

T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



BLOKZİNCİR TEKNOLOJİSİ VE
KAMU YÖNETİMİNDE UYGULANABİLİRLİĞİ
DOKTORA TEZİ

DANIŞMAN
Prof. Dr. Selma KARATEPE

HAZIRLAYAN
Bilgehan CİHANGİR

Malatya, 2023

T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

BLOKZİNCİR TEKNOLOJİSİ VE
KAMU YÖNETİMİNDE UYGULANABİLİRLİĞİ

DOKTORA TEZİ

Bilgehan CİHANGİR

Danışman: Prof. Dr. Selma KARATEPE

Malatya, 2023

ONUR SÖZÜ

Prof. Dr. Selma KARATEPE danışmanlığında doktora tezi olarak hazırladığım **“Blokzincir Teknolojisi ve Kamu Yönetiminde Uygulanabilirliği”** başlıklı tez çalışmasının, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın tarafımdan yazıldığını ve yararlandığım tüm kaynakları hem metin içerisinde hem de kaynakça bölümünde uygun bir şekilde yerleştirdiğimi belirtir, onurumla doğrularım.

Bilgehan CİHANGİR

Malatya, 2023

TEŞEKKÜR

Bu araştırmanın ortaya çıkarılmasında emeği geçen ve doktora eğitimim süresince değerli yönlendirmeleri, eleştirileri ve düzeltmeleri ile araştırmaya katkı sağlayan tez danışmanım Prof. Dr. Selma KARATEPE'ye ve Tez İzleme Komitesinde yer alarak görüş ve önerileri ile araştırmanın niteliğinin artmasına destek veren Prof. Dr. Lütfiye ÖZDEMİR, Prof. Dr. S. Mustafa ÖNEN, Doç. Dr. Mehmet Burhanettin COŞKUN ve Dr. Öğr. Üyesi Handan BOYALI hocalarıma teşekkürlerimi arz ederim.

Her zaman yanımda olduğu ve doktora süresince gösterdiği tüm sabır ve sağduyu için sevgili eşim Betül'e ve hayatım boyunca desteklerini hiçbir zaman esirgemeyen kıymetli aileme en içten sevgi, saygı ve teşekkürlerimi sunarım.

ÖZET

BLOKZİNCİR TEKNOLOJİSİ VE KAMU YÖNETİMİNDE UYGULANABİLİRLİĞİ

Bilgehan CİHANGİR

Doktora Tezi

Danışman: Prof. Dr. Selma KARATEPE

İnönü Üniversitesi Sosyal Bilimler Enstitüsü

Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı, Yönetim Bilimleri Bilim Dalı

Blokszincir teknolojisi, bilgi teknolojileri alanında son on beş yılın en çok ses getiren konulardan biri olmuş, dünyanın farklı ülkelerindeki ve farklı sektörlerindeki kurum ve kuruluşlarda ilgi görmeye ve benimsenmeye başlamıştır. İlk başlarda sadece kripto para bağlamında ele alınan bu teknoloji, daha sonradan finans, sağlık, tedarik zinciri, sigorta ve nesnelerin interneti gibi alanlarda bireylerin yaşam tarzını etkilemeye başlamış ve aynı şekilde daha birçok alanı da dönüştürme potansiyeline sahip olduğunu göstermeye devam etmektedir.

Blokszincir, en temel anlamıyla işlemlerin, kayıtların vb. verilerin tutulduğu şifreli bir yazılım teknolojisidir. Bu teknolojiyi dönüştürücü kılan ise kayıt defterinin “dağıtık” olmasıdır. Başka bir deyişle ağa bağlı olan bütün paydaşların, defterin tamamına veya bir kısmına aynı anda sahip olmasıdır. Bu yapının blokszincir olarak adlandırılmasının nedeni, defterde yapılan her güncellemenin bir önceki bloğa bir bilgi bloğu olarak eklenerek değiştirilemez ve denetlenebilir bir işlemler zinciri oluşturmaktır. Defter, üzerinde mutabakat sağlanmadan değiştirilememektedir. Burada blokszincirin getirdiği asıl önemli yenilik ise, tüm bu işlemleri merkezi bir otoriteye ihtiyaç duymadan gerçekleştirmesi, böylelikle üçüncü taraflara olan ihtiyacı ortadan kaldırmasıdır.

Kamu yönetimini değişime iten etkenlerin kabullenilmesine yol açan sebepler, geleneksel yönetim anlayışının eksikliklerinden kaynaklanmaktadır. Geleneksel kamu yönetimi anlayışı, istikrarlı dönemlerinde elde ettiği başarılarına rağmen, hızlı ve yaygın

bir teknolojik deęişimin yaşıandığı günümüzde işlevselliğini kaybetmiştir. Bu yönetim anlayışının esneklikten yoksun olması, kamu yönetimlerinin deęişen şartlara uyum sağlamada önemli sorunlar yaşamasına neden olmaktadır. Bunun yanında küreselleşme ile bilginin çok hızlı bir şekilde yayılması, farklı ülkelerdeki halkların dięer ülkelerdeki örnekler ile mukayese ederek kendi ülkelerindeki yönetimlerden daha hızlı, güvenilir ve kaliteli hizmet talebinde bulunmalarına sebep olmaktadır.

Blokzincir, sunduęu dağıtık ve güven gerektirmeyen altyapısı, sistemin şeffaf ve izlenebilir olması, işlemlerin kesin ve mutabakat sağlanmadan deęiştirilemezlięi, maliyet tasarrufu ve verimlilik gibi üstün yönleri ile kamu yönetimine açıklık, etkililik, hesap verebilirlik, güvenilirlik ve katılımcılık bağlamında fayda sağlama potansiyeline sahiptir. Bu yönleriyle kimlik yönetimi, varlık kaydı ve tapu tescili, noter ve kayıtlandırma, elektronik oylama, akıllı kontratlar, saęlık hizmetleri ve gıda güvenlięi gibi kamu yönetiminin farklı alanlarında kendine uygulama imkânı bulmaktadır.

Bu araştırmada blokzincir teknolojisinin kamu yönetiminde uygulanabilirlięi incelenmektedir. Öncelikle blokzincirin kavramsal çerçevesi sunulmuş, üstün ve zayıf yönlerine yer verilmiştir. Ardından blokzincir teknolojisi kamu yönetimi bağlamında ele alınarak kamu yönetimine sağlayacağı faydalar ve kamu yönetimindeki uygulama alanları ele alınmıştır. Müteakiben teknolojiyi daha iyi anlamak için, blokzincir altyapısı ile hayata geçirilmiş, dünyada ve Türkiye’deki uygulamalarından örnekler verilmiştir. Son olarak mevcut riskler ve engeller ele alınarak, blokzincir teknolojisinin kamu yönetiminde uygulanabilirlięi konusunda deęerlendirmelerde bulunulmuştur.

Anahtar Kelimeler: Blokzincir, Dağıtık Kayıt Defteri, Bitcoin, Kamu Yönetiminde Bilgi Teknolojileri, Kamu Yönetiminde Dijitalleşme, e-Devlet, Endüstri 4.0, Kamu Yönetiminde Blokzincir.

ABSTRACT

BLOCKCHAIN TECHNOLOGY

AND ITS APPLICABILITY IN PUBLIC ADMINISTRATION

Bilgehan CİHANGİR

Ph. D. Thesis

Adviser: Prof. Dr. Selma KARATEPE
Inonu University Institute of Social Sciences
Department of Political Science and Public Administration. Administrative Sciences

Blockchain technology has been one of the most prominent topics in the field of information technologies in the last fifteen years, and it has started to attract attention and be adopted by companies in different countries and different sectors of the world. This technology, which was initially considered only in the context of cryptocurrency, later started to affect the lifestyle of individuals in areas such as finance, health, supply chain, insurance and the internet of things, and it continues to show that it has the potential to transform many more areas.

Blockchain, in its most basic sense, is an encrypted software technology in which transactions, records, etc. are kept. What makes this technology transformative is that the ledger is “distributed”. In other words, all stakeholders connected to the network have all or some part of the ledger at the same time. The reason why this structure is called a blockchain is that each update to the ledger is added to the previous block as an information block, creating an unalterable and auditable chain of transactions. The ledger cannot be changed without consensus of the nodes. The main innovation brought by the blockchain is that it performs all these transactions without the need for a central authority, thus eliminating the need for third parties.

The reasons that lead to the acceptance of the factors that push the public administration to change are due to the deficiencies of the traditional management approach. Despite the success it has achieved in its stable periods, the traditional public administration approach is losing its functionality in today's world, where a rapid and

widespread technological change is experienced. However, the rapid spread of information with globalization results people in different countries to make new demands from the governments in their own countries by comparing them with the examples in other countries.

Blockchain has the potential to provide benefits to the public administration in terms of openness, effectiveness, accountability, reliability and participation, with its distributed and trustless infrastructure, transparency and traceability of the system, certainty, unchangeability of transactions without consensus, cost savings and efficiency. With these aspects, it finds the opportunity to be applied in different areas of public administration such as identity management, asset registration and land registry, notary and registration, electronic voting, smart contracts, health services and food safety.

In this study, the applicability of blockchain technology in public administration is examined. First of all, the conceptual framework of the blockchain is presented, and its advantages and disadvantages are reviewed. Then, the benefits of blockchain technology in the context of public administration and its application areas are discussed. Subsequently, in order to better understand the technology, the use cases of blockchain technology in the world and Turkey are reviewed. Finally, the current risks and obstacles are discussed and evaluations are made on the applicability of blockchain technology in public administration.

Keywords: Blockchain, Distributed Ledger, Bitcoin, Information Technologies in Public Administration, Digitalization in Public Administration, e-Government, Industry 4.0, Blockchain in Public Administration.

BLOKZİNCİR TEKNOLOJİSİ VE
KAMU YÖNETİMİNDE UYGULANABİLİRLİĞİ

İÇİNDEKİLER

ONUR SÖZÜ.....	iii
TEŞEKKÜR	iv
ÖZET	v
ABSTRACT.....	vii
İÇİNDEKİLER	ix
TABLolar LİSTESİ	xvi
ŞEKİLLER LİSTESİ	xvii
KISALTMALAR LİSTESİ.....	xviii

BİRİNCİ BÖLÜM

1. ARAŞTIRMA HAKKINDA AÇIKLAMALAR	1
1.1. Araştırmanın Konusu ve Önemi	1
1.2. Araştırmanın Amacı	2
1.3. Araştırmanın Soruları	2
1.4. Araştırmanın Yöntemi	3
1.5. Araştırmanın Anahtar Kavramları	4
1.6. Araştırmanın Sunuş Sırası	5

İKİNCİ BÖLÜM

2. BLOKZİNCİR TEKNOLOJİSİ.....	7
2.1. Blokzincir Kavramı	8
2.1.1. Dağıtık Veri Tabanı	11
2.1.2. Şifrelenmiş Özet (Hash) İşlevi	12
2.1.3. Blokzincirin Veri Yapısı	13
2.1.4. Dijital İmza.....	16
2.1.5. Blokzincir Sistemlerinin Sınıflandırılması.....	17
2.1.6. Blokzincirde İşlem	19
2.2. Mutabakat Mekanizmaları.....	21
2.2.1. İş İspatı.....	22
2.2.2. Pay İspatı.....	23
2.2.3. Yetkilendirilmiş Hisse İspatı.....	24
2.2.4. Pratik Bizans Hata Toleransı.....	24
2.2.5. Geçen Zamanın İspatı	25
2.3. Blokzincirin Üstün Yönleri ve Faydaları.....	25
2.3.1. Güvenlik, Güven Gerektirmeyen Ortam	25
2.3.2. Dağıtık Yapı, Esneklik, Her Zaman Erişilebilirlik:	26
2.3.3. Şeffaflık ve İzlenebilirlik (Denetlenebilirlik):	27
2.3.4. Kesinlik ve Değiştirilemezlik (Geri Alınamazlık):	27
2.3.5. Kurcalamaya Direnç.....	27
2.3.6. Anonimlik	28
2.3.7. Sansüre Direnç	28
2.3.8. Maliyet Tasarrufu.....	28
2.3.9. Verimlilik	29
2.4. Blokzincirin Zayıf Yönleri ve Blokzincire Yöneltilen Eleştiriler	29

2.4.1. Güvenlik.....	29
2.4.2. Ölçeklenebilirlik.....	31
2.4.3. Gizlilik	31
2.4.4. Bencil Madencilik	32
2.4.5. Değiştirilemezlik	32
2.4.6. Kurcalamaya Karşı Dirençlilik	33
2.4.7. Boyut ve Bant genişliği.....	33
2.4.8. Adem-i Merkeziyetçilik	34
2.4.9. Boşa Harcanan Kaynaklar.....	34
2.5. Blokzincirin Geleceği.....	34
2.6. Bir Blokzincir Uygulaması Olarak Bitcoin	37
2.6.1. Bitcoin Nedir?	37
2.6.2. Bitcoin'in Tarihçesi.....	40
2.6.3. Bitcoin'de İşlem.....	41
2.6.4. Bitcoin Madenciliği.....	42

ÜÇÜNCÜ BÖLÜM

3. BLOKZİNCİR VE KAMU YÖNETİMİ	44
3.1. Kamu Yönetimini Değişime Zorlayan Etkenler	44
3.1.1. Ekonomik Etkenler.....	44
3.1.2. Yönetimsel Etkenler	44
3.1.3. Özel Sektörün Kaydettiği Gelişmeler	45
3.1.4. Sosyolojik Etkenler	46
3.2. Kamu Yönetiminde Bilgi Teknolojilerinin Kullanımı	46
3.2.1. E-Devlet ve Kamu Yönetiminde Dijitalleşme	48
3.2.2. Endüstri 4.0 ve Kamu Yönetimine Etkileri.....	50

3.2.3. Blokzincir ve Endüstri 4.0 Arasındaki İlişki.....	52
3.3. Blokzincirin Kamu Yönetimine Sağlayacağı Faydalar	54
3.3.1. Etkililik ve Verimlilik	56
3.3.2. Şeffaflık ve Hesap Verebilirlik	57
3.3.3. Veri Güvenliği ve Bütünlüğü	58
3.3.4. Katılımcılık ve Yönetişim	58
3.4. Blokzincir Teknolojisinin Genel Kullanım Alanları	59
3.4.1. Bankacılık İşlemleri / Finansal Hizmetler	59
3.4.2. Kripto Para	62
3.4.3. Kitle Fonlama Hizmetleri.....	63
3.4.4. Sigortacılık Hizmetleri	64
3.4.5. Lojistik / Tedarik Zinciri Takibi	66
3.4.6. Dijital Sertifikalar.....	69
3.5. Blokzincir Teknolojisinin Kamu Yönetiminde Olası Kullanım Alanları.....	71
3.5.1. Akıllı Sözleşmeler	72
3.5.2. Kimlik Yönetimi	74
3.5.3. Kamu Mali Denetimi	75
3.5.4. Tapu Tescili.....	79
3.5.5. Elektronik Oylama	81
3.5.6. Sağlık Hizmetleri	84
3.5.7. Vergilendirme / Muhasebe	87
3.5.8. Varlık Kaydı.....	89
3.5.9. Gıda Güvenliği	89
3.5.10. Savunma Sanayi	91
3.6. Uygulamada Karşılaşılabilecek Sorunlar	92

DÖRDÜNCÜ BÖLÜM

4. DÜNYADA VE TÜRKİYE’DE BLOKZİNCİR UYGULAMALARI	95
4.1. Dünyada Blokzincir Uygulamaları	95
4.1.1. Birleşmiş Milletler	96
4.1.2. Amerika Birleşik Devletleri	97
4.1.3. Avrupa Birliği	98
4.1.3.1. Almanya.....	100
4.1.3.2. Danimarka.....	101
4.1.3.3. Estonya	101
4.1.3.4. Fransa.....	102
4.1.3.5. İsveç	103
4.1.4. Birleşik Arap Emirlikleri	104
4.1.5. Çin	105
4.1.6. İngiltere	107
4.1.7. Güney Kore	109
4.1.8. Singapur	111
4.2. Türkiye’de Blokzincir Uygulamaları.....	111
4.2.1. Türkiye’de Blokzincirin Gelişimi	112
4.2.2. TÜBİTAK Blokzincir Araştırma Laboratuvarı.....	116
4.2.3. BiGA Projesi	117
4.2.4. Blokzincir Araştırma Ağı.....	118
4.2.5. Blockchain Economy İstanbul Summit.....	118
4.2.6. Blockchain Türkiye Platformu (BCTR).....	118

BEŞİNCİ BÖLÜM

5. BLOKZİNCİRİN KAMU YÖNETİMİ AÇISINDAN İNCELENMESİ	120
--	------------

5.1. Kamu Yönetiminde Blokzincirle İlgili Yanlış Bilinenler.....	120
5.1.1. Blokzincirin Kamu Yönetimini Tümüyle Dönüştüreceği Beklentisi.....	121
5.1.2. Kamuda Başarılı Blokzincir Uygulamaları Oluşturmanın İmkânsızlığı.	121
5.1.3. Blokzincirin Kamu Yönetimine Duyulan Güvenin Yerine Geçmesi.....	122
5.1.4. Her Geliştirilen Teknolojinin Kullanıcıları Olacağı Beklentisi	123
5.1.5. Blokzincirin Kapsamlı ve Yıkıcı Olması Gerekliliği.....	124
5.1.6. Kamuda Blokzincirin Nasıl Uygulanacağını Bilinmemesi	125
5.1.7. Kullanıcıların Hizmetin Blokzincire Dayalı Olmasını Önemsemesi	125
5.2. Teknoloji-Organizasyon-Çevre Çerçevesi ve Engellerin Sınıflandırılması	126
5.2.1. Teknolojik Bağlam.....	127
5.2.2. Organizasyonel Bağlam	128
5.2.3. Çevresel Bağlam	128
5.2.4. Engellerin Sınıflandırılması	129
5.3. Blokzincirin Kamu Yönetiminde Uygulanabilirliği Önündeki Engeller.....	129
5.3.1. Teknolojik Sorunlar	132
5.3.1.1. Kurulum ve Çalıştırma Maliyeti.....	132
5.3.1.2. Birlikte Çalışabilirlik ve Entegrasyon Sorunları.....	132
5.3.1.3. Ölçeklenebilirlik	134
5.3.1.4. Gizlilik ve Güvenlik	134
5.3.1.5. Gecikme Sorunları	136
5.3.2. Organizasyonel Sorunlar	136
5.3.2.1. Altyapı Eksikliği.....	136
5.3.2.2. Nitelikli Personel Eksikliği.....	137
5.3.2.3. Bilgi Eksikliği, Düşük Anlayış ve Farkındalık.....	138
5.3.2.4. Teknolojiyi Kullanma Konusundaki İsteksizlik	138
5.3.3. Çevresel Sorunlar	140

5.3.3.1. Yasalara ve Düzenlemelere Uyum Sorunları	140
5.3.3.2. Standartların Eksikliği	141
5.3.3.3. Örnek Uygulamaların Eksikliği	142
5.3.3.4. Etik Sorunlar	142
5.4. Blokzincir İhtiyacına Karar Verme Modelleri.....	144
5.4.1. Deloitte Üç V Modeli.....	144
5.4.2. Peck Modeli	146
5.4.3. Wüst ve Gervais Modeli	147
5.4.4. ABD Ulusal Güvenlik Bakanlığı Modeli.....	148
5.4.5. Casino, Dasaklis ve Patsakis Modeli	150
5.4.6. Oxford GO Lab ve CIPFA Modeli.....	152
5.5. Kamuda Blokzincirin Uygulanabilirliğinde Kritik Başarı Faktörleri.....	154
5.5.1. Net Katma Değer Faktörü	155
5.5.2. Teknolojinin Uygunluğu	156
5.5.3. Paydaşların Sürece Dâhil Edilmesi	156
5.5.4. Kullanıcı Odaklılık.....	157
5.5.5. Test Etme	158

ALTINCI BÖLÜM

6. BULGULAR, ÖNERİLER VE SONUÇ	160
6.1. Bulgular	160
6.2. Öneriler.....	175
6.3. Sonuç	177
KAYNAKÇA.....	181

TABLÖLAR LİSTESİ

Tablo 1: Blok Yapısı.....	14
Tablo 2: Genel, Özel, Hibrit ve Konsorsiyum Blokzincirlerin Karşılaştırılması	18
Tablo 3: Blokzincir Teknolojisinin Potansiyel Faydaları ve Vaatleri	55
Tablo 4: Blokzincirin Kamu Yönetiminde Kullanılabilirliği Önündeki Engeller	130
Tablo 5: Blokzincir Uygulama Alanlarının Gerek Duyduğu Özellikler.....	151
Tablo 6: Geleneksel Veri Tabanlarına Karşı Blokzincirin Niteliklerinin ve Ön Koşullarının Analizi.....	152

ŞEKİLLER LİSTESİ

Şekil 1: Ağ Tipleri.....	12
Şekil 2: Blok Yapısı	15
Şekil 3: Merkle Ağacı.....	15
Şekil 4: Blokzincir Türleri.....	19
Şekil 5: Blokzincirde İşlem	20
Şekil 6: Kamu Mali Denetimi Blokzincir Şeması	77
Şekil 7: Sayıştay Denetim Alanı	78
Şekil 8: Teknoloji - Organizasyon - Çevre Çerçevesi.....	126
Şekil 9: Üç V Modeli.....	145
Şekil 10: Peck Modeli Akış Şeması	147
Şekil 11: Wüst ve Gervais Modeli Akış Şeması	148
Şekil 12: ABD Ulusal Güvenlik Bakanlığı (DHS) Modeli Akış Şeması	149
Şekil 13: Blokzincirin Benimsenmesine Yönelik Karar Ağacı.....	153

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AED	: United Arab Emirates Dirham, Birleşik Arap Emirlikleri Dirhemi
AML	: Anti-Money Laundering, Kara Para Aklamayı Önleme
BCTR	: Blockchain Türkiye
BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
BIS	: Bank for International Settlements, Uluslararası Ödemeler Bankası
BiGA	: Bir Gram Altın Projesi Fiziksel Karşılığı Olan Blokzincir Tabanlı Yeni Nesil Transfer Sistemi
BİLGEM	: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BİT	: Bilgi ve İletişim Teknolojileri
BLUEDU	: Blockchain Technologies for VET Education
BKYS	: Belge Kanıt Yönetim Sistemi
BT	: Bilgi Teknolojileri
BZLab	: Blokzincir Araştırma Laboratuvarı
CBDC	: Central Bank Digital Currency, Merkez Bankası Dijital Para Birimi
CFT	: Combating the Financing of Terrorism Terörün Finansmanı ile Mücadele
CIPFA	: The Chartered Institute of Public Finance and Accountancy Birleşik Krallık Yeminli Kamu Maliyesi ve Muhasebesi Enstitüsü
CSB	: T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı

DAPA	: Defense Acquisition Program Administration Güney Kore Savunma Edinme Programı İdaresi
DeFi	: Decentrilized Finance, Merkezi Olmayan Finans
DHS	: Department of Homeland Security, ABD Ulusal Güvenlik Bakanlığı
DID	: Decentrilized Identity, Merkezi Olmayan Kimlik
DLT	: Distributed Ledger Technologies, Dağıtık Defter Teknolojileri
DPoS	: Delegated Proof of Stake, Yetkilendirilmiş Hisse İspatı
EBP	: European Blockchain Partrenship, Avrupa Blokzincir Ortaklığı
EBSI	: European Blockchain Services Infrastructure Avrupa Blokzincir Hizmetleri Altyapısı
ECTO	: Emerging Citizen Technology Office Gelişmekte Olan Vatandaş Teknoloji Ofisi
eIDAS	: Electronic Identification and Trust Services Elektronik Kimlik Tespiti ve Güven Hizmetleri
Eurosystem	: Avrupa Merkez Bankası ve Üye Devletlerin Ulusal Merkez Bankaları
FCA	: Financial Conduct Authority, Finansal Yürütme Otoritesi
FD2A	: Fransız Dijital Varlık Derneği
FED	: Federal Reserve, Amerikan Merkez Bankası
FinHub	: Finansal Teknoloji Merkezi
FinTech	: Financial Technology, Finans Teknolojisi
GDPR	: General Data Protection Regulation, Genel Veri Koruma Yönetmeliği
GMT	: Greenwich Mean Time, Dünya Saati
GO Lab	: Government Outcomes Lab, Hükümet Sonuçları Laboratuvarı

GSA	: The General Services Administration, Genel Hizmetler İdaresi
HIPAA	: Health Insurance Portability and Accountability Act ABD Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası
HMRC	: Her Majesty's Revenue and Customs, Kraliyet Vergi ve Gümrük Dairesi
ICO	: Initial Coin Offering, İlk Dijital Para Arzı
IMF	: International Money Fund, Uluslararası Para Fonu
INATBA	: International Association for Trusted Blockchain Applications Uluslararası Güvenilir Blokzincir Uygulamaları Birliği
IOSS	: Import One Stop Shop
IoT	: Internet of Things, Nesnelerin İnterneti
ISTBCW	: Istanbul Blockchain Women
KCS	: Korea Customs Service, Güney Kore Gümrük Servisi
KDCA	: Korea Disease Control and Prevention Agency Güney Kore Hastalık Kontrol ve Önleme Ajansı
KDV	: Katma Değer Vergisi
KPI	: Key Performance Indicator, Temel Performans Göstergeleri
KOBİ	: Küçük ve Orta Büyüklükteki İşletmeler
KYC	: Know Your Customer, Müşterini Tanı
MAS	: Monetary Authority of Singapore, Singapur Para Otoritesi
MASAK	: Mali Suçları Araştırma Kurulu Başkanlığı
MOHAP	: BAE Sağlık ve Önleme Bakanlığı
MSC	: Marine Stewardship Council, Deniz Koruma Konseyi
MEDE	: Malta Ministry for Education and Employment

Malta Eğitim ve İstihdam Bakanlığı

MIT	: Massachusetts Institute of Technology Massachusetts Teknoloji Enstitüsü
NAPR	: Gürcistan Cumhuriyeti Ulusal Kamu Sicil Dairesi
NFT	: Non-Fungible Token, Gayri Misli Jeton (Değiştirilemez Jeton)
PACTE	: İşletmelerde Büyüme ve Dönüşüm İçin Eylem Planı
PBFT	: Practical Byzantine Fault Tolerance, Pratik Bizans Hata Toleransı
PoET	: Proof of Elapsed Time, Geçen Zamanın İspatı
PoS	: Proof of Stake, Pay İspatı
PoW	: Proof of Work, İş İspatı
SEC	: U.S. Securities and Exchange Commission ABD Menkul Kıymetler ve Borsa Komisyonu
SHA256	: Secure Hash Algorithm, 256 Bitlik Güvenli Şifrelenmiş Özet Algoritması
SPK	: Sermaye Piyasası Kurulu
SKAT	: Danimarka Vergi İdaresi
STK	: Sivil Toplum Kuruluşu
TBV	: Türkiye Bilişim Vakfı
TCMB	: Türkiye Cumhuriyeti Merkez Bankası
TOE	: Technology – Organization – Environment Teknoloji – Organizasyon – Çevre
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
URL	: Uniform Resource Locator, Birörnek Kaynak Konumlayıcı

UTC : UAE Trade Connect, BAE Ticarî Baęlantı Platformu

WFP : World Food Programme, Dünya Gıda Programı



BİRİNCİ BÖLÜM

1. ARAŞTIRMA HAKKINDA AÇIKLAMALAR

Bu bölümde, araştırmaya ilişkin temel nitelikleri özetleyen; araştırmanın konusu, önemi ve amacı, araştırma soruları, yöntemi, bilgi derleme ve işleme araçları, araştırmanın anahtar kavramları ve sunuş sırasına yer verilmiştir.

1.1. Araştırmanın Konusu ve Önemi

İnternetin yaygın olarak kullanılmaya başlanması 1990'lı yıllardan sonra olmuştur. Üzerinden sadece çeyrek asır geçmesine rağmen internet, günümüzde hayatın her alanında yer almakta, internetsiz bir toplum ve devlet yapısı düşünülememektedir. İnternet, 2000'li yıllardan sonra e-devlet uygulamalarıyla kamusal alanda da devrimsel yeniliklere yol açmıştır. İnternet devrimiyle birlikte bilgi, insanlık tarihinde hiç olmadığı kadar hızlı bir şekilde yayılma imkânı bulmuş, bu da üretilen bilginin çok yüksek miktarlara ulaşmasına ön ayak olmuştur. Bu dönem, “bilgi interneti” olarak da adlandırılmaktadır. Blokzincir teknolojisi ise tamamıyla şeffaf, güvenilir, herkes tarafından görülebilen ve doğrulanabilen bir dağıtık veri tabanıdır. Bu teknoloji tarafların birbirine güven duyması gerekliliğini ortadan kaldıracak bir altyapıyı beraberinde getirerek toplumsal, finansal ve hukuki büyük değişimlere gebe olmaktadır. Bu yönüyle internetten sonra (ve onun bir devamı şeklinde) insanlığı etkileyecek en önemli buluşlardan biri olabileceği değerlendirilmekte ve blokzincirle birlikte ‘bilgi interneti’nden ‘değer interneti’ne geçileceği savunulmaktadır.

Blokzincir teknolojisinin hayatın her alanında olduğu gibi kamusal alanda da büyük etkileri olması beklenmektedir. Blokzincirin olası uygulama alanları arasında kimlik yönetimi, tapu tescili, elektronik oylama, sağlık, vergilendirme/muhasebe, bankacılık işlemleri, kripto para, akıllı kontratlar, varlık kayıtları, dijital sertifikalar, noter işlemleri, kitle fonlama, gıda güvenliği, lojistik/tedarik zinciri takibi, savunma sanayi gibi birçok alan sayılmaktadır. Bütün bunlar, blokzincir teknolojisinin kamusal alandaki potansiyelini ortaya koymakta ve önemini ortaya çıkarmaktadır.

1.2. Araştırmanın Amacı

Araştırmanın amacı, blokzincir teknolojisinin kamu yönetiminde uygulanabilirliğini incelemek ve kamu yönetimine olası etkilerini araştırmaktır. Bu kapsamda araştırma; okuyucuya blokzincir teknolojisinin ne olduğu, faydalarının ve sınırlamalarının neler olduğu ve potansiyel olarak daha geniş toplumsal etkilerinin neler olabileceği hakkında kapsamlı bir anlayış sağlamak amacıyla yazılmıştır. Temel kavramlar ve ilkeler hakkında bütüncül bir anlayış sunduktan sonra, okuyucuların devam eden tartışmayı anlamaları, farklı bakış açılarını eleştirel bir şekilde değerlendirmeleri ve yapılandırılmış bir şekilde daha derine inmeleri için araçlar ve çerçeve ile donatmayı amaçlamaktadır.

Blokzincir teknolojisi son on beş yılda ortaya çıkmış yeni bir teknolojidir. Literatürde oldukça fazla İngilizce kaynak olmasına rağmen Türkçe kaynak miktarı sınırlı sayıdadır. Mevcut kaynakların birçoğu ise birbirini tekrar etmektedir. Ayrıca her iki dilde de kaynakların büyük bir kısmı özellikle kripto para bağlamında finans, mühendislik ve bilgisayar bilimleri alanındadır. Bu nedenle araştırma ile, Kamu Yönetimi alanında sınırlı sayıdaki Türkçe literatüre katkı sağlaması amaçlanmıştır.

1.3. Araştırmanın Soruları

Teknolojinin gelişimiyle birlikte kamu yönetiminde bilgi teknolojilerinin kullanımı gün geçtikçe artmaya başlamıştır. Kamusal alanda artan dijitalleşme ile e-devlet uygulamaları hayata geçirilmiş ve kamusal hizmetlerin sunumunda oldukça ilerleme kaydedilmiştir.

Blokzincir de bilgi ve iletişim teknolojilerinin gelişimi ile son on beş yılda geliştirilmiş dağıtık bir kayıt defteri teknolojisidir ve kamu yönetimini dönüştürme potansiyeline sahiptir. Bu teknoloji ile çok daha bütüncül, şeffaf ve güvenilir bir teknolojik altyapının kurulması ve bunun kamu yönetimine uyarlanması olanağı ortaya çıkmıştır. Bununla paralel olarak araştırmada şu sorulara cevap aranmıştır:

Araştırma Sorusu 1 : Blokzincir teknolojisi kamusal hizmetlerin sunumunda kullanılabilir mi?

Araştırma Sorusu 2 : Kamusal alanda blokzincir teknolojisinin kullanımı gerekli midir?

Araştırma Sorusu 3 : Blokzincir teknolojisi kamusal hizmetlerin sunumunda kullanılabilir ise hangi kamusal hizmetlerde kullanılmalıdır?

Araştırma Sorusu 4 : Blokzincirin kamu yönetiminde kullanılması ile ilgili yanlış bilinenler nelerdir?

Araştırma Sorusu 5 : Blokzincir teknolojisinin kamu yönetiminde uygulanabilirliğinin önündeki engeller nelerdir?

Araştırma Sorusu 6 : Blokzincir teknolojisinin kamu yönetiminde uygulanabilirliğinin önündeki engellerin birbirleriyle ilişkisi var mıdır ve varsa belirli karakteristik özelliklerine göre gruplandırılmaları mümkün müdür?

Araştırma Sorusu 7 : Kamu kurumları blokzincir teknolojisine ihtiyacı olup olmadıklarına nasıl karar verebilirler?

Araştırma Sorusu 8 : Kamuda blokzincir teknolojisinin uygulanabilirliğindeki kritik başarı faktörleri nelerdir?

1.4. Araştırmanın Yöntemi

Araştırma, benimsediği yaklaşıma göre kuramsal araştırmadır; dolaylı teknik ve yöntemler bağlamında ikincil veri kaynakları ve belgeler taranmıştır. Veri analizine göre, nitel araştırma yöntemlerinden betimsel analiz yöntemine başvurulmuştur. Bu kapsamda, belirlenen amaçlar ve araştırma soruları doğrultusunda konuyla ilgili yerli ve yabancı kaynaklardan literatür taraması yapılmıştır. Araştırma konusuyla doğrudan ya da dolaylı olarak ilgili olan ve bilimsel niteliğiyle öne çıkan Türkçe ve İngilizce kitap, dergi, makale, süreli yayın, çeviri, inceleme, konferans bildirileri, tez gibi yazılı materyaller incelenmiş ve elektronik kaynaklar taranarak konuya ilişkin veriler toplanmıştır. Bilgi toplama teknikleri sonucunda elde edilen bilgiler; sınıflandırma, metin ve içerik çözümleme, karşılaştırma ve yorumlama araçları kullanılarak tümevarımsal bir yaklaşımla işlenmiş ve değerlendirmelerde bulunulmuştur.

Araştırma, amacına göre keşif amaçlı araştırmadır. Araştırmada blokzincir teknolojisinin yönetim alanında kullanıma potansiyeli, kamu yönetimi bağlamında analiz edilmiştir. Blokzincir teknolojisinin kamu sektöründeki kullanım alanlarını tanımlarken, örnek olay incelemesi yaklaşımı kullanılmıştır. Bu örnekler hem kamu sektörüyle

bağlantılı olduklarından hem de teknolojinin bir bilgi altyapısına dönüşme potansiyelini ortaya çıkarmaları bakımından seçilmişlerdir. Ayrıca farklı ülkelerden örnekler sıralanarak detaylı bir şekilde ele alınmışlardır. Örnek olay incelemesi metodu daha çok araştırmacının çalışılacak konuyla ilgili yeterli literatür oluşmadığında, nasıl ve niçin sorularına cevap aradığında kullandığı bir yöntemdir. Araştırmada blokzincir teknolojisinin kamu sektöründe kullanım alanları da bu şekilde aktarılmaya çalışılmıştır.

Araştırma için literatür taraması yapılırken; Scopus, Web of Science, Elsevier, Emerald gibi dünyanın en büyük yabancı akademik veri tabanlarının ve ULAKBİM gibi yerli veri tabanlarının başlık, özet ve anahtar kelimeler alanında “blokzincir”, “bitcoin”, “blockchain”, “kamu sektöründe blokzincir”, “blockchain in public” ve “blockchain in government” gibi anahtar kelimelerinin kombinasyonunu kullanılarak tarama yapılmıştır. Aynı konular ile ilgili Google arama motorundan elde edilen bazı açık kaynaklı bloglar, forumlar ve incelemelere de başvurulmuştur. Sonuç olarak konu ile ilgili yaklaşık 300’e yakın kaynak incelenerek, araştırmacının ana temalarıyla eşleşen araştırmalardan faydalanılmıştır.

1.5. Araştırmanın Anahtar Kavramları

Blok: Belirli bir süre zarfında yapılmış olan işlemlere ilişkin işlem ve onay kayıtlarının tutulduğu şifrelenmiş veri kümesini ifade eder (BCTR, 2019: 13).

Blokzincir: Yapılan işlemlerin ağdaki bütün katılımcılar tarafından görülebildiği ve doğrulanabildiği, şeffaf, sıralı ve zaman damgalı dijital hesap defteri teknolojisidir. İşlemler, doğrulanması için önce belirli büyüklükten oluşan işlem blokları haline getirilmektedir. Daha sonra bu bloklar kriptografik özet (hash)’e dönüştürülerek birbirine bağlanmaktadır. Zincir kelimesi bu bağlantıya işaret etmektedir.

Dağıtık Kayıt Defteri: En basit anlamıyla dağıtık kayıt defteri, her katılımcı (veya düğüm - node) tarafından büyük bir ağda bağımsız olarak tutulup güncellenebilen bir veri tabanıdır. Normal kayıt (hesap) defterinden farkı, işlemlerin tek bir defterde değil aynı anda ve tamamen aynı olarak herkes tarafından tutulabilmesidir. Böylelikle işlemlerin herkes tarafından görülebilmesi ve doğrulanabilmesi sağlanır.

Hash: Kriptografik özet işlevidir. Farklı uzunluktaki dijital mesajlardan sabit uzunlukta mesaj özeti çıkartmaya yarayan şifreleme yöntemidir. Aynı mesajın özeti

sürekli olarak aynı özeti verir. Mesajdaki en küçük bir değişiklik bile özeti tamamen farklı olmasına sebep olmaktadır. En çok kullanılan çeşidi ABD Ulusal Güvenlik Ajansı (NSA) tarafından geliştirilen SHA256'dır.

Kripto: Gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği unsurlarını sağlamak için çalışan matematiksel yöntemler bütünü ifade eder. Bitcoin işlemlerini doğrulamak ve güvenliğini sağlamak için kullanılır (BCTR, 2019: 20).

Kripto para: Merkezi otoritelerce kabul gören ödeme araçlarına eşler arası bir alternatif olarak ortaya çıkan ve bir değişim aracı olarak kullanılabilen kriptografik mekanizması ile güvence altına alınmış dijital ortamdaki bir değerini ifade eder (BCTR, 2019: 20).

Madencilik: Blokzincir ağında onaylanmayı bekleyen işlemleri blok haline getirerek, zincirin önceden belirlenmiş kurallarına göre kriptografik özeti çıkaran ve daha sonra bunu ağdaki diğer katılımcılara yayarak zincire eklenmesini sağlayan, bunun karşılığında da belirli bir oranda ödüllendirilen katılımcı bilgisayar ya da düğüm (node)dür. Kriptografik özet çıkarma işlemi yüksek dijital işlem kapasitesi gerektirdiğinden yapılan işlem altın, gümüş vs. madenciliğine benzetilmiştir.

Özel Anahtar: Blokzincirde kripto para adreslerinin sahipliğini belirten ve garanti altına alan gizli ve özel anahtarları ifade etmektedir. Üretilen her bir genel adresin özel anahtarı bulunmaktadır ve yapılan işlemler, özel anahtarlar yoluyla şifrelenerek blokzincir ağında yayınlanır.

1.6. Araştırmanın Sunuş Sırası

Araştırma altı bölümden oluşmaktadır. Birinci bölüm olan bu bölümde araştırmanın konusu ve önemi, amacı ve araştırma soruları, yöntemi, araştırmanın anahtar kavramları ve sunuş sırasına yer verilmiştir.

Kavramsal çerçevenin sunulduğu ikinci bölümde; blokzincir kavramı, mutabakat mekanizmaları, blokzincirin üstün ve zayıf yönleri ile blokzincir teknolojisinin ilk örneği olan Bitcoin hakkında bilgi verilmiştir.

Üçüncü bölümde, öncelikle bilgi teknolojileri kapsamında kamu yönetimini değişime zorlayan etkenler aktarılmıştır. Müteakiben kamu yönetiminde bilgi

teknolojilerinin kullanımı; e-devlet, endüstri 4.0, kamu yönetiminde dijitalleşme ve bunların blokzincirle ilişkileri bağlamında incelenmiştir. Ardından blokzincirin kamu yönetimine sağlayacağı faydalara değinilmiş, teknolojinin genel ve kamu yönetimindeki kullanım alanları aktarılmıştır.

Dördüncü bölümde blokzincir teknolojisinin dünyada ve Türkiye’deki uygulama örnekleri ele alınmıştır. Burada ülkelerin seçiminde teknolojiyi uygulamada öncü olan ülkeler belirlenmiştir.

Beşinci bölümde öncelikle kamu yönetiminde blokzincirle ilgili yanlış bilinenlere ve teknolojinin uygulanması ile ilgili bir takım sınırlılıklara değinilmiştir. Ardından blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği önündeki engeller; teknoloji – organizasyon – çevre çerçevesi bağlamında incelenmiş ve bu bağlam içerisinde sınıflandırılmış, müteakiben kamu kurumlarının blokzincir teknolojisine ihtiyacı olup olmadıklarına nasıl karar verebilecekleri sorusuna cevap aranmıştır. Burada ayrıca konuyla ilgili geliştirilen modellere yer verilmiş ve kamuda blokzincirin uygulanabilirliğinde kritik başarı faktörleri sıralanmıştır.

Son olarak altıncı bölümde; elde edilen bulgular ve araştırma sorularının cevaplarına karşı geliştirilen öneriler aktararak araştırmanın genel sonucu arz edilmiştir.

İKİNCİ BÖLÜM

2. BLOKZİNCİR TEKNOLOJİSİ

Kasım 2008’de gizemli bir izahname internette yayılmaya başlamıştır. Satoshi Nakamoto takma adıyla yayımlanan dokümanda, veri bloklarının zincirler halinde kriptografik olarak şifrelenmesiyle oluşturulan dağıtık bir dijital para birimi sistemi anlatılmaktadır. Bir süre boyunca bu sistemin altında yatan teknoloji, para biriminden daha geri planda kalmıştır (Mattila, 2016: 3).

2009 yılında ortaya çıkan ilk kripto para birimi olan Bitcoin’in başarısından sonra blokzincir teknolojisi, akademisyenlerin ve iş dünyasının ilgisini çekmiştir. Mevcut durumda blokzincir teknolojisi; kripto para, sigortacılık, tıp, ekonomi, tedarik zincirleri ve yazılım mühendisliği gibi pek çok farklı alanda kendisine uygulama alanı bulmuştur.

Blokzincir teknolojisi genel olarak büyük bir heyecan uyandırsa da bu olguya daha şüpheci yaklaşımlar da bulunmaktadır. Bir kısım bu teknolojiyi hükümetleri ve ulusal para birimlerini anlamsız kılacak bir araç olarak görürken, bir kısım da kullanışsızlığı nedeniyle kendi kendini yok edeceğini iddia etmektedir.

Blokzincir teknolojinin nasıl algılandığı ile ilgili de farklı yaklaşımlar bulunmaktadır. Bazıları bu teknolojiyi daha çok Bitcoin özelinde olmak üzere kripto para tabanında değerlendirirken, kimileri de teknolojiyi ele alırken Bitcoin’e hiç değinmemektedir. Kimileri ise blokzincirin sadece bir veri yapısı olduğunu iddia ederek terimin bu kadar geniş kapsamlı kullanılmasının, teknolojinin gerçek niteliğini gölgede bıraktığını belirtmektedir (Mattila, 2016: 3).

Dijital ağlarda, veriler genellikle bir yerden başka bir yere kopyalanarak iletilir. Bu konudaki temel sorunlardan biri, ağdan alınan bilgilerin orijinal ve güncel olduğunu nasıl doğrulayacağımızdır. Bu, kendi içinde çözülmesi özellikle zor bir sorun olmasa da, şimdiye kadar tüm çözümler birine güvenmeyi gerektirmiştir. Birçok durumda, verilerin gerçekliği için güvenilir bir otoriteye başvurmak iyi olabilir, ancak bazı durumlarda da değildir. Dahası, iyi olsa bile, sürekli bir aracıya başvurmak zorunda kalmak genellikle masraflı olmaktadır.

Blokszincir teknolojisinin bu kadar yıkıcı olarak görülmesinin nedeni, araçlara ihtiyaç duyma sorununu çözme yeteneğine sahip olmasıdır. Verilerin kimden veya ağda nereden geldiğine bakmaksızın veya başkasının sözünü almak zorunda kalmadan, verilerin doğruluğunu bağımsız olarak doğrulamasına olanak tanır.

Blokszincir teknolojisi; hem internet üzerinden etkileşimle yeni çözümler sunarak, hem de mevcut endüstriyel sistemlerin verimliliğini arttırarak toplumun tüm sektörlerini ve katmanlarını etkileme potansiyeline sahiptir (Mattila, 2016: 5).

2.1. Blokszincir Kavramı

Blokszincirle ilgili yapılan birçok tanım bulunmaktadır. En temel anlamıyla blokszincir, dijital ortamda yapılan işlemlerin hesabının tutulduğu bir dijital hesap ya da kayıt defteridir.

Blokszincir, işlemlerin bilgisayarlardan ya da düğümlerden oluşan bir ağda gerçek zamanlı olarak kaydedildiği ve kopyalandığı dijital bir dağıtık kayıt defteridir. Her işlem, zincire yeni bir blok olarak eklenmeden önce düğümler arasındaki mutabakat mekanizmasında kriptolu olarak doğrulanmak zorundadır. İşlemin onaylanması için merkezi bir otoriteye ihtiyaç duyulmamasından ötürü uçtan uca güven gerektirmeyen mekanizma olarak da anılmaktadır (Deloitte, 2018: 2).

En basit anlamıyla blokszincir; özellikle işlemlerin, kayıtların vb. bilgilerin tutulduğu şifreli yazılım teknolojisidir. Bu teknolojiyi dönüştürücü kılan ise kayıt defterinin “dağıtık” olmasıdır. Başka bir deyişle ağa bağlı olan bütün bilgisayarların, defterin tamamına veya bir kısmına sahip olmasıdır. Defter, üzerinde mutabakat sağlanmış bir sistem bünyesinde çalışan birçok “madenci”nin çabasıyla sürekli olarak güncellenmektedir. Bu yapının blokszincir olarak adlandırılmasının nedeni defterde yapılan her güncellenmenin bir önceki bloğa bir bilgi bloğu eklenerek değiştirilemez ve denetlenebilir bir işlemler zinciri oluşturmalarıdır. Blokszincir özet olarak bütün işlemlerin saklandığı dağıtık bir veri tabanıdır. Burada blokszincirin getirdiği asıl önemli yenilik, bu organizasyonun merkezi bir otoriteye ihtiyaç duyulmadan gerçekleştirilmesini sağlamasıdır (Spielman, 2018: 4).

Blokszincir fenomeni etrafındaki terminoloji halen belirsiz olsa da teknolojinin arkasındaki temel kavram aslında oldukça basittir. Bir veri tabanının aynı anda birden çok

paydaş tarafından değiştirilmesi gerektiğinde, ya değişikliklerinin bir şekilde bir araya getirilmesi gerekir, ya da aynı veri tabanının birden fazla farklı değiştirilmiş sürümü ortaya çıkar. Yazılım veri tabanlarında, farklı sürümler uygun şekilde izlendiği sürece, birden çok sürüm sorun oluşturmaz. Bununla birlikte, finansal defterler gibi diğer veri tabanları, yalnızca tek bir sürümünün olması gerekliliğine dayanır.

Bu gerekliliği karşılamaya yönelik olarak geliştirilen geleneksel yaklaşım, tüm veri tabanı üzerinde eşzamanlı olarak kontrol sağlayan merkezi bir otoriteyi tanımak olmuştur. Bu yöntem, veri tabanında eşzamanlı olarak değişiklik yapabilme problemini çözerken, ikincil bir problemi ortaya çıkarır. Örneğin, merkezi bir otorite maliyet getirir ve dürüst davranacağına dair güvenilmesi gereklidir.

Blokszincir teknolojisi, eşzamanlılık sorununu merkezi bir otoritenin olumsuzlukları olmadan tamamen dağıtık olarak çözmenin daha etkili bir yolunu sağlar: Veri tabanını koruyan ve özgünlüğünü muhafaza eden merkezi bir otorite yerine, tüm veri tabanının bir kopyası, her bir katılımcının bağımsız olarak doğrulaması için erişime açık bir ağa dağıtılır. Daha sonra, kopya sahipleri önceden belirlenmiş kurallara göre doğrulama işlemini gerçekleştirir (Mattila, 2016: 7). Burada katılımcıları hatalı davranmaktan sakındırmak için, oylama sürecine akıllı bir teşvik yapısı dokunmuştur. Çoğunlukla, zaman içinde ağ tarafından orijinal olarak kabul edilen veri tabanı sürümü için oy kullananlar ödüllendirilir. Bu, tüm katılımcıların birbirlerinin seçimlerini tahmin etmeye ve nihayetinde orijinal olarak kabul edilecek veri tabanı sürümüne oy vermeye çalıştığı en iyi oyun teorik dengesini sağlar. Başka bir deyişle, her şeyi senkronize eden ve veri tabanının değişiklik geçmişini dikte eden merkezi bir otorite yerine, blokszincir teknolojisi ile her katılımcı olayların gerçek seyrinin ne olduğunu kendileri görebilmektedir. Bu, ortak bir fikir birliği görüşü için birlikte çalışmaya teşvik edilen, lidersiz cihaz demokrasisinde veri tabanlarını organize etmenin ve yönetmenin yeni bir yoludur.

Bitcoinin altında yatan teknoloji olan bu dağıtık kayıt defteri teknolojisi, her tür işlemi ya da dijital etkileşimi güvenilir, saydam, kesintisiz ve denetlenebilir olarak kayıt altına almaya yarayan bir yöntemdir (Schatsky ve Muraskin, 2015: 1). Blokszinciri, dağıtılmış mimari yapısı, eşler arası ağ protokolü, şifreleme algoritması, akıllı sözleşme, kimlik doğrulama, bulut bilgi işlem vb. gibi çeşitli teknikleri birleştirerek şeffaf ve

oldukça güvenilir bir teknolojik altyapı sunar (Wan vd., 2020: 1). Bu teknoloji, değeri saklama ve takas etme yöntemini değiştirme potansiyeline sahiptir. Bu yönüyle, 1990’larda internetin icadından sonraki en büyük teknolojik atılım olarak nitelendirilebilir.

Blokszincir veya Dağıtık Kayıt Defteri Teknolojisi, bir aracıya gereksinim duymadan bir verinin iki taraf arasında doğrudan değiş tokuşuna imkan sağlayan teknoloji protokolüdür. Zincirdeki paydaşlar kriptolu kimliklerle anonim bir şekilde işlemlerini gerçekleştirirler. Her bir işlem değiştirilemeyen işlem zincirine eklenir ve ağdaki tüm kullanıcılara dağıtılır (Güven ve Şahinöz, 2018: 44).

Blokszincir teknolojisi, Bizans generalleri probleminin daha karmaşık bir versiyonu olan zamanla katılımcıların artması sorununa yeni bir çözüm getirmektedir. Blokszincir, farklı bilgisayarlarda eşzamanlı tutulan özdeş kopyaların kaydedildiği dijital bir dağıtık kayıt defteridir. Ağdaki her katılımcı verileri görüntüleyebilmektedir. Zincirde yapılacak değişiklikler ise sadece çoğunluğun onayı ile gerçekleştirilebilir (Schatsky ve Muraskin, 2015: 2).

Blokszincir teknolojisi yalnızca tek bir teknik değildir. Aynı zamanda kriptografi, matematik, algoritma ve ekonomik modelleri içinde barındırır. Eşler arası ağları birleştirir ve geleneksel dağıtık veri tabanı senkronizasyon problemini çözmek için dağıtık mutabakat mekanizması algoritmasını kullanır. Kendi içinde birçok alanı barındıran bir altyapı sunmaktadır (Lin ve Liao, 2017: 653).

Zincirdeki ilk bloğa “genesis blok” ismi verilir. Her blok, kendinden önceki bloğun özet (hash) algoritmasından geçirilmiş içeriğine sahip olmaktadır. Ağdaki bir işlemi değiştirmek isteyen kişi, geriye doğru bütün işlemlerin özet sonucunu hesaplamak mecburiyetindedir. Bu işlem pratikte mümkün değildir, çünkü hesaplanan sonuçların tüm madencilerde de aynı olması gerekmektedir (Taş ve Kiani, 2018: 4).

Blokszincir gelişim açısından üç aşamada incelenebilir (Swan, 2015; Zhao vd., 2016, 1; Tanrıverdi vd., 2019, 205):

Blokszincir 1.0: Dijital para evresi olarak da isimlendirilen Blokszincir 1.0, para transferleri ve dijital ödeme gibi uygulamaları bulunan kripto paraları ifade etmektedir. Bu dönemde Bitcoin, blokszincir kuramının kendisinden daha fazla dikkat çekmektedir.

Blokszincir 2.0: Dijital ekonomi olarak da ifade edilen Blokszincir 2.0, basit ödemeler ve para transferi işlemlerin ötesinde çok çeşitli ekonomik ve finansal uygulamaları kapsamaktadır. Bu tür uygulamalar arasında, krediler ve ipotekler gibi geleneksel bankacılık araçları, hisse senetleri, tahviller, vadeli işlemler ve sözleşme gibi araçlar yer almaktadır.

Blokszincir 3.0: Blokszincirin kripto para, akıllı sözleşmeler ve finansal enstrümanların da ötesine geçerek kamu, sağlık, bilim, kültür ve sanat gibi alanların tamamına yayılmaya başladığı dijital toplum dönemidir.

Blokszincir teknolojisinin en önemli özellikleri küresel ölçekte olması, merkezi olmayan ve dağıtık yapısı, yapısal olarak şeffaf olması ve araçları ortadan kaldırmasıdır. Yüksek maliyetli ve verimsiz süreçleri yeniden tasarlayanın yolunu açarak daha vizyoner ve insan odaklı sistemler kurmak için öncü olabilecek niteliktedir. Bu nitelikleriyle özellikle devlete olan güvenin düşük ve yolsuzluğun yüksek görüldüğü ülkelerde önem kazanmaktadır (Ølnes ve Jansen, 2018: 1; TÜSİAD, 2018: 14).

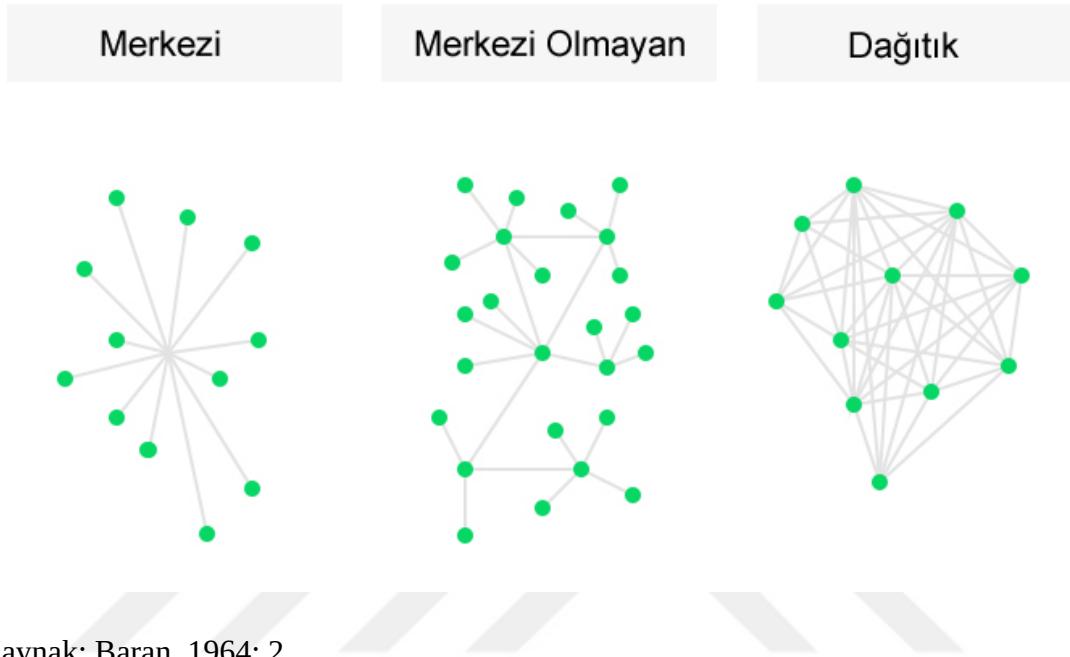
2.1.1. Dağıtık Veri Tabanı

Dağıtık veri tabanı ya da dağıtık kayıt defteri, her katılımcı (veya düğüm – node) tarafından büyük bir ağda bağımsız olarak tutulup güncellenebilen bir veri tabanıdır. Normal kayıt (hesap) defterinden farkı, işlemlerin tek bir defterde değil aynı anda ve tamamen aynı prosedüre bağlı olarak herkes tarafından tutulabilmesidir. Böylelikle işlemlerin herkes tarafından görülebilmesi ve doğrulanabilmesi sağlanır. Bu sistem, tüm verinin sadece bir yerde tutulması durumunda meydana gelebilecek bozulma, silinme, kayıp ve saldırıya uğrama sorunlarına alternatif bir çözüm getirmektedir.

İşlem yapan paydaşlar arasında bir güven problemi bulunmuyorsa ya da işlemleri kaydeden ve teyit eden merkezi bir otorite mevcutsa, dağıtık kayıt defteri oluşturmaya ihtiyaç kalmaz. Bu sistemde girdilerin değiştirilemez ve müdahale edilemez oluşu sisteme güven unsuru sağlamış olur. Böylelikle aralarında güven olmayan ve birbirini tanımayan taraflar arasında işlemlerin sağlıklı bir şekilde kaydı tutulmuş olur (Güven ve Şahinöz, 2018: 74).

İşlemleri yapan taraflar arasında güven sorunu varsa dağıtık kayıt defteri sistemine başvurulabilir. Blokzincir de bir dağıtık kayıt defteri uygulamasıdır. Merkezi, merkezi olmayan ve dağıtık veri tabanı tipleri yukarıdaki şekilde gösterilmiştir.

Şekil 1: Ağ Tipleri



2.1.2. Şifrelenmiş Özet (Hash) İşlevi

Blokzincirin güvenilirliğini nasıl sağladığını anlayabilmek için “özet (hash)” kavramının ne olduğunu ele almak gerekmektedir. Türkçeye parmak izi olarak da çevirenler olmakla (Güven ve Şahinöz, 2018: 50) birlikte hash kavramını kriptografik özet olarak tanımlamak daha doğrudur. Şifrelenmiş özet işlevi, farklı uzunluktaki herhangi bir veriden ya da dijital mesajdan sabit uzunlukta mesaj özeti çıkartmaya yarayan (Çarkacıoğlu, 2016: 21) bir özetleme yöntemidir.

Hash fonksiyonunda girdi tek bir karakter, on kelimelik bir cümle olabileceği gibi çok uzun bir kitap da olabilir. Aynı girdi ile sürekli aynı çıktı oluşur ve iki farklı girdinin çıktısı asla birbirleriyle aynı olamaz. Girdideki en küçük bir değişiklik bile özeti tamamen farklı olmasına sebep olmaktadır. Mesele şu ki, girdi sonsuz büyüklükte olabilir. Fakat hash algoritma, ihtiyaca bağlı olarak sonsuz bit girdisinden yaptığı hesaplamalar sonucunda belirli sayıda bite dönüştürebilmelidir.

Birçok hash fonksiyonu algoritması olmasına rağmen bunlardan en çok kullanılan çeşidi ABD Ulusal Güvenlik Ajansı (NSA) tarafından geliştirilen ve “256 bitlik güvenli şifrelenmiş özet algoritması” anlamına gelen SHA256’dır. SHA256 algoritması adından da anlaşılabilir olduğu üzere 256 bitlik bir özet çıkarmaktadır.

Blokszincirde her bir blok birbirine özet değeri ile bağlıdır. Önce bir bloktaki verilerin özeti türetilir. Bu bloğun özet değeri müteakip bloğun girdilerinden birisidir. Dolayısıyla sonraki bloğun özet değeri üretilirken, kullanılan bilgilerden biri de önceki bloğun özet değeridir. Bu nedenle bir bloğun içinde herhangi bir değişiklik olması, bu bloğun özet değerini değiştirecek, bu değer sonraki bloğun girdilerinden biri olduğundan bu özet değerinin değişmesi sebebiyle bir sonraki bloğun da özet değeri değişecektir (Güven ve Şahinöz, 2018: 51). Bu durumda bir sonraki blok ve bir sonraki blok derken zincirdeki tüm müteakip blokların özet değeri değişmiş olacaktır.

2.1.3. Blokszincirin Veri Yapısı

Blokszincir, birbirine kriptografik özetler ile bağlanmış ve içerisinde yapılan işlemlerin bilgisi de dâhil olmak üzere birden fazla verinin saklandığı bloklardan oluşmaktadır. Her zincirin kendine özgü blok yapısı bulunmaktadır. Burada Bitcoin zincirindeki blok yapısı örnek gösterilmektedir.

Sihirli Sayı: Blokszincir ağı için tanımlayıcı kod olup her zaman 0xD9B4BEF9 değeridir. Zinciri çalıştıran program bu koddan sonra gelen verilerin bir blok olduğunu anlar (Hill vd., 2018: 63).

Blok Boyutu: Bloğun kaç byte’tan oluştuğunu belirtir.

Blok Başlığı: Sürüm, önceki blok hash’i, merkle kökü hash’i, zaman damgası, zorluk derecesi ve tek seferlik anahtar bilgilerini kapsayan bölüme denmektedir.

Sürüm: Zincirin ilgili bloğunda hangi kurallar bütünüünün geçerli olacağını belirtildiği yerdir. Blok oluşturulurken yapısı, uzunluğu, alanların sırası gibi birçok uyulması gereken kural bulunmaktadır. Bu kurallar zamanla topluluğun mutabakatıyla değiştirilebilir.

Önceki Bloğun Hash’i: Blokszincir blokların birbirine kriptografik özetlerle bağlanmasıyla oluşmaktadır. Bloğun oluşturulması tamamlandıktan sonra bloğun hash

değeri hesaplanır. Bu hash değeri, bir sonraki bloğun girdilerinden birini teşkil etmektedir.

Tablo 1: Blok Yapısı

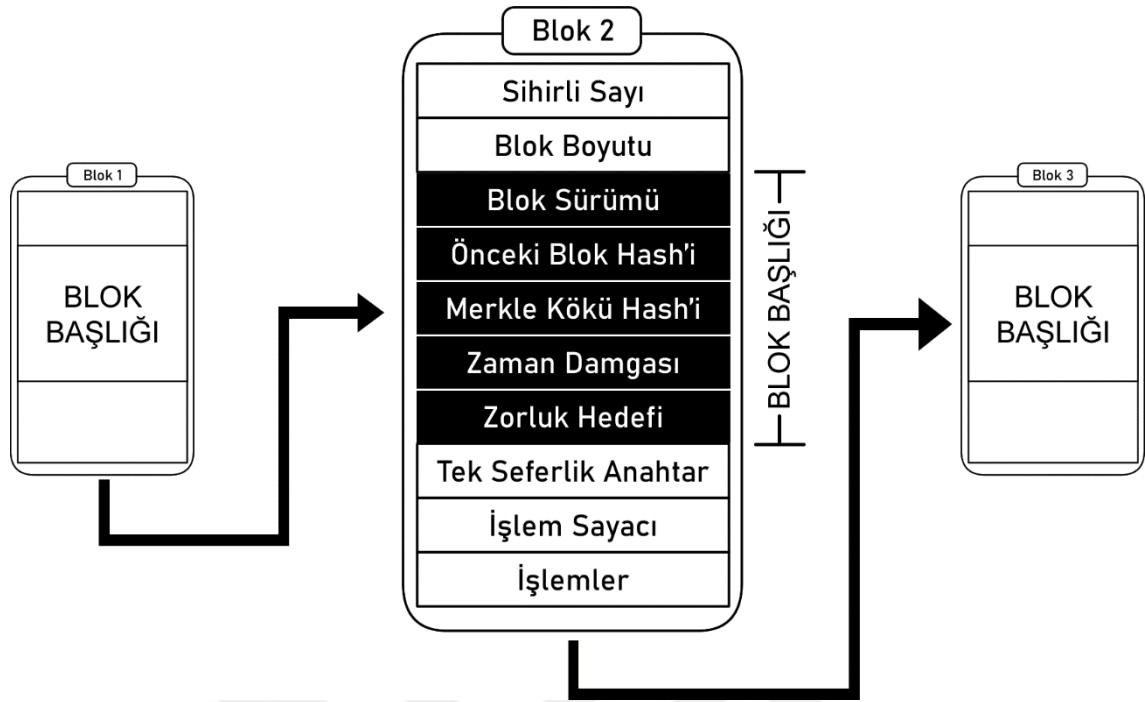
ALAN ADI	BOYUTU	AÇIKLAMASI
Sihirli Sayı	4 Byte	Bloğun başladığını belirtir.
Blok Boyutu	4 Byte	Bloğun büyüklüğünü gösterir.
Sürüm	4 Byte	Bloğun sürümünü gösterir
Önceki Blok Hash'i	32 Byte	Bir önceki blogun hash değeri
Merkle Kökü Hash'i	32 Byte	Bu bloktaki işlemlerin Merkle ağacı kökünün hash değeri
Zaman Damgası	4 Byte	Bloğun oluşturulma zamanı
Zorluk Hedefi	4 Byte	İş ispatında hedeflenen zorluk derecesi
Tek Seferlik Anahtar	4 Byte	Farklı hash değeri bulmak için değiştirilen sayı
İşlem Sayacı	1-9 Byte	Kaç adet işlem olduğunu gösteren sayaç
İşlemler	Değişken	Bloğa kaydedilen işlemler

Kaynak: Antonopoulos, 2017: 197

Zorluk Hedefi: Her zincirin kendine ait blok üretme kuralları bulunmaktadır. Bloğun üretilmesi demek Hash değerinin hesaplanması demektir. Bitcoin zincirinde her bloğun 10 dakikada üretilmesi hedeflenmektedir (Antonopoulos, 2017: 2). Bunun sebebi, iki blok arasının zaman bakımından dar olması durumunda ortaya çıkan senkronizasyon ve “yetim blok” sorununun yaşanmasını engellemektir (Öztürk, 2018). Bunun için iş ispatı yöntemine başvurulmaktadır. Normal şartlar altında ortalama bir bilgisayar bile Hash değerini çok kısa bir sürede hesaplayabilir. Bu süreyi uzatmak için bilgisayardan bir problemi çözmesi istenir. Bu problem ise hesaplanacak Hash değerinin belli bir değerinin altında olmasını istemektir (Joint Research Centre, 2019: 24). Bu da örneğin hesaplanacak Hash değerinin ilk 30 bitinin 0 olmasıdır.

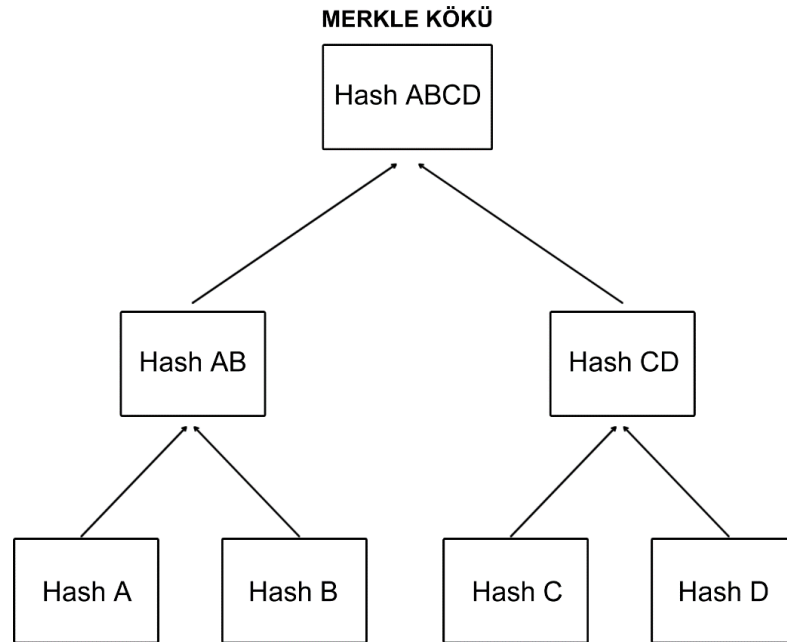
Tek Seferlik Anahtar (Nonce): Nonce, İngilizcede bir kez kullanılan sayı anlamına gelen “*number only used once*” ifadesinin kısaltmasıdır (Frankenfield, 2019). Normal şartlar altında bloğun içeriği değişmediği için hesaplanan Hash değeri her seferinde aynı olacaktır. Bu durumda kuralda istenilen şartların ya da zorluk hedefinin sağlanabilmesi için blok bünyesinde bir değer değiştirilmesi gerekir ki üretilen Hash değeri de farklı olsun (Yaga vd., 2018: 9). Bunun için tek seferlik anahtar olan nonce değeri kullanılır. Bu değer her seferinde değiştirilerek kurala uygun Hash değeri hesaplanmaya çalışılır. Bu aslında bir deneme yanılma yönteminden başka bir şey değildir.

Şekil 2: Blok Yapısı



Kaynak: Güven ve Şahinöz (2018: 54-55)'den esinlenilerek araştırmacı tarafından oluşturulmuştur.

Şekil 3: Merkle Ağacı



Kaynak: Becker, 2008: 8

2.1.4. Dijital İmza

Genel - özel anahtar şifreleme sistemi olarak da bilinen asimetrik anahtar şifreleme, bir blokzincir üzerinde kimlik oluşturma işlevi görmektedir. Ağa girdi yapacak kullanıcı; blokzincir üzerindeki işlemlerini tanımlamaya yardımcı olan bir genel anahtar ve genel anahtarla işlem yürütmek için gerekli olan bir özel anahtar olmak üzere iki öge oluşturmaktadır. Asimetrik şifreleme, yalnızca özel anahtara sahip olanların genel anahtarla şifrelenmiş verilerin şifresini çözmesine izin vererek; ya da genel anahtar şifresini çözmek için verilerin şifrelemesine ve böylece bir imza oluşturmaya imkân tanıyarak kullanıcıların kimlik doğrulamasına izin vermektedir (Jaikaran, 2018: 1).

Asimetrik kriptografide kullanılan dijital imzalar, blokzincirde veri aktarımı sırasında kaydedilen bilgilerin güvenliğini sağlamaya yarayan bir araçtır (Villanueva, 2022). Kişiye özgü olan ve imzalayanları tanımlamak ve dijital belgelerdeki verileri güvenli hale getirmek için kullanılan sanal bir parmak izidir. Dijital bir belgenin geçerliliğini ve özgünlüğünü ve imzalayanın kimliğini sağlayarak yasal düzenlemelere uyumu sağlayan elektronik imza türüdür. Dijital imzalar, bir dijital belgenin menşei, zamanı, kimliği ve durumu hakkında kanıt sağlar. İmza, verilerin imzalayandan geldiğini ve aktarım sırasında değiştirilmediğini ispat eder (Paul, 2017).

Blokzincirde özel anahtar, dijital imzayı oluşturmak için, başka bir deyişle "imzalamak" için; genel şifreleme anahtarı ise dijital imzayı doğrulamak için kullanılır. Dijital olarak imzalanan işlemler bütün blokzincir ağında yayınlanır.

Kaynağın bağlı olduğu genel anahtarın sahibi, kaynağın kilidini kendi özel anahtarıyla açmadıkça (veya şifresini çözmedikçe), blokzincirdeki başka bir kimliğe (bir genel anahtara veya adrese) aktarılmasına ve ikinci kullanıcının özel anahtarıyla kilitlenmesine izin vermedikçe kaynak kullanılamaz. Kaynağın mülkiyetinin değiştiğinin diğer kullanıcılar tarafından doğrulanabilmesi için bu işlem blokzincir üzerindeki günlüğe kaydedilir (Jaikaran, 2018: 2).

Bir dijital imza, imzalama ve doğrulama olmak üzere iki aşamadan oluşmaktadır. Örneğin A kullanıcısı B kullanıcısına dijital imzalı bir mesaj göndermek istediğinde önce verilerini özel anahtarı ile şifreler. Sonrasında B kullanıcısına şifrelenmiş mesajı ve orijinal verileri gönderir. Doğrulama aşamasında B kullanıcısı, eline geçen mesajı A

kullanıcısının genel anahtarı ile doğrular. Böylelikle, B kullanıcısı verilerin bozulup bozulmadığını kolayca kontrol edebilir (Tanrıverdi vd., 2019: 207).

Dijital imzalar ile başlıca üç önemli avantaj elde edilebilir. İlk olarak, bilgi bütünlüğü sağlanır. Şifrelenmiş veri değiştirilirse dijital imza da değişir ve geçersiz olur. İkincisi, bir kimlik kartı gibidir, sahibi bellidir. Böylece iletişim kuran ortaklar, amaçladıkları kişilerle iletişim kurduklarından emin olabilirler. Son olarak, dijital imza “reddedilemezlik” sağlar. Dijital imzalar yasal olarak bağlayıcıdır. Dijital imzanın sahibi yasal olarak yaptığı işlemlerden sorumludur.

2.1.5. Blokzincir Sistemlerinin Sınıflandırılması

Blokzincir sistemleri, özelliklerine göre genel, özel, konsorsiyum ve hibrit blokzincir olmak üzere dört kategoride sınıflandırılmıştır. Bunlar arasındaki temel fark katılımcılara verilen erişim seviyesiyle ilgilidir.

Genel (Public) Blokzincir: Herkese açık olan, geçerli olduğu sürece talep eden herkesin işlem yapabildiği ve hangi blokların zincire ekleneceğini belirleyen mutabakat süreçlerine katılabildiği blokzincirlerdir. Bu yönüyle “izinsiz blokzincirler (permissionless)” olarak da adlandırılırlar (Puthal vd., 2018: 5). En önemli avantajı güven gerektirmemesidir. Bir sistemin merkezi olmasından kaynaklanan güven unsuru, genel blokzincirlerde kriptoekonomik teşvikler (örneğin madencilerin kazançları) ile ikame edilir. Bu blokzincirler “tamamen merkezi olmayan” blokzincirler olarak kabul edilir (Buterin, 2015). Bütün katılımcılar açık olması sebebiyle daha şeffaf ve dışardan gelebilecek saldırılara karşı dirençlidirler. Fakat özel blokzincirlere göre daha yavaşırlar. Aynı zamanda genel blokzincirlerde ölçeklenebilirlik hususu da bir sorun olarak ortaya çıkmaktadır. Fakat genel blokzincirlerde, gizliliğin korunması konusunda endişeler ortaya çıkmıştır. Her ne kadar zincire kaydedilen veriler kriptografik olarak şifrelense de, gizli kalması gereken veriler sürekli olarak herkese açık olan bir ağda depolanırlarsa, ilerleyen zamanlarda ele geçirilme tehlikesine maruz kalabilirler. Bu gibi endişeler özel blokzincirleri doğurmuştur.

Özel (Private) Blokzincir: Sadece belirli katılımcıların, dışarıya kapalı olan bir ağa girmelerine müsaade edildiği blokzincirlerdir. Genellikle küçük bir grup tarafından kontrol edildiği için daha merkezi bir yapısı vardır. İzin verilmeyen kişiler zincire

katılamadıkları için “izinli (permissioned) blokzincir” olarak da adlandırılır (Tanrıverdi vd., 2019: 206). Sınırlı katılımcı nedeniyle mutabakata ulaşmak daha kolaydır. Bu yönüyle genel blokzincirlere göre daha hızlı ve ölçeklenebilir olmalarıyla öne çıkarlar. Fakat merkezi yapısı nedeniyle güvenilirlik ve şeffaflık konusunda genel blokzincirlerin gerisinde kalırlar.

Konsorsiyum (Consortium) Blokzincir: Konsorsiyum blokzincirler, özel blokzincirlerde olduğu gibi blok doğrulama ve uzlaşma işlemlerinin tek bir varlık yerine bir grup düğüm tarafından yönetildiği kısmen özel ve izinli blokzincirlerdir. Bu nedenle, özel blokzincirlerden daha fazla adem-i merkeziyetçi bir yapıdadır ve bu da daha yüksek güvenlik sağlar (Wegrzyn ve Wang, 2021). Ağa kimlerin katılabileceğine ve madencilik yapabileceğine, ağın kimlere açık ya da sınırlı olacağına, kimlerin veri okuma ve yazma yetkilerine sahip olacağına bu düğümlerin oluşturduğu konsorsiyum karar verir.

Hibrit Blokzincir: Hibrit blokzincirler, tek bir kuruluş tarafından kontrol edilen, ancak işlemlerin doğrulamaları halka açık bir gözetim düzeyinde gerçekleştirilen blokzincirlerdir. Zincirdeki işlemleri doğrulamak için yalnızca birkaç düğüm gerektiğinden genel blokzincirlere göre hem daha hesaplı hem de daha hızlıdır. Ayrıca genel blokzincir ağlarından daha ölçeklenebilir özelliktedirler. Hibrit blokzincirin dikkate değer bir örneği, IBM’in tüm gıda tedarik zinciri boyunca verimliliği artırmak için geliştirdiği “Food Trust”tır (Ivičević, 2022).

Tablo 2: Genel, Özel, Hibrit ve Konsorsiyum Blokzincirlerin Karşılaştırılması

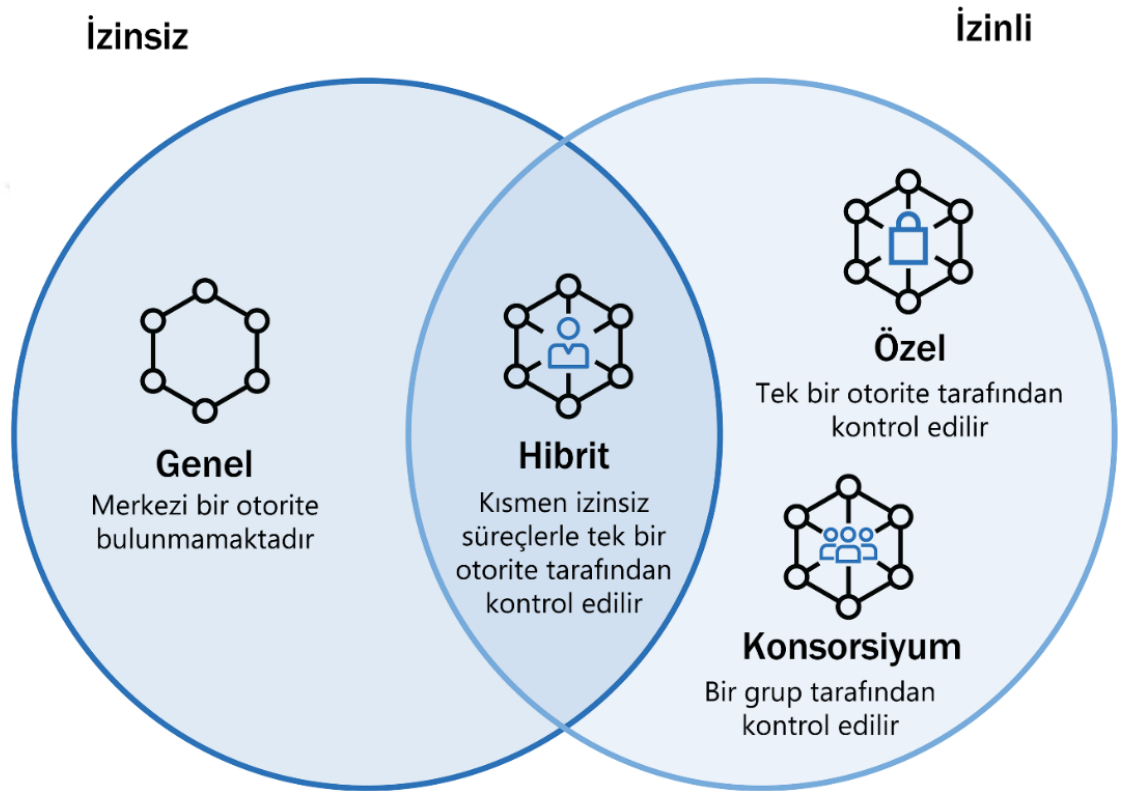
Özellik	Genel Blokzincir	Hibrit Blokzincir	Konsorsiyum Blokzincir	Özel Blokzincir
Uzlaşma sağlayıcılar	Bütün madenciler	Bir organizasyon	Seçilmiş düğümler	Bir organizasyon
Okuma izinleri	Açık	Açık	Açık veya izinli olabilir	Açık veya izinli olabilir
Verimlilik	Düşük	Yüksek	Yüksek	Yüksek
Merkeziyet	Hayır	Kısmen	Kısmen	Evet
Uzlaşma süreçlerine katılım	İzinsiz	Kısmen İzinsiz	İzinli	İzinli

Kaynak: Zheng vd. (2017: 559)’nden esinlenilerek araştırmacı tarafından türetilmiştir.

Tablo 2’de Genel, Özel, Hibrit ve Konsorsiyum blokzincirlerin uzlaşma sağlayıcılar, katılımcıların veri okuma izinleri, verimlilik, merkezilik ve uzlaşma süreçlerine katılım durumlarına göre karşılaştırılmasına yer verilmiştir.

Tabloda yer alan genel, özel, hibrit ve konsorsiyum blokzinciri türlerinin özellikleri Şekil 4’te resmedilmektedir.

Şekil 4: Blokzincir Türleri

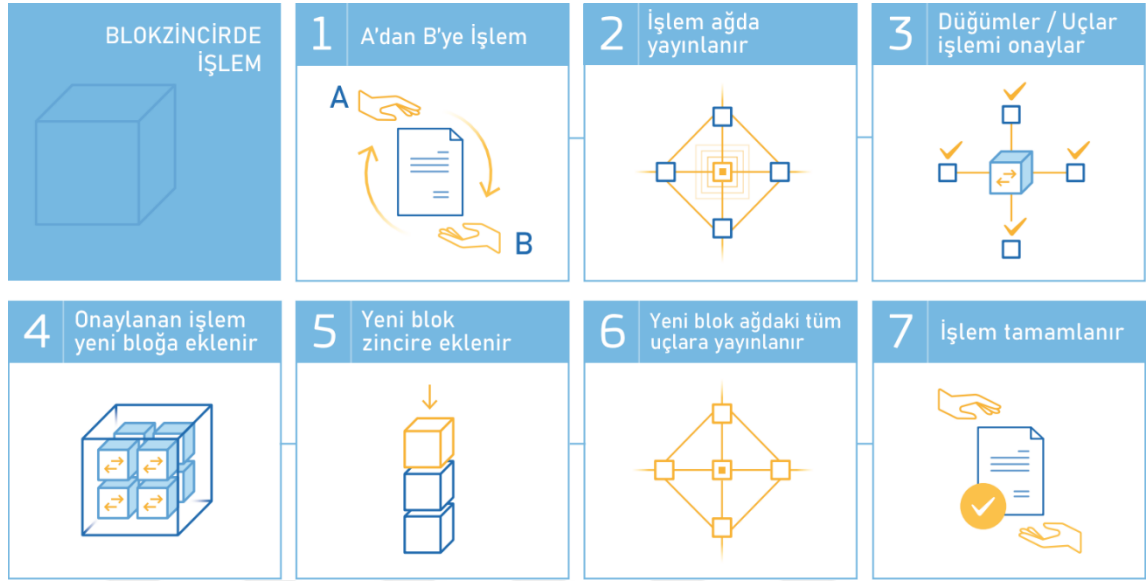


Kaynak: Wegrzyn ve Wang, 2021

2.1.6. Blokzincirde İşlem

Bir işlem kaydının doğrulanması ve zincire eklenmesi süreci çeşitli aşamalardan oluşmaktadır. Bu süreç öncelikle işlemin ağda yayınlanması ile başlamaktadır. Ardından işlemlerin düğümler tarafından onaylanması aşaması gelmektedir. İşlem onaylandıktan sonra yeni bloğa eklenir. Müteakiben yeni blok, bloğu oluşturan düğüm tarafından zincire eklenir. Son olarak bu blok ağdaki tüm uçlara yayınlanarak sürecin tamamlanması sağlanmış olur. Süreç Şekil 5’deki gösterildiği gibi gerçekleşmektedir.

Şekil 5: Blokzincirde İşlem



Kaynak: European Commission, 2019: 14

Örneğin A kişisi B kişisine bir miktar para veya dijital bir varlık göndermek istemektedir. Bu varlık dijital bir cüzdanda depolanmaktadır. A kişisi varlığı göndermek istediği kişinin cüzdan adresini kendi gizli anahtarı ile şifreler. Bu ağdaki başka kişilerin içeriği değiştirmesine engel olur. Şifrelenen işlem ardından yayınlanmak üzere ağa gönderilir. Diğer düğümler dijital imzayı kontrol ederek imzanın A kişisine ait olduğunu teyit ederler. Daha sonra A'nın cüzdanındaki bakiye B'ye göndermek istediği tutar ile uyuyor mu kontrol edilir. Aynı zamanda olası çifte harcama durumları tespit edilir. Kontroller tamamlandıktan sonra onaylanan işlem yeni bloğa dâhil edilir. Blok, zincire eklendikten sonra ağdaki tüm düğümlere / uçlara yayınlanır. Böylelikle işlem tamamlanmış olur.

Blokzincirin güvenliği ve tutarlılığı için bahsedilen kontrollerin sağlanması çok önemlidir. Ayrıca karşılaşılan uyumsuzlukların çözülmesi ve güvenlik açıklarına karşı da bir korumanın oluşturulmalıdır. Blokzincirde merkezi bir otorite mevcut olmadığı için ağdaki uçlar/düğümler tarafından uyulması gereken kurallar belirlenmeli ve bir mutabakat mekanizması oluşturulmalıdır (Tanrıverdi vd., 2019: 208).

2.2. Mutabakat Mekanizmaları

Dağıtık bir sistemde tutarlılık sorunu, 1970'lerden beri üzerinde çalışılan önemli ve klasik bir sorundur. Hesaplamaya yapan düğümlerin güvenilir olmayabileceğine ve başarısız olabileceğine dair temel bir varsayım bulunmaktadır. Normalde başarısızlıklar temel olarak dört türde gelir. Bunlar: ağ arızaları, çökme arızaları, eşzamanlı ve tekrarlanan arızalar ile Bizans başarısızlıkları (Sayson, 2017). Aradaki fark, ilk üçünün sadece normal işlev kaybına sebep olmasıdır. Sonuncusu ise yalnızca düzgün çalışmamakla kalmaz, aynı zamanda normal düğümlerin çalışmasına kötü niyetli saldırılar yapılmasına sebep olabilir.

Bizans başarısızlığı terimi, Leslie Lamport tarafından tanımlanan Bizans Generalleri Probleminden türetilmiştir (Lamport vd., 1982): Bizans Roma İmparatorluğu'nun geniş toprakları bulunması nedeniyle, her bir kraliyet ordusu savunma için birbirinden ayrılmış ve farklı orduların generalleri bilgi alışverişinde bulunmak için yalnızca habercileri kullanabilmektedirler. Her bir eylemden önce, saldırmak veya geri çekilmek konusunda anlaşmaları gerekmektedir. Ancak burada generaller arasında hain bulunması ve diğer generalleri yanlış yönlendirme ihtimalinden ötürü sadık bir general, savaş planını nasıl oluşturacağı sorunu ortaya çıkmaktadır. Bu soruna Bizans Generalleri problemi denmektedir (Wan vd., 2020: 2). Bir blokzincir sisteminde, her düğüm, blokzincir defterinin tutarlılığını sağlamak isteyen bir general olarak görülebilir. Ancak defterin içeriğini kurcalamaya ve daha fazla ekonomik gelir elde etmeye çalışan kötü niyetli düğümler olabilir. Sorunla nasıl başa çıkılacağı, mutabakat mekanizmalarının mevcudiyetine, türüne ve niteliklerine bağlıdır.

Düğümler zincire veri eklemeye ve oluşturdukları blokları ağda yayınlamaya başlamalarının ardından, güvenlik açıklarının önlenmesi için bütün düğümlerin ortak bir güncelleme protokolü üzerinde anlaşma yapmaları gerekmekte ve çoğunluğun onayı alınmadan yeni bir kayıt oluşturulması önlenmelidir. Bu gibi durumlarda blokzincirin tutarlılığının ve güvenliğinin sağlanması için uzlaşma protokolleri geliştirilmiştir (Tanrıverdi vd., 2019: 208). Nakatomo (2008) ilk uzlaşma protokolü olarak İş İspatı (Proof of Work) protokolünü tanıtmıştır. Daha sonra araştırmacılar tarafından bu sistemin zayıf yönlerinden hareketle Pay İspatı (Proof of Stake), Geçen-zaman Kanıtı (Proof of Elapsed-time), Otorite İspatı (Proof of Authority) gibi protokoller geliştirilmiştir.

İş ispatı ve pay ispatı, mutabakat mekanizmaları olarak kullanılan yöntemlerden en yaygın olan ikisidir. Burada amaç, blokları üretenlerin, başka bir deyişle madencilerin üst üste blok üretmelerini engellemek ve salt çoğunluğun onayı olmadan zincire yeni blok eklenmesinin önüne geçmektir. Aksi durumda binlerce madenci her saniye on binlerce blok üretecek ve hepsi birbirinden farklı olarak gelişecek birçok zincir oluşacaktır. Mutabakat mekanizmaları zincirin belirlenen kurallar dâhilinde ilerlemesini sağlayan prosedürlerdir.

2.2.1. İş İspatı

En çok bilinen mutabakat mekanizması, karmaşık bir matematiksel bulmacayı olabildiğince çabuk çözmek için düğümlerin veya “madenci” olarak adlandırılan bilgisayarların hesaplama veya işlem gücüne dayanan “iş ispatı”dır (Proof of Work - PoW) yöntemidir (European Commission, 2019: 16).

Hangi düğümün blok oluşturabileceğini belirlemeye yarayan mutabakat modellerinden ilkidir. Bir bilgisayarın (düğümün), bir iş (işlemi doğrulamak) için çalıştığının ispatlanmasında kullanılır. Bilgisayarlar bazı işlemleri çok hızlı yapabilirler. Örneğin e-posta atmak, çok hızlı yapılabilir bir işlemdir. Bu sebeple, bir bilgisayarın dakikalar içerisinde milyonlarca, istenmeyen e-posta atması da mümkündür. Bunu engellemek için, e-posta sunucusu, e-posta atan bilgisayardan, biraz çalışmasını ve bunu ispatlamasını isteyebilir. Bu sayede, e-posta atmak isteyen bilgisayar, biraz çalışarak, birkaç e-posta atabilecek ama milyonlarca e-posta atması için gerekli zamanı bulamayacaktır.

Blokszincir teknolojisinde de iş ispatı bu maksatla kullanılır. Bilgisayardan ya da madenciden çalışması ya da başka bir deyişle bir problemi çözmesi istenir. Burada bahsedilen problem, kriptografik özet bölümünde belirtildiği gibi bir bloğun hash’inin belirli bir değerin altında olacak şekilde hesaplamasını istemektir. Ağdaki düğümler zincirdeki kuralı sağlayan hash değerini bulabilmek için on binlerce deneme yapar. Kurala uyan blok üretimini ilk yapan madenci hem iş ispatını yapmış olur hem de bloğu zincire yayınlar.

İş ispatı yönteminde madenciler, daha önceden belirlenmiş özelliklere sahip bir hash değerine ulaşmak için karmaşık hesaplamalar yapmaktadır. Temelde Bizans generalleri probleminin bir varyantına olasılıksal bir çözüm sağlarlar.

İdeal olarak iş ispatını hesaplaması zor ama doğrulaması kolay olmalıdır. Zorluğu ayarlanabilir olmalı ve doğrusal olarak hesaplanabilir olmamalıdır. İş ispatı yöntemi, merkezi olmayan bir piyango gibidir. Herkes tek biletle kazanabilir ancak sahip olunan bilet sayısı arttıkça kazanma olasılığı da artar. Örnek olarak Bitcoin, bir veya daha fazla madencinin rastgele seçildiği ve bloklarının zincire dâhil edilmesi maksadıyla buna benzer bir piyango sistemi uygulamak için iş ispatı mekanizması kullanır. Blok başlığının içindeki nonce değeri, blok başlığının hash'i hedeften daha düşük bir hash değeri elde edilene kadar artırılır (Ateniese vd., 2017: 123). Belirlenen hash değerine ulaşan ilk madenci zincire yeni bir blok ekleme hakkı elde eder. İlgili blok hesaplanan hash değeriyle ağa yayımlandıktan ve bütün düğümlerden hash değerinin doğru olduğu onaylandıktan sonra blokzincire eklenir. Müteakiben tüm madencilerin oluşturulan bloğu zincire eklemesiyle bütünlük sağlanmış olur. Bu işlemin ardından yeni bloğu yayınlayan madenci ödüllendirilir (Tanrıverdi vd., 2019: 209).

2.2.2. Pay İspatı

Pay ispatı yönteminde blok oluşturma, blokzincire bağlı belirli miktarda dijital varlığın (örneğin dijital para birimleri) sahiplik kanıtına bağlıdır. Bir sonraki bloğu doğrulamak için belirli bir kanıtlayıcının seçilme olasılığı, kanıtlayıcının sistem içinde sahip olduğu varlıkların payı ile doğru orantılı olarak artar. Bunun altında yatan varsayım, sistem hacminde büyük paya sahip kullanıcıların doğrulama süreciyle ilgili olarak daha güvenilir bilgi sağlayacaklarına ve daha güvenilir bir doğrulayıcı olacaklarına olan inançtır (Tasca ve Tessone, 2019: 11).

Pay ispatı, iş ispatındaki iki sorunu (tek madencilik riski ve madencilik sürecinde boşa harcanan kaynaklar) çözme imkânına sahip olsa da, “nothing at stake” (risksiz işlem) sorunundan etkilenir. İş ispatının aksine pay ispatı yönteminde zincir üzerinde çalışmanın maliyeti çok az olduğu için, çifte harcama yapılmasını önleyen birden çok blokzincir geçmişine oy vererek sistem kötüye kullanılabilir (Rebello vd., 2022: 522-523). Bu sorun, gerçek paya sahip olan kullanıcılar tarafından, yetki verilen ve

önceden belirlenmiş kullanıcılar tarafından blokların oluşturulduğu, Delegated Proof-of-Stake (Yetkilendirilmiş Pay İspatı) yöntemi ile çözülmektedir.

İş ispatı protokolüne pay ispatı protokolü, büyük ölçüde enerji tasarrufu sağlamaktadır. Fakat madencilik maliyeti sıfıra yakın olsa da ağa yapılacak saldırılara karşı daha savunmasız bir yapı sunar.

2.2.3. Yetkilendirilmiş Hisse İspatı

DPoS, doğrulama sürecine dış kaynak kullanılarak PoS'a demokratik bir unsurun eklendiği bir mutabakat mekanizmasıdır. PoS'ta olduğu gibi, blok doğrulama rastgele yapılır ve belirli bir kripto varlığının en yüksek miktarını elinde tutan paydaşın bir bloğu doğrulama ve ödül oluşturma fırsatını kazanma olasılığı daha yüksektir. DPoS modeli, bir bloğu doğrulamak için seçilen paydaşların çalışmalarını üçüncü bir tarafa dış kaynak olarak kullanabilecekleri bir oylama sistemi çalıştırır. Bu üçüncü taraflar "tanıklar" olarak bilinir ve yeni blokların oluşturulması ve onaylanması sırasında fikir birliğine varılmasından sorumludur. Ödüller tanıklar ve paydaşlar arasında paylaştırılır. DPoS'un faydaları arasında enerji tasarrufu, daha fazla merkeziyetsizlik ve olumlu katılımcı davranışları yer alır. Bir ağa değer katan ve iyi bir ağ vatandaşı olan tanıkların tekrar tekrar oylanma olasılığı daha yüksektir (Bains, 2022: 12).

DPoS, token sahiplerinin, işlemleri doğrulamaktan ve yeni bloklar oluşturmaktan sorumlu seçilmiş bir grup delege için oy kullanabileceği bir oylama mekanizması sunar. Bu delegeler genellikle daha az sayıda güvenilir kuruluştan oluşur ve bir miktar merkezi olmayan yapıyı korurken kaynak gereksinimlerini azaltır.

2.2.4. Pratik Bizans Hata Toleransı

Pratik Bizans Hata Toleransı, 90'ların sonlarında Barbara Liskov ve Miguel Castro tarafından tanıtilen bir fikir birliği algoritmasıdır. PBFT, asenkron (isteğe yanıtın ne zaman alınacağına dair üst sınır bulunmayan) sistemlerde verimli çalışacak şekilde tasarlanmıştır. Amaçları arasında Bizans Hata Toleransı ile ilgili sorunları çözmek de yer alır. Bizans Hata Toleransı (BFT), ağdaki bazı düğümlerin yanıt vermemesi veya yanlış bilgilerle yanıt vermesi durumunda bile dağıtık bir ağın mutabakata ulaşma özelliğidir. BFT mekanizmasının amacı, hatalı düğümlerin etkisini azaltarak kolektif karar almak ve böylelikle sistem arızalarına karşı koruma sağlamaktır. Böylelikle tüm dürüst düğümler

çoğunluk kuralını kullanarak sistemin durumu hakkında fikir birliğine varılmasına yardımcı olur. BFT, Bizans Generalleri Probleminden türetilmiştir (Hooda, 2022). PBFT, izin verilen blokzincirlerde kullanılır ve hızlı fikir birliğine odaklanır. Düğümler sırayla blok önerir ve düğümlerin belirli bir yüzdesinin, bir blok eklenmeden önce geçerlilik konusunda anlaşması gerekir.

2.2.5. Geçen Zamanın İspatı

PoET, enerji tüketimini en aza indirirken uzlaşmaya yönelik farklı bir yaklaşım sunan bir mutabakat mekanizmasıdır. Enerji verimliliği göz önünde bulundurularak geliştirilen PoET, merkezi olmayan doğrulama ile kaynak tasarrufu arasında bir denge kurmak üzere tasarlanmıştır. PoET'te katılımcılar hesaplama gücü veya bahis yoluyla değil, rastgele oluşturulmuş bir zaman dilimini bekleyerek rekabet etmektedirler. Burada, bekleme süresini tamamlayan ilk katılımcıya bir sonraki bloğu oluşturma ayrıcalığının verildiği "piyango" konseptinin hayata geçirilmesi amaçlanmıştır. Enerji yoğun İş Kanıtı (PoW) sistemlerinden farklı olarak PoET, blok doğrulayıcıyı belirlemek için zamanın doğal geçişinden yararlanır (Frankenfield ve Anderson, 2023). Dolayısıyla PoET, özel veya izinli blokzincir ağları gibi enerji verimliliğinin en önemli konu olduğu senaryolar için özellikle uygundur. PoET, kaynak yoğun hesaplamalara olan bağımlılığı azaltarak daha sürdürülebilir ve çevre dostu bir blokzincir ekosistemine katkıda bulunurken, aynı zamanda dağıtık defter teknolojisinin merkezi olmayan ve güvenli doğasını da korumaktadır.

2.3. Blokzincirin Üstün Yönleri ve Faydaları

Blokzincirin potansiyeli, sahip olduğu bazı özelliklerinden kaynaklanmaktadır. Burada blokzincir neyi ve hangi sorunu çözmektedir sorusu karşımıza çıkmaktadır. Bunu anlamak için blokzincirin temel özelliklerini anlamak gerekmektedir. Bu karakteristik özellikler şu şekilde sıralanabilir:

2.3.1. Güvenlik, Güven Gerektirmeyen Ortam

Bilgileri güvenli bir şekilde takip etmek ve doğrulamak, blokzincirin en önemli avantajlarından biridir. Blokzincir teknolojisi kriptografik kanıtları esas aldığı için herhangi bir aracıya ihtiyaç duyulmaksızın tarafların birbirleriyle işlem yapabilmesine olanak sağlar (Sultan vd., 2018, 52). Blokzincir, sistemlerin otonom olmasını ve araçların

ve merkezi otoritelerin risklerinden arınmış olmasını sağladığı için, güvene dayalı olmayan sistemler için daha uygun hale gelmektedir. Bununla birlikte, özel blokzincirler kısmen veya tamamen merkezileştirilmiş olabilir, ancak yine de blokzincirin diğer özelliklerinden yararlanmaktadırlar (Sanka vd., 2021: 181).

Blokzincirde tüm işlemler zaman damgalıdır; bir ödeme, sözleşme, mülkiyet devri vb. ile ilgili ayrıntıları barındıran veriler halka açık olarak belirli bir tarih ve saate bağlıdır (European Commission, 2019: 18). Bu, farklı tarafların belirli bir işlemi kimin, ne zaman yaptığını kontrol etmesini sağlar ve kimsenin kaydedilen ve zaman damgalı olan veriyi değiştiremeyeceği anlamına gelir.

Ayrıca blokzincir, veri alışverişlerinin veya işlemlerinin gerçekliğini ve bütünlüğünü sağlamak için genel-özel anahtar kriptografisine güvenir. Katılımcılar, genel ve özel anahtarların birleşimine dayalı olarak farklı bir kimliğe sahiptir: genel anahtarlar, ağdaki diğer kişilerle geniş çapta paylaşılırken, özel anahtarlar gizli tutulur (European Commission, 2019: 18). Örneğin, özel bir anahtarla şifrelenen mesajlar veya işlemler, yalnızca karşılık gelen genel anahtara (gönderen tarafından paylaşılan) sahip alıcılar tarafından açılabilir. Bir mesaj bir ortak anahtarla şifrelenmişse, şifresi yalnızca belirli bir alıcı tarafından kendi özel anahtarını kullanarak çözülebilir.

2.3.2. Dağıtık Yapı, Esneklik, Her Zaman Erişilebilirlik:

Blokzincirde sistemi kontrol eden merkezi bir otoritenin olmaması, blokzincirler için güçlü bir esneklik yaratır. Veriler, ağda aynı anda farklı kullanıcılar (düğümler) tarafından depolanmaktadır. Bir düğüm arızalandığında veya verilerini kaybettiğinde, ağdaki diğer düğümler hala zincirin kopyasına sahip olduğundan zincir güncellenmeye devam eder. Zincir birçok katılımcı tarafından aynı anda tutulduğundan, sistemin tek bir arıza noktası yoktur ve ayrıca sisteme saldırmak çok zordur. Çoklu ve dağıtılmış düğümlerin varlığı, çoğunluğu aynı anda hedeflemeyi veya tüm ağı tamamen bozmayı çok zorlaştırır (European Commission, 2019: 16). Etkilenen düğüm, zinciri diğer düğümlerden yeniden kopyalayabilir. Bu özellik, veri kaybını, kayıtların bozulmasını ve kripto para birimlerinde çifte harcamayı önler (Zhao vd., 2016: 2).

2.3.3. Şeffaflık ve İzlenebilirlik (Denetlenebilirlik):

Doğası gereği merkezi olmayan bir yapıya sahip olduğu için blokzincirde üçüncü bir tarafa ihtiyaç yoktur (Hill vd., 2018: 16). Tüm katılımcılar veya önceden tanımlanmış bir katılımcı grubu blokzincire erişebilmektedir. Özel veya kapalı blokzincirlerde kayıtlara erişim belirli katılımcılarla sınırlandırılabilirken, genel blokzincirlerde ağa internet bağlantısı olan herkes, yürürlükteki mutabakat mekanizmasına göre erişim hakkına sahiptir.

Blokzincir kayıtları zaman damgalı olduğundan ve ağdaki tüm düğümlerde saklandığından, önceki kayıtlar da dâhil olmak üzere tüm faaliyetler ve işlemler ağdaki herkes tarafından kontrol edilebilir ve görülebilir. Bir düğümün adresi biliniyorsa, tüm faaliyetleri ve işlemleri izlenebilmektedir. Zincirde yapılan bütün işlemlerin herkes tarafından görülebilmesi sistemin saydam olmasını ve izlenebilir hale getirmektedir (Schatsky ve Muraskin, 2015: 2; Yang, 2019: 83). Ayrıca blokzincir ile dolandırıcılık tespiti daha kolay sağlanır ve denetim ve kamu hizmetleri için iyi bir araçtır (Government Office for Science, 2016: 71).

2.3.4. Kesinlik ve Değiştirilemezlik (Geri Alınamazlık):

Blok oluşturulup ağa yayımlandıktan ve onaylandıktan sonra kaydedilen işlemler (topluluğun onayı olmadan) geri alınamaz. Bu özelliği sistemin güvenilirliğini temin eder, fakat gerçek gerçek hayattaki uygulamalarda her zaman istenilen bir durum olmayabilir. Nakamoto (2008: 9) da ağa saldıranlar tarafından kayıtların değiştirilmesinin imkânsız değil hesaplama için pratik olmadığını iddia etmiştir. Ağa yayılan işlemlerin her birinin onaylanması ve tüm ağa dağıtılan bloklara kaydedilmesi gerektiğinden zincire mutabakat sağlanmadan müdahale etmek neredeyse imkânsızdır. Ek olarak, yayınlanan her blok diğer düğümler tarafından doğrulanacak ve işlemler kontrol edilecektir. Böylece herhangi bir kurcalama kolayca tespit edilebilecektir (Wang vd., 2018: 357).

2.3.5. Kurcalamaya Direnç

Blokzincirin bir diğer önemli özelliği de işlem kaydını değiştirmenin veya silmenin son derece zor olmasıdır. Bu yalnızca “yüzde 51 saldırısı” veya ağ katılımcılarının mutabakatı ile gerçekleştirilebilir. Blokzincirdeki değişiklikler herkes tarafından görülebilir olduğu için birileri fark etmeden değişiklik yapmak neredeyse

imkansızdır. Genel-özel anahtarlar veya kriptografik imzalar da işlemlerin bütünlüğünü ve kimlik doğrulamasını sağlar.

Bir bloktaki herhangi bir veri değiştiğinde, oluşacak olan mevcut ve müteakip bütün hash'ler değişeceği için, değişikliğin algılanması anlamında blokzincir, (mutabakatsız) müdahaleye (değişikliğe) karşı dirençlidir. Bunu gerçekleştirmek isteyenlerin başarılı olabilmesi için, ağdaki tüm uçlardaki (bilgisayarlardaki) blok verilerini değiştirmesi gerekir ki bu, büyük bir ağ için pratik olarak mümkün değildir (Sanka vd., 2021: 181). Bu nedenle, veriler bu bağlamda müdahaleye karşı blokzincir üzerinde güvence altına alınmıştır.

2.3.6. Anonimlik

Her kullanıcı, oluşturulan bir adresle blokzincir ağıyla etkileşime girebilmektedir. Ayrıca, bir kullanıcı kimliğinin açığa çıkmasını önlemek için birçok adres üretebilir. Çünkü kullanıcıların özel bilgilerini tutan herhangi bir merkezi otorite yoktur. Bu mekanizma, blokzincirde yer alan işlemlerde belirli bir miktarda gizlilik sağlamaktadır. Fakat blokzincir içsel sınırlılıkları nedeniyle mükemmel derecede gizlilik vaat etmemektedir (Wang vd., 2018: 357).

2.3.7. Sansüre Direnç

Blokzincir sistemindeki ekonomik getiriler, düğümlerin blokları doğrulamaya devam etmesini teşvik ederek önceki blokların değiştirilmesi için dışarıdan gelecek etkilere karşı dirençli olmasını sağlar (Kejriwal ve Mahajan, 2017: 2).

2.3.8. Maliyet Tasarrufu

Geleneksel merkezi sistemlerde, her işlemin güvenilir bir kurum (örneğin merkez bankası) aracılığıyla doğrulanması gerekir, bu da kaçınılmaz olarak merkezi sunucularda maliyet ve performans darboğazlarına neden olur. Farklı olarak, blokzincir ağındaki bir işlem, herhangi iki eş (P2P) arasında, merkezi kurum tarafından kimlik doğrulaması yapılmadan gerçekleştirilebilir. Bu şekilde blokzincir, geliştirme ve işletme maliyetleri dâhil olmak üzere sunucu maliyetlerini azaltma potansiyeline sahiptir (Wang vd., 2018: 357).

Blokszincirde, aracı sistemlerle ilişkili maliyetlerden tasarruf edildiğinden büyük maliyet tasarrufu sağlanabilir. Blokszincir verimli kullanıldığında bankalar tarafından yılda yaklaşık 20 milyar dolar tasarruf edilebilir (Steenis vd., 2016: 15). Bu, bazı bankaların ve işletmelerin maliyetleri azaltmak için blokszinciri sistemlerine dâhil etmek istemelerinin nedenlerinden biridir (Sanka vd., 2021: 181). Diğer teknolojiler gibi, blokszincirde de maliyetler zamanla azalacak; bilgi işlem, depolama ve bant genişliğinde yetenekler zamanla artacaktır (Deloitte, 2018: 4).

2.3.9. Verimlilik

Blokszincir, alt sistemlerdeki araçların kaldırmasından kaynaklanan verimlilikle sistemlerin otonom olarak çalışmasına olanak sağlar. Bu, birçok şirket ve ülkenin blokszincir kullanımından elde etmeye çalıştığı faydalar arasında yer almaktadır (Sanka vd., 2021: 181). Blokszincir, güveni sağlamanın daha verimli bir yolunu ortaya koyar. Verilen değiştirilemez karakteristiği, dolandırıcılık ihtimalini azaltarak tarafların birbirine olan güvenini arttırmaktadır (Deloitte, 2018: 5). Örneğin, işlem yapan iki paydaş kendi işlem kayıtlarını tutması gerekmeyecek, bunun yerine blokszinciri tek gerçek kaynak olarak kullanabilecektir.

Blokszincirde kayıtlı işlemlerin tahakkuku neredeyse gerçek zamanlı olarak gerçekleşmektedir. Bu yönüyle olası ihtilafları ve riski azaltır fakat bu aynı zamanda işlemlerin geri alınmasını zorlaştırır. Burada blokszincirin hızı ele alınırken kullanım amacına göre değerlendirmeli ve neye göre hızlı neye göre yavaş olduğunun göreceli olduğu unutulmamalıdır.

2.4. Blokszincirin Zayıf Yönleri ve Blokszincire Yöneltilen Eleştiriler

Blokszincir teknolojisinin sahip olduğu büyük potansiyele rağmen yaygın kullanımını sınırlayan bazı zorluklar da bulunmaktadır. Karşılaşılan zorluklardan bazıları aşağıda açıklanmıştır.

2.4.1. Güvenlik

Blokszincir teknolojisi oldukça güvenli bir veri yapısı vaat etmesine rağmen (Chhina vd., 2019: 766), uygulamada özellikle halka açık, çoğunlukla kripto para birimleri gibi genel blokszincirlerde bazı güvenlik açıklarıyla karşılaşmıştır. Özel, hibrit ve konsorsiyum blokszincirler, kısıtlı erişimleri nedeniyle daha güvenlidir (Sanka vd.

2021: 195). Dolandırıcılıklar, kötü amaçlı yazılım saldırıları, hizmet reddi (DoS), Sybil saldırıları, uygulama ve ağ güvenlik açıkları yaygın olarak bildirilen güvenlik sorunlarıdır (Meng vd., 2018: 10186). Saldırılar veya kullanıcı hatasıyla özel anahtarların kaybı da büyük güvenlik açıklarına neden olmaktadır.

Madencilik, özellikle büyük ölçekli genel blokzincirler için çok yüksek miktarda bilgi işlem gücü gerektirir. Ancak bir madenci veya bir grup madenci yeterli kaynağı toplayabilirse, bir blokzincir ağının madencilik gücünün yüzde 50'sinden fazlasını elde edebilir (Lin ve Liao, 2017: 656). Gücün yüzde 50'sinden fazlasına sahip olmak, defter üzerinde kontrol sahibi olmak ve onu manipüle etme yeteneği anlamına gelir. Yeni işlem bloklarını kaydetme rekabeti, birkaç büyük madencilik havuzunun işlem kaydının çoğunluğunu kontrol ettiği anlamına gelen madencilikte merkezileşme eğilimini doğurabilir (Swan, 2015: 83). Ancak, bu tür saldırılar, daha çok blokzincir uygulamasının küçük bir toplulukta olduğu ve madenci sayısının daha az olduğu ağlarda görülmüştür (Al-Jaroodi ve Mohamed, 2019: 36508).

Kimlik Dolandırıcılığı Saldırıları: Kimlik dolandırıcılığı, bir kullanıcının kimlik bilgilerini elde etmek için yapılan bir dolandırıcılık girişimidir. Dolandırıcılar, cüzdan anahtarı sahiplerine meşru bir kaynaktan geliyormuş gibi görünecek şekilde tasarlanmış e-postalar gönderirler. E-postalar, sahte köprüler kullanarak kullanıcılardan kimlik bilgilerini ister. Bir kullanıcının kimlik bilgilerine ve diğer hassas bilgilere erişim sahibi olmak, kullanıcı ve blokzincir ağı için kayıplara neden olabilmektedir (IBM, 2022).

Yönlendirme (Routing) Saldırıları: Blokzincir teknolojisi gerçek zamanlı, büyük veri aktarımlarına dayanmaktadır. Bilgisayar korsanları (hackerlar), internet servis sağlayıcılarına aktarılan verileri yakalayabilirler. Bir yönlendirme saldırısında, blokzincir katılımcıları genellikle tehdidi anlayamaz, bu nedenle her şey normal görünür. Fakat, perde arkasında dolandırıcılar gizli verileri veya para birimlerini ele geçirebilirler (Apostolaki vd., 2017: 1).

Sybil Saldırıları: Sybil ile çoklu kimlik bozukluğu teşhisi konulan ünlü bir kitap karakterine atıfta bulunmaktadır. Sybil saldırısında bilgisayar korsanları, ağa akın etmek için birçok sahte ağ kimliği oluşturmakta ve sistemi çökertmeye çalışmaktadır (Douceur, 2002: 1).

2.4.2. Ölçeklenebilirlik

Ölçeklenebilirlik, bir sistemin artan sayıda ögeyi veya nesneyi barındırma, artan iş hacimlerini incelikle işleme ve/veya genişlemeye duyarlı olma yeteneğini ifade etmektedir (Bondi, 2000: 195).

Temel olarak ölçeklenebilirlik sorunu, blokzincirdeki artan sayıda düğüm ve işlem nedeniyle ortaya çıkmaktadır. Blokzincir ağında bulunan her düğüm doğrulama ve uzlaşma işlemleri için bütün blok verilerini saklamak zorunda olduğundan zincir giderek hantal hale gelmekte ve zincir boyutu sürekli olarak artmaktadır. Bu sorun, özellikle Bitcoin ve Ethereum gibi genel blokzincirlerde görülmektedir. Çünkü her düğümün, her işlemi doğrulaması için hesaplamalı bir görevi depolaması ve yürütmesi gerekir. Bu yüzden özellikle halka açık blokzincirler, her zaman büyük miktarda hesaplama gücüne, yüksek bant genişliği olan bir internet bağlantısına ve büyük depolama alanına gereksinim duymaktadır (Khan vd., 2021: 2).

Örneğin Bitcoin blokzincirinde saniyede yaklaşık 7 işlem onaylanmaktadır. Diğer ödeme yöntemleriyle karşılaştırıldığında Bitcoin çok yavaş kalmaktadır. Örneğin VISA ağının (VisaNet) saniyede 65.000 işlem gerçekleştirebilme yeteneğine sahip olduğu iddia edilmektedir (VISA, 2022). Blokzincirin blok yapısından kaynaklanan sınırlılıkların dışında, madencilerin yüksek gelir elde edebilmek için büyük miktardaki para transferine öncelik vermesi ve küçük miktardaki işlemleri göz ardı etmeleri nedeniyle de işlem sürelerinde gecikmeler yaşanabilmektedir (Tanrıverdi vd., 2019: 211).

2.4.3. Gizlilik

Blokzincir karakteristik olarak merkezi bir idare ya da otorite olmadan sistemin işletilmesini sağlamaktadır. Kullanıcılar, gerçek kimliklerini açığa vurmada genel ve özel anahtarlarıyla işlem yapabilmekte ve gizliliklerini koruyabilmektedirler. Aynı şekilde blokzincirde yapılan işlemlerin izlenebilirliği esas olduğu için; alıcı, gönderen, zaman ve transfer edilen değer gibi veriler herkesin görebileceği şekilde yayınlanmaktadır (Tanrıverdi vd., 2019: 212). Ancak bu özellikler aynı zamanda sistemin en çok eleştiri alan noktalarını da oluşturmaktadır. Blokzincir, kullanıcıların yaptıkları işlem kayıtlarından, kiminle alışveriş yaptıklarına ve bakiye bilgilerine kadar gizli kalması istenen bilgilerin ele geçirilmesine olanak vermektedir. Paylaşılan bu verilerin üçüncü taraflar tarafından analiz edilmesi sonucu kullanıcıların gerçek kimliklerine

eriřim de mmkn olabilmektedir (Wang vd., 2018: 367). Bu durum, gerek devletler gerek de iřletmeler aısından istenmeyen bir durumdur. nk kontrol edilmeyen bir sistemin iřleyiři ve her katılımcının verilere ulařması ciddi endiřelerin ortaya ıkmasını da beraberinde getirmektedir (Uma Uysal ve Kurt, 2018: 471). Bu soruna zm olarak zel, konsorsiyum ve hibrit blokzincirleri řeklinde sınıflandırmalara gidilmiřtir.

Blokzincirde karřılařılabilecek bu tr gizlilik ihlallerine karřı anonimlięi geliřtirmek iin bazı alıřmalar yapılmıřtır. Bu alıřmalar karıřtırma ve anonimleřtirme olarak iki kategoride incelenmektedir. Bilindięi gibi blokzincirde kullanıcı adresleri anonimdir. Ancak birok kullanıcı aynı adresle sık sık iřlem yaptığı iin adresleri kullanıcıların gerek kimlięiyle baędařtırmak mmkndr. Karıřtırma, birden ok giriř adresinden birden ok ıkıř adresine veri aktararak anonimlik saęlayan bir hizmet trdr (Mser, 2013). Anonimleřtirme ise iřlem grafięi analizini nlemek iin deme kaynaklarının baęlantısını kaldırmaya yarayan bir yntemdir (Joshi vd., 2018: 140).

2.4.4. Bencil Madencilik

Bencil madencilik, blokzincirdeki bařka bir gvenlik aıęıdır. Genel olarak, yzde 51'in zerinde bilgi iřlem gcne sahip dęmlerin blokzinciri tersine evirebileceęine inanılsa da son arařtırmalar, yzde 51'den daha az gce sahip dęmlerin bile hala tehlikeli olabileceęini gstermektedir (Wang vd., 2018: 368). Eyal ve Sirer (2013: 17), aęın kk bir blmne ait bilgisayar gcnn bile kt niyetli saldırılarıyla blokzinciri savunmasız bırakabileceęini bildirmiřtir. Kt niyetli ve yksek bilgi iřlem gcne sahip madenciler, rakipsiz kaldıklarında en uzun zinciri oluřturana kadar ıkardıkları geerli blokları yayınlamayabilirler. Daha sonra kendi oluřturdukları yeni bloęu yayınladıklarında ise yeni zincir en uzun zincir haline gelir ve ana zincir olarak kabul edilir (Grunspan ve Prez-Marco, 2018: 2). Bunun neticesinde, drst madencilerin ıkarttığı asıl bloklar reddedilmiř olur. Bu, drst madencileri iřlem yapmaktan caydırır ve kayıplara uęramalarına neden olur. Aynı zamanda aęın leklenebilirlięine ve gvenlięine zarar verir.

2.4.5. Deęiřtirilemezlik

Blokzincirin deęiřtirilemez veya geri alınamaz olması, ya da bir sonraki maddede aıklandığı gibi deęiřiklięin ok zor olması da eleřtirilere konu olmaktadır. Blokzincir, belirli řartlarda, kiřinin řahsi verilerinin silinmesini isteme ya da unutulma hakkından

ödün vermesine yol açabilecektir. Ayrıca herhangi bir nedenle internet hizmetini kullanamayan kişiler, yaptıkları işlemlerde kendilerini daha fazla kontrol altına alacak olan gelişmelerin avantajlarından tam ve doğrudan yararlanamayabilir (Akdemir Altunbaşak, 2018: 369).

2.4.6. Kurcalamaya Karşı Dirençlilik

Kurcalamaya karşı dayanıklılığın "değişmez" veya "değiştirilemez" ile aynı şey olmadığına dikkat etmek önemlidir. Merkezi olmayan doğasına rağmen, bu teknoloji bireylerin veya grupların kayıtları değiştirmesine karşı varsayımsal olarak tamamen koruma sağlamamaktadır. Ayrıca, yürürlükteki mutabakat mekanizmasına bağlı olarak, bir blokzincirdeki katılımcılar aslında oy kullanabilir veya değişiklik yapmayı veya kaydı değiştirmeyi seçebilir (European Commission, 2019: 17). Bu, kurcalamaya karşı dayanıklılığın "değiştirilemez" değil, "değiştirilmesi zor" olarak anlaşılması gerektiği anlamına gelir (Walsch, 2017: 713-714).

Mutabakat yoluyla işlemlerin kaydını veya zincirin tamamını değiştirmesi daha önce vuku bulmuştur. Bu konuda en tartışmalı vaka, fon hırsızlığının, "çatallanma (hard fork)" yönündeki bir topluluk kararıyla geri yüklendiği "DAO hack'i"dir. Bu vaka, blokzincirin ne derece güvenli olduğu konusunda geniş tartışmalara yol açmıştır. Aynı zamanda yönetişimin de önemini ortaya koymuştur. Çünkü blokzincir, hala belirli rollere sahip olan ve gerekli olduğunda müdahale edebilen bir dizi aracıya (geliştiriciler, madenciler, kullanıcılar ve diğer katılımcılar) sorunları düzeltmek, sistemi yükseltmek veya istenmeyen sonuçları tersine çevirmek için ihtiyaç duymaktadır (European Commission, 2019: 17).

2.4.7. Boyut ve Bant genişliği

1 Ocak 2023 itibarıyla, Bitcoin blokzincirinin boyutu 445 GB'ı geçmiştir (Blockchain.com, 2022). VISA'nın işlem hacmi Bitcoin tarafından işlenecek olsaydı, tüm blokzincir verisinin tam olarak kopyalanması çok uzun zaman alır ve büyük sorunlar doğururdu (Yli-Huumo vd., 2016: 3). Bitcoin topluluğu, bir bloğun boyutunun 1 MB olduğunu ve her on dakikada bir blok oluşturulduğunu varsaymaktadır. Bu nedenle, gerçekleştirilebilecek işlem sayısında bir sınırlama vardır (bir blokta ortalama 500 işlem) (Antonopoulos, 2017: 196). Her ne kadar bu veriler sadece Bitcoin için geçerli olsa da,

yaygın kullanım amaçlayan her blokzincir ağı, boyut ve bant genişliği sorunlarını çözülmelidir.

2.4.8. Adem-i Merkeziyetçilik

Son zamanlarda yapılan bazı araştırmalar, blokzincirin adem-i merkeziyetçilik iddiasını reddetmektedir. Gencer vd. (2018)'lerine göre sınırlı sayıda katılımcının olduğu veya madenciliğin büyük ölçekli madencilik havuzları arasında toplandığı blokzincir sistemlerine ait kanıtlar (Rauchs vd., 2018: 44-45), gerçekte çok az zincirin gerçekten merkezi olmadığını göstermektedir. Örneğin, belirtilen durumlar, bilgi işlem kaynaklarının çoğunluğunu kontrol eden bir grup katılımcının olası gizli anlaşmaları durumunda zinciri saldırıya (ör. yüzde 51 saldırısı) açık hale getirebilir.

2.4.9. Boşa Harcanan Kaynaklar

İş ispatı yönteminin geçerli olduğu blokzincirlerde madencilik muazzam miktarda enerji tüketmekte ve bunun da tamamı çevresel anlamda boşa gitmektedir. Daha önce belirtilen tahminlerde madencilik günlük 15 milyon dolarlık enerjini boşa harcanmasına sebep olmaktadır. Şimdiki tahminler ise bu rakama göre çok daha yüksektir. Bir yandan, madenciliği güvenilir kılan süreç aynı zamanda israfa da sebep olmaktadır. Çünkü madenciler, kazanç için başka bir işe yaramayan bir çaba uğruna enerji harcamaktadırlar (Swan, 2015: 83).

2.5. Blokzincirin Geleceği

Blokzincir teknolojisi gerçek hayattaki ilk uygulamasını 2009 yılında Bitcoin'in piyasaya sürülmesiyle bulmuştur. O zamandan bu yana çeşitli sektörlerdeki girişimciler, teknolojinin potansiyelini keşfetmeye çalışmaktadır. Blokzincirin geleceği hakkında tahminde bulunurken, benzer şekilde çılgır açıcı teknolojilerin geçmişinden ders alınabilir. Bu noktada masaüstü bilgisayarların gelişimi örnek olarak verilebilir.

Masaüstü bilgisayarlar 1970'lerde ilk kez piyasaya çıktığında az sayıdaki erken meraklılar arasında bir pazar bulmuştur. Fakat asıl başarı, VisiCalc adı verilen bir elektronik tablo programı olan ilk "mükemmel uygulama"nın geliştirilmesiyle elde edilmiştir. Yazılım, getirdiği kullanışlılık ve esneklik ile büyük ve küçük işletmelerin bilgisayarı satın almasında bir dönüm noktası olmuştur. IBM uyumlu masaüstü bilgisayarlar sahneye çıktığında ise satın almanın gerekçesi Lotus 1-2-3 olmuştur. IBM

PC, makul fiyata iyi bir teknoloji olarak kendini gösterse de, Lotus 1-2-3'ü çalıştırmak bir gereklilik haline gelinceye kadar yükselişe geçmemiştir. Microsoft Windows, 1980'lerde PC kullanıcılarına pek çok yenilik sunmuştur. Ancak Windows olmadan kullanılamayacak bir üretkenlik araçları paketi olan Microsoft Office'in piyasaya sürülmesine kadar geleceği belirsiz olmuştur. Birkaç yıl sonra ise Microsoft'un kurucusu Bill Gates, internet tarayıcısını Windows 95'in en etkili uygulaması olarak tanımlamıştır (KRIPTOMAT, 2022).

Blokszincirin geleceğinin de benzer yolu izleyeceğini düşünmek için birçok haklı sebep mevcuttur. Teknoloji; ilk kişisel bilgisayarlar, IBM PC veya Microsoft Windows gibi bir altyapı niteliğindedir. Blokszincirin yararlı olabileceği tüm pazarlarda potansiyelini ortaya çıkarabilmesi için, öncelikle pazarlar arasında geniş bir ilgi uyandıran vazgeçilmez bir uygulama veya hizmetin temelini ortaya koyması gerekmektedir. İnsanlar “blokszincir neden önemlidir?” sorusu sorulduğunda “karşı konulmaz bir hizmet sağlıyor” cevabını verilebilmelidir (KRIPTOMAT, 2022).

Blokszincir teknolojisi altyapısı kullanılarak ortaya konulan ürünler arasında en yaygın ürün olan Bitcoin ve bazı diğer kripto para birimleri olup bunların yakın gelecekte insan hayatını kalıcı bir şekilde etkileyeceğini söylemek (örneğin günlük alışverişlerde tamamen kripto paraların kullanımı gibi), en azından şimdilik zor görünmektedir. Kripto para birimleri tek başına blokszincirin tam potansiyeline ulaşması için yeterli değildir. Eğer blokszincir sadece bu işe yararsa, blokszincirin ana akım teknoloji haline gelmeyi başaramamasının nedenlerinden birinin de bu olacağı söylenebilir.

Bazı araştırmacılar, blokszincir teknolojisi konusunda son derece heyecanlı olduklarını belirtse de, çoğu insanın geleneksel hükümet (itfaiye teşkilatları, ordu) tarafından sağlanan hizmetleri talep etmeye ve bunlara ihtiyaç duymaya devam edeceklerine inandıklarını belirtmektedirler. Buna göre hükümetlerin yerini blokszincir teknolojisinin alması yerine, teknolojinin ilerleyerek hükümetlerin vatandaşlarına hizmet etme şeklini geliştirmesi daha olasıdır. Benzer şekilde geleneksel olarak hükümetler tarafından sağlanan bazı hizmetlerin yerini blokszincir destekli mutabakat mekanizmalarının alması ihtimali daha yüksek görülmektedir. Fakat ulusal hükümetler ve onların sağladığı hizmetlerin mevcudiyetini sürdüreceğine olan inanç ağır basmaktadır (ConsenSys Media, 2018).

Yeni teknolojilerin yayılma ve benimsenmesinin bilgi, ikna, karar, uygulama ve doğrulama olmak üzere beş temel aşaması bulunmaktadır (Prager vd., 2021). Blokzincir şu anda büyük ölçüde bu sürecin erken geliştirme aşamalarında ve pazarın nispeten küçük bir bölümü, uygulama ve onaylamanın sonraki aşamalarına ilerlemiştir. Bir PWC anketi, yanıt veren şirketlerin yüzde 20'sinin araştırma aşamasında, yüzde 30'unun geliştirme aşamasında, yüzde 10'unun pilot aşamada olduğunu ve yüzde 15'inin aktif blokzincir projeleri yürüttüğünü ortaya çıkarmıştır (PwC, 2018: 2).

TÜSİAD'ın Deloitte ile yaptırdığı bir ankette (2018: 22) katılımcılara “Blokzincir teknolojisinin gelecek dönemde şirketinizi ne derece etkileyeceğini düşünüyorsunuz?” sorusu sorulmuş; katılımcıların yüzde 10,3'ü blokzincir teknolojisinin önümüzdeki 1 yıl içerisinde şirketlerini önemli ölçüde etkileyeceğini düşündüğünü belirtirken yüzde 33,6'sı ise henüz bir şey söyleyebilmek için erken olduğunu belirtmişlerdir. Aynı soru önümüzdeki 5 yıl için tekrarlandığında ise şirketlerini önemli ölçüde etkileyeceğini düşünen katılımcıların oranının yüzde 26,2'ye yükseldiği, diğer taraftan ise henüz bir şey söyleyebilmek için erken olduğunu söyleyen katılımcıların oranının yüzde 16,7'ye düştüğü görülmüştür. Bu da blokzincir teknolojisinin Türkiye'de kısa vadeden ziyade orta vadede etki göstereceği beklentisini olduğunu ortaya koymaktadır. Blokzincir teknolojisinin gelecek 5 yılda şirketini hiç etkilemeyeceğini düşünenlerin oranı ise yüzde 1,9'da kalmaktadır.

Yapılan bazı araştırmalara göre kuantum tabanlı bilgisayarlar, keşfedilmeleriyle birlikte en güçlü geleneksel bilgisayarların bile çözemediği şifreleme yöntemlerini kırabilme potansiyeline sahip olacaktır (Werbach, 2018: 513). Kuantum bilgisayarların geliştirilmesi, bilgisayar bilimleri ve kriptografi alanlarında önemli değişikliklere yol açabilir. Klasik bilgisayarlar üzerinde çalışan bazı kriptografi algoritmaları, kuantum bilgisayarlar tarafından hızlı bir şekilde çözülebilir. Bunun ne zaman olabileceği konusunda net bir fikir birliği olmamakla birlikte (European Commission, 2019: 19) blokzincir teknolojisi de bu değişikliklerden etkilenebilir. Ancak, kuantum tabanlı bilgisayarlar geliştirildiğinde kuantum dirençli blokzincir protokollerinin de geliştirileceği düşüncesi ile bu sorunların üstesinden gelinebileceği iddia edilmektedir (Usta ve Doğanekin, 2018: 101).

Özetle blokzincir, gelecekte büyük potansiyel taşıyan ve birçok sektörü dönüştürebilecek bir teknolojik inovasyon olarak görülmektedir. İlerleyen yıllarda, finans, sağlık, tedarik zinciri yönetimi ve kamu yönetimi gibi birçok sektörde daha fazla benimsenmesi beklenmektedir. Blokzincir, güvenli ve şeffaf veri saklama ve paylaşma yeteneği nedeniyle iş ve yönetim süreçlerini optimize edebilir, dolandırıcılığı azaltabilir ve kaynakların daha verimli kullanılmasına yardımcı olabilir. Ancak, bunların gerçekleştirilebilmesi için müteakip bölümlerde daha detaylı olarak incelenen bazı engellerin aşılması gerekmektedir. Gelecekte, devletlerin gerekli adımları atmasıyla kitlesel benimsemenin temin edilmesi ve vatandaşların günlük yaşamları üzerindeki etkisinin artması sağlanabilecektir.

2.6. Bir Blokzincir Uygulaması Olarak Bitcoin

Bitcoin, blokzincir teknolojisini kullanan, tamamen dijital bir para birimi, ödeme sistemi ve merkezi olmayan bir mutabakat ağıdır. Sistem üzerinde, kullanıcılar birbirlerine aracı olmadan doğrudan transferler yapabilir. Transferler merkezi olmayan dağıtık bir kayıt ve mutabakat sistemi olan blokzincire kaydedilir. Bitcoin ağı üzerinde transfer edilen değer birimi Bitcoin (BTC) olarak adlandırılır. Bitcoin, blokzincirin şifreli (kriptolu) yapısı nedeniyle kripto para olarak da tanımlanır. Fiziksel olarak kullanılmaz, tamamen dijital olarak üretilip, eşler arası ağ üzerinden transfer edilir.

2.6.1. Bitcoin Nedir?

Bitcoin, ikili sayı anlamındaki “binary digit” ve madeni para anlamındaki “coin” kelimelerinin birleşiminden oluşmaktadır (Sheldon, 2022). 2008 yılında Satoshi Nakamoto rumuzlu bir kişi ya da ekibin yayınladığı doküman (Nakamoto, 2008) ile hayata geçen, sahibi ve merkezi olmayan bir ödeme aracı ve para birimidir. Herhangi bir kurum ya da kuruluşa bağlı değildir. Temsilciliği ya da bayileri yoktur. Herkesin kullanımına açık bir teknolojidir ve isteyen herkes herhangi bir engelleme ya da kısıtlama olmadan ağa katılabilir, cüzdandan cüzdanda herhangi bir aracıya gerek olmadan transfer yapabilir, blokzincirin bir kopyasını cihazında saklayabilir.

Bitcoinde, teknoloji olarak blokzincir kullanır fakat aslında blokzinciri var eden bitcoindir. Daha doğrusu bitcoin, blokzincir teknolojisinin ilk örneğidir.

Bitcoin, dijital bir cüzdanda saklanabilen ve para birimi olarak çalışmak üzere tasarlanmış dijital bir tokendir (jetondur). İşlemleri güvence altına almak ve kontrolsüz üretimini engellemek için şifreleme (kriptografi) teknikleri kullanıldığı için genellikle kripto para birimi olarak adlandırılır. Bitcoin en çok bilinen dijital para birimidir, ancak ondan önce üretilen dijital para birimleri de olmuştur. Onu benzersiz kılan şey, önceki dijital paraların çözemediği özellikle çifte harcama gibi sorunları yenilikçi ve merkezi olmayan bir doğrulama sistemi aracılığıyla çözmesidir (The Institutes, 2017: 10).

Bitcoin eşler arası bir ağıdır. Örneğin Visa ve MasterCard gibi kredi kartı sistemlerinde veya PayPal gibi online bir ödeme sisteminde, ortada ödemeleri merkezileştiren, ağı işleten ve güvenliğini sağlayan kâr amacı güden bir şirket bulunmaktadır. Ancak Bitcoin'in tamamen farklı bir çalışma modeli bulunmaktadır, güvenliği bir merkez tarafından değil kriptografik bir algoritma olan, 256 bitlik Secure Hash Algorithm (SHA-256) ile temin edilmektedir (Rose, 2015: 619).

Bitcoin arzı merkezi bir otorite tarafından yapılmamaktadır. Madenci olarak adlandırılan ve Bitcoin açık kaynak kodunu çalıştırarak işlemci gücü ile küresel Bitcoin ağına katılan herkes tarafından üretimi yapılabilir. Madencilik ismi, altın ve gümüş gibi insanlık tarihinde değer saklama aracı olarak kullanılmış madenlerin elde edilmesi için yapılan sürece atfen verilmiştir. Madenciler bitcoin yazılımı ile belirlenen matematiksel hesaplamayı çözmek için birbiriyle yarışır. Problemin sonucuna ilk olarak ulaşan madenci belirli bir miktar Bitcoin ile ödüllendirilir. Bitcoin ağının işlem gücüne göre blok üretme oranı 10 dakikada bir bitcoin üretilecek şekilde problemin zorluğu artar veya azalır (Narayanan vd., 2016: 206). Madencilere verilen ödül yaklaşık her dört yılda bir yarıya inmektedir. Kurala göre bitcoin arzı her iki yüz on bin (210.000) üretildiğinde yarıya inecektir. Bu sürece yarılanma (halving) denmektedir. Toplamda üretilecek bitcoin sayısı 21 milyon ile sınırlandırılmıştır (Narayanan vd., 2016: 95).

Bitcoin mevcut durumda reel ekonomiye henüz tam anlamıyla entegre değildir. Bu yüzden Bitcoin'in fiyat hareketlerinin gerçek değerinden bağımsız olarak popülerliği ile orantılı şekilde artıp azaldığını düşünen kimi araştırmacılar (Dulupçu vd., 2017) VAR Modeline dayanan Varyans Ayrıştırma Analizi ve Granger Nedensellik Testleri kullanarak bu hipotezlerini sınamışlardır. Araştırmanın verileri, Bitcoin'in ABD doları cinsinden karşılığı ile dolaşımdaki Bitcoin miktarı ve tanınırlığını yansıtacağı düşüncesi

ile Google arama motorunda aylık frekansta “bitcoin” sözcüğü içeren arama sayıları kullanılarak elde edilmiştir. Sonuçlar, Bitcoin’in tanınırlığı ve fiyatı arasında çok güçlü bir ilişki olduğunu ve aralarındaki nedenselliğin yönünün Bitcoin’in tanınırlığından fiyatına doğru olduğunu göstermiştir. Dolayısıyla Bitcoin’in bilinirliği arttıkça fiyatı da yükselmektedir. Başka bir deyişle Bitcoin’in fiyatının gerçek değerinden çok spekülative hareketlere bağlı olduğu söylenebilir (Çetiner, 2018: 8-9).

Bitcoin sisteminde merkezi bir otorite olmaması ve yapılan işlemlerde tarafların öğrenilebileceği merci bulunmaması, yasa dışı finansal aktivitelere olanak sağlamakta; kazançların vergi dışına çıkarılması, kara para aklama ve terörün finansmanı gibi alanlarda kullanılması riskini ortaya çıkarmaktadır (Bozkurt Yüksel, 2016: 195).

Bitcoin, yakın geçmişte ortaya çıkmış ve gelecekte dünyadaki etkisinin ne olacağı henüz kestirilemeyen bir finansal enstrümandır. Daha ucuza ödeme sağlaması, daha hızlı işlem gerçekleştirmesi, anonimliği muhafaza etme gibi özellikleri yanında daha da yaygınlaşması için; kullanım kolaylığı, satıcılar tarafından benimsenme, daha fazla kullanım alanı sunma gibi konularda gelişime ihtiyaç duyan bir değişim ve değer saklama aracıdır. Genel kabul oranının artması için kullanıcı deneyiminin iyileştirilmesi gerekmektedir (Çetiner, 2018: 14).

Bitcoin en başından itibaren bir kripto para olarak tasarlandığı için kamu sektörünün kullanacağı genel maksatlı bir platform olması planlanmamıştır. Fakat yine de bu teknolojinin potansiyelinin birçok toplulukta farklı şekillerde paylaşılması için Bitcoin blokzincirinde yeni uygulamalar geliştirilmiştir. Bu geliştirmeler Bitcoin’in açıklığını ve dönüşebilen yapısını göstermektedir (Ølnes ve Jansen, 2018: 6).

Özetle Bitcoin; güvenilir bir değer saklama vasıtası olup işlem maliyetini minimum düzeyde tutmayı amaçlayan, global piyasalara erişim sağlayan, ödemelerin hızlı ve anonim bir şekilde gerçekleştirilebildiği, kayıtları kalıcı olup depolama maliyetini asgari seviyede tutan aracısız bir ödeme aracıdır. Bu gibi avantajlarının yanında, daha çok yeni ve halen tam olarak kendini ispatlamamış ve yaygınlaşmamış, yasal boşluklar içeren ve değeri spekülative bir teknoloji ürünüdür (Çetiner, 2018: 14). Bu ürünün, sunduğu fırsatlarla birlikte henüz öngörülemeyen ve kullanımla birlikte ortaya çıkacak olan bilinmeyen noktaları da mevcuttur.

2.6.2. Bitcoin'in Tarihçesi

İnsanlık tarihi boyunca para, fiziksel olarak değişik şekillere bürünmüştür. İlk metal paranın geçmişi M.Ö. 1000'li yıllara kadar uzanır. Bu paralar, bronz ve bakır gibi değerli metallere üretilmiştir. Zamanla bu madeni paralar, bugün parayla ilişkilendirilen gümüş ve altına dönüşmüştür. Madeni paralar, insanların ağırlıktan ziyade miktara (madeni para sayısı) göre ödeme yapmasına izin veren ilk para birimleri olduğu için para tarihinde büyük kilometre taşı oldular (Ritchie, 2022).

Bugün paranın yaşadığı dönüşümün geldiği nokta paranın dijitalleşmesidir. 1980'lerin sonlarında, Avrupa'da benzin istasyonlarının hırsızlığa karşı korunmak için, kartlara para yüklenmesi talebi ve bu kartlar ile yakıt alınabilmesi, elektronik ödemenin ilk örneklerinden sayılmaktadır. Yine benzer tarihlerde mağaza sahiplerinin, müşterilerine ait banka hesaplarından doğrudan ödeme yapabilmeleri için bankalara baskı yapmaları sonucunda POS cihazları kullanılmaya başlanmıştır (BCTR, 2022).

Paranın dijitalleşmesi sürecinde kriptoloji kullanımının öncü çalışmalarından ilki, matematikçi David Chaum tarafından 1983 yılında yayınlanan makaledir (Chaum, 1983). David Chaum daha sonra 1990 yılında Amerika'daki ilk kriptografik elektronik ödeme sistemi olan DigiCash'i geliştirmiştir. Bu sistemin en önemli özelliği, tam bir para birimi olmamasına rağmen hesaplar arası hızlı ve kolay transfer ile kullanıcılarına gizlilik sağlaması olmuştur. Fakat sistem başarı sağlayamadığı için geliştirici şirket 1998 yılında batmıştır (Usta ve Doğantekin, 2018: 44). DigiCash'in ardından First Visual ve PayPal elektronik ödeme sistemi olarak kullanılmaya başlanmıştır. PayPal sistemi dijital para olarak gerçek para birimine dayanmaktadır. Devletlerin yasal yükümlülüklerine uyumludur (Pirinççi, 2018: 3) ve halen aktif olarak işlemektedir.

Bitcoin, mucidi Satoshi Nakamoto tarafından, 2008 krizinin sorumlusu olarak kabul edilen merkez bankalarının kontrol ettiği parasal sisteme alternatif olması için üretildiği öne sürülmektedir (Shen ve Pena-Mora, 2018: 3).

Bitcoin piyasaya sunulmuş ilk kripto para olarak görülse de daha önce kriptografi ile korunan dağıtık defter teknolojisi girişimleri (B-Money ve Bit Gold) olmuştur (Marr, 2017).

Fiyatının astronomik bir şekilde artması hem Bitcoin'e hem de aynı zamanda blokzincire olan merakı oldukça arttırmıştır. Global anlamda para transferleri için oldukça etkin bir yöntem olmasının yanı sıra halihazırda vergilendirilemiyor oluşu da sistemin çekiciliğini arttırmaktadır (Çetiner, 2018: 5). Bitcoin'e olan artan talebin üç temel nedeni bulunmaktadır:

İlk olarak, bitcoin de altın gibi nadir bulunur özelliktedir. Nakamoto tarafından ortaya konan para politikasına göre, 2140 yılına dolaşıma kadar yaklaşık olarak toplam 21 milyon bitcoin girecektir. Bu da onu nadir bulunan bir dijital değer saklama aracı haline getirmektedir.

Bitcoin'in piyasa talebi oluşturmalarının ikinci nedeni, elektronik iletim yoluyla nakit paraya benzer bir eşler arası değişim sunmasıydı. Bitcoin'ler bir e-posta kadar kolay bir şekilde gönderilebilmektedir. Her işlem kaydedilmesine rağmen, bitcoin genellikle anonim olarak kabul edilir. Çünkü kriptografi, insanların kişisel bilgilerini ifşa etmeden bitcoin işlemleri yapmasını mümkün kılar. Bitcoin'leri elektronik olarak gönderme yeteneği ve sistemin neredeyse tamamen anonim olması, online sistemlere güvenin azaldığı bir zamanda bitcoin'i popüler hale getirmiştir. Bununla birlikte, bitcoin'in kendi anonimliği de, itibarını kaçınılmaz olarak zedeleyen dolandırıcıların ilgisini çekmiştir (The Institutes, 2017: 11).

Son olarak, 2008'deki global krizde finansal sisteme olan güven aşınmıştır ve bitcoin geleneksel bankacılık sistemine bir alternatif olarak öne çıkmıştır. Bitcoin'in eşler arası işlem protokolü, bankalarda para saklama ihtiyacını ortadan kaldırmıştır. Bitcoin, Federal Rezerv'in alışılmadık para politikalarına (sıfır faiz oranı politikası ve niceliksel genişleme gibi) karşı korunmak için alternatif yatırımlar arayanlar için hızla cazip hale gelmiştir. Mevcut bankacılık zeminindeki hayal kırıklığı büyüdükçe, bitcoin, erken benimseyen birçok kişinin temel değişikliğe yol açabileceğini düşündüğü alternatif bir yapı sağlamıştır.

2.6.3. Bitcoin'de İşlem

Bitcoin blokzincirinde taraflar arasındaki kripto para transfer işlemleri kayıt altına alınır. İşlemdeki her tarafın bir açık anahtarı bir de özel anahtarı vardır. Açık anahtarın hash değeri, kimlik ya da işlem adresi olarak kullanılır. Taraflar işlemi özel anahtarlarını kullanarak imzalar. Diğer katılımcılar daha sonra imzalayanın açık anahtarı ile bu işlemi

teyit eder. İşlemler daha sonra ağdaki bütün katılımcılara yayınlanır. Dağıtık bir mutabakat mekanizması ile hangi işlemlerin geçerli olduğu ve gerçekleşen işlemlerin sırası katılımcılar tarafından kararlaştırılır. Bu işlemler blok olarak isimlendirilen veri yapılarına dönüştürülerek ortak veri tabanına yüklenir. Böylelikle birbirine bağlı veri bloklarından oluşan zincir ortaya çıkmış olur. Zincirdeki her blok kendini bir önceki bloğa bağlayan bir zaman damgasına ve kriptografik özete sahiptir. Bloklar sadece eklenebilir, silinemezler. Sonuç; sürekli büyüyen ve değiştirilemez ve geri döndürülemez kayıtlardan oluşan ortak veri tabanıdır (Shen ve Pena-Mora, 2018: 4).

Bitcoin blokzincirini güvenilir kılan blokların özet fonksiyonlarıyla birbirlerine bağlanmasından çok mutabakat modeli ve iş ispatı yöntemidir. Blokları özet göstergeleri (bir önceki bloğun özet bilgisi) ile birbirine bağlamak zincire yapılacak müdahaleleri açığa çıkartırken iş ispatı zinciri bu müdahalelerden korumaktadır. İş ispatı tabanlı güvenlik modeli, zincire zarar vermenin maliyetinin bu işlemi yapmakla elde edilecek getiriden fazla olacağı kabulüne dayanmaktadır (Ølne ve Jansen, 2018: 2).

2.6.4. Bitcoin Madenciliği

"Madencilik" kelimesi, değerli metallerin çıkarılmasını çağrıştırarak, her blokta oluşturulan "Bitcoin" ödülüne dikkatleri çekmektedir. Fakat madencilik bu ödülle teşvik edilse de, madenciliğin birincil amacı ödül olarak görülmemelidir. Madencilik, işlemlerin doğrulandığı ve onaylandığı merkezi olmayan takas odasının temelini oluşturan mekanizmadır. Madencilik, dijital paranın uçtan uca iletilmesinin temelini oluşturan ve merkezi olmayan bir güvenlik mekanizması olan Bitcoin blokzincirini özel hale getiren buluştur (Antonopoulos, 2017: 213).

Madencilik, Bitcoin sistemini güvence altına alır ve merkezi bir otorite olmadan ağ çapında fikir birliğinin ortaya çıkmasını sağlar. Yeni basılan coinlerin ve işlem ücretlerinin ödülü, madencilerin eylemlerini ağın güvenliği ile uyumlu hale getirirken aynı zamanda parasal arzı destekleyen bir teşvik planıdır (Antonopoulos, 2017: 213).

Bitcoin madenciliği ile hileli işlemler önlenir ve çifte harcama engellenir. Onaylanmış transfer işlemleri, Bitcoin blokzincirine madenciler vasıtasıyla yapılır. Zincire bloğu ekleyen madenci, yeni bloğun üretilmesi ile arz edilen para ve Bitcoin işlemlerindeki işlem masrafı ile ödüllendirilir (Çarkacıoğlu, 2016: 46).

Henüz onaylanmamış Bitcoin transfer işlemleri, geçici olarak onaylanmamış işlemler havuzunda tutulurlar. Madencilerin havuzları ağdaki gecikmeler sebebiyle aynı olmak zorunda da değildir. Bu havuzdaki işlemlerden bir blok/öbek oluşturmak ve zincire bu bloğu eklemek her madenci için oldukça kolay ve hızla halledilebilecek bir süreçtir. Fakat bu durumda her madenci kendi oluşturduğu bloğu zincire eklemek isteyeceği için ağ karmaşası oluşacaktır. Bunu önlemek maksadıyla, blok oluşturmak isteyen madencilerden, birbirleriyle rekabet etmeleri ve bunu ispatlamaları talep edilir. Bu, iş ispatı yöntemiyle gerçekleştirilir ve sonunda madencilerden sadece bir tanesinin bloğu geçerli olur (Çarkacıoğlu, 2016: 46). Bitcoin blokzincirinde ortalama olarak 10 dakikada bir blok üretilmesi hedeflenmektedir. Bu hedef, iş ispatının, zorluk seviyesi otomatik olarak değiştirilerek gerçekleştirilir. Bir madenci, iş ispatını yapmasını müteakiben, bu bilgiyi ağ ile paylaşır. Bunu alan diğer uçlar üretilen bloğun zincir yazılımı ile uyumlu olup olmadığını kontrol eder. Bloğun kurallara uygun olarak üretildiği diğer uçlar tarafından da teyit edildikten sonra, blok, zincirin sonuna eklenir.

ÜÇÜNCÜ BÖLÜM

3. BLOKZİNCİR VE KAMU YÖNETİMİ

Bu bölümde öncelikle kamu yönetiminin sorunları ve kamu yönetimlerini değişime zorlayan etkenler ele alınmaktadır. Daha sonra blokzincirin kamu yönetimine sağlayacağı faydalar incelenmektedir. Son olarak da blokzincirin genel kullanım alanları ve kamu yönetimindeki kullanım alanlarına değinilmektedir.

3.1. Kamu Yönetimini Değişime Zorlayan Etkenler

Yaşadığımız çağ, yapısı itibariyle hayatın her alanında hızlı bir değişimi barındırmaktadır. Bu değişim bireyleri olduğu kadar ülkeleri ve kurumları da etkilemektedir. Dünyada yaşanan bu değişim, özellikle yönetim anlayışında köklü bir yeniden yapılanmayı gündeme getirmiştir. Bu dönüşüme sebep olan etkenler dört başlık altında özetlenebilir.

3.1.1. Ekonomik Etkenler

1970’li yıllardan itibaren yaşanan küresel krizler ile bazı gelişmiş ülkelerde bile kamu finansmanı ile ilgili mali sorunlar ortaya çıkmaya başlamıştır. Bu problemler çoğunlukla devletin iktisadi faaliyetlere müdahale etmesi, devlet etkinlik alanının genişlemesi ve devletin boyutunun artması ile bağlantılı olarak değerlendirilmiş ve 1980’lerin başından itibaren kamu bütçesinin küçültülmesi, kamuda istihdamın azaltılması, vergi düzeyinin indirilmesi gibi devletin küçültülmesine yönelik, Keynesçiliğin çöküşü ve Refah devleti anlayışının terkedilmesi anlamına gelen konular siyasi hayatın merkezine yerleşmiştir (Gökçe ve Turan, 2008: 192-193). Bu kapsamda devletin ekonomideki rolü sorgulanmaya başlanmış ve özel sektörün uygulamalarını örnek alan liberal yaklaşım benimsenmeye başlamıştır.

3.1.2. Yönetimsel Etkenler

Geleneksel kamu yönetimi, 19’uncu yüzyılın ikinci yarısında sanayi devriminden başlayarak 20’nci yüzyılın son çeyreğine kadar kamu yönetiminde geçerli olan hâkim paradigmanın adıdır. Geleneksel kamu yönetimi anlayışının entelektüel temelleri, büyük ölçüde Woodrow Wilson, Fredrick Taylor, Henri Fayol ve Max Weber’in düşüncelerine

dayanmaktadır (Eryılmaz vd., 2019: 8). Wilson yönetimde siyaset yönetim ayrımını (dikotomi), Taylor işlerin bilimsel ve verimlilik esasına göre yapılmasını, Fayol işlerin yerine getirilmesinde yönetim işlevlerinin (PÖYED) uygulanmasını ve Weber ise mal ve hizmetlerin sunumunda bürokrasi modelinin yerine getirilmesini savunmuştur. Bu dönemde ortaya çıkan kamu hizmeti anlayışında kamu yönetiminin geleneksel yapısına uygun düşecek biçimde kamu hizmetlerinin sunulması görevi devlete yüklenmiştir (Önen ve Kahraman, 2022: 426).

Kamu yönetimini değişime iten etkenlerin kabullenilmesine yol açan sebepler, geleneksel yönetim anlayışının eksikliklerinden kaynaklanmaktadır. Sanayi toplumunun örgütlenme modeli olan mekanik örgütlenme modeli, birtakım başarılarının yanında önemli zayıflıkları da beraberinde getirmiştir. Geleneksel kamu yönetimi anlayışı, istikrarlı dönemlerinde elde ettiği başarılarına rağmen, hızlı ve yaygın bir teknolojik değişimin yaşandığı günümüzde işlevselliğini kaybetmiştir. Bu modelin esneklikten yoksun olması, değişen şartlara uyum sağlamada önemli sorunlar yaşanmasına neden olmuştur (Al, 2022: 97). Bu çerçevede prosedürlerden çok sonuç odaklı, sadece harcama yapmayı değil para kazanmayı da ilke edinen (girişimci), piyasa mekanizmalarını bürokratik mekanizmalara tercih eden (piyasa yönelimli), kürek çeken değil dümen tutan (katalizör), hizmet sunduğu vatandaşları ‘müşteri’ olarak yeniden tanımlayan (müşteri odaklı), hizmet sunan birimler arasında rekabeti özendiren, kamu örgütlerinin katı kural ve düzenlemelerle yönetilmesi yerine amaçları gerçekleştirmeye yönelik etkinlikleri ön plana çıkaran (amaçlara yönelmiş), sorunlar ortaya çıktıktan sonra harekete geçmekten ziyade sorunların önlenmesine önem veren uzak görüşlü bir yönetim anlayışı ortaya çıkmıştır (Eryılmaz vd., 2019: 62). Başka bir ifade ile, devletin ne yapması gerektiğinden ziyade yüklendiği işlevleri nasıl yapması gerektiği yeniden tanımlanmaya başlanmıştır.

3.1.3. Özel Sektörün Kaydettiği Gelişmeler

Piyasa koşullarının rekabet şartları içinde gelişen özel sektörün dinamizmi ve yeniliklere uyum sağlama becerisi, kamuda yaşanan gelişmelerin tetikleyicisi olmuştur. Gelişen teknolojiler ve organizasyon teknikleri kullanarak verimliliğini ve rekabet gücünü artıran özel sektör karşısında kamu kuruluşları, sanayi toplumuna özgü hantal ve büyük ölçekli yapıları ile rekabet edemez hale gelmişlerdir. Verimliliği artan özel sektör; sermaye hareketlerinin serbestleştiği birçok ülkede gelişimin ana dinamiği haline

gelmiştir. Bu gelişim karşısında, klasik olarak kamu tarafından yürütülen birçok mal ve hizmetin özel sektöre açılması, kamu kurumlarının çalışma süreçlerinde esnekliklerin artırılması, kamunun çeşitli hizmetleri piyasadan tedarik etmesi ve özel sektörde gelişen yaklaşımlara uyarlanması gündeme gelmiştir (Dinçer ve Yılmaz, 2003: 22).

3.1.4. Sosyolojik Etkenler

Küreselleşme hem doğrudan hem de dolaylı olarak, kamu yönetiminin yapısına ve işleyişine etki etmektedir. Halkların yönetime katılma kapsamındaki istekleri gün geçtikçe artmaktadır. Bu anlamda vatandaşların hükümetlerden beklentileri ve talepleri birçok ülkede benzerlik göstermektedir. Vatandaşlar gelişmiş ülkelerin yönetimleriyle yaşadıkları ülkenin yönetimini mukayese etmekte ve yeni taleplerde bulunmaktadırlar (Al, 2022: 66-67).

Türkiye’de de kamuda gelir gider dengesinin bozulması, kalkınmanın yavaşlaması ve istihdamın düşmesi, vergilerin artması ve buna rağmen kamu hizmetlerinde etkinliği azalması, kamuda kurumsal yapının ve personel politikasının günümüz standartlara ulaştırılamaması ve vatandaşların, haklarının bilincine varması ve daha kaliteli hizmet talep etmesi gibi sebepler, kamu yönetimini değişime zorlamaktadır. Modern dünyada artık, kamu yönetimlerini yeniden yapılandırma yaklaşımlarının merkezinde bilgi teknolojilerinin kullanımının yaygınlaştırılması yer almaya başlamaktadır (Öktem ve Aydın, 2005: 258). Kısaca küreselleşme ve bilgi toplumuna geçiş şeklinde özetlenebilecek bu süreçte bilginin ve teknolojik gelişmenin katkısı belirleyici hale gelmiştir. Bu yönüyle etkili ve halkın taleplerine cevap verebilen standartlarda kamu hizmeti verebilmek için, kamu hizmetinin sunumunda bilgi teknolojilerinin kullanılmasının önemi ortaya çıkmaktadır.

3.2. Kamu Yönetiminde Bilgi Teknolojilerinin Kullanımı

Geleneksel yönetim yaklaşımından yeni kamu işletmeciliğine kadar geçen süreç içerisinde yönetim anlayışı, ülkelerin sahip oldukları yönetim şekillerinden teknolojik atılımlara, sosyal-toplumsal değişimlerden küreselleşmeye kadar farklı unsurların etkisinde bir dönüşüm geçirmiştir. 1980’li yıllardan itibaren yönetimde ortaya çıkan ağ tipi toplum ve yönetim modelinde; veri iletimindeki gelişmeler ile bilgi paylaşımı ve mal

ve sermaye dolaşımı hızlanmış, kamusal mal ve hizmetlerin sunumunda ağlar, ilişkiler ve entegrasyon gibi kavramlar önem kazanmaya başlamıştır (Şahin ve Örselli, 2016: 47-79).

Yaşanan dönüşümler, toplumsal ve yönetsel birtakım değişimleri ya beraberinde getirmiş ya da zorunlu kılmıştır. Örneğin buhar makinesinin üretimde kullanılması ile el emeğinin yerini makinelerin alması 1'inci Endüstri Devrimini doğurmuştur. 1'inci Endüstri Devrimi'nin önemli getirilerinden biri de demir yolu ağının yaygınlaşması ve ulaşımın ivme kazanması olmuştur. Birinci sanayi devrimi, bir diğer adıyla Endüstri 1.0 olarak ifade edilen bu dönem sanayileşme sürecinin, dört aşamasının birinci basamağını oluşturmuştur (Koca, 2020: 4534). Bir önceki dönem su ve buhar gücüyle çalışan tezgahların üretime geçmesi, elektriğin üretime girmesi ve iş bölümünde uzmanlaşmanın artması 2'nci Endüstri Devrimi'ne (Endüstri 2.0) geçişi hazırlamıştır. Henry Ford'un yeni enerji türü elektriği üretimde kullanmasıyla seri üretime geçişi sağlaması ise o dönemin sembolü olmuştur. (Berktaş ve Oraklıbel, 2021: 2).

1960 - 1990 yılları arasında teknolojinin de ilerlemesi ile 3'üncü Endüstri Devrimi olgunlaşmaya başlamıştır. Yaygınlaşan bilgisayar kullanımı ile daha önce kâğıtlarda saklanan her türlü bilginin dijital ortama aktarılarak bilginin dijitalleşmesi süreci hızlanmıştır. Günümüzde kullanılan yazılımlarının temelleri atılmış ve geliştirilen bu yazılımlar sayesinde bilgi dijitalleşmiştir. Geliştirilen yazılımların etkili bir şekilde kullanılabilmesi için yeni nesil donanımlar üretilmiş ve kullanılmıştır (Özdoğan, 2017: 25). Bu dönem elektronik ve bilgi teknolojilerinin ileri seviye imalat aşamalarında kullanılmaya başladığı dönem olmuştur.

3'üncü Endüstri Devrimi'nin ardından siber-robotik teknolojilerin üretime katılmasıyla 4'üncü Endüstri Devrimi başlamıştır. Bu iki dönemin ortak özelliği, yeni bir "bilginin" öğrenilmesi ve onun üretim sürecine dâhil edilmesi olmuştur (Karagöz, 2020: 17). Almanca "Industrie 4.0" kelimesinden türetilen Endüstri 4.0, kavramı; imal ve üretim alanlarında büyük veri analitiğini kullanabilen bir dizi bağlantılı siber-fiziksel nesne olarak tanımlanmaktadır (Vogel-Heuser ve Hess, 2016: 411). Kavram, Alman hükümetinin yürüttüğü üretimin bilgisayarlaştırılması temalı bir proje ile ortaya çıkmış ve resmi olarak ilk kez 2011 yılında Hannover Fuarı'nda kullanılmıştır. Daha önceki sanayi devrimlerinin önemli dönüşümlerden ilham alan projede, yeni dönem Endüstri 4.0. olarak adlandırmıştır (Banger, 2016: 79).

Kavramın kuramsal olarak gündeme gelmesi ise Kagermann vd. tarafından 2011 yılında yayınlanan “Endüstri 4.0: Nesnelerin interneti ile 4. Endüstri Devrimine Giderken” başlıklı makale ile olmuştur (Kagermann vd., 2011). Makalede dünyanın yeni bir sürece girdiği ve bu sürecin Endüstri 4.0 olarak adlandırılması gerektiği aktarılmakta ve bu dönemi oluşturan bileşenler hakkında bilgi verilmektedir (Soylu, 2018: 45).

3.2.1. E-Devlet ve Kamu Yönetiminde Dijitalleşme

E-Devlet kavramı ilk olarak “elektronik hükümet” şeklinde 1993 yılında ABD’de yayımlanan “Ulusal Performans Değerlendirmesi” adlı çalışmada kullanılmıştır. Kavramın e-devlet veya e-hükümet olarak ilk kez kullanılması ise 1997 yılında yayımlanan bir çalışmada olmuştur ve o tarihten itibaren gelişim süreci başlamıştır (Heeks ve Bailur, 2007: 244).

E-devlet, genel olarak "çevrimiçi devlet hizmetlerinden", "vatandaşlar, işletmeler ve devletin diğer kolları ile elektronik olarak bilgi ve hizmet alışverişine" kadar her şeyi ifade etmek için kullanılmıştır. Geleneksel olarak e-devlet, devlet kurumlarının verimliliğini artırmak ve devlet hizmetlerini çevrimiçi sağlamak için BİT’in kullanımı olarak kabul edilmiştir. Daha sonra, e-devletin çerçevesi, vatandaşlar ve işletmelerle çok çeşitli etkileşimleri yürütmek için devlet tarafından BİT kullanımını ve ayrıca açık devlet verilerini ve yönetişimde yenilikçiliği sağlamak için BİT kullanımını içerecek şekilde genişletilmiştir (UN, 2023).

Kamu yönetiminde hizmetlerin dijital ortamda sunulmasıyla başlayan e-Devlet çalışmaları, bilişim teknolojilerinin ve internetin yaygınlaşmasıyla birlikte sadece hizmetlerin değil; yazışmaların, belgelerin, mevzuatın ve personelin de elektronik ortama aktarıldığı bir dijital dönüşüm sürecine evrilmiştir. Kimi ülkeler e-Devlet kavramını Dijital Devlet olarak algılarken kimi ülkeler kavramı akıllı devlet veya dijital yönetişim gibi tanımlamalar altında hayata geçirmeye başlamıştır (Karagöz, 2020: 21).

Dijital devlet, kamu değeri yaratmak için hükümetlerin modernizasyon stratejilerinin entegre bir parçası olarak dijital teknolojilerin kullanılması anlamına gelmektedir. Devlet aktörleri; STK’lar, işletmeler, vatandaş dernekleri ve hükümetle etkileşimler yoluyla veri, hizmet ve içeriğin üretimini ve bunlara erişimi destekleyen bireylerden oluşan bir dijital hükümet ekosistemine dayanmaktadır (OECD, 2014: 6).

Dolayısıyla e-devlet, devlet hizmetlerini vatandaşlara ve işletmelere daha etkin ve verimli bir şekilde sunmak için BİT'in kullanılması olarak tanımlanabilir. BİT'in devlet operasyonlarında uygulanması, kamu amaçlarına dijital yollarla ulaşılmasıdır. Etkili bir e-yönetişim kurumsal çerçevesi tarafından desteklenen e-devletin altında yatan ilke, iş akışlarını ve süreçleri daha iyi entegre etmek ve sürdürülebilir çözümler hedefleyen çeşitli kamu sektörü kurumlarında etkin kaynak kullanımını sağlamak için finansal maliyetleri ve işlem sürelerini azaltarak kamu sektörünün iç işleyişini iyileştirmektir. İnovasyon ve e-devlet sayesinde, dünyanın her yerindeki hükümetler daha verimli olabilir, daha iyi hizmetler sunabilir, vatandaşların şeffaflık ve hesap verebilirlik taleplerine yanıt verebilir, daha kapsayıcı olabilir ve böylece vatandaşların hükümetlerine olan güvenini geri kazanabilir (UN, 2023).

E-devlet kavramı kendiliğinden oluşmuş bir kavram değildir. Aksine, zaman içerisinde vatandaşların giderek artan ihtiyaçlarının yarattığı, bilgi ve iletişim teknolojileri yardımıyla ayakta duracak, yeni bir devlet anlayışının ifadesi olarak ortaya çıkmıştır (İnce, 2001: 12). Başka bir ifadeyle, e-devletin bugünkü konuma gelmesi bir süreci ifade etmektedir. Bu süreç Leigh ve Atkinson (2001: 6-8) tarafından üç dönemde incelenmiştir:

- Birinci dönem (1993-1998); internetin bilgi paylaşımı amacıyla kullanıldığı dönemdir. Bilgi sunmak amacıyla ortaya çıkan e-devlet vatandaşlara bu dönemde interaktif olarak hizmet sunmamıştır.
- İkinci dönem (1998-2001); çevrimiçi olarak işlemlerin yapılmaya ve hizmetlerin sunulmaya başladığı dönemdir. Kamu yönetimine ait siteler 1990'lu yılların sonlarına doğru bilgi sağlayıcı işlevlerinden işlemsel modele doğru geçiş yapmaya başlamışlardır. Elektronik posta ile bilgi gönderimi, online işlem tamamlamaları, çeşitli vergilerin, sigorta primlerinin ödenmesi ve bu işlemlere ait belgelerin internet yoluyla elde edilebilmesi bu dönemde gerçekleşebilmiştir.
- Üçüncü dönem (2001-2010); web sitelerinin bütünleşmeye başladığı dönemdir. 2000'li yılların başından itibaren kamu kuruluşlarının, kendilerinin üretmedikleri hizmetler de dâhil olmak üzere web siteleri vasıtasıyla vatandaşlara geniş kapsamlı hizmet vermeye başladığı dönemdir. (Şahin ve

Örselli, 2003: 345) Bu dönem teknolojinin ve web altyapısının gelişimiyle hızlanarak devam etmiştir.

- Dördüncü dönem sosyal medyanın tüm dünyada yaygın olarak kullanılmaya başlanmasıyla birlikte kamu kurumlarının da bu alana dâhil olması, vatandaş etkileşimlerinin hızlanması ve güçlenmesi olarak tanımlanabilir (Yıldız vd., 2016: 55). Bu dönem yaklaşık olarak 2005 yılında başlamıştır ve halen devam etmektedir.
- Beşinci Dönem ise Endüstri 4.0'ın etkisi ile son yıllarda görülen; yapay zekâ, büyük veri, nesnelerin interneti, robotik teknolojiler ve blokzincir gibi farklı teknolojik alanlarda büyük değişimlerin yaşandığı, bilgi ve iletişim teknolojilerinin aritmetik değil, geometrik bir hızda gelişim kaydettiği dönem olarak ele alınmaktadır. Kesin olarak tarihlendirmek kolay olmasa da bir sınır çizmek açısından bu sürecin başlangıcı için kimi yazarlar tarafından 2015 yılı sonrasına işaret edilmektedir (Karasoy ve Babaoğlu, 2020: 122). Bu dönemde artık e-devlet kavramından ziyade dijital devlet kavramı önemi çıkmaya başlamıştır.

3.2.2. Endüstri 4.0 ve Kamu Yönetimine Etkileri

Genellikle dördüncü sanayi devrimi olarak anılan Endüstri 4.0, Nesnelerin İnterneti (IoT), yapay zekâ (AI), büyük veri analitiği, robotik ve gelişmiş iletişim ağları gibi gelişmekte olan teknolojilerin sağladığı üretim süreçlerinin devam eden otomasyonunu ve dijitalleşmesini tanımlayan bir terimdir. Endüstrilerin nasıl çalıştığı ve etkileşimde bulunduğu konusunda bir paradigma değişimini temsil ederek artan verimlilik, üretkenlik ve yeni iş modellerinin yaratılmasına yol açar.

Endüstri 4.0'ın kamu yönetimi üzerindeki etkileri önemli ve geniş kapsamlı olup, devlet operasyonlarının ve hizmetlerinin çeşitli yönlerine dokunmaktadır. Bu etkilerden bazıları şunlardır:

Akıllı Yönetişim: Akıllı şehirler ve bölgeler oluşturmak için Endüstri 4.0 teknolojilerinden yararlanılabilir. Hükümetler, kentsel altyapıyı, trafiği, atık yönetimini ve enerji tüketimini izlemek ve yönetmek için IoT sensörlerini ve veri analitiğini kullanabilir. Böylelikle, kaynak tahsisi daha iyi optimize edilebilir, maliyetler

düşürülebilir ve vatandaşların yaşam kalitesi iyileştirilebilir (Republic of Turkey Ministry of Environment, Urbanization and Climate Change, 2020: 30-33).

E-Devlet Hizmetleri: Dijitalleştirme ve otomasyon, hükümetlerin vatandaşlara, işletmelere ve diğer paydaşlara çevrimiçi hizmetler sunmasına olanak tanır (Akçakaya, 2017: 27). Buna vergi beyannamesi, izin başvuruları, sosyal hizmetler ve daha fazlası gibi hizmetler için kullanılan dijital platformlar dâhildir (Çarıkçı, 2010: 106-107). Bu tür platformlar hizmetlere erişilebilirliği, kolaylığı ve şeffaflığı artırır.

Veriye Dayalı Karar Verme: Büyük miktarda verinin ve gelişmiş analitik araçlarının kullanılabilirliği, kamu yöneticilerinin daha bilinçli kararlar vermesini sağlar. Hükümetler, kanıta dayalı politikalar ve stratejiler oluşturmak için eğilimleri, davranış kalıplarını ve vatandaş geri bildirimlerini analiz edebilirler (Kaura, 2023).

Verimli Hizmet Sunumu: Endüstri 4.0 teknolojileri, hükümetlerin idari süreçleri kolaylaştırmasına, evrak işlerini ve manuel görevleri azaltmasına olanak tanır. Bu, daha hızlı ve daha doğru hizmet sunumunun yanı sıra maliyet tasarrufu sağlayabilir (Schrauf ve Bertram, 2016: 16).

Kamu Güvenliği ve Emniyeti: IoT cihazları ve yapay zekâ destekli analizler; tahmine dayalı polislik, afet müdahalesi ve tehdit algılamayı etkinleştirerek kamu güvenliğini artırabilir. Akıllı gözetim sistemleri ve iletişim ağları, daha hızlı acil durum müdahalelerine ve suçun önlenmesine katkıda bulunabilir (Antunes vd., 2021: 131-132).

İş Birliği ve Ortaklıklar: Endüstri 4.0, hükümetler, endüstriler, akademi ve sivil toplum arasındaki iş birliğini teşvik eder (Schwab, 2016: 2). Kamu yönetimi, yeniliği teşvik etmek, en iyi uygulamaları paylaşarak arttırmak ve toplumsal zorlukları toplu olarak ele almak için ortaklıkları teşvik edebilir.

Bu faydalı etkilerinin yanında Endüstri 4.0'ın kamu yönetiminde yerleştirilebilmesi için aşılması gereken bazı zorluklar da bulunmaktadır. Bunlar şu şekilde sıralanabilir:

İşgücü Dönüşümü: Endüstri 4.0 teknolojilerinin benimsenmesi, yetenekli bir iş gücü gerektirir. Kamu idaresi kurumlarının, çalışanları yeni sistem ve teknolojileri kullanabilmeleri için gerekli dijital becerilerle donatmak maksadıyla eğitim ve öğretime yatırım yapması gerekebilir (Li, 2022: 11-12).

Mevzuat ve Politika Zorlukları: Endüstri 4.0, gizlilik, veri koruma, siber güvenlik ve etik hususlarla ilgili yeni zorluklar getirmektedir (Bron, 2023). Hükümetler, bu endişeleri gidermek ve bu teknolojilerin sorumlu ve güvenli bir şekilde uygulanmasını sağlamak için uygun düzenlemeler ve politikalar geliştirmelidir.

Özetle, Endüstri 4.0 daha verimli, veriye dayalı ve vatandaş merkezli yönetim sağlayarak kamu yönetimini dönüştürme potansiyeline sahiptir. Bununla birlikte, başarılı bir şekilde uygulanması, dikkatli planlama, yatırım ve bu teknolojik devrimden kaynaklanan fırsatlar ve zorluklarla başa çıkmak için uyarlanabilirlik gerektirir.

3.2.3. Blokzincir ve Endüstri 4.0 Arasındaki İlişki

Endüstri 4.0 ve blokzincir, iki farklı teknolojik kavramdır, ancak modern endüstriyel ve teknolojik gelişmeler bağlamında yolları çeşitli şekillerde kesişmekte ve birbirlerini tamamlamaktadırlar.

Endüstri 4.0, çeşitli endüstriyel süreçlerde ve üretimde dijital teknolojilerin, otomasyonun, veri alışverişinin ve ileri analitiğin entegrasyonu ile karakterize edilen dördüncü sanayi devrimini ifade eder. Nesnelerin İnterneti (IoT), büyük veri analitiği, yapay zekâ ve siber-fiziksel sistemler gibi kavramları kapsar. Endüstri 4.0'ın amacı, makinelerin, süreçlerin ve sistemlerin birbirine bağlı olduğu ve birbirleriyle iletişim kurabildiği, böylece verimliliğin, esnekliğin ve üretkenliğin arttığı "akıllı fabrikalar" yaratmaktır (IBM, 2021).

Blokzincir, birden çok katılımcı arasında işlemlerin güvenli ve şeffaf bir şekilde kaydedilmesini sağlayan merkezi olmayan ve dağıtılmış bir dijital defter teknolojisidir. Genellikle Bitcoin gibi kripto para birimleri ile ilişkilendirilse de uygulamaları dijital para birimlerinin ötesine geçmektedir (IBM, 2018). Blokzincir, kurcalamaya dayanıklı ve değiştirilemez bir yol sunarak verileri, şeffaflık ve güvenliğin çok önemli olduğu senaryolarda kaydetmek için son derece uygun hale getirir.

Endüstri 4.0, üretim ve endüstriyel süreçlerin dijitalleşmesi ve otomasyonunun dördüncü aşamasını temsil ederken, blokzincir; dağıtık, güvenli ve şeffaf veri kayıt altyapısını sağlayan bir teknolojidir. İlk bakışta farklı alanlar gibi görünürseler de Endüstri 4.0 ve blokzincir arasında çeşitli ortak noktalar bulunmaktadır:

Akıllı Sözleşmeler: Akıllı sözleşmeler, sözleşme şartlarının doğrudan koda yazıldığı, kendi kendini yürüten sözleşmelerdir (Christidis ve Devetsikiotis, 2016: 2292). Endüstri 4.0'da ekipman bakımı, kalite kontrol ve üretim çizelgeleme gibi çeşitli süreçleri otomatikleştirebilir ve kolaylaştırabilirler (Gohil ve Thakker, 2021: 81-82). Blokzincirin kurcalamaya dayanıklı yapısı, bu sözleşmelerin koşullarının, aracılara ihtiyaç duyulmadan amaçlandığı gibi yürütülmesini sağlar.

Tedarik Zinciri Yönetimi: Endüstri 4.0 ve blockchain'in kesiştiği alanlardan biri de tedarik zinciri yönetimidir. Endüstri 4.0'da kullanılan IoT cihazları ve sensörler, malların ve ham maddelerin hareketi hakkında çok miktarda veri üretebilir. Bu veriler, tedarik zinciri boyunca şeffaflık, izlenebilirlik ve özgünlük sağlayarak bir blokzincire kaydedilebilir (Soori vd., 2023: 193-196).

Dijital Kimlik ve Kimlik Doğrulama: Endüstri 4.0 ortamlarında, çeşitli varlıkların (makineler, cihazlar, insanlar) belirli kaynaklara erişmek için kimliklerinin doğrulanması ve yetkilendirilmesi gerekir (Lucia vd., 2023: 1). Blokzincir, dijital kimlikleri yönetmenin merkezi olmayan ve kurcalamaya karşı korumalı bir yolunu sunarak, yalnızca yetkili varlıkların sistemle etkileşime girmesini sağlar.

Veri Güvenliği ve Gizliliği: Endüstri 4.0'ın artan bağlanabilirliği, veri güvenliğini ve mahremiyetini önemli endişe konuları haline getirmektedir (Mentsiev vd., 2020: 1). Blokzincirin şifrelemesi ve merkezi olmayan yapısı, hassas bilgilere yetkisiz erişimi ve kurcalamayı önleyerek veri güvenliğini artırabilir.

Merkezi Olmayan Üretim Ağları: Blokzincir, farklı üreticilerin ve tedarikçilerin daha verimli, güvenli ve şeffaf bir şekilde iş birliği yapabileceği merkezi olmayan üretim ağları oluşturmak için kullanılabilir (Baumunga ve Fomin, 2019: 456). Bu, üretim yeteneklerinin, fikri mülkiyetin ve kaynakların paylaşımını kolaylaştırabilir.

Veriden Para Kazanma: Endüstri 4.0'ın çok miktarda veri üretmesiyle, blokzincir, üreticilerin verileri güvenli bir şekilde satabilecekleri yeni iş modelleri ve gelir akışları sağlayan veri pazarları oluşturmaya yardımcı olabilir (Silva vd., 2020: 47).

Özetle, Endüstri 4.0 ve blokzincir arasındaki ilişki, hızla gelişen teknolojik bir ortamdaki endüstriyel süreçlerde, daha çok veri yönetiminde ve iş birliğinde şeffaflığı, güvenliği ve verimliliği artırma bağlamında kendini göstermektedir.

Netice olarak, bilgi teknolojilerinin mevcudiyeti, kendi kendini yöneten aktörlerin değer yaratmasına olanak sağlaması nedeniyle gelecekteki organizasyon tasarımı biçimlerinin yetki devrine dayalı tasarım ve karar alma tarzına geçirebilecektir. Genel olarak blokzincirin ortaya çıkışı ve özel olarak akıllı sözleşmeler bu gelişmenin önemli itici güçleridir. Blokzincir teknolojisi, dünya çapında dağıtılan, zahmetsizce ve gerçek zamanlı olarak iş birliği yaparak tüm ilgili aktörler için değer yaratmak üzere eşler arası aktörlerden oluşan bir ağ aracılığıyla kriptografi, mutabakat mekanizmaları ve akıllı sözleşmeler kullanarak değer yaratılmasına katkıda bulunur. Bu 'değer interneti' yapılandırmasında;

- Madenciler işlemleri doğrulayarak değer yaratır,
- Akıllı sözleşmeler belirli görevleri otomatik olarak yerine getirerek değer yaratır,
- Kamu kurumları ve özel kuruluşlar dağıtılmış defterleri kullanarak artan verimlilik ve azaltılmış maliyetler yoluyla değer yaratır ve
- Artan hizmet kalitesi ile vatandaşlar için veya genel olarak daha düşük fiyatlar ve daha fazla boş zaman yoluyla tüketiciler için değer yaratılır, bu da bir bütün olarak toplumun tamamı için artan değer yaratımıyla sonuçlanır.

Bu özellikler, en uç noktaya kadar uygulandığında hem kamu yönetiminde hem de özel sektörde organizasyonları ve organizasyonlar arası ilişkileri etkileyen yeni organizasyon tasarımı biçimlerinin yanı sıra otomatik karar alma getirisi sayesinde değişen stratejik yönetim uygulamalarıyla sonuçlanabilir (Rijmenam vd., 2017: 7-8).

3.3. Blokzincirin Kamu Yönetimine Sağlayacağı Faydalar

Blokzincir teknolojisinin bütünlüğü, kurcalamaya karşı dirençliliği (tek bir zayıf noktasının olmaması) ve saydamlığı, işletmelerin iş süreçlerinde olduğu kadar (Viriyasitavat ve Hoonsopon, 2019: 32) kamunun da yönetsel süreçlerinde devrim yapabilmesine olanak sağlayacak bir potansiyeli bünyesinde barındırmaktadır. Endüstri 4.0 ve Nesnelerin İnterneti (IoT) teknolojileri yaygınlaştıkça, blokzincir teknolojisi sağladığı açıklık, maliyet etkinlik, hesap verebilirlik, katılımcılık ve en önemlisi güvenilirlik özellikleriyle yönetsel süreçlere katkı sağlayacaktır.

Blokzincir teknolojisi, kamusal hizmetlerin sunumunda; maliyetlerin ve karmaşıklığın azaltılmasına, yönetsel süreçlerin güvenilir bir şekilde paylaşılmasına, gelişmiş denetime ve güvenilir kayıt tutmaya imkân sağladığı için e-devletin gelişiminde bir sonraki adımı sunabilir (Palfreyman, 2015). Ølnes vd.leri (2017: 359-360), blokzincirin kamu yönetimine getireceği faydaları; şeffaflığın artması, dolandırıcılığının önlenmesi, yolsuzluğun azaltılması, kamuya olan güvenin, kamuda denetlenebilirliğin, dayanıklılığın, güvenliğin ve veri kalitesinin artması olarak sıralamıştır. Aşağıdaki tabloda (Tablo 3), blokzincir teknolojisinin stratejik, organizasyonel, ekonomik, bilgilendirici ve teknolojik alanlardaki potansiyel faydaları ve vaatleri listelenmiştir.

Tablo 3: Blokzincir Teknolojisinin Potansiyel Faydaları ve Vaatleri

Kategori	Avantajlar ve vaatler
Stratejik	Şeffaflık
	Dolandırıcılığı ve manipülasyonu önlemek
	Yolsuzluğu azaltmak
Organizasyonel	Artan güven
	Şeffaflık ve denetlenebilirlik
	Artan öngörü yeteneği
	Denetim yeteneğinin artması
	Mülkiyetin netleşmesi
Ekonomik	Maliyetlerin düşmesi
	Spam ve DDOS saldırılarına karşı artan dayanıklılık
Bilgilendirici	Veri bütünlüğü ve daha yüksek veri kalitesi
	İnsan hatalarının azaltılması
	Bilgiye ulaşmanın kolaylaşması
	Mahremiyet
	Güvenilirlik
Teknolojik	Dayanıklılık
	Güvenlik
	Kalıcılık ve tersinmezlik (değişmezlik)
	Azaltılmış enerji tüketimi

Kaynak: Ølnes vd., 2017: 359

Tablo 3’te, teknolojiye atfedilen çeşitli faydalar gösterilmektedir. Bunlardan birçoğu sadece blokzincire özgü olmayabilir. Nitekim blokzincir teknolojisinin faydalarının, potansiyel risklerinden daha fazla olacak şekilde çalışması için önemli organizasyonel ve kurumsal uygulamalar gerekmektedir. Benzer şekilde sosyal hizmetlerin sunumunda dolandırıcılığı veya yolsuzluğu azaltmak için sosyal hizmet tedarik sisteminin değiştirilmesi gerekmektedir. Bu yönüyle olası faydalar bazen abartılabilmektedir. Yine de blokzincir teknolojisi, gerekli kurumsal düzenlemelerin mevcut olması koşuluyla, kamuda daha iyi bir denetim mekanizmasının oluşturulmasını kolaylaştırabilir (Ølnes vd., 2017: 360).

Dünyanın dört bir yanındaki hükümetler, blokzincir tabanlı uygulamaları kamu-özel sektör ortaklığında yönetsel süreçlerine entegre etmenin olası faydalarını ve zorluklarını araştırmaktadırlar. Blokzincir teknolojisinin devletler için veri bütünlüğü, veri kalitesi, şeffaflık, dolandırıcılık ve manipülasyona engel olma, yolsuzluğu azaltma, gizlilik ve güvenlik sağlama ve devleti olan güveni artırma gibi potansiyel faydaları olduğuna inanılmaktadır (Baturbara vd., 2018: 1-2). Aşağıda blokzincirin kamu yönetimine getireceği faydalar, genel başlıklar halinde incelenmiştir.

3.3.1. Etkililik ve Verimlilik

Kamu yönetiminin fonksiyonları artış gösterirken ve etkililiği tartışılırken, artan bu fonksiyonlar karşısında sınırlı sayıda olan kamuda kaynaklarının etkili bir şekilde kullanılması ön plana çıkmaktadır. Bu durum, kaynakları kullananların hesap verme sorumluluğunu arttırırken geleneksel düzenlilik denetiminin yetersiz kalmasına sebep olmuştur. Dolayısıyla denetimin yeni bakış açılarıyla ve farklı tekniklerle gerçekleştirilmesi zorunluluğu ortaya çıkmıştır (Akyel ve Köse, 2010: 13). Blokzincir teknolojisinin kamu yönetiminde kullanılması ile denetim gerekliliği farklı yöntemler vasıtasıyla karşılanmış olacaktır.

Geleneksel devlet süreçleri genellikle aracıları, evrak işlerini ve manuel doğrulama adımlarını içermektedir. Blokzincir, bu süreçleri otomatikleştirip düzene sokarak evrak işlerini, idari yükü ve aracılara olan ihtiyacı azaltabilir. Bu, önemli maliyet tasarruflarına ve daha hızlı hizmet sunumuna olanak sağlayabilir. Ayrıca, belge doğrulama, yasal uyumluluk ve departmanlar arası iş birliği için güvenli, izlenebilir ve verimli bir platform altyapısı oluşturarak karmaşık bürokratik süreçleri basitleştirebilir.

3.3.2. Şeffaflık ve Hesap Verebilirlik

Kamu yönetimi bağlamında açıklık veya şeffaflık, kurumların yaptığı bütün işlemlerin vatandaşlar tarafından görülebilmesi demektir. Blokzincir teknolojisinde açıklık kavramı tüm blokların tüm işlemleri görebilmesi ile gerçekleşir (Yli-Huumovd., 2016). Bu durum, sistemin üçüncü bir taraf eliyle yönetildiği merkezi bir sistemden daha şeffaf olduğunu göstermektedir.

Birçok kaynak Nakamoto'nun raporunda belirttiği gibi blokzincir teknolojisinin sahipsiz olduğunu söylemektedir. İşlemlerin tamamen kimliği belirsiz kişiler tarafından yapıldığı nakit işlemler aksine, Bitcoin işlemleri her zaman bir hesapla ilişkilendirilir. Her kullanıcı kendi kimliğinin tespit edilmesi için benzersiz bir adrese yani takma ada sahiptir ve işlemler bu takma adlar üzerinden gerçekleşir (Yli-Huumo vd., 2016). Blokzincir teknolojisinde kullanıcılar bu takma adlar sayesinde isimsiz kalacak ve gerçek kimliklerini açıklamaya gerek duymayacaklardır.

Kamu sektöründeki yolsuzluklara karşı hesap verebilirlikteki zayıflığının topluma maliyeti oldukça yüksektir. Dünyanın birçok yerinde kamu sektöründeki yolsuzluk, sosyal, ekonomik ve çevresel kalkınmayı engelleyen en büyük sorundur. Yolsuzluk genellikle şeffaflık eksikliği, yetersiz kayıt tutma ve düşük kamu hesap verebilirliğinden kaynaklanmaktadır. Blokzincir ve dağıtık defter teknolojisi, yolsuzluğa yatkın kamu yönetimi süreçlerine dikkatli bir şekilde uygulandığında, potansiyel olarak bu sistemlerde şeffaflığı ve hesap verebilirliği artırabilir, yolsuzluk faaliyetinin riskini veya yaygınlığını azaltabilir (World Economic Forum, 2020: 4).

Blokzincirin farklı türleri, farklı hesap verebilirlik biçimlerini ve mekanizmalarını, daha önce literatürde daha az kabul edilen yeni şekillerde ortaya koymaktadır. Daha da önemlisi bu uygulamalar, hesap verebilirliğin bir asil-vekil ilişkisi gerektirmediğini ve disiplinler arası literatürde daha önce blokzincir kullanımına ilişkin tavsiyelerde savunulanların aksine, geniş bir paydaş yelpazesinde blokzincir teknolojisinin daha az saf uygulamalarında kendini gösterebileceğini ortaya çıkarmaktadır (Tyma vd., 2022: 1625).

Blokzincirde kayıtlarının değişmezliği, dolandırıcılık faaliyetlerinin yapılmasını zorlaştırır. Bu, özellikle dolandırıcılığı önlemenin çok önemli olduğu oylama sistemleri,

kimlik doğrulama ve finansal işlemler gibi alanlarda hususiyet kazanmaktadır. Nihayetinde blokzincirdeki dağıtık kayıt defteri, tüm işlemleri kurcalamaya dayanıklı ve değiştirilemez bir şekilde kaydederek şeffaflık sağlar. İşlemler ilgili tüm paydaşlar tarafından bağımsız olarak doğrulanabildiğinden, hesap verebilirliğin sürdürülmesi ve dolandırıcılığın önlenmesi sağlanmış olur.

3.3.3. Veri Güvenliği ve Bütünlüğü

Blokzincir, münferit veri tabanlarını, paylaşılan bilgilerin dağıtık defteriyle değiştiren ve böylelikle daha yüksek veri güvenliği ve erişilebilirliği sağlayan bir teknolojidir (Ølnes vd., 2017: 357).

Blokzincir teknolojisi depolanan kayıtların geri döndürülememesi adına hesaplama algoritmaları ve yaklaşımları kullanır. Buna rağmen Nakamoto 2008 yılında yayınladığı bir raporda dönüşümün imkânsız olmak yerine “dönüşümün hesaplama için pratik olmadığını” iddia etmiştir. Kavramdaki “zincir” terimi, blokzincir üzerindeki blokların, kronolojik bir sırada ve önceki kayıtlarla bağlantılı olarak peşpeşe dizilmesini ifade etmektedir (Yli-Huomo vd., 2016).

Blokzincirde içinde bulunan ana kadar yapılan işlemlerin tamamı depolanır. Zinciri bozmadan eski bir bloğun içindeki bilgiyi değiştirmek imkânsızdır ve bu nedenle veri bozulduysa tüm düğümler içinde görünebilir bir hale gelir. Blokzincirde verilerin güvenliğini sağlamak için kriptografik teknikler kullanır, bu da kayıtların değiştirilmesini veya hacklenmesini son derece zorlaştırır. Bu yönüyle, veri ihlali ve yetkisiz erişim riskini azalttığı için hassas devlet bilgileri ile vatandaş verilerini korumak bağlamında özellikle önemlidir.

3.3.4. Katılımcılık ve Yönetişim

Kamu yönetimi bağlamında katılımcılık; yönetimin planlama, karar alma ve uygulama süreçlerine devlet dışındaki kurumların, kuruluşların ve vatandaşların dâhil edilmesi anlamına gelmektedir. Bu, sürece bir sivil toplum kuruluşunun katılması şeklinde olabileceği gibi, politikaların uygulanmasında vatandaş bilgilendirme veya uygulamadan sonra geri bildirim yapma şeklinde de olabilmektedir. Her ne şekilde olursa olsun, kullanılan yol fark etmeksizin yönetim yeteneklerinin iyileştirilmesinde katılım

etkili bir araçtır (Ateş ve Buyruk, 2018: 86). Katılımcılık ilkesini kamusal alana yerleştirmenin üç temel işlevi bulunur. Bunlar (Ruige vd., 2014):

- Politikaların ve uygulamaların etkililiğini arttırmak,
- Kararlara meşruiyet kazandırmak,
- Vatandaşı aktifleştirmek ve demokrasiyi güçlendirmektir.

Blokzincir ile tek bir varlık tarafından yürütülen yönetim işlevi, birden fazla tarafın yönetimden ve işlemlerden sorumlu olduğu ağ tabanlı yönetişime dönüşür. Blokzincirin vatandaşlar arasında doğrudan etkileşimi kolaylaştırması, yöneticileri aradan çıkartarak yönetimi gerçekleştirmesi ve devletler tarafından sağlanan hizmetleri vatandaşlar için uyarlaması beklenmektedir. Bu, toplumu yönetme şekli için yeni yollar gerektirir (Ølnes vd., 2017: 362). Böyle bir durumda, bir arabanın mülkiyet devri, tapu teşkilatlarının herhangi bir müdahalesi olmaksızın yapılabilir. Örneğin, bir aracın satıcısı, alıcısı ve banka gerekli bilgileri sağladıktan ve işlemin gerçekleştirildiğini onayladıktan sonra aracın mülkiyeti yeni sahibine geçmiş olur.

Blokzincirin merkezi olmayan doğası, merkezi yetkililere ve araçlara bağımlılığı azaltır. Bu, vatandaşlar arasında güveni artırarak devlet kurumları arasındaki etkileşimleri kolaylaştırabilir. Son olarak blokzincir teknolojisi, elektronik oylama gibi alanlarda getireceği gelişmeler ile kamu yönetiminde katılımcılığa ve iyi yönetişime katkı sağlayabilir.

3.4. Blokzincir Teknolojisinin Genel Kullanım Alanları

Blokzincir teknolojisi son yıllarda birçok yeniliğe konu olsa da hala emekleme aşamasındadır. Blokzincirdeki birkaç yatay uygulama neredeyse her sektörü ilgilendirmektedir. Bunlar; akıllı kontratlar, otomatik denetim ve gelişmiş siber güvenliktir (Schatsky ve Muraskin, 2015: 5).

3.4.1. Bankacılık İşlemleri / Finansal Hizmetler

Global ödemelerin toplam büyüklüğü, 2021 yılı sonunda bir önceki yıla göre yüzde 13 artışla yaklaşık olarak 2.1 trilyon dolar büyüklüğüne ulaşmıştır. 5 sene içerisinde ise 3 trilyon dolara ulaşması beklenmektedir (Bansal vd., 2022). Hâlihazırda bu transferlerin yapısı incelendiğinde, aradaki aracılardan ötürü, global transfer işlemleri

uzun sürmekte ve oldukça maliyetli olarak gerçekleşmektedir. Ayrıca yasalara ve mevzuata uyumluluk konularında denetim ve raporlama sorunları olduğu belirtilmektedir. Burada kullanılacak yeni bir Blokzincir ve Akıllı Sözleşme altyapısıyla, bu transferlerin gerçek zamanlı olarak, düşük maliyet ve zincirdeki bütün kayıtlara erişim kabiliyeti ile yetkili kurumların daha kolay denetleyebildiği bir yapının oluşturulması sağlanabilir (Usta ve Doğantekin, 2018: 57).

Dağıtık kayıt defterleri, finansal işlemlerin teyidi için merkezi otoritelere olan ihtiyacı ortadan kaldırmaktadır. Tarafların ticari işlemlerini, hisse senedi alışverişlerini ve ödeme süreçlerini bankalara gerek duymadan yapabildiği bir dünya, bugünkünden oldukça farklı olacaktır.

Blokzincir tabanlı değer aktarımı ve depolama sistemlerinin geleneksel sistemlere kıyasla belirli teknik faydaları vardır. Özel kişiler için, kişisel finansal varlıkları üzerinde daha fazla güvenlik, daha fazla gizlilik ve daha iyi kontrol temin edebilir. İşletmeler için ise daha düşük ödeme işlem ücretleri, dünyanın herhangi bir yerinden ödeme alabilme imkânı sağlar. Blokzincir teknolojisi bununla birlikte bankalar ve kredi kartı şirketleri gibi ödeme işlemcileri arasındaki mevcut değer transferi yapılarının verimliliğini de artırabilir (Mattila, 2016: 11).

InnoVentures analizi, dağıtık kayıt defteri teknolojisinin; bankaların sınır ötesi ödemeler, menkul kıymet ticareti ve yasal uyumluluklarla ilgili altyapısal maliyetlerini 2022 yılına kadar yıllık 15-20 milyar dolar azaltacağını öne sürmektedir. Halihazırda dünyanın en büyük bankalarından 30'u finans endüstrisi için blokzincir teknolojisinin geliştirilmesi girişimine iştirak etmişlerdir.

Yine Nasdaq borsasında hayata geçirilen bir projede hisse senetlerinin alım-satımında blokzincirin kullanılması denenmektedir. Nasdaq'taki ekip blokzincir tabanlı çözümlerin güvenilirlik, tutarlılık, doğruluk ve dağıtık mutabakat özelliklerinin özel borsalara yapabileceği katkılara ilgi duymaktadır (Schatsky ve Muraskin, 2015: 3).

Blokzincir, finansal faaliyetlerin maliyetlerini düşürürken işlemsel ve operasyonel hataları azaltacaktır. Sigorta poliçelerini ve müzakereler, anlaşmalar ve hasar yönetimi gibi ilgili faaliyetleri geliştirme potansiyeline sahiptir. Üçüncü bir taraf olmadan borsa yatırımlarına ve finansal anlaşmalara olanak sağlayabilir.

Blokzincir tabanlı deęer aktarım sistemlerinde ortaya ıkabilecek bir dięer yenilik, k miktarlı demelerdir. Geleneksel deme sistemlerinde, bugne kadar bu tr iřlemeleri byk lde olanaksız hale getiren sabit maliyetler ve teknolojik limitler bulunmaktadır. Nano veya mikro demeler, mřterilerin haber makaleleri, videolar ve benzeri ierikler iin doęrudan grntleme bařına deme temelinde cretlendirilebileceęi, ierik oluřturucular iin tamamen yeni iř modellerini hayata geirebilir (Mattila, 2016: 12).

Blokzincirin medya sektrndeki muhtemel katkısı dřk maliyetli mikro demelerle ilgili olacaktır. rneęin bir gazetenin internet sitesi okuyucularını aylık olarak cretlendirmek yerine okunan sayfa ya da makale kadar cretlendirebilecektir. Bazıları blokzinciri fikri mlkiyet haklarının ya da fotoęraf veya mzik gibi dijital sanat eserlerinin korunması yntemi olarak deęerlendirmektedir. Blokzincir bir eserin sahiplięi noktasında emniyetli ve gvenilir bir kanıt olacaktır. Dijital blokların programlanabilir doęası da geliřmiř kullanım haklarına riayet edilmesine mmkn kılacaktır (Schatsky ve Muraskin, 2015: 3).

Blokzincirin řirketler arası mahsuplařma iřlemlerini de kolaylařtıracaktır. Mahsuplařma, birbirine borlu olan tarafların sadece borlar arasındaki farkı deme hakkıdır. Bu hak hem sigortacılar hem de reasrrler iin mevcuttur ve bunu szleřme şartlarına dhil etmek iin planlama gerekmektedir.

Blokzincir ile, paylařılan bir konsorsiyum defteri (ledger), katkıda bulunan yelerin nceden szleřme kuralları oluřturmasına ve buna gre bu kuralları akıllı szleřmelere eklemesine izin verebilir. Akıllı szleřmeler aracılıęıyla otomatik mahsuplařma, sigortacılar iin nemli tasarruflar saęlayabilir.

Geleneksel olarak, A řirketinin B řirketine 500.000 TL borcu varsa, B řirketinin kayıtlarında bu 500.000 TL alacak hesabı ve A řirketinin de bor hesaplarında 500.000 TL olmasını gerektirir. Bu iřlem, tipik olarak, personel ve onay srelerini ieren ve ek onaylar veya iřlemler gerektirebilen faturalar aracılıęıyla koordine edilir. Blokzincir ile, hem A řirketi hem de B řirketi, bireysel defterler yerine aynı paylařılan deftere eriřebilir ve iřlemi daha verimli bir řekilde sonulandırabilir. Bu da iřlemlerin hızlanmasına yardımcı olabilir (The Institutes, 2017: 31).

3.4.2. Kripto Para

Bitcoin’le başlayan ve şu an neredeyse on bine yaklaşan (CoinMarketCap, 2023) kripto para türü ile popülerleşen Blokzincirin uygulama alanları içerisinde en çok kendine yer bulan, paranın dijitalleştirilmesidir. Temeli araçların kaldırılması ve merkezi bir otoriteye dayanmadan bir değer üretilmek olsa da blokzincir teknolojisi, hükümetlerin resmî paranın üretilmesi ile ilgili süreçleri merkez bankaları ve özel bankalardan blokzincir altyapısına transfer etmesine olanak sağlayacaktır. Kâğıt parayı dijitalleştirme, finans ve bankacılık hizmetlerini yaygınlaştırma alanındaki yeteneği ile nakitsiz yaşama geçişte önemli bir mihenk taşıdır. Ayrıca farklı token uygulamaları da finansal hizmetlerin gerçek hayatta kullanımında yenilikler getirecektir (Usta ve Doğantekin, 2018: 55).

Kripto para birimi, bir değişim aracı, bir değer saklama aracı ve bir ölçü birimi olarak hizmet eder. Kripto para birimleri çok az bir içsel değere sahipken, diğer varlıkların değerini fiyatlandırmak için kullanılabilirler. Bitcoin bir kripto para birimidir (ödeme aracıdır), ancak fiyatı spekülatif bir meta olarak görülebilir. 2009 yılında piyasaya sürülmüştür ve yaygın olarak ilk dijital varlık olarak kabul edilmektedir.

Kripto varlıklar olarak da bilinen dijital varlıklar, kriptografi ve blokzincir tarafından mümkün kılınan değerlerin dijital temsilleridir. Asıl amaçları, bir banka veya başka bir güvenilir üçüncü taraf varlığı kullanmadan değer aktarımı için bir araç olarak hizmet etmektir. Kripto varlıklar (dijital varlıklar) üç ana türe ayrılır: kripto para birimleri, kripto emtiaları ve kripto jetonları. Ortaya çıkan tartışmalardan biri, ABD doları gibi istikrarlı bir varlığa sabitlenen ve merkezi olmayan finasta (DeFi) kritik bir bileşen haline gelebilecek kripto para birimleri olan stablecoin (sabit kripto para) kavramıdır (Weinstein, 2022).

Para transferleri ve elektronik alışverişlerde geleneksel yöntemler ile Bitcoin karşılaştırıldığında işlem ücretinin Bitcoin’de çok küçük miktarlara düştüğü görülmektedir. Bitcoin hesaplarının anonimliği sayesinde gizlilik de kredi kartlarıyla kıyaslandığında daha çok artmakta, bu sayede kullanıcılara güvenli bir alışveriş ortamı oluşturduğu görülmektedir. Geleneksel para birimleri, para basımı ve mali düzenlemeler gibi pek çok işlem için bir merkez bankasına bağlı olmak zorundadır. Bitcoin ve diğer dijital para birimlerinde ise böyle bir durum olmamakla birlikte sabit para arzını

garantilemek için kriptografi kullanılmaktadır. Kriptografi sayesinde dijital paraların enflasyona karşı koruma altına alınması sağlanmaktadır (Tanrıverdi vd., 2019: 3).

Burada Merkez Bankası Dijital Paralarına da değinmek gerekmektedir. Dünyadaki birçok merkez bankası, Merkez Bankası Dijital Para Birimlerinin (CBDC) geliştirilmesi üzerinde çalışmaktadır. Merkez Bankası Dijital Paraları, gerçekte kripto para birimi değildir; bunlar daha ziyade blokzincir tabanlı fiat para birimidir. Başka bir deyişle yasal statüye sahip, itibari paranın blokzincir tabanlı dijital bir biçimidir (Dimitropoulos, 2022: 330-331). Merkez Bankası Dijital Para Birimleri, fiziksel ve dijital parayı tamamlamak veya onların yerine geçmek için kullanılabilir veya geleneksel banka mevduatlarına alternatif olabilir. Türkiye ve Çin Halk Bankası gibi merkez bankaları şu anda CBDC'leri denemektedirler.

3.4.3. Kitle Fonlama Hizmetleri

Yeni iş fikirlerinin hayata geçirilmesinde uygun finansman desteğinin sağlanması, günümüzün rekabetçi piyasa koşullarında oldukça zor bir süreçtir. Kredi alabilmek ve devlet desteklerinden yararlanabilmek ise daha da zordur. Bu açıdan gerekli sermayenin oluşturulması, bir projenin hayata geçirilmesinde en önemli hususlardan biri olarak öne çıkmaktadır. Sermayeye ulaşım araçlarındaki yetersizlikler sebebiyle son dönemlerde bu ihtiyacı karşılamak için kitlesel fonlama yöntemi kullanılmaya başlanmıştır (Yiğit, 2020: 111). Blokzincir yaklaşımının ortaya çıkması ile firmalar, sermaye ihtiyaçlarını karşılamak için herhangi bir aracı kuruma ihtiyaç duymadıkları, kendi yönettikleri yeni bir alternatif modele sahip olmuşlardır.

Kitle fonlaması, finansal teknolojide yaşanan gelişmelerin en başarılı örneklerinden biridir. Bu yönüyle, araçları ortadan kaldırabilecek bir uygulama olarak görülebilir. Kitle fonlaması, çoğunlukla standart finansal araçlar olmaksızın internet tabanlı platformlarda gerçekleşen finansal kaynak sağlamaya yönelik açık bir çağrıdır. Kitle fonlaması, kaynak yaratma faaliyetleri ve fon karşılığında sunulanlar açısından ikiye ayrılmaktadır. Bunlar yatırıma dayalı kitle fonlaması ve ödül ve bağışa dayalı kitle fonlamasıdır. Yatırıma dayalı kitle fonlamalarında, fon sağlayıcıları bir kampanyaya yatırımcı olur ve parasal fayda elde etmek için borç verir. Bağışa dayalı kitle fonlamasında ise, parasal bir menfaat sağlanmaz. Sponsorlar genellikle fon karşılığında bir token ile ödüllendirilir (örneğin, müzik CD'si, tişört veya ürünlerde indirim). Yatırıma

dayalı kitle fonlaması, alternatif bir finansal yatırım aracı olarak ortaya çıkmıştır: standart finansal araçlar ve pahalı kayıt gereklilikleri olmaksızın, bağış toplayanın karmaşık düzenleme gerekliliklerinden kaçınmasını ve işlem maliyetlerini azaltmasını sağlar (Cai, 2018: 973-974). Blokzincir kitlesel fonlama ihtiyacına ICO'lar (Initial Coin Offering) vasıtasıyla pratik bir çözüm sunmaktadır.

ICO, blokzincir alt yapısı kullanılarak bir iş fikrinin ihtiyaç duyduğu kaynağın sağlanması amacıyla token üretilmesi ve halka arz edilerek gerekli sermayenin elde edilmesidir. Türkçeye “İlk Dijital Para Arzı” olarak çevrilebilecek bu yöntem, proje sahibinin kendi parasını oluşturmaya ve bunun karşılığında belirlediği cinsten dijital para alması anlamına gelmektedir. Tam karşılığı olmamakla birlikte proje sahibinin, şirket hissesi satmak yerine dijital para satarak kendine ortak bulması demektir (Yiğit, 2020: 120).

3.4.4. Sigortacılık Hizmetleri

Blokzincirin fayda sağlayacağı alanlardan bir diğeri de sigortacılık hizmetleridir. Dünya çapında sigortacılık sektörünün toplam büyüklüğü 2022 yılı itibariyle yaklaşık 6 trilyon dolara ulaşmıştır ve 2026 itibariyle bu rakamın 8,5 trilyon dolara ulaşacağı tahmin edilmektedir (Rudden, 2022). Sigortacılık hizmetlerinde blokzincir; akıllı sözleşmeler vasıtasıyla verimliliğin artırılmasında, araçların ortadan kaldırılmasında, dayı iyi fiyatlandırma ve risk değerlendirmesi yapılmasında ve yeni sigorta türleri oluşturulmasında yardımcı olabilir (Lounds, 2020).

Blokzincir teknolojisi sigorta sektörünü, dijital dönüşümünde bir sonraki aşama hazırlamaktadır. Sigorta şirketleri küresel olarak verimliliği artırmak için dijitalleşmeyi benimserken, blokzincir operasyonel verimliliği daha da artırma, iş birliği zorluklarını çözme ve iş modellerini yeniden şekillendirme vizyonu sunmaktadır. Bu kapsamda blokzincir teknolojisi sigorta sektöründe kendine çeşitli uygulama alanları bulmaktadır. Bu alanların bazıları aşağıda özetlenmiştir (Georgiou, 2023):

Dolandırıcılığın Önlenmesi: Blokzincir, ailelerin her yıl ekstra prim ödemesine neden olan sigorta dolandırıcılığıyla mücadelede yardımcı olabilir. Sigorta taleplerini sigorta şirketleri arasında paylaşılan değişmez bir blokzincir defterinde saklayarak

dolandırıcılık tespitini kolaylaştırabilir. Ayrıca, hassas kişisel verileri ifşa etmeden talep edilen bilgilerin güvenli bir şekilde paylaşılmasına olanak tanır.

Hasar Yönetimi: Sigorta poliçelerinin bir blokzincir üzerinde akıllı sözleşmeler vasıtasıyla uygulanması, verimliliği önemli ölçüde artırabilir ve işletme maliyetlerini azaltabilir. Sigortacılar, reasürörler ve komisyoncular da dâhil olmak üzere ilgili tarafların paylaşılan verilere erişmesine izin verilerek hasar yönetim süreci kolaylaştırılır. Bu, mükerrer işleri azaltarak talep işlemeyi otomatikleştirir ve ödemelerin daha hızlı yapılmasını sağlar.

Sağlık Sigortası: Blokzincir, tıbbi verilerin sağlık hizmeti sağlayıcıları ve sigortacılar arasında hızlı, doğru ve güvenli paylaşımını kolaylaştırır. Hasta verilerinin paylaşılmasının karmaşık ve zaman alıcı sürecini kolaylaştırarak, hasta gizliliğini korurken sağlık sigortası taleplerinin daha hızlı işlenmesine olanak sağlar.

Otomobil Sigortası: Blokzincir, otomobil sigortası taleplerinde anında ödeme ve şeffaflık sağlar. Hem müşteriler hem de sigortacılar temel bilgilere erişerek genel hasar karşılama deneyimini geliştirebilirler.

Reasürans: Blokzincir, sigortacılar ve reasürörler arasındaki veri paylaşımını basitleştirir, süreçleri kolaylaştırır, verimsizlikleri azaltır ve tazminat taleplerinin işlenmesini ve çözümlenmesini otomatikleştirir. Bu, her iki tarafa da fayda sağlayarak kazalar esnasında risk yönetimini geliştirir.

Gelişmekte Olan Piyasalarda Mikro Sigorta: Blokzincir, mikro sigorta planlarında sigortalama ve talep işlemlerini otomatik hale getirerek bunları gelişmekte olan pazarlarda minimum idari masraf ve daha düşük ücretlerle daha uygulanabilir hale getirebilir.

Sigortacılık sektöründe blokzincirin uygulanmasına hakların devri örneği verilebilir. Bilindiği üzere halefiyet, başka bir tarafın (başka bir sürücünün sigorta şirketi gibi) borçlu olduğu bir ödemeyi (sigortalıya) yapan bir tarafın (bir sigortacının), kayıptan yasal olarak sorumlu olan taraftan parayı tahsil etme hakkıdır. Sigortada kusurun tespitinde genellikle bir gecikme olduğu için, bir taraf bir hasarda kusurlu görüldüğünde, bir sigorta şirketi sigortalısı için tazminatı öder ve sonra o parayı (veya en azından bir kısmını) kusurlu taraftan geri almaya çalışır.

Halefiyet genellikle sigortacılar arasında bir para değişimidir. Bu nedenle, paylaşılan bir defter, özellikle bir konsorsiyum tarafından paylaşılan bir defter, ödemelerin netleştirilmesini kolaylaştırabilir, manuel süreçleri ortadan kaldırabilir ve tüm süreci hızlandırabilir. Ayrıca, özellikle mahsuplaşma kuralları akıllı sözleşmeler yoluyla otomatikleştirilirse, idari ve üçüncü taraflarla ilgili olan maliyetler ortadan kaldırabilir veya azaltabilir (The Institutes, 2017: 32).

Deniz sigortacılığı da blokzincirin başka bir potansiyel uygulama alanıdır. Uluslararası ticaretin yüzde 90'ı deniz yoluyla gerçekleşmektedir. Küresel deniz sigortası primleri 2021 yılı sonu itibarıyla 33 milyar dolara ulaşmıştır (IUMI, 2022: 2). Deniz sigortası endüstrisi birçok bilgiyi işlemek zorunda olmasına rağmen hala manuel süreçlere ve kâğıt belgelere dayanmaktadır. Deniz sigortacılığında farklı ülkelerdeki yargısal süreçlere uyum sağlamak oldukça zordur. Blokzincir teknolojisi bu sektörde küresel ekosistemdeki katılımcıların güvenli ve özel bir ağa bağlıyken ortak bilgiye aynı anda erişimini sağlayabilir. Deniz ticareti için blokzincir tabanlı bir sigorta sistemi oluşturarak ödemelerin otomatikleştirilmesinden ticaret ortakları, komisyoncular, sigortacılar ve talep işleyicileri arasında gerçek zamanlı sevkiyat bilgilerinin paylaşılmasına kadar tüm adımlar dijitalleştirilebilecektir. Risk analizi daha sağlıklı yapılacağı için prim maliyetlerinin yüzde 60'a kadar düşmesi beklenmektedir. Ayrıca akıllı sözleşmeler sayesinde dolandırıcılık tespiti, yanlış ürün fiyatlandırması ve deniz sigortası için diğer diğer özel risklerle ilgili verimsizlikler de ortadan kalkacaktır (KPMG, 2021: 23).

Gerçek dünya uygulamaları, blokzincir teknolojisinin sigorta sektöründe nasıl bir dönüşüm yaratabileceğini göstermektedir. Bu teknoloji, müşteri deneyimlerini geliştirme, pazarlarda sigorta erişimini genişletme, güvenlik, verimlilik ve maliyet tasarrufu sağlama gibi konularda önemli vaatler sunmaktadır. Nihayetinde blokzincir teknolojisi, sigorta sektöründe büyük bir potansiyele sahiptir ve bu sektördeki süreçleri daha verimli, güvenli ve şeffaf hale getirmek için önemli bir rol oynayabilir.

3.4.5. Lojistik / Tedarik Zinciri Takibi

Tedarik zincirleri, bilgi, ürün ve hizmetler ile paranın uçtan uca akışını kapsamaktadır. Geleneksel tedarik zinciri anlayışında bilgi paylaşımı genellikle birbirleri ile direkt ilişki kuran taraflar arasındadır. Zincir büyüdükçe bu bilgiler kaybolmakta ve

son tüketicilere veya ara aşamalarda rol alanlara veriler yeterli seviyede ulaşmamaktadır. Teknolojik gelişmeler bu süreci dinamikleştirse de henüz tam olarak entegrasyon sağlanamamıştır. Uyumluluk, izlenebilirlik, paydaş yönetimi ve esneklik bu noktada görülen sorunların başlıcalarındandır (TÜSİAD, 2018: 20).

Blokszincir teknolojisi, geleneksel tedarik zinciri yaklaşımından farklı olarak ürünlerin üretim noktasından son kullanıcıya ulaşana kadar her eksiksiz bir gözetim imkanı sağlama potansiyeline sahiptir. İşlemlerinin zaman damgalı ve sonradan değiştirilemez olması, veri bütünlüğünü sağlayarak sahteciliğin önüne geçmektedir. Akıllı kontratlar sayesinde eşzamanlı olarak izlenebilirlik sağlanabilmektedir. Bu da hızlı karar verebilmeye imkan tanımakta, maliyetleri düşürmekte ve stok seviyelerini güncel tutma elastikiyeti sağlamaktadır (TÜSİAD, 2018: 20).

Blokszincir, tedarikçileri, nakliyecileri, yüklenicileri ve diğer otoriteleri birbirine bağlayarak tedarik zinciri süreçlerinin iyileşmesini sağlar. Zaman gecikmelerini, yönetim maliyetlerini ve insan hatalarını azaltmaya yardımcı olmaktadır. Lojistik faaliyetlerde bulunan şirketler arasında daha hızlı ve verimli anlaşmalar yapılmasına imkan sağlar. Ayrıca lojistik faaliyetlerin planlanmasını, programlanmasını, koordinasyonunu, izlenmesini ve doğrulanmasını güvenli ve verimli bir şekilde destekler.

Blokszincir, tedarik zinciri ve ticaret için güvenlik, şeffaflık, hız ve düşük maliyet sağlamaktadır. Denetimin ve doğrulamanın daha iyi gerçekleştirilmesi için mal tedariki ve ticaret kayıtları blokszincirde saklanabilir. Böylelikle herhangi bir anda, tedarik zincirinde yer alan tüm taraflar, belirli malların belirli bir yerde olduğunun veya belirli bir ticaretin gerçekleştiğinin farkında olacaktır. Kötü niyetli hareket edebilecek merkezi otoritelere güvenmeden bilgiler çok daha hızlı alınabilecektir. Blokszincir kullanmak, tedarik zincirinde kayıtların kaybını da önleyecektir. Örnek olarak TradeLens, Maersk tarafından kurulan ve şu anda küresel nakliye şirketlerinin yaklaşık yarısının ortak olduğu bir blokszincir tabanlı tedarik zinciri ağıdır. Aynı şekilde Grainchain, tahılları ve diğer tarımsal emtiaları satmak, satın almak ve izlemek için blokszincir teknolojisini kullanmaktadır. Mediledger ilaç takibi ve tedariği için ödemeler gibi blokszincir çözümleri sağlamaktadır (Sanka vd., 2021: 188).

Tedarik zinciri yönetiminde blokszincir, teknolojinin temel özelliklerinden ve daha spesifik olarak aracısızlaştırmadan yararlanılarak, zincir boyunca araçların rolünü

ortadan kaldırır ve böylece maliyetler azaltılır. Ayrıca, akıllı sözleşmelerin kullanımı ile mal teslimatının takibinden ödeme işlemlerine kadar çeşitli süreçlerde doğrudan alıcılar ve satıcılar arasında şeffaflığa dayalı yeni bir güven modeli ortaya çıkmaktadır. Skuchain, ödemelerin (akreditif ve banka havalesi) ve finansın (işletme ve kısa vadeli ticari krediler) kesiştiği noktada blokzincir teknolojisini kullanarak kurumsal tedarik zincirlerini güçlendirmeyi amaçlayan bir blokzincir girişimidir. Başka bir proje olan Provenance, kaynaktan son tüketiciye kadar ürünlerin menşeyini izleyerek tüketiciler ve perakendeciler arasında güven oluşturmaya odaklanmaktadır. Bu girişimlere ek olarak, Walmart gibi mevcut perakendeciler, verimliliği artırmak ve tedarik zinciri maliyetlerini azaltmak için blokzincir teknolojisinin avantajlarından yararlanmaya çalışmaktadırlar. Nestle, süt ürünlerinin tazeliğini hedeflerken, diğer blokzincir uygulamaları, bir ürünün orijinalliğinin (ör. sahte olmadığını) ve kaynağının (ör. Bir balığın nerede ve ne zaman yakalandığının) takibine odaklanmaktadırlar. Ayrıca IBM, daha fazla güvenilirlik, şeffaflık ve güvenlik sağlamak için üreticiler, perakendeciler ve tedarikçiler arasındaki veri entegrasyon süreçlerini desteklemek için bir blokzincir sistemi geliştirmiştir (Makridakis ve Christodoulou, 2019: 9). Bahsedilen projeler, blokzincirlerinin özelliklerinin izlenebilirlik uygulamaları için nasıl yeni fırsatlar açtığının gösterge niteliğindeki örnekleridir.

Örnek olarak bir perakendeci ile bir tedarikçiyi arasındaki işlemlerin blokzincir ağı üzerinde nasıl gerçekleştirilebileceğini ele alalım. İlk olarak, perakendeci bir sipariş oluşturur ve bunu tedarikçiye gönderir. Bu noktada herhangi bir mal veya hizmet alışverişi gerçekleşmediği için mali deftere herhangi bir giriş yapılmayacaktır. Bununla birlikte, blokzincir ile perakendeci, sipariş için dijital bir token kaydı oluşturur. Tedarikçi daha sonra siparişte oturum açar ve perakendeciye siparişin alındığını onaylar; bu, tekrar blokzincire kaydedilen ancak finansal defterde girişi oluşturmayan bir eylemdir. Daha sonra tedarikçi, malların üretimini finanse etmek için bankadan işletme sermayesi kredisi talep eder. Banka, paylaşılan blokzincir ağından siparişi doğrular, krediyi onaylar ve kredinin dijital tokenini aynı blokzincire kaydeder (Gaur ve Gaiha, 2020).

Bu kullanım alanına Pacifical şirketinin geliştirdiği blokzincir platformu örnek verilebilir. Pacifical, Nauru Anlaşmasına üye sekiz ada ülkesi tarafından, dünya çapındaki tüketicilere ton balığı satmak amacıyla ortaklaşa kurulan küresel bir pazarlama şirkettir. Şirket, ton balığı ürünlerinin sürdürülebilirliğini izlemek ve doğrulamak için Ethereum

blokzincirinden yararlanacak şekilde bir izlenebilirlik platformu geliřtirmiřtir. Kresel ton balıęı endstrisinde řeffaflıęı arttıran ve iletiřimi standartlařtıran bu yeniliki giriřimde, Deniz Koruma Konyei (Marine Stewardship Council - MSC) ton balıęı srdrlebilirlik sertifikası ve izlenebilirlik bilgileri de dhil olmak zere ticari olmayan ve gizli olmayan veriler, Ethereum genel blokzincirinde yayınlanmaktadır. Sistem, Pacifical'ın mevcut izlenebilirlik zmleriyle entegre edilmiř blokzincir akıllı szleřmelerini ve merkezi olmayan depolamayı kullanmaktadır. Balıkılar, tccarlar, reticiler, toptancılar, distribtrler ve perakendeciler iin iř birlięine dayalı bir aę sunarak onların seilen Pacifical MSC izlenebilirlik ve sertifikasyon kayıtlarına sorunsuz bir řekilde eriřmesine, ynetmesine ve paylařmasına olanak tanınmaktadır. Pacifical ve MSC logolarını taşıyan rnler, benzersiz izleme kodları kullanılarak blokzincir zerinde takip edilebilmektedir. 220'den fazla byk balıkı teknesini ve her yıl yakalanan 35 milyon ton balıęının tm tedarik zincirini kapsayan bu giriřim, ton balıęı endstrisinde řeffaflık ve izlenebilirlik konusunda yeni bir standart belirlemekte ve ton balıęı rnlerinin srdrlebilirlięine olan gveni arttırmaktadır (PRNewswire, 2018).

3.4.6. Dijital Sertifikalar

Her yıl milyonlarca ęrenci liselerden ve niversitelerden mezun olmakta ve kurumlarından eęitimlerini tamamladıklarına dair belge almaktadır. Mezunların bu belgelerle iř bařvurusunda bulundukları gz nnde bulundurulduęunda iřverenler aısından zgemiřlerde yer alan bilgilerin ve kendilerine sunulan belgelerin doęruluęu byk nem taşımaktadır. Her ne kadar eęitim belgeleri e-Devlet uygulamasında gzkyor olsa bile bu veri giriřlerinin kontrol istismara aıktır. Ayrıca eęitim belgelerinin ve diplomaların kopyalanabildięi, sahtelerinin retildeęi bilinen bir gerektir. Sahte diplomalarla onlarca yıl ęretmenlik, doktorluk vb. yapanlarla ilgili haberler oęalmaktadır. Eęitim belgeleri e-devlet uygulamasında grlebilse bile dięer kurumlardan alınan katılım belgeleri, sertifikalar, tamamlama belgeleri gibi dokmanların oęunun doęrulanabilmesi ya da gereklięinin sorgulanabilmesi olanaęı bulunmamaktadır. Blokzincir teknolojisi bu konuda kapsamlı bir zm getirmektedir.

Daha nce verilen rneklerde olduęu gibi blokzincir altyapısı kurulduęunda her vatandařın dijital bir kimlięi olacaktır. ęrenci bir okuldan mezun olduęunda bu okulu tamamladıęına dair ilgili okul tarafından ęrencinin dijital kimlięine giriř yapılacaktır.

Bilgi blokzincir ağına olduğu için de değiştirilmesi mümkün olmayacaktır. Aynı şekilde özel kurumlar da eğitimine iştirak eden bir katılımcının dijital kimliğine sertifikasını yükleyebilecektir. Böylelikle işverenler, iş başvurusuna bulunanların özgeçmişlerini dijital kimlikleri üzerinden görüntüleyebilecektir. Bu hem sahte özgeçmişler ile yetkinliği olmayan kişilerin hak etmediklerin pozisyonlarda çalışmasını önleyerek emek ve para kaybının önüne geçecek, hem de daha adil bir rekabet ortamı yaratacaktır.

Dijital sertifikasyon süreçlerinde blokzincirin kullanımına yönelik uygulamalara “checkdiploma.org” verilebilir. Bu uygulamada Ethereum ağına akıllı sözleşmeler ile mezuniyet bilgilerinin depolanması yöntemi uygulanmıştır. Lefkoşa Üniversitesi ise, ülkemizde Bitcoin blokzincirinde gerçekliği teyit edilebilen sertifikalar oluşturan ilk yükseköğrenim kurumu olmuştur. Ayrıca uygulamanı kaynak kodlarını herkesin kullanımına açmıştır. 2017 yılında Massachusetts Teknoloji Enstitüsü (MIT), pilot program olarak blokzincir altyapısını kullanan bir sertifika doğrulama uygulamasını devreye almıştır. Program ile mezunlarının diplomaları mobil ortamda doğrulanabilmesi sağlanmıştır. MIT 2017 yılında geliştirdiği uygulamayı kendi lisansı altında kamuya açmıştır (Ayberkin vd., 2018: 77).

Ekim 2017'de Malta hükümeti, blokzincir teknolojisini kullanarak akademik yeterlilik doğrulaması geliştiren bir proje başlatmıştır. Malta Eğitim ve İstihdam Bakanlığı (MEDE), akademik kayıtların yönetimi için “Blockcerts” açık standardını kullanmaya karar vermiştir. Blockcerts, sertifikaların oluşturulması, verilmesi, görüntülenmesi ve doğrulanmasında altyapı olarak blokzincir teknolojisini kullanmıştır. Pilot uygulama, vatandaşlar için doğrulanabilir bir eğitim kanıtı oluşturmak amacıyla başlatılmıştır. Blockcerts sistemi kullanılarak akademik sertifikanın verilmesi ve doğrulanması süreci aşağıdaki adımlardan oluşur (Allessie vd., 2019: 22-23):

- Akademik kurum, mezunlarına Blockcerts uygulamasını indirmeleri ve yayıncı olarak eklemeleri için bir istek gönderir.
- Mezun, cüzdanı kurar ve kurumun isteğini kabul eder. Bunu yaparken, cüzdan özel ve genel bir anahtar oluşturur.
- Daha sonra, kurumu sertifika sağlayıcısı olarak onayladığından, Blockcerts uygulaması genel anahtarını kuruma gönderir.

- Kurum, Blockcerts uygulamasında vatandaşın açık anahtarını içeren bir dijital sertifika oluşturur. Bu sertifika, kurumun özel anahtarıyla imzalanır. Sertifika, mezunun genel anahtarı oluşturulduğunda otomatik olarak Blockcerts cüzdanına kaydedilir.
- Kurum, Blockcerts uygulamasında sertifikanın şifrelenmiş özetini alır ve Bitcoin blokzincirine kaydeder.
- Kurum, blokzincirde depolanan özet ve Blockcerts URL bilgisini de içeren sertifikayı mezuna e-posta ile gönderir.
- Mezun, artık elektronik sertifikayı ve URL'yi üçüncü taraflara gönderebilir.
- Üçüncü bir taraf (ör. potansiyel işveren), sağlanan sertifikanın özet değerinin URL'de belirtilen Bitcoin blokzincirindeki özet değerle eşleşip eşleşmediğini kontrol eden online Blockcerts uygulamasında sertifikayı ve URL'yi kontrol eder. Özet eşleşirse, sertifika doğrulanmış olur. Üçüncü taraf artık belgenin doğru olduğundan emin olabilecektir.

3.5. Blokzincir Teknolojisinin Kamu Yönetiminde Olası Kullanım Alanları

E-devlet girişimleri, daha doğrudan, dağıtılmış ve vatandaşların ihtiyaçlarına göre uyarlanmış kamu hizmetleri sağlamaya çalışsa da devlet kurumlarının kayıt tutma ve yönetim işlevlerini tam olarak değiştirememişlerdir. Blokzincir teknolojisinin en önemli faydalarından biri, devlet kurumları, vatandaşlar ve işletmeler arasındaki doğrudan etkileşimleri teşvik etme yeteneğidir. Nihayetinde blokzincir teknolojisi, hükümetlerin bireylerle ve birbirleriyle nasıl etkileşim kurduğunu yeniden tanımlama potansiyeline sahiptir ve kamu idarelerini kamu hizmetleri sağlamadaki rollerini yeniden gözden geçirmeye zorlamaktadır.

Hükümetler bu teknolojiyi, blokzincir tabanlı bir altyapıdaki bilgi alışverişi gerektiren kurumlar üzerinde denetim işlevlerini üstlenmek için kullanabileceklerdir. Blokzincir, hükümetlerin şu anda toplumda oynadığı idari işlevlerin önemli bir bölümünü ortadan kaldırma potansiyeline sahiptir ve bu da (kamu) hizmet arzının yönetişiminde bir değişiklik gerektirmektedir. Bu yönüyle, yasal ve kamusal alanda mevcut kurumsal çerçeveleri değiştirme potansiyeline sahiptir (Krichen vd., 2022: 14-15).

Kaldıraç, nesnelerin, başka türlü elde edilmesi imkânsız olan veya çabaya değmeyecek başarıları ne ölçüde mümkün kıldığını açıklamaktadır. Blokzincir de bazı

alanlarda kaldıraç görevi görmektedir. Blokzincir, yeterli teknik veya kurumsal altyapının bulunmadığı ortamlarda güvenli ve şeffaf ödeme ile diğer finansal işlemler için bir platform sunmaktadır. Yolsuzluğun sıradan olduğu ülkelerde, en azından devlet ile yapılan işlemlerde, kurcalamaya dayanıklı BİT (Bilgi ve İletişim Teknolojisi) sistemleri önemli faydalar sağlayabilir (Ølnes ve Jansen, 2017: 223).

Blokzincir teknolojisi, bir önceki bölümde sıralanan uygulama alanlarında olduğu kadar kamu yönetiminde de büyük bir uygulama potansiyele sahiptir. Blokzincir, kamu hizmetlerinin sunumunu iyileştirerek ve kamu sektörüne olan güveni artırarak devlet operasyonlarını daha verimli hale getirebilir. Ayrıca, işlemlerin kaydedilme şeklini değiştirebileceğinden dönüştürücü olabilir (Baturbara vd., 2018: 1). Bu yönüyle teknoloji ulusal ya da uluslararası bir yaklaşımla ele alındığında ve açık bir platform ve gelişen bir bilgi altyapısı olarak görüldüğünde potansiyeli kendini daha net ortaya koyacaktır (Ølnes ve Jansen, 2018: 1). Kamu hizmetlerinde kullanılan blokzincir uygulamalarından bazıları aşağıda sıralanmıştır.

3.5.1. Akıllı Sözleşmeler

Akıllı sözleşmeler, en çok alıntı yapılan blokzincir uygulamalarından biridir. Akıllı sözleşmeler kısaca kâğıt yerine kodla yazılan sözleşmelerdir. Dijital imzalarla imzalanır ve otomatik olarak uygulanır. Bu, sözleşmede yazılı olan koşulların sözleşmenin yürütülmesini belirlediği anlamına taşımaktadır. Koşullar karşılanır ve doğrulanırsa, sözleşme otomatik olarak yürürlüğe girer. Bu prosedür, diğer blokzincir işlemlerine benzer şekilde, araçları ortadan kaldırmaktadır (Kossow ve Dykes, 2018: 9).

Blokzincirin getirdiği kayıt tutma, doğrulama ve güvenlik özellikleri akıllı sözleşmeleri etkinleştirmektedir. Akıllı sözleşmeler, üçüncü bir taraf olmadan açık bir ağ üzerinden sözleşmelerin güvenilir bir şekilde yürütülmesine izin verir. Böylelikle sözleşmeler denetlenebilir ve değiştirilemez nitelik kazanır. Blokzincir tabanlı akıllı sözleşmeler, birçok endüstriyel sektörü farklı şekillerde geliştirme potansiyeline sahiptir. Bu gelişmelerden biri, şirketler ile ortakları arasındaki veya şirketler ile müşterileri arasındaki anlaşma süreçlerinin otomatikleştirilmesidir. Bu, işlem süresini ve idari maliyetleri önemli ölçüde azaltacak ve üçüncü taraf kayıtlarına veya bürokratik belgelere güvenmeye gerek kalmadan sözleşmeleri başlatmak, müzakere etmek ve sonuçlandırmak için daha verimli bir model oluşturacaktır (Al-Jaroodi ve Mohamed, 2019: 36502).

Akıllı kontratlar para, mülk, hisse senedi ya da değer atfedilen her şeyi şeffaf ve tartışmasız olarak aracıya gerek kalmaksızın takas etmeye yaramaktadır. Akıllı kontratlar bir sözleşmenin şartlarını kodlayarak onları blokzincirin kayıt defterine yükleyen bilgisayar programlarıdır. Bu sadece sözleşmenin bağımsız bir şekilde çalışmasını değil aynı zamanda parasal karşılık gibi değerlerin sözleşmeye konulmasını da sağlar. Bu senaryoda blokzincir, önceden belirlenmiş kurallara göre anlaşma koşullarını yerine getirilmesini temin eder (Belirli şartlar sağlandığında bir sonuç, diğer şartlarda da alternatif sonuç gibi). Bu yüzden akıllı kontratlar “eğer-ise” kodu olarak da düşünülebilir (Spielman, 2018: 4).

Akıllı kontratlar için blokzincir, araçlar olmadan tarafların güven gerektirmeyen işlemler yapabilmesine olanak sağlayan açık ve izlenebilir bir platform olması nedeniyle oldukça güvenli bir altyapı sunmaktadır. Kontratlarda belirlenmiş tetikleyici koşullar gerçekleştiğinde programlar otomatik olarak hayata geçirilir. Bu koşullar diğer işlemlerin ya da akıllı kontratların sonuçları da olabilir (Shen ve Pena-Mora, 2018: 5).

Blokzincir tabanlı akıllı kontratları geleneksel olanlardan ayıran üç temel karakteristik özellik bulunmaktadır. Birincisi herhangi bir blokzincirde çalışan akıllı kontratlar merkezi bir oluşum değil tamamen bilgisayar koduyla yönetilir. İkinci olarak mevcut bir akıllı kontratı değiştirmenin tek yolu tüm katılımcıların rızasıyla yeni bir kontrat oluşturmaktır. Aksi halde eski kontrat geri çekilemez. Üçüncüsü de fazlaca koşulun bulunduğu çok taraflı anlaşmaları maliyet etkin bir şekilde tesis etmenin bir yöntemi olmasıdır (Shen ve Pena-Mora, 2018: 5).

Akıllı sözleşmelerin en çok iş fayda sağlayacağı alanlardan birinin de iş anlaşmaları alanı olacağı tahmin edilmektedir. Tarafların üzerinde mutabık olduğu sözleşmelere herhangi bir noter vb. üçüncü taraf olmadan uyma mecburiyeti getirmektedir. Akıllı sözleşmeler ile, günlük hayatta ev, araba alırken karşılaşılan uzun ve yorucu süreçler hızlanacak ve kolaylaşacaktır. Ayrıca doğrulama işlemini kodlar yapacağı için aracı kişi ve kurumların sayısı da azalacaktır (Taş ve Kiani, 2018: 4).

Denetimler ve güvenlik önlemleri, teorik olarak dolandırıcılık ve yolsuzluğun kapsamını sınırlayabilecek akıllı bir sözleşmeye kodlanabilir. Akıllı sözleşmeler, blokzincire kaydedildikleri için şeffaftır ancak izin alınmadan değiştirilemez. Düzgün bir şekilde kodlanırsa, yolsuzluk fırsatları bu nedenle sınırlıdır. Bu, akıllı sözleşmeleri,

özellikle kamu ihale süreçleri sırasında manipölasyonu sınırlandırma potansiyeli ile ilgili olarak, devlet sözleşmelerinin çeşitli alanlarında potansiyel olarak uygulanabilir hale getirir (Kossow ve Dykes, 2018: 9).

3.5.2. Kimlik Yönetimi

Kimlik doğrulamak, önemi çoğu zaman göz ardı edilen ya da sadece kötü bir olay tecrübe edildiğinde anlaşılan ve neredeyse her gün yapılan rutin bir faaliyettir. Gerçek hayatta kimliğimizi gümrüklerde, havalimanlarında, bankacılık işlemlerinde, devlet dairelerinde vb. alanlarda kanıtlamamız istenmektedir. Bu durumda ilgili mercilere kimliğimizi kimlik kartları, sürücü belgeleri ve pasaport gibi resmî belgelerle kanıtlamaya çalışırız. Fakat bu belgeler kâğıt bazlı olduklarından dolayı kopyalanabilmekte, kısmen ya da tamamen değiştirilebilmekte ve kötü amaçlı kullanımlara konu olabilmektedir.

Birçok ülkede devlet görevlileri resmî belgeleri maddi menfaat gibi nedenlerden ötürü değiştirebilmektedir. Bu yaş büyölmek, küçölmek, evli göstermek, askerlik yapmış gibi göstermek vb. şekillerde kendini göstermektedir. Pasaport gibi kopyalanması zor resmî dokümanlar bile görevlilere rüşvet verilerek resmî belgenin yanlış bilgi içermesi şeklinde değiştirilebilmektedir.

Blokszincir veri tabanlarının değiştirilemez ve dağıtık yapısı, kimlik yönetimi için de kullanılabilir. Mevcut dijital tanımlama yöntemleri ile ilgili genel sorun, bir kimliğin gerçekliğini doğrulamak için çoğunlukla güvenilir bir arabulucuya ihtiyaç duymalarıdır. Blokszincir teknolojisi, modern dijital kimlik hizmetlerine iki yönden iyileştirme getirmektedir. İlk olarak, güvenilir bir üçüncü tarafa olan ihtiyacı ortadan kaldırır, böylece hizmetle ilgili ücretler ortadan kalkar. Ayrıca, mevzubahis hizmetle ilgili olmayan bilgilerin ortaya çıkarılmasının önüne geçer (Mattila, 2016: 14).

Birleşmiş Milletlere göre dünya üzerinde 1.1 milyon insanın resmî kimliği bulunmamaktadır. Bu sayının yüzde 75'i Afrika ve Asya'da olup bunların yarıya yakını çocuklar oluşturmaktadır. Resmî kimlikleri olmamaları nedeniyle bu insanlar hükümet yardımı, eğitim, çalışma, barınma, finansal hizmetler gibi temel insani hizmetlerden mahrum kalmaktadırlar. Bu grubun içerisindeki çocuklar ise insan kaçakçılığı, zorla çalıştırma, erken yaşta evlendirme ve cinsel istismar gibi durumlara maruz kalabilmektedirler (Woods, 2018).

Blokszincir teknolojisi bu konuda devrimsel yenilikler sağlayacak potansiyele sahiptir. Burada devletlerin yapması gereken blokszincir tabanlı olarak geliştirilmiş bütüncül bir kimlik yönetimi altyapısı oluşturmaktır. Bütün vatandaşların kişisel bilgileri blokszincire aktararak zincir üzerinde tanımlı dijital bir kimlik oluşturulacaktır. Bu kimlikte vatandaşın adı, soyadı, doğum yeri, doğum tarihi, anne baba adı gibi normal belgelerde yer alan ya da ihtiyaç duyulacak bütün bilgiler kriptografik tekniklerle şifrlenerek blokszincir ağına yüklenecektir. Ayrıca doğrulamanın yapılabilmesi için parmak izi, yüz tarama, retina tarama gibi biyometrik veriler dijital kimliklere bağlanacaktır.

Dijital kimliğin kullanımı devletin belirleyeceği kurallara göre ilgili kurumlar gerektiği kadar yetkilendirilecek şekilde kullanılacaktır. Bir vatandaş devlet dairesine gittiğinde belirlenen doğrulama yöntemleriyle kim olduğunu ispatlayacak, devlet dairesi ise sadece kendi alanı ile ilgili bilgileri dijital kimlikte okuyabilecek ya da girdi yapabilecektir. Örneğin, vatandaş kredi için bankaya başvurduğunda maaş bordrosunu kurumuna onaylatıp götürmeye ihtiyaç duymayacak. Bu bilgi şahsın dijital kimliğine işli olacak ve banka da bu bilgiyi okuyabildiği için işlemler çok daha hızlı gerçekleştirilebilecek.

3.5.3. Kamu Mali Denetimi

Blokszincirin kamusal alanda fayda sağlayabileceği bir diğer alan da kamu mali denetimidir. Çünkü bu teknoloji, araştırmada ele alındığı gibi verilerin şeffaf, güvenli ve geriye dönük izlenebilir bir şekilde saklanmasını sağlamaktadır. Sağladığı şeffaflık ve izlenebilirlik özelliği ile blokszincir, kamu mali denetçilerinin kamu kaynaklarının nasıl harcandığını ve dağıtıldığını daha iyi anlamalarına yardımcı olabilir. İşlemler geriye dönük olarak izlenebilir olduğundan, denetimler daha etkili ve güvenilir hale gelir.

Blokszincir tabanlı sistemler ile anlık olarak güncellenen raporlar oluşturabilir. Bu, kamu mali denetçilerinin anlık olarak kamu kurumunun mali durumunu izlemelerine ve gerektiğinde hızlı müdahale etmelerine yardımcı olabilir. Blokszincirde verilerin güvenli bir şekilde saklanması sağlanır. Verilerin değiştirilmesi veya silinmesi neredeyse imkânsız olduğundan, veri bütünlüğü sağlanarak sahtekarlık önlenir. Blokszincir, otomatik olarak işlemleri kaydederek insan hatalarını ve suistimalleri azaltabilir. Akıllı

sözleşmeler belirli koşulların yerine getirilmesini otomatik olarak doğrulayarak mali işlemlerin daha hızlı ve doğru bir şekilde denetlenmesine yardımcı olur.

Blokzincir altyapısı kullanılarak iyileştirilen bir kamu mali denetimi ile kamusal kaynakların sorumlu bir şekilde harcandığına dair vatandaşlara güvence verilmesi, hükümete olan güvenin yeniden tesis edilmesine ve hesap verebilirliğin arttırılmasına yardımcı olacaktır (IBM, 2017: 12). Blokzincirin, özellikle akıllı sözleşmeler yoluyla kullanılması ile hukuki güvenlik dijital olarak teminat altına alınabilir. Öngörülebilir usulle ve rasyonel açıdan kabul edilebilir, şeffaf, hukuki değerlere dayanan bir hukuk düzenin sağlanması (Çaptuğ, 2021: 140), blokzincir kapsamında önceden belirlenmiş ve herkes için geçerli olan kuralların yürütülmesi ile güvence altına alınabilir.

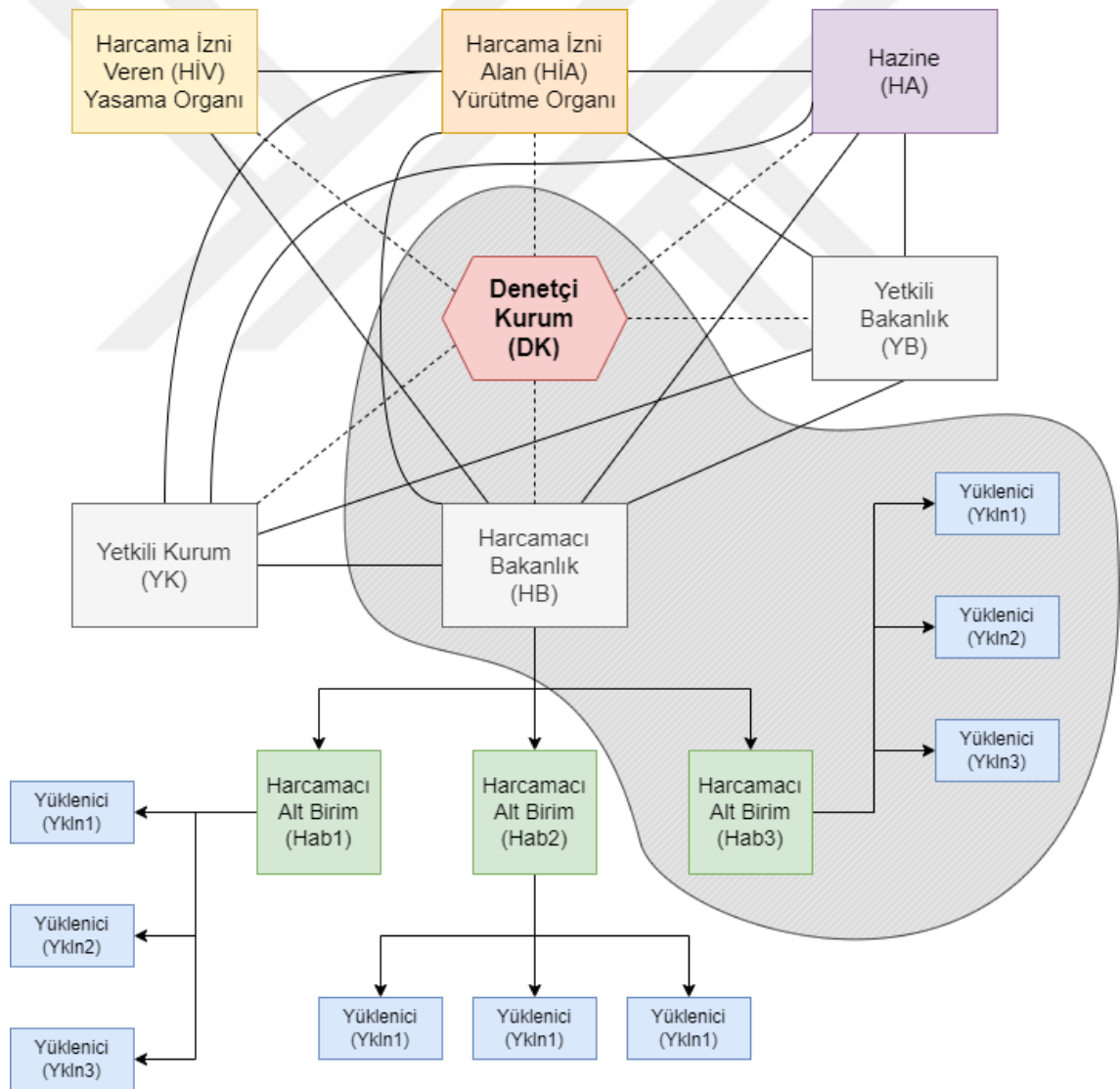
Blokzincir teknolojisi, kamusal hesapların denetim raporları ve bütçe gerçekleştirmelerinin şeffaf ve güvenilir bir şekilde yayımlanmasını sağlayabilir. Oluşturulan protokol ile belgelerin eksiksiz ve otomatik bir şekilde yayınlanması garanti edilirken, akıllı sözleşmeler ile bireysel hataların önüne geçilebilir. Bu yaklaşım, kamu idarelerinin hesap verebilirliğini artırır ve kurumsal disiplini teşvik eder, böylece belgelerin tamamlanmasını geciktiren sorunları ortadan kaldırır.

Blokzincirde yaptırımlar da otomatikleştirilerek tekrar eden suç geçmişisi olan yükleniciler cezalandırılabilirliğinden ötürü kamusal hizmetlerin etkinliğinde artış sağlanabilir (Mulligan ve Omar, 2016). Ancak hesap verebilirliğin tam olarak sağlanabilmesi için söz konusu yaptırımların kamusal gücü elinde bulunduranlar için de uygulanabilmesi gerekmektedir.

Aşağıdaki şema (Şekil 6), blokzincir teknolojisi kullanılarak kamu mali denetiminin sağlanmasına yönelik olarak sunulmuş bir modeldir. Kamu harcamaları konusundaki (akıllı sözleşmelerle getirilecek) katı sınırlamaların, devlet fonksiyonlarının aksamasına yol açması ihtimaline binaen, harcamacı alt birimler ile yükleniciler dışında kalan ilişkiler ağında blokzincir teknolojisinin kullanımına bu modelde yer verilmemiştir. Harcamacı alt birimler ile yükleniciler arasındaki ilişkilerde ise akıllı sözleşmelerin kullanılması, blokzincirin kamu mali denetiminde kullanımında örnek olması açısından önem taşımaktadır. Bu ilişkideki diğer tarafların yüksek denetim kurumu ve harcamacı bakanlıktan oluştuğu gözükmemektedir (*gri alan*). Kamusal mal ve hizmetlerin satın alınması sürecinin gerçekleştiği alan olması nedeniyle bu alan, dikkate alınması ve

protokollerin hazırlanmasında bir rehber olması bakımından iyi düzenlenmiş bir kamu ihale mevzuatı gerektirmektedir. Akıllı sözleşmeler bu kapsamda şekillendirilen yasal mevzuata göre hazırlanacak ve süreç otomatikleştirilecektir. Böylece ihale aşamasına gelmeden bütün koşullar belirlenecek ve bu koşullar yerine getirildikçe karşılıklı yükümlülükler kendiliğinden tatbik edilmiş olacaktır. Blokzincir teknolojisinin niteliksel diğer getirileri ile karşılaştırıldığında, ihale koşullarında gizli veya geriye dönük usulsüzlüklerin yapılması, hizmet ifası veya mal temini olmadan ödemenin gerçekleştirilmesi, hak ediş ödemelerinin keyfi olması, ihale koşulları haricinde fiyatlama yapılması vb. çok sayıda yolsuzluğun önüne geçilebilecektir (Eroğlu, 2023: 201-202).

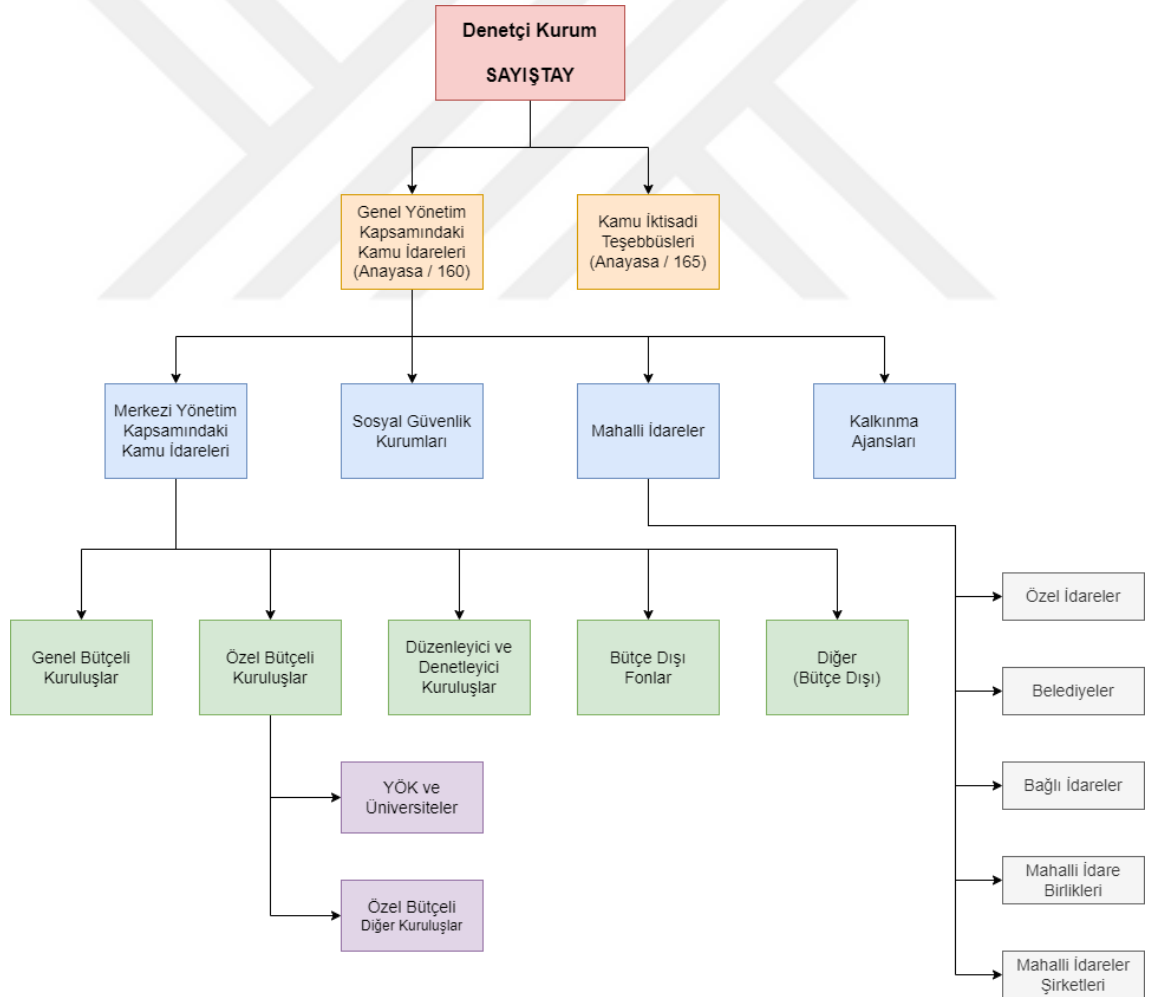
Şekil 6: Kamu Mali Denetimi Blokzincir Şeması



Kaynak: Eroğlu (2023: 201)'ndan esinlenilerek araştırmacı tarafından oluşturulmuştur.

Yukarıdaki şema (Şekil 6) genel bir çerçeve oluşturmakla birlikte her ülkenin kendi mali yapısına göre farklılaştırılabilir. Örneğin Türkiye’de yüksek denetim kurumu (DK) olan Sayıştay’ın Şekil 7’de gösterilen denetim alanına giren merkezi yönetim kapsamındaki kamu idareleri, sosyal güvenlik kurumları, mahalli idareler, kalkınma ajansları ve kamu iktisadi teşebbüsleri, harcamacı bakanlıklar (HB) kategorisinde değerlendirilmelidir. Bunlar arasında doğrudan bir bakanlığın altında özel bütçesi bulunan 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 (Hab) olarak bu sürece dâhil edilmelidir.

Şekil 7: Sayıştay Denetim Alanı



Kaynak: Sayıştay, 2023

Yetkili bakanlık (YB), bütçe hazırlığı esnasında birinci dereceden sorumluk verilen Hazine ve Maliye Bakanlığı (HA); yetkili kurum (YK) ise bütçeleme sürecinden birinci derecede sorumlu Strateji ve Bütçe Başkanlığıdır. Örnek olarak Karayolları Genel Müdürlüğüne altındaki harcamacı bir birimin yapacağı mal alım ihalesi (akıllı sözleşme vasıtasıyla) blokzincir üzerinden gerçekleştirildiğinde, bu sürecin daha önce tespit edilmiş kurallar çerçevesinde yapılması ve sonuçlandırılması gerekecektir. Dolayısıyla sürece yükleniciler (Ykln) de dâhil edilecektir. Bu süreçte bütçe ödeneklerinin serbest bırakılması, kullanılması ve takibinin doğrudan Hazine ve Maliye Bakanlığı ile Strateji ve Bütçe Başkanlığı tarafından icrası mümkün hale gelecektir. Gerekğinde bütçeyi onaylayan Meclis (veya Meclis'te kurulacak bir komisyon) da süreçteki tüm kamusal harcamaları anlık olarak izleyebilecektir. Bu sürecin sonucunda elde edilen veriler, daha sonra Sayıştay tarafından gerçekleştirilen denetim sonuçları ile de kıyaslanabilecektir. Sayıştay bu çerçeve içerisinde merkezi bir konumda yer alarak hem harcamacı birimlerin faaliyetlerini denetleyebilecek hem de bu denetim sonuçlarını Meclis'e aktarabilecektir (Eroğlu, 2023: 202-203).

Kamu mali denetimine yönelik olarak hükümetler, blokzincir teknolojisini kullanmaya özellikle akıllı sözleşmeye dayalı protokoller oluşturarak aşamalı olarak başlayabilirler. Ancak blokzincirin kamu mali denetimine entegre edilmesi zorlu bir süreç olabilir ve bazı zorluklarla karşılaşılabilir. Örneğin, mevcut mevzuat ve düzenlemelere uygun olarak çalışması gereken yeni bir teknolojiyi uygulamak karmaşıklık yaratabilir. Bu nedenle, blokzincir tabanlı sistemlerin kamu mali denetimine entegre edilmesi için iyi bir planlama ve uygun düzenlemeler gereklidir.

3.5.4. Tapu Tescili

Tapu tescili, mülkle ilgili detayların toplanmasını kaydedilmesi sürecidir. Halihazırda tüm tapu sicil süreci oldukça zaman alıcıdır. Çünkü süreç, büyük hacimli sicillerin yazılı biçimde saklanması gerektirmektedir. Ayrıca sürecin çoğu şeffaf olmadığından ve sistem yavaş olduğundan mevcut sistem güvenli değildir. Defter tutma sürecini ortadan kaldırarak tapu sicil verilerinin kaydını otomatikleştirmek için çeşitli çözümler geliştirilmiştir. Bu, başlangıçta verileri büyük veri tabanlarında depolayarak yapılmıştır. Ancak bu yöntem, veri güvenliği açısından verimli değildir, çünkü veri içeriklerinin kolayca ihlal edilme ihtimali bulunmaktadır. Blokzincir kullanarak tapu

tescilinin yapılması uygulanması, hileli faaliyetlerden korunmaya yardımcı olacak ve sistemi daha güvenli hale getirecektir (S ve Sarath, 2020: 1708-1709). Bu teknolojiyi kullanarak tapu sicilini uygulamak, arazi işlemlerindeki olası yasa dışı faaliyetlerden kaçınmaya yardımcı olacaktır.

2016 yılında Gürcistan Cumhuriyeti Ulusal Kamu Sicil Dairesi (NAPR), dünyanın ilk blokzincir tabanlı tapu kayıt sistemini devreye almıştır. NAPR, blokzincir altyapısını kullanarak vatandaşların güvenliğini artırırken ve veri güvenliğini geliştirirken, zaman alıcı idari süreçleri otomatikleştirmeyi başarmıştır. NAPR, dijital sahiplik belgesini yayınladığında, belge güvenli bir hash'e dönüştürülür ve üç dakikadan kısa bir sürede blokzincirde saklanır (REI, 2022). Bu, kayıt sürecini önemli ölçüde hızlandırır. Buna ek olarak, arazi mülkiyeti kayıtlarının değiştirilemez, güvenli ve şeffaf bir blokzincir platformunda saklanması, arazi sahiplerine mülkiyetlerine dair sağlam kanıtlar sağlar; böylelikle dolandırıcılık riski ve belirsiz tapu zinciri olasılığı azaltılarak mülkiyet denetimleri yetkili personel tarafından gerçek zamanlı olarak gerçekleştirilmiş olur (Ahma ve Al-Saleh, 2021: 19).

Tapu tescili uygulamalarına bir diğer örnek olarak Honduras hükümetinin Factom firması ile arazi sahipliği kayıtlarını tutmak üzere başlattığı blokzincir tabanlı pilot program verilebilir. Burada amaç dağıtık ve şeffaf bir kayıt sistemi oluşturarak, hükümet yetkilileri kontrolündeki merkezi kayıt sisteminden kaynaklanan yolsuzluk ve dolandırıcılığı önlemek olmuştur (Schatsky ve Muraskin, 2015: 4).

İsveç'te yapılan bir araştırmada blokzincir teknolojisinin tapu tescilinde kullanılması halinde şu dört faydanın ortaya çıkacağını savunulmaktadır (Ølnes ve Jansen, 2018: 3):

- Üçüncü taraflara olan ihtiyacın azalması
- Yapılması gereken işlemlerin ve zamanın azalması
- Kâğıt doküman kullanımının bitmesi
- Dijital imzaların onay süreçlerini kısaltması

Gana'da hayata geçirilen BenBen projesinde tüm tapu kayıtlarının Ethereum ağında tutulması öngörülmüştür. Bu projede tüm arazi sahipleri ve tapu parsellerine ait detaylar blokzincire kaydedilmekte ve diğer paydaş kurumlar ile paylaşılmaktadır.

BenBen sayesinde Gana’da gayrimenkul alım satım süreleri yüzde 75 oranında kısalmış ve hukuki anlaşmazlıkların sayısı önemli oranda azalmıştır (Tanrıverdi vd., 2019: 213).

3.5.5. Elektronik Oylama

İdeal bir seçim sisteminde olması gereken; her vatandaşın oyunu kimsenin baskısı altında kalmadan serbestçe kullanabilmesi, oylamanın da gizli oy ve açık sayım şeklinde gerçekleştirilmesidir. Nitekim Anayasanın 67’nci maddesinde de “Seçimler ve halkoylaması serbest, eşit, gizli, tek dereceli, genel oy, açık sayım ve döküm esaslarına göre, yargı yönetim ve denetimi altında yapılır.” denilmektedir.

Çevrimiçi oylama sistemlerinin oluşturulması, bu tür sistemlerde tarafsızlığın sağlanması gerekliliği nedeniyle zorlu olabilir. Adil bir seçim sağlamak için, çevrimiçi oylama sistemleri anonim ancak denetlenebilir olmalı, aynı zamanda dış müdahaleye dirençli fakat arabulucu nitelikte olmamalıdır (Mattila, 2016: 18). Blokzincir teknolojisi bu açıdan oldukça caziptir, çünkü teknik açıdan, tüm gereklilikleri karşılayabilme yeteneğine sahiptir.

Özellikle ülke çapındaki seçimler birçok zorluğu bünyesinde barındırmaktadır. Blokzincir altyapısının kurulmasıyla birlikte oylama işlemi tarafların güven duymasına gerek kalmaksızın emniyetli bir şekilde gerçekleştirilebilecektir. Bazı araştırmalarda (Kshetri ve Voas, 2018: 1) bunun cep telefonları vasıtasıyla yapılabileceği öne sürülmektedir. Yine de seçmenlerin baskı altında kalmadan oyunu kullanabilmesi için halihazırda kurulan oy sandıkları gibi dijital oy sandıkları (bilgisayarları) kurulabilir. Oyunu kullanmaya gelen vatandaş, üzerinde mutabakat sağlanan doğrulama yöntemleriyle kimliğini kanıtladıktan sonra oyunu dijital olarak kullanacaktır. Gönderenin ve alıcının gizlendiği kripto para sistemlerine benzer şekilde sistem sadece hangi partiye oy kullanıldığını sayıma dâhil edecek, oyun kimin tarafından kullanıldığı bilgisi ise kesinlikle paylaşılmayacaktır. Burada sadece vatandaş kendisine ait gizli anahtar ile oyunun gerçekten kullandığı gibi sisteme işlenip işlenmediğini kontrol edebilecektir. Bununla birlikte seçime katılan bütün taraflar/partiler bitcoin ağındaki madenciler gibi oyların doğrulanması için düğüm görevi görecektir. Bu ağa örneğin seçime katılan yirmi parti varsa bu partilerin tamamı, ayrıca yüksek seçim kurulu, bunlarla birlikte izin verilen tarafsız denetim kuruluşları katılabilecek, oy doğrulama işlemi bunlar tarafından gerçekleştirilecektir. Sistem dijital olduğu için vatandaşın oyunu

kullanması için ikametinin olduğu yere gitmesine gerek kalmayacak, dijital oy sandığında kimliğini kanıtladığında sistem ona otomatik olarak dijital oy pusulasını karşısına çıkaracaktır. Örneğin belediye seçimlerinde ikameti Afyonkarahisar’da olan ama geçici olarak İstanbul’a gelmiş bir vatandaş oy kullanmak için Afyonkarahisar’a gitmek zorunda kalmayacak, kendisini sisteme tanıtır tanıtmaz sırasıyla Afyonkarahisar belediye başkanı, belediye meclis üyesi ve muhtar adaylarının yer aldığı oy pusulalarından seçimini yapacaktır.

Böyle bir seçim sistemi ile oylama biter bitmez ya da çok kısa bir süre içerisinde seçim sonuçları açıklanabilecektir. Sistem tarafların birbirine güvenme gerekliliğini ortadan kaldırdığı için de seçim sonuçları kesin olacaktır. Böylelikle mevcut seçimlerde yaşanan sorunların hiçbiri yaşanmayacaktır.

Blokzincirlerin halka açık ve anonim olarak tasarlanabilmesi nedeniyle, herkes oylama sonucunu kolayca doğrulayabilir ve oy pusulası gizliliğini korurken kendi oylarının da buna göre dikkate alındığını kontrol edebilir. Bu nedenle Blokzincir teknolojisi, siyasi sistemlerde yolsuzluğu azaltmaya yardımcı olabilir ve katı seçimlere karşı bir koruma görevi üstlenebilir (Mattila, 2016: 18).

Blokzincir tabanlı oylama sistemi sadece ülke çapında değil kurumsal seviyede de uygulanabilecektir. Örneğin stratejik bir kararla ilgili paydaşlarının onayını almak isteyen bir kurum, bu maksadını gerçekleştirebilmek için blokzincir altyapısını kullanarak yüksek maliyetli giderlerden de tasarruf etmiş olacaktır.

Bu sistemin hayata geçirilmesi ile her türlü seçim/oylama daha şeffaf ve güvenilir olacaktır. Bu nedenle seçimlere katılımın artması sistemin sağlayacağı avantajların başında gelmektedir. Ayrıca mührün dışarı taşırılması, yanlış yere vurulması vb. gibi seçimden kaynaklanan hataların önüne geçilecektir.

Bu uygulamaya örnek olarak Endonezya’da hayata geçirilen blokzincir tabanlı elektronik oylama denemesi verilebilir. Karmaşık kâğıt tabanlı oylama sistemi ve 17.000 ada ve 193 milyon seçmeni kapsayan zorlu coğrafi yapısıyla Endonezya, seçim sonuçlarının açıklanmasında sıklıkla uzun süreli gecikmeler yaşanan ve bu nedenle sık sık seçim manipülasyonu şüphelerinin olduğu bir ülkedir. Bu sorunu çözmek için SettleMint firması ile Endonezya Üniversitesi birlikteliğinde Nisan 2019 seçimlerinde yenilikçi bir blokzincir tabanlı çözüm uygulanmıştır. Sistem, seçim sonuçlarının

blokzincir üzerinde güvenli bir şekilde saklanarak zaman alan, oyların manuel olarak toplanması ve doğrulanması sürecini neredeyse tamamen ortadan kaldırmıştır. Geleneksel olarak resmî sonuçların açıklanması haftaları alırken, bu teknoloji ile sandıkların kapatılmasından birkaç saat sonra 25 milyon oyun rapor edilmesini sağlanmıştır (Settlement, 2020).

Endonezya'da oy sayma işlemi, yerel oy verme merkezlerinde kâğıt oy pusulalarının sayılması, sonuçların "C1" olarak bilinen formlara kaydedilmesi, bu formların fotoğraflarının çekilmesi ve sosyal medya platformlarında paylaşımını içermektedir. Ancak bu kitle kaynaklı veri tabanlarının gerçekliği ve bütünlüğü, oy hırsızlığı ve manipülasyon riski nedeniyle sıklıkla sorgulanmaktaydı. Blokzincir teknolojisi, bu fotoğrafların zincire kaydedilerek ve 25 milyon oya karşılık gelen 100.000'den fazla "değiştirilemez" görüntüden oluşan bir depo oluşturarak, her fotoğrafın doğrulanabildiği bir "bütünlük kanıtı" oluşturulmasını sağlamıştır. Dahası, blokzincirin şeffaflığı herkesin bu iddiaları kamuya açık bir web sitesinde bağımsız olarak doğrulamasına olanak tanımıştır (Settlement, 2020).

Endonezya seçimlerinde blokzincir teknolojisinin başarılı bir şekilde uygulanması, zamanında oy sayımı ve sonuç raporlamasının lojistik zorluklar sebebiyle zorlaştığı Asya ve Afrika'daki demokrasilerde oy verme sürecini kolaylaştırma potansiyelini göstermektedir. Blokzincir, oylama ile sonuçların yayınlanması arasındaki süreyi azaltarak yalnızca siyasi gerilimleri azaltmakla kalmamakta, aynı zamanda seçim sahtekarlığı riskini de azaltarak onu demokratik süreçlerin bütünlüğünü korumak için bir araç haline getirmektedir.

Faydalarının yanında blokzincir tabanlı oylama sisteminin hayata geçirilebilmesi için aşılması gereken önemli sorunlar bulunmaktadır. Öncelikle sistem henüz tasarım/deneme aşamasındadır. Büyük çaplı oylamalarda kullanılmadan önce sistemin tam olarak işler hale getirilmesi gerekmektedir. Sistemin ülke seçimlerinde kullanılabilmesi için gerekli teknolojik altyapının devletler tarafından kurulması ve yaygınlaştırılması şarttır. Ayrıca sisteme olan güvenin sağlanabilmesi için vatandaşların ikna edilmesi gerekmektedir (Kshetri ve Voas, 2018: 3). Ancak bu şartlar sağlandıktan sonra kendisinden beklenen faydalar gerçekleşebilecektir.

3.5.6. Sağlık Hizmetleri

Blokzincir teknolojisinin en çok etkileyeceği sektörlerden biri de sağlık sektörüdür. Bu teknoloji merkezi olmayan ve güvenli olduğu için sağlık kayıtlarını tutmak, almak ve iletmek, ilaç tedarik zinciri yönetimini yönetmek için kullanılabilir, bu da sağlık sektörüne verimli bir çözüm sağlayacaktır (Deloitte, 2016: 1-2). Sağlık sektörünün en büyük zorluğu, birbiriyle bağlantılı olmayan çeşitli kuruluşlar tarafından izole edilmiş elektronik sağlık kayıtlarının muhafazasıdır. Bilgi alışverişi maliyetli olduğundan, her sistem farklı veri standartlarına ve birlikte çalışması zor olan süreçlere ihtiyaç duymaktadır (Orcutt, 2017). Hastanın kayıtları diğer sistemler aracılığıyla iletilir, bu da doktorların tıbbi geçmişlere erişmesini zorlaştırır.

Sağlık sektöründe blokzincir teknolojisinin getireceği birçok fayda bulunmaktadır. Bunlar şu şekilde sıralanabilir (Vaniukov, 2022):

1. Hasta Veri Yönetimi:

Faydası: Geliştirilmiş veri güvenliği, erişilebilirlik ve bütünlük.

Hastaların tıbbi kayıtları merkezi olmayan bir blokzincirde güvenli bir şekilde saklanabilir, bu da onu bilgisayar korsanlığına ve kurcalamaya karşı dayanıklı hale getirir. Böylelikle hem hasta verilerinin gizliliği hem de hastalar ve sağlık hizmeti sağlayıcıları için tıbbi kayıtlara erişim kolaylığı sağlanmış olur.

2. Veri Şifrelemede Yüksek Güvenlik Standartları:

Faydası: Gelişmiş veri güvenliği.

Blokzincir, veri ihlallerini ve hassas tıbbi bilgilere yetkisiz erişimi önleyen güçlü güvenlik standartları sunar. Bu, hasta mahremiyetinin korunması ve HIPAA gibi düzenlemelere uyum açısından önem arz etmektedir.

3. Sağlık İşlemleri Kontrolü:

Faydası: Daha az dolandırıcılık ve kolaylaştırılmış ödeme süreçleri.

Blokzincir, sağlık hizmetleri işlemlerinde talep reddini, eksik ödemeleri ve dolandırıcılık faaliyetlerini en aza indirmeye yardımcı olarak tıbbi tesisler için daha verimli gelir olanakları sunmaktadır.

4. İlaç Tedarik Zinciri Yönetimi:

Faydası: Sahte ilaç önleme ve gelişmiş tedarik zinciri şeffaflığı.

Pek çok tıbbi ürün belirli bir sıcaklık aralığına duyarlı olduğundan, ilaçların tedarik zinciri yönetimi de sağlık hizmetlerinde çok önemli bir husustur. Tedarik zinciri yönetiminde blokzincir teknolojisinin kullanılmasıyla tıp uzmanları, ilaçları çevresel koşullara göre takip edip doğrulayabilir ve tıbbi standartlara göre ilacı atmaya veya kabul etmeye karar verebilir (Alam vd., 2021). Özetle blokzincir, ilaçların üretimini ve dağıtımını takip etmek için kullanılabilir ve böylece piyasadaki sahte ilaçların yaygınlığı azaltılabilir.

5. Klinik Araştırmalar ve Sağlık Hizmetleri Araştırmalarının İyileştirilmesi:

Faydası: Geliştirilmiş veri şeffaflığı, güvenliği ve güvenilirliği.

Blokzincir, klinik deney verilerinin bütünlüğünü sağlayarak onu daha güvenilir ve emniyetli hale getirir. Araştırmacılar verilere güvenle erişebilir ve akıllı sözleşmeler deneme süreçlerini kolaylaştırabilir.

6. Tıbbi Evrak Yönetimi:

Faydası: Daha az evrak işi, daha fazla verimlilik ve daha düşük idari maliyetler.

Blokzincir, sağlık hizmetlerinde kapsamlı evrak ihtiyacını azaltarak işlemleri ve sigorta taleplerini daha yönetilebilir ve hataya daha az eğilimli hale getirebilir.

7. Giyilebilir IoT Cihazlarıyla Entegrasyon:

Faydası: Gelişmiş izleme ve veri paylaşımı.

Blokzincir, giyilebilir IoT cihazlarından gelen verileri güvenli bir şekilde entegre ederek hastaların ve sağlık hizmeti sağlayıcılarının daha iyi sağlık yönetimi için güncel sağlık kayıtlarına erişmesine olanak tanır.

8. Tıbbi Kimlik Bilgilerinin Takibi:

Faydası: Sağlık hizmeti sağlayıcılarının niteliklerinin ve deneyimlerinin doğrulanması.

Blokzincir tıbbi kimlik bilgilerini saklar ve doğrular, tıp profesyonellerinin iş alım sürecini basitleştirir ve niteliklerinin doğruluğunu garanti eder.

9. Sigorta için Akıllı Sözleşmeler:

Faydası: Kolaylaştırılmış sigorta süreçleri ve şeffaflık.

Blokzincir üzerindeki akıllı sözleşmeler, sigorta sözleşmelerini otomatik hale getirerek sigorta kapsamına hızlı erişim sağlar ve ilaç geri ödemesi ve sağlık sigortasıyla ilgili anlaşmazlıkları azaltır.

Blokzincir sağlık sektörüne çok sayıda fayda sunarken, teknik, kültürel, düzenleyici ve yasal engeller de dâhil olmak üzere aşılması gereken zorluklar da mevcuttur. Ancak teknoloji olgunlaştıkça ve daha geniş bir kabul kazandıkça, sağlık hizmetlerini dönüştürme potansiyeli artarak devam edecektir.

Blokzincir tabanlı kayıt hizmeti sağlayan Factom firması sonradan karşılaşılabilecek anlaşmazlık, dava vs. durumlarda kullanılmak üzere hastane faturası ve doktor-hasta etkileşimleri vb. tıbbi kayıtları saklamak için blokzincir teknolojisini kullanmayı amaçlamaktadır. Kayıtların değiştirilemez niteliğinin uyuşmazlıkların çözümünü kolaylaştırması beklenmektedir. Bu şekilde tutulacak kayıtlar içinde hastaların tedarikçilerle bilgi paylaşımına daha yatkın olacakları düşünülmektedir.

Blokzincir sistemleri; hasta onayı ve klinik deney protokollerinin incelenmesi gibi adımların takibi, karmaşık klinik deney verilerinin yönetimi ve onların kötüye kullanımının önlenmesi gibi klinik deney süreçlerinin geliştirilmesi konusunda öne çıkarılmaktadır. Bazı araştırmalarda blokzincir ile hastaların, hasta yakınlarının ve üçüncü tarafların tıbbi kayıtlara güvenilir bir şekilde erişimini sağlayacak sistemlerin tasarımının yapılabileceği ileri sürülmektedir. Burada daha çok özel verilerin gizliliği ve saklanmasıyla ilgili erişim sorunları üzerinde durulmaktadır.

Blokzincir, medikal kayıtların birden fazla sağlık hizmeti sağlayıcısı ve ilgili sektör arasında kontrollü paylaşımını sağlar. Hastaların kayıtlarını sahiplenmelerini kolaylaştırırken onları değiştirmelerini de engeller. Ayrıca hastaların gizliliklerini korurken sağlık verilerini kontrol etmelerine ve güvenli bir şekilde paylaşmalarına olanak sağlar. İlaç tedarik zinciri yönetimi süreçlerini geliştirir. Hasta verilerinin, tıbbi

yeniliklerin ve araştırma sonuçlarının ayrıntılı analizini kolaylaştırır (Al-Jaroodi ve Mohamed, 2019: 36507).

Blokzincirin sağlık hizmetlerinde kullanımına örnek olarak BAE Sağlık ve Önleme Bakanlığı'nın (MOHAP), organ bağıışı tahsisi ve nakillerinde güvenli doğrulama için blokzincir teknolojisinin kullanımını öngören "Hayat" bağıışçı kaydı projesi verilebilir. Projenin; organ nakline erişilebilirliğin iyileştirilmesi, sürecin hızlandırılması ve güvence altına alınması, gelişmiş organ tahsisinin uygulanması ve organ kaynağının mevzuata uygunluğunun sağlanması olmak üzere dört temel hedefi mevcuttur. Projede, BAE'nin karmaşık sağlık sisteminde donör kayıt defterlerinin geliştirilmesine odaklanılmış, ulusal bir bekleme listesi oluşturulmuş ve organ menşei doğrulaması ile yapay zekâ odaklı organ tahsisi birleştirerek üç temel aşamadan oluşan bir yaklaşımı benimsenmiştir (World Economic Forum, 2020: 21-22).

Hayat uygulaması Ocak 2019'da kullanıma sunulduğundan bu yana binlerce kayıtlı bağıışçının ilgisini çekmiş ve tüm yetkili hastanelerin ulusal bekleme listesi ve tahsis platformuna dâhil olmasını sağlamıştır. Bu çözüm ile MOHAP'ın diyaliz maliyetlerinde yıllık 20 milyon dolardan fazla tasarruf olanağı elde edilmiş, vatandaşlara çevrimiçi bağıışçı kaydı imkânı sunulmuş ve çalışma saatleri sırasında kayıt merkezlerine fiziksel ziyaret ihtiyacını azaltma olanağı temin edilmiştir (World Economic Forum, 2020: 21-22).

3.5.7. Vergilendirme / Muhasebe

Muhasebe uygulamalarına Blokzincir teknolojisine sunduğu en önemli yenilik geleneksel olarak bilinen çift taraflı kayıt sistemi yerine Blokzincir teknolojisine kendine has özelliği olan üç taraflı kayıt sisteminin kullanılacak olmasıdır. Muhasebe uygulamalarında bilindiği üzere çift taraflı kayıt sistemi kullanılarak işlem yapılmaktadır. Bir başka deyişle işletmelerde ekonomik işlemlerin raporlanma aşamasında kaynak ve varlık hesaplarından oluşan aynı anda çift tarafında çalışabildiği bir kayıt sistemi kullanılmaktadır. Bu uygulamayla bir işletmeye ait olan ekonomik işlemlerin her iki yönü de kaydedilmektedir. Bunu uygulayabilmek için de finansal kayıtlar işletmeye ait olan özel defterlerde (envanter defteri, yevmiye defteri ve büyük defter) tutulmakta ve beyana dayalı olarak yasal mevzuat dikkate alınarak sunulmaktadır. Her işletme için bu işlem süreci; finansal bilgilerin işletme ile ilgili bilgi kullanıcılarına aktarılmasına imkân

tanımakta ve etkinliği düşük, kaynak maliyeti oldukça yüksek ve uzun zaman alan işlemleri kapsamaktadır. Blokzincirdeki dağıtık yapı, geleneksel muhasebe anlayışındaki iki taralı yapıya üçüncü taraf olarak dâhil olacak ve paydaşların işlem kayıtlarına ulaşmasını ve verilerin şeffaf, erişilebilir ve geri döndürülemez şekilde depolanmasını sağlayacaktır. Bu da geçerli sistemin sağladığı güvencenin çok daha üzerinde bir güvence demektir (Uçma Uysal ve Kurt, 2018: 472-474). Bu anlamıyla da blokzincir teknolojisi muhasebenin bir sonraki adımı olmaktadır. İşletmelerin ayrı ayrı ticari belgeleri üzerinde yürütülen bir kayıt tutma sistemi yerine tüm işletmelerin yer alacağı ortak bir ekosisteme geçişin altyapısını oluşturacaktır.

Blokzincir altyapısına dayanan vergilendirme sistemi ile vergilerin tahsilinde otomatikleşme sağlanabilecektir. Devlet, vergiyi aracı kurumlara gerek kalmadan hızlı bir şekilde tahsil ederek, işlem maliyetlerini büyük ölçüde azaltabilecektir. Böylelikle bir yandan işverenlerin nakit akışı sorunlarını hafifletecek bir yandan da vergi kaçırmanın önüne geçme konusunda mesafe kaydedilebilecektir (Akdemir Altunbaşak, 2018, 369).

Jurowiec (2018), blokzincirin devlet vergi idareleri üzerindeki potansiyel etkilerini şu şekilde sıralamaktadır:

- Hükümet, blokzincir destekli bir vergi idaresi kullanarak büyük avantaj elde edecektir. Bir şirketin dönemsel işlemlerini harmanlamak, tercüme etmek, işlemek ve belgelemek gibi son derece zor bir görev, üzerinde oynanamayan veya değiştirilemeyen daha dijital ve güvenli, paylaşılabılır belgelere elde edilmesine imkan sağlayacaktır.
- Gelirler, giderler, borçlar ve diğer bilgiler gibi işletmelerin işlemlerinin periyodik olarak kendi kendine raporlanması, vergi işlem süresi ve vergi dairesi tarafından, tahsil edilmesi gereken vergilerin derhal tahsilini imkan tanıyacaktır.
- Dolaylı vergiler, blokzincir teknolojisi ile değiştirilebilecek ve basitleştirilebilecektir. Bu teknolojinin şeffaflığı ve hızlılığı, ekonomi sektöründeki vergilerin, özellikle KDV ve diğer satış vergilerinin gerçek zamanlı olarak doğrulanmasına ve havale edilmesine olanak sağlayabilecektir. Bu hem devlet hem de şirketler için özellikle avantajlıdır.

- Vergi ihtilafları, hükümet ve vergi mükellefleri için zamanı büyük ölçüde azaltabilecek ve tasarruf sağlanabilecektir. Blokzincirin şeffaflığı, doğrulamayı, çatışmaları ve tartışmaları neredeyse sıfıra indirebilme potansiyeline sahiptir.

3.5.8. Varlık Kaydı

Mülkiyet yönetimi esas olarak arabalar, evler, sanat eserleri, dijital yayınlar vb. dâhil olmak üzere mülkiyet hakları ve telif haklarının yönetimi ve izlenebilirliği için kullanılmaktadır. Mülkiyet yönetiminin birkaç önemli sorunu vardır: (1) ürün doğrulama ve yönetim mülkiyeti, (2) işlem güvenliği ve güvenilirlik ve (3) gizlilik koruması. Blokzincir teknolojisi kullanılarak, mülkiyet blokzincire işlenebilir ve değiştirilmesi engellenmiş olur. Sözleşme yapıldıktan sonra blokzincir, sözleşmenin doğru şekilde yürütülmesini sağlayacak ve varlık sahipliğini takip edecektir. Blokzincir, zaman damgaları ve hash algoritmaları yoluyla mülkiyeti teyit eder ve metin, video ve ses gibi değerlemelerin varlığını, gerçekliğini ve benzersizliğini kanıtlar. Ayrıca bozulmaya dirençli dijital kanıt sağlar. Mülkiyet doğrulandıktan sonra, mülkiyetin benzersizliğini korumak için kayıtlar ortak defterde depolanır (Yang, 2019: 88).

Blokzincirin varlık kaydında kullanılmasına örnek olarak Danimarka'da yapılan Vehicle Wallet projesi verilebilir. Bu projede her araç için üretim, onarım, kiralama hizmetleri, mülkiyet değişikliği, hurdaya çıkma gibi verilerin, blokzincir üzerindeki dijital cüzdanlarda saklanması amaçlanmıştır. Proje yardımıyla alım satım süreçlerindeki riskler düşürülmüştür. Aynı zamanda Danimarka Vergi Kuramlarının araç cüzdanlarına erişimi sayesinde vergi tahsilatlarının etkili bir şekilde yapılmasına olanak sağlanmıştır (Tanrıverdi vd., 2019: 213).

DocuSign adındaki elektronik imza sağlayıcısı olan firmanın geliştirdiği uygulamada, araç alım satım sözleşmeleri bitcoin blokzincirine entegre edilmiştir. Böylelikle araç satın alma ve kiralama süreçlerini kolaylaştırmayı hedeflemektedir (Schatsky ve Muraskin, 2015: 3).

3.5.9. Gıda Güvenliği

Dünyadaki en önemli sorunlardan bir tanesi gıda güvenliğini sağlayabilmek ve gıdada taklit ve tağşişinin önüne geçerek insan sağlığının ve tüketici menfaatlerinin

korunması, haksız rekabetin önüne geçilmesidir. Blokzincir teknolojisi ile verilerin şeffaflığı ve değiştirilemezliği garanti altına alınarak veriler dijital saldırılardan korunacak, dış etkenlerden etkilenmeyecek ve güvenliği muhafaza edilecektir. Bu sayede gıda güvenliği sağlanarak sektörde sürdürülebilir geniş bir uygulama alanı oluşturabilecektir. Blokzincir, ağırlıklı olarak finans sektöründe uygulamalara sahip olmakla birlikte gıda güvenliği ve bunun takibi amacıyla da kullanılmaya başlanmıştır. Bu teknoloji sayesinde tarımsal bir ürün üretim, işleme, dağıtım ve tüketiciyle bulunduğu ana kadar her aşamasında dijital ve şeffaf bir şekilde kriptolu olarak takip edilebilecek, hatta yüksek güvenliqli olarak ödeme de alınabilecektir (Gerdan vd., 2020: 8).

Buna örnek olarak Carrefour'un, "Quality Line" projesi ile Belçika'da ürünlerinin menşei konusunda tüketicilere tam bir şeffaflık sunmak ve tedarik zincirini blokzincir teknolojisini kullanarak dijitalleştirmek için Belçikalı denetim kurumu Vinçotte ve SettleMint şirketi ile yaptığı iş birliği verilebilir.

Günümüzde tüketiciler daha bilinçli ve satın aldıkları ürünlerin menşesine daha fazla önem vermektedirler. Bu noktada gıda zincirinde daha fazla şeffaflığa yönelik artan bir talep mevcuttur. Bu talebe yönelik olarak Carrefour, Belçika'da bir çözüm geliştirmiştir. Blokzincir tabanlı bu tedarik zinciri yönetiminde, bir ürünün başlangıcından mevcut bulunduğu yere kadar olan yolculuğunun tamamı görselleştirilebilmektedir. Bu da ürünün kaynak takibini çok kolay hale getirmektedir. Dijital izlenebilirlik çözümü, paketleme işlemi sırasında ürüne eklenen dinamik bir karekoda dayanmaktadır. Tüketicinin, ürünün çiftlikten mağazaya kadar tüm yaşam döngüsünü görebilmesi için ürün üzerindeki karekodunu akıllı telefonuyla taraması yeterlidir. Uygulama; ürünü yetiştiren çiftçinin adını ve yerini, yetiştirme koşullarını, kesildiği yeri ve etin nerede kesilip paketlenildiğini göstermektedir (SettleMint, 2020).

Bu uygulama ile gıdanın nereden geldiğine ilişkin gerçek tüketici talebine yanıt verilmekte ve çiftlikten mağazaya kadar olan süreçte tam görünürlük sağlanarak, markaya daha fazla güven ve daha güçlü bir bağlılık oluşmaktadır. Bu girişim, blokzincir teknolojisinin olumlu bir marka deneyimine katkıda bulunabileceğini de göstermektedir. Uygulama aynı zamanda paydaşların tedarik zincirindeki potansiyel sorunlara daha hızlı ve daha doğru tepki vermesini sağlayarak genel gıda güvenliğinin iyileşmesine katkıda bulunmaktadır (SettleMint, 2020).

Blokzincir teknolojisi doğru uygulandığında maliyet etkinliği artıracaktır. Gıda israfının azaltılmasına yardımcı olacak ve tarımla ilgili sigorta destek süreçlerini geliştirebilecektir. Gıda tedarik zinciri yönetiminde güvenilir gıda güvenliği takibi sağlayacak ve gıda sahtekarlığının caydırılmasına yardımcı olacaktır.

3.5.10. Savunma Sanayi

Blokzincir teknolojisinin, başlangıçta özellikle kripto para ve bankacılık sektöründe kullanımı öne çıksa da, zamanla tedarik zinciri yönetimi, sağlık hizmetleri, sigortacılık hizmetleri gibi pek çok sektörde kullanılmaya başlanmıştır. Savunma sanayisi de bu alanların arasında yer almaktadır. Siber saldırılar özellikle savunma sanayisinde başlıca önem arz eden konuların başında gelmektedir. Askeri organizasyonlar, kendilerini hacker'lara ve siber açıklara karşı korumak mecburiyetindedir. Bu nedenle savunma alanında faaliyet gösteren kurumlar, blokzincir sistemlerine yatırım yapmaktadır. Çok sayıda insanın yer aldığı ve yüksek güvenlik düzeyinin korunmasının gerektiği savunma sanayisi blokzincir için kurtarıcı bir niteliktedir (STM, 2020: 1).

Emir komuta zinciri dâhilindeki iletişim ve bilgi aktarımı için bugün askeri yapılarda yüksek kriptografik çözümler kullanılmaktadır. Ancak yine de emir komuta süreçlerinde aksamalar ve yanıltıcı durumlar oluşabilmektedir (Usta ve Doğantekin, 2018: 62). Verilen bir emrin, komuta merkezinden mi geldiği düşmanın bir yanıltması mı olduğu, blokzincir ile daha hızlı ve güvenilir bir şekilde tespit edilebilir.

Blokzincirin merkezi olmayan doğasından kaynaklanan avantajları onu özellikle savunma sanayiinde faydalı kılmaktadır. İlk olarak, blokzincirin dağıtık yapısı kullanılabilirliğini arttırmaktadır. İkinci olarak, verilerin gizliliği, güvenliği ve değişmezliği, bu konuda hassasiyete sahip savunma sanayisi alanında özellikle önemlidir. 2017 yılında Accenture tarafından yapılan ankete katılan havacılık ve savunma endüstrisi yöneticilerinin büyümesini ve verimliliği artırmak için teşvik etmek istedikleri en önemli gelişen teknolojilerden biri olarak blokzinciri göstermelerinin nedeni budur. Ayrıca, dünyanın her yerindeki savunma departmanları, blokzincirin gücünden giderek daha fazla etkilenebilmektedir (Audrey vd., 2020: 8-9). Blokzincir teknolojisi hem operasyonel hem de destek rollerinde kullanılabildiği için savunma sektöründe birçok faydaya sahiptir. Siber savunma ve veri bütünlüğü, tedarik zinciri yönetimi ve esnek iletişim bunların başında gelmektedir (Barnas, 2016: 28).

3.6. Uygulamada Karşılaşılabilecek Sorunlar

Blokzincir elbette tüm maliyet-etkinlik bağlantılı sorunlara çözüm getiren sihirli bir iksir değildir. Organizasyonlar teknolojinin çeşitli alanlarda uygulanabilirliğini ve elverişliliğini kontrol etmelidirler. Gerçekte kriptografik güven modelleri yeni ve beklenmeyen riskler içerebilirler. Bu yüzden organizasyonlar risk yönetimi ve yönetim stratejilerinde gerekli değişiklikleri yapmayı göz önünde bulundurmalıdırlar (Deloitte, 2018: 7).

Halihazırdaki bütün çabalara rağmen blokzincir teknolojisinin kayda değer toplumsal faydalar oluşturmaları için zamana ihtiyaç olduğu birçokları tarafından dile getirilmektedir. Mevcut dijital hizmetlere, süreçlere ve altyapılara nasıl dâhil edileceği sorusu tam olarak çözülmediğinden alan bazen “kullanım alanlarını arayan yenilikçi teknoloji” olarak da isimlendirilmektedir. Burada bilgi ile fiiliyat arasındaki dengesizliğe dikkat çekilmektedir. Son zamanlarda dillere pelesenk olmuş kelimenin yüzeysel veya anlamsız olarak kullanımı daha fazla kafa karışıklığına yol açacaktır. Teknolojinin otomatik olarak ekosistemi dönüştüreceğine inanma eğilimi, altında yatan gerçek potansiyelin ortaya çıkmasına engel olacaktır (Shen ve Pena-Mora, 2018: 3).

Blokzincirdeki eski veriler silinememekte ya da (mutabakat olmadan) değiştirilememektedir. Dolayısıyla kullanıcıların kendileriyle alakalı kişisel bilgilerin silinmesi talebi, Avrupa Birliğinin de üzerinde durduğu unutulma hakkı kapsamında önemli bir sorun olarak ortaya çıkabilir (McKenzie ve Taylor: 2017).

2016 yılında Norveç Vergi İdaresi blokzincir teknolojisini daha iyi anlayabilmek ve potansiyelini keşfedebilmek için küçük bir blokzincir projesi yürütmüştür. Projede kapalı blokzincir kullanılmıştır. Projenin amacı dokümanları muhafaza etmek ve değiştirilemez hale getirmek için blokzincir teknolojisini kullanılmasıdır. Bu zamana kadar Vergi İdaresinin, dokümanların özgünlüğünü garanti edecek ve değiştirilmediklerini kanıtlayacak bir sistemi olmamıştır. Sistem beklenen sonuçları vermiştir. Fakat dokümanların değiştirilemezliğinin, gizlilik ve unutulma hakkı kapsamında sorun yaratabileceği sonucuna ulaşılmıştır.

Yine Norveç Çalışma ve Sosyal Yardım İdaresinin blokzincir teknolojisi ile ilgili yaptığı denemelerde ulaştığı sonuçlara göre blokzincir teknolojisi, tarafların birbirine güvenmediği işlem kaydı ihtiyacı olduğunda kullanıma uygundur. Fakat şimdilik erişim

kontrolü olan ve değiştirilemez olay akışı gerektiren sistemler için daha basit çözümler bulunmaktadır (Ølnes ve Jansen, 2018: 6).

Kripto paraların alım satım platformları çoğaldıkça yatırımcılar kripto paralara daha çok para yatırmaya başlamıştır. Hatta bazı firmalar kripto paralarla ödemeleri kabul etmeye başlamış ve bazı ülkelerde de yasal düzenlemeler yapılmaya başlanmıştır. Ancak kripto paraların vergilendirilmesi ve muhasebeleştirilmesi konusunda henüz standartlar oturmamıştır (TÜSİAD, 2018: 25).

Nesnelerin interneti destekli bir blokzincir sisteminin yeteneklerini genişletmek için, sözleşme yönetimini otomatikleştirerek verimlilik sağlayabilen akıllı sözleşmeler kullanmak gerekir. Ancak IoT ekosisteminde blokzincirin benimsenmesini engelleyebilecek bazı güvenlik riskleri mevcuttur. Merkezi olmayan halka açık blokzincir ağlarını hacklemek zor olsa da, bunları çalıştırmak için kullanılan akıllı sözleşmeler sorunlu olabilir. Bunun en kötü yanı, siber bilgisayar korsanlarının yaygın akıllı sözleşme güvenlik açıklarını aramasıdır. Bu sorundan kurtulmak için akıllı sözleşmeleri kapsamlı bir şekilde incelemek ve test etmek gerekmektedir (Kamal, 2022).

Blokzincir ile çalışırken en büyük bir risk başlangıçta gelmektedir. Başlangıçta yanlış platformu seçmek sonradan geri dönülmesi zor sonuçlara neden olabilir, maliyet aşımalarına ve gecikmelere neden olarak yatırım getirisini azaltabilir.

Sınırlı katılım önemli bir sorundur. Blokzincirin potansiyelini tam olarak gerçekleştirmek ve uygun maliyetli tutmak için birçok kuruluşun katılması gerekmektedir. Şu anda, blokzincir teknolojisi adımlama aşamasındadır ve sadece kuruluşların yalnızca küçük bir yüzdesi tarafından kullanılmaktadır. Bu organizasyonların birçoğu, güvenlik süreçlerine ve veri bütünlüğü mekanizmalarına aşına olmadığı için teknolojiye henüz tam olarak güvenmemektedir.

Teknik deneyim eksikliği de çözülmesi gereken başka bir sorundur. Blokzincir teknolojisini geliştiren yetkin personel sayısı zaten kısıtlı olmakla birlikte bu teknolojiyi kullanacak personelin de eğitilmesi gerekmektedir. Teknolojinin oldukça hızlı bir şekilde değişmesine rağmen, özellikle kamu sektöründe teknik deneyim aynı hızda artmamaktadır.

Blockchain'in farklı uygulamalarını ve bunların yeteneklerini kavramak, gizlilik ve güvenlik düzenlemeleri ve standartları söz konusu olduğunda karar vericiler için

zorluklar yaratmaktadır. Bu tür sorunları ele almak için, politika yapıcılar teknolojiyi değerlendirmek, geliştirilecek standartları aramak ve teknolojiyle ilgili deneyim toplamak için zaman ayırmalıdır. Blokzincirlerin farklı alanlarda kullanılması için standartların tartışılması ve oluşturulması için akademik ve endüstriyel çabalar sarf edilmelidir.



DÖRDÜNCÜ BÖLÜM

4. DÜNYADA VE TÜRKİYE’DE BLOKZİNCİR UYGULAMALARI

Bu bölümde öncelikle blokzincir teknolojisinin dünyada öne çıkan örneklerine yer verilmektedir. Daha sonra teknolojinin Türkiye’deki uygulamalarına değinilmektedir.

4.1. Dünyada Blokzincir Uygulamaları

Kökleri 1990’lı yıllara kadar uzanan Blokzincir teknolojisinin değeri, Bitcoin ortaya çıkana kadar anlaşılamamıştır. Bitcoin uygulamasının bir kripto para çözümü olmasından dolayı Blokzincir kavramı öncelikli olarak finansal teknolojiler alanında yorumlanıp değerlendirilmişse de gerçek durum bundan biraz farklı olarak gelişmiştir.

Blokzincir yoğun olarak finansal çözümler için kullanılabilir. Fakat bunun ötesinde pek çok farklı uygulama alanına da sahiptir. Japonya, Şubat 2018’de kripto paralarından elde edilen kazançları vergilendireceğini açıklamıştır. Dubai kripto para firmalarına lisans alma zorunluluğu getirmiş, aynı zamanda emlak satışlarının Bitcoin ile yapılmasına izin vermiştir. ABD’de ise Arizona eyaleti vergi ödemelerinin Bitcoin ile yapılabilmesinin önünü açan regülasyonların tamamlandığı açıklamalarını yapmıştır (Çetiner, 2018: 11).

Kendilerine ‘Dijital 5 Ulusları’ adını veren D5, Birleşik Krallık, Güney Kore, Estonya, İsrail ve Yeni Zelanda’nın kurucusu olduğu, iş birlikçi bir ağıdır. Dijital bir hükümetin vatandaşlarına en fazla faydayı nasıl sağlayacağını tespit ederek, ortak müşterek çözümünde iş birliği yapmanın, D5’in en büyük hedefi olduğu ifade edilmektedir. 2018 yılı sonrasında D5’e Kanada, Meksika, Uruguay ve Portekiz hükümetleri de dâhil olmuş ve ağın adı Dijital 9 olarak güncellenmiştir (Özaltın ve Ersoy, 2020: 753).

Aşağıda Birleşmiş Milletler, Amerika Birleşik Devletleri, D5 ülkelerinden Birleşik Krallık, Estonya, Güney Kore ile Avrupa Birliği’nden ülkelere örnekler sunulmuştur. Almanya, Fransa vb. ülkeler Avrupa Birliği başlığı altında incelenmektedir. Bu ülkelerin birçoğu Endüstri 4.0’a geçişte de öncü olan ülkelerdir.

4.1.1. Birleşmiş Milletler

Birleşmiş Milletler (BM), blokzincir teknolojisine giderek artan bir ilgi göstermekte ve teknolojinin çeşitli küresel zorlukları aşma ve sürdürülebilir kalkınma hedeflerine ulaşmaya katkıda bulunma potansiyelini kabul etmektedir. Kurum, blokzincirin; insani yardım, tedarik zinciri yönetimi, dijital kimlik, finansal katılım, çevresel sürdürülebilirlik ve küresel iş birliği gibi alanlarda getireceği potansiyel katkıları ele alarak blokzincir teknolojisinden yararlanan proje ve girişimleri desteklemektedir.

Bu noktada Birleşmiş Milletler, alt kuruluşu olan Dünya Gıda Programı (WFP), vasıtasıyla insani yardım sağlamak için Ethereum blokzincirini kullanan bir platform olan Building Blocks'u oluşturmuştur. Yapı Taşları anlamına gelen “Building Blocks”, Dünya Gıda Programı'nın (WFP), özellikle mültecilere ve savunmasız topluluklara nakit transferi sağlanması bağlamında insani yardımın verimliliğini, şeffaflığını ve koordinasyonunu geliştirmek için blokzincir teknolojisinden yararlanan önemli bir girişimdir. Proje, insanların gıda, beslenme, eğitim, sağlık ve daha fazlası dâhil olmak üzere temel ev ihtiyaçlarına dayalı yardımlara güvenli bir şekilde erişmelerine olanak tanıyarak, insanları yardımın merkezinde önceliklendirmeyi amaçlamaktadır (World Food Programme, 2021). Gizlilik ve güvenlik korunurken, tek bir işlemde birden fazla insani yardım kuruluşundan yardım alma süreci kolaylaşmaktadır.

Building Blocks, Pakistan'da 100 katılımcıyla pilot proje olarak başlamış ve WFP İnovasyon Hızlandırıcısından destek almıştır. O zamandan bu yana önemli ölçüde ölçeklenmiş ve Bangladeş ve Ürdün'deki 1 milyon mülteciye 325 milyon dolar değerinde nakit transferi sağlamıştır. Bu da onu insani yardım alanında dünyanın en büyük blokzincir teknolojisi uygulaması haline getirmiştir. Proje ile Ürdün'deki Suriyeli mültecilere gıda yardımında bulunulmuş ve WFP'nin işlem ücretlerinde 2.4 milyon ABD doları tasarruf sağlanmıştır. Bangladeş'te 870.000 Rohingya mülteciye hizmet verilmekte ve e-kupon satış noktaları aracılığıyla yardımların ulaştırılması devam etmektedir. Lübnan'da ise 56 milyon dolarlık yardımın dağıtımını koordine edilirken, Ukrayna'da da 337 milyon dolarlık nakit transferinin koordinasyonu sağlanmış ve 35 milyon dolarlık yardımın kontrol dışı çakışması önlenmiştir (World Food Programme, 2021).

Building Blocks, katılımcı kuruluşlar tarafından bağımsız olarak işletilen bir blokzincir düğümleri ağıdır. Bu düğümler, iş birliğini, gerçek zamanlı işlemleri ve güvenli bilgi paylaşımını kolaylaştıran bir blokzincir ağı oluşturmuştur. WFP, çeşitli yardım türlerini izlemek, koordine etmek ve sunmak için bu ağ üzerinde bir uygulama geliştirmiştir. Teknik altyapı açık kaynaklıdır ve katılımcı kuruluşların serbestçe erişebileceği bir yapıya sahiptir. Kuruluşların iş birliği yapması ve bilgi paylaşması için tarafsız bir alan sağlayarak yardım çabalarının etkin ve şeffaf bir şekilde koordine edilmesini temin etmekte, kaynakların tekrarını azaltmakta ve ihtiyaç sahibi bireylere hedefe yönelik destek sağlamaktadır (World Food Programme, 2021).

WFP, iş birliğini geliştirmek, parçalanmayı azaltmak ve insani yardımın genel etkinliğini artırmak için diğer Birleşmiş Milletler kuruluşlarını ve insani yardım aktörlerini bu tarafsız blokzincir ağı üzerinde iş birliği yapmaya davet etmektedir. Genel olarak Building Blocks, kurumsal bir WFP projesidir ve insani yardım dağıtımını iyileştirme ve yardımın ihtiyacı olanlara en verimli ve güvenli şekilde ulaşmasını sağlama konusunda blokzincir teknolojisinin potansiyelini ortaya koymuş en yenilikçi projelerden bir olagelmıştır.

4.1.2. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri, federal düzeyde halen blokzincir ve diğer DLT'lerin kullanımını kapsamlı bir şekilde ele alan herhangi bir yasa veya düzenlemeden yoksundur. Bununla birlikte, federal kurumlar, tedarik zinciri yönetimi, dijital kimlik ve cihaz kimlik doğrulaması, gümrük uyumluluğu ve malların menşei gibi alanlarda blokzincir teknolojisini ve bunun fırsatlarını ve risklerini aktif olarak araştırmaktadır. Bu kurumlar, mevcut hükümet faaliyetlerini iyileştirip iyileştiremeyeceğini ve yeni düzenlemelerin uygulanmasının mı yoksa mevcut düzenlemelerin değiştirilmesinin mi gerektiğini belirlemek için bu yeni teknolojiyi değerlendirmektedir.

Devlet çapında maliyeti en aza indiren politikalar ve diğer yönetim görevleri geliştiren kurum olan Genel Hizmetler İdaresi (GSA), Gelişen Vatandaş Teknoloji Ofisi'ni (ECTO) kurmuştur. ECTO, gelişen teknolojiler ile BT modernizasyon girişimlerini değerlendirir, test eder ve uygular. ECTO şu an da kurumların blokzincirle ilgili deneyimlerine ve teknolojinin federal kamu sektörü içinde daha iyi anlaşılabilmesi yollar konusunda danışmanlık yapmaktadır. Temmuz 2017'deki başarılı bir forumun

ardından ECTO, federal kamu hizmetindeki potansiyel kullanım örneklerini toplamıştır ve blokzincir teknolojisi konusunda hükümet çapında bir uygulama topluluğunun başlatılmasını teşvik etmiştir. Ayrıca, kamu görevlilerine ve genel olarak vatandaşlara yeni, pratik ve kolay erişilebilir yollarla blokzinciri tanıtmak için ilgili paydaşlarla birlikte aktif olarak çalışmaktadır (GovChain, 2021).

ABD Menkul Kıymetler ve Borsa Komisyonu (SEC), kripto varlıklara karşı görünüşte olumsuz bir yaklaşım benimsemiş olsa da, Ekim 2018’de bir Stratejik İnovasyon ve Finansal Teknoloji Merkezi (FinHub) uygulaması başlatmıştır. FinHub, dağıtık defter teknolojisi (dijital varlıklar dâhil), otomatik yatırım tavsiyesi, dijital pazar finansmanı ve yapay zeka/makine öğrenimi gibi SEC’in FinTech ile ilgili sorunları ve girişimleri hakkında halkın katılımı için bir kaynak görevi görmesi amaçlanmıştır (GovChain, 2021).

ABD hükümeti her yıl bir trilyon doların üzerinde federal hibe sağlamaktadır; bu, çok sayıda hibe programı ve alıcıyı içeren karmaşık bir süreçtir. Hazine Bakanlığı Mali Hizmet Bürosu, hibe ödemelerini tokenize etmek ve fon kullanımına ilişkin gerçek zamanlı bilgiler sağlamak için blokzincir teknolojisini kullanmayı planlamaktadır. Bu yaklaşım şeffaflığı artırmayı, gereksiz veri girişini azaltmayı ve raporlama yükünü hafifletmeyi amaçlamaktadır. Blokzincir, aynı zamanda hibe edilen yardımların federal hükümetten alt alıcılara olan yolculuğunu da takip ederek görünürlük ve verimlilik sunabilmektedir. Akıllı sözleşmeler; hibe verme, performans doğrulama ve ödeme süreçlerini otomatikleştirerek hibe yönetimini daha da kolaylaştırmak için önerilmektedir. Bununla birlikte, blokzincirin hibe yönetiminde uygulanması, federal hibelerin nasıl yönetileceği, izleneceği ve raporlanacağı konusunda potansiyel bir dönüşümü temsil eden ve hibe ekosistemi genelinde şeffaflığın ve verimliliğin artmasını vaat eden organizasyonel düzenlemeler, mevzuat değişiklikleri ve ödeme ayrıntılarının uyumu konusunda mutabakat gerektirmektedir (REI, 2022).

4.1.3. Avrupa Birliği

Avrupa’nın blokzincir teknolojisine olan ilgisi uzun süredir devam etmektedir. Bu anlamda Avrupa Birliği bünyesinde blokzincir teknolojisi alanında hem raporlama hem de uygulamaya dönük çalışmalar devam etmektedir. Özellikle AB Blokzincir Gözlemevi

ve Forumu ile Uluslararası Güvenilir Blokzincir Uygulamaları Birliği'nin (INATBA) kurulmasıyla Avrupa Birliği'nin blokzincir gelişimine verdiği destek artmıştır.

2016 yılında Avrupa Komisyonu bünyesinde, temel amacı blokzincir ve dağıtık kayıt defteri teknolojileri konusunda bilgi toplamak, bilgiyi yaymak, yetenek kazanmak ve erişim sağlamak için bir FinTech Görev Ekibi kurulmuştur. 2017'de duyurusu yapılan ihale ile blokzincir ve dağıtık defter teknolojileri konusunda bir Avrupa Uzmanlık Merkezi kurulması için 500 bin avro bütçe ayrılmıştır. Oluşturulan ekip, ayrıca uluslararası standart geliştirme çalışmalarına da dâhil olmaktadır (Tüfekçi ve Karahan, 2019: 170).

Avrupa Blokzincir Hizmetleri Altyapısı (EBSI), 2018 yılında 27 AB üyesi ülke ile Norveç, Lihtenştayn ve AB Komisyonu'nun, Avrupa Blokzincir Ortaklığını (EBP) oluşturmak için güçlerini birleştirmesiyle doğmuştur. EBP'nin vizyonu, bilgileri doğrulamak ve hizmetleri güvenilir kılmak için kamu idareleri, işletmeler, vatandaşlar ve bunların ekosistemleri için sınır ötesi hizmetler oluşturmak üzere blokzincirden yararlanmaktır (EBSI, 2022).

Avrupa Blokzincir Hizmetleri Altyapısı (EBSI), blokzincir tabanlı bir hizmet altyapısı çalıştıran ve birbirine bağlı düğümlerden oluşan eşler arası bir ağdır. Projede Avrupa Blokzincir Ortaklığının (EBP) her üyesi - 27 AB ülkesi, Norveç, Lihtenştayn ve Avrupa Komisyonu - en az bir düğüm çalıştıracaktır. Proje, şu katmanlardan oluşmaktadır:

Proje, kamu kuruluşlarının EBSI altyapısına bağlanmasını ve bu altyapı üzerinde çalışabilen uygulamalar geliştirmesine olanak sağlayacaktır. Daha sonra, özel kuruluşlara genişletilmesi planlanmaktadır. Önce özel uygulama alanlarına odaklanması, daha sonra ise bunların geliştirilmesi hedeflenmektedir. EBSI kullanım durumlarının ilk seti şunlardır (EBSI, 2022):

Noter Tasdiki: Güvenilir dijital denetim izleri oluşturmak, zamana duyarlı süreçlerde uygunluk kontrollerini otomatikleştirmek ve veri bütünlüğünü kanıtlamak için blokzincirden faydalanmak;

Diplomalar: Eğitim kimlik bilgilerini yönetirken kontrolü vatandaşlara geri vermek, doğrulama maliyetlerini önemli ölçüde azaltmak ve özgünlük güvenliğini artırmak;

Avrupa Dijital Kimliği: Genel bir dijital kimlik yeteneğinin uygulanması, kullanıcıların merkezi makamlara güvenmeden sınırlar ötesinde kendi kimliklerini oluşturmalarına ve kontrol etmesine olanak tanımak ve eIDAS düzenleyici çerçevesine uyum sağlamak;

Güvenilir Veri Paylaşımı: IOSS KDV kimlik numaralarından başlayarak AB'deki yetkililer arasında verileri güvenli bir şekilde paylaşmak ve gümrük ve vergi makamları arasında tek noktadan alışveriş yapmak için blokzincir teknolojisinden yararlanmak.

4.1.3.1. Almanya

Alman blokzincir ekosistemi, önemli kilometre taşlarından ve değişimlerden oluşan bir yolculuğa tanık olmuştur. 2018'de Almanya'da blokzincir teknolojisi, birkaç temel faktörün etkisiyle patlayıcı bir büyüme yaşamıştır. Yapılan düzenlemeler, Alman Federal Mali Denetleme Otoritesi'nin İlk Dijital Para Arzı (ICO'lar) için yönergeler sunması ve kripto para birimlerini finansal araç olarak sınıflandırması ile önemli bir katalizör olarak ortaya çıkmıştır. Bu düzenleyici çerçeve piyasaya güven aşılayarak hem yatırımcıların korunmasını hem de piyasa şeffaflığını güçlendirmiştir. Ek olarak, Alman hükümetinin blokzincir stratejisi, teknolojinin yenilik ve ekonomik büyüme açısından önemini altını çizmiş ve Almanya'yı blokzincir gelişimi için önemli bir merkez olarak konumlandırmıştır. Bitcoin'in çeşitli işletmeler tarafından bir ödeme yöntemi olarak kabul edilmesi, kripto para biriminin kullanımını ve ana akım tarafından benimsenmesini daha da artırmıştır (Ulbrich, 2023).

Alman Federal Göç ve Mülteciler Dairesi, ülkesinde göç ve iltica prosedürleriyle ilgili bilgi kaynaklarının verimli yönetimini sağlamak için blokzincir tabanlı e-Asylum (e-İltica) projesini başlatmıştır. Projenin temel amacı, sığınmacılara ait verilerin daha etkili bir şekilde iletilmesini sağlamaktır. Proje, blokzincir tabanlı iletişim, referans, kişisel profil ve çapraz kontrol yoluyla ilgili veri ve bilgi alışverişinde bulunan devlet kurumları arasındaki iş birliğini ve etkileşimi artırarak potansiyel olarak süreci hızlandırmaya yardımcı olabilecektir. Birçoğu göç sırasında pasaportlarını veya diğer kimlik belgelerini kaybeden mültecilerin yeni dijital kimlikleri gibi veriler, bu kişilerin özellikle Almanya'daki federal ve yerel kurumlar nezdindeki iltica başvurularının durumunu daha etkin bir şekilde takip etmek için geçici bir çözüm sağlayabilecektir (Fridgen vd., 2019: 1).

4.1.3.2. Danimarka

Danimarka Vergi İdaresi (SKAT), bir aracın alım satım, sigorta, mülkiyet değişimi gibi kayıtları ve harçları içeren süreçlerde yaşanan sorunları çözmek için blokzincir altyapısı kullanılarak Vehicle Wallet (Araç Cüzdanı) projesini hayata geçirmiştir.

Bir alım satım ve takas işleminde SKAT'ın mal sahibini tanınması ve ilgili vergileri tahsil edebilmesi için tarafların resmî bir yeniden kayıt formu doldurmaları gerekmektedir. Ayrıca taraflarında işlem yaparken birbirlerine güven duyması gerekmektedir.

Bu soruna Araç Cüzdanı uygulaması ile blokzincir tabanlı bir çözüm getirilmiştir. Araçla ilgili tüm veriler tek bir dağıtılmış deftere kaydedilmekte ve tedarik zinciri boyunca aktarılırken araç geçmişinin üzerinde anlaşmaya varılan ve paylaşılan bir kaydı oluşturulmaktadır. Bu, araçla ilgili sunulan bilgilerin tamamen doğru olacağı anlamına gelir. Böylelikle siber güvenlik ve dolandırıcılık risklerinin azaltılmasıyla artan verimlilik, iyileştirilmiş dayanıklılık sağlanır. Tüm aşamalarda, araç bilgilerinin güvenliği, bütünlüğü ve geçerliliği, kanıtlanmış kriptografik hizmetler kullanılarak temin edilir (Berryhill vd., 2018: 43).

4.1.3.3. Estonya

Bir İskandinav ülkesi ve Avrupa'da uzun süredir e-devlet reformlarının lideri olan Estonya, dijital ulusötesi kimlik kanıtı ve çevrimiçi oylama da dâhil olmak üzere hükümetle etkileşim için 2.500'den fazla dijital işlem sunan, dünyanın dijital alanda en ilerici ülkelerinden birisidir. Estonya'da vatandaşların yüzde 99'unun, düzenli olarak kullandığı bir dijital kimlik kartı vardır. Ayrıca kamu hizmetlerinin yüzde 99'u çevrimiçi olarak sunulmaktadır (REI, 2022).

2007'deki büyük bir siber saldırının ardından Estonya, verilerin bütünlüğünü sağlamak ve verileri içeriden gelen tehditlere karşı korumak için blokzincir teknolojisini içeren bir siber güvenlik stratejisine odaklanmaya karar vermiştir (e-Estonia, 2022). Blokzincir tabanlı ulusal e-Sağlık projesi, 2016 yılında Estonya e-Sağlık Vakfı'nın blokzincir teknolojisini kullanarak ulusal sağlık veri tabanlarını yönetirken hasta verilerinin siber güvenliğini korumayı amaçlayan pilot uygulamasıyla başlatılmıştır

(Einaste, 2018). Bu proje ile Estonya hükümeti, 1.3 milyon vatandaşının sağlık kayıtlarını güvence altına almak ve belgelemek için blokzincir teknolojisini seçmiştir. Bu teknolojiyi kullanmak, ülkenin verileri birden fazla sağlık hizmeti tedarikçisi arasında kolay ve ekonomik bir şekilde gerçek zamanlı olarak paylaşmasına, verilerin bütünlüğünü korumasına ve kritik sağlık verilerinin saldırıya uğrama riskinin azaltmasına olanak sağlamıştır (REI, 2022).

Proje, özellikle kişisel sağlık bilgilerinin işlenmesiyle ilgili faaliyet günlüğünün kayıtlarını korumayı amaçlamaktadır. Özellikle, projenin ana stratejik hedefi, ülkedeki ulusal düzeyde tıbbi verilerin gizliliğini ve bütünlüğünü sağlamaktır. Proje sonucunda bugün, Estonya e-sağlık ekosisteminin yapısına entegre edilmiş, blokzincir tarafından yönetilen kayıt defteri, sürekli olarak güncellenerek ve denetim için tüm günlükleri tutarak, üçüncü şahıslar tarafından hastanın tıbbi verilerine yapılan her türlü erişimi ve değişiklikleri izleyebilmekte ve kaydedebilmektedir (Kassen, 2021: 3).

4.1.3.4. Fransa

2016 yılından bu yana blokzincir ve kripto para birimlerine desteğini açıkça ifade eden Fransa, Avrupa’da blokzincire öncülük eden ülkelerin başında gelmektedir.

Fransa’nın 2019’un başlarında kimlik belirleme gereksinimleri çağrısı ve dijital varlıklarla ilgili artan düzenlemeler de dâhil olmak üzere son kararları, ülkenin kendisini Almanya, Birleşik Krallık veya İtalya gibi komşu ülkelerden farklılaştırmaya başladığını göstermektedir.

2019 yılının Nisan ayında, dijital varlıklarla ilgili düzenlemeleri tanımlayan PACTE yasasını geçirerek, dijital varlıklarla ilgili düzenlemeleri de uygulayan bir dizi Avrupa ülkesine katılmıştır. Bu adım, Fransa’nın son zamanlarda attığı ve Avrupa blokzincir anlatısında daha merkezi bir role doğru ilerlediğini gösteren bir basamak niteliğindedir. Mayıs 2019’da Fransız Dijital Varlık Derneği’nin (FD2A) kurulması, Temmuz 2019’da Finansal Piyasalar Otoritesi’nin deneysel düzenleyici çerçevesinin duyurulması ve bir G7 kripto para birimi görev gücünün oluşturulması, Fransız hükümetinin güçlü bir ekosistem oluşturmaya yönelik aktif yaklaşımını güçlendirmiştir (Nasdaq, 2019).

Banque de France (Fransa Merkez Bankası), Merkez Bankası Dijital Para Birimi (CBDC) alanındaki deneylerinden elde ettiği veriler doğrultusunda ikinci makalesini yayınlamıştır. Buna göre bankalararası CBDC'ler için; DLT sistemlerinde menkul kıymet takası ve sınır ötesi ödemeler olmak üzere iki temel kullanım durumu tanımlamaktadır. Banka bu kapsamda üç potansiyel CBDC modeli sunmaktadır. Bunlardan ilki, tokenize edilmiş varlıkların kendi defterlerinde kaldığı ve CBDC'nin varlık sahipliği değişikliğiyle eş zamanlı olarak bankalar arasında aktarıldığı mevcut DLT etkileşimlerine benzeyen Birlikte Çalışabilirlik Modelidir. İkinci model olan Entegrasyon, hem tokenize edilmiş menkul kıymetler hem de CBDC'ler için Eurosystem tarafından işletilen ortak bir ağ öngörmektedir. Üçüncü model olan Dağıtım, paylaşılan ve bağımsız ağları birleştirerek farklı CBDC ağlarının ve finansal piyasa DLT'lerinin entegre olmasına olanak tanımaktadır. Banque de France, BIS ve IMF'nin birleşik sistemlere yönelik son önerilerini tekrarlayarak, birlikte çalışabilirlik ve standardizasyonun hayati önem taşıdığını vurgulamaktadır. Banka, bu modellerin birbirini dışlamaması gerektiğini ve yaklaşımlarının, Avrupa'nın tüm CBDC'leri ve DLT'leri, başka bir deyişle blokzincir sistemleri ile entegrasyonunu keşfetmeye yönelik devam eden çabalarıyla uyumlu olduğunu savunmaktadır (Banque De France, 2023).

4.1.3.5. İsveç

İsveç Tapu Dairesi, vatandaşlara daha verimli, daha hızlı ve özelleştirilmiş hizmetler sunabilmek için blokzincir teknolojisini kullanmayı düşünmektedir. Bu maksatla arazi ve mülkiyet işlemlerini kaydetmek için mevcut dijital sistemlerin ötesine geçmeyi amaçlamaktadır. Şu anki merkezi bilgi depolama sistemi şeffaflık ve hesap verebilirlik taleplerine cevap artık verememektedir. Ayrıca, Tapu Dairesi de dâhil olmak üzere İsveç devlet kurumlarının dijital ve teknik sorunlarına çözüm bulunmalıdır.

Blokzincir teknolojisinin "mevcut en ileri teknoloji" olduğu kabulü ile Tapu Dairesi, geleneksel teknik veri tabanı ve web uygulama çözümlerine sahip olmak yerine bir gayrimenkul işlemi sürecini desteklemek, alım satım, finans ve ipotek süreçlerini yönetmek ve mülkiyeti denetlemek için blokzincirin bir alternatif olup olmadığını araştırmak istemektedir.

Proje üç aşamaya ayrılmıştır. İlk aşamada Blokzincir teknolojisinin ne olduğu ve nasıl çalıştığı ve Tapu Dairesi bağlamında neden alakalı olacağına dair teorik bir anlayış

geliştirilmiştir. İkinci aşamada, tapu sahiplerinin ve hükümetin ihtiyaç ve taleplerine en iyi şekilde cevap verecek teknolojiyi geliştirmek amaçlanmıştır. Her iki aşama da başarıyla tamamlanmıştır. Projenin üçüncü aşaması olan gerçek bir arazi transferi henüz gerçekleşmese de proje halen devam etmektedir (McMurren vd., 2018: 2-7).

4.1.4. Birleşik Arap Emirlikleri

Dünya nüfusunun artan kentleşmesi ve büyük şehirlerde hayatı kolaylaştıran yeniliklerin artması, blokzincir teknolojisinin kullanımı da dâhil olmak üzere dünyanın çeşitli yerlerinde akıllı şehir planlama çözümlerinin geliştirilmesini gerektirmektedir. Bu bağlamda Birleşik Arap Emirlikleri, şehir düzeyinde çok çeşitli sorunları çözmek için farklı blokzincir tabanlı çözümlerin uygulanmasında dünya liderlerinden biridir. Örneğin, yakın zamanda Smart Dubai projesi tarafından benimsenen Dubai Blokzincir Stratejisi, bu Orta Doğu ülkesinin sakinleri için rahat, güvenli, şeffaf ve verimli bir kentsel ortam yaratma hedeflerinden biri olarak sunulmuştur. Elektronik belge işleme sistemleri (ör. kâğıtsız hükümet, akıllı sözleşmelerin kullanımı vb.) gibi alanlar, kentsel yönetişimde açık inovasyonu (ör. merkezi olmayan e-hizmetlerin geliştirilmesi, toplu taşıma sistemlerinde bir hizmet olarak mobilite, akıllı hükümet, şehir planlama ve geliştirmede yapay zekanın kullanımı vb.) teşvik etmekte ve e-ticaret (nakitsiz ekonomi, dijital hayırseverlik, yeni başlayanlar için uygun bir iş ortamı, mutlu ve konforlu bir kentsel ortam yaratma vb.), önümüzdeki yıllarda blokzincir tabanlı akıllı şehir çözümleri geliştirme stratejisinin öğelerindendir (Kassen, 2021: 4).

Nisan 2018'de BAE Hükümeti, Emirates Blockchain Stratejisi 2021'i başlatmıştır. Proje ile 2021 yılına kadar devlet kurumlarının yüzde 50'sini blokzincir platformuna dönüştürülmesi hedeflenmektedir. BAE hükümeti, bu teknolojiyi benimseyerek rutin işlemlerde ve belgelerde yılda 11 milyar AED tasarruf etmeyi, 398 milyon basılı belgeyi azaltmayı ve 77 milyon çalışma saati düşürmeyi beklemektedir (GovChain, 2021).

BAE, dijital işlemler için blokzincir kullanacak ve her vatandaşa benzersiz bir kimlik numarası verecektir. Blokzincirdeki bilgi ve veriler hacklenemez ve değiştirilemez olduğu için, ulusal belgelerin ve işlemlerin dijital güvenliğini artırılması, operasyonel maliyeti düşürülmesi ve karar süreçlerinin hızlandırılması hedeflenmektedir (GovChain, 2021).

Etisalat Digital, BAE'nin küçük ve orta ölçekli işletme (KOBİ) sektöründe bankalar arasında veri doğrulama ve iletişim eksikliği nedeniyle hileli fatura finansmanı riskine yanıt olarak Haziran 2019'da UAE Trade Connect'i (UTC) tanıtmıştır. Platform, bu sorunla mücadele etmek için First Abu Dhabi Bank (FAB), Emirates NBD ve diğerleri dâhil olmak üzere sekiz büyük BAE bankasını birleştirmiştir. UTC, katılımcı banka ağındaki mükerrer faturaları tespit etmek için blokzincir teknolojisini kullanarak müşteri verilerinin gizliliğini korurken dolandırıcılık riskini de azaltmıştır. Proje, çeşitli kullanım durumlarında gelecekteki iş birlikleri için temel bir blokzincir ağı oluşturmayı amaçlamaktadır. Uygulama stratejisi; iş özellikleri, BT gereksinimleri ve düzenleyici çerçeveler olmak üzere üç yolu içermektedir. Platformun işleyişi, kurucu üyeler arasındaki ortak girişime ve gelişim yol haritasına birlikte yatırım yapılmasına olanak sağlamaktadır. UTC, blokzincirin yanı sıra, daha karmaşık dolandırıcılık tespitine yönelik yapay zekâ ve makine öğrenimini de bir araya getirmiştir. Proje, BAE'nin mali ortamına fayda sağlayacak şekilde yıllık tahmini 435 milyon ABD Doları tutarındaki dolandırıcılık işlemleriyle mücadele ederek başarısını ortaya koymuştur (World Economic Forum, 2020: 17).

4.1.5. Çin

Çin, blokzincir endüstrisine karışık bir yaklaşım benimsemiştir. Kripto para birimlerinin kullanımına karşı güçlü bir tavır alırken, altta yatan teknolojiyi geliştirmeye büyük ilgi göstermiştir. Bu, blokzincir geliştirmenin kilit bir hedef olduğu 13. Beş Yıllık Planında kendini göstermektedir. Çin hükümeti, blokzincir araştırmalarına milyarlarca yatırım yapmıştır ve diğer tüm ülkelerden daha fazla blokzincir patent başvurusunda bulunmuştur. Hükümetin otoriter ve sansür eğilimlerinin, teknolojinin ademi merkeziyetçi doğasıyla bağdaştırılıp uzlaştırılamayacağını zaman gösterecektir (GovChain, 2021).

Çin'deki blokzincir uygulamalarının çoğu, tedarik zinciri yönetimi, vergi tahsilatı ile gıda ve ilaç güvenliği gibi yerel yönetim düzeyinde gerçekleşmiştir. Çin Chongqing Yuzhong Bölgesi Gıda ve İlaç İdaresi, ürün yaşam döngüsünün daha iyi izlenebilirliği ve sahteciliğe karşı önlemlerle gıda ve ilaç kalite güvencesinin denetimini güçlendirmek için blokzincir teknolojisini test etmektedir. Teknolojiyi geliştiren şirket PrimeNumber Chain

Technology, sistemin hükümetin düzenleyici önlemlerini ve denetim etkinliğini iyileştireceğine inanmaktadır (GovChain, 2021).

Hong Kong merkezli dünyanın en büyük elmas satıcılarından Chow Tai Fook, dijital portföyüne blockchain eklemiştir. Chow Tai Fook, ürünlerinin üstün yönlerinden biri olarak Amerika Gemolojik Enstitüsü (GIA) tarafından onaylanan ve etik elmas tedariki için yönergeler belirleyen Birleşmiş Milletler'in Kimberly Süreci gereksinimlerini karşılayan elmaslar satması olduğunu iddia etmektedir. Sorun şu ki, kalite standartlarını önemsemeyen satıcılar bu standartlara uymayarak elmasları daha düşük fiyatlara satmakta, fakat tüketiciler aradaki farkı anlamakta güçlük çekmektedir.

Bu nedenle Chow Tai Fook, tüm elmaslarının sertifika bilgilerini dijitalleştiren bir blokzincir altyapısı kurmaya karar vermiştir. Kaynağı ve sınıfı da dâhil olmak üzere elmasın en önemli bilgilerinin değişmez bir dijital kaydı, Şirket ve GIA tarafından kaydı tutulan iki taraflı bir blokzincir defterindeki belirli bir girişe atıfta bulunan bir seri numarası ile depolanmaktadır. Daha sonra bu seri numarası elmasın üzerine oyularak işlenmektedir. Müşteriler, pırlantayı bir kuyumcuya getirip seri numarasını ve ilgili kaydı sorgulatıp bu kayda özel bir mobil uygulama aracılığıyla elmasın bilgilerini öğrenebilmektedirler. Şirket bu şekilde müşterilerini koruduğunu ve onlara elmaslarının kalitesinden emin olmalarını garanti ettiğini iddia etmektedir (Deloitte, 2021: 50-51).

Çin ayrıca Gıda Tedarik Zinciri İzlenebilirlik Sisteminde blokzincir teknolojisini uygulamaktadır. Gıda güvenliğinin BM Sürdürülebilir Kalkınma Hedeflerinden biri olması nedeniyle mevcut durumda akademisyenlerin, özel sektörün ve kamu sektörünün ilgisini çekmektedir. Bu nedenle, her sektör, gıda güvenliği izlenebilirliği için inovasyonun yanı sıra, gıdanın üretim sürecinden tüketicinin eline ulaşana kadar güvenliğini takip etmeyi sağlayan IoT (Nesnelerin İnterneti) ve Blokzincir teknolojisinin evrimi için yenilik ve geliştirme çabası içindedir (Center of E-Government, 2021: 10).

Çin'de, hükümetin yargı sistemi ve idari yönetimin çeşitli yönleri için blokzincir teknolojisinden yararlanmaya yönelik kayda değer bir çabası bulunmaktadır. Bu girişim vergilendirme, elektronik faturalama ve özellikle yargı sektörü gibi alanlarda blokzincir uygulamalarının geliştirilmesini de içermektedir. Bu çabaların ön saflarında yer alan Çin Yüksek Mahkemesi, Mayıs 2021'de ülke çapında birleşik bir adli blokzincir platformunun hızlı bir şekilde inşa edilmesini teşvik eden bir direktif yayınlamıştır. Bu platformun

amacı, her düzeydeki mahkemeler ve halkın kendisi için standartlaştırılmış veri depolama ve doğrulama yetenekleri sunmak olarak arz edilmiştir (Wang vd., 2023).

Mahkeme tarafından blokzincirin, internetle ilgili davalarda yaygın olan elektronik delillerin işlenmesinde özellikle değerli olduğu benimsenmiştir. Örneğin Hangzhou İnternet Mahkemesi, 2018'de blokzincirde saklanan elektronik verileri yasal delil olarak kabul ederek bir emsal oluşturmuştur. Ayrıca, sözleşmelerin yürütülmesini otomatikleştirmek ve mahkeme yönetimini geliştirmek için akıllı sözleşmeler kullanılmıştır. Veri paylaşımını kolaylaştırmak ve standartları iyileştirmek için telif hakkı blokzincirinin diğer blokzincirlerle entegrasyonu da araştırılmaktadır. Çin Yüksek Mahkemesi, 2022 yılında blokzincir teknolojisinin yargısal kullanımına yönelik hedefleri özetleyen ve 2025 yılına kadar kapsamlı bir blokzincir ittifakı kurmayı amaçlayan bir görüş yayınlamıştır (Wang vd., 2023).

Temelde blokzincirin; bozmaya karşı korumalı veriler oluşturmak, adli verimliliği artırmak, iş birliğini teşvik etmek ve ekonomik ve sosyal yönetimi desteklemek maksadıyla kullanılması düşünülmektedir. Bu benimseme, şeffaflık ve verimlilik açısından umut verici olmakla birlikte, aynı zamanda gizlilik, güvenlik ve gelişen bu ortamda sağlam düzenleme ve standartlara duyulan ihtiyaç konusundaki endişeleri de artırmaktadır.

4.1.6. İngiltere

Finansal ve teknolojik yenilikler için bir merkez olarak güçlü itibarı sayesinde Birleşik Krallık, kendisini küresel sahnede bir blokzincir cenneti olarak tanımlama potansiyeline sahiptir. Gelişmiş yasal ve düzenleyici sistemiyle birlikte bu itibar, Birleşik Krallık'ın işletmeler ve girişimciler için çekici bir ekosistem yaratmasına yardımcı olma potansiyeline sahiptir.

Birleşik Krallık Hükümeti, kripto para birimlerine yönelik yaklaşımını Mart 2015'te açıklamıştır. Yıllık bütçe açıklamasında Birleşik Krallık Şansölyesi George Osborne, Birleşik Krallık Hükümetinin dijital kripto para birimleri ile ilgili düzenleme yapacağını bildirmiştir. Ayrıca hükümetin sadece Bitcoin gibi dijital kripto para birimlerinin "fırsatları ve zorluklarına" değil aynı zamanda finans dünyasını temelden değiştirmek için blokzincir teknolojisinden' yararlanmanın potansiyel geleceğine de

yatırım yapmayı planladığını duyurmuştur. Bu plan, "yenilikçi ödemeler ve finansal teknolojinin geliştirilmesi için dünya lideri bir ortam yaratma" amaçlı projenin bir parçasıdır (Meijer, 2015).

İngiltere hükümeti bir süredir blokzincir uygulamalarını değerlendirmektedir. Birleşik Krallık Hükümeti Baş Bilimsel Danışmanı Sir Mark Walport tarafından hazırlanan Dağıtık Defter Teknolojisi: Blokzincir'in Ötesinde (Ocak 2016) raporu, ulusal ihtiyaçları karşılamak ve Birleşik Krallık'ın küresel arenada rekabet edebilirliğini sağlamak için blokzincir kullanımına yönelik önerilerde bulunmuştur. Öneriler, bakanlık liderliği sağlamayı, düzenleyici bir çerçeve oluşturmayı ve Birleşik Krallık içinde ve Birleşik Krallık ile diğer ülkeler arasında kamu ve özel sektör arasında yakın bir ortaklık sağlamayı içermektedir (GovChain, 2021).

Birleşik Krallık ayrıca blokzincir teknolojisinin uygulanmasında uluslararası iş birliği yaratmayı ve geliştirmeyi amaçlamaktadır. Bu nedenle, Nisan 2018'de diğer 21 ülke ile Blokzincir Ortaklığına imza atmıştır. Deklarasyon, Blokzincir deneyimini ve uzmanlığını Avrupa çapında paylaşmayı ve bir araya getirmeyi amaçlamaktadır.

Birleşik Krallık Parlamentosu da blokzincire büyük ilgi göstermektedir. Lordlar Karaması tarafından hazırlanan bir rapor, kamu sektöründe DLT'nin daha fazla emniyet ve güvenlik, şeffaflık, izlenebilirlik ve güven sağlayabileceği, maliyeti düşürebileceği ve vatandaş için hizmet kalitesini artırabileceği kilit alanları ortaya koymaktadır. Rapora göre blokzincir; sınır kontrolü, ulusal güvenlik, vergilendirme ve yardım ödemeleri, sağlık güvencesi, gıda standartları ve güvenliği, siber güvenlik ve kamu alımları gibi alanlarda gelişmelere olanak sağlayabilir.

Mart 2018'de Maliye Bakanı tarafından, Hazine, İngiltere Merkez Bankası ve FCA (Finansal Yürütme Otoritesi) görevlilerinden oluşan Kripto Varlıklar Görev Gücü'nün başlatıldığı duyurulmuştur. FCA Birleşik Krallık'ta blokzincir inovasyonunu teşvik etmek için politikalar uygulamaktadır. Kurum ayrıca, farklı kripto varlık türlerinin düzenleyici çevrede nerede bulunabileceğine ilişkin ayrıntıları ortaya koyan bir Danışma Belgesi, CP19/3 (Ocak 2019) yayınlamıştır (GovChain, 2021).

Birleşik Krallık, düzenleyici eylemlerin ötesinde, kamu sektöründeki bir dizi politika alanında da blokzincir teknolojisinin kullanımını araştırmıştır. Çalışma ve

Emeklilik Bakanlığı sosyal güvenlik ödemeleri için blokzincir kullanımını test etmiştir. Tasarlanan sistem ile hak sahipleri, telefonlarında bir uygulama ile yan hak ödemelerini alıp harcayabilmışlerdir. Hak sahiplerinin işlemleri, onların rızasıyla dağıtık kayıt defterine kaydedilmiştir (GovChain, 2021).

Çevre, Gıda ve Köy İşleri Bakanlığı, blokzincir teknolojisinin gıda endüstrisindeki tedarikçiler, işleyiciler ve tüketiciler için veri şeffaflığını ve verimliliğini nasıl iyileştirebileceğini, gıda güvenliğini ve hayvan refahını nasıl iyileştirebileceğini değerlendirmektedir. HMRC (Kraliyet Vergi ve Gümrük Dairesi), kuruluşların faaliyetleri koordine etmesine ve gümrük işlemleri sırasında bilgi paylaşmasına yardımcı olmak için Birleşik Krallık sınırında özel bir izin verilen blokzincirin kullanımına ilişkin testler yürütmüştür. Birleşik Krallık Tapu Müdürlüğü, hız, basitlik ve verilere açık bir yaklaşım açısından dünyanın önde gelen tapu sicili olmayı hedeflemektedir. Bakanlık dışı departman, Dijital Sokak araştırma projesi aracılığıyla Corda platformunu kullanarak bir mülkün dijital transferini sağlayan ve tapu kaydını otomatik olarak güncelleyen bir prototip oluşturmuştur (GovChain, 2021).

4.1.7. Güney Kore

Güney Kore hükümeti dünyada blokzincir teknolojisinin benimsenmesinde ön sıralarda yer almaktadır. Bu kapsamda hükümet; çevrimiçi oylama, sosyal refah yönetimi, posta ve finansal hizmetler ve yenilenebilir enerji işlemleri dâhil olmak üzere kamu hizmetlerinin güvenliğini artırmak için Merkezi Olmayan Kimlik'te (DID) projesinde potansiyel görmektedir (GBBC, 2021: 10).

Mart 2017'de, Güney Kore'nin Gyeonggi-do eyaleti, Ddabok Topluluk Destek Projesi'nde oy kullanmak için bir blokzincir tabanlı e-oylama sistemi kullanmıştır. Dokuz bin bölge sakini, akıllı sözleşmeler içeren ve Kore finansal teknoloji girişimi Block tarafından geliştirilen bir blokzincir platformunu kullanarak oy vermiştir. Oylar, sonuçlar ve diğer ilgili veriler bir blokzincirde saklandı. Bu sürece hiçbir yönetim veya merkezi otorite dâhil olmamıştır. Bu, Güney Kore'nin böyle bir teknolojiyi ilk kez uygulaması olmuştur (Kshetri ve Voas, 2018: 2).

Güney Kore, 30 Ocak 2018 tarihinde getirdiği düzenleme ile, kara para aklama ile mücadele ve vergi düzenlemelerinin uygulanabilirliğini izlemek için, kripto paraların

ancak gerçek kişilere ait hesaplar üzerinden işlem görebileceğini açıklamıştır. Böylelikle, anonim banka hesaplarıyla kripto para alım satımı yasaklanmıştır. Ayrıca kripto para üretenlerin bankalarla anlaşma yapma mecburiyeti de getirilmiştir. Bu anlaşmalar sayesinde kripto para ihraç edenlerin kimlikleri, bankalar tarafından işlem esnasında sorgulanabilmektedir (TBV, 2019: 21).

Savunma Edinme Programı İdaresi (DAPA), blokzincir platformu oluşturma çabalarının, savunma verilerinin izinsiz olarak değiştirilmesine karşı koruma sağlayabileceğini belirterek, 2019 yılında savunma alanındaki ticari operasyonları geliştirmeyi amaçlayan bir blokzincir pilot projesi başlatmıştır. Burada amacın, satın alma sürecinde ilk tekliften son değerlendirmeye kadar bütün kayıtların blokzincir defterinde tutularak savunma satın alma fonksiyonlarının güvenilirliğini arttırmak olduğu belirtilmiştir. Blokzincir tabanlı çözümün, aynı zamanda ateşli silah taşıma izinleri konusunda savunma şirketlerinin üzerindeki yükün azaltılmasına da yardımcı olacağı DAPA tarafından bildirilmiştir (Takyar, 2019).

Aralık 2017'de Kore Gümrük Servisi (KCS), ihracat gümrük işlemleri için blokzinciri test etmek üzere Samsung SDS liderliğindeki Nakliye Lojistiği Blokzincir Konsorsiyumu ile ortaklık kurmuştur. Test, gümrük belgelerinin blokzincir ağında paylaşılmasının, bu belgelerin değişmezliğini sağladığını, güvenliğini ve doğruluğunu artırdığını göstermiştir. Ancak Ekim 2020'de konseptin başarıyla uygulanabildiğinin kanıtlanmasına rağmen bütçe kısıtlamaları ve mevcut bilgi sisteminin blokzincire uyarlanmasındaki zorluklar nedeniyle proje ticarileşme aşamasına geçememiştir (GBBC, 2021: 10).

Güney Kore, aşı sertifikasyonu için de blokzincir kullanımını test etmiştir. KDCA, Nisan 2021'de başlatılan bir elektronik COVID-19 aşı sertifikasyonu uygulaması olan COOV'u tanıtmak için Blockchain Labs ile iş birliği yapmıştır. Uygulama, haziran ayına kadar iki milyon indirmeye ulaşmıştır. COOV, QR kodu oluştururken kişisel verileri ekleme seçeneğini sunmasına rağmen, kullanıcıların kişisel bilgilerini doğrudan açıklamadan aşı geçmişlerini doğrulamalarına olanak tanımıştır. Kullanılan blokzincir altyapısı, halka açık bir blokzincirin çok yönlülüğünü özel bir blokzincirin gizlilik avantajlarıyla birleştirmiştir (GBBC, 2021: 11).

4.1.8. Singapur

Singapur Para Otoritesi (MAS), blokzincirin, ülkedeki endüstriyel ve finansal sorunların başında gelen sınır ötesi para ve devlet menkul kıymeti transfer işlemleri için daha verimli, daha ucuz ve daha hızlı bankalar arası ödeme çözümü amacına hizmet edebileceğini tespit etmiştir. MAS, dijital defter teknolojilerinde uzmanlaşmış bankalar ve düzenleyicilerden oluşan bir konsorsiyum olan R3 ile dijital Singapur doları ile Blockchain tabanlı bir işlem süreci geliştirmek ve uygulamak için ortaklık kurmuştur. Bu, yalnızca merkezi olmayan bir güven sistemi yoluyla müdahaleyi önlemekle kalmayacak, aynı zamanda işlemlerin hiçbir merkezi kontrol gerektirmeden yedi gün yirmi dört saat çalışmasına izin verecektir. Ana yararlanıcılar olan bir dizi farklı bankayı teknolojinin ilk geliştirme ve denemelerine katılmaya davet etmiştir.

Prototip, akıllı sözleşmelerden en iyi şekilde yararlanmak için Ethereum platformunu kullanmıştır. Ayrıca, fonların ve Singapur Devlet Menkul Kıymetlerinin gerçek zamanlı ve geri alınamaz bir şekilde transfer edilmesini sağlayan, Singapur tarafından işletilen bir sistem olan MAS MEPS+’dan tam olarak yararlanmıştır. Böylece Project Ubin, dijital işlem mekanizmaları (MEPS+) açısından zaten var olanı kullanmış ve işlemlerin hem zaman hem de maliyet açısından daha yüksek güvenlik ve verimliliği için bir “blokzincir katmanı” eklemiştir.

Aralık 2016’daki 1. Aşamanın sonunda, Project Ubin, özel bir Ethereum ağında çalışan bir bankalararası transfer prototipinin başarıyla oluşturulduğunu ve bir Akıllı Sözleşme kod tabanının geliştirildiğini göstermiştir. Daha da önemlisi, yeni bir teknoloji olan blokzincir ile dijital işlemler üzerindeki mevcut teknolojileri tamamen entegre etmeyi başarmıştır (Berryhill vd., 2018).

MAS, Project Ubin üzerindeki çalışmaya devam etmek için 3 Kasım 2022’deki basın bülteninde uluslararası ortaklarla iş birlikleri yoluyla toptan CBDC’lerle sınır ötesi bağlantıyı ilerletmek için Ubin+’yı duyurmuştur (Monetary Authority of Singapore, 2022).

4.2. Türkiye’de Blokzincir Uygulamaları

Bu bölümde Türkiye’de blokzincir teknolojisinin gelişimi ve mevcut uygulamaları ele alınmaktadır.

4.2.1. Türkiye’de Blokzincirin Gelişimi

Türkiye’de blokzincir teknolojisi, daha çok kripto paralar alanında olsa da, diğer ülkeler ile karşılaştırıldığında oldukça hızlı bir büyüme yaşamıştır. Gate.io’nun 28 Ekim 2022’de yayınladığı Kripto Piyasası ve Yatırım Raporu Türkiye 2022’ye göre blokzincir pazarı 2022-2023 yıllarında muazzam büyümesini sürdürmüştür. Rapora göre Türkiye’de 3.811.882 kripto varlık kullanıcısı bulunmakta ve bu da toplam nüfusun %4,5’ine denk gelmektedir (Gate.io, 2022). Cumhurbaşkanlığı Finans Ofisi koordinasyonunda hazırlanan 2022 Türkiye Fintech Ekosistemi Durum Raporu’nda, Türkiye’de 250 ödeme teknolojisi, 92 blokzincir ve kripto varlık, 89 bankacılık teknolojisi girişi olduğu belirtilmektedir (T.C. Cumhurbaşkanlığı Finans Ofisi, 2023: 14).

Blokzincir teknolojisinin ilk uygulama örneği olan Bitcoin’in hukuki statüsü BDDK (2013) tarafından ilk olarak 25 Kasım 2013 tarih ve 2013/32 sayılı basın duyurusunda açıklanmıştır. Buna göre Bitcoin’in herhangi bir resmî ya da özel kuruluş tarafından ihraç edilmediği ve karşılığı için güvence verilmediğine atıfta bulunularak, mevcut yapısı ve işleyişi itibarıyla 6493 Sayılı Kanun kapsamında elektronik para olarak değerlendirilmediği bildirilmiştir. Duyuruda, Türkiye’de ödeme hizmetleri, menkul kıymet mutabakat sistemleri ve elektronik para kuruluşları gibi finansal faaliyetleri düzenleyen 6493 Sayılı Kanun çerçevesinde gözetim ve denetiminin mümkün görülmediği aktarılmıştır.

Türkiye’de hizmete başlayan ilk kripto para borsası, 2013 yılında Kuzey Kıbrıs Türk Cumhuriyeti (KKTC)’nde faaliyete geçen BTCTurk isimli platformdur (BTCTurk, 2022). Platform, Türkiye’de Bitcoin alım satımı yapan ve kripto para borsası olarak işlem yapan ilk aracı kurumdur. Türkiye’de Bitcoin ve kripto paralara yönelik bir düzenleme olmadığından, şirket o dönemde kuruluşunu KKTC merkezli yapmıştır (Çetiner, 2018). Halihazırda BTCTurk uygulamaları üzerinden Türk Lirası karşılığı bitcoin ve diğer kripto paralar alınıp satılabilmektedir.

Kripto paraların vergilendirilmesi ve muhasebeleştirilmesi hakkında henüz kesin bir düzenleme olmamakla birlikte mevcut yapıya yönelik bazı açıklamalarda bulunulmuştur.

Mali Suçları Araştırma Kurulu Başkanlığı (MASAK) tarafından “*Müşteri hesaplarından Bitcoin satan aracı kuruluşlara Bitcoin alımına yönelik para transferi yapılması*”

ibaresi şüpheli işlem kategorisi altında değerlendirildiğini belirtmiştir. Bu doğrultuda, aracı kuruluşlardan kripto para alınması halinde, yapılan işlemlerin MASAK'a bilgisinin verilmesi mecburiyeti getirilmiştir. SPK'nın basın duyurusunda ise kripto varlıkların satışı vasıtasıyla fon toplamının Kurulun gözetim ve denetleme alanı dışarısında kaldığından ve bu varlıkların değerlerinde aşırı dalgalanmalar görüldüğünden ötürü riskli oldukları belirtilmiştir. Değer artışı veya kripto para madenciliği gibi kripto paralardan elde edilen kazançlarla Gelir Vergisi Kanunu'nda yer alan kazançların eşleştirilmesindeki güçlükler ve Katma Değer Vergisi bağlamında kripto paraların henüz bir para birimi olarak değerlendirilmemesi ve para ile alım satım işlemi olarak nitelendirilmemeleri, bu konunun vergisel boyutunun halen tanımlanamamasına neden olmaktadır (TÜSİAD, 2018: 25).

Akbank, uluslararası para transferinde blokzincir teknolojisinden yararlanmak için Ripple ile anlaşarak bu alanda ilk adımı atan Türk bankası olmuştur. Haziran 2017'de gerçekleşen anlaşma sonucunda Akbank, Ripple ile iş ortaklığına girmiştir. Ripple ile Akbank'ın Almanya'daki faaliyetlerini sürdüren alt şirketi olan Akbank AG'nin ödemeleri kapsayan bir pilot çalışma başlattığı duyurulmuştur (COINTRAL, 2019). Şirket, bu doğrultuda Aralık 2018'de İngiliz Bankası Santander UK'e Ripple üzerinden blokzincir altyapısı ile GBP para transferlerine başladığını açıklamıştır (Akbank LAB, 2018).

Türkiye'de blokzincir altyapısını kullanarak hayata geçirilen ilk finansal proje, Borsa İstanbul Bilişim Teknolojileri Ekibi tarafından başlatılmıştır. Proje kapsamında Merkezi Kayıt İstanbul, Takas İstanbul ve Borsa İstanbul'daki elektronik başvurulara ait müşteri veri tabanlarında bulunan bilgilerin birlikte çalışabilir hale getirildiği basın duyurusuyla açıklanmıştır. Müşterini Tanı (KYC) anlayışı ile temellendirilen projede, yeni müşterilere ait bilgilerin belirtilen veri tabanlarına eklenmesi, mevcut bilgilerin değiştirilmesi ve belge yönetimi blokzincir ağı üzerinden gerçekleştirilecektir. Böylece veri tabanlarına bilgi girerken gerçekleştirilecek hataların önüne geçilerek güvenilir, şeffaf ve hızlı bir platformun oluşması sağlanmıştır (Borsa İstanbul, 2018).

TCMB (2021) tarafından 16 Nisan 2021 tarihinde yapılan basın duyurusunda; kripto varlıkların, (henüz) herhangi bir denetleme veya düzenleme mekanizmasının olmaması, merkezi bir muhatabın bulunmayışı, piyasa değerlerinin aşırı oynaklık

gösterebilmesi, anonim yapıları itibariyle yasadışı faaliyetlerde kullanılabilmesi, kripto cüzdanların çalınabilmesi veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi ile işlemlerin geri dönülemez nitelikte olması gibi nedenlerle ilgili taraflar açısından önemli riskler barındırdığına dikkat çekilmiştir. Duyuruda, son dönemde söz konusu varlıkların ödemeler alanında kullanılmasına ilişkin çeşitli girişimlerin oluşmaya başladığının gözlemlendiği belirtilmiş ve bu varlıkların ödemelerde kullanılmasının, bahsedilen sebeplerle işlemlerin tarafları açısından telafisi mümkün olmayan mağduriyetler yaratma ihtimaline sebep olabileceğinden bahsedilerek, bu varlıkların mevcutta kullanılan yöntem ve araçlara karşı güven zafiyeti meydana getirebilecek unsurlar içerdiğinin değerlendirildiği aktarılmıştır. Aynı gün yayınlanan “Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik” ile;

- Kripto varlıkların ödemelerde doğrudan veya dolaylı olarak kullanılması ve buna yönelik hizmet sunulması,
- Ödeme hizmeti sağlayıcılarının, ödeme hizmeti sunumunda ve elektronik para ihracında kripto varlıkların doğrudan veya dolaylı olarak kullanıldığı bir iş modeli geliştirmesi ya da bu tür geliştirilen iş modellerine hizmet sunması ve,
- Ödeme ve elektronik para kuruluşlarının, kripto varlıklara dair alım ve satım, saklama, transfer veya ihraç hizmeti sunan platformlara veya bu platformlardan yapılacak fon aktarımlarına aracılık etmesi yasaklanmıştır.

MASAK tarafından 2021 yılı mayıs ayında “Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar” konulu bir kılavuz yayınlanmıştır. Bu kılavuzda suç gelirlerinin aklanması ve terörizmin finansmanı suçları açıklanarak kripto varlık hizmet sağlayıcılarının yükümlülüklerine yer verilmiştir. Bu yükümlülükler arasında müşterinin tanınması, şüpheli işlem bildirimi, bilgi ve belge verme, muhafaza ve ibraz ve devamlı bilgi verme yükümlülükleri sıralanmıştır (MASAK, 2021).

Türkiye’de kadınların da blokzincir teknolojisinde kendilerine yer bulabilmesi için Ebru Güven ve Başak Burcu Yiğit tarafından “Blokzincir Women” adında bir dernek kurulmuştur. Dernek, amacını *“kadınlara teknoloji ve blokzincir özelinde pozitif ayrımcılık sağlayacak sosyal sorumluluk projeleri üretmek ve bu projeler sayesinde bilişim sektöründe kadın istihdamını artırarak, kadınların üretim ekonomisinde daha çok*

yer almasını sağlamaktır.” şeklinde belirtmektedir. Bu kapsamda dernek, blokzincir ile ilgilenen kadınlara eğitim vermekte; özel sektör kuruluşları, STÖ’ler ve üniversitelerin desteği ve iş birliği ile blokzincir ekosistemde bulunan kadın sayısının düşüklüğüne dikkat çekmek ve toplumda bu konuda farkındalık yaratmak için çalışmalarda bulunmaktadır (ISTBCW, 2022).

2019-2023 yılları için hazırlanan 11’inci Kalkınma Planı’nın “Mali Piyasalar” başlığı altında 249.5’inci maddede *“Blokzincir tabanlı dijital merkez bankası parası uygulamaya konulması”*; “Lojistik ve Ulaştırma” başlığı altında 508.3’üncü maddede *“Blokzincir uygulamalarının yaygınlaştırılmasını teminen ulaştırma ve gümrük hizmetlerinde gerekli hukuki ve fiziki altyapı çalışmaları tamamlanması”* ve “Kamu Hizmetlerinde e-Devlet Uygulamaları” başlığı altında 809.2’nci maddede *“Kamu hizmetlerinin iyileştirilmesinde büyük veri, bulut bilişim, mobil platformlar, nesnelerin interneti, yapay zekâ, blokzincir gibi yeni teknolojilerden faydalanılabilmesi için süreç ve teknolojik altyapı iyileştirmeleri yapılması”* hedeflerine yer verilmiştir (SBB, 2019).

Sanayi ve Teknoloji Bakanlığı’nın 2023 yılı için hazırlanan Sanayi ve Teknoloji Stratejisi’nde “Ulusal Blokzincir Başlığı” altında, blokzincir teknolojisinin Türkiye’de geliştirilmesi, kamu sektöründe ve özel sektörde kullanılması ve yenilikçi iş modellerinin teşvik edilmesi amacıyla dört hedef belirlenmiştir. Bunlar (2019);

1. Ulusal Blokzincir Altyapısının Geliştirilmesi: Blokzincir teknolojisinin geliştirilmesi ve bu teknolojiyi temel alan ulusal bir ağın oluşturulmasının teşvik edilmesi.
2. Kamu Merkezli Uygulamaların Blokzincir Altyapısına Taşınması: Kamu merkezli uygulamalardan (örneğin tapu kayıtları, diploma sertifikaları, gümrük işlemleri vb.) blokzincir altyapısına taşınabilir olanların tespit edilerek "Açık Kaynak Platformu" inisiyatifi altında projelendirilmesi.
3. Pilot Uygulamalar ve Test Ortamı Oluşturulması: Yeni, güvenli iş modelleri ve süreçlerin (tedarik zinciri yönetimi, bankacılık, hukuki takip uygulamaları vb.) blokzincir altyapısında test edilmesi için kurgu ve uygulama modelleri üzerinden pilot uygulamaların yapılması ve test ortamının oluşturulması.
4. Mevzuata Uyumluluk Testleri ve Sertifikasyon: Geliştirilen blokzincir uygulamalarının mevzuata uyumluluk testlerinin yapılması için "sanal mevzuat test alanı"nın (regulatory sandbox) oluşturulması. Bu alan,

girişimlerin mevzuata uygunluklarını test etmelerine olanak sağlar ve başarılı olan girişimlere sertifikasyon verilerek yatırım almaları desteklenir.

4.2.2. TÜBİTAK Blokzincir Araştırma Laboratuvarı

TÜBİTAK Blokzincir Araştırma Laboratuvarı (BZLab), kamunun ve özel kurumların/kuruluşların ihtiyaçları göz önünde bulundurularak, blokzincir teknolojisinin kurulumunu, altyapısını, gizlilik ve güvenlik analizini, iş modellerini, kitle fonlaması yaklaşımlarını araştırmak ve muhtelif teknik detaylar üzerinde Ar-Ge faaliyetleri yapmak amacıyla, kamudaki ilk blokzincir laboratuvarı olarak, 2017 yılında BİLGEM UEKAE Matematiksel ve Hesaplamalı Bilimler Biriminin bünyesinde kurulmuştur. Fiziksel olarak TÜBİTAK Gebze Yerleşkesi içindedir.

BİLGEM, kamu ve özel kurum/kuruluşlar ve akademisyenlerle iş birliği yaparak güvenli merkeziyetsiz yapıların oluşturulması için blokzincir tabanlı çözümler sunmaktadır. Bu kapsamda, finans, dijital kimlik, dijital para, tedarik zincirleri, akıllı şehirler, nesnelerin interneti (IoT), eğitim ve sağlık hizmetleri gibi, bu teknolojinin uygulama alanlarında çözümler geliştirmek üzere çalışmaktadır.

Kurum, görevleri olarak şunları sıralamıştır (BZLab, 2022):

- Blokzincir ve kripto paralar konusunda literatürü takip etmek ve katkıda bulunmak, uygulama örneklerinin teknolojik altyapılarını analiz etmek.
- Blokzincir ve kripto para teknolojisinin gizlilik ve güvenlik analizini yapmak.
- İşlemlerin geçerli, doğru ve değişmez kriptografik ispat ve matematiksel hesaplamalar ile sağlamasını yapmak.
- İleri seviyedeki kriptografik yapı taşlarının blokzincir teknolojisine olan uyumunu incelemek.
- Mikrofonlama ve mikroödeme yöntemlerinin blokzincir tabanlı olarak yapılabilirliğinin analizini yapmak.
- Kripto paraların denetlenebilirliğine ve gerekli yasal ve regülatif altyapısının oluşturulmasına katkı sağlamak.
- Ülke çapında bilimsel anlamda blokzincir çalıştaylarının yapılmasına ön ayak olmak.
- İlgili özel sektör işletmelerine ve kamu kurum ve kuruluşlarına teknik destek vermek.

- Blokzincir ve kripto para teknolojileri alanında literatüre katkı sağlamak.

Bu kapsamda kurum tarafından sürdürülen ve geliştirilmekte olan projeler şunlardır (BZLab, 2022):

- Dijital Para: Ulusal Merkez Bankası Dijital Parası (CDBC)’nin tasarlanması (Dijital Türk Lirası).
- Dijital Kimlik: Blokzincir tabanlı çalışacak dijital kimlik yönetim sisteminin oluşturulması, kurulumunun yapılması.
- Kripto Radar: Kripto paraların denetim ve incelenmesine altyapının geliştirilmesi.
- BiGA: Altına dayalı gizlilik sağlayan dijital para sisteminin geliştirilmesi.
- BAĞ (Blokzincir Araştırma Ağı): Ulusal çapta blokzincir teknolojisi araştırma altyapısının kurularak projeler geliştirmek ve test ağları oluşturmak.
- BKYS (Belge Kanıt Yönetim Sistemi): Akıllı sözleşme tabanlı kanıt yönetim sistemi.
- Blockchain Technologies for VET Education (BLUEDU)
- Bilgi ve İletişim teknolojileri alanında eğitim veren eğiticilerin ve öğrencilerin blokzincir teknolojilerine ilişkin bilgilerini ve yeteneklerini geliştirmek.

Kurum tarafından Türkiye’de blokzincir teknolojisindeki gelişmeleri değerlendirmek amacıyla Nisan 2018’de 1. Ulusal Blokzincir Çalıştayı ve Eylül 2019’da 2. Ulusal Blokzincir Çalıştayı düzenlenmiştir.

4.2.3. BiGA Projesi

“Bir Gram Altın” ifadesinin kısaltması ile kurulmuş olan BiGA, fiziki karşılığı miktarında depolanmış ve standartları belli olan kaydi altının taraflar arasında blokzincir altyapısında transfer edilmesini sağlayacak bir projedir. BiGA altyapısında geliştirilen ödeme sistemleri, BiGA’da tanımlı altın ve gümüş gibi gerçek değerlerini temsil etmeyi sürdürecektir. BiGA projesi, fiziki dayanağı olan, işlem yapan paydaşlar dışında detayların kimse tarafından görülmediğini garanti altına alarak gizliliğin sağlandığı ve yetkili otorite tarafından işlemlerin denetlenebildiği bir platform olması açısından diğer çözümlerden farklılaşmaktadır (TAKASBANK, 2019).

30 Aralık 2019 tarihi itibarı ile uygulamaya alınan “BiGA Dijital Altın” Projesine ilk etapta altı bankda katılım sağlamıştır. Böylelikle Türkiye’nin finansal alanda bilinen ilk blokzincir ağı kurulmuştur. Takasbank tarafından sunulan platformdan hizmet sağlayacak olan katılımcı bankaların kendi sistemlerinde yapacakları geliştirmelerle birlikte altın bakiyeleri katılımcı bankalar arasında 7 gün 24 saat transfer edilebilecektir (TAKAS İstanbul, 2020).

4.2.4. Blokzincir Araştırma Ağı

Blokzincir araştırmacılarına test ve geliştirme ortamı sunacak olan Blokzincir Araştırma Ağı (BAĞ), TÜBİTAK BİLGEM çatısı altında 2019 yılında kurulmuştur. BAĞ, blokzincir teknolojileri konusundaki rekabet gücünü yükseltmek için konu ile ilgilenen araştırmacıları bir araya getirmek ve eş güdüm içinde çalışmalarına yardımcı olmak amacıyla TÜBİTAK ve üniversitelerimizin iş birliği ile kurulan bir araştırma ve geliştirme ekosistemidir (CSB, 2022: 32). Gerekli donanım ve ağ altyapısı kaynağını sisteme ekleyen kuruluşlar sisteme üye olabilecekler ve giriş yapabileceklerdir.

4.2.5. Blockchain Economy İstanbul Summit

Blockchain Economy İstanbul Summit, finansın geleceğini yeniden tanımlamak için Türkiye’deki kripto para endüstrisinin kilit oyuncularını ve uzmanları bir araya getiren ve halihazırda yedi kere düzenlenmiş olan özel bir etkinliktir. Blockchain Economy Summit’in sekizincisi 8-11 Mayıs 2023’de İstanbul’da iki gün boyunca dünyanın önde gelen kripto para şirketleri ve blokzincir girişimcilerinin katılımı ile gerçekleştirilmesi planlanmaktadır (Blockchain Economy Istanbul, 2022).

4.2.6. Blockchain Türkiye Platformu (BCTR)

Türkiye Bilişim Vakfı (TBV) liderliğinde “Adem-i merkeziyetçi sisteme bölgesinde liderlik eden bir Türkiye yaratmak” vizyonu ve “Türkiye’de sürdürülebilir blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapış biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu oluşturmak.” misyonu ile 8 Haziran 2018 tarihinde kurulmuştur (TBV, 2020).

BCTR altında üyelerin ve iş birliklerinin katılımı ile ilk başta oluşturulan dört ana çalışma grubunun sayısı halihazırda dokuza yükselmiştir. Bunlar:

- Finans, Bankacılık ve Sigortacılık

- Hukuk, Düzenlemeler ve Kamu İlişkileri
- Üretim, Lojistik ve Ulaşım
- Uluslararası ve Akademik İlişkiler
- Sağlık
- Teknoloji
- Enerji
- Vergi, Muhasebe ve Denetim
- On-Chain

Çalışma grupları BCTR'nin kuruluşundan itibaren gerçekleştirdikleri düzenli toplantılarla belirlenen başlıklar altında çalışmalar yaparak, konuları ile ilgili 15 adet özel rapor hazırlamıştır ve bu raporlar, herkesin erişimine açık şekilde BCTR web sitesi üzerinden yayımlanarak, ilgili tüm paydaşlara ulaştırılmıştır (BCTR, 2022).

BEŞİNCİ BÖLÜM

5. BLOKZİNCİRİN KAMU YÖNETİMİ AÇISINDAN İNCELENMESİ

Bu bölümde blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği incelenmektedir. Öncelikle kamu yönetiminde blokzincirle alakalı yanlış bilinenlere yer verilmekte, ardından teknolojinin kamuda uygulanabilirliği önündeki engellerin hangi çerçevede ele alındığına değinilmektedir. Müteakiben bu engeller incelenerek, kamu yönetiminde blokzincir kullanmak gerekli midir, gerekli ise hangi tür blokzincir seçilmelidir sorularına cevap aranmaktadır.

5.1. Kamu Yönetiminde Blokzincirle İlgili Yanlış Bilinenler

19'uncu yüzyılda Alexander Graham Bell döneminde yaşasaydınız ve iletişimi kökten değiştirmeyi vaat eden yeni bir icadı duysaydınız, evliliğinizde yaşadığınız iletişim sorunlarınıza telefonun çözüm olabileceğini düşündüğünüz için belki mazur görülebilirdiniz. Fakat telefon gerçekten de küresel olarak iletişimin çehresini değiştirmiş olsa da, asıl işlevi hiçbir zaman evlilik içi iletişim sorunlarını çözmek olmamıştır (Ehsani, 2021).

Bugün blokzincire yönelik beklentilerin bir kısmının durumu da böyledir. Blokzincir güçlü bir araçtır, ancak onu her dokunduğunu dönüştüren sihirli bir değnek olarak kabul etmek doğru değildir.

Teknolojik atılımlar kimilerine göre çoğu zaman, kimilerine göre de her zaman yersiz beklentileri ve aldatmacayı beraberinde getirir (Ramiller ve Swanson, 2003: 40). Bunun ister istemez kötü bir şey olduğu düşünülse de teknolojinin potansiyelini hayal etmek, olası kullanım alanlarını somut hale getirmeye yardımcı olması açısından faydalı yönlerini kendi içerisinde barındırır (Lindman vd., 2020: 14). Blokzincir de bu açıdan bir istisna değildir. Kamuoyu kimi zaman teknolojinin ne olduğu ve geleceği hakkında abartılı beklentiler içerisinde girebilmektedir.

Aşırı beklentiler, özellikle teknolojinin gelişimi devam ediyorsa risk arz etmektedir. Kuruluşlarında teknolojinin kullanımını anlamak ve takip etmek isteyen profesyoneller için abartılı beklentileri gerçek çözümlerden ayırt etmek zorluk teşkil

edebilir. Çünkü mevcut gelişmelerin gerisinde kalmak istemeyen yöneticiler, yeterli muhakemede bulunmadan ilgili teknolojinin kuruluşlarında uygulanmasını talep edebilirler. Bu noktada teknoloji ile ilgili temelsiz beklenti ve varsayımları tartışmak önemlidir. Bu varsayımları görünür kılmak, belirli projelerin risklerini azaltmaya ve kamu sektörü için blokzincirle ilgili vaatleri gerçekleştirmeye yardımcı olur (Lindman vd., 2020: 14). Bu doğrultuda aşağıda kamu yönetiminde blokzincirle alakalı yanlış bilininlere yer verilmiştir.

5.1.1. Blokzincirin Kamu Yönetimini Tümüyle Dönüştüreceği Beklentisi

Bitcoin'in ortaya çıkmasından sonra fiyatının aşırı yükselmesi ile paralel olarak kripto paralara karşı oluşan ilgi, zamanla sosyal medya ve erken benimseyenlerin etkisiyle blokzincire duyulan merakı arttırmıştır. Bu da tüm dünyada ve kamu yönetiminin her düzeyinde blokzinciri esas alan büyük bir kamu sektörü revizyonu yapılmış izlenimi oluşmasına neden olmuştur.

Fakat gerçek hayattaki uygulamalar, en azından şimdilik durumun bu olmadığını göstermektedir. Birçok ülkede, hükümet ve yerel yönetimler teknolojiyi inceleme ve fikir geliştirme aşamasındadır. Bazıları bu fikirleri test etmiştir. Ancak bazı araştırmalara göre, gerçek kullanıcıları olan blokzincir altyapısını kullanan kamu hizmeti uygulamalarının sayısı yüksek değildir (Lindman vd., 2020: 15). Bu tür büyük bir revizyon gelecekte gerçekleşebilecek olsa da, şimdiye kadar büyük ölçekli dönüşümlerin ufukta olduğuna dair fazla kanıt bulunmamaktadır.

5.1.2. Kamuda Başarılı Blokzincir Uygulamaları Oluşturmanın İmkânsızlığı

Genel olarak kamu kurum ve kuruluşları belirli özelliklere sahip olsa da kamu sektöründe blokzincir altyapısı ile desteklenen hizmetlerin geliştirilmemesi, uygulanmaması ve kullanılmamasını gerektiren özel bir neden yoktur. Kamu sektörü, toplumdaki teknolojik değişimin itici gücü olmasa da teknolojinin geliştirilmesinde ve yayılmasında genellikle önemli bir ortaktır. Kamu sektörü ayrıca, blokzincir teknolojisinin test edilmesinde ve uygulanmasında kullanılabilecek bir dizi hizmeti bünyesinde barındırır (örneğin kimlik tespit uygulamaları, noter tasdik hizmetleri, vergi takip programları). Daha spesifik olarak, blokzincirin destekleyebileceği eğitim, sağlık ve kültür gibi bazı hizmetler belirli oranda kamu sektörü tarafından gerçekleştirilir.

5.1.3. Blokzincirin Kamu Yönetimine Duyulan Güvenin Yerine Geçmesi

Blokzincir teknolojisinin sunduğu altyapı ile dünyadaki güven ihtiyacını ortadan kaldıracığı aktarılmakta; yozlaşmış hükümetlere, açgözlü şirketlere ve hileli seçim sistemlerine güvenmek zorunda kalınmayacağı söylenmektedir. Buna göre tapu dairelerinden tedarik zincirlerine, oylama sistemlerine ve kimliğe kadar her alanda yaşanan devrimle bir daha asla bir insana, kuruma veya hükümete güvenme gereği kalmayacaktır (Ehsani, 2021).

Swan (2015: viii), blokzinciri baskıcı siyasi rejimlere karşı koymanın bir yolu olarak görmektedir. Bu yanıltıcı bir varsayımdır. Gerçek şu ki, blokzincir dijital dünyaya aittir. Fiziksel ve dijital dünyalar arasındaki ilişki (en azından mevcut ve öngörülebilir teknolojiler göz önüne alındığında) doğası gereği devam edecektir.

İçinde bulunduğumuz fiziksel dünyada, fiziksel varlıkları temsil eden dijital jetonlar bir blokzincirde yayınlandığında, bu dijital jetonların aslında temsil ettiklerini iddia ettikleri fiziksel varlıklar tarafından desteklendiğinin doğrulanması gerekmektedir. Bununla birlikte, herkesin bunu kendisi için doğrulaması pratik değildir ve ekonomik olarak verimsizdir. Doğrulama ihtiyacı, güvenilir bir aracı ihtiyacını yeniden gündeme getirir. Dolayısıyla blokzincirler veya dağıtılmış kayıt defterleri her zaman iddia edildiği gibi bu güveni ortadan kaldırmamaktadır (Ehsani, 2021).

Teknik bir çözümün (blokzincir), bir kamu kurumuna duyulan güvenin yerine geçeceği varsayımı, hatalı bir düşüncedir. Çünkü bu, basit bir süreç değildir ve istenmeyen sonuçlara yol açabilecek yeni bir güven zedelenmesine yol açabilir. Blokzincir de insanlara ve kurumlara olan güvenin bir kısmını teknolojiye kaydırmayı önermektedir. Buna göre kriptografiye, protokollere, yazılıma, bilgisayarlara ve ağa güvenmeniz gerekir. Çünkü bunlar genellikle tek başarısızlık noktalarıdır (Schneier, 2019). Örneğin, Bitcoin veya Ethereum gibi kripto para birimlerinden biri küresel ödeme yöntemlerinden biri haline dönüşseydi, para arzı ve maliye politikası üzerindeki kontrolü sağlamak açısından doğrudan önemli etkileri olurdu ki bu, birçok hükümetin kabul etmeyi istemeyeceği bir durum olurdu.

Devlete olan güveni belirli bir teknolojiye olan güven ile değiştirmekle ilgili ikinci bir hatalı varsayım bulunmaktadır. Hükümetler vatandaşlar tarafından sürekli olarak test

edilirler ve kendilerine duyulan güveni yalnızca teknik yollarla değil, demokratik süreçlerle de kazanmaları gerekir. Devletin hesap verebilirliği ve şeffaflığı, hukukun üstünlüğü, dava hakkı ve diğer temel hakların tümü, bir yetkinin test edildiği ve kamu sektörü aktörlerine devredildiği bu sürecin parçalarıdır (Lindman vd., 2020: 17). Hâlihazırda oldukça merkezi olan bu sürece, blokzincir gibi merkezi olmayan bir teknoloji aracılığıyla teknolojik güven eklemenin etkilerinin neler olacağı zamanla şekillenecektir.

5.1.4. Her Geliştirilen Teknolojinin Kullanıcıları Olacağı Beklentisi

"Yaparsan gelirler (If you build it, users will come)" ifadesi, 1989 yapımı "Field of Dreams" filminden ünlü bir alıntıdır. Filmde ana karakter, kendisine mısır tarlasına bir beyzbol sahası inşa etmesini söyleyen bir ses duyar ve buna göre, bunu yaptığında eski beyzbol oyuncularının hayaletleri oraya geleceklerdir. Bu ifade genellikle, iyi veya değerli bir şey yaratırsanız, insanların doğal olarak ona çekileceğini ifade etmek için kullanılmaktadır (Sage, 2023). Bu ifadeyle paralel olarak, yeni geliştirilen blokzincir teknolojisinin de ne olursa olsun kamu yönetiminde kesinlikle kullanılacağını varsaymak, yanlış bir yaklaşım olacaktır. Kamu hizmeti sağlayıcıları, teknolojinin ve sunduğu çözümün son kullanıcı için ne anlama geldiğini ve hizmeti kullanıp kullanamayacaklarını asla gözden kaçırmamalıdır.

Bu yaklaşım, dijital teknolojiler için her zaman geçerli olmayabilir: Çünkü dijital teknolojilerin çoğu için, ilk savunucular genellikle gönüllü, açık kaynak yazılım uygulamalarını benimsemiş ve geliştirici odaklı topluluklar olagelmıştır. Buna örnek olarak Linux işletim sistemi veya daha yakın zamanda Bitcoin ve Ethereum açık kaynak projeleri verilebilir. Dolayısıyla, erken aşamalara katılmak için teknolojiye büyük ilgi duyan yetenekli geliştiricilere odaklanmak ve bunları çekmek bazı faydalar sağlayabilir, ancak son kullanıcılar ihmal edilirse, ürün veya hizmet daha sonra piyasaya sürüldüğünde bu başarısızlığa sebep olacaktır. Çünkü yetenekli geliştiriciler, ortalama kullanıcılardan çok daha farklı bir kullanıcı havuzu oluşturmaktadırlar (Lindman vd., 2020: 18-19).

Belirli bir teknolojinin bazı üstün niteliklere sahip olması nedeniyle otomatik olarak benimseneceği ve yaygınlaşacağı varsayılabilir. Bazı teknoloji savunucuları, teknolojinin belirli bir bölümüyle son derece ilgilidir ve örneğin blokzincir tabanlı hizmetleri, diğer teknolojiler kullanılarak oluşturulan geleneksel hizmetlerden çok

farklı veya daha iyi olarak tasvir edebilmektedirler (Lindman vd., 2020: 19). Örneğin teknoloji uzmanları, finansal hizmetler endüstrisi tarafından geleneksel olarak sağlanan; ödemeleri takas etme ve dolandırıcılığı önleme gibi olanakların blokzincir altyapısı ile dönüştürülmesinden bahsetmektedir. Ancak pek çoğuna göre, bankalar bu hizmeti yeterince iyi ve son kullanıcıya görünürde düşük bir maliyetle sağlamaktadır. Bu nedenle ilk blokzincir uygulaması olan Bitcoin'in, 2008 mali krizinin hemen ardından, medya ve kamuoyunun yerleşik finansal kurumlara ve araçlara karşı yaygın bir memnuniyetsizliği ve artan güvensizliği yansıttığı bir zamanda, halkın radarına girmesi tesadüf değildir (Marr, 2018). Dolayısıyla “sokaktaki adamın”, başka bir deyişle son kullanıcının her zaman kullandıkları hizmetlerin yararları konusunda ikna olmaları gerekmektedir. Ayrıca kullanıcıların ihtiyaçlarını dikkate alan ve teknolojinin kamu hizmetlerine yönelik faydalarını net bir şekilde açıklayan daha kapsamlı geliştirme çabalarına ihtiyaç bulunmaktadır.

5.1.5. Blokzincirin Kapsamlı ve Yıkıcı Olması Gerekliliği

Blokzincir alanında yazılan ilk eserler, blokzinciri yıkıcı bir teknoloji olarak müjdelemiş ve etkilerine yönelik beklentileri orantısız bir şekilde yükseltmiştir (Tapscott ve Tapscott, 2016). Gerçekten de blokzincir, kırk yılı aşkın süredir bilgi işlemde birincil paradigma olan merkezi bilgisayar mühendisliğinden radikal bir ayrılma olması yönüyle heyecan vericidir. Teknoloji, merkezi olmayan hizmetler hakkında temelde farklı bir düşünce tarzı sunmaktadır. Fakat bu, bu teknoloji üzerine inşa edilen hizmetler için beklenti seviyesini oldukça yüksek tutmaktadır (Lindman vd., 2020: 19).

Yıkıcı ve devrim niteliğindeki hizmetler çok karmaşık olabilir ve proje olarak bir araya getirilmesi zorluk teşkil eder. Daha evrimsel, başka bir deyişle zamanla evrilen ve gelişimini tamamlayan projeler, özellikle kamu sektöründe daha kolay bir şekilde kurumsal meşruiyet kazanabilmekte ve kurumsal engeller ve diğer geçerli kaygılarla karşılaşma riski daha az olabilmektedir. Örneğin blokzincir, belirli bir hizmette daha şeffaf bir zaman damgalı günlük kaydı algoritması sağlayabilir. Ancak pilot uygulama için doğru çözüm bu olsa da, bu çözüm paydaşların beklentilerini karşılayacak kadar yıkıcı olmayabilir (Lindman vd., 2020: 19).

Artan teknolojik karmaşıklıkla beraber oluşan artan hizmet karmaşıklığı, büyük, yıkıcı projeleri yönetmeyi ve başarılı bir şekilde gerçekleştirmeyi daha zor hale

getirmektedir. Öte yandan, daha küçük projeler, çok yüksek beklentileri karşılamak için cevap vermiyor gibi görünmektedir. Bu, birçok kamu sektörü projesi için de gerçek bir sorun teşkil eden bir dinamiktir. Fakat küçük, pragmatik ve yinelemeli blokzincir uygulamaları da aynı derecede değer üretebilir; blokzincirin tüm kamu sektörünü yeniden icat etmesi gerekmemektedir (Lindman vd., 2020: 19-20).

5.1.6. Kamuda Blokzincirin Nasıl Uygulanacağını Bilinmemesi

Kamu sektörü yeni teknolojileri genellikle özel sektörden temin etmektedir. Bu, kamu sektörü satın alma profesyonelleri tarafından iyi bilinen sorunlara yol açmaktadır. Uzmanlığın dış kaynaklardan edinilmesi durumunda, hizmetin sağlanmasından sorumlu olan kamu sektörünün hangi teknolojiyi satın alacağını bilmesi gerekir. Bu, blokzincir tabanlı hizmet için iş ihtiyacının dikkatli bir şekilde değerlendirilmesini, kamu satın alma veya devreye alma süreci hakkında bilgi sahibi olmayı ve ilgili blokzincir tabanlı hizmetin satıcılarının dikkatli bir şekilde değerlendirilmesini gerektirir (Lindman vd., 2020).

Blokzincirle alakalı ilk sorunlardan biri, kamu çalışanlarının bu alandaki teknik becerilerinin eksikliği idi. Bilgisayar bilimi ve yazılım mühendisliğinde yıllar boyunca çalışmalar yapılmış olsa da geliştirme çabaları daha çok merkezi bilgi işlem mimarileri ve veri depolama çözümlerinin geliştirilmesine odaklanmıştır. Teknik becerilerin eksikliği artık ana engel değildir. Teknoloji ve ilgili beceriler son birkaç yılda hızla gelişmektedir. Bu hem kamu sektöründe hem de kamu görevlilerinin erişebildiği (örneğin, ortaklıklar veya satın alma yoluyla) özel sektör satıcıları arasında bir dereceye kadar geçerlidir. Halen bir miktar blokzincir becerileri açığı kalmasına rağmen, daha fazla kaynak mevcuttur ve bu projeleri geliştirmeyi desteklemek için çok fazla altyapı vardır. Erken inovasyon projelerinden toplanan zengin bir uzmanlığın yanı sıra hizmetleri sağlayabilen artan sayıda potansiyel satıcı bulunmaktadır (Lindman vd., 2020: 20-21). Bu, teknolojinin uygulanması için kamu yönetiminin olgunlaştığı anlamına gelmektedir.

5.1.7. Kullanıcıların Hizmetin Blokzincire Dayalı Olmasını Önemsemesi

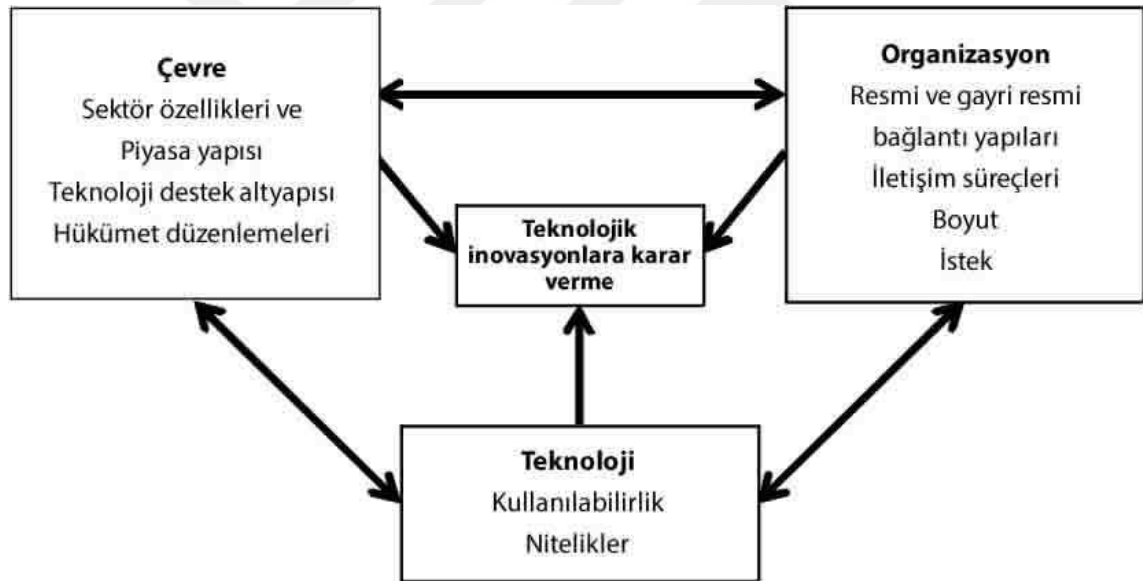
Bazen belirli bir teknolojinin savunucuları, başkalarının da kendileri kadar o teknoloji ile ilgilendiğini düşünür. Bu tutum; geliştiricilerin, kullanıcıların teknolojiyi kullanma konusunda kendileri kadar iyi olacağını düşünmesinden ve teknolojideki teknik üstünlüğün, kullanıcıların o teknolojiyi "daha iyi olduğu için" otomatik olarak

kullanacaklarını düşünmelerine dayanmaktadır (Lindman vd., 2020: 23). Bu her zaman böyle olmamaktadır. Bununla birlikte, diğer her şey eşit olduğunda, hizmetlerin çoğu son kullanıcısı, genellikle hangi teknolojik altyapının kendilerine bir hizmet sağladığını pek umursamaz, hatta bilmez (Sueoka, 2019).

Çoğu kullanıcı, başka bir teknoloji kullanılarak yürütülen uygulamaya kıyasla sırf blokzincir altyapısı kullanıldığı için uygulamaya değer vermeyebilir. Aslında, çoğu yeni teknoloji kullanıma sunulurken olduğu gibi, blokzincirde de üstesinden gelinmesi gerekebilecek ek bir güvensizlik unsurları mevcut olabilir (Werbach, 2019). Bu nedenle kamu sektörü aktörlerinin vatandaşların ihtiyaçlarını anlaması ve ardından onları blokzincirin değerli olduğuna ve gerekli bir hizmeti sağladığına ikna etmeleri önemlidir.

5.2. Teknoloji-Organizasyon-Çevre Çerçevesi ve Engellerin Sınıflandırılması

Şekil 8: Teknoloji - Organizasyon - Çevre Çerçevesi



Kaynak: Baker, 2012: 236

Araştırmada blokzincirin kamu yönetiminde uygulanabilirliği önündeki engelleri sınıflandırmak için, araştırmacılar tarafından bilgi teknolojilerinin benimsenmesini incelemek amacıyla yaygın olarak kullanılan bir yöntem olan ve Şekil 8’de sunulan Tornatzky vd.lerinin (1990) Teknoloji - Organizasyon - Çevre çerçevesi kullanılmıştır.

Bu çerçevede; teknolojik, organizasyonel ve çevresel olmak üzere teknolojik yeniliklerin bir örgüt tarafından benimsemesi kararına etki eden faktörler üç bağlamda incelenmektedir (Baker, 2012: 232).

5.2.1. Teknolojik Bağlam

Teknolojik bağlam, hem bir örgüt tarafından hâlihazırda kullanılmakta olan hem de örgütün bulunduğu ortamda mevcut, fakat şu anda örgüt tarafından kullanılmayan teknolojileri içermektedir. Bir örgütün mevcut teknolojileri, yeni teknolojileri benimseme sürecinde önemlidir. Çünkü örgütün üstlenebileceği teknolojik değişimin kapsamı ve hızına geniş bir sınır koymaktadır (Collins vd., 1988: 513). Örgütte var olan ancak henüz kullanılmayan teknolojik yenilikler de hem mümkün olanın sınırlarını çizerek hem de hangi teknolojilerin örgütü geliştirip yeniliklere uyum sağlamayı kolaylaştırdığını göstererek inovasyonu etkilemektedir (Baker, 2012: 232).

Örgüt dışında var olan inovasyonlar grubu içinde, kademeli, sentetik veya süreksiz değişiklikler yaratan yenilikler olmak üzere üç tür inovasyon bulunmaktadır (Tushman ve Nadler, 1986: 76). Kademeli değişim üreten yenilikler, mevcut teknolojilerin yeni özelliklerini veya yeni sürümlerini ortaya çıkarır. Bu kademeli yenilikler, benimseyen organizasyon için en az risk ve değişimi temsil eder. Katod ışın tüplü (CRT) bilgisayar monitörlerinden sıvı kristal ekranlı (LCD) monitörlere geçmek veya kurumsal kaynak planlama (ERP) sisteminin bir sürümünden aynı sistemin daha yeni bir sürümüne geçmek örnek olarak verilebilir (Baker, 2012: 232).

Sentetik değişiklik üreten yenilikler, mevcut fikirlerin veya teknolojilerin yeni bir tarzda birleştirildiği, ılımlı bir değişimin orta noktasını ifade eder. Buna örnek olarak üniversitelerin ders içeriğini internet aracılığıyla sunması verilebilir. Kayıt, depolama veya iletimde hiçbir yeni teknoloji kullanılmaz ve kurs içeriğinde bir yenilik yoktur (Baker, 2012: 232). Sadece mevcut teknolojiler inovasyon için yeni bir şekilde birleştirilmektedir ve kullanılmaktadır.

"Radikal" yenilikler olarak da adlandırılan (Ettlie vd., 1984) süreksiz bir değişim üreten yenilikler ise, mevcut teknoloji veya süreçlerden önemli sapmaları temsil eder (Baker, 2012: 232). Örneğin daktilolardan bilgisayarlara geçiş ya da e-devlet

uygulamaları kamusal hizmetlerin sunumu alanında yaşanan radikal yeniliklere örnek olarak verilebilir.

5.2.2. Organizasyonel Bağlam

Organizasyonel bağlam, bir örgütün çalışanları arasındaki bağlantı yapıları, örgüt içi iletişim süreçleri, örgütün büyüklüğü ve kaynakların miktarı da dâhil olmak üzere örgütün nitelikleri ve kaynakları ile ilgilidir. Bu bağlamın teknolojik yenilikleri benimseme ve uygulama kararlarını etkilemesinin birkaç yolu bulunmaktadır. Burada örgütsel yapının inovasyon benimseme süreciyle ilişkisine atıfta bulunmaktadır. Organik ve merkezi olmayan örgütsel yapılara sahip kuruluşlar ekip çalışmasına önem verir, çalışanlarına yönelik sorumluluklarda bir dereceye kadar geçişkenliğe sahiptir ve raporlamada hiyerarşiye ek olarak yatay iletişimi teşvik eder. Örgütsel yapı üzerine yapılan diğer araştırmalar, yenilik sürecinin benimsenme aşamasına en uygun organizasyon yapısı olarak organik ve merkezi olmayan yapıları gösterirken yenilik sürecinin uygulama aşaması için ise resmi raporlama ilişkilerine, merkezi karar vermeye ve çalışanlar için açıkça tanımlanmış rollere vurgu yapan mekanik (organik olmayan) yapıların en uygun organizasyon yapısı olacağını belirtmektedir (Baker, 2012: 232-233).

Teknolojik inovasyon için destek altyapısı da olumlu etkiye sahiptir. Vasıflı iş gücü için yüksek ücretler ödemek zorunda olan örgütler, genellikle emek tasarrufu sağlayan yenilikler yoluyla inovasyon yapmaya mecbur kalırlar (Globerman, 1975: 428-429). Nitelikli işgücünün mevcudiyeti ve danışmanların veya diğer hizmet tedarikçilerinin mevcudiyeti de teknolojik yenilikleri teşvik eder.

5.2.3. Çevresel Bağlam

Çevresel bağlam; endüstrinin yapısı, teknoloji hizmeti sağlayıcılarının mevcudiyeti ve düzenleyici ortam ile ilgilidir. Endüstri yapısı çeşitli şekillerde incelenmiştir. Örneğin, yoğun rekabet, yeniliğin benimsenmesini teşvik eder. Ayrıca, değer zincirindeki baskın firmalar yenilik yapmaları için diğer değer zinciri ortaklarını etkileyebilir (Baker, 2012: 235).

Son olarak, hükümet düzenlemelerinin inovasyon üzerinde olumlu veya olumsuz etkisi olabilir. Örneğin hükümetin, otomobil firmaları için emisyon sınırlaması getirmesi gibi endüstriye yeni kısıtlamalar getirdiğinde, inovasyon esasen bu firmalar için

zorunludur. Benzer şekilde, katı güvenlik ve test gereklilikleri, çok sayıda endüstride inovasyonu geciktirebilir. Yeni malzemelerin kullanılmadan önce kapsamlı bir şekilde test edilmesi gereken inşaat sektöründe veya yeni ürün çeşitlerinin patentlenmesi ve lisanslanması gereken tarım, hayvancılık ve gıda sektöründe, inovasyonun maliyeti oldukça yüksek olabilir. Başka bir örnek, gizlilik gerekliliklerinin bankaların müşteri hesap bilgilerine erişmesi için yeni yollar sunmasını engelleyebileceği bankacılık sektörüdür. Bu nedenle, hükümet düzenlemeleri yeniliği teşvik edebilir veya caydırabilir.

5.2.4. Engellerin Sınıflandırılması

Araştırmada blokzincirin kamu yönetiminde uygulanabilirliği önündeki engeller TOE çerçevesi kapsamında teknolojik, organizasyonel ve çevresel olmak üzere üç alt başlıkta sınıflandırılmıştır. Kamu yönetimi açısından incelendiğinde teknolojik bağlam, henüz geliştirilme aşamasında olan blokzincirdeki teknik eksiklikleri tanımlamaktadır. Organizasyonel bağlam, blokzincir teknolojisinin benimsenmesiyle ilgili olan örgütsel hazırlık, alt yapının kurulması ve nitelikli personelin mevcudiyeti gibi kamu kurum ve kuruluşlarının örgütsel özellikleri ve kaynakları ile ilgili konuları kapsamaktadır. Çevresel bağlam ise, yasal ve düzenleyici ortam, standartların ya da örnek uygulamaların eksikliği gibi kurum ve kuruluşların hizmetlerini yürüttüğü çevresel ortam ile ilgilidir. Bu üç bağlam kullanılarak yapılan literatür taraması sonucunda blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği önünde on üç temel engel belirlenmiş ve bu belirlenen engeller ve zorluklar da üç kategoride sınıflandırılmıştır.

5.3. Blokzincirin Kamu Yönetiminde Uygulanabilirliği Önündeki Engeller

Blokzincir teknolojisi, ikinci bölüm üçüncü kısımda sıralanan üstün yönleri ve faydaları ve üçüncü bölüm ikinci kısımda yer verilen özellikleri ile kamu yönetimini birçok açıdan dönüştürme potansiyeline sahiptir. Bu potansiyele rağmen, aslında her yeni teknolojinin gelişim aşamasında olduğu gibi bazı riskleri, sorunları ve zayıflıkları da bulunmaktadır. Blokzincir teknolojisinin vaat edilen faydaları kanıtlanabilirse, teknolojinin bir dönüm noktası olması (Baturbara vd., 2018: 2) ve yakın gelecekte dünyadaki birçok hükümet tarafından yaygın bir şekilde kabul görmeye başlaması mümkündür. Ancak bunun için, bu potansiyel faydaların deneysel kanıtlarla (Ølnes vd., 2017: 359) ve gerçek hayattan uygulamalarla kanıtlanması ve desteklenmesi gerekmektedir.

Araştırmada yapılan literatür taraması sonucunda, blokzincir teknolojisinin kamu yönetiminde benimsenmesi önünde on üç temel engel belirlenmiştir. Bu engeller bazı araştırmalarda olumlu kullanımlarıyla ya da farklı şekilde ifade edilmekte olup benzer ifadeler bir başlık altında toplanmıştır. Örneğin, bazı araştırmalarda teknolojiyi kullanma konusundaki isteksizlik, kültürel direnç (Chhina vd., 2019) veya mevcut sistemleri değiştirmek istememe (Sanka vd., 2021) şeklinde ele alınırken, bazı araştırmalarda kültürel benimseme (Patel vd., 2017) şeklinde ifade edilmektedir. Buna göre tespit edilen ve sınıflandırılan edilen engeller Tablo 4’te sunulmaktadır.

Tablo 4: Blokzincirin Kamu Yönetiminde Kullanılabilirliği Önündeki Engeller

Kategori	Engel Açıklaması	Kaynaklar
Teknolojik	Gizlilik ve güvenlik	(Sanka vd., 2021), (Chhina vd., 2019), (Lin ve Liao, 2017), (Swan, 2015), (Al-Jaroodi ve Mohamed, 2019), (Apostolaki vd., 2017), (Douceur, 2002), (Joshi vd., 2018), (Wang vd., 2018)
	Ölçeklenebilirlik	(Bondi, 2000), (Khan vd., 2021), (Sanka vd., 2021), (Casino vd., 2019), (Meng vd., 2018), (Zheng vd., 2017), (Tanrıverdi vd., 2019), (Rana vd., 2022), (Yli-Huumo vd., 2016), (Yang, 2019)
	Gecikme sorunları	(Rauchs vd., 2018), (Gencer vd., 2018), (Chhina vd., 2019), (Hill vd., 2018), (Swan, 2015), (Casino vd., 2019), (Rana vd., 2022), (Sanka vd., 2021)
	Kurulum ve çalıştırma maliyeti	(Deloitte, 2018), (Allessie vd., 2019), (Lin ve Liao, 2017), (Meng vd., 2018), (Berryhill vd., 2018), (Erola vd., 2022), (Baturbara vd., 2018), (Cagigas vd., 2022)
	Birlikte çalışabilirlik sorunları	(Suominen vd., 2018), (European Commission, 2019), (Sanka vd., 2021), (Casino vd., 2019), (Tasca ve Tessone, 2019), (Deloitte, 2018), (Kejriwal ve Mahajan, 2017), (Ølnes ve Jansen, 2018), (Reddick vd., 2021), (Allessie vd., 2019),

	Eski sistemlerle entegrasyon	(Sanka vd., 2021), (Casino vd., 2019), (Rana vd., 2022), (Al-Jaroodi ve Mohamed, 2019), (European Commission, 2019) (Ølnes ve Jansen, 2018), (Deloitte, 2021), (Reddick vd., 2021)
Organizasyonel	Altyapı eksikliği	(Kossow ve Dykes, 2018), (Bistarelli, 2022), (Cagigas vd., 2022), (Deloitte, 2022), (Chhina vd., 2019), (Ølnes ve Jansen, 2018), (Erola vd., 2022)
	Yetkin personel eksikliği	(TÜSİAD, 2018), (Deloitte, 2022), (Reddick vd., 2021), (Chhina vd., 2019), (Center of E-Government, 2021), (Rana vd., 2022), (Al-Jaroodi ve Mohamed, 2019),
	Bilgi eksikliği, düşük anlayış ve farkındalık	(Walsch, 2017), (Erola vd., 2022), (Sanka vd., 2021), (Deloitte, 2018), (Swanson, 2016)
	Teknolojiyi kullanma konusundaki isteksizlik	(Sanka vd., 2021), (Erola vd., 2022), (Rana vd., 2022), (Cagigas vd., 2022), (Mougayar, 2015), (Swanson, 2016), (Chhina vd., 2019), (Patel vd., 2017)
Çevresel	Yasalara ve mevzuata uyumluluk sorunları	(Kossow ve Dykes, 2018), (Deloitte, 2018), (Walsch, 2017), (Patel vd., 2017), (European Commission, 2019), (Sanka vd., 2021), (Deloitte, 2022), (Swan, 2015), (Rana vd., 2022)
	Standart eksikliği	(European Commission, 2019), (Erola vd., 2022), (Sanka vd., 2021), (Casino vd., 2019), (Tasca ve Tessone, 2019), (Deloitte, 2018), (Kejriwal ve Mahajan, 2017), (Ølnes ve Jansen, 2018)
	Örnek uygulamaların eksikliği	(Yli-Huumo vd., 2016), (Bistarelli, 2022), (Baturbara vd., 2018), (Rana vd., 2022), (Erola vd., 2022)
	Etik sorunlar	(Walsch, 2017), (Swan, 2015), (Yli-Huumo vd., 2016), (Meng vd., 2018)

Kaynak: Araştırmacı tarafından hazırlanmıştır.

5.3.1. Teknolojik Sorunlar

Teknolojik sorunlar; ölçeklenebilirlik, gizlilik ve güvenlik, gecikme sorunları, kurulum ve çalıştırma maliyeti, birlikte çalışabilirlik ve entegrasyon sorunları başlığı altında incelenmektedir.

5.3.1.1. Kurulum ve Çalıştırma Maliyeti

Yerleşik sistemi değiştirmek ve blokzincir tabanlı yeni bir altyapı oluşturmak, büyük teknolojik dönüşüm gerektireceği için zaman ve para dâhil olmak üzere oldukça yüklü bir maliyet gerektirecektir. Blokzincir de devletler için hem sosyo-ekonomik maliyetler doğurmakta hem de yüksek sermaye yatırımları gerektirmektedir. Blokzincirin yerel uygulamalarına odaklanan bazı önceki araştırmalar, blokzincire geçişin mevcut teknolojik maliyetinin, sağladığı ek güvenlikten daha ağır basmayacağı sonucuna varmıştır (Gabison, 2017: 340). Xie vd.lerine (2019: 2822) göre, blokzincir tabanlı bir sistemi kurmanın ve çalıştırmanın maliyeti henüz tam olarak bilinmemektedir. O yüzden bu yeni teknolojinin ekonomik getiri ve götürülerinden, mevcut sistemler ile çalışabilirliğinden ve organizasyonel faydalarından emin olduktan sonra kullanılıp kullanılmayacağına karar verilmelidir (Lin ve Liao, 2017: 658). Fakat örnek olarak bilgisayar teknolojisinin dünya çapında kullanılmaya başlamasından hareketle, her yeni teknolojinin ilk başlarda daha fazla maliyet gerektirdiği, sonradan ise asıl ekonomik getirilerini ortaya çıkardığı da unutulmamalıdır.

Devlet kurumları, sıkı mali denetimlere, bütçe kısıtlamalarına ve kamu hesap verebilirliğine tabidir. Dolayısıyla herhangi bir blokzincir çözümünün faydaları, kamunun sınırlı kaynaklarına yatırım yapmadan önce açık ve net bir şekilde hesaplanmalı ve belirlenmelidir.

5.3.1.2. Birlikte Çalışabilirlik ve Entegrasyon Sorunları

Teknolojik sorunların bir diğeri birlikte çalışabilirlik sorunlarıdır. Birlikte çalışabilirlik, çeşitli sistemler arasında kolayca bilgi paylaşma, çalıştırma ve işlem yapabilme becerisini ifade etmektedir (Chang vd., 2020: 2092). Bu, üstesinden gelinmesi gereken temel bir sorundur. Çünkü en olası senaryo, internet gibi tek bir defter (blokzincir) yerine, muhtemelen bir tür birlikte çalışabilirlik gerektiren çok sayıda farklı genel ve özel platform olacaktır (Allen vd., 2020: 7).

Tıpkı bireysel kullanıcıları olan bir sosyal medya ağı veya bağımsız alıcı ve satıcılardan oluşan bir e-ticaret platformu gibi, blokzincirin değeri, kullanıcı tabanı genişledikçe artma eğilimindedir. Ancak, herhangi bir alanda tek bir küresel blokzincir olmayacak; bunun yerine, hayatın farklı alanlarında dünyanın dört bir yanında birden fazla blokzincir sistemi geliştirilecektir. Bu blokzincirin yaygınlaşması için olumlu olmakla birlikte ister bir işletme ister bir kişi olsun, herhangi bir kullanıcının, her biri kendi teknolojisine ve yönetimine sahip birçok blokzincir sisteminin ortaya çıkacağı anlamına gelmektedir. Böyle bir durumda ise farklı ağların veri sistemlerinin veya "şemalarının" birlikte çalışabilirlik sorunlarının ortaya çıkmasına sebep olabilir (Suominen vd., 2018). Örneğin A blokzinciri kullanıcılarının B blokzincirindekiler ile etkileşime girmesinde zorluklar çıkabilir.

Blokzincir çözümleri bağımsız uygulamalar için değil, daha çok kuruluş içinde ve dışında kullanılan birden çok uygulama ile entegre olması için tasarlanmıştır. Fakat blokzincir çözümlerini, eski veya mevcut sistemlerle entegre etmek zor olabilir. Bu zorluk temel olarak birlikte çalışabilirlik sorunlarından kaynaklanmaktadır. Örneğin, eski uygulamalar, blokzincir çözümleri dâhil olmak üzere yeni sistemler ve uygulamalarla sorunsuz ve güvenli bir şekilde çalışmaya hazır olmayabilir. Başka bir örnek, blokzincir tabanlı uygulamaları çalıştırmak için birlikte çalışması gereken farklı platformlar ve işletim ortamlarıdır. Ayrıca eski ve yeni uygulamalar, farklı satıcılar tarafından farklı geliştirme metodolojileri, ortamları ve programlama dilleri kullanılarak geliştirilmiş olabilir. Bu nedenle entegrasyon süreci karmaşık hale gelebilecektir (Al-Jaroodi ve Mohamed, 2019: 36508).

Kullanılan herhangi bir entegrasyon modeli, mevcut uygulamaların işlevlerinin doğruluğunu ve güvenilirliğini ve tüm entegre sistemler arasında iş verilerinin tutarlılığını sağlamalıdır. Ayrıca, herhangi bir entegrasyon ilgili tüm uygulamalar için iyi güvenlik önlemleri sağlamalıdır. Bu entegrasyon, güvenlik açıkları, gizlilik endişeleri veya güvenilirlik ve kullanılabilirlik sorunları için herhangi bir açık kapı bırakmamalıdır. Blokzinciri çeşitli entegre endüstriyel uygulamalara dâhil edecek etkili entegrasyon modelleri sağlamak için bazı çalışmalar devam etmektedir. Bununla birlikte, daha yararlı ve spesifik çözümler bulunmalı ve geliştirilmelidir (Al-Jaroodi ve Mohamed, 2019: 36508). Benze şekilde hükümetin tasarladığı bir blokzincir söz konusu olduğunda, dâhil

olan bütün kurum/kuruluşların aynı platform üzerinde olması gerekliliği akılda tutulmalıdır.

5.3.1.3. Ölçeklenebilirlik

Blokzincir teknolojisinde karşılaşılabilecek başka bir risk, blokzincirin etkinliği ve verimliliği ile yakından ilgili olan ölçeklenebilirlik problemidir. Ölçeklenebilirlik, bir blokzincir ağında işlemlerin gerçekleştirilebileceği ölçek ve hızı ifade etmektedir (Cagigas vd., 2022: 13912). Buradaki işlem hızı, bir işlemi bir bloğa eklemek veya düğümler arasında mutabakata varmak için gereken süreyi belirler. Blokları doğrulamak için ne kadar çok düğüm gerekiyorsa, doğrulama işlemi o kadar yavaş olacaktır. Ayrıca, daha fazla veri dâhil edildiğinde ve blok boyutu artırıldığında, blokları oluşturmak ve yaymak daha zor hale gelecektir (Xie vd., 2019: 2820). Böylece, ölçeklenebilirlik ve güvenlik arasında bir denge kurulur. Blokzincir teknolojisi, ölçeklenebilirlik açısından olgunlaşmamış bir teknolojidir ve hala çok sayıda işlemin üstesinden gelmek için mücadele etmektedir (Saber vd., 2019: 2126).

Blokzincirde ağ boyutu büyüdükçe performans düşmektedir. Yerine geçmesi planlanan farklı alanlardaki mevcut çözümler ile mukayese edildiğinde daha düşük işlem performansı göstermektedir. Örnek olarak VISA kredi kartı altyapısı ile saniyede 65 bin işlem yapılabilir (VISA, 2022). Bitcoin blokzincirinde ise saniyede ortalama yedi işlem yapılabilir (IMF, 2022: 9). Burada sorun, Bitcoin'in ne amaçla kullanılacağını netleştirilmesi gerekliliğidir. Bitcoin'e karşı çıkanlar işlem performansı bağlamında Bitcoin'in oldukça geride kaldığını savunurken (Usta ve Doğantekin, 2018: 97), savunular ise Bitcoin'in bir ödeme sistemi değil, altın gibi bir değer saklama aracı niteliğinde olduğu, o yüzden çok hızlı olması gerekmediği söyleminde bulunmaktadır (Popper, 2015). Dolayısıyla işlem performansını değerlendirirken, sistemin ne amaçla kullanılacağını belirlemek gerekmektedir.

5.3.1.4. Gizlilik ve Güvenlik

Blokzincirin bir güven mekanizması olarak tanıtılması da risk unsurlarından birisidir. Blokzincir hükümetler için birçok fayda sunsa da tamamen güvenden bağımsız bir sistem olarak değerlendirilmemelidir. Başka bir deyişle blokzincir, kurumsal güven ve kurumsal altyapının yerine geçemez (Hyvärinen vd., 2017: 453). Aslında, yüksek

derecede kaliteli kamu ve kamu hizmetlerine sahip ülkeler blokzincir teknolojisini daha erken ve başarılı bir şekilde benimsemektedir (Cagigas vd., 2022: 13913).

Blokzincir sistemlerinde güvenliğin ve gizliliğin korunması, önemli bir endişe konusudur. Aynı şekilde kamu yönetiminde de blokzincir uygulamaları hayata geçirilirken, hassas verilerin yanlış yönetimi ve sistemlerin kusurlu tasarımı nedeniyle siber saldırılar ve güvenlik açıkları mümkün hale gelebilir. Bu yüzden; verilerin yanlış yönetiminden, bilgi sızıntıları vs. gibi uygulama güvenlik açıklarından, yanlış şifreleme algoritması seçilmesinden ve kullanım yetkilerinin yanlış tanımlanmasından kaynaklanan gizlilik ve güvenliği tehlikeye atabilecek risklere karşı önlemler alınmalıdır (Tasca ve Tessone, 2019: 24).

Blokzincirde gizlilik ve güvenlikle ilgili potansiyel risk oluşturabilecek en önemli hususlardan birisi de kuantum bilgisayarlardır. Halihazırdaki bilgisayarlar, sadece 1 ve 0 ile işlem yapabilen ikili (binary) sistemi kullanılmaktadırlar. Fakat kuantum bilgisayarların geliştirilmesiyle birlikte 1 ve 0'ın yanında aynı anda geçerli olan üçüncü bir durum daha (1-0) bulunacaktır. Bu bilgisayarların geleneksel bilgisayarlara karşı milyonlarca kat daha hızlı işlem yapabilme kabiliyetine sahip olması beklenmektedir (Mermin, 2007: 3).

Blokzincirin özünde, işlemleri imzalamak için kullanılan şifrelenmiş özetler (hash'ler) ve açık anahtar şifrelemesi olmak üzere iki tür şifreleme bulunmaktadır. Çoğu blokzincirde kullanılan hash algoritması SHA-256'dır ve kuantum bilgisayar algoritması kullanılarak bu algoritmayı kırmak için 2128 işleme ihtiyaç duyulmaktadır (Casino vd., 2019: 70). Bu, SHA-256'yı kuantum saldırılarına karşı dayanıklı hale getirirken, açık anahtar şifreleme algoritmaları için geçerli değildir. Günümüzün gelişmiş ikili şifreleme yöntemleri, yeterince gelişmiş bir kuantum bilgisayar oluşturulduğunda kırılabilir ve bu durum, mevcut blokzincir platformlarının çoğu için bir risk oluşturacaktır. Bununla birlikte, kuantum bilgisayarların geliştirilmesiyle birlikte blokzincir tabanlı ve kuantum dirençli yeni algoritmaların keşfedileceği de iddia edilmektedir (Usta ve Doğantekin, 2018: 101).

5.3.1.5. Gecikme Sorunları

Blokszincirde gecikme, bir girdinin alınmasından çıkışta işlemin tamamlanmasına kadar ölçülen bir işlemin işlem süresi demektir. İzinsiz blokszincirlerde, bir işlemi doğrulamak ve işlemek için binlerce düğümün fikir birliğine ihtiyacı vardır. İşlemler, doğrulanmayı bekleyen bir kuyrukta arabelleğe alınır, bu da mantıksal olarak artan gecikmeye neden olur. Genel blokszincirlerde, her düğüm, veri bütünlüğünü ve veri güvenliğini korumak için her bir işlemi doğrulamakta ve depolamaktadır. Ancak bu süreç ne yazık ki gecikmeye neden olmaktadır (Khan vd., 2021: 15). Dolayısıyla, blokszincir mimarileri, özellikle boyut arttıkça ciddi gecikme sorunlarıyla karşı karşıya kalmaktadır. Özel blokszincirler ise çok daha verimli olmalarına rağmen henüz gerekli standartlara ulaşamamışlardır (Casino vd., 2019: 69). Bununla birlikte, blokszincirdeki yüksek gecikme süresi, merkezi olmayan halka açık blokszincir ağlarında tutarlılığı sağlamak için kullanılabilir.

5.3.2. Organizasyonel Sorunlar

Örgütün içyapısı ile ilgili sorunları ifade eden organizasyonel sorunlarda altyapı eksikliği, nitelikli personel eksikliği, bilgi, anlayış ve farkındalık eksikliği ile teknolojiyi kullanma konusundaki isteksizlik engellerine yer verilmektedir.

5.3.2.1. Altyapı Eksikliği

Blokszincir teknolojisini yerleştirmek için aşılması gereken en önemli sorunlardan biri de gerekli olan altyapı eksikliğidir. Blokszincir teknolojisi doğası itibarıyla yüksek işlem gücü gerektiren bilgisayarlara ihtiyaç duymaktadır. Bu hem işletmeler hem de hükümetler için yüksek bir donanım maliyeti demektir. Daha sonra bu donanım üzerinde gerekli olan yazılımın ve veri tabanlarının kurulması gerekmektedir. Bunun için ise bir sonraki kısımda ele alındığı gibi nitelikli personele ihtiyaç vardır. Ayrıca blokszincir sürekli internet bağlantısı gerektirdiği için bunu sağlayacak altyapının da mevcut olması gerekmektedir. Deloitte (2022: 9) tarafından yapılan bir araştırmaya göre ankete katılan 1280 katılımcıdan yüzde 62'si altyapı eksikliğini blokszincirin benimsenmesi önündeki engellerden biri olarak gördüğünü belirtmiştir.

5.3.2.2. Nitelikli Personel Eksikliği

Herhangi bir teknolojiyi veya sistemi uygulamak için gerekli olan en önemli unsurlardan biri, destek altyapısıdır. Nitelikli insan kaynağı, bu destek altyapısının en önemli bileşenlerinden biridir. Blokzincir teknolojisi gelişme aşamasındadır ve bu alanda gerekli sayıda kalifiye profesyonel bulmak önemli bir zorluktur. Blokzincir her ne kadar güvenli bir platform olarak addedilse de yine de her teknolojiye olduğu gibi insan hatalarına açıktır ve düzenli olarak güncellenmesi gerekir. Nitelikli profesyonellerin yokluğunda, güvenli ve güvenilir mekanizmalar sağlamak için destek altyapısı sağlamak oldukça zordur (Alam vd., 2021: 13).

Blokzincir teknolojilerini geliştirmek ve kullanmak, bu alanda eğitimli profesyoneller gerektirmektedir. Bilgi ve iletişim teknolojilerini farklı endüstriyel alanlara dâhil etmek, bu endüstrileri verimli sistemlere dönüştüren etkili ve büyük adım olmuştur. Her ne kadar BİT uzmanları, çeşitli türde uygulamalar oluşturma ve yönetme yeteneğine sahip olsa da blokzincir teknolojisi endüstriyel uygulamalara entegrasyonda yeni zorluklar doğurmaktadır (Al-Jaroodi ve Mohamed, 2019: 36509).

BİT alanındaki önceki uygulamalar ile blokzincir oluşturmak için kullanılan temel teknolojiler birçok yönden ortaktır. Fakat işleme dayalı sistemler, dağıtık kayıt defterleri, kriptografik özetler, dijital imzalar ve güvenlik modelleri, yeni entegrasyon ve kullanım yöntemleri benzersizdir. Tamamen entegre blokzincir tabanlı endüstriyel uygulamalar oluşturmak için tasarım ve geliştirme ekiplerinin; çalıştıkları endüstriyel alan, kullanılacak BİT, blokzincir teknolojileri ve modelleri ile çeşitli yazılım ve sistem geliştirme süreçleri gibi çeşitli alanlarda bilgi sahibi olması gerekmektedir. Teknik ve profesyonel iş gücünde devam eden eksiklikler nedeniyle, bu projeler için gerekli profesyonelleri bulmak ve eğitmek zorlu bir süreçtir. Ayrıca, bu alanda ihtiyaç duyulan profesyonel işgücünü hızlı bir şekilde üretebilecek uygun ve etkili bir eğitim ve gelişim programlarına da ihtiyaç vardır (Al-Jaroodi ve Mohamed, 2019: 36509).

Devlet memurlarının gerekli becerilere sahip olmaması, blokzincir teknolojisinin kamu yönetiminde yaygınlaştırılamamasının önündeki en önemli engellerden birisidir. Açıkçası tüm paydaşların, başarılı bir şekilde uygulanması için blokzincir teknolojisi konusunda eğitime ihtiyacı olacaktır (Shang ve Price, 2019: 77). Bununla birlikte, blokzincir karmaşık bir teknolojidir ve blokzincir okuryazarlığı, yalnızca kullanıcı olarak

vatandaşlar için değil, aynı zamanda kamu hizmetlerinin yöneticileri ve çalışanlar olarak memurlar için de zorluk teşkil etmektedir. Blokzincirin yeni bir teknoloji olduğu göz önünde bulundurulduğunda, teknolojiye aşina olan uzmanların, programcılarının ve geliştiricilerin sayısı ve kamu hizmetleri için olanakları sınırlıdır (Thakur vd., 2020: 6). Çoğu memur bu tür bir bilgi ve deneyime sahip değildir ve kamu kuruluşlarının blokzincir teknolojisi uygulamasını geliştirmek için teknik uzmanları ve yetenekli personeli eğitmesi ve işe alması gerekmektedir (Hyvärinen vd., 2017: 77).

5.3.2.3. Bilgi Eksikliği, Düşük Anlayış ve Farkındalık

Değişim veya reform, bir değişim veya reform ihtiyacını öngören ve kabul eden bilinçli ve bilgili karar vericiler tarafından başlatılır ve yürütülür. Ekonomik ve siyasi bir sistemin insan kaynağı, öncelikle bir değişim veya reform ihtiyacının farkında olmalıdır. Değişimin gerekliliğine dair cehalet ve farkındalık eksikliği ile değişimin veya reformun nasıl yapılacağına dair bilgi eksikliği değişimi engelleyecektir (Demir ve Aktan, 2016: 231). Bununla birlikte toplumda bazı kesimler gerçek bir değişimin asla olmayacağına inanabilir. Bu inançsızlık ve karamsarlık, siyasi ilgisizlik yaratabilir ve değişim desteğini sınırlayabilir. Devlet politikalarının devam etmesi, kısa vadeli değişikliklerin uzun vadede kaynak ve güç dağılımını değiştirmeyeceği fikrini destekleyebilir (Demir ve Aktan, 2016: 236).

Blokzincire olan ilgi son iki üç yılda artsa da bu ilginin sebebi daha çok kripto paralarda yaşanan yüksek fiyat hareketleridir. Kripto paralardan ziyade altında yatan teknoloji ise halen hem bireyler hem özel sektör hem de kamu sektörü tarafından tam olarak anlaşılabilmiş değildir. Özel sektör blokzincir teknolojisinin geliştirilmesinde başı çekse de hükümetlerin blokzincirin benimsenmesi konusunda teşviki sınırlıdır.

5.3.2.4. Teknolojiyi Kullanma Konusundaki İsteksizlik

İş yapış şeklindeki mevcut alışkanlıklar, statükoculuğa katkıda bulunarak değişim veya reformu engelleyebilmektedir. Bu nedenle, değişim veya reform, geçiş ve uyum maliyetleriyle birlikte geldiğinden, çalışanların alışkanlıklarından vazgeçmesi ancak bugünkünden daha fazla fayda öngördükleri takdirde olacaktır (Demir ve Aktan, 2016: 235). Örneğin bundan on yıllar daktiloya alışkın olanlar, becerilerinin eskiyeceğini düşünerek bilgisayara karşı direnç göstermişlerdir (Jost, 2015: 607).

Yeni bir teknoloji hayata geçtiğinde bu teknoloji yeterince olgunlaşana kadar bu teknolojiye geçme konusunda isteksizlik olması oldukça olağan bir durumdur. Blokzincir için de durum aynıdır. Blokzincir teknolojisine intibak etmek, dijital teknolojileri yerleştirmek için halihazırda önemli bir dönüşüm geçirmiş olan endüstriler için bile, bir şeyleri yapmanın geleneksel yollarından tamamen uzaklaşmak demektir. Burada güçlü bir merkezi kurum yerine merkezi olmayan bir ağa güven ve yetki verilmektir. Birçok kurum için bu kontrol kaybı, son derece rahatsız edici olabilir (Swanson, 2016: 11). Bir blokzincirin yaklaşık yüzde 80'inin iş süreci değişikliği ve yüzde 20'sinin teknoloji uygulaması olduğu tahmin edilmektedir (Mougayar, 2015). Dolayısıyla fırsatların ve iş süreçlerinin nasıl değişeceğini anlamak için daha yaratıcı bir yaklaşıma ihtiyaç vardır.

Kamu yönetimi ise bu konudan daha çok muzdariptir. Blokzincir teknolojisinin kamu idarelerinde kullanılması konusunda kamu çalışanları aşağıdaki sebeplerden ötürü direnç gösterebilmektedirler (Cagigas vd., 2022: 346):

- Teknolojinin gerektirdiği ekonomik maliyetler ve/veya teknolojinin tam olarak olgunlaşmaması
- Mevcut çalışma kalıplarını değiştirmeye yönelik atalet
- Geçmiş eylemlerin sorgulanması endişesi
- İşini kaybetme korkusu
- Kamu idarelerinin kamunun gözüne açılmasına yönelik olumsuz tutumlar
- Bilginin uygunsuz şekilde açıklanmasından endişe etme
- Teknolojik deneyim ve farkındalık eksikliği
- Mevcut hiyerarşideki değişiklikler

Herhangi bir kamu kurumunu yöneten bürokratik idare, önceden tanımlanmış süreçler ve organize hiyerarşiler ile karakterize edilmektedir (Allessie vd., 2019: 8). Bu hiyerarşik yapıların, gücün birkaç üst düzey memurun elinde merkezileştirilmesini kolaylaştırmak için organize edildiği ileri sürülmüştür (Cagigas vd., 2022: 13913). Bu nedenle, teknolojinin statükodan yararlanan memurların direnişiyle karşılaşması muhtemeldir (Ooijen, 2017).

Memurlar için blokzincir uygulamasının doğuracağı başka bir önemli potansiyel risk, iş imkanlarının azalması ihtimalidir. Blokzincirin birçok bürokratik süreci

otomatikleştirme vaadi, kamu çalışanları tarafından icra edilen birçok işi ortadan kaldırma tehdidi oluşturmaktadır (Manski, 2017: 517) ve bu sürecin coğrafi olarak ve cinsiyete göre oldukça eşitsiz olması muhtemeldir. Blokzincir kullanımıyla gereksiz hale gelecek olacak işlerin yerini, otomatikleştirilmiş görevler ve sanal emek alacaktır. Düşük vasıflı işçiler muhtemelen bu süreçten daha yoğun bir şekilde etkilenecektir (Cagigas vd., 2022: 13914).

Özetle blokzincir teknolojisi, yönetim yapılarını ve hükümetlerin operasyonlarını yapılandırma şeklini değiştirerek devlet kurumlarını etkileme potansiyeline sahiptir (Sinclair vd., 2016: 23). Sistemin güçlü pozisyonlara sahip aktörleri mevcut olduğunda, blokzincir uygulamasını zorlaştıran bu kurumsal yapıları değiştirmek zorlaşmaktadır.

5.3.3. Çevresel Sorunlar

Bu kısımda blokzincirin hukuki altyapısına yönelik yasaların henüz oluşmamasından kaynaklanan sorunlar ile standartların eksikliği, örnek uygulamaların azlığı ve etik sorunlardan kaynaklanan engeller ele alınmaktadır.

5.3.3.1. Yasalara ve Düzenlemelere Uyum Sorunları

Yeni bir teknoloji ortaya çıktığında kamu idareleri tarafından yasalar ve ilgili düzenlemeler genellikle süreci hep geriden takip etmektedir. Bu gerçek kripto paralar özelinde blokzincir teknolojisinde de görülmektedir. Merkezi olmayan özellikleri ile en temel olarak Bitcoin'i ele alırsak, kripto paralar merkez bankalarının ekonomi politikalarını ve para miktarını kontrol etme yeteneğini zayıflatacaktır. Bu da hükümetin blokzincir teknolojilerine karşı temkinli olmasına neden olmaktadır. Fakat bunun en büyük nedenlerinden biri, kamunun bu yeni teknolojinin kullanımı için gerekli olan yasal ve regülatif altyapıyı henüz oluşturmamış olmasıdır.

Birçok ülkede blokzincir ve mevcut yasalar arasında çeşitli potansiyel çatışmalar ortaya çıkmaktadır (Filippi ve Hassan, 2016). Zincirdeki veriler için hangi tür yasal tanımlamanın yapılacağı ve ilave koşullar gerekip gerekmeyeceği, gerekecek ise bunların neler olacağı halen belirsizdir (Lemieux, 2019: 12). Başka bir potansiyel zorluk, blokzincirlerin düğümlerinin dünyanın farklı ülkelerinde konumlanmasından

kaynaklanmaktadır. Bu durumda yargı yetkisinin hangi ülkenin yasalarına dayalı olarak verileceği konusunda belirsizlikler bulunmaktadır (Sinclair vd., 2018: 642).

Blokzincir teknolojisi mülkiyet, mutabakat ve sorumlulukların teknik kanıtlarını sağlasa da, bu kanıtların yasal olarak desteklenmesi gerekmektedir. Hukuk sistemi, teknoloji ve teknik ihtilaflar söz konusu olduğunda geride kalmaktadır. Örneğin bir akıllı sözleşme, yüklenicileri teknik olarak bağlasa da, yasal sistem dünyanın hiçbir ülkesinde bunu hala doğrudan tanımamaktadır. Bu, bir sorun ortaya çıktığında ilgili taraflar için anlaşmazlıklara ve maliyetli süreçlere yol açacaktır. Bu tür sorunları doğrudan ele almak için kurallara, yasalara ve özel düzenlemelere ihtiyaç vardır. Düzenlemeler olmadan, blokzinciri kullanmak zordur (Al-Jaroodi ve Mohamed, 2019: 36509).

Örnek olarak, bir üretici bir tedarikçiyle malzeme alımları konusunda anlaşır ve bunu her iki tarafça onaylanan bir akıllı sözleşme kullanarak belgeler ve ardından dijital para birimini kullanarak ödeme yapar. Sipariş kararlaştırılan süre veya gerekli özellikler içinde teslim edilmediyse bir sorun olabilir. Bu sorunun hukuk sisteminin desteğiyle çözülmesi gerekebilir. Gerçek bir doğrulanmış sözleşmenin olmaması, hukuk sisteminin akıllı sözleşmeyi bağlayıcı bir anlaşma olarak kabul etmeyebileceği için bu büyük bir sorun haline gelebilir. Yasa, bağlayıcı anlaşmalar oluşturmada blokzincirin özelliklerinin teknik yeteneklerini kabul edecek şekilde genişlerse, bu hem kanun koyucu hem de taraflar için süreci daha az karmaşık hale getirilebilecektir. Blokzincirin yasal yönlerinin hukuk perspektifinden incelenip ele alınması ve onu desteklemek için uygulanabilir çözümlerin ve düzenlemelerin oluşturulması zorunludur (Al-Jaroodi ve Mohamed, 2019: 36509). Yetkililer bu teknoloji hakkında araştırmalar yapmalı ve yeni politikalar formüle etmeyi hızlandırmalıdır.

5.3.3.2. Standartların Eksikliği

Birçok yeni blokzincir tabanlı çözümler geliştirilse de, blokzincir teknolojisinde evrensel olarak belirlenmiş standartlar mevcut değildir. Bu, başlı başına bir sorun olmasının yanında, birlikte çalışabilirlik ve entegrasyon sorunlarına da sebep olmaktadır. Deloitte (2017) tarafından yapılan bir ankete göre, işletme yöneticilerin yüzde 56'sı teknik standartların, blokzincirin daha geniş çapta benimsenmesi için kritik olduğunu düşündüğünü ortaya çıkarmıştır. Bu yüzden kurum/kuruluşların kendi teknoloji

geliştirme süreçlerini yürütmek yerine, tek tip standartlar ve protokoller oluşturmak için daha iyi iş birliği yapmaları gerekmektedir.

Birleşik standartların eksikliği (örneğin terminoloji ve kavramlar netleştirilmesi, güvenlik riskleri ve güvenlik açıklarının belirlenmesi, dijital kimliklerin tasarlanması, referans mimarisi, sınıflandırılmaları, yasal olarak bağlayıcı akıllı sözleşmeler vb.), blokzincir teknolojisinin kamu sektöründe düzgün bir şekilde uygulanmasını ve kullanılmasına olumsuz etkide bulunmaktadır. Rana vd. göre (2022: 566) blokzincir teknolojisinde standart eksikliği, hızla büyüyen teknolojinin benimsenmesi için diğer zorlukları tetikleyen temel zorluklardan biridir. Buna göre standartların eksikliği, kamu sektörü kuruluşlarında blokzincirin kullanımıyla ilgili daha yüksek güvenlik sorunlarına ve gizlilik endişelerine yol açmaktadır. Bu nedenle, blokzincirin benimsenmesi için birleşik ortak standart oluşturmak, hükümetler için bir öncelik olmalıdır.

5.3.3.3. Örnek Uygulamaların Eksikliği

Her geçen gün uygulamaya yönelik yeni blokzincir çözümleri geliştirilse de bunların sayısı henüz yeterli seviyede değildir. Özellikle kamu sektörü, bu açıdan daha şanssız durumdadır. Fakat bu sadece blokzincire özgü bir olgu değildir. Özellikle bilgi teknolojileri bağlamında getirilen yenilikler, önce özel sektörde rüştünü ispat ettikten sonra kamu sektörü tarafından benimsenmeye başlamakta ve daha sonra kendine uygulama alanı bulabilmektedir. Küreselleşme ile bu teknolojinin en iyi uygulamalarının ortaya çıkması, farklı devlet kuruluşları tarafından örnek alınacak ve kendi ülkelerinde uygulama alanı bulacaktır.

5.3.3.4. Etik Sorunlar

Blokzincir teknolojisinin uygulanabilirliği önündeki bir diğer unsur, teknolojinin sebep olduğu etik sorunlardır. Teknoloji çevreye verdiği zarar konusunda eleştirilmektedir. Blokzincir teknolojisinin, özellikle halka açık blokzincirleri etkileyen ana dezavantajlarından biri, madencilik için kullanılan enerjidir. Çin'in başını çektiği Bitcoin madenciliği, dünyanın 159 ülkesinden daha fazla elektrik tüketmektedir (Casino vd., 2019: 70). Bu da madencilik için kullanılan enerjinin boşa harcandığı ve israf edildiği ve bu nedenle çevreye zarar verdiği düşüncesini doğurmaktadır. Her ne kadar bu iddia kısmen doğru olsa da madenciler ise aynı işlemi yapmak için mevcut sistemlerin çok daha

fazla maliyetli olduğunu ve enerji kullanımı gerektirdiğini iddia etmektedirler. Yine de bu endişe, enerji tüketimini azaltacak yollar geliştirilmesi gerektiğini öne çıkartmaktadır.

Etik sorunlardan bir diğeri de, kullanıcıların bir blokzincirdeki verilerini silip silemeyeceği sorunsalıdır. Prensip olarak, blokzincirler internetin kullanımı ile ilgili olan aynı düzenlemelere ve gizlilik yasalarına tabidir. Örneğin, Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR), bir kullanıcının bir internet servis sağlayıcısından verilerini arama sonuçlarından kaldırmasını isteyebileceği bir "unutulma hakkı" ilkesine sahiptir. Teorik olarak Blokzincirin de bu prensibi yansıtmaması gerekir. Sağlık, finans gibi alanlardaki hassas verilerin sahipleri, verilerinin tamamının veya bir kısmının blokzincirden kaldırılmasını talep edebilmelidir (Suominen vd., 2018: 19). Ancak blokzincir üzerindeki veriler değişmez olacak şekilde tasarlandığından bunun tam olarak nasıl yapılacağı net değildir.

Başka bir konu, blokzincirin gizlilik ve anonimlik sağlaması nedeniyle yasadışı işlemlerde kullanılabilmesi ve bu nedenle kara para aklama ve terörün finansmanı gibi suçlara konu olması sorunsalıdır. Kara para aklama, dünya GSYİH'sının yaklaşık yüzde 2-5'ine karşılık gelen 1-2 trilyon dolar kadar büyük bir küresel sorundur (UNODC, 2020). Bankalar ve yetkililer sorunla mücadele etmek için yılda yaklaşık 8 milyar dolar harcamaktadırlar. Zorunlu müşterini tanı (KYC) kontrollerine uymak için, dünya çapındaki bankaların yeni müşterilerden bireysel veya kurumsal kimlik belgesi ibraz etmelerini istemesi gerekmektedir. Bankaların ayrıca kara para aklamanın önlenmesi (AML) ve terörizmin finansmanı ile mücadele (CFT) süreçlerine bağlı kalma mecburiyeti bulunmaktadır (Suominen vd., 2018: 20). Konuyla ilgili küresel standartlar tam olarak yerleşmediğinden her bankanın farklı düzenleme gerekliliklerini karşılaması gerekmektedir.

Blokzincir kullanıcılarına anonimlik sağlasa bile bu, kötü niyetli kullanıcıların yasa dışı işlemlerde izlerini örtmelerine yardımcı olur mu? Bu soruya cevap olarak; şu anki bankacılık sistemi mevcut hali ile kara para aklama konusunda oldukça başarısız iken, suçluların blokzincir kullanarak çok az fayda sağlayabileceği şeklinde verilebilir. Başka bir yanıt ise, işlemlerin boyutuna bağlı olduğudur. Göreceli olarak küçük boyutlu yasa dışı işlemler için, izinsiz blokzincirler anonimlik sağlayabilir. Fakat, bankacılık

sistemlerinde dolaşan daha büyük miktardaki işlemler için, blokzincir altyapısı dolandırıcılık yapmayı veya kara para aklamayı zorlaştırabilir.

5.4. Blokzincir İhtiyacına Karar Verme Modelleri

Blokzincir teknolojisi, son yıllarda hayatın her alanında oldukça fazla dikkat çekmeye başlamış olsa da; geleneksel veri tabanlarından her zaman daha iyi bir seçenek değildir. Geleneksel veri tabanları sunduğu bazı avantajları ile hala blokzincirden daha iyi performans göstermektedir. Blokzincir, tarafların doğrudan işlem yapmadığı veya bir aracının olmadığı düşük güven ortamlarında özellikle değerlidir. Bilgi teknolojisi uzmanları ve bu teknolojiyle ilgilenen yöneticiler, hemen hemen her projede blokzincir kullanımını öngörseler de, özellikle veri yönetimi açısından, blokzincir kullanımının temel nedenlerini tam olarak anlamış değildirler. Örnek olarak, herhangi bir verinin saklanması gerekmiyorsa, blokzincir mevcut teknik çözümlere herhangi bir değer katmayacaktır. Benzer şekilde, bir sistemde veriyi üreten sadece bir merkez varsa, blokzincir özellikle işlem hızı performansı açısından geleneksel veri tabanlarının gerisinde kalacaktır (Greenspan, 2015). Öte yandan, işlem yapacak taraflar birbirlerine güvenmiyorsa ve bu işlemlerin kalıcı bir kaydı tutulması gerektiğinde blokzincirin kullanımı ise uygundur (Wüst ve Gervais, 2018: 46). Bu nedenle, blokzincir özellikli çözümleri benimsemeden önce, blokzincir teknolojisinin kullanım durumu gereksinimlerine uygunluğu incelenmelidir. Bu maksatla araştırmacılar tarafından blokzincirin uygulanabilirliği için çeşitli modeller oluşturulmuştur.

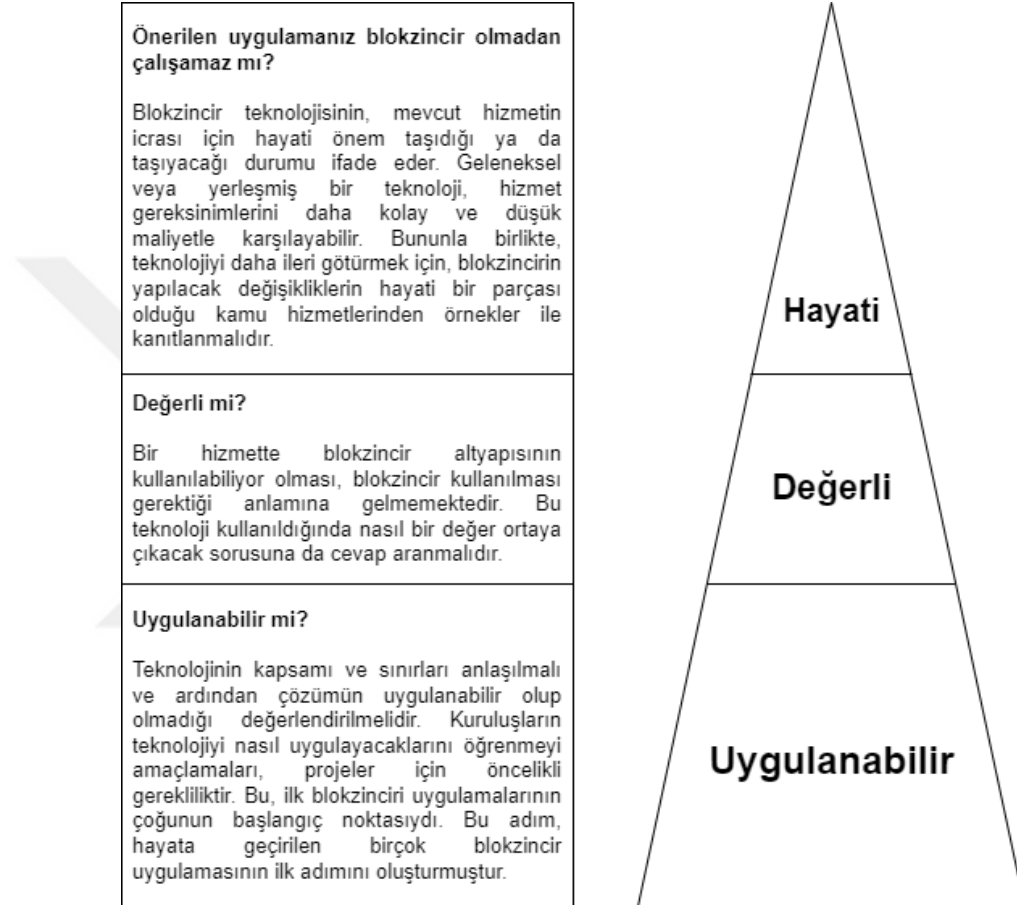
Geliştirilecek bir uygulamada veri kaydının tutulması gerekmiyorsa blokzincire gerek yoktur. Geleneksel veri tabanları ihtiyacınızı karşılıyorsa bu yöntemler tercih edilmelidir. Veri kaydının tutulması ihtiyacı mevcut fakat veri girişi sadece bir merkezden yapılacaksa o zaman da blokzincir kullanılmasına gerek yoktur. Bunların dışındaki durumlar için farklı modeller geliştirilmiştir. Bu modellerin bazıları aşağıda sıralanmıştır.

5.4.1. Deloitte Üç V Modeli

Üç V modeli, yeni bir teknolojinin viable (uygulanabilir), valuable (değerli) ve vital (hayati) olup olmadığına göre değerlendirilmesini esas alan ve öncelikli olarak Deloitte tarafından yapay zekâ gibi bilişsel teknolojiler için önerilmiş bir modeldir (Schatsky vd., 2015). Daha sonra ise OECD'nin bir alt kuruluşu olan Kamu Sektörü

İnovasyonu Gözlemevi (OPSI) tarafından blokzincir kullanım durumlarını analiz etmek için uygun ve yararlı oldukları tespit edilerek (Lindman vd., 2020: 12) blokzincir alanında kullanım durumları bağlamında dikkate alınacak hususlar oluşturmak üzere uyarlanmıştır.

Şekil 9: Üç V Modeli



Kaynak: Schatsky vd., 2015: 13

Modelde üç düzey bulunmaktadır. Uygulanabilir düzeyde, blokzincirin bir hizmet için uygun olup olmadığı sorgulanır. İkinci düzey değeri ölçer. Blokzincir bir hizmet için değerliyse, o zaman net faydaları bulunmalıdır. Üçüncü ve en yüksek düzey, blokzincirin hayati önem derecesidir. Bu düzeyde, blokzincir belirli bir hizmet için bir "zorunluluktur" çünkü hizmetin gereklilikleriyle uyumlu benzersiz özelliklere sahiptir (Lindman vd., 2020: 13). Kamu kurumlarına getirilmesi planlanan herhangi bir potansiyel blokzincir hizmeti, bu kontrol listesi kullanılarak analiz edilebilir.

5.4.2. Peck Modeli

Peck'e göre (2017: 38) blokzincir teknolojisi her ne kadar birçok avantajı kendinde bulundursa da blokzincirin her sorunun çözümü olmadığını belirterek “bu teknolojiye gerçekten ihtiyacınız var mı?” sorusunu sormaktadır. Blokzinciri kullanmamak için kullanmaktan daha fazla sebep olduğunu iddia etmektedir.

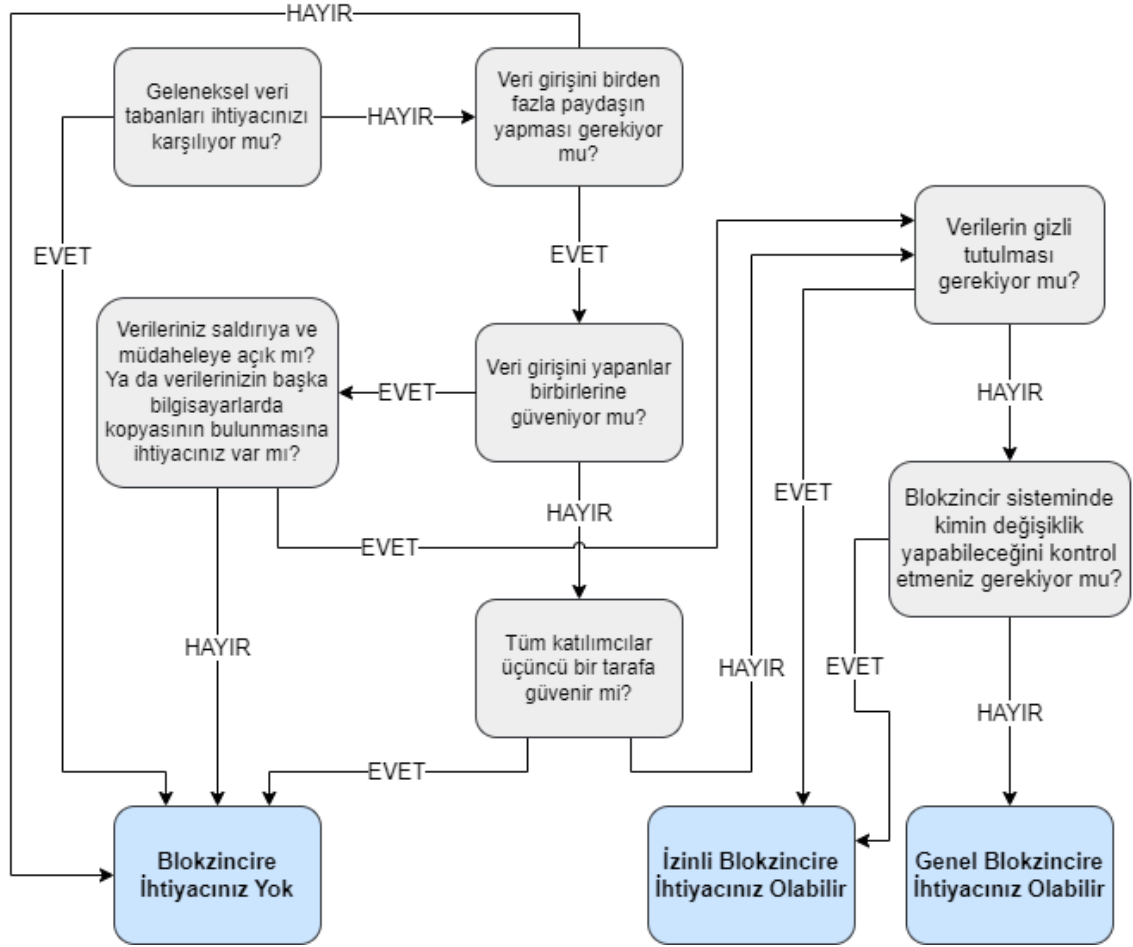
Şekil 10'da sunulan bu model ağacı “Geleneksel veri tabanları ihtiyacınızı karşılıyor mu?” sorusu ile başlamaktadır. Eğer sorunun cevabı evet ise blokzincire ihtiyacınız olmadığı çok açıktır. Hayır ise ikinci soru olan “Veri girişini birden fazla paydaşın yapması gerekiyor mu?” sorusu gelmektedir. Bu sorunun cevabı hayır ise yine blokzincire ihtiyacınız yok demektir. Bu soru blokzincirin kamu yönetimi bağlamında değerlendirmesi açısından önemlidir. Çünkü kamu idareleri belirli alanlarda veri tabanını yöneten tek taraftır. Dolayısıyla veri girişini tek bir paydaş yapacak ise bu durumda blokzincir kullanımının sisteme katacağı bir katma değer bulunmayacaktır.

Veri girişi birden fazla paydaşın yapması gerekiyorsa, paydaşların birbirlerine olan güveni sorgulanır. Paydaşlar arasında güven sorunu yoksa ve verilerin müdahaleye açık değilse ya da başka bir yerde kopyasının bulunması gerekmiyorsa yine blokzincir kullanmaya gerek yoktur.

Paydaşlar arasında güven sorunu yok fakat verilerin başka bir bilgisayarda ya da veri tabanında tutulması gerekiyorsa verilerin gizlilik ihtiyacına göre kontrol yapılır. Verilerin gizli tutulması gerekiyorsa izinli blokzincire ihtiyaç olabilir. Verilerin gizli tutulması gerekmiyorsa ağda kimin değişiklik yapacağı kontrol edilmek isteniyorsa yine izinli blokzincir tercih edilebilir.

Blokzincir ağında kimin değişiklik yapabileceğini kontrol etmek gerekmiyorsa genel blokzincir kullanılabilir. Veri girişi birden fazla paydaş tarafından yapılıyorsa fakat birbirlerine güvenmiyorsa, güvenilir bir üçüncü taraf mevcudiyeti sorgulanır. Varsa blokzincir kullanımına gerek yoktur. Yoksa verilerin gizlilik ve değişiklik denetimi ihtiyacına göre tekrar kontrol edilerek uygun blokzincir sınıfı seçilebilmektedir. Şekil 10'da Peck tarafından blokzincir teknolojisine ihtiyaç olup olmadığı, ihtiyaç varsa ne tür bir blokzincir sistemine ihtiyaç olduğunu belirlemek maksadıyla sunulan model görülmektedir.

Şekil 10: Peck Modeli Akış Şeması

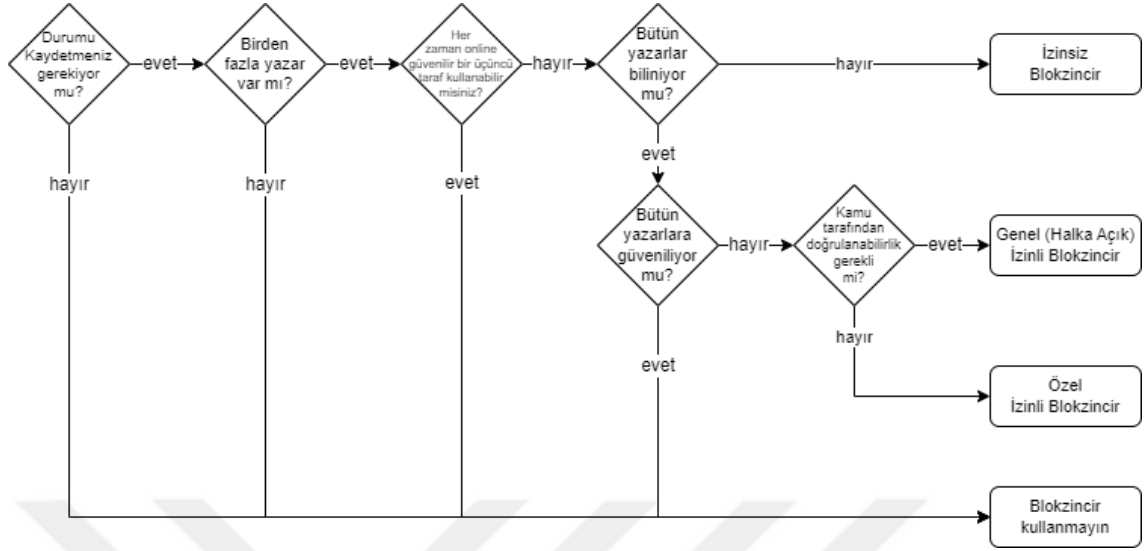


Kaynak: Peck, 2017: 39

5.4.3. Wüst ve Gervais Modeli

Wüst ve Gervais (2018) tarafından geliştirilen bu model diğerleri ile benzer şekilde birden fazla yazarın varlığını sorgulayarak başlamaktadır. Fakat daha çok her zaman çevrimiçi olan güvenilir bir üçüncü tarafın varlığına dikkat çekmektedir. Her zaman çevrimiçi olan güvenilir bir üçüncü taraf mevcutsa blokzincir kullanmaya gerek yoktur. Mevcut değil ve bütün yazarların kimliği bilinmiyorsa izinsiz blokzincir kullanılmalıdır. Bütün yazarların kimliği biliniyor ve yazarlara güveniliyorsa blokzincir kullanmaya gerek yoktur. Yazarlara güvenilmiyorsa ve kamu tarafından doğrulanabilirlik gerekli ise halka açık bir izinli blokzincir kullanılabilir. Yazarlara güvenilmiyorsa ve kamu tarafından doğrulanabilirlik gerekli değilse, özel izinli blokzincir kullanılabilir.

Şekil 11: Wüst ve Gervais Modeli Akış Şeması



Kaynak: Wüst ve Gervais, 2018: 47

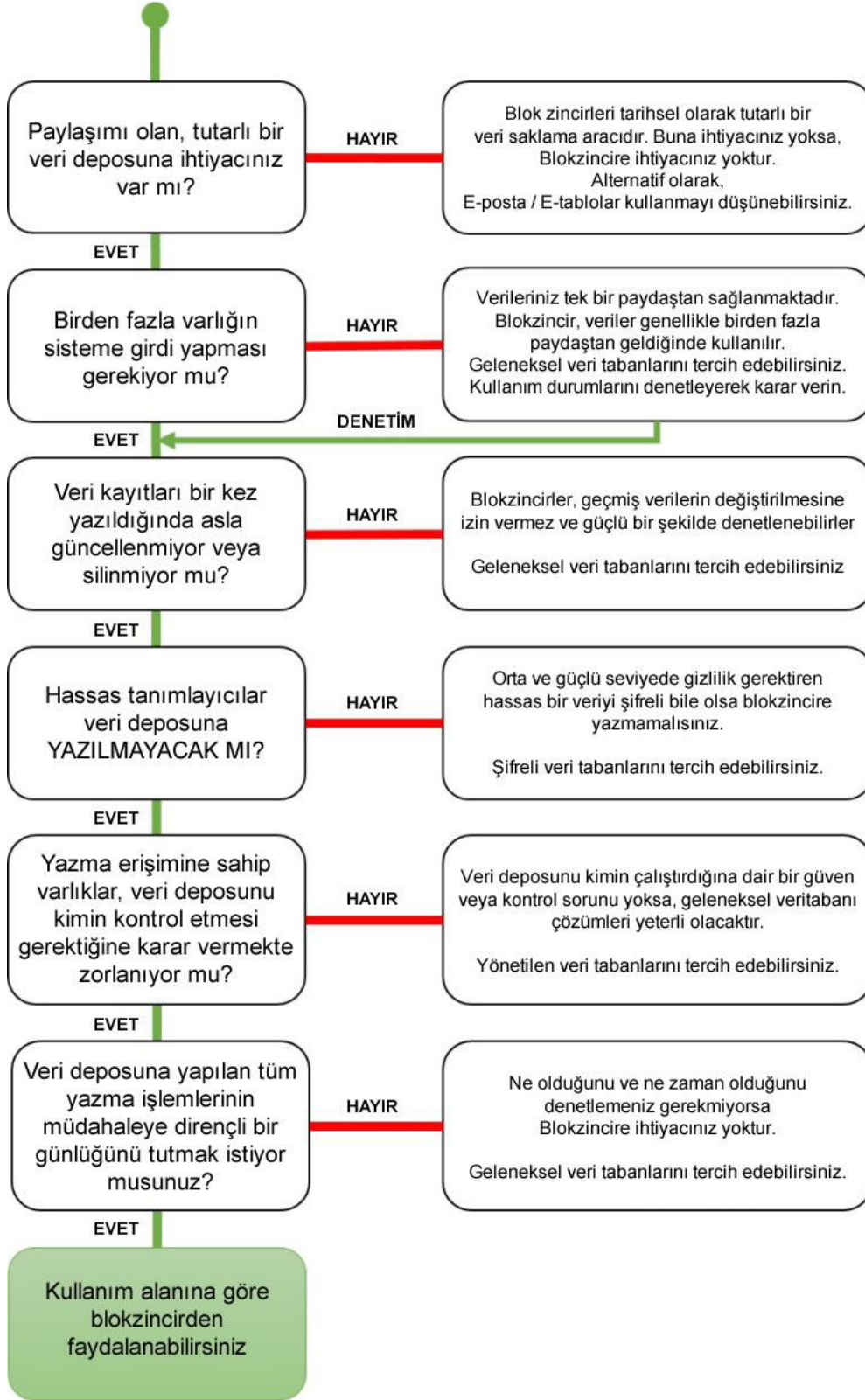
5.4.4. ABD Ulusal Güvenlik Bakanlığı Modeli

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü tarafından yayınlanan ve blokzincir teknolojisinin başarılı bir şekilde benimsenmesi için en iyi uygulamaları araştıran bir rapor yayınlanmıştır. Bu raporda ABD Ulusal Güvenlik Bakanlığı (DHS) tarafından geliştirilen ve kurumların blokzincire ihtiyacı olup olmadığının belirlemesi için yol gösterici nitelikte bir akış şeması sunulmuştur. Bu akış şeması Şekil 12’de sunulmuştur. Raporda blokzincir teknolojisini daha iyi kullanabilmek için, önce teknolojinin hangi ihtiyaçları karşıladığını sorgulamak ve ardından blokzincir paradigmasına uyabilecek sistemleri belirlemek gerekmektedir.

Buna göre faaliyetler veya sistemler aşağıdaki gibi özellikler gerektiriyorsa blokzincir teknolojisi çözümlerine başvurmak uygun olabilir (Yaga vd., 2018: 41):

- Birden fazla katılımcının bulunması,
- Katılımcıların dağıtık olması,
- Güvenilir bir üçüncü tarafın olmayışı,
- İş akışının doğası gereği işleme dayalı olması (ör. taraflar arasında dijital varlıkların/bilgilerin aktarımı),

Şekil 12: ABD Ulusal Güvenlik Bakanlığı (DHS) Modeli Akış Şeması



Kaynak: Yaga vd., 2018: 42

- Küresel olarak az bulunan bir dijital tanımlayıcıya (ör. dijital sanat, dijital arazi, dijital mülkiyet) ihtiyaç olması,
- Merkezi olmayan bir adlandırma hizmetine veya sıralı kayıt defterine ihtiyaç duyulması,
- Kriptografik olarak güvenli bir sahiplik sistemine ihtiyaç duyulması,
- Uzlaşma ve uyuşmazlık çözümlerine yönelik manuel çabaları azaltma veya ortadan kaldırma ihtiyacı,
- Düzenleyiciler ve düzenlenen kuruluşlar arasındaki faaliyetin gerçek zamanlı izlenmesini sağlama ihtiyacı,
- Dijital varlıkların tam kaynağına ve katılımcılar arasında paylaşılacak eksiksiz bir işlem geçmişine ihtiyaç duyulması.

Bu model, diğer modeller ile karşılaştırıldığında hangi blokzincir türünün kullanılması ile ilgili değil, daha çok genel olarak blokzincir kullanılmalı mı kullanılmamalı mı sorusuna odaklanmaktadır. Her maddede daha spesifik sorular sorularak olumsuz cevaplar karşısında geleneksel veri tabanlarının kullanımının değerlendirilmesi gibi alternatif çözüm önerileri sunulmaktadır.

5.4.5. Casino, Dasaklis ve Patsakis Modeli

Başka bir araştırmada (Casino vd., 2019), blokzincir teknolojisinin etkileyeceği belirlenen sektörlerin gereksinimlerine göre (Tablo 5) blokzincir tabanlı çözümlerin uygunluğunu değerlendirmek için bir çerçeve (Tablo 6) geliştirmiştir. Bu çerçevede blokzincirin geleneksel veri tabanlarına karşı potansiyeli, gerekli güven varsayımları, bağlam gereksinimleri, performans özellikleri ve gerekli fikir birliği mekanizmaları olmak üzere dört ana başlıkta değerlendirilmektedir.

Her bir ön koşulun alaka düzeyini ölçmek için üç düzeyli bir ölçek (düşük, orta ve yüksek) kullanılmaktadır. Bu çerçeve, sistemlerinin blokzincir tarafından geliştirilip geliştirilmeyeceğini değerlendirmek isteyen uygulayıcılar için kapsamlı bir araç olarak kullanılabilir.

Tablo 5: Blokzincir Uygulama Alanlarının Gerek Duyduğu Özellikler

*Kontrol (✓) gerekliliğin zorunlu olduğunu, (O) ise duruma bağlı olduğunu göstermektedir.

	Ölçeklenebilirlik	Gizlilik	Birlikte Çalışabilirlik	Denetim	Gecikme	Görünebilirlik
Finans	✓	O	✓	✓	✓	✓
Vatandaşlık Hizmetleri		✓	✓	✓		
Doğruluk Teyidi				✓		✓
Yönetim	O	✓	✓	✓		
IoT	✓	✓			✓	
Sağlık	✓	✓	✓	✓		
Gizlilik ve Güvenlik		✓		✓		
Ticaret	O	O		✓	O	
Eğitim			✓	✓		
Veri Yönetimi	✓		✓	✓	O	✓

Kaynak: Casino vd., 2019: 69

Güvenilirlik açısından blokzincir, veri tabanlarının dayandığı güvenilir üçüncü tarafların kullanımını önler ve böylece içeriklerin güvenilirliğini ve doğrulanabilirliğini artırır. Blokzincir, işlemlerin ve operasyonların izlenmesi gerektiğinde (sıralı olaylar zinciri) veya operasyonlar güçlü güvenlik ve gizlilik gerektirdiğinde (merkezi veri yapıları, merkezi olmayan yapılara göre kötü niyetli saldırılara karşı daha savunmasızdır) de uygundur. Bakım ile ilgili olarak, blokzincir barındırma gerektirmediği için önemli bir maliyet düşüşü sağlayabilir. Son olarak, blokzincirdeki mutabakat mekanizmaları, birden çok veri kaydedicinin, veri tabanını değiştirmesine ve tüm düğümlerin kanıtlanabilir bir şekilde hemfikir olduğu yetkili bir işlem günlüğü oluşturmaya olanak sağlar (Casino vd., 2019: 68-69).

Tablo 6: Geleneksel Veri Tabanlarına Karşı Blokzincirin Niteliklerinin ve Ön Koşullarının Analizi

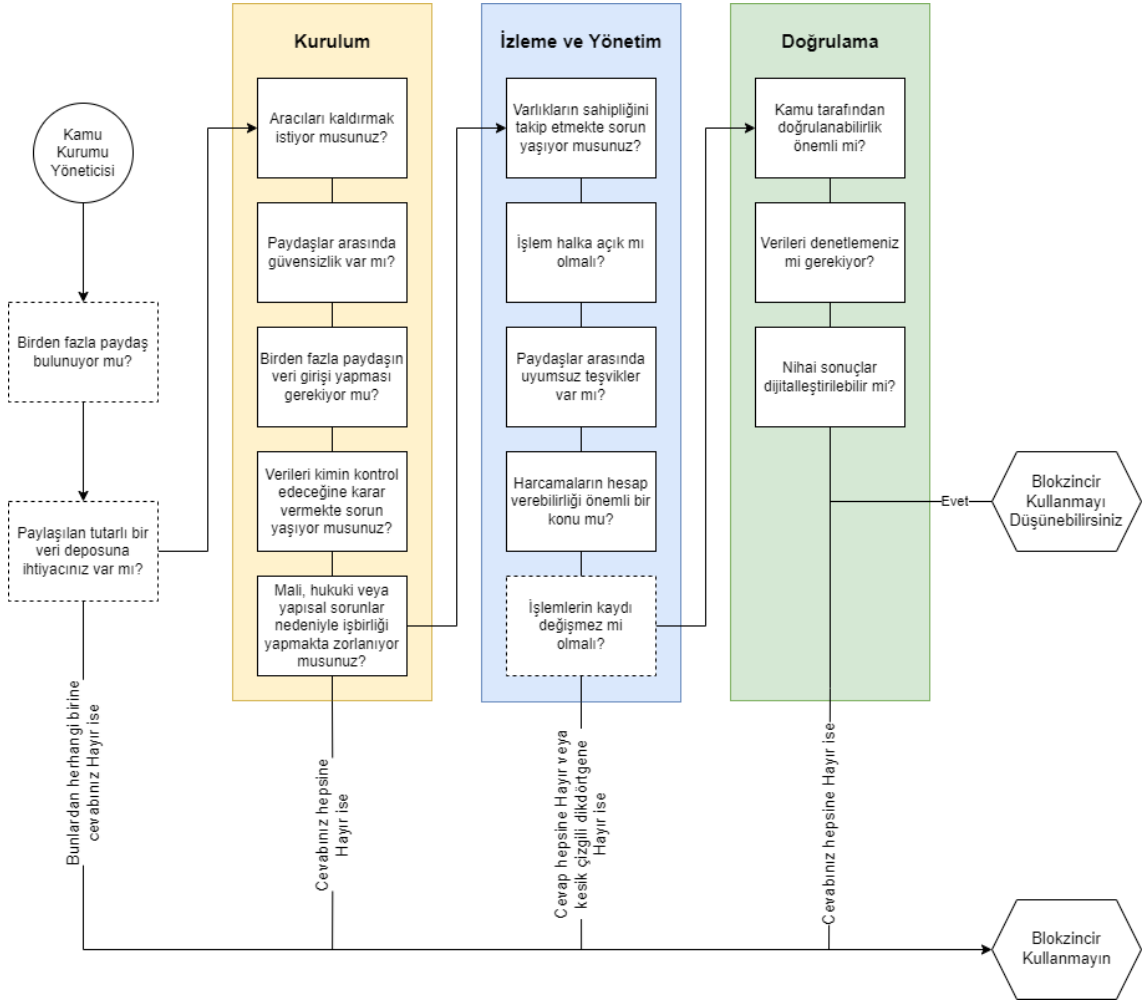
Öznitelikler	Önkoşullar ve belirleyiciler	Blokzincir Mimarisi		
		İzinsiz	İzinli	Veri Tabanı
Güven	Güvenilir Üçüncü Tarafların Eksikliği	Yüksek	Yüksek	Düşük
	Hesap verebilirlik	Yüksek	Yüksek	Yüksek
	Değişmezlik	Yüksek	Yüksek	Orta
	Birden çok güvenilir olmayan yazar	Yüksek	Yüksek	Düşük
	Eşler arası işlemler	Yüksek	Yüksek	Düşük
Bağlam	İşlemlerin izlenebilirliği	Yüksek	Yüksek	Düşük
	İşlemlerin doğrulanabilirliği	Yüksek	Yüksek	Düşük
	Veri/işlem noter onayı	Yüksek	Yüksek	Düşük
	Veri şeffaflığı	Yüksek	Yüksek	Düşük
	Güvenlik	Yüksek	Yüksek	Düşük
	Gizlilik	Yüksek	Orta	Düşük
Performans	Gecikme ve işlem hızı	Düşük	Orta	Yüksek
	Bakım maliyetleri	Yüksek	Yüksek	Düşük
	Fazlalık	Yüksek	Yüksek	Orta
	Ölçeklenebilirlik	Düşük	Orta	Yüksek
Mutabakat	Angajman kuralları	Yüksek	Yüksek	Düşük
	Doğrulamaya duyulan ihtiyaç	Yüksek	Yüksek	Düşük
	Farklı yazarların işlemleri arasındaki otonom/dinamik etkileşimler	Yüksek	Yüksek	Düşük

Kaynak: Casino vd., 2019: 69

5.4.6. Oxford GO Lab ve CIPFA Modeli

Blokzincir teknolojinin geniş çapta benimsenmesinin önündeki ana engellerden biri, teknoloji hakkında yeterli bilgi eksikliğidir. Bu eksiklik, kamu politikası sonuçlarını daha iş birlikçi yollarla iyileştirmek için teknolojinin nasıl kullanılacağına ilişkin tartışmaları engelleyebilir. Bu yüzden blokzincir tabanlı çözümleri uygulama kararı verilirken, ihtiyaç odaklı bir yaklaşım benimsenmelidir (Shiva vd., 2023: 51).

Şekil 13: Blokzincirin Benimsenmesine Yönelik Karar Ağacı



Kaynak: Shiva vd., 2023: 52

Kamu kurumu yöneticilerine karar verme süreçlerinde yardımcı olmak için, Oxford Üniversitesi bünyesindeki GO Lab (Hükümet Sonuçları Laboratuvarı) ile İngiltere merkezli bir uluslararası kamu muhasebe standartları belirleme organı olan CIPFA tarafından bir çerçeve hazırlanmıştır. Bu çerçevede uygulayıcıları iş birliğinin üç aşaması boyunca temel hedefleri dikkate almaya teşvik eden bir karar mekanizması önerilmiştir. Şekil 13'te sunulan çerçeve, kurumların yaptığı anket sonuçları dikkate almakta ve neyin işe yaradığına dair mevcut kanıtları sentezlemektedir. Karar vericiler, bu basitleştirilmiş mantık şeması üzerinde çalışarak aşağıdakiler üzerinde düşünebilir ve blokzinciri uygun bir çözüm olarak değerlendirmek amacıyla sistematik bir araç olarak kullanabilirler (Shiva vd., 2023: 51):

- potansiyel ortaklar arasındaki güven açığı,
- veri katkısı ve sahiplik kontrolü,
- değişmez kayıtların gerekliliği,
- yanlış hesaplanmış teşvik riski,
- iş birliğinin sonuçlarının nasıl değerlendirileceği.

Çerçeveye göre karar alırken odak noktası, teknolojinin basitçe uygulanabilir olmaktan ziyade ne zaman gerekli olabileceğini belirlemek olmalıdır. Paydaşlar, temel hedefleri ve tasarım özelliklerini göz önünde bulundurarak, blokzincir teknolojisinin değer katıp katmadığını ve belirli bir iş birliği projesi için hayati önem taşıyıp taşımadığını belirlemelidir. Çerçeve, blokzincir teknolojisi hakkındaki bilgi eksikliğini gidermeyi ve uygulayıcılara teknolojinin benimsenmesi konusunda bilinçli kararlar vermeleri için rehberlik sağlamayı amaçlamaktadır (Shiva vd., 2023: 51).

5.5. Kamuda Blokzincirin Uygulanabilirliğinde Kritik Başarı Faktörleri

Bu bölüme kadar blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği önündeki engeller ele alınmıştır. Bir blokzincir projesi hayata geçirilirken bu engellerin ortadan kaldırılması, bir yönüyle projenin başarıya ulaşması için destekleyici birer faktör olarak kendini gösterir. Bu başlıkta bunların dışında kalan ve teknolojinin hayata geçirilmesinde önemli olan kritik başarı faktörlerine yer verilmektedir.

Blokzincir teknolojisinin yıllar süren geliştirilme çabalarına rağmen gerçek hayattaki uygulama örnekleri halen sınırlı sayıdadır. Bu doğrultuda kamu sektörü bağlamında teknolojinin tamamen veya daha geniş bir projenin parçası olarak kullanım örneklerine üçüncü ve dördüncü bölümde yer verilmiştir. Buna göre teknoloji kamu yönetimini ilgilendiren kimlik yönetimi, kamu ihale sistemleri, sağlık hizmetleri, varlık kaydı, vergilendirme vb. alanlarda kendine kullanım alanı bulmaktadır. Ancak, hayata geçirilen blokzincir uygulamaları için önemli olan, bu uygulamaların çıktılarının, son kullanıcı olan vatandaşların kamu hizmetine ulaşmalarında ne derece katkı sağlayacağıdır. Bu noktada, bir kamuda blokzincir projesinin uygulanabilirliği açısından önemli olan kritik başarı faktörleri aşağıda özetlenmektedir.

5.5.1. Net Katma Değer Faktörü

Bir kamu hizmeti projesi blokzincir tabanlı olarak gerçekleştirmek istendiğinde göz önünde bulundurulması gereken en kritik başarı faktörü, proje ile ortaya çıkması beklenen faydanın veya katma değerın açıkça belirlenmesidir. Bu husus blokzincir ihtiyacına karar verme modelleri kısmında, Deloitte Üç V Modelinin “değerli mi?” veya Peck Modelinin “bu teknolojiye gerçekten ihtiyacınız var mı?” sorularında da kendisini göstermektedir. Nitekim danışmanlık firması Gartner Insight, blokzincir projelerinin yüzde 90'ının çoğunluğa yetişememe korkusuyla yürütüldüğünü, gereksinimlerini karşılamak için aslında blokzincire ihtiyaç duymadıklarını veya mevcut BT altyapısı için uygun olmayan çözümlerle sonuçlandığını öne sürmektedir (Furlonger ve Valdes, 2017).

Pandey'e (2020) göre blokzincir teknolojisinin devlet kurumlarında yaygınlaştırılması için öncelikle çözülmekte olan sorunun belirlenmesi ve temel performans göstergeleri (KPI'ler), katılımcı teşvikleri, teknoloji uyumluluğu ve gerekli yatırımlar dâhil olmak üzere hizmetin gerekçesini tanımlamak için yeterli ayrıntının sağlanması gerekmektedir. Bu süreç, blokzincirin, sorunu çözmek için en basit ve en iyi yaklaşım olduğunu kanıtlamalıdır.

Yukarıda bahsedilen kullanım alanları düşünüldüğünde şu soruları da sormak gerekmektedir (Spielman, 2018: 5):

- Blokzincir teknolojisini kullanmadan bu teknolojinin vadettiği blokzincir tabanlı çözümlere ulaşılabilir mi?
- Eğer cevap evet ise; bu çözüm neden halihazırda uygulanmıyor?
- Blokzincir çözümünün yerine bu çözüm mü tercih edilmelidir?
- Cevap hayır ise, blokzincir tabanlı çözümün getirdiği ekstra katma değer nedir?
- İstenilen faydalar blokzincir tabanlı çözümü uygulamak için gerekli olan zaman, maliyet ve eğitim ihtiyaçlarına katlanmaktan daha avantajlı mıdır?

Dolayısıyla bir kamu hizmeti projesi tasarlanırken, blokzincir altyapısı kullanılmasının projeye katma değer sağlayıp sağlamayacağı net olarak belirlenmelidir.

5.5.2. Teknolojinin Uygunluđu

Blokszincir tabanlı kamu hizmetleri geliştirilirken göz önünde bulundurulması gereken ikinci önemli etken, sunulacak hizmetler için bu teknolojinin uygun olup olmadığı hususudur.

Blokszincirin faydalarının farkına varmak, hükümet süreçlerinin ve hükümete yüklenen koşul ve gereksinimlerin anlaşılmasını gerektirir. Hizmetlere eşit bir şekilde erişim, şeffaflık, hesap verebilirlik ve mahremiyet gibi kamusal değerleri karşılayan uygun bir kamu yönetiminin işleyişini sağlamak için uyarlanan yapının toplumsal gereklilikleri dikkate alması gerekir. Blokszincir teknolojisinin faydaların çođu, diğer teknolojik araçlar kullanılarak da gerçekleştirilebilir. Bu, teknolojinin hala gelişmekte olduğunu ve dolayısıyla değişime tabi olduğunu hesaba katarken, hangi faydaların blokszincire özgü olduğu ve hangi durumlarda istenen çözümün blokszincir olduğu sorusunu gündeme getirir (Ølnes vd., 2017: 360).

Teknolojinin uygunluđu hususu, bir önceki kısımda Deloitte Üç V Modelinin “uygulanabilir mi?” sorusu ile ele alınmıştır. Ayrıca DHS modelinde (Yaga vd., 2018: 42) blokszincir değerlendirmesi için kullanılan; paylaşılan tutarlı veri depolama ihtiyacı, verilere birden fazla katılımcının katkıda bulunup bulunmadığı, değişmezlik, hassas veri eksikliği, veri depolama kontrolündeki değişiklikler ve kurcalamaya karşı korumalı günlük kaydıyla ilgili sorgulamalar da teknolojinin kamu hizmeti için uygunluđu ile ilgili kriterler olarak sıralanmıştır. Bu farklı kriterlerin önemi, kullanım durumuna ve projenin özelliklerine bağlıdır. Ancak genel olarak, teknolojinin uygunluđu bir proje için kritik bir başarı faktörüdür.

5.5.3. Paydaşların Sürece Dâhil Edilmesi

İlgili paydaşları belirlemek ve onları sürece dâhil etmek, herhangi bir geliştirme projesi için önemlidir, ancak özellikle teknik yeniliği ve tüm paydaş ağlarını yerleşik hale getirme ihtiyacı nedeniyle bir blokszincir projesi için daha da önemlidir (Lindman vd., 2020: 30).

Paydaş teorisi, paydaşların örgütsel planları etkilediğini iddia eder. Bu nedenle, herhangi bir örgütsel kararın başarısı veya başarısızlığı, birden çok paydaşın algısı tarafından belirlenmektedir. Freeman (1984: 46), paydaşları "bir kuruluşun hedefine

ulařılmasını etkileyebilen veya bundan etkilenen herhangi bir grup veya birey" olarak tanımlamaktadır. Bu nedenle paydař teorisi, bir kuruluřun; müşteriler, çalışanlar, tedarikçiler, topluluklar vb. gibi kuruluřun başarısını etkileyebilecek kilit gruplarla ilişkilerini yönettiğini öne sürer.

Hükümetler, tüm olası faydaları elde etmek ve kurum ve kuruluřlarında blokzinciri ölçeklendirmeye yardımcı olmak için gereken yönetiřimi oluřturmalıdır. Teknolojiyi etkili bir řekilde geliřtirmek ve yönetmek için kuruluřların, yazılım geliřtirmeyi başarıyla yürütebilen daha büyük bir çalışan havuzunu iře alması gerekecektir (Pandey, 2020). Bununla birlikte ağıdaki önemli aktörler arasında, genellikle blokzincir yazılımı için harici uzmanlık saėlayan teknoloji řirketleri bulunmaktadır. Bir kamu kurumu, blokzincir altyapısı kullanarak bir kamu hizmeti uygulaması geliřtirmek istediğinde, teknolojiyi saėlayan řirketlerden veya giriřimlerden hizmet satın alır. Halka açık ortamlarda bu, blokzincir teknolojisinin bir kamu ihale süreci aracılığıyla tedarik edilmesi ve yönetilmesi anlamına gelmektedir.

Bir blokzincir ağının deėeri, daha fazla kullanıcı katıldıkça artmaktadır. Fakat birden fazla paydařın dâhil olması karmařıklığı da beraberinde getirir. Bu nedenle, başarılı, uzun vadeli kurumsal sürdürülebilirlik için paydař ilişkilerinin etkin bir řekilde yönetilmesi gerekmektedir (Mishra vd., 2023). Paydařların sürece dâhil edilmesi, olası problemleri iř birlikçi bir řekilde çözebilmeyi kolaylařtırır. Daha fazla taraf sorunları çözmek için birlikte çalıştıkça sorunların çözülmesi daha olasıdır. Dolayısıyla bir projede paydařları yönetmek ve onların sürece dâhil olmasını saėlamak kritik bir başarı faktörüdür.

5.5.4. Kullanıcı Odaklılık

Blokzincir teknolojisinin "kullanılabilirliği", ana akım benimseme için önemli bir engeldir. Kullanılabilirlik terimi, yazılım ve diėer teknolojik uygulamalar gibi ürünlerin gerekli hedeflere etkili ve verimli bir řekilde ulaşmak için kullanılabileceėi kolaylık derecesini ifade etmektedir. Bilgi ve teknik beceri eksikliği, çeřitli vatandaş gruplarının blokzincir teknolojisinden yararlanmalarını engellemektedir. Bu nedenle, sezgisel blokzincir arayüzleri geliřtirilmeli ve daha fazla kullanıcıya sunulmadan önce bir dereceye kadar blokzincir okuryazarlığı arttırılmak gerekmektedir. Son olarak, blokzincir altyapısı, sürekli olarak internet baėlantısına ve dijital cihazlara eriřim gerektirir ki bu,

özellikle az gelişmiş ülkelerde, belirli bağlamlarda çoğu vatandaş için her zaman geçerli değildir (Cagigas vd., 2022: 13915).

Güncel yazılım yaklaşımlarının çoğu, tasarım ve geliştirme sürecinde aktif katılımcılar olarak müşterilerin ve kullanıcıların önemini vurgulamaktadır. Birçok mevcut blokzincir projesi, bir hizmet için belirli bir fikri uygulamayı amaçlayan teknoloji süreçleri olarak başlamıştır. Ancak müşteriyi kontrol altına almak ve son kullanıcı girdilerini elde etmek hizmet tasarımı için önemli kabul edilir (Lindman vd., 2020: 31).

Bir kamu hizmetini blokzincir altyapısı ile sunmayı amaçlayan bir projede son kullanıcının vatandaşlar olduğu hususu her zaman göz önünde bulundurulmalıdır. Başarılı olmak için, bir blokzincir uygulamasının, tüm vatandaşların, hatta en teknik olmayan kullanıcıların bile anlayabileceği bir düzeye basitleştirilmesi gerekir. Bu nedenle teknolojinin kullanıcılara bakan arayüzü sade ve anlaşılır olmalıdır. Bununla doğrultulu olarak, blokzincir projeleri tasarlanırken teknoloji uzmanlarına güvenildiği kadar vatandaşların taleplerine ve temsiliyetine de önem verilmelidir (Hargrave ve Karnoupakis, 2021). Bu yüzden, blokzincir hizmetleri teknoloji odaklı projeler olarak görülmemeli, önceliğin vatandaşların hizmetlere erişimini kolaylaştırmak olduğu unutulmamalıdır. Dolayısıyla kullanıcı odaklılık, kamuda blokzincir projelerinin başarıya ulaşmasında kritik bir faktör olarak kendini göstermektedir.

5.5.5. Test Etme

Teknolojik uygunluk faktörü ile üzerinde durulması gereken bir diğer aşama test veya deney aşamasıdır. Deney aşaması uygunlukları takip eder, çünkü denemenin uygulanabilir kullanım durumları üretebilmesi için önce uygunlukların var olması gerekir. Kullanım durumlarının tanımlanması ve geliştirilmesi, aktörlerin uygunlukları tanımasına da yardımcı olur. Bir blokzincir uygulaması hayata geçirilmeden önce sistemin çalıştığı test edilmelidir. Bunun için, kurum içindeki kullanım durumlarını belirlemek, geliştirmek ve test etmek maksadıyla bir deneme aşamasına ihtiyaç vardır. Test etme, aynı zamanda nihai sonuçları üretmek için gerekli bir eylemdir ve bir teknolojinin kullanım senaryolarını araştıran ve onu aktörlerin kullanması için hazırlayan bir eylemdir (Wenyu vd., 2019: 59).

Denemenin amacı, belirli bir yenilik süreci için bir miktar esneklik ve çeşitlilik oluşturmaktır, böylece teknolojinin çeşitli nitelikleri (fırsatlar), potansiyel sonuçları hakkında bilgi edinmek için gerçekleştirilebilir. (Lindman vd., 2020: 31) Avantajlar ortaya çıktıktan sonra, mevcut kullanım durumları ölçeklendirilmeli ve teknoloji, birden çok varlığı ve veri kümesini içeren süreçler gibi daha karmaşık kullanım durumlarına uygulanmalıdır (Pandey, 2020). Bu, proje sırasında çeşitli potansiyel kavramları test etmeye ve kısıtlamaları öğrenmeye olanak sağlayacaktır.



ALTINCI BÖLÜM

6. BULGULAR, ÖNERİLER VE SONUÇ

Bu bölümde araştırmada elde edilen bulgulara ve bu bulgular doğrultusunda geliştirilen önerilere yer verilerek araştırmanın genel sonucuna ulaşılmaktadır. Ayrıca gelecekteki araştırmacılara yol göstermesi için bazı önerilere de yer verilmektedir.

6.1. Bulgular

Bu araştırmada, blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği incelenmiştir. Bu amaçla literatürdeki araştırmalar sistematik bir şekilde taranarak blokzincirin kamu sektöründe benimsenmesi noktasında hem araştırmacılara hem de uygulamacılara ışık tutacak mevcut uygulama alanlarına ve aynı zamanda uygulanabilirliği önündeki engellere genel bir bakış açısı sunulmaya çalışılmıştır. Bu kapsamda öncelikle blokzincir kavramı ele alınmış, ardından sırasıyla blokzincir teknolojisinin üstün yönleri ve faydaları, müteakiben teknolojinin zayıf yönleri ile teknolojiye yöneltilen eleştiriler açıklanmıştır.

“Blokzincir teknolojisi kamusal hizmetlerin sunumunda kullanılabilir mi?”

şeklinde olan ilk araştırma sorusu, sahip olduğu genel üstünlükleri ve faydaları ile ikinci bölümde; Bilgi Teknolojileri kapsamında blokzincir teknolojisini değişime zorlayan etkenlere yer verilerek, kamu yönetimi bağlamında sağlayacağı faydalar ile üçüncü bölümde yanıtını bulmaktadır. Blokzincir teknolojisi; dağıtık yapısı, güvenilirliği, esnekliği, şeffaflık ve denetlenebilirliği, kesinliği, kurcalamaya ve sansüre dirençliliği ve maliyet tasarrufu gibi birçok faydalı özelliği ile kamu yönetimine açıklık, etkililik, saydamlık ve hesap verebilirlik, güvenilirlik, kesinlik ve katılımcılık dâhil olmak üzere, fakat bu alanlarla sınırlı olmayan şekilde fayda sağlayabilme potansiyeline sahiptir.

“Kamusal alanda blokzincir teknolojisinin kullanımı gerekli midir?”

sorusunun yanıtı ise şartlara bağlı olarak değişmektedir. Blokzincir teknolojisinin hükümette kullanımı bir tartışma ve değerlendirme konusudur ve bunun gerekli olup olmadığı, hükümetin karşı karşıya olduğu belirli hedefler ve zorluklar da dâhil olmak üzere çeşitli faktörlere bağlıdır. İkinci bölümde ele alındığı üzere, blokzincir teknolojisinin hükümette kullanılması lehinde ve aleyhinde bazı argümanlar

bulunmaktadır. Lehte olan argümanlara göre blokzincir; güvenilirliği, esnekliği, şeffaflık ve denetlenebilirliği, kesinliği, kurcalamaya ve sansüre dirençliliği ve maliyet tasarrufu gibi birçok faydalı özelliği ile kamu yönetimine fayda sağlayabilir. Teknolojinin hükümette kullanımına karşı olanlar ise blokzinciri; karmaşıklığı, ölçeklenebilirlik sorunları, güvenlik ve gizlilik kaygıları, geri alınamazlığı, boyut ve bant genişliği, enerji tüketimi ve olası insan hataları gibi argümanlarla eleştirmektedirler.

Blokzincir, bilgi ve iletişim teknolojileri alanında son yılların en çok dikkat çeken teknolojilerinden biri olsa da her zaman geleneksel veri tabanlarından daha iyi bir seçenek değildir. Geleneksel çözümler belirli koşullarda halen blokzincirden daha iyi performans gösterebilmektedirler. Blokzincir, tarafların doğrudan işlem yapamadığı veya güvenilir bir üçüncü tarafın olmadığı ortamlarda değerlidir. Önkoşul olarak, herhangi bir verinin saklanması gerekmiyorsa, blokzincirin mevcut çözümlere ekleyeceği bir katma değer olmayacaktır. Benzer şekilde, bir sistemde veriyi üreten sadece bir merkez varsa, yine blokzincir kullanımı anlamsız olacaktır. Kamu kurum ve kuruluşları blokzincir teknolojisinin kullanımı ile ilgili bir karar verirken bu noktaya özellikle dikkat etmeleri gerekmektedir. Çünkü kamu kurum ve kuruluşlarının veri tabanlarının önemli bir kısmı, yapısı itibarıyla tek bir merkez tarafından yönetilmektedir. Bu durum, blokzincir kullanımını kısıtlayan bir sorun olarak değerlendirilebilir olsa da, aynı zamanda kullanımını teşvik etmek için teknolojiyi yerleştirme konusunda bir motivasyon kaynağı olabilme imkanına haizdir.

Örnek olarak; ülkemizdeki mali yargı kurumlarından olan ve kamu idarelerinin mali faaliyet, karar ve işlemlerini hesap verme sorumluluğu çerçevesinde denetleyen Sayıştay ile, bu kurumun denetlediği kamu idareleri arasında yapılan işlemler için geliştirilecek bir blokzincir altyapısı verilebilir. Bu altyapı üzerine kurulacak bir blokzincir ağında ilgili kamu idarelerinin, Sayıştay denetlemesine tabi olduğu bütün alanlar ile ilgili işlemlere ait bilgiler saklanabilir ve bu verilerin şeffaflığı, güvenliği, değiştirilemezliği ve bozulmasının önlenmesi sağlanarak kamu yararı garanti altına alınmış olur.

Özetle, blokzincir teknolojisinin hükümette kullanılmasının gerekli olup olmadığı, spesifik bağlama ve hedeflere bağlıdır. Blokzinciri benimsemeyi düşünen hükümetler, potansiyel faydaları zorluklara ve maliyetlere karşı dikkatli bir şekilde

tartmalıdır. Bazı durumlarda alternatif teknolojiler veya yaklaşımlar, blokzincir ile ilgili karmaşıklıklar olmadan istenen sonuçlara ulaşmak için daha uygun olabilir. Fakat “Blokzincir ve Kamu Yönetimi” başlığı altında verilen ve hem genel olarak hem de kamu yönetimi başlığı altında sıralanan blokzincir kullanım alanları, blokzincir teknolojisinin artan bir ivme ile hayatın her alanında kendine yer bulmaya devam edeceğini göstermektedir. Bu yüzden hükümetler ve kamu idareleri, aynı internet teknolojisinin yaygınlaşması gibi, çağın gerisinde kalmamak için hizmet alanlarının gereklilikleri ve koşullarını göz önünde bulundurarak kamusal alanda blokzincir teknolojisinin kullanımını kesinlikle değerlendirmelidirler.

“Blokzincir teknolojisi kamusal hizmetlerin sunumunda kullanılabilir ise hangi kamusal hizmetlerde kullanılmalıdır?” ise birden fazla cevabı bulunmaktadır. Araştırmada incelendiği gibi blokzincir teknolojisinin doğrudan veya dolaylı olarak etkilediği birçok alan bulunmaktadır. Bu alanların bir kısmı genel kullanım alanlarıdır ve kamu yönetimini dolaylı olarak etkiledikleri için ayrı bir başlık altında incelenmiştir. Doğrudan kamu yönetimindeki olası kullanım alanları ise aşağıdaki şekilde sıralanabilir.

Kimlik Yönetimi: Blokzincir, kimlikleri yönetmek için güvenli ve kurcalamaya dayanıklı bir sistem sağlayabilir. Vatandaşların kişisel bilgileri bir blokzincir üzerinde saklanabilir ve devletler, vatandaşların verilerine kimin eriştiği konusunda daha fazla kontrole ve bilgiye sahip olabilirler. Bu özellikle seçmen kaydı, çeşitli ruhsatların alınması, sosyal yardım dağıtımı ve sağlık kayıtları gibi kamu hizmetlerine erişmek açısından yararlı olabilir.

Kamu Kayıtları ve Belgeleme: Blokzincir, mülkiyet tapuları, doğum ve ölüm belgeleri, evlilik ruhsatları ve daha fazlası gibi önemli belgelerin kalıcı ve şeffaf bir kaydını oluşturmak için kullanılabilir. Bu, dolandırıcılığı azaltabilir, idari süreçleri kolaylaştırabilir ve belgelerin doğruluğunun doğrulanmasını kolaylaştırabilir. Blokzincir, belge doğrulama, yasal uyumluluk ve departmanlar arası iş birliği için güvenli, izlenebilir ve verimli bir platform sağlayarak karmaşık bürokratik süreçleri basitleştirebilir.

Tedarik Zinciri Yönetimi: Kamu satın alma süreçlerinde blokzincir, tedarik zincirinin her adımını kaydederek şeffaflığı sağlayabilir. Hükümetler, malların hareketini izlemek ve ürünlerin orijinalliğini sağlamak için blokzincir kullanabilir. Bu, yolsuzluğun

önlenmesinde ve kaynakların tahsisinde hesap verebilirliğin geliştirilmesine yardımcı olabilir.

Şeffaf Bütçeleme ve Harcama: Blokzincir, hükümet bütçesinin hazırlanmasında ve kamu harcamalarında şeffaflık ve hesap verebilirlik getirebilir. Vatandaşlar fonların nasıl tahsis edildiğini ve harcadığını takip ederek yolsuzluk potansiyeli azaltılabilecektir.

Arazi ve Mülk Sahipliği: Blokzincir, güvenli ve şeffaf bir tapu sicil sistemi oluşturmak, mülk sahipliği konusundaki anlaşmazlıkları azaltmak ve mülk işlemlerinin verimliliğini artırmak için kullanılabilir. Arazi ve mülk sahipliğinin güvenli ve kurcalamaya karşı dayanıklı bir kaydını sağlayarak mülkiyetin aktarılmasını kolaylaştırabilir ve dolandırıcılık faaliyetlerinin önlenmesine yardımcı olabilir.

Noter Tasdiki: Blokzincir, belgelerin ve işlemlerin değişmez ve zaman damgalı kaydını sağlayan dijital bir noter görevi görebilir.

Oylama Sistemleri: Blokzincir tabanlı oylama sistemleri seçimlerin güvenliğini ve şeffaflığını artırabilir. Her oy blokzincir üzerine kaydedilerek oyların tahrif edilemeyeceğinden emin olunur ve seçim sonuçları için şeffaf bir denetim izi sağlanır.

Sosyal Refah Dağıtımı: Blokzincir, sosyal refah faydalarını dağıtmak için şeffaf ve verimli sistemler oluşturmak için kullanılabilir. Bu, dolandırıcılığı azaltabilir ve fonların amaçlanan yararlanıcılara ulaşmasını temin edebilir.

Afet Yönetimi ve Yardım Dağıtımı: Sosyal refah dağıtımına benzer şekilde blokzincir, doğal afetler veya acil durumlar sırasında, yardım ve yardım kaynaklarını verimli bir şekilde dağıtmak için blokzincir kullanılabilir. İşlemlerin şeffaflığı, kaynakların hedeflenen alıcılara ulaşmasını sağlar.

Sağlık Verilerinin Yönetimi: Vatandaşlara ait en önemli bilgilerden olan tıbbi kayıtlar ve hasta verilerinin güvenliğini ve gizliliğini korumak ve aynı zamanda hastalara kendi sağlık bilgileri üzerinde daha fazla kontrol olanağı sunmak için blokzincir kullanılabilir. Yine blokzincir, hastaların tıbbi kayıtlarının farklı sağlık hizmeti sağlayıcıları arasında güvenli bir şekilde saklanmasını ve paylaşılmasını sağlayabilir,

Devlet Hizmetleri için Akıllı Sözleşmeler: Akıllı sözleşmeler, koşulları doğrudan koda yazılan ve kendi kendini yürüten sözleşmelerdir. Bu sözleşmeler, belirtilen koşullar karşılandığında otomatik olarak yürütülerek aracılara olan ihtiyacı ortadan kaldırır ve insan hatası veya manipölasyon riskini azaltır. Bu sayede, çeşitli devlet hizmetlerini otomatikleştirmek ve kolaylaştırmak, bürokrasiyi ve işlem sürelerini azaltmak için kullanılabilirler.

Dolayısıyla, dikkatli bir şekilde uygulandığında blokzincir, kamu hizmetlerinin sunulma biçiminde devrim yaratarak kamu yönetimine etkililik, şeffaflık ve hesap verebilirlik, güvenilirlik, katılımcılık ve yönetim dâhil olmak üzere, fakat bu alanlarla sınırlı olmayan şekilde fayda sağlayabilme potansiyeline sahiptir.

Bu noktada Dünyada ve Türkiye’de blokzincir alanında hayata geçirilmiş ve yürütülmekte olan uygulama örneklerine yer verilmiştir. Dünyadaki uygulama örneklerine yer verilirken, bu teknolojinin benimsenmesinde başı çeken ve farklı alanlarında örnekler sunan ülkelerin seçilmesine özen gösterilmiştir. Dünyada Amerika Birleşik Devletleri, kurumsal olarak Avrupa Birliği, kendi özelinde Fransa, Almanya ve Estonya, Birleşik Krallık, Birleşik Arap Emirlikleri, Çin, Güney Kore ve Singapur bu ülkelerden bazılarıdır.

Türkiye’deki blokzincir uygulamaları kamu yönetimi kapsamında değerlendirildiğinde bazı adımlar atıldığı görülmektedir. TÜBİTAK BİLGEM’in bünyesinde kurulan Blokzincir Araştırma Ağı (BAĞ) ve Blokzincir Araştırma Laboratuvarı (BZLab), TAKASBANK tarafından yürütülen Bir Gram Altın (BiGA) projesi, Türkiye Bilişim Vakfı (TBV) liderliğinde kurulan Blockchain Türkiye Platformu (BCTR) bunlardan bazılarıdır. Diğer bir yandan blokzincir kullanımını destekleyecek süreçlerin politika ve strateji belgelerinde yer almaya başladığı görülmektedir. Yayınlanan 11. Kalkınma Planı’nda gümrük ve ulaştırma hizmetlerinde kullanılması için gerekli altyapının hazırlanacağına, blokzincir tabanlı dijital merkez bankası parasının uygulamaya konulacağına ve e-Devlet Uygulamaları kapsamında kamu hizmetlerinin iyileştirilmesi için blokzincir gibi yeni teknolojilerden faydalanılabilmesi maksadıyla altyapı iyileştirilmeleri yapılması gerektiğine yer verilmiştir. Aynı zamanda Sanayi ve Teknoloji Bakanlığı’nın yayınlamış olduğu 2023 Sanayi ve Teknoloji Stratejisi’nde “Ulusal Blokzincir Altyapısı” kurulması planlanarak, blokzincir teknolojisi üzerinde

uygulama geliştirme yetkinliğinin oluşması için öncelikle kamu merkezli uygulamalardan blokzincir altyapısına taşınabilir olanların tespit edilerek projelendirilmelerinin sağlanacağı aktarılmıştır.

Blokzincir teknolojisi, özellikle ilk aşamalarında kamu yönetimi de dâhil olmak üzere çeşitli sektörlerde önemli ilgi ve heyecan uyandırmıştır. Bu ilgi ve beklentiler, teknolojinin gelişimi devam ederken birtakım riskler oluşturabilmektedir. Teknolojinin potansiyelinin hayal edilmesi faydalı olsa da aşırı abartılı beklentilere kapılmamak gerekmektedir. Benzer şekilde blokzincir teknolojisinin yetenekleri ve potansiyel etkileri hakkında bazı yanlış anlamalar mevcuttur. Bu kapsamda **“Kamu yönetiminde blokzincirle ilgili yanlış bilinenler nelerdir?”** araştırma sorusuna yanıt olarak araştırmada blokzincir teknolojisinin kamu yönetiminde uygulanabilirliğiyle alakalı sınırlılıklara ve yaygın yanlış kanılara da yer verilmiştir. Bunlar aşağıdaki şekilde sıralanabilir.

Garantili Güvenlik ve Değişmezlik: Blokzincir, kriptografik özet ve dağıtık mutabakat mekanizmaları yoluyla yüksek düzeyde güvenlik ve değişmezlik sağlamak üzere tasarlanmış olsa da her türlü saldırıya karşı bağımsız değildir. Uygulamada halen yazılımda, akıllı sözleşmelerde ve ağın kendisinde güvenlik açıkları bulunabilir. Ek olarak, ağın bilgi işlem gücünün büyük bir kısmı kötü niyetli bir paydaş tarafından kontrol ediliyorsa, blokzincirin bütünlüğü tehlikeye girebilir.

Anlık İşlemler: Blokzincir, geleneksel sistemlere kıyasla daha hızlı ve daha verimli işlemlere olanak sağlarken, anlık işlemleri garanti etmez. Blokzincir işlemlerinin hızı, kullanılan mutabakat mekanizması, ağ tıkanıklığı ve işlem karmaşıklığı gibi faktörlere bağlıdır. Bitcoin ve Ethereum gibi halka açık blokzincirler, genellikle yüksek ağ etkinliği sırasında gecikmelere yol açabilecek ölçeklenebilirlik sorunları yaşamaktadır.

Tam Anonimlik: Birçok durumda blokzincir işlemlerinin tamamen anonim olduğu varsayılmaktadır. Blokzincir işlemleri, gerçek dünya kimliğinden ziyade kriptografik bir adrese bağlı oldukları anlamına gelen takma adla yapılabilir de, özellikle işlemler diğer sistemlerle etkileşimleri içerdiğinde veya davranış kalıpları analiz edildiğinde, çeşitli tekniklerle kullanıcıların belirlenmesi mümkün olabilir.

Aracıların Ortadan Kaldırılması: Blokzincir genellikle araçları ortadan kaldırabilen ve bürokrasiyi azaltabilen bir teknoloji olarak lanse edilir. Blokzincir, doğrudan eşler arası işlemlere ve veri paylaşımına izin vererek süreçleri kesinlikle düzene sokabilirken; yasal, düzenleyici ve yönetim yönleri dikkate alınmadan tüm araçlar ortadan kaldırılamaz. Ayrıca, ihtilafların çözümü, uyum ve belirli eylemlerin uygulanması için bazı araçlara ihtiyaç duyulabilmektedir.

Kapsamlı Maliyet Azaltma: Blokzincir teknolojisi, süreçleri otomatikleştirerek ve araçlara olan ihtiyacı azaltarak kamu yönetiminin belirli alanlarında maliyetleri düşürme potansiyeline sahiptir. Bununla birlikte, bir blokzincir ağının uygulanması ve sürdürülmesi, özellikle geliştirme, altyapı, (PoW blokzincirleri için) enerji tüketimi ve yönetim açısından önemli maliyetler getirebilir.

Evrensel Uygulanabilirlik: Tüm süreçler ve kullanım durumları, blokzincir uygulaması için uygun değildir. Bazı işlemler, hız, ölçeklenebilirlik, gizlilik ve karmaşıklık gibi faktörler nedeniyle geleneksel veri tabanları veya merkezi sistemler tarafından daha iyi sunulabilir. Blokzincirin belirli bir sorun için doğru çözüm olup olmadığını dikkatlice değerlendirmek önemlidir.

Düzenleyici Zorlukların Çözümü: Blokzincir şeffaflığı ve denetlenebilirliği kolaylaştırabilirken, tüm düzenleyici zorlukları otomatik olarak çözmez. Blokzinciri kamu yönetimine entegre etmek, veri koruma, uyumluluk ve yargı sorunları gibi ele alınması gereken yasal ve düzenleyici hususları içermektedir.

Güven Gerektirmemesi: Blokzincir, merkezi olmayan yapısı nedeniyle genellikle güven gerektirmeyen bir teknoloji olarak görülür. Bununla birlikte, teknolojik altyapıya, ağdaki katılımcılara ve blokzinciri koruyan yönetim mekanizmalarına güven duyulması hâlâ gereklidir. Ayrıca, akıllı sözleşmelerin sebep olduğu güvenlik açıkları ve insan hataları istenmeyen sonuçlara yol açarak güven ve durum tespitinin önemini vurgulayabilir.

Blokzincir kamu yönetimine önemli faydalar sağlama potansiyeline sahip olsa da; hükümetler, teknolojinin yeteneklerini ve sınırlılıklarını net bir şekilde anlayarak benimsenmesine karar verilmelidirler. Bu teknoloji, her duruma uygun tek bir çözüm değildir ve spesifik kullanım durumunun, teknik hususların, düzenleme ortamının ve

potansiyel zorlukların dikkatli bir şekilde değerlendirilmesi, başarılı uygulama için büyük öneme sahiptir.

Blokzincir teknolojisi, araştırmada belirtilen özellikleriyle kamu yönetimini birçok açıdan dönüştürme potansiyeline sahiptir. Bu potansiyele rağmen, her yeni teknolojinin gelişim aşamasında olduğu gibi uygulanabilirliğinin önünde bazı engeller bulunmaktadır. **“Blokzincir teknolojisinin kamu yönetiminde uygulanabilirliğinin bu önündeki engeller nelerdir?”** araştırma sorusu ile bu engeller tespit edilmeye çalışılmıştır. Blokzincir teknolojisinin vaat ettiği faydalar kanıtlanabilirse ve dördüncü bölümde ele alındığı gibi dünyadaki ve Türkiye’deki uygulama örnekleri hayata geçirilebilir ve çoğaltılabilirse yakın gelecekte teknolojinin bir dönüm noktası olması ve yaygın bir şekilde kabul görmeye başlaması mümkündür. Bu doğrultuda araştırmada yapılan literatür taraması sonucunda, blokzincir teknolojisinin kamu yönetiminde benimsenmesi önünde on üç temel engel belirlenmiştir.

Maliyetler ve Bütçe Kısıtlamaları: Blokzincir ağlarını geliştirmek ve sürdürmek, özellikle altyapı, geliştirme, güvenlik ve sürekli bakım söz konusu olduğundan dolayı maliyetlidir. Devlet kurumlarının, blokzincir projelerine yatırım yapma yeteneklerini sınırlayan bütçe kısıtlamalarıyla karşı karşıya kalabilme ihtimali bulunmaktadır.

Birlikte Çalışabilirlik Sorunları: Blokzincir sistemlerini mevcut eski sistemler ve veri tabanlarıyla entegre etmek, birlikte çalışabilirlik sorunları nedeniyle karmaşık olabilir. Standartlaştırılmış protokollerin ve formatların olmaması, kesintisiz veri alışverişini engelleyebilir.

Ölçeklenebilirlik Sorunları: Bazı blokzincir platformları, ağ büyüdükçe daha yavaş işlem hızlarına ve daha yüksek maliyetlere yol açan ölçeklenebilirlik sınırlamalarıyla karşı karşıyadır. Bu sınırlamalar, yüksek hacimli devlet süreçleriyle uğraşırken bir engel olabilir.

Veri Gizliliği ve Koruma Sorunları: Kamu idareleri genellikle gizliliğin önemli olduğu hassas vatandaş verileriyle ilgilenmektedir. Teknolojinin şeffaf doğası bazı veri koruma gereksinimleriyle çeliştiğinden, veri gizliliği yasalarına uyumu sağlarken blokzinciri uygulamak zor olabilir.

Karmaşıklık ve Teknik Zorluklar: Blokzincir teknolojisi karmaşıktır ve uygulanması, kriptografik ilkelerin, mutabakat mekanizmalarının ve dağıtık sistemlerin derinlemesine anlaşılmasını gerektirir. Blokzincir ağlarını geliştirmek ve sürdürmek, özellikle bu alanda sınırlı uzmanlığa sahip devlet kurumları için teknik olarak zorlayıcı olabilir.

Eski Sistemler: Birçok hükümet süreci, blokzincir teknolojisiyle kolayca uyumlu olmayan eski sistemler üzerine kuruludur. Bu sistemlerden blokzincir tabanlı çözümlere geçiş, zaman alıcı ve kaynak yoğun olabilir.

Yetenek ve Uzmanlık Eksikliği: Blokzincir teknolojisi nispeten yenidir ve blokzincir geliştirme ve uygulama konusunda uzmanlığa sahip vasıflı profesyonellerin mevcudiyeti halen sınırlıdır. Devlet kurumlarının nitelikli personeli işe alması ve elde tutması zor olabilir.

Halkın Algısı ve Güveni: Blokzincir teknolojisine ilişkin halkın algısı, teknolojinin benimsenmesini etkileyebilir. Teknolojinin gerekliliği devlet tarafından net bir şekilde aktarılamazsa veya vatandaşlar blokzincire aşina değilse ve güvenmezse, hükümetin blokzincir girişimleri konusunda halktan destek alması zorlaşabilir.

Farkındalık ve Anlayış Eksikliği: Birçok hükümet yetkilisi ve çalışanı, blokzincir teknolojisini ve potansiyel faydalarını tam olarak anlamayabilir. Bu farkındalık eksikliği, şüpheciliğe, değişime karşı dirence ve blokzincir projelerine kaynak yatırma konusunda isteksizliğe yol açabilir.

Değişime Karşı Direnç: Devlet kurumları genellikle riskten kaçınır ve başarısızlık korkusu, yerleşik süreçlerin bozulması ve olumsuz sonuç potansiyeli nedeniyle yeni teknolojileri benimsemeye karşı dirençlidir.

Düzenleyici ve Yasal Belirsizlikler: Düzenleyici çerçeveler genellikle blokzinciri gibi hızla gelişen teknolojilere ayak uydurmak için mücadele eder. Mevcut düzenlemelerin blokzincir çözümlerine nasıl uygulanacağına dair belirsizlik, yasal engeller oluşturabilir ve benimsemeyi engelleyebilir.

Yavaş Bürokratik Süreçler: Devletin karar alma mekanizması genellikle yavaştır ve bürokratik süreçleri içinde barındırır. Bu da blokzincir gibi yeni gelişen teknolojileri hızla benimsemeyi ve uygulamayı zorlaştırır.

Yönetişim ve Koordinasyon Eksikliği: Blokzincirin merkezi olmayan doğası, özellikle birden fazla devlet kurumu söz konusu olduğunda, yönetişimi ve karar vermeyi karmaşık hale getirebilir. Paydaşlar arasında koordinasyon ve iş birliği sağlamak beklenenden zor olabilir.

Sınırlı Kullanım Durumları: Blokzincirin potansiyel uygulamaları olsa da, tüm hükümet süreçleri blokzincir uygulaması için uygun değildir. İlgili kullanım durumlarını belirlemek ve hayata geçirmek kapsamlı ve etkili bir planlama gerektirir.

Önceliklerle Uyumsuzluk: Blokzincirin uygulanması, ele alınması gereken daha acil endişeleri olabilecek devlet kurumlarının acil öncelikleriyle uyumlu olmayabilir. Ayrıca teknolojinin sebep olduğu etik sorunlar da bu öncelikleri olumsuz anlamda destekleyebilir. Bu sebeple teknolojinin uygulanması ilgili kamu kurumları tarafından geri plana bırakılabilir.

Müteakip araştırma sorusu olan **“Blokzincir teknolojisinin kamu yönetiminde uygulanabilirliğinin önündeki engellerin birbirleriyle ilişkisi var mıdır ve varsa belirli karakteristik özelliklerine göre gruplandırılmaları mümkün müdür?”** sorusuna yanıt bulmak için; engellerin sınıflandırılması, araştırmacılar tarafından bilgi teknolojilerinin benimsenmesini incelemek maksadıyla yaygın olarak kullanılan bir yöntem olan Teknoloji – Organizasyon – Çevre (TOE) çerçevesi ile ele alınmıştır. Bu çerçeve ile engeller sınıflandırılarak, bir kamu kurumunda teknolojik yeniliklerin benimsenmesi kararına etki eden faktörlerin teknoloji, organizasyon ve çevre bağlamında incelenmesi ve blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği önündeki bu engellerin daha iyi anlaşılması amaçlanmıştır.

Bu engelleri ele almak, paydaşları eğitmeyi, iş birliğini teşvik etmeyi, düzenleyici zorlukların üstesinden gelmeyi ve blokzincir projelerinin fizibilitesine ve potansiyel etkisine ilişkin kapsamlı değerlendirmeler yapmayı içeren stratejik bir yaklaşım gerektirir. Kamu idareleri, teknolojinin uygulanabilirliği önündeki bu engelleri aşma konusunda sistematik ve iş birliğine dayalı bir yaklaşım sergiler ve buna yönelik uygulamalar geliştirebilirlerse, blokzincirin potansiyel faydaları daha net şekilde ortaya çıkacaktır. Bunu yaparak, hükümetler bu zorlukların üstesinden gelebilir ve blokzincir teknolojisinin kamu yönetimine sunabileceği faydaların kilidini açabilir.

Blokzincir teknolojisini kullanarak kamu hizmeti uygulaması oluşturmak isteyen bir kamu kurumu yöneticisi, öncelikle **“Kamu kurumları blokzincir teknolojisine ihtiyacı olup olmadıklarına nasıl karar verebilirler?”** sorusunu sormalıdır. “Kamusal alanda blokzincir kullanımı gerekli midir?” sorusunda belirtildiği gibi blokzincir teknolojisi, geleneksel veri tabanlarından her zaman daha iyi bir seçenek değildir. Geleneksel veri tabanları, belirli özellikleriyle blokzincir teknolojisine göre üstünlük gösterebilmektedir. Kamu kurumları, bir kamu hizmetinin sunulmasında blokzincir teknolojisinin kullanılmasına karar verirken, bu husus üzerinde önemle durmalıdırlar. Bu noktada kamu idarelerinin faydalanabileceği bazı karar verme modelleri geliştirilmiştir. Araştırmada bu modellerden özgün olanlara kronolojik olarak yer verilmiştir.

Deloitte 3 V modeli, yeni bir teknoloji hayata geçirilirken uygulanabilirliğine (viable), bir katma değer ortaya koyup koymayacağına (valuable) ve hayati (vital) olup olmadığına göre değerlendirilmesini esas alan bir modeldir.

Peck modeline göre ise blokzincir teknolojisi her ne kadar birçok avantajı kendinde bulundursa da blokzincirin her sorunun çözümü olmadığını belirterek “bu teknolojiye gerçekten ihtiyacınız var mı?” sorusunu sormaktadır. Bu model ağacı “Geleneksel veri tabanları ihtiyacınızı karşılıyor mu?” sorusu ile başlayarak eğer sorunun cevabı evet ise blokzincire ihtiyacın olmadığı sonucuna ulaşmakta; hayır ise ikinci soru olan “Veri girişini birden fazla paydaşın yapması gerekiyor mu?” sorusuna yönlendirmektedir. Sorunun cevabı hayır ise yine blokzincire ihtiyaç yok demektir. Bu soru, kamu kurumlarının birçok alanda veriyi yöneten tek taraf olması nedeniyle, blokzincirin kamu yönetimi bağlamında değerlendirilmesi açısından önemlidir. Model, veri girişi yapan paydaşların birbirine olan güveni, verilerin müdahaleye açık olup olmadığı, verilerin birden fazla veri tabanında tutulmasının gerekip gerekmediği gibi hususlara göre ilerlemektedir. Müteakiben gizlilik ihtiyacına, ağda kimin değişiklik yapacağına ve güvenilir üçüncü taraf mevcudiyetine göre ne tür bir blokzincir sistemine ihtiyaç olduğu belirlenir.

Wüst ve Gervais modelinde de benzer şekilde verilerin kaydedilmesi ihtiyacı olup olmadığı, birden fazla yazarın varlığı, güvenilir bir üçüncü tarafın mevcudiyeti ve kamu tarafından doğrulanabilirlik gerekliliğine göre blokzincir ihtiyacına karar verilmektedir.

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü tarafından yayınlanan DHS modeline göre önce teknolojinin hangi ihtiyaçları karşıladığını sorgulamak ve ardından blokzincir paradigmasına uyabilecek sistemleri belirlemek gerekmektedir. Buna göre bir sistemde; birden fazla katılımcının bulunması, katılımcıların dağıtık olması, güvenilir bir üçüncü tarafın olmayışı, iş akışının işleme dayalı olması, merkezi olmayan bir sıralı kayıt defterine ihtiyaç duyulması, kriptografik olarak güvenli bir sahiplik sistemine ihtiyaç duyulması, uyuşmazlık çözümlerine yönelik manuel çabaları azaltma ihtiyacı, düzenleyiciler ve düzenlenen kuruluşlar arasındaki faaliyetin gerçek zamanlı izlenmesi ihtiyacı, dijital varlıkların tam kaynağına ve katılımcılar arasında paylaşılacak eksiksiz bir işlem geçmişine ihtiyaç duyulması durumunda blokzincir teknolojisine başvurulabilir.

Casino, Dasaklis ve Patsakis modelinde blokzincir teknolojisinin etkileyeceği sektörlerin gereksinimlerine göre blokzincir tabanlı çözümlerin uygunluğunu değerlendirmek için bir çerçeve geliştirmiştir. Bu sektörler arasında yer alan “vatandaşlık hizmetleri”, “doğruluk teyidi”, “yönetim”, “sağlık”, “gizlilik ve güvenlik”, “eğitim” ve “veri yönetimi” gibi alanlar kamu yönetimini doğrudan veya dolaylı olarak ilgilendirmektedir. Çerçevede blokzincirin geleneksel veri tabanlarına karşı potansiyeli; gerekli güven varsayımları, bağlam gereksinimleri, performans özellikleri ve gerekli fikir birliği mekanizmaları olmak üzere dört ana başlıkta değerlendirilmektedir. Her bir ön koşulun alaka düzeyini ölçmek için üç düzeyli bir ölçek (düşük, orta ve yüksek) kullanılmaktadır. Kamu kurumları, sundukları kamu hizmetlerinin blokzincir tarafından geliştirilip geliştirilmeyeceğini değerlendirmek için bu çerçeveyi bir araç olarak kullanabilirler.

Son olarak sunulan GO Lab ve CIPFA çerçevesinde, blokzincir teknolojisinin kamu sektöründe benimsenmesi önündeki engeller ve yeterli bilgi eksikliği nedeniyle karşılaştığı zorluklar tartışılmaktadır. Bu konuyu ele almak ve kamu görevlilerine karar verme süreçlerinde yardımcı olmak amacıyla Oxford Üniversitesi bünyesindeki GO Lab ve Birleşik Krallık'taki uluslararası kamu muhasebe standartları organı CIPFA tarafından bir çerçeve geliştirilmiştir. Bu çerçevede, kurulum, izleme ve yönetim ile doğrulama olmak üzere iş birliğinin üç aşamasına odaklanılarak blokzincir çözümlerinin uygulanmasında ihtiyaç temelli bir yaklaşım teşvik edilmektedir. Çerçevede potansiyel ortaklar arasındaki güven, veri katkısı ve sahiplik kontrolü, değişmez kayıtların gerekliliği, teşviklerin yanlış hesaplanması riski ve iş birliği sonuçlarının

değerlendirilmesi gibi faktörler dikkate alınmaktadır. Temel vurgu, blokzincir teknolojisinin basit bir şekilde uygulanabilir olmaktan ziyade ne zaman gerekli olabileceğini belirlemek ve paydaşlara, belirli iş birlikçi projeler için teknolojinin değerini ve uygunluğunu değerlendirmede rehberlik etmektir. Netice olarak çerçevede, blokzincir teknolojisi hakkındaki bilgi açığını kapatmak ve bilinçli benimseme kararları için kamu kurumu yöneticilerine rehberlik sağlamak amaçlanmaktadır.

Organizasyonların blokzincire ihtiyacı olup olmadıklarıyla ilgili geliştirilen yaklaşımlar burada belirtilenler ile sınırlı değildir. Blokzincir sistemleri, özelliklerine göre genel, özel, konsorsiyum ve hibrit blokzincir olmak üzere dört kategoride sınıflandırılmaktadır. Bunlar arasındaki temel fark katılımcılara verilen erişim seviyesiyle ilgilidir. Blokzincirlerin uzlaşma sağlayıcılar, katılımcıların veri okuma izinleri, verimlilik, merkezilik ve uzlaşma süreçlerine katılım durumlarına göre farklılıkları bulunmaktadır. Kamu kurumları sunulan bu modeller sonucunda blokzincire ihtiyaç duyup duymadıklarına ya da ihtiyaçları varsa hangi tür blokzincir sınıfını kullanmaları gerektiğine karar verebilirler.

Bunun dışında mevcut iş süreçlerinin değerlendirildiği ve sorunlu noktaların, verimsizliklerin ve şeffaflık ile güvenin kritik olduğu alanların belirlendiği “iş süreci analizi” ile blokzincir uygulamanın potansiyel maliyet ve faydalarının kapsamlı bir analizinin yapılacağı bir “maliyet-fayda analizi” de uygulanabilecek analizler arasındadır. Burada geliştirme maliyetleri, operasyonel tasarruflar ve potansiyel gelir yaratma olanakları da dâhil olmak üzere hem kısa vadeli hem de uzun vadeli finansal etkiler göz önünde bulundurulmalıdır. Ayrıca önerilen blokzincir uygulamasına özel bir GZFT (Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler - SWOT) analizi yapılabilir. Bu yöntem, projenin başarısını etkileyebilecek iç ve dış faktörlerin belirlenmesine yardımcı olabilir.

Kamu hizmetlerinin sunumunda blokzincir teknolojisinin uygulama kararının, kuruluşun daha geniş dijital dönüşüm stratejisiyle uyumlu hale getirilmesi, kamu yönetiminde hayata geçirilecek projelerin potansiyel başarısını arttıracaktır. Burada blokzincirin, kurumun hedeflerine nasıl uyduğunun ve süreçlerin ve hizmetlerin nasıl geliştirebileceğinin belirlenmesi önemlidir. Maliyet-fayda analizine benzer şekilde risk-getiri analizi de yapılarak blokzincirin uygulanmasıyla ilişkili potansiyel riskler ve ödülleri değerlendirilmelidir. Teknoloji riskleri, yasal uyumluluk sorunları, etik sorunlar

ve arařtırmada belirtilen diğerk engeller gibi faktörler de hesaba katılmalıdır. Ayrıca kuruluşun inovasyon kültürü ve gelişmekte olan teknolojileri keşfetme isteğı de göz önünde bulundurulmalıdır. Kuruluş yenilik ve deneylere açıksa, blokzincir çözümlerini keşfetmeye daha yatkın olabilir.

Blokzincirin hem dâhili personel hem de harici paydaşlar olan son kullanıcılar üzerindeki etkisi değerdendirilmelidir. Teknoloji, kullanıcı deneyimini geliştiriyor, süreçleri basitleştiriyor veya benzersiz bir değersunuyorsa, bu iyi bir uyum sağlanmasına yardımcı olabilir. Bu modeller ve çerçeveler, blokzincirin belirli bir sorun veya kullanım durumu için doğru çözüml olup olmadığını değerdendirmek maksadıyla yapılandırılmış bir yaklaşım sağlayabilir. Bu nedenle blokzincirin benimsenmesi hakkında bilinçli kararlar almak için değerdendirme sürecinin kuruluşun özel bağlamına ve ihtiyaçlarına göre uyarlanması büyük önem arz etmektedir.

Blokzincir teknolojisinin kamu sektöründe başarılı bir şekilde uygulanması, teknik hususların ötesine geçen çeşitli faktörlere bağlıdır. Bir kamu hizmeti sunumunun, blokzincir teknolojisi kullanılarak hayata geçirilebilmesi için arařtırmada belirtilen kritik başarı faktörleri üzerinde önemle durulması gerekmektedir. **“Kamuda Blokzincirin Uygulanabilirliğindeki Kritik Başarı Faktörleri Nelerdir?”** sorusunun cevabı aşağıdaki başlıklar altında özetlenmiştir.

Net Kullanım Örneğı Tanımlaması: Blokzincirin çözmesi öngörülen sorunun veya sürecin açıkça tanımlanması gerekmektedir. Arařtırmada belirtildiğı gibi her süreç, bir blokzincir çözümlüne ihtiyaç duymamaktadır. Bu nedenle blokzincirin (şeffaflık, değışmezlik ve merkezi olmama gibi) özelliklerinin belirgin avantajlar sağladığı kullanım durumlarının belirlenmesi çok önemlidir. Bu noktada blokzincir uygulamasının finansal sonuçlarını değerdendirmek için kapsamlı bir maliyet-fayda analizi ve olası kamusal faydalarını değerdendirmek için bir risk-getiri analizi yapılabilir. Geliştirme, bakım ve olası tasarruflar dâhil olmak üzere hem kısa hem de uzun vadeli maliyetler göz önünde bulundurulmalıdır.

Teknolojik Uygunluk: Blokzincir çözümünün mevcut sistemler, veri tabanları ve teknolojilerle nasıl bütünleşeceğini düşünölmelidir. Birlikte çalışabilirliğı, kesintisiz veri alışverişı ve daha geniş ekosistemler içinde verimli çalışma için önemli olduğı unutulmamalıdır. Zaman içinde artan kullanıma uyum sağlamak için, seçilen blokzincir

teknolojisinin ölçeklenebilirliđi deđerlendirilmelidir. Bu açıdan, kullanılacak blokzincir platformunun işlem hacmi ve ađ kapasitesi açısından sınırlamalarla karşılaşılabileceđi unutulmamalıdır. Kullanım durumlarına bađlı olarak, blokzincirde depolanan veya işlem gören verilerin gizlilik gereksinimleri göz önünde bulundurulmalıdır. Şeffaflıđın avantajlarından yararlanmaya devam ederken hassas bilgileri korumak için uygun mekanizmalar seçilmelidir.

Paydaş Katılımı: Paydaşları sürece erken aşamalarda dâhil etmek, blokzincir çözümünün, paydaşların ihtiyaçlarını karşılamasını sađlamasına yardımcı olacak ve uygulama için destek sađlayacaktır. Kamu kurumları; kaynakların, bilginin ve uzmanlıđın paylaşımı için diđer devlet kurumları, özel sektör ortakları ve ilgili paydaşlarla iş birliđi yapmalıdır. Devlet kurumlarından, endüstriden ve sivil toplumdan ilgili paydaşların planlamaya ve tasarım aşamalarına dâhil edilmesi kullanım süreçlerinin ilerlemesini hızlandıracaktır. Bu noktada potansiyel yasal engellerin aşılması için gerekirse alanında uzman hukuk danışmanları ile iş birliđi de düşünölmeli ve düzenleyici zorluklar ele alınarak önerilen blokzincir çözümünün mevcut yasa ve yönetmeliklere uygun olması sađlanmalıdır.

Kullanıcı Deneyimi: Blokzincir teknolojisinin hem devlet çalışanları hem de vatandaşlar tarafından benimsenmesini teşvik etmek için kullanıcı dostu arayüzler ve deneyimler tasarlanmalıdır. İyi tasarlanmış bir kullanıcı arayüzünün, blokzincir çözümünü daha erişilebilir ve sezgisel hale getireceđi unutulmamalıdır. Ayrıca devlet çalışanlarına ve blokzincir sistemleriyle etkileşime girecek kullanıcılara yeterli eğitim sađlanmalıdır. Halkla İletişim sađlanması açısından blokzincir uygulamasının faydaları ve amacı halka iletilmelidir. Teknolojinin kullanımıyla ilgili şeffaflıđın, vatandaşlar arasında güven ve anlayış oluşturacađı; bilgi eksikliklerinin ise teknolojinin benimsenmesini engelleyebileceđi ve hatalara yol açabileceđi unutulmamalıdır.

Test Etme: Tam ölçekli uygulamaya geçmeden önce; teknik, operasyonel veya kullanılabilirlik zorluklarını belirlemek ve bu sorunları çözmek için pilot testler veya küçük ölçekli uygulamalar gerçekleştirilmelidir. Pilot uygulamalar, çözümü iyileştirmeye ve teknolojinin uygulanabilirliğini dođrulamaya yardımcı olacaktır. Blokzincir ađında yükseltmeler, bakım ve deđişikliklerle ilgili karar vermeden önce net yönetişim

mekanizmaları oluşturulmalıdır. İyi tanımlanmış yönetim, blokzincir çözümün uzun vadeli sürdürülebilirliğini sağlayacaktır.

Blokzincirin kamu sektöründe başarılı bir şekilde uygulanması, teknik, organizasyonel, düzenleyici ve sosyal yönleri kapsayan bütüncül bir yaklaşım gerektirmektedir. Kamu idareleri, blokzincirin uygulanmasının getirebileceği organizasyonel ve kültürel değişikliklere karşı değişimi yönetmeye hazır olmalıdır. Devlet kurumları, teknolojinin potansiyel faydalarını vatandaşlara, memurlara ve diğer tüm paydaşlara aktarabilmeli, onların muhtemel endişelerini giderebilmeli ve beklentilerini yönetebilmelidir. Aynı şekilde başarılı bir blokzincir girişimi için kamu yönetimleri tarafından uzun vadeli vizyon geliştirilmelidir. Blokzincir çözümün zaman içinde nasıl gelişeceğinin, değişen teknolojilere nasıl uyum sağlanacağını ve daha geniş devlet stratejileriyle nasıl uyumlu hale gelineceğinin vizyonu oluşturulmalıdır. Hükümetler, operasyonlarında şeffaflığı, verimliliği ve hesap verebilirliği artırmak için blokzincir teknolojisinin potansiyelini en üst düzeye çıkartmak maksadıyla bu kritik başarı faktörlerini dikkatli bir şekilde ele almalıdırlar.

6.2. Öneriler

Araştırmada blokzincir teknolojisinin kamu kurumlarında yüklenebileceği stratejik rolüne ilişkin çeşitli perspektifler ele alınmıştır. Bu teknolojinin özellikle kamu yönetimi alanında geliştirilmesi gereken birçok yönü olduğunun altı çizilmektedir. Blokzincir teknolojisi henüz emekleme aşamasındadır ve yazılım altyapısı geliştirilmeye devam etmektedir. Sağlanan gelişmeler ile doğru orantılı olarak teknolojinin gerçek hayattaki uygulama alanları da artan bir ivme ile çoğalmaktadır. Blokzincir gelişmeye devam ettikçe, tıpkı geçmişte internet vasıtasıyla bilginin aktarıldığı gibi, değer de güvenli bir şekilde aktarılmasını sağlayacak işlemler için ana teknoloji haline gelmesi olasıdır. Aynı durum blokzincirin kamu yönetiminde uygulanabilirliği alanında da geçerlidir.

Teknolojinin kamu kurumlarında uygulanabilir olması için, kamu idarecilerinin, araştırmacıların ve uygulayıcıların, işlemlerin verimliliği ve maliyet kontrolünün ötesine geçen uygulamalar geliştirmenin yollarını aramaya devam etmeleri gerekmektedir. Yöneticiler, teknoloji vasıtasıyla yeni kamusal hizmetler sunarak kamu kurumlarının stratejisini şekillendiren sembolik ve işlevsel etkilerin ötesinde faydalar aramalıdırlar. Bu

kapsamda blokzincirin risk azaltma özelliklerinin, “vatandaşların hayatını kolaylaştıracak hizmetler oluşturulmasında veya mevcut hizmetlerin verimliliğinin artırılmasında kullanılabilir mi”, “akıllı şehirler kurulmasında ne gibi katkılar sağlayabilir”, “arazi ve gayrimenkul anlaşmazlıklarında vatandaşların mülkiyet haklarının korunması için ne gibi yeni çözümler getirebilir”, “vergilendirme sisteminin geliştirilmesinde ve daha adil bir vergilendirme sistemi oluşturulmasında bir faydası olabilir mi” gibi kamu yönetiminin kronikleşmiş sorunlarına cevap olup olmayacağı araştırılmalıdır.

Risk azaltma ve maliyetleri düşürme stratejileri, yeni iş modellerinin gelişmesine ve kamu sektöründe tasarruf fırsatlarının artmasına katkıda bulunabilir. Örneğin, birçok ülkede sağlık bakım maliyetlerinin önemli bir kısmı, özellikle sigorta taleplerinin işlenmesi gibi idari işlemlerden kaynaklanmaktadır. Benzer şekilde, hasta tıbbi geçmişine dair güvenilir kayıtların eksikliği, teşhis testlerinin tekrarlanmasına ve dolayısıyla artan maliyetlere neden olabilir. Blokzincir teknolojileri, bu sorunların üstesinden gelmek ve sağlık geçmişini yetkililere güvenli bir şekilde sunmak için etkili bir çözüm sunabilir.

İkinci bir araştırma yönü, kurulum ve çalıştırma maliyeti, ölçeklenebilirlik sorunları, işlem sürelerindeki gecikmeler, nitelikli personel eksikliği, yasalara ve düzenlemelere uyum sorunları ve etik sorunlar gibi benimseme engellerinin nasıl aşılanacağını incelemektir. Gelecekteki araştırmacılar, bu araştırmada tespit edilen ve teknolojinin kamu yönetimi alanında uygulanabilirliği önündeki engeller olarak sunulan bu engellerin giderilmesi konusunda araştırmalar sunabilirler. Ayrıca uygulama örneklerinin artmasıyla elde edilecek veriler ile hâlihazırda kısıtlı sayıda olan deneysel araştırmalara yoğunlaşarak ve aynı zamanda teknolojiyi yerleştirmeye çalışan kamu kurum ve kuruluşları ile iş birliği yaparak, blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği konusundaki süreçlere katkı sağlayabilirler.

Son olarak gelecekteki araştırmaların bir diğer yönü, örneğin çok taraflı işlemlerin otomatik olarak yürütülmesine ve kaydedilmesine olanak tanıyan akıllı sözleşme uygulamaları oluşturmak amacıyla blokzincirin yapay zekâ ile birleştirilmesi gibi, kamu yönetimine fayda sağlayacak yenilikçi uygulamalar oluşturmak için blokzincirin diğer ileri teknolojilerle nasıl birleştirilebileceğini keşfetmek olabilir.

6.3. Sonuç

Kamu yönetimindeki yeni gelişmeler ve reformlar, yeni teknolojilerin bir sonucu olarak değerlendirilmektedir. Özellikle 2000’li yıllardan sonra bilgi ve iletişim teknolojilerindeki gelişmeler, “e-devlet” kavramını ortaya çıkarmış, vatandaşların günlük yaşamlarını ve hükümetlerle olan ilişkilerini büyük ölçüde değiştirmiştir. Bu gelişmeler, devletlere idari faaliyetlerinin oldukça önemli bir kısmını dijital ortama taşımasına ve kamu yönetiminde verimlilik ve etkililiğin artmasına imkân vermiştir.

Vatandaşların idari hizmetlerden veya genel olarak kamu yönetiminden memnuniyetsizliği, devletin sorumluluk, verimlilik, şeffaflık ve hesap verebilirlik düzeyini artırması için sadece bir göstergedir. Vatandaşların diğer vatandaşlarla yaptıkları iş birliği ve karar alma süreçlerine doğrudan veya dolaylı katılımları da kamu yönetiminde sorumluluk düzeyini yükseltmektedir. Vatandaşlar iyi yönetişimin geliştirilmesi için daha fazla sorumluluk üstlenmeli, bilgi toplamalı ve kendilerine sunulanı seçerken katkıda bulundukları süreçlere sahip çıkmalıdır. Bu noktada blokzincir, vatandaşların yönetsel süreçlere katılımını arttıracak ve bunu yaparken güvenliği ve gizliliği sağlayacak bir teknolojik altyapı özelliği taşımaktadır.

Her ne kadar öncelikle kripto para ve finans sektöründeki kullanımı öne çıksa da, dünya genelinde bir çok devlet tarafından blokzincir teorik veya uygulamalı olarak araştırılmaya devam etmektedir. Blokzincirin birçok alanda eksiklikleri olsa da uygulama tarafında yeni tekniklerin geliştirilmesiyle birlikte mevcut sorunları iyileştirilmeye devam etmekte, daha olgun ve istikrarlı hale gelmektedir. Bu yönde ilerleyen blokzincir tabanlı bir kamu sektörü, hükümete ve vatandaşlara ait verilerin güvenli bir şekilde saklanmasını, operasyonel süreçlerdeki fazlalığın ve hesap verebilirliğin yönetilmesiyle, ilgili maliyetlerin ortadan kaldırılmasını, verimsizliğin azaltılmasını ve hükümet ile sivil kurum/kuruluşlara olan güvenin artırılması gibi birçok sayıda faydayı beraberinde getirebilecektir.

Blokzincir işlemleri güvenilir, hızlı ve etkili bir şekilde yapmayı taahhüt etmektedir. Geleneksel olarak devletler tarafından sağlanan hizmetlerin merkezi olmayan, daha ucuz, daha verimli ve kişiselleştirilmiş bir şekilde verilmesini sağlayacak farklı bir yönetişim modeli olma imkanına sahiptir. Fakat blokzincir işlemleri her zaman en hızlı çözüm değildir. Özellikle açık blokzincirlerde bütün düğümlerin işlemleri kontrol

ettiği iş ispatı mekanizmaları sebebiyle işlem hızı düşmektedir. Doğrulama işlemi genellikle dakikaları bulmaktadır ki bu da geleneksel veri tabanı çözümlerine göre oldukça yavaştır. Dolayısıyla bir blokzincir altyapısı kullanılacağı zaman genel, özel, konsorsiyum ya da hibrit blokzincir türlerinden hangisinin kullanılacağına karar verilmelidir.

Bazı kripto varlıklar, ödeme ve transferleri daha verimli hale getirme potansiyeline sahipken, bazı özellikleri ile kara para aklama ve terörün finansmanı risklerini artırabilir. Özellikle, işlemlerin hızı, küresel erişim ve artan anonimlik potansiyeli ile işlem akışının ve alıcının gizliliği gibi özellikler, kripto varlıkları suç amaçlı kullanımlar için uygun hale getirmektedir. Ayrıca, bazı işlemler finansal aracılardan katılımı olmadan gerçekleştirilebilmektedir. Bu durumda, hiçbir finansal kuruluş, müşteri durum tespiti, kayıt tutma veya şüpheli işlem bildirimini gibi önleyici tedbirleri uygulayamamaktadır. Kripto varlıkların bu özellikleri ve halen gerekli yasal ve düzenleyici altyapısının oluşmamış olması, blokzinciri olumsuz etki etmektedir.

Küreselleşme süreci, vatandaşların yenilik beklentileri ve bilgi ve iletişim teknolojilerinin kullanımı, hükümetlerin vatandaşlarla olan ilişkilerindeki performansını arttırmaya zorunlu kılmaktadır. Kamu yönetimi, vatandaşların ihtiyaç ve beklentilerine uyumlu tepki verebilmek için önemli bir araç olarak vatandaşların karar alma merkezindeki konumunu dikkate almalıdır. Bu bağlamda kamu yönetimi vatandaşların karar alma süreçlerine doğrudan veya dolaylı olarak katılımını kolaylaştırmalıdır.

Blokzincir teknolojisi, küreselleşmenin getirdiği birçok zorluğu çözmeye potansiyeline sahiptir. Küreselleşmenin kendini gösterdiği en büyük alanlardan birisi uluslararası ticaret, bu alandaki en büyük zorluklardan birisi de tedarik zinciri yönetimidir. Blokzincir teknolojisi, ticarete aracılardan kaldırma, sınır ötesi ödemeleri kolaylaştırma ve uluslararası ticaret için akıllı sözleşme altyapısı oluşturabilme olanakları ile tedarik zinciri yönetiminin küreselleşmesine katkı sağlayabilir. Ayrıca blokzincir, kimlikleri doğrulamak için güvenli ve kurcalamaya dayanıklı bir yol sağlayarak dolandırıcılıkla mücadele ve uluslararası seyahat ve çevrimiçi hizmetleri kolaylaştırmaya yardımcı olabilir.

Blokzincir havale hizmetlerini daha verimli ve uygun maliyetli hale getirebilir. Yabancı ülkelerde çalışan birçok kişi parayı kendi ülkelerine geri gönderme ihtiyacı

duymaktadır. Blokzincir, bu transferlerle ilgili ücretleri ve işlem sürelerini azaltabilir. Bununla birlikte küreselleşmeyle birlikte veriler sıklıkla sınırların ötesine akar ve bu da veri gizliliği ve güvenliğine ilişkin endişeleri artırmaktadır. Blokzincir, kullanıcıların kendi bilgileri üzerinde daha fazla kontrole sahip olmasını sağlayacak verileri yönetmek ve korumak için daha güvenli ve şeffaf bir yol sağlayabilir.

Küreselleşmenin getirdiği bir diğer zorluk fikri mülkiyet haklarının korunmasıdır. Blokzincir teknolojisi, dijital varlıkların menşei ve sahipliğini belirlemek için kullanılarak telif haklarının ve patentlerin uygulanmasını kolaylaştırır. Bu konudaki uygulama adımları NFT'ler ile kendini göstermeye başlamıştır. Ayrıca mümkün kıldığı mikro ödeme altyapısı ile fikri hem fikri mülkiyet alanında hem de insani yardım konusunda katkı sağlayabilir. İnsani Yardım ve uluslararası kalkınmada blokzincir, yardımın hedeflenen alıcılara şeffaf ve verimli bir şekilde ulaşmasını sağlayarak yolsuzluk ve kaynakların yanlış tahsisi riskini azaltabilir.

Blokzincir teknolojisi doğası gereği merkeziyetsizlikle uyumludur. Bu bağlamda küreselleşmenin getirdiği zorluklara sağlayabileceği çözümler kadar, yerelleşmenin geliştirilmesi ve yönetilmesiyle ilgili birçok zorluğa da çözüm sağlayabilir.

Blokzincirin merkezi olmayan dağıtık defteri, tüm katılımcıların işlemleri doğrulamasına ve kaydetmesine olanak tanıyarak merkezi yetkililere veya aracılara olan ihtiyacı ortadan kaldırır. Bu, merkezi olmayan sistemlerdeki güven sorunlarının çözülmesine yardımcı olabilir. Teknoloji, bireylerin verileri üzerinde sahiplik ve kontrol sahibi olmalarına olanak tanır. Kullanıcılar, merkezi olmayan uygulamalarda gizliliği ve kontrolü geliştirerek belirli tarafların verilerine erişmesine izin verebilir.

Blokzincir, dijital kimliklerin yerel kurumlar tarafından oluşturulmasına ve yönetilmesine imkân tanıyacak güvenli bir altyapı sağlayabilir. Ayrıca merkezi olmayan karar alma ve yönetim sistemleri için kullanılabilir. Böylelikle şeffaf ve doğrulanabilir oylama mekanizmaları oluşturulabilir. Blokzincir tabanlı DeFi platformları, geleneksel bankalara veya aracılara bağlı kalmadan merkezi olmayan borç verme, borç alma ve finansal varlıkların alım satımını sunar. Bu, finansal katılımı teşvik edebilir ve finans sektöründe merkezileşmeyi azaltabilir.

Bu avantajlara rağmen, blokzincir teknolojisinin yerelleşme sorunlarını çözmedeki etkinliğinin, özel kullanım durumuna ve uygulamaya bağlı olarak değişebileceğini unutmamak önemlidir. Ek olarak, blokzincir sistemlerinin, merkezi olmayan yönetimin faydalarından tam anlamıyla yararlanabilmek için ölçeklenebilirlik, yönetim ve düzenleme zorluklarının dikkate alınması gerekmektedir.

Sonuç olarak blokzincir teknolojisi, dijital stratejilerinin yeniden yapılandırılmasında, kamu kurumlarının verimsiz merkezi sistemlerden uzaklaşmasına yardımcı olma imkanına sahiptir. Ayrıca bu teknoloji, güvenli olmayan ve maliyetli mevcut sistemlere kıyasla daha güvenli, hızlı ve uygun maliyetli yapılar sunmalarına olanak sağlayabilecektir. Bununla birlikte, kamu sektörü kuruluşlarında blokzincirin başarılı bir şekilde benimsenmesine yönelik birtakım zorluklar da mevcuttur. Uygulamaya yönelik bu zorlukları anlamak ve bunların birbirleriyle ilişkilerini belirlemek son derece önemlidir.

Bu araştırmada, blokzincir teknolojisinin kamu yönetiminde uygulanabilirliği incelenmiş ve kamu yönetimine olası etkileri tespit edilmeye çalışılmıştır. Blokzincir teknolojisi; devletler, bireyler ve işletmeler arasında mal ve hizmet işlemlerini destekleyen merkezi olmayan ve dağıtık bir sistem sağlayabilen ilk başarılı uygulamadır. Araştırmanın sonucu, blokzincir teknolojisinin, hayatın neredeyse her alanında olduğu gibi kamu yönetimi alanında da fırsatlar sunduğunu göstermektedir. Hükümetler tarafından gerekli yasal düzenlemelerde kolaylık sağlanır ve teşvikler yapılırsa, kamu yönetimi alanında da blokzincirin gelişimi hızlanacak ve teknoloji başarıyla uygulanabilecektir. Bunun için teknolojinin önündeki engellerin kaldırılması, doğru uygulama stratejilerinin belirlenmesi ve kritik başarı faktörlerinin göz önünde bulundurulması gerekmektedir.

KAYNAKÇA

- Al-Jaroodi, J. ve Mohamed, N. (2019). Blockchain in Industries - A Survey. *IEEE Access*, 7, 36500-36515. doi:10.1109/ACCESS.2019.2903554
- Ahmad, M. ve Al-Saleh, A. (2021). Harnessing Blockchain to Facilitate Digital Transformation: The Future of Public Services in Georgia. *Law in Transition Journal*: 14-23.
- Akbank LAB. (2018). *Akbank'ta Ripple Üzerinden Sterlin Transferleri Başladı!* <<https://www.akbanklab.com/tr/guncel/basinda-biz/akbankta-ripple-uzerinden-sterlin-transferleri-basladi>> (11.07.2021).
- Akçakaya, M. (2017). E-Devlet Anlayışı ve Türk Kamu Yönetiminde E-Devlet Uygulamaları. *Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 8-31.
- Akdemir Altunbaşak, T. (2018). Blok Zincir (Blockchain) Teknolojisi ile Vergilendirme. *Maliye Dergisi*(174), 360-371.
- Akyel, R. ve Köse, H. Ö. (2010). Kamu Yönetiminde Etkinlik Arayışı: Etkin Kamu Yönetimi İçin Etkin Denetimin Gerekliği. *Türki İdare Dergisi*(466), 9-45.
- Al, H. (2022). *Kamu Yönetiminde Paradigma Değişimi*. Sakarya: Sakarya Üniversitesi Sosyal Bilimler Enstitüsü.
- Alam, S., Shuaib, M., Khan, W. Z., Garg, S., Kaddoum, G., Hossain, M. H. ve Zikria, Y. B. (2021). Blockchain-Based Initiatives: Current State and Challenges. *Computer Networks*, 198, 1-20. doi: 10.1016/j.comnet.2021.108395
- Allen, D., Berg, C., Markey-Towler, B., Novak, M. ve Potts, J. (2020). Blockchain and the Evolution of Institutional Technologies: Implications for Innovation Policy. *Research Policy*, 49(1), 1-8.
- Allessie, D., Janssen, M., Ubacht, J., Cunningham, s. ve Van der Harst, G. (2019). The Consequences of Blockchain Architectures for the Governance of Public Services - A Case Study of the Movement of Excise Goods under Duty

- Exemptions. *Information Polity*, 24(4), 1-27.
<<https://core.ac.uk/download/pdf/275571543.pdf>> (15.10.2021).
- Allessie, D., Sobolewski, M. ve Vaccari, L. (2019). *Blockchain for Digital Government*. Luxemburg: European Comission.
- Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. Sebastopol, CA: O'Reilly Media, Inc.
- Antunes, M. E., Barroca, J. G. ve de Oliveira, D. G. (2021). *Urban Future With a Purpose: 12 Trends Shaping the Future of Cities by 2030*. Deloitte.
<<https://www.deloitte.com/global/en/Industries/government-public/perspectives/urban-future-with-a-purpose.html>> (03.04.2023).
- Apostolaki, M., Zohar, A. ve Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. *2017 IEEE Symposium on Security and Privacy (SP)* (375-392). IEEE. doi:10.1109/SP.2017.29
- Ateniese, G., Magri, B., Venturi, D. ve Andrade, E. R. (2017). Redactable Blockchain - or- Rewriting History in Bitcoin and Friends. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (111-126). IEEE. doi:10.1109/EuroSP.2017.37
- Ateş, H. ve Buyruk, G. C. (2018). Bir İyi Yönetişim İlkesi Olarak Katılımcılık ve Türk Kamu Yönetiminde Katılımcılığın Konumu. *Ombudsman Akademik*(Özel Sayı 1), 81-98. doi: 10.32002/ombudsmanakademik.494014
- Audrey, Q., Robin, V., Gilles, W. ve Clementz, G. (2020). Blockchain in Defence: A Breakthrough? *Food for Thought*: 1-28. <<https://finabel.org/blockchain-in-defence-a-breakthrough/>> (20.08.2021).
- Ayberkin, D., Beştaş, M. ve Özen, Ü. (2018). Blok Zinciri ile Gerçek Zamanlı Doğrulanabilir Eğitim Belgeleri. *İktisadi Yenilik Dergisi*, 5(2), 75-82.
- Bains, P. (2022). *Blockchain Consensus Mechanisms: A Primer for Supervisors*. Washington, DC: International Monetary Fund. <<https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/25/Blockchain-Consensus-Mechanisms-511769>> (18.04.2023).

- Baker, J. (2012). The Technology–Organization–Environment Framework. Y. Dwivedi, M. Wade ve D. Schneberger içinde, *Information Systems Theory. Integrated Series in Information Systems* (Cilt 28: 231–245). New York: Springer. doi:10.1007/978-1-4419-6108-2_12
- Banger, G. (2016). *Endüstri 4.0 ve Akıllı İşletme*. Ankara: Dorlion Yayınevi.
- Banque De France. (2023). *The Banque de France Publishes a Second Report to Share Lessons Learned From Its Wholesale CBDC experiments using Distributed Ledger Technologies*. <<https://www.banque-france.fr/en/communique-de-presse/banque-de-france-publishes-second-report-share-lessons-learned-its-wholesale-cbdc-experiments-using>> (19.08.2023).
- Bansal, S., Bionducci, L., Bruno, P., Denecker, O. ve Klopčič, G. (2022). *The Chessboard Rearranged: Rethinking the Next Moves in Global Payments*. McKinsey&Company: <<https://www.mckinsey.com/industries/financial-services/our-insights/the-chessboard-rearranged-rethinking-the-next-moves-in-global-payments>> (14.11.2022).
- Baran, P. (1964). *On Distributed Communications, Memorandum RM-3420-PR*. Santa Monica, CA: The Rand Corporation.
- Barnas, N. B. (2016). *Blockchains in National Defense: Trustworthy Systems in a Trustless World*. Alabama: Air University.
- Baturbara, F. R., Ubacht, J. ve Janssen, M. (2018). Challenges of Blockchain Technology Adoption for e-Government: A Systematic Literature Review. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. Association for Computing Machinery (ACM). doi: 10.1145/3209281.3209317
- Baumunga, W. ve Fomin, V. (2019). Framework for Enabling Order Management Process in a Decentralized Production Network Based on the Blockchain-Technology. *Procedia CIRP*, 79, 456-460. doi:10.1016/j.procir.2019.02.121

- BCTR. (2019). *Blokzinciri Teknolojisi Terminoloji Çalışması*. İstanbul: Türkiye. <https://bctr.org/dokumanlar/Blokzinciri_Teknoloji_Terminoloji.pdf> (07.02.2021)
- BCTR. (2022). *BLOCKCHAIN TÜRKİYE*. <<https://bctr.org/>> (10.12.2022).
- BCTR. (2022). *Yeni Ticaret Biçimleri: Merkez Bankası Dijital Parası (CBDC) Üzerine Değerlendirme Raporu*. İstanbul: TBV. <<https://bctr.org/wp-content/uploads/2022/11/MBRaporuV03.pdf>> (30.12.2022).
- BDDK. (2013). *Bitcoin Hakkında Basın Açıklaması*. <<https://www.bddk.org.tr/Duyuru/Detay/510>> (23/01/2017).
- Becker, G. (2008). *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis*. Bochum: Ruhr-Universität. <http://pauljoseph.news/docs/becker_1.pdf> (29.12.2022).
- Berktaş, S. ve Oraklıbel, R. D. (2021). Sanayi Devrimi ile Gelen Değişim: İş Bölümü ve Yabancılaşma. *Atlas Sosyal Bilimler Dergisi*, 1(6), 112-121. <<https://dergipark.org.tr/tr/pub/atlas/issue/60404/782216>> (22.01.2022).
- Berryhill, J., Bourger, T. ve Hanson, A. (2018). Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. *OECD Working Papers on Public Governance*(28), 1-53. doi: 10.1787/3c32c429-en (11.02.2019).
- BİLGEM. (2018). *Blokzincir Araştırma Ağı (BAĞ) TÜBİTAK BİLGEM'in Öncülüğünde Kuruluyor*. TÜBİTAK BİLGEM: <<https://bilgem.tubitak.gov.tr/tr/haber/blokzincir-arastirma-agi-bag-tubitak-bilgemin-onculugunde-kuruluyor>> (28.05.2019).
- Bistarelli: (2022). Government by Code? Blockchain Applications to Public Sector Governance. *Frontiers in Blockchain*, 5, 15. <<https://www.frontiersin.org/articles/10.3389/fbloc.2022.869665/full>> (27.04.2023).
- Blockchain Economy Istanbul. (2022). *Blockchain Economy İstanbul Summit*. <<https://blockchaineconomy.istanbul/tr>> (04.11.2022).

- Blockchain.com. (2022). *Blockchain Size (MB)*.
<<https://www.blockchain.com/explorer/charts/blocks-size>> (06.06.2022).
- Bondi, A. B. (2000). Characteristics of Scalability and Their Impact on Performance. M. Woodside, H. Gomaa ve D. Menasce içinde, *WOSP '00: Proceedings of the 2nd International Workshop on Software and Performance* (195-203). Ontario: Association for Computing Machinery. doi:10.1145/350391.350432
- Borsa İstanbul. (2018). *Türkiye'nin İlk Finansal Blockchain Projesi Borsa İstanbul Bilişim Teknolojileri Ekibi Tarafından Hayata Geçirildi*.
<<https://www.borsaistanbul.com/tr/duyuru/1096/turkiyenin-ilk-finansal-blockchain-projesi-borsa-istanbul-bilisim-teknolojileri-ekibi-tarafindan-hayata-gecirildi>> (30.03.2019).
- Bozkurt Yüksel, A. E. (2016). Elektronik Para, Sanal Para, Bitcoin Ve Linden Doları'na Hukuki Bir Bakış. *Journal of Istanbul University Law Faculty*, 73(2), 173-220.
- Bron, D. (2023). *Shaping the Future: Navigating the Fourth Industrial Revolution through Innovation, Regulation, and Ethical Consideration*. LinkedIn: <<https://www.linkedin.com/pulse/shaping-future-navigating-fourth-industrial-revolution-daniel-bron/>> (17.07.2023).
- BTCTurk. (2022). *Genel Bakış*. <<https://www.btcturk.com/btcturk/hakkimizda>> (21.10.2022).
- Buterin, V. (2015). *On Public and Private Blockchains*. <<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>> (02.05.2020).
- BZLab. (2022). *BİLGEM'de Blokzincir*. BİLGEM: <<https://blokzincir.bilgem.tubitak.gov.tr/>> (14.12.2022).
- Cagigas, D., Clifton, J., Diaz-Fuentes, D., Fernandez-Gutierrez, M., Echevarria-Cuenca, J. ve Gilsanz-Gomez, C. (2022). Explaining Public Officials' Opinions on Blockchain Adoption - A Vignette Experiment. *Policy and Society*, 41(3), 343–357. doi: 10.1093/polsoc/puab022

- Cai, C. W. (2018). Disruption of Financial Intermediation by FinTech: A review on Crowdfunding and Blockchain. *Accounting & Finance*, 965-992. doi: 10.1111/acfi.12405
- Casino, F., Dasaklis, T. K. ve Patsakis, C. (2019). A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. *Telematics and Informatics*, 36, 55-81. doi:10.1016/j.tele.2018.11.006
- Center of E-Government. (2021). *Blockchain for Digital Government - The ASEAN Way*. Lao PDR.
- Chang, Y., Iakovou, E. ve Shi, W. (2020). Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-Of-The-Art, Challenges and Opportunities. *International Journal of Production Research*, 58(7), 2082-2099. doi: 10.1080/00207543.2019.1651946
- Chaum, D. (1983). *Blind Signatures for Untraceable Payments*. Boston, MA: Springer. doi: 10.1007/978-1-4757-0602-4_18
- Chhina, S., Chadhar, M., Vatanasakdakul, S. ve Chetty, M. (2019). Challenges and Opportunities for Blockchain Technology Adoption: A Systematic Review. *Australasian Conference on Information Systems* (761-770). Perth Western Australia: Association for Information Systems.
- Christidis, K. ve Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292-2303. doi:10.1109/ACCESS.2016.2566339
- Coelho, R., Fishman, J. ve Ocampo, D. G. (2021). *Supervising Cryptoassets for Anti-Money Laundering*. Bank for International Settlements (BIS).
- CoinMarketCap. (2023). *Today's Cryptocurrency Prices by Market Cap*. CoinMarketCap: <<https://coinmarketcap.com/>> (03.01.2023).
- Collins, P. D., Hage, J. ve Hull, F. M. (1988). Organizational and Technological Predictors of Change in Automaticity. *The Academy of Management Journal*, 31(3), 512-543.

- ConsenSys Media. (2018). *The Future of Government on Blockchain*. Medium: <<https://media.consensys.net/the-future-of-government-on-blockchain-32c8a03cf95c>> (24.08.2022).
- CSB. (2022). *Blok Zincir ve Metaverse Teknolojisi Çalışma Heyeti Sonuç Raporu*. Ankara: Coğrafi Bilgi Sistemleri Genel Müdürlüğü.
- Çaptuğ, M. (2021). Hukuki Güvenlik İlkesinin Kavramsal Gelişimi. *Uyuşmazlık Mahkemesi Dergisi*(17), 133-160. doi.org/10.18771/mdergi.957891
- Çarıkçı, O. (2010). Türkiyede E-Devlet Uygulamaları Üzerine Bir Araştırma. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 2(12), 95-122.
- Çarkacıoğlu, A. (2016). *Kripto-Para Bitcoin*. Ankara: Sermaye Piyasası Kurulu Araştırma Dairesi.
- Çetiner, M. (2018). Bitcoin (Kripto Para) ve Blok Zincirin Yeni Dünyaya Getirdikleri. *Istanbul Journal of Social Sciences*(20), 1-16.
- Deloitte. (2016). *Blockchain: Opportunities for Health Care*. Mart 18, <<https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html>> (18.03.2018).
- Deloitte. (2018). *Assessing Blockchain Applications For The Public Sector - Blockchain Basics For Government*. Deloitte Insights.
- Deloitte. (2018). *Blockchain: A Technical Primer*. Deloitte Insights. <<https://www2.deloitte.com/za/en/insights/topics/emerging-technologies/blockchain-technical-primer.html>> (13.01.2021).
- Deloitte. (2021). *Blockchain: Ready for Business*. Deloitte Insights. <<https://www.deloitte.com/global/en/our-thinking/insights/topics/technology-management/tech-trends/2022/blockchain-trends.html>> (18.02.2022).
- Deloitte. (2021). *Deloitte's 2020 Global Blockchain Survey From promise to reality*. Deloitte Insights. <<https://www2.deloitte.com/mt/en/pages/technology/articles/2020-global-blockchain-survey.html>> (02.01.2022).

- Deloitte. (2022). *Deloitte's 2021 Global Blockchain Survey: A New Age of Digital Assets*. Deloitte Insights. <<https://www2.deloitte.com/jp/en/pages/financial-services/articles/bk/2021-global-blockchain-survey.html>> (19.03.2023).
- Demir, İ. ve Aktan, C. C. (2016). Resistance to Change in Government: Actors And Factors That Hinder Reform in Government. *International Journal of Social Sciences and Humanity Studies*, 8(2), 226-242.
- Dimitropoulos, G. (2022). The Use of Blockchain by International Organizations: Effectiveness and Legitimacy. *Policy and Society*, 41(3), 328–342. doi: 10.1093/polsoc/puab021
- Dinçer, Ö. ve Yılmaz, C. (2003). *Değişimin Yönetimi İçin Yönetimde Değişim*. Ankara: T. C. Başbakanlık.
- Douceur, J. R. (2002). The Sybil Attack. *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 251-260.
- Dulupçu, M. A., Yiyit, M. ve Genç, A. G. (2017). Dijital Ekonominin Yükselen Yüzü: Bitcoin'in Değeri ile Bilinirliği Arasındaki İlişkinin Analizi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler*, 22(Kayfor15 Özel Sayısı), 2241-2258.
- EBSI. (2022). *European Blockchain Services Infrastructure*. European Comission: <<https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure>> (05.12.2022).
- EBSI. (2022). *Experience Cross-borders Services with EBSI*. European Comission: <<https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>> (21.10.2022).
- e-Estonia. (2022). *Cyber Security*. e-estonia.com: <<https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>> (02.04.2022).
- Ehsani, F. (2021). *The False Promise Blockchains Will Revolutionize Real-World Assets*. CoinDesk: <<https://www.coindesk.com/markets/2019/01/05/the-false-promise-blockchains-will-revolutionize-real-world-assets/>> (19.06.2023).

- Einaste, T. (2018). *Blockchain and healthcare: The Estonian experience*. Nortal: <<https://nortal.com/insights/blockchain-healthcare-estonia/>> (17.12.2019).
- Eroğlu, A. (2023). Kamu Mali Denetiminin Dijitalleşmesi: Blokzincir Teknolojisinin İncelenmesi. *Alanya Akademik Bakış*, 7(1), 187-207.
- Erola, I., Neuhoferb, I. O., Dogru, T., Oztel, A., Searcy, C. ve Yorulmaz, A. C. (2022). Improving Sustainability in the Tourism Industry Through Blockchain Technology: Challenges and Opportunities. *Tourism Management*, 93(104628), 1-20. doi: 10.1016/j.tourman.2022.104628
- Eryılmaz, B., Sözen, S. ve Köseoğlu, Ö. (2019). *Kamu Yönetimi*. Eskişehir: Anadolu Üniversitesi.
- Ettlie, J. E., Bridges, W. P. ve O'Keefe, R. D. (1984). Organization Strategy and Structural Differences for Radical Versus Incremental Innovation. *Management Science*, 30(6), 682–695. <<https://www.jstor.org/stable/2631748>> (03.06.2023).
- European Commission. (2019). *Blockchain Now And Tomorrow - Assessing Multidimensional Impacts Of Distributed Ledger Technologies*. Brussels: Joint Research Centre.
- Eyal, I. ve Sirer, E. G. (2013). Majority is not Enough: Bitcoin Mining is Vulnerable. *CoRR*, doi: 10.48550/arXiv.1311.0243
- Filippi, P. ve Hassan: (2016). Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code. *First Monday*, 21(12). doi: 10.5210/fm.v21i12.7113
- Frankenfield, J. (2019). *Nonce*. <<https://www.investopedia.com/terms/n/nonce.asp>> (12.11.2019).
- Frankenfield, J. ve Anderson: (2023). *Proof of Elapsed Time (PoET) Definition, Purposes, Vs. PoW*. Investopedia: <<https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp>> (01.09.2023).
- Freeman, R. E. (1984). *Strategic Management: A Stakeholder Approach*. Minnesota: Pitman.

- Fridgen, G., Guggenmos, F., Lockl, J., Rieger, A. ve Urbach, N. (2019). *Supporting Communication and Cooperation in the Asylum Procedure with Blockchain Technology - A Proof of Concept by the Federal Office for Migration and Refugees*. Ausburg: Federal Office for Migration and Refugees. <<https://www.bamf.de/SharedDocs/Anlagen/EN/Digitalisierung/blockchain-whitepaper-2018.html?nn=1494174>> (21.10.2022).
- Furlonger, D. ve Valdes, R. (2017). *Practical Blockchain: A Gartner Trend Insight Report*. Gartner. <<https://www.gartner.com/en/documents/3628617>> (09.07.2023).
- Gabison, G. (2017). Policy Considerations for the Blockchain Technology Public and Private Applications. *SMU Science and Technology Law Review*, XIX, 327-350. <<https://scholar.smu.edu/scitech/vol19/iss3/4>> (11.11.2020).
- Gate.io. (2022). *Gate.io Kripto Piyasası & Yatırım Raporu: Türkiye 2022*. <<https://www.gate.io/tr/article/28485/gate.io-crypto-market-investment-report-turkiye-2022>> (03.01.2023).
- Gaur, V. ve Gaiha, A. (2020). *Building a Transparent Supply Chain*. Harward Business Review: <<https://hbr.org/2020/05/building-a-transparent-supply-chain>> (14.04.2021).
- GBBC. (2021). *Global Standards Mapping Initiative (GSMI) 2.0 - South Korea*. Global Blockchain Business Council.
- Gencer, A. E., Basu, S., Eyal, I., Renesse, R. v. ve Sirer, E. G. (2018). Decentralization in Bitcoin and Ethereum Networks. *Financial Cryptography and Data Security (FC)*. doi: 10.48550/arXiv.1801.03998
- Georgiou, M. (2023). *Top 7 Use Cases of Blockchain in the Insurance Industry (with Examples)*. Imaginovation Insider: <<https://imaginovation.net/blog/blockchain-insurance-industry-examples/>> (24.06.2023).
- Gerdan, D., Koç, C. ve Vatandaş, M. (2020). Gıda Ürünlerinin İzlenebilirliğinde Blok Zinciri Teknolojisinin Kullanımı. *Tarım Makinaları Bilimi Dergisi*, 16(2), 8-14.

- Globerman: (1975). Technological Diffusion in the Canadian Tool and Die Industry. *The Review of Economics and Statistics*, 57(4), 428-434.
- Gohil, D. ve Thakker: V. (2021). Blockchain-Integrated Technologies for Solving Supply Chain Challenges. *Modern Supply Chain Research and Applications*, 3(2), 78-97. doi:10.1108/MS CRA-10-2020-0028
- GovChain. (2021). <<https://govchain.world/>> (12.10.2022).
- Government Office for Science. (2016). *Distributed Ledger Technology: Teyond Block Chain*. Government Office for Science.
- Gökçe, O. ve Turan, E. (2008). Kamu Yönetiminin Dönüşümü ve Dönüşümün Temel Unsurları. *Sosyal Ekonomik Araştırmalar Dergisi*, 8(15), 175-200. <<https://dergipark.org.tr/tr/download/article-file/289411>> (06.06.2023).
- Greenspan, G. (2015). *Avoiding the Pointless Blockchain Project*. MultiChain: <<https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/>> (07.08.2019).
- Grunspan, C. ve Pérez-Marco, R. (2018). On Profitability of Selfish Mining. *CoRR*, 1-20. doi: 10.48550/arXiv.1805.08281
- Güven, V. ve Şahinöz, E. (2018). *Blokzincir - Kripto Paralar - Bitcoin: Satoshi Dünyayı Değiştiriyor*. İstanbul: Kronik Kitap.
- Hargrave, J. ve Karnoupakis, E. (2021). *Blockchain Success Stories: Case Studies from the Leading Edge of Business*. Sebastopol: O'Reilly.
- Heeks, R. ve Bailur: (2007). Analyzing E-Government Research: Perspectives, Philosophies, Theories, Methods and Practise. *Government Information Quarterly*(24), 243-265. doi:10.1016/j.giq.2006.06.005
- Hill, B., Chopra, S. ve Valencourt, P. (2018). *Blockchain Quick Reference: A Guide to Exploring Decentralized Blockchain Application Development*. Birmingham: Packt Publishing.
- Hooda, P. (2022). *practical Byzantine Fault Tolerance(pBFT)*. GeeksforGeeks: [geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/](https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/)> (08.01.2023).

- Hyvärinen, H., Risius, M. ve Friis, G. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. *Business & Information Systems Engineering*, 59(6), 441–456.
- IBM. (2017). *Building Trust in Government: Exploring the Potential of Blockchains*. IBM Institute for Business Value. <<https://www.ibm.com/downloads/cas/WJNPLNGZ>> (10.07.2022).
- IBM. (2018). *What is Blockchain Technology?* IBM: <<https://www.ibm.com/topics/blockchain>> (04.02.2019).
- IBM. (2021). *What is Industry 4.0?* IBM: <<https://www.ibm.com/topics/industry-4-0>> (25.09.2022).
- IBM. (2022). *What is Blockchain Security?* IBM: <<https://www.ibm.com/topics/blockchain-security>> (07.07.2023).
- IMF. (2022). Blockchain Consensus Mechanisms: A Primer for Supervisors. (P. Bains, Dü.) *Fintech Notes*(2022/003), 1-18.
- İnce, N. M. (2001). *Elektronik Devlet: Kamu Hizmetlerinin Sunulmasında Yeni İmkanlar*. Devlet Planlama Teşkilatı.
- ISTBCW. (2022). *Manifesto*. Istanbul Blockchain Women: <<https://istanbulblockchainwomen.org/>> (22.11.2022).
- IUMI. (2022). *IUMI's 2022 Analysis of the Global Marine Insurance Market*. Hamburg: International Union of Marine Insurance. <<https://iumi.com/statistics/public-statistics>> (22.12.2022).
- Ivičević: (2022). *Blockchain part Three: Types of Blockchains and their Applications*. Serengeti Software Tech: <<https://serengetitech.com/tech/blockchain-part-three-types-of-blockchains-and-their-applications/>> (13.03.2023).
- Jaikaran, C. (2018). Beyond Bitcoin: Emerging Applications for Blockchain Technology. *Congressional Research Service Prepared for Congress* (1-9). Committee on Science, Space and Technology. <<https://crsreports.congress.gov/product/pdf/TE/TE10025>> (12.12.2020).

- Joint Research Centre. (2019). *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts Of Distributed Ledger Technologies*. Brussels: European Commission.
- Joshi, A. P., Han, M. ve Wang, Y. (2018). A Survey on Security and Privacy Issues of Blockchain Technology. *Mathematical Foundations of Computing*, 121-147. doi:10.3934/mfc.2018007
- Jost, J. T. (2015). Resistance to Change - A Social Psychological Perspective. *Social Research*, 82(3), 607-636.
- Jurowiec, P. (2018). *Blockchain Applications in the World Tax Regime*. Good Audience: <<https://blog.goodaudience.com/blockchain-applications-in-the-world-tax-regime-ea2111741f0b>> (05.11.2019).
- Kagermann, H., Wolf-Dieter, L. ve Wahlster, W. (2011). Industrie 4.0 –Mit dem Internet der Dinge auf dem Weg zur 4. Industriellen Revolution. *VDI Nachrichten*(13): 2.
- Kamal, R. (2022). *IoT In Blockchain: Benefits, Use Cases, and Challenges*. Intuz: <<https://www.intuz.com/blog/iot-in-blockchain-benefits-use-cases-and-challenges>> (01.12.2022).
- Karagöz, U. (2020). *Türkiye’de Kamu Yönetiminin Dijital Dönüşümü: Ulusal Veri Santrali Model Önerisi*. Ankara: Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü.
- Karasoy, H. A. ve Babaoğlu, P. (2020). Türkiye’de Elektronik Devletten Dijital Devlete Doğru. *Karadeniz Sosyal Bilimler Dergisi*, 12(23), 115-134. doi: 10.38155/ksbd.825899
- Kassen, M. (2021). Blockchain and e-Government Innovation – Automation of Public Information Processes. *Information Systems*, 103, 1-11. doi:10.1016/j.is.2021.101862
- Kaura, C. (2023). *Data-Driven Decision-Making in Government: Improving Policy Formulation and Public Services*. LinkedIn: <<https://www.linkedin.com/pulse/data-driven-decision-making-government-improving-policy-chirag-kaura/>> (10.08.2023).

- Kejriwal, S. ve Mahajan: (2017). *Blockchain in Commercial Real Estate*. Deloitte
<<https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html>> (10.10.2019).
- Khan, D., Jung, L. T. ve Hashmani, M. A. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*, 11(20), 1-27. doi:10.3390/app11209372
- Koca, D. (2020). Sanayi Devrimlerinin Tarihsel Arka Planı ve İşgücü Becerileri Üzerindeki Yansımaları. *OPUS International Journal of Society Researches*, 16(31), 4531-4558. doi:10.26466/opus.704841
- Kossow, N. ve Dykes, V. (2018). *Linkages Between Blockchain Technology And Corruption Issues*. Berlin: Transparency International.
- KPMG. (2021, Haziran 3). Uluslararası Ticarete Blokzinciri... *Dünya Gazetesi*: 23. <<https://home.kpmg/tr/tr/home/gorusler/2021/06/uluslararasi-ticarete-blokszinciri-donemi-basliyor.html>> (02.01.2023).
- Krichen, M., Ammi, M., Mihoub, A. ve Almutiq, M. (2022). Blockchain for Modern Applications: A Survey. *Sensors*, 22(14). doi: 10.3390/s22145274
- KRIPTOMAT. (2022). *What Is the Future of the Blockchain Revolution?* <<https://kriptomat.io/blockchain/future-of-blockchain/>> (05.05.2023).
- Kshetri, N. ve Voas, J. (2018). Blockchain-Enabled E-Voting. *IEEE*. <<https://www.researchgate.net/publication/326239528>> (05.05.2018).
- Kumar, M. (2017). Deloitte Survey: Blockchain Reaches Beyond Financial Services With Some Industries Moving Faster. *Deloitte Press Release*. <<https://www2.deloitte.com/hr/en/pages/press/articles/blockchain-2017.html>> (16.10.2021).
- Lamport, L., Shostak, R. ve Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, 4(3), 382–401.
- Leigh, A. ve Atkinson, R. D. (2001). Breaking Down Bureaucratic Barriers: The Next Phase of Digital Government. *Progressive Policy Institute*: 1-29.

- <[http://andrewleigh.org/pdf/Digital%20government%20report%20\(PPI\).pdf](http://andrewleigh.org/pdf/Digital%20government%20report%20(PPI).pdf)>
(23.01.2022).
- Lemieux, V. L. (2019). Blockchain and Public Record Keeping: Of Temples, Prisons, and the (Re)Configuration of Power. *Front. Blockchain*, 2, 14. doi:10.3389/fbloc.2019.00005
- Li, L. (2022). Reskilling and Upskilling the Future-ready Workforce for Industry 4.0 and Beyond. *Information Systems Frontiers*, 1-16. <<https://doi.org/10.1007/s10796-022-10308-y>>
- Lin, I.-C. ve Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5): 653-659.
- Lindman, J., Berryhill, J., Welby, B. ve Barbieri, M. P. (2020). *The Uncertain Promise of Blockchain for Government*. OECD. doi:<<https://dx.doi.org/10.1787/d031cd67-en>>
- Lounds, M. (2020). *Blockchain and Its Implications for the Insurance Industry*. Munich RE: <<https://www.munichre.com/us-life/en/perspectives/underwriting/blockchain-implications-insurance-industry.html>> (04.11.2021).
- Lucia, C., Zhiwei, G. ve Michele, N. (2023). Biometrics for Industry 4.0: A Survey of Recent Applications. *Journal of Ambient Intelligence and Humanized Computing*(14), 11239–11261. doi: 10.1007/s12652-023-04632-7
- Makridakis, S. ve Christodoulou, K. (2019). Blockchain: Current Challenges and Future Prospects/Applications. *Future Internet*, 11(12), 1-16. doi:10.3390/fi11120258
- Manski: (2017). Building the Blockchain World: Technological Commonwealth or Just More of The Same. *Strategic Change*, 26(5), 511-522. <<https://onlinelibrary.wiley.com/doi/10.1002/jsc.2151>> (21.06.2019).
- Marr, B. (2017). *A Short History Of Bitcoin And Crypto Currency Everyone Should Read*. Forbes: <<https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/?sh=378b60633f27>> (15.02.2022).

- Marr, B. (2018). *The 5 Big Problems With Blockchain Everyone Should Be Aware Of*. Bernard Marr & Co.: <<https://bernardmarr.com/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/>> (20.06.2023).
- MASAK. (2021). *Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar*. Ankara: Hazine ve Maliye Bakanlığı.
- Mattila, J. (2016). *The Blockchain Phenomenon - The Disruptive Potential of Distributed Consensus Architectures*. Berkeley, CA: Berkeley Roundtable On The International Economy (BRIE). <<https://brie.berkeley.edu/sites/default/files/juri-mattila-.pdf>> (10.01.2018).
- McKenzie, I. ve Taylor, M. (2017). *An Introduction to Blockchain: The Key Legal Issues*. <<https://www.osborneclarke.com/insights/an-introduction-to-blockchain-the-key-legal-issues/>> (17.01.2019).
- McMurren, J., Young, A. ve Verhulst: (2018). *Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers*. GOVLAB <<https://blockchan.ge/blockchange-land-registry.pdf>> (19.02.2021).
- Meijer, C. R. (2015). The UK and Blockchain Technology: A Balanced Approach. *Journal of Payments Strategy & Systems*, 9(4), 220-229 <<https://hstalks.com/article/2295/the-uk-and-blockchain-technology-a-balanced-approa/>> (04.04.2019).
- Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y. ve Han, J. (2018). When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access*, 6, 10179-10188. doi:10.1109/ACCESS.2018.2799854
- Mentsiev, A. U., Guzueva, E. R. ve Magomaev, T. R. (2020). Security Challenges of the Industry 4.0. *Journal of Physics: Conference Series* (1-4). IOP Publishing. doi:10.1088/1742-6596/1515/3/032074
- Merkle, R. C. (1988). *Protocols For Public Key Cryptosystems*. Sunnyvale, CA: ELXSi International.

- Mermin, N. D. (2007). *Quantum Computer Science: An Introduction*. New York: Cambridge University Press.
- Mishra, R., Singh, R. K., Kumar, S., Mangla: K. ve Kumar, V. (2023). Critical Success Factors of Blockchain Technology Adoption for Sustainable and Resilient Operations in the Banking Industry During an Uncertain Business Environment. *Electronic Commerce Research*. doi:10.1007/s10660-023-09707-3
- Monetary Authority of Singapore. (2022). *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology*. Monetary Authority of Singapore: <<https://www.mas.gov.sg/schemes-and-initiatives/project-ubin>> (01.01.2023).
- Mougayar, W. (2015). *A Decision Tree for Blockchain Applications: Problems, Opportunities or Capabilities?* S-U-M: <<http://startupmanagement.org/2015/11/30/a-decision-tree-for-blockchain-applications-problems-opportunities-or-capabilities/>> (03.03.2019).
- Möser, M. (2013). Anonymity of Bitcoin Transactions. *Münster Bitcoin Conference (MBC)*. Münster.
- Mulligan, C. ve Omar, L. (2016). *The Potential for Blockchain in Local Government*. Cities Today: <<http://cities-today.com/the-potential-for-blockchain-in-local-government/>> (06.06.2018).
- Nakamoto: (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org: <<https://bitcoin.org/bitcoin.pdf>> (09.10.2018).
- Narayanan, A., Bonneau, J., Felten, E., Miller, A. ve Goldfeder: (2016). *Bitcoin and Cryptocurrency Technologies - A Comprehensive Introduction*. New Jersey: Princeton University Press.
- Nasdaq. (2019). *Vive la Blockchain: Why the French Government is Embracing Blockchain and Implementing Regulation*. www.nasdaq.com: <<https://www.nasdaq.com/articles/vive-la-blockchain%3A-why-the-french-government-is-embracing-blockchain-and-implementing>> (03.06.2020).
- OECD. (2014). *Recommendation of the Council Digital Government Strategies*. OECD Public Governance and Territorial Development Directorate.

- Ølnes, S. ve Jansen, A. (2017). Blockchain Technology as s Support Infrastructure in e-Government. *International Conference on Electronic Government* (215–227). Cham: Springer. doi: 10.1007/978-3-319-64677-0_18
- Ølnes, S. ve Jansen, A. (2018). Blockchain Technology as Infrastructure in Public Sector - an Analytical Framework. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. Delft: ACM Publications.
- Ølnes, S., Ubacht, J. ve Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, 34(3), 355-364. doi: 10.1016/j.giq.2017.09.007
- Ooijen, C. v. (2017). *How Blockchain Can Change Voting: The Colombian Peace Plebiscite*. OECD Forum: <<https://www.oecd-forum.org/posts/28703-how-blockchain-can-change-voting-the-colombian-peace-plebiscite>> (02.01.2020).
- Orcutt, M. (2017). *Who Will Build the Health-Care Blockchain?* MIT Technology Review: <<https://www.technologyreview.com/2017/09/15/149153/who-will-build-the-health-care-blockchain/>> (03.09.2019).
- Öktem, M. K. ve Aydın, M. D. (2005). Bilgi Teknolojileri ve Türk Kamu Yönetiminde Dönüşüm. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 23(1), 257-282.
- Önen: M. ve Kahraman, N. (2022). Kamu Hizmetlerinin Sunumunda Dijitalleşme Üzerine Bir Değerlendirme. *Uluslararası Akademik Birikim Dergisi*, 5(5), 424-432.
- Özaltın, O. ve Ersoy, M. (2020). Kamu Yönetiminde Blokzincir Kullanımı: D5 Örneği. *Nevşehir Hacı Bektaş Üniversitesi SBE Dergisi*, 10(2), 746-763. doi:10.30783/nevsosbilen.748379
- Özdoğan, O. (2017). *Endüstri 4.0: Dördüncü Sanayi Devrimi ve Endüstriyel Dönüşümün Anahtarları*. İstanbul: Pusula. <<https://books.google.com.tr/books?id=zktDwAAQBAJ>> (04.11.2022).

- Öztürk, T. (2018). *Bitcoin Zorluğu (Difficulty) Nedir?* <<https://medium.com/@toprakozt/bitcoin-zorlu%C4%9Fu-difficulty-nedir-73487053d4ac>> (11.12.2019).
- Palfreyman, J. (2015). *Blockchain for Government?* Medium: <<https://medium.com/@JohnP261/blockchain-for-government-184ace54756d>> (18.02.2018).
- Pandey, A. (2020). *How Governments Can Harness the Potential of Blockchain*. McKinsey: <<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/how-governments-can-harness-the-potential-of-blockchain>> (12.07.2023).
- Patel, D., Bothra, J. ve Patel, V. (2017). Blockchain exhumed. *2017 ISEA Asia Security and Privacy (ISEASP)*, 1-12. doi: 10.1109/ISEASP.2017.7976993
- Paul, E. (2017). *What is Digital Signature: How It Works, Benefits, Objectives, Concept*. EMP Trust HR: <<https://www.emptrust.com/blog/benefits-of-using-digital-signatures/>> (12.09.2020).
- Peck, M. E. (2017). Blockchain World - Do You Need a Blockchain? This Chart Will Tell You If the Technology can Solve Your Problem. *IEEE Spectrum*, 54(10), 38-60. doi:10.1109/MSPEC.2017.8048838
- Pirinççi, A. E. (2018). Yeni Dünya Düzeninde Sanal Para Bitcoin'in Değerlendirilmesi. *International Journal of Economics Politics Humanities and Social Sciences*, 1(1), 45-52.
- Popper, N. (2015). *Digital Gold - Bitcoin and the Inside Story of the Misfits and the Millionaires Trying to Reinvent Money* (1'inci b.). New York, NY, USA: Harpercollins.
- Prager, F., Martinez, J. ve Cagle, C. (2021). Blockchain and Regional Workforce Development: Identifying Opportunities and Training Needs. C. G. Reddick, M. P. Rodríguez-Bolívar ve H. J. Scholl içinde, *Blockchain and the Public Sector: Theories, Reforms, and Case Studies* (Cilt 36: 47-72). Cham: Springer. doi:10.1007/978-3-030-55746-1_3

- PRNewswire. (2018). *Pacific MSC Sustainable Tuna Now Traceable via Ethereum Blockchain*. Cision PRNewswire: <<https://www.prnewswire.com/news-releases/pacific-msc-sustainable-tuna-now-traceable-via-ethereum-blockchain-856511594.html>> (04.03.2021).
- Puthal, D., Malik, N. S., Mohanty: P. ve Kougianos, E. (2018). Everything You Need to Know About the Blockchain: Its Promise, Components, Processes, and Problems. *IEEE Consumer Electronics Magazine*, 7(4), 6-14.
- PwC. (2018). *Blockchain is here. What's your next move?* PwC: <<https://www.pwc.com/jg/en/publications/blockchain-is-here-next-move.html>> (23.10.2022).
- Ramiller, N. C. ve Swanson, E. B. (2003). Organizing Visions for Information Technology and the Information Systems Executive Response. *Journal of Management Information Systems*, 20(1), 13-50. <<https://www.jstor.org/stable/40398616>> (29.01.2022)
- Rana, N. P., Dwivedi, Y. K. ve Hughes, D. L. (2022). Analysis of Challenges for Blockchain Adoption Within the Indian Public Sector: An Interpretive Structural Modelling Approach. *Information Technology & People*, 35(2), 548-576. doi: 10.1108/ITP-07-2020-0460
- Rauchs, M., Andrew, G., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., Zhang, B. Z., vd. (2018). *Distributed Ledger Technology Systems: A Conceptual Framework*. Cambridge Centre for Alternative Finance. doi:10.2139/ssrn.3230013
- Rebello, G. A., Camilo, G. F., Guimaraes, L. C., Souza, L. A., Thomaz, G. A. ve Duarte, O. C. (2022). A Security and Performance Analysis of Proof-Based Consensus Protocols. *Annals of Telecommunications*(77), 517-537. doi: 10.1007/s12243-021-00896-2
- Reddick, C. G., Rodríguez-Bolívar, M. P. ve Scholl, H. J. (2021). *Blockchain and the Public Sector: Theories, Reforms, and Case Studies*. Cham: Springer.

- REI. (2022). *Blockchain—Smart Use Cases in the Public Sector*. REI Systems: <<https://www.reisystems.com/blockchain-smart-use-cases-in-the-public-sector/>> (01.01.2023).
- Republic of Turkey Ministry of Environment, Urbanization and Climate Change. (2020). *Smart Governance: Smart Cities Capacity Building and Guidance Project*. Directorate General Of Geographic Information Systems. <https://www.akillisehirler.gov.tr/wp-content/uploads/KapasiteGelistirme/Egitim_Pdf/ingilizce/smart_governance_web_formati.pdf> (14.03.2021).
- Rijmenam, M. V., Schweitzer, J. ve Williams, M.-A. (2017). A Distributed Future: How Blockchain Affects Strategic Management, Organisation Design & Governance. *Academy of Management Proceedings*, 1-46.
- Ritchie, J. (2022). *The History of Money: How Our Currency Evolved from Pelts to Money*. INTUIT: <<https://mint.intuit.com/blog/investments/the-history-of-money/>> (14.02.2023).
- Rose, C. (2015). The Evolution Of Digital Currencies - Bitcoin, A Cryptocurrency Causing A Monetary Revolution. *International Business & Economics Research Journal*, 14(4), 617-622. doi: 10.19030/iber.v14i4.9353
- Rudden, J. (2022). *Forecast of the Global Insurance Market in 2021 and 2022, with Forecasts from 2023 to 2026*. Statista: <<https://www.statista.com/statistics/1192960/forecast-global-insurance-market/>> (07.01.2023).
- Ruige, A., Üskent, S. ve Micka, P. (2014). *Yönetişim ve Katılım: Etkili Katılım İçin Araçlar, Yöntemler, Mekanizmalar*. Ankara: TEPAV.
- S, K. ve Sarath, G. (2020). Securing Land Registration using Blockchain. *Procedia Computer Science*(171), 1708-1715. doi: 10.1016/j.procs.2020.04.183
- Saberi, S., Kouhizadeh, M., Sarkis, J. ve Shen, L. (2019). Blockchain Technology and Its Relationships to Sustainable Supply Chain Management. *International Journal of Production Research*, 57(7), 2117–2135. doi: 10.1080/00207543.2018.1533261

- Sage. (2023). *Where does the phrase, "If you build it, they will come," come from? What does it mean?* Quora: <<https://www.quora.com/Where-does-the-phrase-If-you-build-it-they-will-come-come-from-What-does-it-mean>> (04.07.2023).
- Sanka, A. İ., Irfan, M., Huang, I. ve Cheung, R. C. (2021). A Survey of Breakthrough in Blockchain Technology - Adoptions, Applications, Challenges and Future Research. *Computer Communications*, 169, 179-201. doi: 10.1016/j.comcom.2020.12.028
- Sayıştay. (2023). *Denetim Alanı*. T.C. Sayıştay Başkanlığı: <<https://www.sayistay.gov.tr/pages/42-denetim-alani>> (10.09.2023).
- Sayson, M. (2017). *Types of Failures in Distributed Systems*. <<https://www.marksayson.com/blog/types-of-failures-in-distributed-systems/>> (23.08.2019).
- SBB. (2019). *On Birinci Kalkınma Planı*. Ankara: T.C. Cumhurbaşkanlığı. <https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Planı-2019-2023.pdf> (11.06.2022).
- Schatsky, D. ve Muraskin, C. (2015). *Beyond Bitcoin: Blockchain is Coming to Disrupt Your Industry*. Deloitte University Press. <<https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html>> (05.03.2018).
- Schatsky, D., Muraskin, C. ve Gurumurthy, R. (2015). *Cognitive Technologies: The Real Opportunities for Business*. Deloitte. Deloitte: <<https://www2.deloitte.com/us/en/insights/deloitte-review/issue-16/cognitive-technologies-business-applications.html>> (13.06.2023).
- Schneier, B. (2019). *There's No Good Reason to Trust Blockchain Technology*. Wired: <<https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/>> (20.06.2023).
- Schrauf, S. ve Bertram, P. (2016). Industry 4.0: How Digitization Makes The Supply Chain More Efficient, Agile, and Customer-Focused. *Strategy&*, 1-32.

- <<https://www.strategyand.pwc.com/gx/en/insights/2016/industry-4-digitization/industry40.pdf>> (10.12.2018).
- Schwab, K. (2016). *The Fourth Industrial Revolution*. Cenevre: World Economic Forum.
- Settlemint. (2020). *Carrefour Brings Full Transparency to the Food Supply Chain*. <<https://www.settlemint.com/stories-carrefour>> (10.07.2023).
- Settlemint. (2020). *Indonesia secures election results and speeds up reporting*. <<https://www.settlemint.com/stories-indonesia/>> (11.07.2023).
- Sevinç, İ. (2006). *Bilgi Teknolojileri Kullanımının Kamu Kurumları Üzerindeki Etkileri: Kavramsal Ve Ampirik Bir Çalışma (Konya Örneği)*. Konya: Selçuk Üniversitesi.
- Shang, Q. ve Price, A. (2019). A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations: Technology, Governance, Globalization*, 12(3-4), 72-78.
- Sheldon, R. (2022). *Definition: Bit (Binary Digit)*. TechTarget: <<https://www.techtarget.com/whatis/definition/bit-binary-digit>> (23.04.2023).
- Shen, C. ve Pena-Mora, F. (2018). Blockchain for Cities - A Systematic Literature Review. *IEEE Access*, 76787-76819. doi: 10.1109/ACCESS.2018.2880744
- Shiva, M., Matsu, J., Ishibashi, Y. ve Rosenbach, F. (2023). *Exploring Blockchain Technologies for Collaboration and Partnerships*. Blavatnik School of Government, University of Oxford: Government Outcomes Lab <<https://golab.bsg.ox.ac.uk/documents/exploring-blockchain-technologies-for-collaboration-and-partnerships.pdf>> (08.08.2023).
- Silva, T. B., Morais, E. S., Almeida, L. F., Rosa Righi, R. ve Alberti, A. M. (2020). Blockchain and Industry 4.0: Overview, Convergence, and Analysis. R. d. Rosa Righi, A. M. Alberti ve M. Singh içinde, *Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment* (27-58). Singapore: Springer Singapore. doi:10.1007/978-981-15-1137-0_2

- Sinclair, D., Flippi, P. D. ve Potts, J. (2018). Blockchains and the Economic Institutions of Capitalism. *Journal of Institutional Economics*, 14(4), 639-658. doi:10.1017/S1744137417000200
- Sinclair, D., Primavera, D. ve Potts, J. (2016). Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. *SSRN Electronic Journal*, 1-27. doi: 10.2139/ssrn.2811995
- Soori, M., Arezoo, B. ve Dastres, R. (2023). Internet of Things for Smart Factories in Industry 4.0, A Review. *Internet of Things and Cyber-Physical Systems*, 3, 192-204. doi: 10.1016/j.iotcps.2023.04.006
- Soylu, A. (2018). Endüstri 4.0 ve Girişimcilikte Yeni Yaklaşımlar. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*(32), 43-57. doi: 10.30794/pausbed.424955
- Spielman, A. (2018). *Blockchain and Commercial Real Estate*. <https://www.sior.com/docs/default-source/Thought-leadership/blockchain-and-commercial-real-estate-real-final_.pdf?sfvrsn=5cbceba8_0> (13.10.2019).
- Steenis, H. V., Graseck, B. L., Simpson, F. ve Faucette, J. E. (2016). *Global Insight: Blockchain in Banking: Disruptive Threat or Tool?* Morgan Stanley. <<https://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf>> (18.09.2019).
- STM. (2020). *Savunma Sanayiinde Blokzincir*. Ankara: STM thinktech.
- Sueoka, M. (2019). *Blockchain doesn't matter. Here's why*. invision: <<https://www.invisionapp.com/inside-design/blockchain-ux/>> (04.07.2023).
- Sultan, K., Ruhi, U. ve Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications. *11th IADIS International Conference Information Systems* (49-57). Lisbon: IADIS Press. doi: 10.48550/arXiv.1806.03693
- Suominen, K., Chatzky, A., Reinsch, W. ve Robison, J. (2018). 10 Big Questions (and Myths) Surrounding Blockchain. *JSTOR*, 15-22. <<https://www.jstor.org/stable/resrep22491.6>> (06.08.2020).

- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.
- Swanson, T. (2016). *Blockchain Enigma. Paradox. Opportunity*. London: Deloitte.
- Şahin, A. ve Örselli, E. (2003). E-Devlet Anlayışı Sürecinde Türkiye. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 343-356.
- Şahin, A. ve Örselli, E. (2016). *Türk Kamu Yönetiminde Yapısal Dönüşüm ve E-Devlet*. Konya: Atlas Akademi.
- T.C. Cumhurbaşkanlığı Finans Ofisi. (2023). *2022 Türkiye Fintech Ekosistemi Durum Raporu*. İstanbul. <https://www.cbfo.gov.tr/sites/default/files/docs/2023-03/fintek-durum-raporu-2022_v0.9_digital_lowsize_ayrisayfalar-compressed.pdf> (25.07.2023).
- T.C. Sanayi ve Teknoloji Bakanlığı. (2019). *2023 Sanayi ve Teknoloji Stratejisi*. Ankara.
- TAKAS İstanbul. (2020). *BiGA Platformu*. TAKASBANK: <<https://www.takasbank.com.tr/tr/hizmetler/verilen-hizmetler-1/biga-platformu>> (02.10.2021).
- TAKASBANK. (2019). *Biga Projesi*. İstanbul: FinTechHub. <https://biga.takasbank.com.tr/biga_whitepaper.pdf> (06.10.2022).
- Takyar, A. (2019). *Initiatives Around Blockchain Technology In South Korea*. <<https://www.leewayhertz.com/blockchain-south-korea/>> (16.11.2022).
- Tanrıverdi, M., Uysal, M. ve Üstündağ, M. T. (2019). Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), 203-217. doi: 10.17671/gazibtd.547122
- Tapscott, D. ve Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Portfolio / Penguin.
- Tasca, P. ve Tessone, C. J. (2019). A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger*, 4, 1-39. doi: 10.5195/ledger.2019.140

- Taş, O. ve Kiani, F. (2018). Blok Zinciri Teknolojisine Yapılan Saldırıları Üzerine Bir İnceleme. *Bilişim Teknolojileri Dergisi*, 11(4), 369-382. doi: 10.17671/gazibtd.451695
- TBV. (2019). *Dünyada Blokzinciri Regülasyonları ve Uygulama Örnekleri*. İstanbul: Türkiye Bilişim Vakfı.
- TBV. (2020). *2019 Çalışma Raporu*. İstanbul: Türkiye Bilişim Vakfı. <<http://tbv.org.tr/wp-content/uploads/2020/10/Rapor2020.pdf>> (20.06.2022).
- TCMB. (2021). *Ödemeler Alanına İlişkin Basın Duyurusu (2021-17)*. <<https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB%20TR/Main%20Menu/Duyurular/Basin/2021/DUY2021-17>> (14.02.2022).
- Thakur, V., Dojab, M. N., Dwivedic, Y. K., Ahmad, T. ve Khadanga, G. (2020). Land Records on Blockchain for Implementation of Land Titling in India. *International Journal of Information Management*, 52, 101940. doi: 10.1016/j.ijinfomgt.2019.04.013
- The Institutes. (2017). *Blockchain Building Blocks: Creating a World of Opportunity for Insurance from an Evolving Area of Technology*. Malvern, PA: The American Institute For Chartered Property Casualty Underwriters.
- Tornatzky, L. G., Fleischer, M. ve Chakrabarti, A. K. (1990). *The Processes of Technological Innovation*. Lexington: Lexington Books.
- Tushman, M. ve Nadler, D. (1986). Organizing for Innovation. *California Management Review*, 28(3), 74-92. doi:10.2307/41165203
- Tüfekçi, A. ve Karahan, Ç. (2019). Blokzincir Teknolojisi ve Kamu Kurumlarının Verilen Hizmetlerde Blokzincirin Kullanım Durumu. *Verimlilik Dergisi*(4), 157-193.
- TÜSİAD. (2018). *Blokzincir Potansiyelinin Keşfi - 2018 Yılı Türkiye Blokzincir Araştırması*. Deloitte Türkiye.

- Tyma, B., Dhillon, R., Sivabalan, P. ve Wieder, B. (2022). Understanding Accountability in Blockchain Systems. *Accounting, Auditing & Accountability Journal*, 35(7), 1625-1655. doi: 10.1108/AAAJ-07-2020-4713
- Uçma Uysal, T. ve Kurt, G. (2018). Muhasebede ve Denetimde Blok Zinciri Teknolojisi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 23(2), 467-481.
- Ulbrich, E. K. (2023). *Mapping the evolution of Germany's blockchain ecosystem*. DataConomy: <<https://dataconomy.com/2023/08/01/mapping-the-evolution-of-germanys-blockchain-ecosystem/>> (02.09.2023).
- UN. (2023). *E-Government*. UN E-Government Knowledgebase: <<https://publicadministration.un.org/egovkb/en-us/Overview#whatis>> (17.07.2023).
- UNODC. (2020). *Money Laundering*. United Nations Office on Drugs and Crime: <<https://www.unodc.org/unodc/en/money-laundering/overview.html>> (13.08.2022).
- Usta, A. ve Doğantekin: (2018). *Blockchain 101*. Bankalar Arası Kart Merkezi.
- Vaidya, K. (2016). *Decoding the enigma of Bitcoin Mining - Part I : Mechanism*. <<https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2?>> (17.12.2019).
- Vaniukov: (2022). *Top 9 Use Cases of Blockchain in Healthcare & Benefits You Should Know*. Softermii: <<https://www.softermii.com/blog/blockchain-in-healthcare-practical-use-cases-benefits-you-should-know>> (14.12.2022).
- Villanueva, J. C. (2022). *What is a Digital Signature?* JScape by Redwood: <<https://www.jscape.com/blog/what-is-a-digital-signature>> (09.05.2023).
- Viriyasitavat, W. ve Hoonsopon, D. (2019). Blockchain Characteristics and Consensus in Modern Business Processes. *Journal of Industrial Information Integration*(13), 32-39. doi: 10.1016/j.jii.2018.07.004

- VISA. (2022). *VISA Fact Sheet*. VISA.CO.UK: <<https://www.visa.co.uk/content/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf>> (28.12.2022).
- Vogel-Heuser, B. ve Hess, D. (2016). Guest Editorial Industry 4.0–Prerequisites and Visions. *IEEE Transactions on Automation Science and Engineering*, 13(2), 411-413. doi: 10.1109/TASE.2016.2523639
- Walsch, A. (2017). The Path of the Blockchain Lexicon (And the Law). *Review of Banking & Financial Law*, 36: 713-765. <<https://ssrn.com/abstract=2940335>> (12.10.2019).
- Wan, S., Li, M., Liu, G. ve Wang, C. (2020). Recent Advances in Consensus Protocols for Blockchain: A Survey. *Wireless Networks*(26), 5579-5593. doi: 10.1007/s11276-019-02195-0
- Wang, H., Zheng, Z., Xie, S., Dai, H.-N. ve Chen, X. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14(4), 352-375.
- Wang, V., Zhao, X., Wang, E. ve Chen, L. (2023). *Blockchain 2023 - China: Trends and Developments*. Chambers and Partners: <<https://practiceguides.chambers.com/practice-guides/blockchain-2023/china/trends-and-developments/O13714>> (31.05.2023).
- Wegrzyn, K. E. ve Wang, E. (2021). *Types of Blockchain: Public, Private, or Something in Between*. FOLEY: <<https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between>> (13.05.2023).
- Weinstein, L. (2022). *Cryptocurrency & Blockchain Technology*. Library of Congress: <<https://guides.loc.gov/fintech/21st-century/cryptocurrency-blockchain>> (19.12.2022).
- Wenyu, D. D., Pan: L., Leidner, D. E. ve Ying, W. (2019). Affordances, Experimentation and Actualization of Fintech: A Blockchain Implementation Study. *Journal of Strategic Information Systems*(28), 50-65. doi: 10.1016/j.jsis.2018.10.002

- Werbach, K. (2018). Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, 33(2), 487-550. <<https://www.jstor.org/stable/26533144>> (23.09.2020).
- Werbach, K. (2019). *People Don't Trust Blockchain Systems*. Slate: <<https://slate.com/technology/2019/02/blockchain-government-regulation-cryptocurrency-bitcoin.html>> (04.07.2023).
- Woods, J. (2018). *Blockchain - Public Sector Use Cases*. LinkedIn: <https://www.linkedin.com/pulse/blockchain-public-sector-use-cases-jorden-woods/> (01.06.2019).
- World Economic Forum. (2020). *Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption*. Cenevre: IDB. <<https://www.weforum.org/reports/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption/>> (02.09.2023).
- World Economic Forum. (2020). *Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates*. Geneva: World Economic Forum. <<https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-case-studies-and-learnings-from-the-united-arab-emirates/>> (25.03.2021).
- World Food Programme. (2021). *Building Blocks*. Innovation Accelerator: <<https://innovation.wfp.org/project/building-blocks>> (20.07.2023).
- Wüst, K. ve Gervais, A. (2018). Do you Need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology* (45-54). IEEE. doi:10.1109/CVCBT.2018.00011
- Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J. ve Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, 21(3), 2794-2830. doi:10.1109/COMST.2019.2899617
- Yaga, D., Mell, P., Roby, N. ve Scarface, K. (2018). *NISTIR 8202: Blockchain Technology Overview*. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.IR.8202

- Yang, L. (2019). The Blockchain: State-of-the-art and Research Challenges. *Journal of Industrial Information Integration*, 15: 80-90. doi: 10.1016/j.jii.2019.04.002
- Yiğit, A. G. (2020). Sanal Yardımlaşma: Kitlese Fonlama. Y. Demirdöğen içinde, *Dijital Dönüşüm ve Finansal Teknolojilere Yansımaları* (109-127). Ankara: Nobel Yayınevi.
- Yıldız, M., Ocak, N., Yıldırım, Ç. ve Çağıltay, K. (2016). Usability in Local E-Government: Analysis of Turkish Metropolitan Municipality Facebook Pages. *International Journal of Public Administration in the Digital Age*, 3(1), 53-69.
- Yli-Huumo, J., Ko, D., Choi, S., Park, S. ve Smolander, K. (2016). Where Is Current Research on Blockchain Technology? - A Systematic Review. *PLoS ONE*, 11(10), 1-27. doi:10.1371/journal.pone.0163477
- Zhao, J. L., Fan, S. ve Yan, J. (2016). Overview of Business Innovations And Research Opportunities in Blockchain And Introduction to the Special Issue. *Financial Innovation*, 2, 1-7. doi:10.1186/s40854-016-0049-2
- Zheng, Z., Xie, S., Dai, H., Chen, X. ve Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE 6th International Congress on Big Data*, (557-564). doi: 10.1109/BigDataCongress.2017.85