 69), blokzincir teknolojisi ile işlemlerin daha hızlı izlenmesi ve belirlenen kurallar dışında işlemin yürütülememesi sayesinde ortadan kalkmaktadır.

Aşağıdaki diyagramda olası bir kamu mali denetiminin gündeme gelmesi halinde nasıl bir blokzincir ilişkisinin kurulabileceğini göstermektedir (ilişkinin kurulmasında, bütçeleme sürecinde yer alan kurumların fonksiyonları dikkate alınmıştır).



Diyaqram 1. Kamu Mali Denetimi Blokzincir Şeması

Not: HİV harcama izni veren/yasama organını; HİA harcama izni alan/yürütme organını; HB harcamacı bakanlıkları; Ha hazineyi; DK yüksek denetim kurumunu; YB yetkili bakanlığı; YK yetkili kurumu; HBa'lar harcamacı alt birimleri; Cnt'ler mal ve hizmet sunanları/yüklenicileri ifade etmektedir.

Yukarıdaki diyaqram blokzincir teknolojisi kullanılarak kamu mali denetiminin ve şeffaflığın sağlanması öngörülmektedir. Harcamacı alt birim ile yüklenici ikilisi dışında kalan ilişkiler ağında blokzincir teknolojisinin akıllı sözleşmeler üzerinde kurulu olmasına gerek olmayacağı düşünülmektedir. Bunun en önemli nedeni, ülke uygulamalarında bütçe hesaplarının öngörülemeden/kaotik faktörlerin yol açtığı belirsizliklerden etkilenmeleridir. Diğer bir deyişle, gerek görüldüğü durumlarda kamu harcamaları konusundaki (akıllı sözleşmelerle getirilecek) katı sınırlamaların, devlet fonksiyonlarının aksamasına yol açması muhtemeldir. Esasında bu tür durumlara karşı akıllı sözleşmelerin güncellenmesi mümkündür. Harcama izni veren/yasama organının yüzde 50'sinden fazlasının onay vermesi ile olası aksamalar durumunda hızlıca karar verilebilir. Böylece belirlenecek sınırlar içinde yasama organının izin verebileceği bir *mali alan* oluşturulabilir. Diğer taraftan, blokzincir teknolojisinin; güvenlik, şeffaflık, yolsuzluğu engellenme ve hesap verebilirliği sağlama prensiplerinden faydalanmak da mümkündür.

Harcamacı alt birim - yüklenici arasındaki ilişkide ise akıllı sözleşmelerin kullanılması önem taşımaktadır. Dikkat edilecek olursa, bu ilişkideki diğer tarafların harcamacı bakanlıktan ve yüksek denetim kurumundan oluştuğu görülmektedir (*gri alan*). Bu alanda özellikle kamusal mal ve hizmetlerin satın alınması süreci gerçekleşmektedir. Dolayısıyla bu süreçte dikkate alınması ve protokollerin hazırlanmasında bir rehber olması bakımından iyi kurgulanmış/düzenlenmiş bir kamu ihale mevzuatı gerekmektedir. Bu bağlamda, yasal mevzuata göre akıllı sözleşmeler hazırlanacak ve süreç otomatikleştirilecektir. Böylelikle ihale

süreci başlamadan tüm şartlar tanımlanır ve bu şartlar yerine getirildikçe karşılıklı yükümlülükler kendiliğinden yerine getirilmiş olur. Blokzincir teknolojisinin niteliksel diğer faydaları ile birlikte değerlendirildiğinde, ihale şartlarında geriye dönük veya gizli usulsüzlüklerin yapılması, hak ediş ödemelerinin keyfi olması, mal temini veya hizmet ifası olmadan ödemenin yapılması, ihale şartları dışında fiyatlamının olması vb. çok sayıda yolsuzluğun önüne geçilebilecektir.

Kamusal hesapların denetim raporları veya bütçe gerçekleştirmelerinin yayımlanması konusunda da blokzincir teknolojisinden faydalanmak mümkündür. Oluşturulacak protokol ile bu belgelerin yayımlanması konusunda ihtiyari kararlara bırakılmayacak veya bireysel hataların önüne geçilecek kurallar tanımlanabilir. Böyle bir yaklaşım, belgelerin eksik hazırlanmasının ve bunun ileri tarihlerde tamamlanmasının önüne geçecek, kurumsal bir disiplin sağlayacaktır. Örneğin, tüm hesaplar tamamlanmadan bir denetim raporu hazırlanamayacağı için idarelerin bu konuda hesap verilebilir bir tutum sergilemeleri sağlanabilir. Bununla birlikte, protokolün tamamlanması ancak tüm raporlama işlemlerinin tamamlanması şartına bağlanması, belgelerin noksatsız yayımlanmasını teşvik edecektir. Örneğin, kamu idarelerinin kesin hesaplarının yayımlandığı muhasebat.hmb.gov.tr adresinde 2017 yılına ait genel bütçeli idarelerden Başbakanlığa ait kesin hesabın olmadığı Mayıs 2021 tarihinde bir araştırmacının bu belgeye ihtiyaç duyması üzerine anlaşılmıştır. Bu örnekte, eğer blokzincir teknolojisi kullanılsaydı hem raporu hazırlayan hem yayımlayan hem de ilgili idare arasında yapılacak bir protokol bu sorunun olmasına izin vermeyecekti. Akıllı sözleşmelerin “tamamen otomatikleştirilmiş süreçler” olarak tanımlanması (Unsworth, 2019: 22) dikkat alındığında, sonradan bireylerden kaynaklanacak sorunların giderilmesine önemli ölçüde katkı sağlayacağı ifade edilebilir.

Blokzincir, işlemlerin otomatikleştirilmesi olarak dikkate alındığında yaptırımların da otomatikleştirilmesi söz konusu olacaktır. Bu bakımdan akıllı sözleşmeler tekrar eden suç geçmişine olan ikinci yüklenicileri cezalandırabilir (IBM, 2017: 12). Yaptırım mekanizmasının ilk yükleniciye (Cnt'ler) de uygulanması kamusal hizmetlerin etkinliğine katkı sağlayabilir. Ancak hesap verebilirliğin ön plana alınabilmesi için söz konusu yaptırımların kamusal gücü/yetkiyi elinde bulunduranlar için de uygulanabilmesi gerekmektedir.

Yüksek denetim kurumunun (DK) blokzincir bloklarının tümünü takip edebilecek yerde konumlanmış olması, yapılan tüm işlemleri denetleyebilmesine imkan sağlar. Ayrıca, denetimi gerçekleştiren düğümlerin (denetim elemanlarının) tüm orijinal belgelere anlık olarak ve buldukları yerde erişebilmeleri, mevzuata uygun olmayan işlemleri hızlıca tespit etmelerine ve gereğinin yapılması için raporlamalarına imkan sağlar (Ciğerci ve Eğmir, 2020: 213). Bu süreçte gerçekleştirilen işlemlerin değiştirilmesi veya ortadan kaldırılması mümkün olmadığından, gerektiği durumlarda işlemlerin tekrar kontrolü mümkündür.

Yukarıdaki şema genel bir çerçeve oluşturmakla birlikte ülkelerin mali süreçlerine göre düzenlenebilir. Örneğin Türkiye’de yüksek denetim kurumu olan Sayıştay’ın denetim alanına giren merkezi bütçe kapsamındaki kurum ve kuruluşlar, sosyal güvenlik kurumları, yerel idareler, kamu iktisadi teşebbüsleri ve ortaklıklar harcamacı bakanlıklar (HB) kategorisinde değerlendirilmelidir. Bunlardan doğrudan bir bakanlığın alt birimi olduğu halde bütçe koduna sahip özel bütçeli bir kurum/müdürlük/başkanlık olarak yapılandırılanlar bağımsız birimler olarak (HB’nin tabi olduğu sürece tabi olmalı); özel bütçeli olmayanlar ve ayrıca harcama yetkisine sahip olan birimler ise harcamacı alt birimler (HBa) olarak sürece dahil edilmelidir. Yetkili bakanlık (YB), bütçeleme sürecinde birinci dereceden sorumluluk altına alınan Hazine ve Maliye Bakanlığı; yetkili kurum (YK) da bütçeleme sürecinden birinci dereceden sorumluluk altına alan Strateji ve Bütçe Başkanlığıdır. Örneğin Karayolları Genel

Müdürlüğüne bağlı harcamacı bir birimin yapacağı mal alım ihalesi blokzincir üzerinden gerçekleştirildiğinde -akıllı sözleşme vasıtasıyla- bu sürecin önceden belirlenmiş kurallar çerçevesinde yapılması ve sonuçlandırılması gerekecektir. Dolayısıyla sürece yükleniciler (Cnt) de dahil edilecektir. Bu sürecin, bütçe ödeneklerinin serbest bırakılması, kullanılması ve takip edilmesi ile doğrudan ilgili Hazine ve Maliye Bakanlığı ile Strateji ve Bütçe Başkanlığı tarafından izlenmesi mümkün olacaktır. Gerekmesi halinde bütçeyi onaylayan Meclis (veya Meclis'te kurulacak bir birim) tarafından da tüm kamusal harcamaların nasıl ilerlediği anlık olarak izlenebilecektir. Böyle bir izlenme daha sonra Sayıştay tarafından yapılan denetim sonuçları ile kıyaslanacak verinin üretilmesini de sağlayacaktır. Zira Sayıştay bu çerçevede merkezi bir konumda yer almak suretiyle hem harcamacı birimlerin faaliyetlerini denetleyecek hem de bu denetim sonuçlarını Meclis'e sunacaktır.

6. SONUÇ

İçinde fırsatlar barındıran blokzincir teknolojisine yönelik fikir daha eski yıllara dayandığı gibi gelişmesi de henüz tamamlanmış değildir. Bu bağlamda, yenilikçi olduğu kadar deneysel bir alan olarak da değerlendirilmiştir. İlk olarak özel sektör ve sonrasında da kamu sektörü tarafından bu yeni alanı test edilmiş ve uygulama alanları araştırılmıştır. Fikir olarak merkezi olmayan bir yapıya dayansa da merkezi devletler blokzincir teknolojisinden farklı şekillerde yararlanmaya başlamıştır.

Blokzincirin getirdiği yeni fikir merkezi ve güvenilir bir otoritenin olmamasına dayanmaktadır. Ancak güvenilir bir merkez, daha şeffaf ve hesap verilebilir bir yapılanmaya engel oluşturmamaktadır. Özellikle çok sayıda sürecin ve tarafın olduğu kamu bütçesi konusunda temel ilkelerin sağlanmasına yönelik alınabilecek her türlü önlem yarar sağlayacaktır.

Ülke uygulamaları itibarıyla blokzincir teknolojisinin kullanım alanının çok sınırlı ve deneysel düzeyde kaldığı görülmektedir. Teknolojinin yeni olması nedeniyle de uygulama sonuçlarını ortaya koymak için henüz erken bir dönemde olduğu söylenebilir. Uygulamalardaki başarının artmasıyla daha geniş kamusal alanlarda ve başka ülkelerde kullanımı teşvik edilecektir. Bireysel kararların arka plana atılması ve kurumsal yapılanma ile karar verme sürecinin ön plana çıkması blokzincir teknolojisinin kullanımını destekleyecek bir anlayışa hizmet etmektedir. Kamu harcamalarının, vergilerin ve borçların -neredeyse- sürekli olarak arttığı bu dönem, şeffaflık ve hesap verebilirlik için kullanılacak her türlü aracın denenebileceği bir dönemdir. Blokzincir teknolojisi, hesap verebilirlik ve mali denetimi güçlendirmesi bakımından denenebileceği gibi kamusal masrafların azaltılmasına da katkı sağlayabilecek bir potansiyel taşımaktadır.

Ülkeler, mali denetime yönelik blokzincir teknolojisini kullanmaya aşamalı olarak başlayabilirler. Harcamacı birimlerin bir kısmı, mal ve hizmet temin edecek yüklenici ile denetim organının bir departmanı arasında akıllı sözleşmeye dayalı bir protokol oluşturulabilir. Geleneksel yöntemlerle yapılan işlemler ile kıyaslanmak suretiyle yeni yöntemin etkinliği dikkate alınarak sistemin geliştirilmesi sağlanabilir. Böylelikle kamu fonlarının harcanması sürecinde bürokratik tasarrufların/ihtiyari kararların önüne geçilmesi, hesap verebilirliğin sağlanması, belge/rapor kayıtlarının güvenlik altına alınması, sürecin şeffaflaşması ve gerçek zamanlı takibi mümkün hale gelir. Bunun sonucunda mali denetime belli bir standardizasyon getirilecek ve buna bağlı olarak bütçeleme süreci sağlıklı bir yapıya kavuşturulacaktır. Diğer taraftan kamu harcamalarının tahsisatının bütçede belirlendiği şekilde gerçekleşmesine imkan sağlayacak ve çeşitli ödenek aktarmaları yoluyla zayıflatılan bütçe hakkının güçlendirilmesine önemli katkılar sağlayacaktır. Son tahlilde, harcamacı birimlerin ve yürütme organının önceden belirlenmiş ve kesin olan sorumluluklar çerçevesinde hareket etmeleri teşvik edilecektir.

KAYNAKÇA

- ALEXOPOULOS, C., CHARALABIDIS, Y., ANDROUTSOPOULOU, A., LOUTSARIS, M. A., & LACHANA, Z. (2019). "Benefits and Obstacles of Blockchain Applications in E-Government", Proceedings of the 52nd Hawaii International Conference on System Sciences, 3377-3388, 8 January 2019-11 January 2019, Grand Wailea, Hawaii.
- ALLESSIE, D., SOBOLEWSKI, M., & VACCARI, L. (2019). Blockchain for Digital Government, Publication Office of the European Union, Luxembourg.
- ALTUNDIŞ, M. (2008). "Hukuki Güvenlik İlkesi", Yasama Dergisi, 10: 60-94.
- ANTIPOVA, T. (2018). "Using Blockchain Technology for Government Auditing", 13th Iberian Conference on Information Systems and Technologies (CISTI), 1-6. doi: 10.23919/CISTI.2018.8399439, 20.10.2021.
- ARUN, J. S., CUOMO, J., & GAUR, N. (2019). Blockchain for Business, Addison-Wesley, New York.
- ATZORI, M. (2015). "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?", SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713, 30.10.2021.
- BAMBARA, J., & R. ALLEN, P. R. (2018). Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions, McGraw-Hill Education, Chicago.
- BECK, R. (2018). "Beyond Bitcoin: The Rise of Blockchain World", Computer, 51(2): 54-58.
- BITFURY. (2016). "The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project", https://bitfury.com/content/downloads/the_bitfury_group_republic_of_georgia_expand_blockchain_pilot_2_7_16.pdf, 22.11.2021.
- BUTERIN, V. (2014). "A Next-Generation Smart Contract and Decentralized Application Platform", White Paper, 3(37): 1-35.
- CAI, Y., & ZHU, D. (2016). "Fraud Detections for Online Businesses: A Perspective from Blockchain Technology", Financial Innovation, 2(20): 1-10.
- CASEY, M. J., & VIGNA, P. (2018). The Truth Machine: The Blockchain and the Future of Everything, St. Martin's Press, New York.
- ÇİĞERCİ, İ., & EĞMİR, R. T. (2019) "Kamu Mali Denetiminde Olası Blok Zincir Teknolojisinin Denetim Etkinliği Açısından Değerlendirilmesi" Maliye Dergisi, 177: 203-217.
- CORRALES, M., FENWICK, M., & HAAPIO, H. (2019). "Digital Technologies, Legal Design and the Future of the Legal Profession", M. Corrales, M. Fenwick & H. Haapio (eds.), Legal Tech, Smart Contracts and Blockchain (1-17), Springer, Singapore.
- ÇAPTUĞ, M. (2021). "Hukuki Güvenlik İlkesinin Kavramsal Gelişimi", Uyuşmazlık Mahkemesi Dergisi, 17: 133-160.
- EL IONI, N., & PAHL, C. (2018). "A Review of Distributed Ledger Technologies", OTM Confederated International Conferences On the Move to Meaningful Internet Systems (277-288), Springer, Cham.

- GATES, M. (2017). *Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money*, Wise Fox Publishing.
- HAGAN, M. (2019). “Exploding the Fine Print: Designing Visual, Interactive, Consumer-Centric Contracts and Disclosures”, M. Corrales, M. Fenwick & H. Haapio (eds.), *Legal Tech, Smart Contracts and Blockchain* (93-122), Springer, Singapore.
- HB 2417. (2017). “Signatures; Electronic Transactions; Blockchain Technology”, <https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf>, 27.10.2021.
- HOU, H. (2017). “The Application of Blockchain Technology in E-Government in China”, 26th International Conference on Computer Communication and Networks (ICCCN), 31 July-3 July 2017, Vancouver, BC, Canada, Doi: 10.1109/ICCCN.2017.8038519, 10.12.2021.
- IANSTITI, M., & LAKHANNI, K. R. (2017). “It Will Take Years to Transform Business, But The Journey Begins Now”, *Harvard Business Review*, 3: 118-127.
- IBM. (2017). “Building Trust in Government: Exploring the Potential of Blockchains”, <https://www.ibm.com/downloads/cas/WJNPLNGZ>, 13.12.2021.
- INTERNATIONAL TRADE ADMINISTRATION. (2021). “Malta Country Commercial Guide”, <https://www.trade.gov/country-commercial-guides/malta-blockchain-and-artificial-intelligence>, 01.01.2022.
- LESSIG, L. (2006). *Code: Version 2.0*, Basic Books, New York.
- LEE, W. M. (2019). *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript*, Apress, Singapore.
- MEGCHELEN, J. v. (2021). “Blockchain”, Netherlands Innovation Network, <https://www.rvo.nl/sites/default/files/2019/12/Blockchain-Netherlands-Innovation-Network-versie-RVO.pdf>, 03.01.2022.
- McKENZEI, L. (2019). “Boosting Degree Completion with Blockchain”, *Inside Higher Ed*, 9 July 2019, <https://www.insidehighered.com/news/2019/07/09/arizona-state-tackling-college-completion-blockchain>, 16.11.2021.
- MOUGAYAR, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, John Wiley & Sons, New Jersey.
- OECD. (2018). “Guide to Blockchain Technology and Its Use in the Public Sector”, OECD Working Paper, <https://www.oecd.org/fr/gov/administration-innovante/oecd-guide-to-blockchain-technology-and-its-use-in-the-public-sector.htm>, 21.12.2021.
- OECD. (2022). “Recommendation of the Council on Public Integrity”, OECD/LEGAL/0435.
- OLNES, S. (2016). “Beyond Bitcoin Enabling Smart Government Using Blockchain Technology”, Scholl H. et al. (Eds.), *Electronic Government* (253-264), Springer, Cham.
- OLNES, S., UBACHT, J., & JANSSEN, M. (2017). “Blockchain in Government: Benefits and Implication of Distributed Ledger Technology for Information Sharing”, *Government Information Quarterly*, 34: 355-364.

- PARK, S., SPECTER, M., NARULA, N., & RIVEST, R. L. (2021). "Going From Bad to Worse: From Internet Voting to Blockchain Voting", *Journal of Cybersecurity*: 1-15.
- PETERS, G. W., & PANAYI, E. (2016). "Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money", Tasca P., Aste T., Pelizzon L. & Perony N. (Eds.), *Banking Beyond Banks and Money (239-278)*, New Economic Windows, Springer, Cham.
- PRUSTY, N. (2017). *Bulding Blockchain Projects: Develop Real-Time Practical DApps Using Ethereum and JavaScript*, Packt Publishing, Mumbai.
- RIVER FINANCIAL. (2021). "Bitcoin Node", <https://river.com/learn/terms/n/node-bitcoin/>, 19.10.2022.
- RUEHL, M. (2021). "Crypto Groups Shelter in Singapore as Global Regulators Crack Down", *Financial Times*, 8 July 2021, <https://www.ft.com/content/f74d4e60-93b5-46ef-8b3f-71754cbc8a26>, 09.11.2021.
- SHRIER, D. L. (2020). *Basic Blockchain: What is It and How It Will Transform the Way We Work and Live*, Robinson, London.
- SOUZA, R. C. d., LUCIANO, E. M., & WIEDENHÖFT, G. C. (2018). "The Uses of the Blockchain Smart Contracts to Reduce the Levels of Corruption: Some Preliminary Thoughts", *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (1-2)*, <https://doi.org/10.1145/3209281.3209408>, 18.12.2021.
- STATISTA. (2021). "Size of The Legal Service Market 2020", 16 July 2021, <https://www.statista.com/statistics/605125/size-of-the-global-legal-services-market/>, 04.01.2022.
- SWAN, M. (2015). *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Sebastopol.
- TANRIVERDİ, M., UYSAL, M., & ÜSTÜNDAĞ, M. T. (2019). "Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi", *Bilişim Teknolojileri Derisi*, 12(3): 203-217.
- TAPSCOTT, D. & TAPSCOTT, A. (2018). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*, Penguin Random House LLC, New York.
- TIMMER, I. (2019). "Contract Automation: Experiences from Dutch Legal Practice", M. Corrales, M. Fenwick & H. Haapio (eds.), *Legal Tech, Smart Contracts and Blockchain (147-172)*, Springer, Singapore.
- VILNER, Y. (2018). "How the Netherlands is Blazing a Trail Through The Blockchain Scene", *Forbes*, <https://www.forbes.com/sites/yoavvilner/2018/10/13/how-the-netherlands-is-blazing-a-trail-through-the-blockchain-scene/?sh=114215447e48>, 17.12.2021.
- UNDERWOOD, S. (2016). "Blockchain Beyond Bitcoin", *Communication of the ACM*, 59(11): 15-17.
- UNSWORTH, R. (2019). "Smart Contract This! An Assessment of the Contractual Landscape and the Herculean Challenges it Currently Presents for "Self-executing" Contracts",

M. Corrales, M. Fenwick & H. Haapio (eds.), *Legal Tech, Smart Contracts and Blockchain* (17-62), Springer, Singapore.

YLI-HUUMO, J., KO, D., CHOI, S., PARK, S., & SMOLANDER, K. (2016). "Where is Current Research on Blockchain Technology? A Systematic Review", *PLoS ONE*, 11(10): 1-27.

WANG, A. W. (2018). *Crypto Economy: How Blockchain Cryptocurrency, and Token-Economy Are Disrupting The Financial World*, Racehorse Publishing, New York.

WEY, A. (2018). "Switzerland's First Municipal Blockchain Vote Hailed a Success", *SWI*, 2 July 2018, https://www.swissinfo.ch/eng/crypto-valley_-_switzerland-s-first-municipal-blockchain-vote-hailed-a-success/44230928, 22.12.2021.