

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

YÜKSEK LİSANS TEZİ

BLOK ZİNCİRİ TEKNOLOJİSİNİN MUHASEBE VE DENETİM
MESLEĞİNE ETKİSİ

Ceren DİNÇEL

25011700624

TEZ DANIŞMANI
Prof.Dr. Kerem SARIOĞLU
İSTANBUL – 2020

ÖZ

BLOK ZİNCİRİ TEKNOLOJİSİNİN MUHASEBE VE DENETİM MESLEĞİNE ETKİSİ CEREN DİNÇEL

Teknoloji ve dijitalleşme şirketlerin ve sektörlerin iş yapış şeklini değiştirmekte ve her geçen gün daha da önemini arttırmaktadır. Teknolojinin en son gelişmelerinden biri olan blok zinciri teknolojisi, günümüzde birçok sektör ve kurum tarafından araştırılmaya ve uygulanmaya başlanmıştır. 2008 yılında Satoshi Nakamoto isimli kişi ya da kişiler tarafından yapılan bir çalışma ve Bitcoin'in ortaya çıkışı ile adından söz ettiren bu teknoloji daha çok ödeme işlemleri ve finans sektöründe kendine yer bulmuştur. Zaman içerisinde bu teknoloji sadece kripto paralar ve ödeme işlemleri için değil tüm sektörler için kullanılabileceği görülmüş ve çok sayıda proje geliştirilmiştir.

Blok zinciri teknolojisinin kayıtları değiştirememe, şeffaflık, denetlenebilirlik, zaman damgası özellikleri sayesinde muhasebe ve denetim mesleğinin iş yapış şeklini değiştireceği düşünülmektedir. Küresel bir kayıt defteri olan blok zinciri, muhasebedeki çift taraflı kayıt düzenine göre tutulan kayıtların ve finansal raporlamanın daha şeffaf ve daha güvenilir bir şekilde hazırlanmasına yardımcı olacaktır. Günümüzde mutabakat, örneklem seçme gibi bağımsız denetim mesleğinde denetçiler tarafında gerçekleştirilen birçok iş blok zinciri teknoloji sayesinde daha verimli bir şekilde yapılabilecektir. Çok fazla teknik bilgi gerektiren bu teknoloji, denetçilerin bilgi teknolojileri konusunda bilgilerini arttırmasını gerektirmektedir.

Her yeni teknolojinin getirdiği faydalar olmakla birlikte, riskleri de mevcuttur. Blok zinciri teknolojisinin getireceği riskler ve bu risklerin muhasebe ve denetim mesleğinin hangi noktalarında etkileneceği

arařtırılmalıdır. Bu risklerin tespit edilmesi ve risklere karřı önlem alınması için özellikle iç denetim departmanlarına bu konuda büyük iş düşmektedir.

Bu çalışmada blok zinciri teknolojisinin finansal muhasebe, bağımsız denetim ve iç denetim üzerine etkileri açıklanmış, test aşamasındaki uygulamalar anlatılmış ve küresel faaliyetleri olan denetim firmaların çalışmalarına yer verilmiştir. Çalışmada ayrıca blok zinciri teknolojisinin tarihsel gelişimi, temel kavramları, farklı sektörlerdeki uygulama alanları anlatılmıştır.

Anahtar Kelimeler: Blok Zinciri Teknolojisi, Muhasebe, Bağımsız Denetim, İç Denetim, Finansal Muhasebe, Üç Taraflı Kayıt Düzeni, Dağıtık Defter Teknolojisi, Şifreleme, Elektronik Veri.

ABSTRACT

THE IMPACT OF BLOCKCHAIN TECHNOLOGY ON ACCOUNTING AND AUDITING PROFESSION

CEREN DİNÇEL

Today, technology and digitalization are changing the way of companies and sectors do business and increasing their importance every day. Blockchain technology, one of the latest developments in technology, has started to be researched and applied by many sectors and institutions. This technology, which made a name for itself with the emergence of Bitcoin and a study conducted by a person or persons named Satoshi Nakamoto in 2008, has found a place in the payment transactions and finance sector. Over time, it has been seen that this technology can be used not only for cryptocurrencies and payment transactions, but for all sectors and many projects have been developed.

It is thought that blockchain technology will change the way the accounting and auditing profession does business, especially due to the inability to change records, transparency, auditability, and time stamp features. As a global ledger, the blockchain will help prepare the records and financial reporting more transparent and more accurately according to the double-entry bookkeeping in accounting. Today many tasks carried out by the auditors in the independent audit profession such as reconciliation and sample selection can be done more efficiently thanks to blockchain technology. This technology, which requires a lot of technical knowledge, requires auditors to increase their knowledge on information technologies.

Although every new technology has benefits, there are also some risks. The risks to be brought by blockchain technology and at what points these risks will be affected by the accounting and auditing profession should be investigated. In order to identify these risks and to take precautions against these risks, especially internal audit departments have a big job in this regard.

In this study, the effects of blockchain technology on financial accounting, independent auditing and internal audit are explained, the applications in the test phase are explained, and the studies of audit companies with global activities are included. In the study, the historical development, basic concepts and application areas of blockchain technology in different sectors are explained.

Keywords: Blockchain Technology, Accounting, External Audit, Internal Audit, Financial Accounting, Triple Entry Accounting, Distributed Ledger Technology, Cryptography, Electronic Data.



ÖNSÖZ

Meslek hayatımın ilk gününden beri bana her zaman yol gösteren, desteğini esirgemeyen ve tüm tez yazma sürecimde önerileri, yönlendirmeleri ve bana öğrettiği her şey için tez danışman hocam sayın Prof.Dr. Kerem SARIOĞLU'na teşekkür ederim.

Beni yetiştiren ve bugünlere getiren, babam Ercüment DİNÇEL'e, annem Gülay DİNÇEL'e ve her zaman yanımda olan kız kardeşim Selin DİNÇEL'e destekleri, fedakârlıkları ve gösterdikleri sabır için sonsuz teşekkür ederim.

CEREN DİNÇEL

İSTANBUL, 2020

İÇİNDEKİLER

ÖZ.....	ii
ABSTRACT	iiiv
ÖNSÖZ.....	vi
TABLolar LİSTESİ.....	xi
ŞEKİLLER LİSTESİ.....	xii
RESİMLER LİSTESİ.....	xiv
KISALTMALAR LİSTESİ.....	Hata! Yer işareti tanımlanmamış.
GİRİŞ	1

BİRİNCİ BÖLÜM

ELEKTRONİK VERİ VE BİLGİ

1.1. Veri ve Elektronik Verinin Tanımı	2
1.2. Elektronik Verinin Saklanması	3
1.3. Elektronik Veri İletişimi ve Güvenlik Sorunları	10
1.3.1. Elektronik Veri İletişiminin Tarihsel Gelişimi	10
1.3.2. Elektronik Veri İletişiminde Güvenlik Sorunları	14
1.4. Elektronik Ortamda Veri İletişiminde Bilgi Güvenliğinin Unsurları.....	20

İKİNCİ BÖLÜM

BLOK ZİNCİRİ TEKNOLOJİSİ

2.1. Blok Zinciri Teknolojisinin Tarihsel Gelişimi	25
2.2. Blok Zinciri Teknolojisinin Tanımı ve Çalışma Prensipleri.....	28
2.3. Blok Zinciri Teknolojisinin Temel Kavramları.....	30
2.3.1. Eşten Eşe Ağ	30
2.3.2. Dağıtık Defter Teknolojisi	33

2.3.3.	Kriptoloji.....	37
2.3.3.1.	Şifreleme.....	37
2.3.3.1.1.	Simetrik Şifreleme.....	38
2.3.3.1.2.	Asimetrik Şifreleme.....	39
2.3.3.2.	Özetleme Fonksiyonu	40
2.3.3.3.	Dijital İmza	43
2.3.4.	Mutabakat Mekanizması ve Algoritmaları.....	46
2.3.4.1.	İş İspatı (Proof of Work –PoW).....	48
2.3.4.2.	İş Payı (Proof of Stake-PoS).....	49
2.3.5.	Blok ve Blok Yapısı	50
2.3.5.1.	Blok Boyutu.....	50
2.3.5.2.	Blok Başlığı	50
2.3.5.2.1.	Sürüm	51
2.3.5.2.2.	Önceki Blok Özet Değeri	51
2.3.5.2.3.	Merkle Kökü.....	52
2.3.5.2.4.	Zaman Damgası.....	54
2.3.5.2.5.	Zorluk Hedefi	54
2.3.5.2.6.	Nonce.....	55
2.3.5.3.	İşlem Sayacı.....	55
2.3.5.4.	İşlemler	55
2.3.6.	Madencilik.....	57
2.3.7.	Akıllı Sözleşmeler.....	58
2.4.	Blok Zincirinin Karakteristik Özellikleri	62
2.5.	Blok Zinciri Ağ Çeşitleri	64
2.5.1.	Açık (Public) Blok Zinciri	65
2.5.1.1.	Açık ve İzin Gerektirmeyen (Public Permissionless) Blok Zinciri.....	65
2.5.1.2.	Açık ve İzin Gerektiren (Public Permissioned) Blok Zinciri	66
2.5.2.	Özel (Private) Blok Zinciri.....	66
2.5.2.1.	Özel ve İzin Gerektirmeyen (Private Permissionless) Blok Zinciri.....	67
2.5.2.2.	Özel ve İzin Gerektiren (Private Permissioned) Blok Zinciri.....	67
2.5.1.	Konsorsiyum Blok Zinciri	68

2.6.	Blok Zinciri Platformları	69
2.6.1.	Bitcoin	70
2.6.2.	Ethereum	71
2.6.3.	Hyperledger	73
2.6.4.	Ripple	74
2.6.5.	Corda	77
2.7.	Blok Zinciri Teknolojisinin Karşılaştığı Zorluklar	78
2.8.	Blok Zinciri Teknolojisinin Günümüzdeki Durumu ve Geleceği	83
2.9.	Blok Zinciri Teknolojisinin Uygulama Alanları	91
2.9.1.	Lojistik ve Tedarik Zinciri	92
2.9.2.	Emlak ve Tapu Kayıtları	94
2.9.3.	Sağlık Hizmetleri	95
2.9.4.	Finans ve Bankacılık	96

ÜÇÜNCÜ BÖLÜM

MUHASEBE VE DENETİMDE VERİ GÜVENLİĞİ VE BLOK ZİNCİRİ TEKNOLOJİSİNİN BU ALANDA KULLANIMI

3.1.	Finansal Raporlama ve Blok Zinciri Teknolojisi	101
3.1.1.	Muhasebede Kayıt Düzeni	101
3.1.1.1.	Tek Taraflı Kayıt Düzeni	102
3.1.1.2.	Çift Taraflı Kayıt Düzeni	103
3.1.1.3.	Üç Taraflı Kayıt Düzeni	103
3.1.1.3.1.	Dai ve Vasarhelyi (2017)- Üç Taraflı Kayıt Düzeninde Muhasebe Bilgi Sistemi	108
3.1.1.3.2.	Ledgerium Uygulaması	112
3.1.1.3.3.	zkLedger Uygulaması	114
3.1.2.	Gerçek Zamanlı Muhasebe	118
3.1.2.1.	Muhasebeciler ve Aracı Kurumlar	120
3.1.2.2.	Kâr Yönetimi	121
3.1.2.3.	İlişkili Taraf İşlemleri	122
3.2.	İç Denetim ve Blok Zinciri Teknolojisi	123
3.2.1.	Standart Risk Faktörleri	126

3.2.2. Değer Transferi Risk Faktörleri.....	134
3.2.3.Akıllı Sözleşme Risk Faktörleri.....	136
3.3.Bağımsız Denetim ve Blok Zinciri Teknolojisi	139
3.3.1.Blok Zinciri Teknolojisinin Denetim Kanıtları Üzerine Etkisi	146
3.3.2.Blok Zinciri Teknolojisinin Yönetimin İddiaları Üzerindeki Etkisi.....	154
3.3.3.Akıllı Sözleşmeler ile Denetim.....	156
3.3.4.Küresel Faaliyeti olan Denetim Firmaları ve Uygulamaları.....	159
3.3.4.1.Deloitte.....	159
3.3.4.2.KPMG	161
3.3.4.3.Ernts & Young	162
3.3.4.4.PWC	164
3.3.4.5.Diğer.....	166
SONUÇ.....	168
KAYNAKÇA	170

TABLÖLAR LİSTESİ

Tablo 2.3.3.2.1. Özetleme Fonksiyonları ve Üretilen Toplam Özetleme Sayısı.....	41
Tablo 2.3.5.1. Blok Yapısı.....	50
Tablo 2.3.5.2.1. Blok Başlığı.....	51
Tablo 2.3.5.2.3.1. Merkle Ağacı Verimliliği.....	54
Tablo 2.8.1. Kripto Paralar ve Blok Zinciri Teknolojisine Olan Yaklaşım....	88
Tablo 3.3.1. ABD’de Dört Büyük Denetim Firmalarının 2019 Yılında Elde Ettikleri Gelirlerin Faaliyet Kolu Bazında Dağılımlar.....	140
Tablo 3.3.2. Blok Zinciri Teknolojisinin Denetim Mesleğine Olası Etkileri...	144
Tablo 3.3.1.1. Geleneksel Prosedürler İle Blok Zinciri Destekli Prosedürlerin Karşılaştırılması.....	149,150

ŞEKİLLER LİSTESİ

Şekil 1.3.1.1. Sezar Şifresi.....	11
Şekil 1.3.1.2. Sezar Şifrelemesi, Şifrelenmiş Mesaj Örneği.....	12
Şekil 1.3.1.3. Mors Alfabeti.....	13
Şekil 1.3.2.1. Elektronik Sinyallerin Şifrelemeyi Atlaması (Bypass).....	16
Şekil 2.2.1. Bir Blok Zinciri Nasıl Çalışır?.....	29
Şekil 2.3.1.1. İstemci/Sunucu Ağ ve Eşler Arası Ağ.....	32
Şekil 2.3.2.1. Merkezi, Merkezi Olmayan ve Dağıtık Ağ Yapısı.....	33
Şekil 2.3.2.2. Mevcut Dağıtık Defter Teknolojisi Uygulamalarına Genel Bakış.....	35
Şekil 2.3.2.3. Blok Zinciri ve Arapsaçı Karşılaştırılması.....	36
Şekil 2.3.2.4. Arapsaçı Yapısında İşlemlerin Onaylanması.....	36
Şekil 2.3.3.1.1. Şifreleme ve Şifre Çözme İşlemleri.....	38
Şekil 2.3.3.1.1.1. Simetrik Şifreleme.....	39
Şekil 2.3.3.1.2.1. Asimetrik Şifreleme.....	40
Şekil 2.3.3.2.1. Verinin SHA-256 Karşılığı Örneği.....	42
Şekil 2.3.3.2.2. SHA-256 Özet Fonksiyonu Örneği.....	43
Şekil 2.3.3.3.1. Dijital İmza Algoritması.....	45
Şekil:2.3.5.2.2.1. Blok Zinciri Yapısı.....	52
Şekil 2.3.5.2.3.1. Merkle Ağacı.....	54
Şekil 2.3.5.4.1. 2016 Yılı Haziran Ayı Başı Bitcoin Blok Zincirinin 40 Dakikasının Görselleştirilmesi (415.346-415.350 Numaralı Bloklar).....	56
Şekil 2.3.7.1. Örnek Bir Ethereum Akıllı Sözleşmesi.....	61
Şekil 2.5.1. Blok Zinciri Ağ Türlerinde Faaliyet Gösteren Uygulamalar.....	68
Şekil 2.5.2. Şirketiniz Hangi Blok Zinciri Modeline Odaklanmaktadır?.....	69
Şekil 2.6.1.1. Dolaşımdaki Bitcoin Sayısı, Mayıs 2020.....	71
Şekil 2.6.4.1. Ödeme Sistemlerinin Maliyetlerinin Karşılaştırılması.....	76
Şekil 2.7.1. Bitcoin Madenci Havuzları Dağılımı.....	81
Şekil 2.8.1. Teknolojilerin Adaptasyon Süreci.....	84
Şekil 2.8.2. Blok Zinciri Gelişim Süreci-Mevcut Durum.....	86

Şekil:2.8.3. Gelişmekte Olan Teknolojilerin Gelişim Grafiği, 2018.....	87
Şekil 2.8.4. Blok Zinciri Teknolojileri Beklenti Döngüsü Grafiği, 2019.....	90
Şekil 2.9.1. Blok Zinciri Teknolojisinden En Fazla Etkileneceği Düşünülen Alanların Dağılımı.....	92
Şekil 3.1. Blok Zinciri Tabanlı Muhasebe Ekosistemi.....	101
Şekil 3.1.1.1.1. Kontra Giriş için Bir Hesap Göstergesi Olmayan Tek Taraflı Defter.....	102
Şekil 3.1.1.3.1. Üç Taraflı Muhasebe Sistemi Örneği.....	106
Şekil 3.1.1.3.1.1. Üç Taraflı Kayıt Düzeninde Muhasebe Bilgi Sistemi	110
Şekil 3.1.1.3.2.1. Luca+.....	113
Şekil 3.1.1.3.2.2. Luca+ Ledgerium Örnek Uygulama.....	114
Şekil 3.1.1.3.3.1. Açık Defter (Public Ledger) Uygulama Örneği.....	116
Şekil 3.1.1.3.3.2. zkLedger Uygulama Örneği.....	117
Şekil 3.2.1. Etkin Bir Blok Zinciri Risk Yönetimi Çerçevesinin Bileşenleri...	126
Şekil 3.3.1. Blok Zinciri Teknolojisinin Güvenilir Bir Taraf Olmadan Eksiksiz ve Kesin Doğrulama Sağlaması.....	141
Şekil 3.3.1.1. Blok Zinciri Kullanarak Kayıtların Bütünlüğünü Doğrulamak İçin Bir Yaklaşım.....	153
Şekil 3.3.3.1. Satışlardaki Önemli Yanlışlık Riskinin Tespitinde Akıllı Denetim Prosedürlerinin Kullanılması.....	157
Şekil 3.4.1.1. Deloitte Tarafından Kurulan Bitcoin ATM'si.....	160

RESİMLER LİSTESİ

Resim 1.2.1. Jacquard Dokuma Makinesi.....	5
Resim 1.2.2. IBM Tarafında Geliştirilen Bir Delikli Kart.....	6
Resim 1.2.3. Manyetik Bantlar ve Çeşitleri.....	7
Resim 1.3.1.1. Teleks Makinesi.....	14
Resim 1.3.2.1. Bir Enigma Makinesi.....	15
Resim 1.3.2.2. Belgelerin Posta ve Faks İle İletimi.....	17



KISALTMALAR

ABD	: Amerika Birleşik Devletleri
AI	: Artificial Intelligence
AICPA	: American Institute of Certified Public Accountants
AML	: Anti Money Laundering
ASIC	: Application Specific Integrated Cicurit
ATM	: Automated Teller Machine
BaaS	: Blockchain as-a-Service
BIAB	: Blockchain in a Box
BIS	: Bank for International Settlements
BT	: Bilgi Teknolojileri
BTC	: Bitcoin
CAAT	: Crypto-Asset Accounting and Tax
CCO	: Chief Commercial Officer
CD	: Compact Disc
DAG	: Directed Arcylic Graph
DDT	: Dağıtık Defter Teknolojisi
DLT	: Distributed Ledger Technology
DoS	: Denial of Servis Attack
DVD	: Digital Versatile Disc
EDI	: Electronic Data Interchange
EFT	: Electronic Fund Transfer
ETH	: Ether
EVD	: Elektronik Veri Değişimi
EVM	: Ethereum Virtual Machine
EY	: Ernst & Young
FATF	: Financial Action Task Force
FDA	: Food and Drug Administration
FinCEN	: Financial Crimes Enforcement Network
FSB	: Financial Stability Board

GB	: Gigabayt
GBP	: Sterlin
GDPR	: General Data Protection Regulation
HIPAA	: Health Insurance Portability and Accountability Act
HP	: Hewlett Packard
IBM	: International Business Machines
ICO	: Inital Coin Offerring
IDC	: International Data Corporation
ILP	: Interledger Protokolü
IMF	: International Monetary Fund
IOSCO	: International Organization of Securities Commissions
IRS	: Internal Revenue Service
ISO	: International Organization for Standardization
KGK	: Kamu Gözetim Kurumu
LAN	: Local Area Network
MB	: Megabayt
MD	: Message Digest
MIT	: Massachusetts Institute of Technology
P2P	: Peer to Peer
PII	Personally Identifiable Information
PoS	: Proof of Stake
PoW	: Proof of Work
RAMAC	: Random Access Method of Accounting and Control
RFID	: Radio Frequency Idendification
RSGT	: Real-Time Gross Settlement
SAN	: Storage Area Network
SHA	: Secure Hash Algorithm
SLA	: Service Level Agreement
SWFT	: Society for Worldwide Interbank Financial Telecommunications
TB	: Terabayt
TB	: Ticari Borçlar

TDK	: Türk Dil Kurumu
TMS	: Ticari Mal Stoku
TÜSİAD	: Türk Sanayicileri ve İş İnsanları Derneği
UNIVAC	: Universal Automatic Computer
US	: United States
USB	: Universal Serial Bus
USD	: United States Dollar
VANs	: Value Added Networks
WAN	: Wide Area Network
WFE	: World Federation of Exchanges
WSBA	: Wall Street Blockchain Alliance
XR	: Extended Reality
XRP	: Ripple
YDA	: Yönlü Düz Ağaçlar

GİRİŞ

Yazının icadından günümüze kadar geçen sürede verinin/bilginin saklanması ve iletilmesi her zaman çok önemli olmuştur. Yazının icadı ile ilk olarak kil tabletlerde saklanan bilgiler, toplumların gelişmesi ve kaydedilen verinin/bilginin çoğaltılması ile verilerin saklandığı yerler değişim göstermiştir. Zamanla insanlara bu verilerin saklanması yeterli gelmemiş ve veri iletimi başlamıştır. Verinin/bilginin iletimi sırasında güvenlik sorunları ile karşılaşmış, bilgiler istenmeyen kişilerin eline geçmiş veya değiştirilmiştir. Bu durum bilgi güvenliği konusu gündeme getirmiştir. Üretilen bilgiler çoğaldıkça verilerin saklanma ortamları değişim göstermiş ve çeşitlenmiştir. Geçmişten günümüze kadar geçen bu sürede veri formunun, verinin saklanmasının, insanlar ve kurumlar arası iletişimin ve teknolojinin gelişmesi ve değişmesi sonucunda bilgi güvenliği konusu daha da önemli bir hale gelmiştir. Bilginin tek bir yerde saklanması yerine birden fazla yerde saklanması ile bulut kavramı hayatımıza girmiştir.

Günümüzde izlenebilirlik, paylaşılan bilgilere anında erişim, şeffaflık ve güvenilirlik için yeni teknolojilere ihtiyaç duyulmaktadır. Blok zinciri teknolojisinin ise bu ihtiyaçları giderecek bir teknoloji olduğu kabul edilmektedir. Verilerin değiştirilememesi ve silinememesi, şeffaflık, takip edilebilirlik, zaman damgası gibi özellikler muhasebede finansal raporlamayı, bağımsız denetimi ve iç denetimi etkileyeceği alanların başında gelmektedir. Gerçek zamanlı izlenebilme ve muhasebe sunan blok zinciri teknolojisi ile daha güvenilir finansal raporlama ve denetim izleri hazırlanmaktadır.

Bu çalışmada ilk olarak elektronik verinin tanımı yapılmış ve verinin zaman içerisindeki değişimi ve verinin saklanmasında ve iletimindeki güvenlik sorunlarına yer verilmiştir. İkinci bölümde ise blok zinciri teknolojisi detayları ile anlatılmıştır. Üçüncü bölümde ise blok zinciri teknolojisinin muhasebe ve denetim mesleğindeki etkileri ele alınmıştır.

BİRİNCİ BÖLÜM

ELEKTRONİK VERİ VE BİLGİ

1.1. Veri ve Elektronik Verinin Tanımı

İngilizce’ de “data” anlamına gelen “veri” kelimesinin kökeni Latince’ den gelmektedir. Latince’ de anlamı “vermek” olan “dare” sözcüğü Türkçe’de ise “verilen şey” anlamında, veri olarak kullanılmaktadır. Veri kavramı araştırma, deney, gözlem, internet, sosyal medya, sensörlerden vb. çok farklı ortamlardan elde edilen genel bir terimi ifade etmektedir (Doğan ve Arslantekin, 2016:16).

Veri ve bilgi çoğu zaman birbirinin yerine kullanılmakla birlikte, birbirinden farklı kavramlardır. Veri işlenmemiş ham bilgidir ve tek başına bir anlam taşımamaktadır. Verilerin anlamlı bir hale dönüşmesi için işlenmesi gerekmektedir. Verilerin işlenerek belirli bir amaç için anlamlı hale getirilmesi sonucunda ise bilgi elde edilir. Örneğin, kişilerin isimleri, yıllar, parasal tutarlar, tarihler tek tek bakıldığında bir anlam taşımazken, bunlar ancak bir araya getirilip işlendiğinde bir anlam ifade eder hale gelir. Bu örnekteki bilgiler işlendiğinde belirli bir kişinin vadeli borcuna ait bir tablo ortaya çıkması gibi. Bilgi, kim, nerede, ne zaman, ne kadar gibi tanımlayıcı sorulara cevap verir. İşlenmiş verilerin sonucunda elde edilen bilgiler başka bir çalışma için veri olarak kullanılabilir.

İlk veriler milattan önce, eski medeniyetlerin tarım faaliyetleri sonucu elde ettiği mahsullerin kayıt altına alınması amacı ile tutulduğu görülmüştür. Veri, günümüzde ise genel anlamda hesaplama, gözlem, deney ve kayıtlardan ortaya çıkarılan kanıtlar, gerçekler veya olguları temsil eden formlar olarak nitelendirilmektedir. Zaman içerisinde bilimin ve teknolojinin gelişmesi, verinin anlamının ilk kullanıldığı zamandan günümüze kadar gelen sürede değişmesine sebep olmuştur. Gelişen teknoloji ile birlikte günümüzde sıklıkta duyduğumuz elektronik veri kavramı hayatımıza girmiştir. Elektronik ortamda sayısal olarak kodlanmış verilere elektronik veriler denmektedir. Verilerin/bilgilerin belirli bir formata dönüştürülmüş hâlini ifade etmektedir. Elektronik veri, 5070 sayılı Elektronik İmza Kanunu’nun (EİK) 3/a maddesinde “*elektronik, optik ve benzeri yollarla üretilen, taşınan veya saklanan*

kayıtlar” olarak tanımlanmıştır. Elektronik veri, bilişim sistemlerinin temelini oluşturmaktadır. Canberk ve Sağıroğlu’na göre (2006), bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanmaktadır.

Elektronik ortam denilince akla ilk olarak internet ortamı gelmektedir. Ancak internet ortamı elektronik ortamlarından sadece bir tanesidir. Elektronik ortam sayısallaştırılmış verilerin, kaydedilip saklandığı ortamlara verilen genel bir isimdir (Oğuz, 2013). Bilgisayarlar, flash diskler, akıllı cihazlar, telefonlar elektronik ortamlara örnek olarak gösterilebilir.

1.2. Elektronik Verinin Saklanması

İnsanoğlu var olduğundan beri bilerek ya da bilmeyerek anlamlı ya da anlamsız birçok veri üretmektedir. Bilgisayarların olmadığı çağlarda üretilen bu veriler/bilgiler ilk olarak hayvanların kemiklerine ve taşlara kazılarak kaydedilmiştir. Verilerin üzerine kaydedilip saklandığı ortamlara “veri kayıt ortamı” denir (Vikipedi, 2020a). Yazının keşfi ile kâğıt ve defterlere kaydedilmeye başlayan verilerin, teknolojinin gelişmesi ile birlikte kaydedildiği ortamlar değişmeye ve gelişmeye başlamıştır. Haberleşme ve bilgisayar teknolojisinin gelişmesi ve yaygınlaşması ile birlikte üretilen verilerde ciddi bir artış görülmüştür. Sırası ile delikli kartlar (punch card), manyetik bantlar, disketler (floppy discs), kompakt diskler (compact disc-CD), çok amaçlı sayısal disk (Digital Versatile Disc-DVD), taşınabilir diskler ve USB (Universal Serial Bus) flash sürücüler makineler ya da bilgisayarlar tarafından üretilen verileri kaydetme ortamı ve depolama aracı olarak kullanılmıştır.

Yazı, şehirlerin oluşması ve ortaya çıkması ve tarımın ve ticaretin gelişmesinden kaynaklı bir ihtiyaçtan doğmuştur. Ticaret faaliyetlerinin artması ve karmaşıklaşması, ticarete ve tarıma konu olan malların kayıt altına alınmasını gerekli kılmıştır. Çivi yazısı da denen bu ilk yazıda günümüzde kullanılan alfabetik düzendeki harfler değil, olayları temsil eden semboller ve resimler kullanılmıştır. İlk olarak milattan önce Sümerler tarafından ticaret ve tarımdaki ilgili olaylar veya mallar kil tabletler üzerine kaydedilmiştir. Milattan önce kullanılan diğer yazı örneği olan ve eski Mısırlıların

kullandığı hiyeroglif yazısında da nesneler ve olaylar sembollerle tapınak, mezar ve saray gibi yapıların duvarlarına yazılıp kaydedilmiştir. Ayrıca papirüs bitkisinden yapılan papirüs kâğıtlarının üzerine bu sembollerden oluşan yazı ile bilgiler kaydedilmiştir. Hayvan kemikleri, hayvan derilerinden elde edilen parşömenler, ahşap çubuklar ise eski ve orta çağlarda yazının kaydedildiği diğer ortamlardı (Gümüshan, 2018).

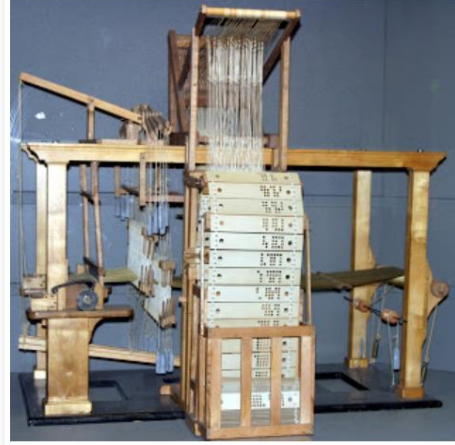
Yapılan arkeolojik çalışmaların sonucunda günümüzde kullandığımız kâğıdın yapımı milattan önce ikinci yüzyılda Çin ve bölgesinde kullanıldığını göstermiştir (Goda ve Kitsuregawa, 2012). Kâğıdın icadından önce, bilgileri kaydetmek için kullanılan hayvan derileri, kil tabletler, taşlar ve hayvan kemikleri üzerine yazı yazmak oldukça zordu. Kâğıdın icadı okuma ve yazmayı ve bilgi yoğunluğunu önemli ölçüde kolaylaştırmıştır. Yine Çin’de ilk matbaanın bulunması ve 1450 yılında Johannes Gutenberg’in günümüz matbaasını geliştirmesi ile kaydedilen bilgilerin çoğaltılabilmesi ve bunu takiben bilginin yayılması hızlanmıştır (Wikitarıh, erişim tarihi: 30 Nisan 2020).

Verilerin insan kontrolünde makine diline dönüşmesi ise delikli kartlarla verilerin depolanması ile başlamıştır (Usta ve Doğantekin, 2018). Verilerin ilk depolama formu olarak bilinen delikli kartların geçmişi 1725’e dayanmaktadır (Triksa, 2010). Tekstil işi ile uğraşan Fransız Baise Bouchon el dokuma tezgâhlarındaki desenli dokumalarda yapılan hataları giderecek bir sistem geliştirmiştir. Bu sisteme göre dokumaların desenlerini kâğıt şeritlere aktararak boyalı noktalarda delikler açmıştır. Bu makine yanlış dokumaların önüne geçebilmiş olsa da tam otomatik değildi ve delikli kâğıdın bir insan tarafından yavaş yavaş makinenin içine doğru yönlendirilmesi gerekiyordu.

1805’te delikli kartları, insana ihtiyaç duymadan tam otomatik halde işlenmesini sağlayan Joseph Marie Jacquard ise verinin saklama ve depolamasını günümüzdeki anlamını kazandıran kişidir. Resim 1.2.1.’de görüldüğü gibi, dokuma desenleri bir dizi karton kart üzerindeki delikler ile oluşturulmuş ve kartlar bir teyp ile birbirine bağlanmıştır.

Kolaylıkla çoğaltılabilen delikli kartlar başka dokumacılara satılmış veya farklı dokuma makinelerinde aynı anda çalışıp, desenli kumaş üretimini arttırmıştır. Günümüzde Jakar tezgâhları ve Jakarlı kumaş isimlerini buradan almaktadır.

Resim 1.2.1. Jacquard Dokuma Makinesi



Kaynak: ECLECTICA, ERİŞİM TARİHİ: 19 NİSAN 2020. Jacquard's Loom and the stored programme concept, (Çevrimiçi) <http://addiator.blogspot.com/2011/10/jacquards-loom-and-stored-programme.html>, 19 Nisan 2020.

8 Haziran 1887 yılında, delikli kartların patentini alan Herman Hollerith, delikli kartları ABD’de nüfus sayımı bilgilerini depolamak ve işlemek için kullanmıştır. Hollerith, Jacquard’ın desenlerin dokumasını yapabilmek için bilgileri delikli kartlara kaydettiği gibi sayım sonuçlarını otomatik olarak toplayan ve bilgileri delikli kartlara kaydeden bir makine yapımını düşünmüştür.

Amerika Birleşik Devletleri’nde (ABD) 1800’lü yıllarda sanayileşme ve göç ile birlikte nüfus artmış ve artan nüfus ile nüfus sayımında yaş, etnik grup, meslek gibi farklı türlerde bilgilerin de toplanması istenmiştir. Nüfus sayımındaki toplanan verileri el ile kaydetmek ve değerlendirmek oldukça zorlaşmış ve zaman almaya başlamıştır. Her on yılda bir yapılan ABD nüfus sayımında, 1880 yılına ait nüfus sayımı bilgilerini derlemek yedi yılı almış ve böyle giderse 1890 yılına ait nüfus sayımı sonuçlarının değerlendirilmesi tamamlanmadan 1900 yılının nüfus sayımı gerçekleşmesi beklenmekteydi (Essinger, 2004:157).

Nüfus sayım dairesinde görevli bir kişi olan Hollerith, nüfus sayım verilerinin daha verimli tablolamasını ve daha hızlı işlenmesini mümkün kılan bir tablolama

makinesi (tabulating machine) icat etmiştir. Bu makine verilerin sayısal olarak kodlanabileceği fikrine dayanmaktadır. Böylelikle veri işleme kavramı da ilk kez kullanılmıştır. Bu makine ile 1890 yılı ABD nüfus sayımı yapılmıştır.

Delikli kartların kullanılabilmesi için birden fazla makinenin çalışması gerekmektedir. Bunlar tablolaştırma makinesi (tabulator dials), kart okuyucular (card reader), kart deliciler (pantograph) ve kartları sıralama makinesidir (sorter table) (US Census Bureau, erişim tarihi: 30 Nisan 2020). New Yorklu bir mühendis olan Hollerith'in kendi makinelerini satmak için kurmuş olduğu Tabulation Machine Company ilerleyen yıllarda iki şirket ile birleşerek, Computing-Tabulating-Recording Company isimli yeni bir şirket kurulmuştur. Bu birleşme ilerleyen yıllarda isim değiştirilerek 1924 yılında International Business Machines (IBM)'i kurmuştur.

Resim 1.2.2.'te yer alan IBM tarafından üretilen 80 sütunlu bir delikli karttır. 1950'liler ortasına kadar delikli kartların kullanımı oldukça yaygındı.

Resim 1.2.2. IBM Tarafında Geliştirilen Bir Delikli Kart



Kaynak: IBM, ERIŞİM TARİHİ: 19 NİSAN 2020, The IBM Punch Card, (Çevrimiçi)
<https://www.ibm.com/ibm/history/ibm100/us/en/icons/punchcard/transform/>, 19 Nisan 2020

Veri saklanması getirdiği büyük değişimin yanında delikli kartlar yavaş, düşük kapasiteliydi ve kartların kullanılabilmesi için birçok makinenin çalışması gerekiyordu. Bu yüzden delikli kartlara veri depolama oldukça zaman ve iş gücü gerektirmekteydi. Ayrıca delikli kartların kullanımının artması ile onları saklayacak yer bulmak da çok zorlaşmıştı. Bu yüzden delikli kartların yerini alacak daha kapasiteli ve daha verimli çalışan manyetik bantlar (magnetic tape) geliştirilmiştir. Manyetik bantlarda veri kaydedilmesi ilk kez 1951 yılında ilk ticari bilgisayar olan UNIVAC I (Universal Automatic Computer) bilgisayarında kullanılmıştır. Delikli kartlarda

fiziksel olarak görülebilen veriler, manyetik ortama aktarıldıktan sonra veri depolama aracı üzerinde görülememekteydi. Böylece, manyetik bantlarla depolama dijital depolama fikrini ilk kez uygulamaya geçirmiştir. Verilerin daha büyük alanlarda depolanmasına imkân sağlayan manyetik bantlar, 10.000 delikli kartın toplamı kadar veri depolayabilmektedir (Triksa, 2010). Ancak manyetik bantlar çok hassastı ve kolayca bozuluyordu. Resim 1.2.3.'te manyetik bantların çeşitli kullanım araçları gösterilmiştir. Kasetler de manyetik veri kayıt ortamının bir unsurudur. Ses kaydı yapmak için kullanılan kasetler ilk olarak Philips tarafından tanıtılmıştır.

Resim 1.2.3. Manyetik Bantlar ve Çeşitleri



Kaynak: IASA, ERIŞİM TARİHİ: 29 NİSAN 2020. Magnetic Tape Alert Project (Çevrimiçi)
<http://www.mtap.iasa-web.org/>, 29 Nisan 2020.

Delikli kartlarda ve manyetik bantlarda istenilen bilgiye hemen erişilememekte ve bilgiye erişmek zaman almaktadır. Manyetik bantın içindeki bir bilgiye ihtiyaç duyulduğunda bantı geri sarmak ya da en baştan başlatmak gerekmektedir yani bantlarda depolanan verilere rast gele değil sıralı erişim vardır. 1956 yılında IBM tarafından üretilen ve rastgele seçim (random access) yapan ilk bilgisayar 305 RAMAC'ın (Random Access Method of Accounting and Control) bir parçası olan IBM 350 disk depolama birimi, ilk sabit disklerdir. Sabit diskler bilgilerin bilgisayarın içinde depolanmasını sağlamaktadır. Sabit disk teknolojisi ile veriye anında erişebilme kavramı hayatımıza girmiştir. Sabit diskler ile bilgiler meydana geldikleri anda kaydedilebilmiş ve veri depolama alanı da artmıştır. İlk sabit disk olan RAMAC 305'in kapasitesi yaklaşık olarak 5 megabayt (MB)'tır. Günümüzde ise sabit disklerin veri depolama alanı terabaytlara (TB) ulaşmıştır.

1960'lı yılların sonunda IBM tarafından ilk disket teknolojisi geliştirilmiştir. Yine IBM tarafından 1971 yılında ilk kez 8 inç büyüklüğündeki disket (floppy disket) üretilmiştir (IBM, erişim tarihi: 21 Nisan 2020). Daha sonrasında farklı büyüklük ve özellikte disketler geliştirilmiştir. İlk geliştirilen disketlerde kaydedilen verilerin sadece okunabilme özelliği varken daha sonra geliştirilen modellerinde ise kaydedilen verilerde değişiklik yapılabilme imkânı da sunulmuştur. Ayrıca ilk geliştirilen disketler çok fazla yer kapladığı için bir sonra gelen model küçültülerek geliştirilmiş ve aynı zamanda veri depolama kapasitesi de artmıştır.

Disketler verilerin bir bilgisayardan diğerine taşınabilmesini sağlamıştır. Bu durum insanların tek bir bilgisayara bağımlı olmadan çalışabilmesini mümkün kılmış ve insanların çalışma ve iş yapma şekillerini değiştirmiştir. Ancak disketler çok çabuk bozulabilmekte ve hasar görebilmektedir. Şifreleme özelliği olmadığı için içindeki bilgilerin de herkes tarafından okunabilme, erişilebilme ve ele geçirilme olasılığı vardır.

Bir başka veri depolama aracı 1980'lerin başlarında tanıtılmıştır. Disketlere göre çok daha fazla veri depolama alanı olan CD'ler, oyun, ses, video veya diğer formda olan verileri dijital olarak kaydedebilen, saklayabilen ve oynatabilen taşınabilir veri saklama ortamlarından bir diğeridir. Ancak CD'lerdeki veriler de disketlerde olduğu gibi zaman içinde bozulabilmektedir.

DVD'ler 1990'lı yılların ortalarında çıkan özellikle sinema sektöründe filmleri kaydetmede sıklıkla kullanılan bir veri kayıt ortamı olmuştur. CD'lere göre oldukça fazla kapasiteleri vardır. 2000'li yılların ortalarında sıklıkla kullanılan DVD'lerin 4 gigabayt (GB)'tan fazla veri depolama kapasitesi bulunmaktadır.

1990'lı yıllarda hayatımıza giren ve yedekleme birimlerinin en popülerlerinden olan USB flash bellekler halen günümüzde en yaygın olarak kullanılan depolama birimidir. USB flash bellekler boyut olarak küçük, rahatça taşınabilen ve oldukça büyük veri depolama kapasitesi olan veri kayıt ortamıdır. Ancak boyutları küçük olduğu için kaybolma ve çalınmaya oldukça müsaittir. Günümüzde bu taşınabilir veri depolama cihazında sunumları, fotoğrafları, dosyaları kaydetmekteyiz.

Taşınabilir hard diskler bilgisayarlarda yer alan harici disklere benzemekte olup, en önemli farklı USB flash bellekler gibi taşınabilir özellikte olmasıdır. Taşınabilir hard disklerin (portable hard drive) kapasitesi ise günümüzde 1 TB'yi geçmiş durumdadır.

İnternet teknolojisinin hayatımıza girmesi ile birlikte kişilerin ve kurumların ürettikleri ve saklamak istedikleri veri miktarı artmış, günümüze büyük veri (big data) kavramını getirmiştir. Çok kısa bir sürede çok fazla ve çok çeşitli verilerin üretilmesi ve bunların işlenmesi ihtiyacı fiziksel depolama yöntemlerini yetersiz bırakmıştır. Özellikle taşınabilir veri depolama cihazlarındaki en önemli risk fiziksel olarak zarar görebilmeleri ve yok edilmeleri ve kaydedilen verilerin de beraberinde yok olmasıdır. Bütün bunlar yeni bir veri depolama ortamına olan ihtiyacı ortaya çıkarmış ve bulut (cloud) kavramı hayatımıza girmiştir.

Bilgisayarın sabit sürücüleri yalnızca sınırlı miktarda veri depolayabilir. Kullanıcıların depolama alanı bittiğinde, dosyaları harici bir depolama cihazına aktarmaları gerekir. Geleneksel olarak, kuruluşlar veri ve dosyaları arşivlemek için depolama alan ağları (Storage Area Network-SAN) oluşturmuş ve bunları sürdürmüştür. Depolanan veriler büyüdükçe şirketler, artan talebi karşılamak için sunucu ve altyapı eklemeye yatırım yapmak zorundadır, bu yüzden de depolama alan ağlarının bakımı pahalıdır (IBM Cloud Education, 2019). Bulut depolama, dosyaları şirket içi sabit disklerde veya depolama ağlarında depolamaya uygun maliyetli, ölçeklenebilir bir alternatif sunar. Bulut depolama, verileri ve dosyaları internet veya özel bir özel ağ bağlantısı üzerinden eriştiğiniz kuruluşunuzun dışında bir konuma kaydetmenize olanak tanır. Verilere, bulunulan mekândan bağımsız olarak, istenilen her yerden ulaşabilme bulut sistemlerini kullanarak depolamayı esnek yapmaktadır. Fiziki değil sanal bir ortamda veri depolaması gerçekleştiği için verilerin kaybolması ya da bozulması riski oldukça düşüktür. Bulut depolama ile veriler ya da kaynaklar birden fazla kişi ile aynı anda paylaşılabilir. Google Drive, Box, Drop box, iCloud ve Amazon Cloud Drive ve Yandex.Disk günümüzde en bilinen ve yaygın olarak kullanılan bulut depolama hizmetlerinin başında gelmektedir.

Son olarak, tüm bu teknolojik ilerlemelerin sonucunda verilerin sanal ortamda daha güvenilir bir şekilde saklanması için blok zinciri teknoloji kullanılmaya başlanmıştır.

1.3. Elektronik Veri İletişimi ve Güvenlik Sorunları

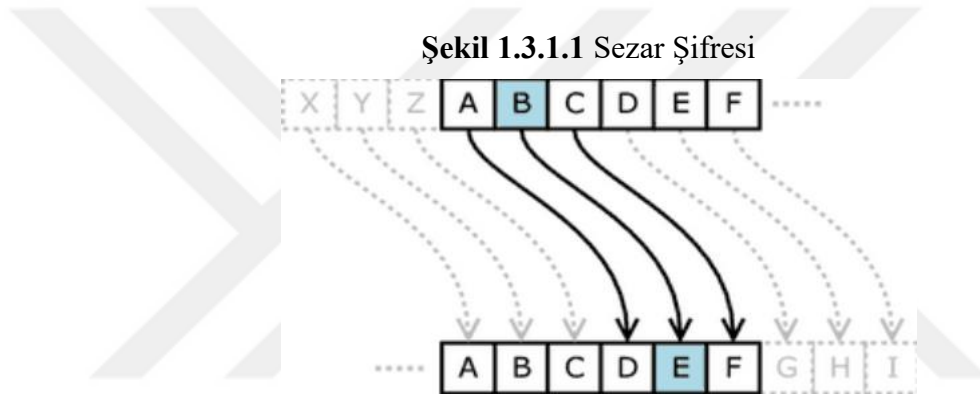
1.3.1. Elektronik Veri İletişiminin Tarihsel Gelişimi

Bölüm 1.2.'de bahsedildiği gibi ilk çağlarda insanoğlunun sahip olduğu tüm varlıklar fiziksel bir formdaydı. İnsanlar için önemli olan bilgiler ilk olarak taşlara kazılıp daha sonra ise kâğıtlara yazılarak saklanmaya başlandı. Bilgilerin kaydedildiği bu varlıkları korumak için ise fiziksel güvenlik önlemleri alınmıştır. Duvarlar örülüp kaleler inşa edilmiş hatta kalelerin etraflarına hendekler kazılmıştır. Ayrıca bu varlıkları gözetmeleri için duvarların ve kalelerin giriş çıkışlarında görevliler yer almıştır (Maiwald, 2003).

Zamanla bilginin sadece saklanması veya depolanması insanların ihtiyaçlarına yetmemiş, bilginin aktarılması ve iletilmesi de temel ihtiyaç haline gelmiştir. Yazının keşfinden önce insanlar mağara duvarlarına resim yaparak birbirleri ile iletişim kurmuşlardır. Duman ve güvercinler uzak mesafede iki kişinin iletişim kurabilmesi için kullanılan yöntemlerdi. Dumanla iletişim ilk olarak milattan önce, Çin de Çin seddindeki askerlerin düşman saldırısına karşı birbirlerine haber verme amacı ile kullanılmıştır. Yerli Amerikalılar ise ateş yakıp dumanlara şekil vererek iletişim kurmaya çalışmıştır. Dumanlar, yeni bir haber, bir tehlike veya insanları bir yere toplamak amacı ile kullanılmıştır. Yazının keşfinden sonra güvercinler ya da ulaklar kullanılarak uzaktaki kişilerle iletişim kurulmuştur. Ancak bu iletişim araçları hava durumunun iyi olmasına ve alıcının görüşünü engelleyen bir unsurun olmamasına bağlı idi. Saklanan varlıklar ya da bilgiler başka bir kişiye gönderilmek istendiğinde, bu varlıklar yolda çalınabilmekte ve belgedeki önemli bilgiler istenmeyen kişilerin eline geçebilmekteydi. Bu durum bilginin sadece saklanmasında değil iletilmesi sırasında da güvenliğini gündeme getirmiştir.

Fiziksel yöntemlerle bilginin korunmasının yetersiz kalması haberleşme tekniklerini değiştirmek durumunda bırakmıştır. Bu durum haberleşme güvenliği

kavramını da beraberinde getirmiştir. İletilen belgeler fiziksel olarak korunamayınca, belgelerde yer alan mesajların içeriği şifrelenmiş ve haberleşme güvenliği sağlanmıştır. Bunun eski örneği ise ismini Roma İmparatoru Julies Sezar'dan alan Sezar Şifresi (Caesar CIPHER)' dir. Sezar'ın askerlerine göndermek istediği mesajdaki harflerin yerleri değiştirilerek mesajın içeriği gizlenmek istenmiştir. Böylelikle, düşmanlar mesajları ele geçirseler bile, mesaj onlara anlamsız gelecektir. Sezar şifreleme metodu alfabetik düzendeki her bir harfin belli bir sayıda ileriye kaydırılmasına dayanmaktadır (Kumari, 2013). Sezar Şifresi Şekil 1.3.1.1.'te gösterilmiştir.



Kaynak: VİKİPEDİ, 2020b, Sezar şifrelemesi, Vikipedi, 5 Şubat, 2020, (Çevrimiçi), https://tr.wikipedia.org/wiki/Sezar_%C5%9Fifrelemesi, 19 Nisan 2020.

Şekil 1.3.1.1.'de anahtar sayı 3 olarak belirlenmiştir. Alfabetik düzen baştan belirlenen bu anahtar sayı kadar kaydırılacaktır. Buna göre A harfi yerine A'dan sonraki 3. harf olan D harfi, B harfi yerine B'den sonraki 3. harf olan E harfi yazılarak metin şifrelenir.

Anahtar sayının 3 olduğu bir Sezar Şifrelemesinde Türk Alfabesine göre şifrelenecek harfler ve şifrelenmiş mesaj Şekil 1.3.1.2.'te gösterilmiştir.

Şekil 1.3.1.2. Sezar Şifrelemesi, Şifrelenmiş Mesaj Örneği

Şifrelenecek Harf: ABCÇDEFGĞHIİJKLMNOÖPRSSŞTUÜYVZ
Şifrelenmiş Harf: ÇDEFGĞHIİJKLMNOÖPRSSŞTUÜYVZABC
Şifrelenecek Mesaj: İŞLETME FAKÜLTESİ
Şifrelenmiş Mesaj: MÜOĞYÖĞ HÇNZOYĞUM

Sanayi devriminden önce iletişimde en büyük sorunlardan biri coğrafya idi. Ancak telgrafın icadı ile uzak mesafe iletişimde çok önemli bir adım atılmış ve ardından gelecek iletişim araçları için öncü olmuştur. Özellikle telgrafın icadı ile hem zamansal hem de mekânsal sorunlardan kaynaklı problemler çözülmüş ve iletişimi daha kolay bir hale getirmiştir. Telgraf zaman içerisinde değişip gelişim göstermiş ve farklı türde telgraf modelleri ortaya çıkmıştır. Elektrikli telgraf sistemi ise iletişim mekanizmasında çok büyük değişime sebep olmuştur. Elektrikli telgraftan önce optik telgraflar kullanılmıştır ancak optik telgraflar da hava koşullarından etkilenebilmekteydi.

Ancak telgraf sadece mekânlar arasındaki sınırları ortadan kaldırmamış zamandaki sınırları da ortadan kaldırmış, iletişimin ulaşımından bağımsız olmasını sağlamıştır. Örneğin, sermaye piyasalarının merkezi olan New York'ta mısır, buğday, hisse senedi ve bonoların fiyatları belirlenmekteydi. Telgrafın kullanımı yaygınlaşmadan önce ABD'deki başka şehirler bu fiyatları New York şehrinde belirlendikten birkaç gün sonra öğrenebilmekteydi. Telgrafın kullanımı ile birlikte piyasadaki fiyatların aynı günde öğrenilebilme imkânı olmuştur (Nonnenmacher, 2001).

Elektrikli telgraflar bir verici, bir alıcı ve iki taraf arasındaki elektrik hattından meydana gelmektedir. Elektrik devresinin bobini bir kolu çekerek kâğıt üzerine izler bırakarak iletişim sağlanmaktaydı. 1836 yılında Samuel Mors tarafından icat edilen elektrikli telgrafta Mors Alfabetesi ile iletişim sağlanıyordu. Şekil 1.3.1.3.'te görüldüğü gibi Mors alfabesi, nokta ve çizgilerden (dot and dash) oluşan bir kodlamadır. Alfabadeki her harfin belli bir uzunluğu vardır. Bobinin kolu kısa veya uzun çekilerek, kâğıt üzerinde kısa ve uzun izler bırakılmaktadır.

Şekil 1.3.1.3. Mors Alfabeti

A	• —	U	• • —
B	• • • —	V	• • • —
C	— • • •	W	— • • •
D	— • • •	X	— • • • —
E	•	Y	— • • • —
F	• • • —	Z	— • • •
G	— • • •		
H	• • • •		
I	• •		
J	• — • • —		
K	— • • • —	1	• — • • • —
L	• • • •	2	• • • • —
M	— • • —	3	• • • • —
N	— • •	4	• • • •
O	— • • —	5	• • • •
P	• • • •	6	• • • •
Q	— • • • —	7	• • • •
R	• • • •	8	• • • •
S	• • •	9	• • • •
T	— •	0	• • • •

Kaynak: DEMİREL, C:2018, “Mors Kodu Hakkında Bilmeniz Gereken Her Şey”, 18 Haziran, 2018 (Çevrimiçi) <http://blog.milliyet.com.tr/mors-kodu-hakkinda-bilmeniz-gereken-her-sey/Blog/?BlogNo=589773>, 30 Nisan 2020

Telgraf postaya göre çok daha kısa bir sürede saatler içerisinde verileri iletmekteydi. Telgraf sadece verinin iletim şeklini değiştirmemiş, aynı zamanda insanların dili kullanma şeklini de değiştirmiştir. Telgraf ile mesaj göndermek pahalı olduğu için, o dönemde toplumun orta ve alt gelirli kesimi tarafından kullanılması çok fazla mümkün değildi. Örneğin, New York’tan New Jersey’e 10 kelimelik bir mesaj göndermek 1860 yılında 2.70\$’dı (bu rakam 2018 yılında 76\$’a karşılık gelmektedir) (Callahan, 2019). Bu nedenle uzak mesafe iletişimin devam ettirilmesinde posta, toplumun geniş kesimince kullanılmaya devam etmiştir. Telefon ve radyonun icat edilmesine dek, telgraf evlerde kullanılan bir haberleşme aracı haline gelememiştir.

Telgraf finansal bilgilerin iletilmesinde ve hatta para transferi aracı olarak da kullanılmıştır. 1872 yılında Western Union (ilk kurulduğu zaman şirketin adı New York and Mississippi Valley Printing Telegraph Company idi) telgraf kabloları ile tek seferde en fazla 100\$ dolar olacak şekilde bir sistem kurarak, ilk fon transferini gerçekleştirmiştir (Callahan, 2019). Telefonun icadı ile telefon kullanımının yaygınlaşmasından dolayı telgraf için işletmeler tarafından farklı kullanım alanları bulunmuştur. 1910 yılında ise Amerikan Merkez Bankası (Federal Reserve of America) para transferini gerçekleştirebilmek için telgrafı kullanmaya başlamıştır (Francis-Poulin, erişim tarihi: 30 Nisan 2020).

Telgrafla iletişimin önemli eksiklerinden bir tanesi tek seferde sadece bir tane mesajın iletilebilmesiydi. Bu yüzden o dönemde telgrafın geliştirilmesi üzerine birçok çalışma yapılmış ve tek seferde birden fazla mesaj iletilme olasılığı düşünülmüştür. 1876 yılında Alexendar Graham Bell tarafından telefonun icat edilmesi ile elektrik hatları üzerinden insanların uzaktan birbirleri ile konuşabilmesi mümkün olmuştur. Telgraflarla insan sesinin iletilmesi mümkün değildi.

1930'ların sonuna doğru ise telefon ya da telgraf hatları kullanılarak metin transferlerinin gerçekleşmesini sağlayan teleks isimli yeni bir iletişim aracı geliştirilmiştir. Resim 1.3.1.1.'te görüldüğü gibi daktilo yapısında olan teleksin, telefonlarda olduğu gibi bir telefon numarası vardır. Haber göndermek isteyen taraf karşı tarafın teleks numarası arar ve göndermek istediği mesajı telekte bulunan klavye ile yazar. Bu yazma işlemi tıpkı daktilo ile yazmaya benzemektedir. Klavyedeki her harf karşı tarafın teleks makinesine elektrik akımları ile iletilir. Gönderilmek istenen mesaj karşı tarafın teleks makinesindeki kâğıda yazılır. Faks makinesinin geliştirilmesi ile teleks kullanımı azalmıştır.

Resim 1.3.1.1. Teleks Makinesi



Kaynak: VİKİPEDİ: 2020C, Telex, (Çevrimiçi) <https://en.wikipedia.org/wiki/Telex> ,30 Nisan 2020

1.3.2. Elektronik Veri İletişiminde Güvenlik Sorunları

Şifreleme yöntemleri ile şifrelenmiş bir verinin içeriğine erişebilmek zaman alan ve zahmetli bir iştir. Resim 1.3.2.1.'de görülen İkinci Dünya Savaşı sırasında Alman mühendisler tarafından geliştirilen Enigma makinesi, Sezar şifrelemesinden sonra şifrelemede en bilinen ikinci örnektir. Hem operatörlerin yaptığı hatalar hem de

İngilizlerin yoğun çabası ile şifreler çözülmüş, iletilen mesajların içeriği okunabilmiştir.

Resim 1.3.2.1. Bir Enigma Makinesi

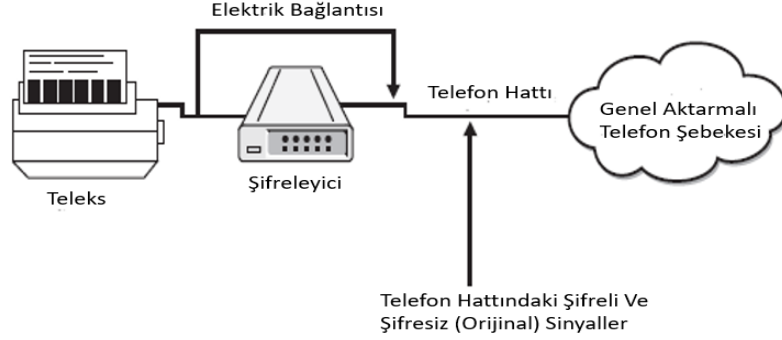


Kaynak: TAŞYÜREK, G.:2020, Enigma Nedir?, 16 Ocak, 2020, (Çevrimiçi)
<https://www.iienstitu.com/blog/enigma-nedir>, 19 Nisan 2020

Ancak İngilizler Enigma makinesindeki şifreyi kırabilmek için çok uzun süre uğraşmış, hatta bu şifreyi kırabilmek için kendileri de makine geliştirmişlerdir. Şifreleri kırmak zahmetli ve zaman alan bir iş olduğu için, gizlenen bilginin veya mesajın şifrelenmeden önceki haline ulaşıp ulaşılamayacağı sorgulanmıştır. Teleks makinesi ile telefon hatları üzerinden gönderilen şifrelenmiş bir mesajın elektrik sinyallerinden mesajın şifreli ve şifresiz haline erişilebilmiştir (Maiwald, 2003).

Fiziksel yöntemlerle iletişim sağlanırken iletilen bilginin gizliliği ve güvenliği konularında sorunlar yaşanabildiği gibi telgraf, telefon, teleks ve faksta da veri iletişimi sağlanırken bilginin istenmeyen kişiler tarafından ele geçirilme durumu söz konusudur. Tüm elektronik sistemler elektrik yayılımları meydana getiriler. Bu durum yayılım güvenliği konusunu gündeme getirmiştir.

Şekil 1.3.2.1. Elektronik Sinyallerin Şifrelemeyi Atlaması (Bypass)



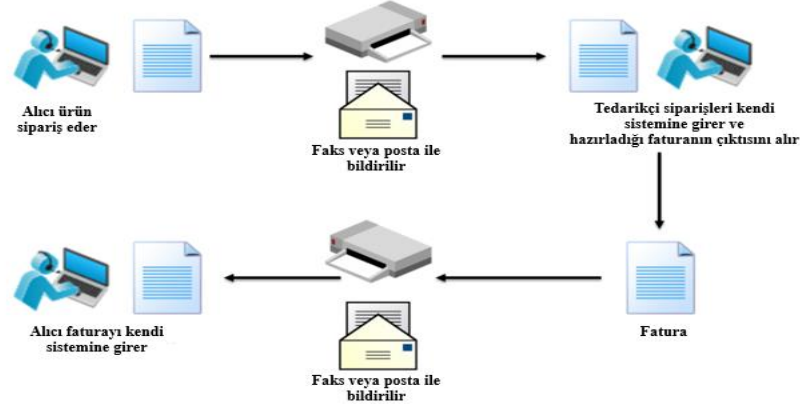
Kaynak: MAIWALD, E.:2001. *Network security: a beginner's guide*.2, s. 11.

Şekil 1.3.2.1.'de görüldüğü gibi teleks makinesi ile yazılan mesaj şifreleyici ile şifrelenir ve telefon hattına iletilir. Hem istemsiz olarak teleks makinesinden yayılan elektrik sinyalleri hem de mesajın şifrelenmemiş hali telefon hattı üzerindedir.

Elektronik veri iletişimi sağlayan araçların ilk örnekleri olan telgraf, telefon, teleks ve faks verilerin daha hızlı bir şekilde iletimine imkân sağlamıştır. Ancak bu teknolojiler ile veri iletişimi kâğıt ve evrak işine dayanmaktadır.

Resim 1.3.2.2.'te bir müşteri ile tedarikçisi arasındaki veri iletimi anlatılmıştır. Satın alma siparişi müşterinin kendi bilgisayarında hazırlanır ve posta, faks veya telefon gibi iletişim kanallarından biri ile tedarikçiye iletilir. Tedarikçiye ulaşan sipariş bilgileri, tedarikçinin sistemine el ile girilir. Belgenin çıktısı alınır ve fatura düzenlenerek müşteriye gönderilir.

Resim 1.3.2.2. Belgelerin Posta ve Faks İle İletimi



Kaynak: VBAP, ERIŞİM TARİHİ: 30 NİSAN 2020. EDI-Elektronik Veri Değişimi(Electronic Data Interchange) , (Çevrimiçi) <https://www.vbap.com.tr/blog/edi-elektronik-veri-degisimielektronic-data-interchange/>, 30 Nisan 2020

Resim 1.3.2.2.'te görüldüğü gibi belgeyi hazırlayıp gönderen firma, kendi hazırladığı belgeyi saniyeler içerisinde basıp çıktısını alabilir. Ancak, belgeyi alan taraf için ise aynı şey geçerli değildir. Karşı taraf belgeyi aldıktan sonra belgenin içindekilerini tekrardan kendi sistemine girmesi gerekmektedir. Çünkü belgeler standart bir formatta hazırlanmamaktadır. İşletmelerin yüzlerce hatta binlerce belge göndererek iş yaptığı düşünülecek olursa bu oldukça zaman alan ve maliyetli bir iştir. Belgelerin nihai yere varması ise ayrı bir sorundur ve çoğu zaman bir kaç günü almaktadır. Posta yoluyla gönderilen belgelerden dolayı, iki taraf arasındaki bilgi akışı gecikebilmektedir. Belgenin kaybolma olasılığı ise her zaman mevcuttur.

İngilizcede Electronic Data Interchange (EDI) olarak kullanılan Elektronik Veri Değişimi (EVD), zaman alan bu evrak işlerini ortadan kaldırarak farklı kurumlardaki bilgisayarların verilerini yeniden kayıt altına alınmasının maliyetlerini ve süresini azaltmak için geliştirilmiştir (Giblin, 1991). EVD, ticaret yapan iki taraf arasında belirli standartlar çerçevesinde insan faktörü olmadan dokümanların bilgisayarlar arasında elektronik bir mesajla transfer edilmesidir. Kâğıt tüketimin ve insan müdahalesinin azaltılması amacı ile ortaya çıkıp kullanılmaya başlanmıştır.

EVD ile bilgi, mesaj veya doküman değişimi telefon, faks ve posta gibi değişim sistemlerinden daha farklıdır. Belgelerin faks, telefon, e-posta gibi elektronik ortamlarda iletilmesi mümkün olsa da veri değişiminin etkinliği üzerinde çok fazla bir

etkisi olmamıştır. Bunun sebebi ise bu kanallar ile doküman gönderiminde dokümanda yer alan bilgilerin alıcının bilgisayarına tekrardan el ile girilmesidir. Bu durum verilerin kaydedilmesi sırasında hataların meydana gelmesine sebep olabilmektedir. EVD, bilgisayardan bilgisayara elektronik olarak iletilen bu belgelerin tekrardan bilgisayarlara girişini önleyen organizasyonlar arası bir sistemdir. Büyük uluslararası şirketler 1960'lı yılların ortasında bilgisayar sistemlerinin arasında doğrudan veri bağlantıları kurmaya başlamışlar ve “kâğıtsız ofis” bakış açısı ile insan faktöründen kaynaklı hataları ortadan kaldıran daha güvenilir iletişim kurmayı amaçlamışlardır (Vasters, 2001).

EVD organizasyonlar arası bir iletişim sistemidir. Özellikle tedarik zincirindeki üyelerin iletişimi arttıkça firmalar birbirlerinin isteklerine daha hızlı cevap verebilmiştir. Bu durumda aynı zamanda müşteri hizmetlerinin kalitesini de arttırmıştır. Tarafların arasında daha iyi iletişim kurabilmesi, maliyetlerin azalması, kâğıt ve dokümantasyon işlerinin azalması, iş akışındaki verimliliğin artması EVD'nin sağladığı faydalar arasındadır.

EVD'nin en bilinen örneklerinden birisi de Elektronik Fon Transferidir (Electronic Fund Transfer-EFT). EFT'nin günümüzde bu kadar yaygın olarak kullanılmasının geçmişi Automated Teller Machine (ATM)'lerin ilk ortaya çıktıkları 1960'lı yılların ortasına dayanmaktadır. ATM'ler kişinin kendi başına hizmet eden para çekme makineleri olarak kullanılmaktaydı. ATM ilk olarak İngiltere'deki Barclays Bankası tarafından 1967 yılında kullanılmıştır. ATM'ler ilk kullanıma başlanıldığı zaman günümüzde kullanılan kredi kartları ile değil kâğıt fişler (paper-voucher) ile gerçekleşmekteydi. Bu kâğıt fişler makineye sokulur ve okutulur ve fişin karşılığında tek seferde £10 çekilebilirdi. ATM kullanımı bankanın çalışma saatleri dışında da elektronik olarak hesaplar arasında para transferi yapmayı, hesaba para yatırmayı ve para çekmeyi mümkün kılmıştır.

Birçok avantajı olmasına rağmen EVD'nin dezavantajları da bulunmaktadır. İnternetin ortaya çıkışına kadar EVD teknolojisi katma değer ağları (Value Added Networks -VANs) ile iletişim sağlanıyordu. Özel bir telekomünikasyon altyapısı ve belli standartlar gerektirdiği için kurulum maliyeti ve bakım maliyeti yüksekti. Önemli

ölçüde yatırım gerektiren sistemlerdi. Her kurumun böyle bir sistemi iş yaptığı taraf ile kurması mümkün değildi. Bu yüzden bu teknoloji büyük firmaların kullanımı için uygun olmuştur.

Bilgisayarların ortaya çıkışı ve kullanımının artması ile birlikte kurumlar önemli bilgilerini elektronik formatta bilgisayarlarda depolamaya başlamıştır. Zamanla bilgisayarın kullanımı kolaylaşmış ve çok fazla kişi bilgisayara erişim imkânına sahip olmuştur. Böylelikle bilgisayarlardaki bilgiler sisteme erişebilen herkes için ulaşılabilir hale gelmiştir. Bu durum, bilgisayar güvenliğine olan ihtiyacı gündeme getirmiştir. İlk olarak bilgisayarlarda saklanan bilgiler gizli, çok gizli ya da sınıflandırılmamış gibi gizlilik derecelerine göre sınıflandırılmış, aynı şekilde çalışanların da bilgiye erişim yetkisi sınıflandırılmıştır.

Bilgisayar ağları verileri bir bilgisayardan diğerine ileterek bir işin daha etkin ve kısa sürede yapılmasını mümkün kılmaktadır. Bunun en basit örneği EVD’de olduğu gibi iki bilgisayarı kablolar ile birbirine bağlayarak, noktadan noktaya veri aktarılmasıdır. Ancak EVD’de olduğu gibi özellikle birbirinden çok uzakta olan bilgisayarların bağlantısı da çok masraflı olmaktadır. Ayrıca birbirine bağlanması gereken çok sayıda bilgisayar olması durumunda yine çok masraf olacak ve karmaşa olacaktır. Bu sebeple, bilgisayarları kablolar ile birbirine bağlamak yerine, bir iletişim ağı oluşturarak bilgisayarları bu iletişim ağlarına bağlama fikri ortaya çıkmıştır. Yerel Alan Ağları (Local Area Network-LAN) ile Geniş Alana Ağları (Wide Area Network-WAN) ağ yapıları geliştirilmiştir.

İnternetin ortaya çıkışı ve 2000’li yıllarda kablosuz ağ teknolojilerinin gelişmesi ile birlikte küçük ve büyük ölçekli firmalar internet üzerinden belge gönderimi imkânına sahip olmuştur. EVD uygulamalarına daha ucuz çözümler bulunmuştur. İnternet teknolojileri ile bilgilere herkes tarafından ulaşılabilmekte ve çok fazla bilgi paylaşımı yapılabilmektedir. Özellikle internet üzerinden ticaret imkânının doğması ile birlikte bilgi teknolojileri çok hızlı gelişmiştir.

1980’lerin sonu ve 1990’lı yılların başında internet teknolojisinin ortaya çıkması ve 2000’li yıllarda gelişmesi e-posta, World Wide Web, facebook, instagram, tweeter gibi sosyal medya uygulamalarını hayatımıza sokmuş, bilgi ve para

transferlerinin ve ödemelerin daha hızlı ve kolay şekilde yapılmasına imkân sağlamıştır. İnternet, iletişimin dijitalleşmesinde devrimsel bir adımın atılmasına sebep olmuştur.

Bilgisayarların birbirleri ile iletişiminin yaygınlaşması ve gelişmesi beraberinde ağ güvenliği konusunu meydana getirmiştir. Ağ, iki veya daha fazla bilgisayarın aralarında kaynak paylaşması yapmasını (yazıcı, uygulamalar gibi), dosya değişimi yapmasını veya elektronik iletişimini sağlayan bir yapıdır. Ağdaki bilgisayarlar birbirlerine kablolar, telefon hatları, radyo dalgaları ve uydular ile bağlanabilirler. Birden fazla bilgisayarın bağlı olduğu bu ağlara yapılacak olan kötü niyetli bir saldırıda tüm sistem çökebilir ve paylaşılan bilgiler açığa çıkabilir, değiştirilebilir, yetkisiz kişiler tarafından erişilebilir. Bilgisayar ağlarının yaygınlaşması yeni güvenlik açıklarını ortaya çıkarmıştır. Bu açıklar ise güvenlik ihlallerinin artmasına sebep olmuştur.

Günümüzde fiziksel koruma ile verilerin saklanması teknolojinin gelişmesi ile daha farklı yöntemlerle devam etmektedir. Bina içleri ve dışları kamera ile izlenmekte, odalar kilitlenmekte, şifreli güvenlik sistemleri kullanılmaktadır. Ancak kullanılan tüm bu fiziksel önlemlere rağmen bilgiler istenilen düzeyde korunamamakta, bilgilerin çalınması ya da yetkisi olmayan ve istenmeyen kişilerin eline geçmesinin önüne geçilememektedir.

Geçmişten günümüze kadar geçen bu sürede veri formunun, verinin saklanması, insanlar ve kurumlar arası iletişimin ve teknolojinin gelişmesi ve değişmesi sonucunda bilgi güvenliği konusu daha da önemli bir hale gelmiştir.

1.4. Elektronik Ortamda Veri İletişiminde Bilgi Güvenliğinin Unsurları

Günümüzde işletmelerin birbirleri ile ticaret ve iş yapma ağının ne kadar arttığı düşünülecek olursa işlerin yürütülmesi için bilgi aktarımı kaçınılmaz bir durumdadır. Bu da, işletmelerin en önemli varlıkları arasında olan bilgiyi, çok önemli bir yerde konumlamaktadır. Bu yüzden kişiler ya da kurumlar arasında bilgi iletimi yapılırken bilginin zarar görmemesi gerekmektedir. Bilgiye karşı yapılan saldırılar ve bilginin zarar görmesi işlerin akışının aksamasına sebep olacaktır.

Gün geçtikçe artan bir hızla gelişen bilişim teknolojileri, bilgilerin depolanması, transferi, işlenmesi ve paylaşılması konusunda işletmelere büyük faydalar sağladığı için işletmeler tarafından teknolojiye sürekli yatırım yapılmaktadır. İşletmelerin iş yapış şekillerini daha etkin ve verimli bir hale getirdiği için işletmeler teknolojiye bağımlı hale gelmişlerdir. Faaliyetlerini teknolojik araçlarla, yazılımlarla ve donanımlar ile gerçekleştiren işletmeler için elektronik ortamda bulunan verilerin güvenliğini sağlamak oldukça önem arz etmektedir.

Her ne kadar gelişen teknolojilerin işletme faaliyetlerinin hızlandırılması ve daha verimli çalışması gibi faydaları olsa da bazı tehditleri de içermektedir. Bunlardan en önemlisi bilgi güvenliğidir. Elektronik bilgi güvenliği, haberleşme ve bilgisayar güvenliğini kapsayarak, bilgilerin ifşa edilmesini, yok edilmesini ve değiştirilmesini engellemektedir (Gifford, 1988). Elektronik bilgi güvenliği, elektronik ortamlarda iletilen bilginin güvenliğini ifade etmektedir. Bilgi güvenliğinin sağlanabilmesi için üç temel unsur yeterli düzeyde sağlanması gerekmektedir. Bu üç temel unsur: gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik/erişilebilirliktir (availability). Ancak bu üç temel unsurun yanı sıra inkâr edememe (non-repudiation), güvenilirlik (reliability), kimlik tanımlaması (authentication), yetkilendirme (authorization) ve kayıt tutma da dikkate alınması gereken diğer önemli unsurlardır. Bu unsurlardan birinin eksikliği bilgi güvenliğinde aksamalara ya da istenen seviyede sağlanamamasına sebep olmaktadır. Üç temel unsur literatürde CIA bileşenleri olarak da kullanılmaktadır.

Gizlilik, elektronik ortamlarda iletilen bilgiye, depolanması ya da saklanması, işlenmesi ve iletilmesi sırasında yetkilendirilmemiş bir kişi ya da kurum tarafından ulaşılmamasının sağlanmasıdır. Gizlilik, istenmeyen kişilere karşı bilginin erişiminin engellenmesidir. Gizlilikte amaç elektronik ortamlarda saklanan verilerin saldırganlar tarafından ele geçirilse bile anlaşılmamasıdır. Elde edilen bilgilerin anlamlı olarak ele geçirilmesinin engellenmesidir. Şifreleme, gizliliğin sağlanması için başvuru olan yöntemlerden en bilinenidir.

Bütünlük, elektronik ortamlarda aktarılan bilginin bozulmadan, doğru ve tam bir şekilde aktarıldığının, değiştirilmediğinin garantisidir. Bütünlük, verinin içeriğinin yetkisi olmayan kişilerden korunmasıdır. Bilginin haberleşme sırasında

değiştirilmemiş, zarar görmemiş ve yeni veriler eklenmemiş hali ile alıcıya ulaştırılmasını ifade etmektedir. Bütünlük ile bilginin tutarlılığı, doğruluğu ve güvenilirliği sürdürülür. Bilgi bütünlüğünün sağlanmasının en önemli yöntemlerinden biri özetleme fonksiyonlarının (hash algorithm) kullanılmasıdır. Özellikle blok zinciri teknolojisinde sıklıkla kullanılan bu fonksiyonların önemi daha da ortaya çıkmaktadır.

Erişilebilirlik (kullanılabilirlik), bilgiye erişim yetkisi olan kullanıcılar ya da kurumlar tarafından bilginin kullanılabilir ve ulaşılabilir olmasıdır. İhtiyaç duyulduğu anda herhangi bir engel ile karşılaşmadan bilginin kullanıma hazır halde olmasıdır. Ancak bu erişim kişilerin yetki sınırlarında olmalıdır. Servis dışı bırakma saldırısı (Denial of Servis Attack -DoS) gibi saldırılar bilgiye yetkili kişiler tarafından erişilmesini engellemektedir. Ayrıca bilgisayar yazılımlarının yanlış kodlanması, değiştirilmesi sitemdeki bilgilerin erişilebilirliğini olumsuz yönde etkilemektedir.

Bu temel kavramların yanında inkâr edememe, güvenilirlik, kimlik kanıtlama, yetkilendirme ve kayıt tutma unsurları da bilgi güvenliliğin sağlanması ve güvenlik zafiyetinin oluşmaması için önem arz etmektedir.

Güvenirlik, bir bilgisayarın ya da bilgisayar sisteminin önceden belirlenmiş kurallar doğrultusunda tasarımına uygun olarak sürekli çalışması ve sistemin kendisinden beklenenleri tutarlı ve eksiksiz bir şekilde yerine getirebilme yeteneğidir (Canbek ve Sağıroğlu, 2006). Diğer bir ifade ile sistemin öngörülen, beklenen davranışları ile gerçekleşen davranışları arasında tutarlılığın sağlanmasıdır. Güvenirlik bilgi sistemine olan güveni ifade etmektedir.

Inkâr edememe, elektronik ortamda bilgi gönderimi yapıldığında, ne gönderen bilgiyi gönderdiğini ne de alıcı bilgiyi aldığını inkâr edememelidir. Bunun engellenmesi için alınan önlemleri ifade etmektedir. Bu sayede bilgiyi gönderen ve alan taraf arasında çıkabilecek olası anlaşmazlıkların da önüne geçilmesi sağlanmaktadır. Elektronik imzalar, inkâr edememe güvenlik unsuruna örnek olarak gösterilebilirler.

Kimlik tespiti, bilgi sistemindeki bir kullanıcının, kimliğinin doğrulanması ve kanıtlanmasıdır. Sisteme girmeye çalışan kişinin iddia ettiği kişi olup olmadığının emin olunmaya çalışılmasıdır. Bu süreç kullanıcının sisteme giriş hakkı olup

olmadığının araştırılması ile başlamaktadır. Daha sonrasında, kullanıcıya tanımlanan parola veya şifre ile doğrulama yapılır ve sistemdeki kayıt ile eşleşmesi durumunda sisteme giriş hakkı verilir. Kimlik doğrulaması, kullanıcıların hangi dosyalara erişebileceğini belirlemez. Kimlik doğrulaması, kullanıcıların kim olduğunu tanımlar, doğrular ve sisteme giriş yapmasını sağlar.

Yetkilendirme, bilgiye doğru kişinin ulaşp ulaşmadığını kontrol eden bir sistemdir. Yetkilendirme ile kullanıcı kimliğinin başarılı bir şekilde doğrulandığı varsayılarak, sisteme kayıtlı kullanıcıların bilgilere erişim hakkına ya da iznine sahip olup olmadıkları belirtilir. Yetkilendirme, kullanıcıların hangi bilgiye erişebileceğini ve hangi eylemleri gerçekleştirebileceğini belirtmektedir. Özellikle işten ayrılma gibi durumlarda kişilerin yetkilerinden dolayı sahip olduğu haklar geri alınmalıdır. Sadece işten ayrılma değil aynı kurum içerisinde bölüm değişikliği yapılsa bile kimlik yönetimi oldukça önemlidir.

Kayıt tutma, elektronik ortamlarda meydana gelen olayları işletmelerin kendi sistemlerinde kayıt altına almalarıdır. Merkezi bir sistemde tutulan bu kayıtlar, verilere kimlerin, ne zaman eriştiğini, sisteme nasıl erişim sağlandığını, işleme ait tüm bilgileri içermektedir. İşlemlere ait kayıtların tutulması bilgi güvenliği açısından problemli olan yerlerin denetimi, analizi ve çözümlenmesi için önemlidir.

Bu unsurların büyük ölçekli firmalarda küçük ölçekli firmalara göre karşılanması daha zordur. Büyük ölçekli işletmelerde çalışan sayısının fazla olması, farklı bölgelerde faaliyetlerini sürdürmesi ve ofisinin olması, kullanılan teknolojik cihazların ve donanımların fazla olması sebebi ile büyük ölçekli firmaların bilgi güvenliğini sağlaması küçük ölçekli firmalara göre oldukça zordur.

Toplumların ve teknolojinin gelişmesi ile bilgilerin gizliliğini ve güvenliğini sağlamak oldukça zor bir hale gelmiştir. İletişimin dijitalleşmesi ile gizlilik kavramının ele alınması şekil değiştirmiş ve internet üzerinden paylaşılan bilgilerin gizliliğini çok büyük bir sorun haline dönüştürmüştür. İnternet üzerinden paylaşılan bilgilerin gizliliğine karşı olan bu güven sorununu ortadan kaldırmak için insanlar aracı kurumları tercih etmiş, banka ya da devlet gibi üçüncü taraflar devreye girmiştir. İnternet bilgiye ulaşma ve paylaşma maliyetlerini düşürse de, aracı kurumlar

sundukları bu “güven” hizmeti için ücret almaktadırlar. Her ne kadar aracı kuruluşların rolü güven sorununu ortadan kaldırmak olsa da, internet üzerinden bilgi paylaşımındaki sızıntılar tam anlamıyla önlenememiştir. Kişisel bilgilerin finansal kuruluşlar ya da devlet gibi merkezi bir otoritede toplanması bilgilerin çalınmasında bilgisayar korsanlarının işini kolaylaştırmış ve 2008’de Amerika Birleşik Devletleri’ndeki finansal kriz ile finansal kurumlara olan güven azalmıştır.

Bu güven boşluğu yeni bir teknoloji olan ve tezin ikinci bölümünde detaylıca anlatılan blok zinciri teknolojisini hayatımıza kazandırmıştır.



İKİNCİ BÖLÜM

BLOK ZİNCİRİ TEKNOLOJİSİ

2.1.Blok Zinciri Teknolojisinin Tarihsel Gelişimi

Blok zinciri teknolojisinin ortaya çıkışı ile ilk kripto para birimi olan Bitcoin'in tanıtılması neredeyse birbirinden ayrılmaz bir şekilde bağlantılıdır. 2008 yılında Satoshi Nakamoto isimli bir kişi (ya da bir grup) tarafından “Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi (A Peer-To-Peer Electronic Cash System)” başlıklı bir çalışma yayınlanmıştır. Yayınlanan bu çalışmada, kişilerin aralarında doğrudan ödeme yapabileceği eşler arası, dağıtık bir sistemden bahsedilmiş bu şekilde finansal kurumlar ya da üçüncü kişilere olan ihtiyacın nasıl ortadan kaldırılabilceği ilk kripto para birimi olan Bitcoin açıklanarak anlatılmıştır.

Her ne kadar 2008 yılında Satoshi Nakamoto tarafından yapılan bu çalışma ile blok zinciri teknolojisi adını duyurmuş olsa da bu teknolojinin temelleri aslında daha eskiye dayanmaktadır. Bu alanda sıkça kullanılan kavramlar Bitcoin'in ortaya çıkmasından önce de kullanılmaktaydı. Bunlardan bazıları, merkezi olmayan yapılar, eşler arası iletişim, mutabakat (uzlaş) yapıları, şifreleme ve zaman damgasıdır. Ancak blok zinciri teknolojisini farklı kılan, tüm bu kavramları ilk kez bir arada kullanabilmiş olmasıdır.

Blok zinciri teknolojisine ulaşılan süreçte ilk aşamalardan birisi, 1991 yılında Stuart Haber ve W. Scott Stornetta tarafından ele alınan makaledir. Bu makalede elektronik belgelerin zaman damgası (time-stamping) ile birlikte kriptografik olarak nasıl kullanılacağı, dijital imzalar kullanılarak belgelerin değiştirilmesinin önüne geçilebileceği anlatılmıştır (Haber ve Stornetta, 1991). Belgeler zaman damgalı olacağı için geriye dönük değiştirilmesi engellenmektedir. Aslında, blok zincirinde bahsedilen birbirine bağlı ve değiştirilemeyen blokları anlatan bu çalışma, blok zinciri teknolojisinin ortaya çıkışındaki en önemli çalışma olarak kabul edilmektedir.

Bu çalışmayı takip eden bir başka gelişme, 1992 yılında, Eric Hughes, Timothy C. May ve John Gilmore öncülüğünde Cypherpunk e-posta grubunun kurulmasıdır. Bu

e-posta grubu, grupta yer alan kişilerin kendi aralarında genellikle matematik, şifreleme ve bilgisayar bilimi olmak üzere çeşitli konular hakkında fikir alışverişi yapmalarına imkân sağlamıştır. Cypherpunk e-posta grubu üyesi Eric Hughes 1993 yılında A Cypherpunk's Manifesto'yu (Bir Şifre Haydutu'nun Manifestosu) yayınlamış ve bu manifestoda mahremiyetin (privacy) belli bir otorite olmadan sağlanmasının gerekliliği anlatmıştır. Mahremiyetin devlet kanunları yerine kriptoloji ile sağlanması savunulmuş ve bunu sağlamak için de anonim sistemlerin gerekliliğinden ve öneminden bahsedilmiştir (Hughes, 1993).

1992 yılında, Cynthia Dwork ve Moni Naor tarafından istenmeyen (spam) e-postaları önlemek üzere bir çalışma yapılmıştır. E-posta gönderecek olan kişinin, e-posta göndermeden önce fiyatlandırma fonksiyonunu (pricing function) kullanarak e-posta servisine erişebilmesi için orta derece zorlukta olan bir fonksiyonu hesaplaması gerekmektedir (Dwork ve Naor, 1992). Spam e-postaları, atan kişiler için maliyetli ve zaman alan bir iş olmuştur. Bu hesaplamalara “iş” denilmiş ve e-postayı alan kişi için yapılan bu hesaplamaların maliyeti “kanıt” olarak görülmüştür (Sengel, 2020). Çalışmada iş kanıtı (proof of work) terimi kullanılmamış olsa da günümüzde Bitcoin’de kullanılan iş kanıtı (proof of work) algoritmalarının temelini oluşturmuştur.

1996 yılında Ross Anderson tarafından hazırlanan bir başka makalede ise, kaydedilen belgelerin silinemeyeceği ve verileri makineler arasında çoğaltarak, merkezi olmayan bir veri depolama sistemi tanımlanmıştır (Anderson, 1996).

1997 yılına gelindiğinde, Adam Back tarafından, iş kanıtı algoritması ve kriptografik özetleme (hash) fonksiyonlarını kullanarak, istenmeyen e-postaları ve DoS saldırılarını önlemek üzere Hashcash algoritması tasarlanmıştır. Dwork ve Naor tarafından yapılan çalışmaya benzer bir çalışma olmakla birlikte, Adam Back bu istenmeyen e-postaları özetleme algoritmaları ile önlemiştir (Back, 2002). Bu gelişme blok zinciri teknolojisine ulaşılmasında önemli bir aşamadır. Sonraki yıllarda, Satoshi Nakamoto, Bitcoin’i Adam Back’in çalışmasındaki benzer bir özetleme algoritması ile yaptığını belirtmiştir (Nakamoto, 2008:3).

1998 yılında Wei Dai tarafından “B Money” protokolü geliştirilmiştir. Yayınladığı yazısında göndericilerin ve alıcıların dijital takma adları ile tanımlandığı

ve her mesajın göndericisi tarafından imzalanıp alıcısına şifrelendiği takip edilemez bir ağın varlığından bahsetmiştir (Dai, 1998). Gönderici tarafından şifrelenen işlemler bütün ağa yayılmaktadır. Dai'nin çalışmasında blok zincirinde işlemlerin ağdaki herkesle paylaşılması ve kaydedilmesine benzer bir sistem kullanılmıştır.

1998 yılında Bruce Schneier ve John Kelsey tarafından yazılan bir başka makalede ise, güvenilmeyen makineler üzerinde tutulan günlük dosyalarının (log files) içerdiği hassas bilgilerin saldırganlar tarafından okunmaması, değiştirilmemesi veya yok edilmemesi kısacası korunması için şifrelemenin nasıl kullanılacağı açıklanmıştır (Schneier ve Kelsey, 1998).

1998 yılında Nick Szabo tarafından dağıtık yapıya sahip dijital para Bit Gold öne sürülmüş ve 2005 yılındaki blog yazısında ise bu fikrinden açıkça bahsetmiştir. Nick Szabo yazısında çevrimiçi bir ortamda üçüncü taraflara güvene ihtiyaç olmadan üretilecek paradan ve bunların güvenli bir şekilde saklanacağı, transfer edileceği para olan Bit Gold'dan bahsetmiş, Bitcoinin de temel fikirlerinden olan merkezileştirmeye karşı yapının üzerinde durmuştur (Szabo, 2005).

Tüm bu gelişmeler çerçevesinde 2008 yılında Amerika'daki finansal krizin ortaya çıkması ile finansal kurumlara olan güven sarsılmış ve 1990'lı yıllarından beri gizlilik ve güven için şifreleme ve diğer bilgisayar teknikleri ile alternatif bulmaya çalışan kişilerin çalışmaları ve düşünceleri bir araya getirilerek 2008 yılında Bitcoin tanıtılmıştır. Kriptografi alanından önemli çalışmaları olan ve Cypherpunk grubu üyesi olan Hal Finney, 2009 yılında Satoshi Nakamoto'dan 10 Bitcoin alarak ilk Bitcoin transferini gerçekleştirmiştir.

Yukarıdaki kişilerin yapmış olduğu araştırmalar dijital imzalama, çalışma kanıtı algoritmaları, anonim haberleşme, kriptoloji gibi önemli teknolojik yenilikleri ortaya koymuştur. Her ne kadar Satoshi'nin makalesinde blok zinciri kelimesi açıkça yer almasa da, blok zinciri, çalışmanın yayınlandığı tarihten itibaren günümüze kadar gittikçe artan bir ilgi ile üzerinde konuşulup çalışılan bir teknoloji olmuştur.

2.2.Blok Zinciri Teknolojisinin Tanımı ve Çalışma Prensibi

“Blockchain” kelimesinin henüz herkes tarafından kabul edilmiş ortak bir Türkçe çevirisi bulunmamaktadır. Akademik çalışmalar ve haberler takip edildiğinde, blokzincir; blok zincir; blok-zincir; blokzinciri ve blok zinciri gibi farklı kullanımlara rastlanılmaktadır. “Blockchain” kelimesinin yazılışı ile ilgili Türk Dil Kurumuna (TDK) sorulan soru üzerine, blockchain birleşik kelimesinde “blok” ve “zincir” kelimelerinde bir anlam kayması olmadığı ve “blok zinciri” şeklinde yazılmasının TDK’nin Yazım Kılavuzu açısından uygun olduğu belirtilmiştir (Yıldırım, 2019). Türk dili yazımı konusunda ülkemizdeki yetkili makam olan TDK’nın vermiş olduğu bu cevap üzerine bu tezde “blockchain” kelimesi blok zinciri olarak çevrilmiştir.

Bitcoin, dağıtık bir yapıda üçüncü bir tarafa (banka veya finansal kurumlar gibi) ihtiyaç duyulmadan dijital para transferine imkân sağlamıştır. Yapılan işlemlerin merkezi bir otoriteye ihtiyaç duyulmadan taraflar arasında doğrudan yapılabilmesi ise blok zincirin getirdiği en büyük fayda ve yeniliktir.

Blok zinciri, aracıları ortadan kaldırarak şirketlerin ve bireylerin, üçüncü taraflarla çalışmasından kaynaklı işlem maliyetlerini ve sürelerini kısaltarak işlem yapabilmelerine izin veren internet gibi açık ve küresel bir altyapıdır (Underwood, 2016). Blok zinciri teknolojisi kullanılarak gerçekleşen bir işlem merkezi olmayan bir ortamda gerçekleşeceği için, işlem maliyetleri azalacak ve verimlilik artacaktır.

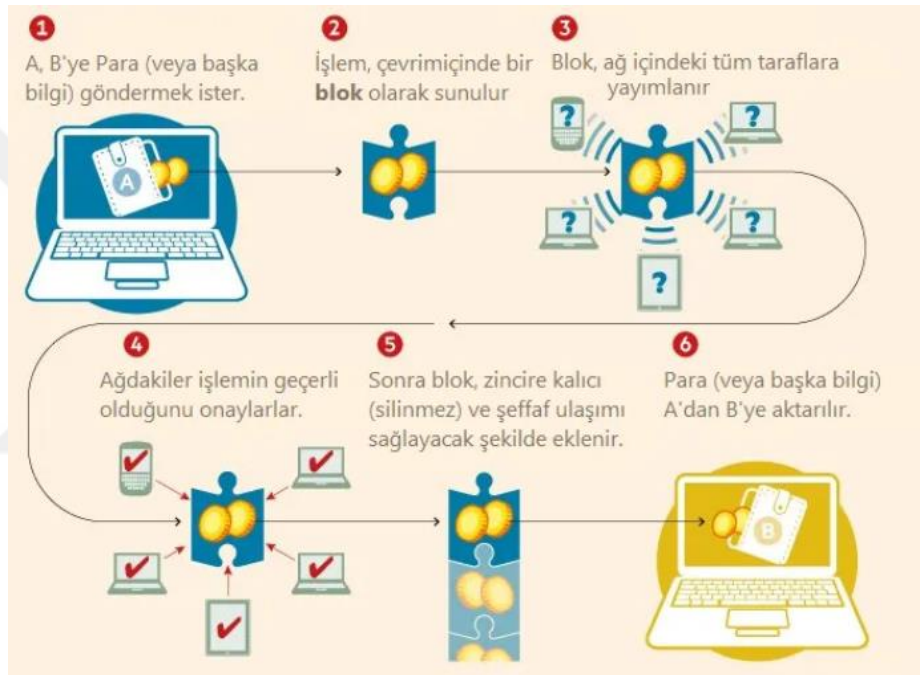
Blok zinciri, dağıtık defter (distributed ledger) yapısına ve mutabakat sürecine (consensus process) dayanmaktadır. Bu yapı dijital defterde yer alan işlemlerin birden fazla bilgisayar arasında yaratılıp paylaşılmasına izin vermektedir. Bu deftere sahip olan ya da kontrol eden merkezi bir otorite ya da kurum yoktur.

Bir kullanıcı bu deftere bir işlem eklemek istediği zaman, işlem verileri şifrelenmekte ve ağdaki diğer bilgisayarlar tarafından şifreleme algoritmaları kullanılarak doğrulanmaktadır. Bilgisayarların çoğunluğu tarafından işlemin geçerli olduğuna dair mutabakata varılırsa, verilerin olduğu yeni bir blok, zincire eklenmekte ve tüm ağ ile paylaşılmaktadır. Ağdaki tüm katılımcılarla paylaşılan bir işlem, bir daha asla silinemez. Bu yüzden blok zincirine kaydedilen işlemler güvenli, güvenilir, izlenebilir ve değiştirilemezdir. İşlemler onaylandıktan sonra kronolojik olarak zincire

kaydedilmektedir. Defterdeki kayıtlar ağdaki tüm kullanıcılar tarafından görülebilmektedir. Verileri herkesin görebiliyor olması şeffaflığı sağlamaktadır.

İşlemler ve işlemlerin hangi hesaptan yapıldığının görülebilmesi mümkünken, şifreleme teknikleri ile anonimlik (anonymity) sağlanarak işlemin kim tarafından yapıldığı veya hesabın kime ait olduğu görülmesi mümkün değildir. Şekil 2.2.1.'de blok zinciri teknolojisinin çalışma mantığı anlatılmaktadır (Aytaç, 2017).

Şekil 2.2.1. Bir Blok Zinciri Nasıl Çalışır?



Kaynak: WILD, J., ARNOLD, M., STAFFORD, P.: 2015. Technology: Banks Seek the Key to Blockchain-FT. com., November 1, 2015, Financial Times. Np, 1., (Çevrimiçi) <https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64>, 11 Mayıs 2020.

İnternette sonrakı en büyük teknoloji olarak görülen blok zincirinin henüz herkes tarafından kabul edilen tek bir tanımını bulunmamaktadır.

Ethereum blok zinciri platformunun yaratıcısı olan Vitalik Buterin 2015 yılında, blok zinciri için farklı bir tanım yapmıştır. Buterin, blok zincirini, herhangi biri tarafından programların yüklenebildiği, bu programların kendiliğinden yürütülebildiği, yüklenen her programın mevcut ve önceki durumlarını her zaman açık bir şekilde herkes tarafından görülebildiği zincirlerdeki güçlü şifrelemeler ile programları güvence altına alan sihirli bilgisayarlar olarak tanımlamıştır (Buterin, 2015).

Bir tanıma göre, bu teknoloji, temel olarak değer içeren verilerin (para, kimlik, değerli kâğıtlar gibi) güvenli ve emin bir şekilde depolanması ve yönetilmesi için tasarlanmıştır (Doğantekin, 2016).

Bir başka tanıma göre, iş ağındaki işlemleri kaydetme ve varlıkları izleme sürecini kolaylaştıran paylaşılan, dağıtılmış bir defter olarak tanımlanmıştır. Burada kaydedilen, ev, araba, nakit, arazi gibi somut varlıklar olabileceği gibi patent, telif hakkı veya marka gibi maddi olmayan varlıklar da olabilir (Gupta, 2017:3).

Swan (2015)'e göre, blok zinciri teknolojisi (diğer adı ile dağıtık defter teknolojisi), bankalar veya diğer finansal kurumlar gibi bir aracıya ihtiyaç duymadan internet üzerinden para, varlık ve bilgilerin güvenli bir şekilde aktarılmasını sağlamaktadır.

Başka bir tanıma göre ise blok zinciri teknolojisi, işlemlerin veya dijital olayların blok zincirine dahil olan tüm katılımcılar arasında yürütülen ve paylaşılan dağıtık bir veri tabanı veya herkese açık olan bir defterdir (Crosby ve ark., 2016).

Kısaca, blok zinciri teknolojisi, ihtiyaçlara karşılık olarak herkese açık, şeffaf, merkezi olmayan ve ara yapılara ihtiyaç duymayan çözüm öneren bir teknolojidir.

2.3.Blok Zinciri Teknolojisinin Temel Kavramları

2.3.1. Eşten Eşe Ağ

Türkçede eşler arası ya da eşten eşe olarak tanımlanan bu ağ çeşidi İngilizcede peer to peer (P2P) olarak ifade edilmektedir. Bunlar, bilgisayarların merkezi bir sunucuya bağlı olmadan aralarında kaynaklarını paylaştıkları dağıtık ağlardır. İstemci/sunucu ağ tiplerinde sunucu, ağdaki kullanıcıların erişebileceği kaynakları bulunduran bilgisayarı ifade etmektedir. İstemci (ya da tüketici) ise ağda bulunan bu sunucudan hizmet alan bilgisayarlardır. Eşten eşe ağ tipinde ise sistemde bulunan kullanıcılar hem istemci hem de sunucu görevindedir.

İstemci/Sunucu (Client/Server) ağı, yüksek performanslı bir **sunucu bilgisayar** ile birden fazla düşük performanslı **istemci bilgisayar** sisteminden oluşan dağıtık bir ağıdır. Merkezi kayıt birimi olan sunucu, aynı zamanda içerik ve hizmet

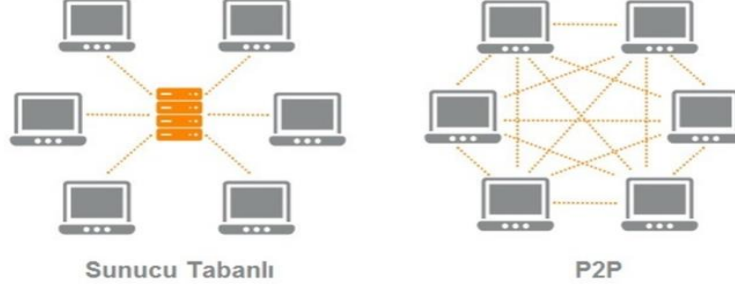
sunan tek birimdir. İstemci sadece içerik ya da servislerin uygulanmasını ister, herhangi bir kaynak paylaşımı yapamaz (Schollmeier, 2001). Bu tip ağlarda tek bir merkezi bilgisayar vardır. Ağdaki bilgisayarlar ya istemcidir ya da sunucudur, her iki görevi aynı anda gerçekleştiremezler.

Eğer sistemdeki katılımcılar işlemci gücü, ağ bağlantı kapasitesi, saklama kapasitesi, yazıcılar gibi kendi kaynaklarının bir kısmını paylaşırlarsa dağıtık ağ yapısı eşten eşe ağ olarak adlandırılabilir. Bu paylaşılan kaynaklar ağda hizmet ve içerik sağlamak için gereklidir. Bu kaynaklar sistemdeki diğer katılımcılar tarafından aracı bir kişiye ihtiyaç duyulmadan doğrudan erişilebilirdir (Schollmeier, 2001).

Eşler arası ağlarda katılımcılara ya da bilgisayarlara eşler denmektedir. Yukarıdaki tanımlara göre eşler arası ağlar tek bir bilgisayara sunucu görevi verilen ağlardan farklıdır. Eşten eşe ağa dahil olan tüm bilgisayarlar birbirine eşittir. Bütün bilgisayarlar ağ hizmetlerini sağlama yükümlülüğünü paylaşmaktadırlar. Eşler arası ağa bağlı bilgisayarlar hem sunucu hem de istemci konumundadır. Kaynaklarını erişime açan bilgisayarların kaynaklarına ulaşılabilir ve kullanılabilir.

Şekil 2.3.1.1’te görüldüğü gibi, sunucu tabanlı ağda her bilgisayar tek bir sunucuya doğrudan bağlıdır. Eşler arası ağda ise, her bilgisayar birbirine bağlıdır ve tek bir sunucu yoktur. Veri akışları eşler arasında gerçekleşmektedir.

Şekil 2.3.1.1. İstemci/Sunucu Ağ ve Eşler Arası Ağ



Kaynak: HAKAN, 2017: Blok Zinciri(Blockchain) Teknolojisine Giriş- 2, 27 Eylül 2017, (Çevrimiçi) <https://www.getrevue.co/profile/Hakan/issues/blok-zinciri-2-merkezi-olmayan-75090>, 20 Mart 2020.

2000’li yıllarda internetin de kullanımının yaygınlaşması ile eşler arası ağlar üzerinden dosya paylaşımı ve anında iletişim oldukça yaygın bir hale gelmiştir. Örneğin BitTorrent uygulamasının altında yatan eşten eşe ağ mimarisi ile birbirini tanımayan bilgisayarların internet üzerinde veri paylaşılması mümkün olmuştur. Buna karşın içeriğin şifrelenmemesi, verinin nerelerde saklanacağına dair seçenek sunmaması gibi nedenlerden dolayı, kurumsal veya mahremiyet içeren kişisel veriler için güvenli bir depolama çözümü olarak değerlendirilmemektedir (Usta ve Doğanekin, 2018:18). Bu sebeplerden dolayı eşler arası ağın şifreleme bilim ile daha güvenilir olacağı düşünülmekte ve dağıtık defter teknolojisinin de ortaya çıkmasına sebep olmaktadır.

Bitcoin, işlemleri izlemek, doğrulamak ve onaylamak ve para arzını yönetmek için merkezi bir parasal otoriteye güvenmek yerine, BitTorrent ve Skype’ı destekleyen ağlara benzeyen kullanıcıların makinelerinden oluşan eşler arası bir bilgisayar ağı tarafından etkinleştirilmektedir (Gupta, 2017:5). Blok zinciri teknolojisi, taraflar birbirlerine güvenmeseler bile katılımcılar arasında bir veri tabanını paylaşmak için bir yöntem sağlamakta ve merkezi bir otorite olmadan eşler arası bir ağı dayalı, varlıkları aktarmak için bir alan oluşturmaktadır. Blok zinciri, eşler arası ağdaki verilerin güvenli bir şekilde saklanamama sorununa kullanmış olduğu kriptografik algoritmalar ve mutabakat yapısı ile çözüm getirmektedir.

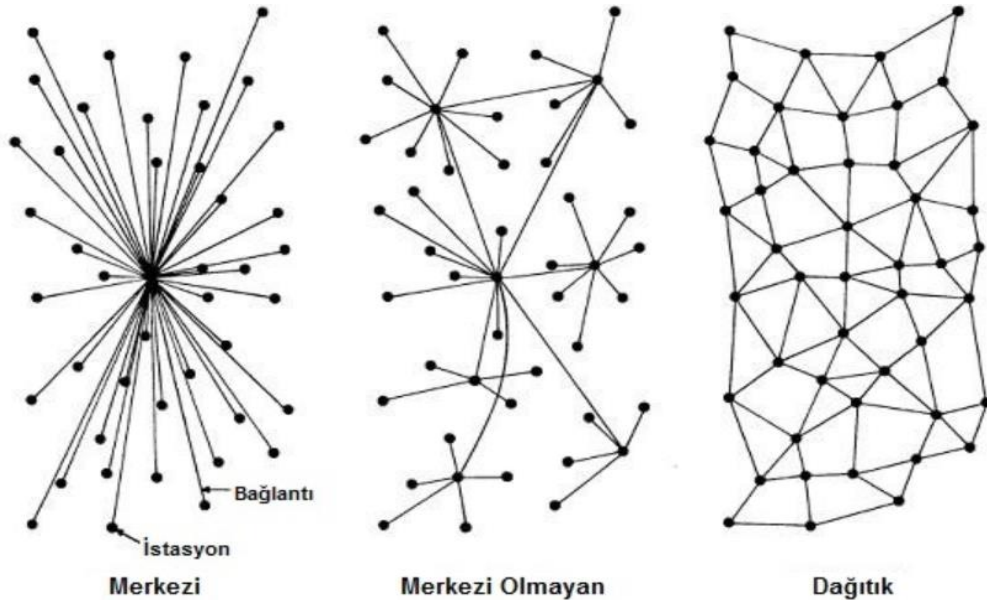
2.3.2. Dağıtık Defter Teknolojisi

Tezin birinci bölümünde bahsedildiği gibi, verilerin depolanma şekli zaman içerisinde, ihtiyaçlar doğrultusunda değişim göstermiştir. Blok zinciri gibi dağıtık defter teknolojisini kullanan yapılar, dağıtık ağ yapılarını benimsemiştir. Ancak blok zinciri teknolojisinde kullanılan dağıtık ağ yapılarını anlamak için ilk olarak merkezi ve merkezi olmayan ağlardan kısaca bahsetmek gerekmektedir.

Merkezi ağ yapılarında, adından da anlaşılacağı gibi veriler tek bir merkezde saklanmaktadır. Tüm yetkiler bu merkeze aittir. Bu tip ağlarda kontrol tek bir merkezde toplanmaktadır. Bu sebeple bu merkezde meydana gelen bir sorun tüm ağı etkilemektedir. Ağdaki bilgisayarlar birbiri ile direkt iletişim kuramamaktadır.

Merkezi olmayan ağ yapılarında merkezi yapılardan farklı olarak birden fazla merkez bulunmaktadır. Ancak bu ağ tipinde de merkezlerin mevcut olması ve verilerin yine bu merkezlerde saklanması, belirli sayıdaki merkezin zarar görmesi durumunda ağın genelinin ciddi bir zarara uğramasına sebep olmaktadır.

Şekil 2.3.2.1. Merkezi, Merkezi Olmayan ve Dağıtık Ağ Yapısı



Kaynak: BARAN, P.:1964, On distributed communications networks. *IEEE transactions on Communications Systems*, 12(1), 1-9.

Dağıtık ağ yapısı, merkezi ve merkezi olmayan ağ yapılarına göre hataya daha dayanıklıdır. Dağıtık ağ yapılarında, merkezi yapıların aksine ağdaki bir kişinin hata

yapması ağıdaki veri akışını bozmamaktadır. Tek kaynaktan saklanan verilerde, bilgisayara izinsiz giriş yapıldığında verinin kaybedilme olasılığı yüksektir. Ancak veri birden fazla yerde kaydedilmiş ise, verinin kaybolma olasılığı düşüktür. Dağıtık ağlarda ağıdaki risk ve kontrol ağı üzerinde tüm bilgisayarlara dağıtılmıştır. Bir dağıtık defter teknolojisi olan blok zincirinde kayıt altına alınan veriler artık tek bir merkezde değil, bu ağı dahil olan herkeste bulunmakta ve kayıt altına alınmaktadır.

Dağıtık Defter Teknolojisi (kısaca DDT) (Distributed Ledger Technology-DLT), her biri tam olarak aynı veri kayıtlarına sahip olan ve düğüm olarak adlandırılan bir dağıtık ağıdaki bilgisayar sunucuları tarafından toplu olarak tutulan ve kontrol edilen birden çok veri deposunda (defterde) veri kaydetmeye ve paylaşmaya yönelik yeni ve hızlı gelişen bir yaklaşımı ifade eder (Natarajan, Krause ve Gradstein, 2017). DDT, belirlenmiş prosedürler ve kurallar kullanılarak kuruluşların defterin tek bir kopyasına sahip olmaları için merkezi bir otoriteye güvenmek zorunda kalmadan işlem yapmalarını sağlar. DDT bir ağıdaki düğümlerin, ağına düğümlerine dağıtılan senkronize edilmiş bir deftere güvenli bir şekilde durum değişikliklerini (veya güncellemelerini) bildirmesini, doğrulamasını ve kaydetmesini sağlayan süreçleri ve ilgili teknolojileri ifade etmektedir (BIS, 2017).

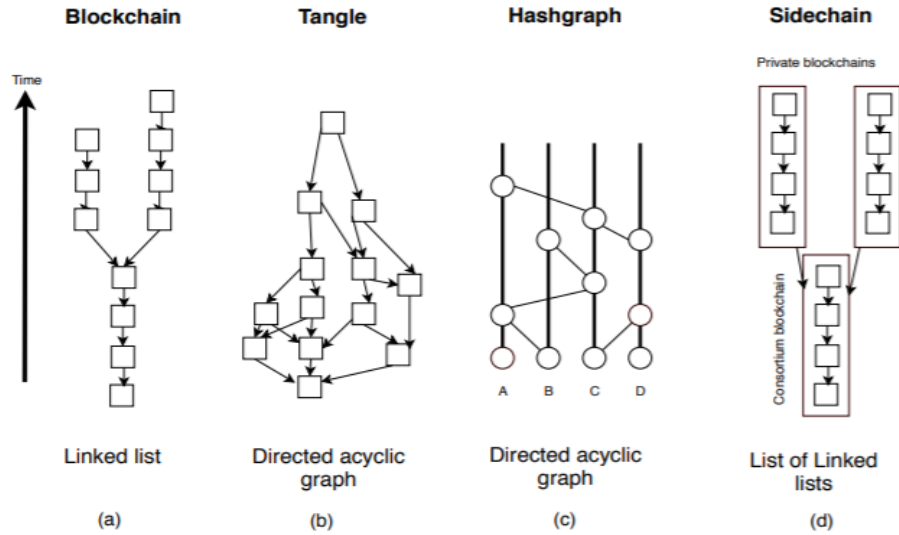
Dağıtık defter (distributed ledger) sistemi tek bir merkezi taraf yerine (banka gibi) bu sistemin tüm katılımcıları tarafından toplu olarak korunur. Bu sistemdeki her katılımcıya düğüm denmektedir. Düğümler, işlem kayıtlarının tam setini bulunduran her bir katılımcının bilgisayarını ifade etmektedir. Aynı deftere ait kopya, belirli bir taraf tarafından merkezi olarak kontrol edilmek ve yönetilmek yerine, her düğümde muhafaza edildiği ve geliştirildiği için sistem “dağıtık” bir defter sistemi olarak adlandırılmaktadır (Astri, 2016). Bir defter (ledger) işlevi gören ve DDT’nin bir türü olan blok zinciri, işlem blokları olarak adlandırılan bir zincir şeklinde sürekli büyüyen, sadece sondan eklenen (append only) bir veri yapısı oluşturmak ve işlemleri doğrulamak için kriptografik ve algoritmik yöntemler kullanmaktadır. Dağıtık defter teknolojisinde her bir bilgisayar ya da düğüm kayıtları kendisi tutmaktadır.

Blok zincirinde ağda bulunan kişilerde aynı defter bulunmaktadır. Ortak olan bu defterde yer alan kayıtlar değiştirilemez. Bu deftere (veri tabanına) yeni eklemeyi

ağdaki katılımcılar (düğümler) yapmaktadır. Düğümler tarafından işlemlerin kaydedilmesi ve bu işlemlerin doğruluğunun sağlanması süreci bu tezin mutabakat mekanizması ve algoritmaları ve kriptoloji bölümünde anlatılacaktır.

Dağıtık defter teknolojisinin çoğu zaman blok zinciri ile aynı olduğu düşünülmekte ve birbirinin yerine kullanılmaktadır. Blok zinciri bir dağıtık defter teknolojisi uygulaması olmakla birlikte, her dağıtık defter teknolojisini kullanan uygulama blok zinciri değildir. Şekil 2.3.2.2’de blok zinciri ile birlikte dağıtık defter teknolojilerini kullanan diğer uygulamalar gösterilmektedir. Bu uygulamalarda işlemler blok zincirinde olduğu gibi blokların içerisinde saklanmak zorunda değildirler.

Şekil 2.3.2.2. Mevcut Dağıtık Defter Teknolojisi Uygulamalarına Genel Bakış



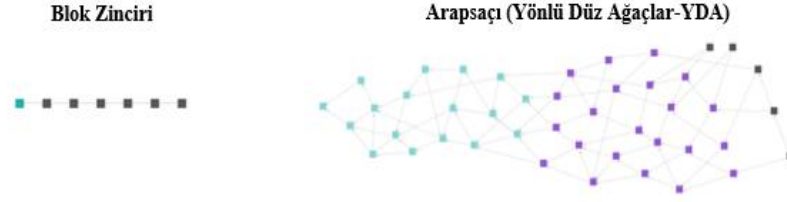
Kaynak: EL IOINI, N., PAHL, C.:2018.A review of distributed ledger technologies. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" (pp. 277-288). Springer, Cham.

Örneğin, IOTA¹ uygulamasında kullanılan Arapsaçı (Tangle) teknolojisi blok zincirindeki bloklar ve zincirlerden oluşmamaktadır. IOTA'nın dağıtık defteri olan Arapsaçı, blok zinciri yerine Yönlü Düz Ağaçlar (YDA) (Directed Arcylic Graph-

¹ IOTA, nesnelerin interneti (Internet of Things) ve kripto paralar arasındaki iletişim ve nesnelerin interneti cihazları arasında bir ödeme sistemi olarak tasarlanmıştır. Örneğin, bir buzdolabının içindeki yumurtaların belli bir sayının altına düşmesi halinde buzdolabının marketten kendi başına yumurta sipariş etmesi için bir ödeme sisteminin geliştirilmesi gerekmektedir. IOTA bu uygulamalardaki mikro ödemeler için geliştirilen bir proje ve aynı zamanda kripto para birimidir (Güven ve Şahinöz, 2018: 120-121).

DAG) altyapısını kullanmaktadır. Arapsacı’nda işlemler gruplanarak bloklar içinde ve sıralı zincirler halinde değil birbirine dolaşık bireysel işlemler akışı şeklinde kaydedilmektedir.

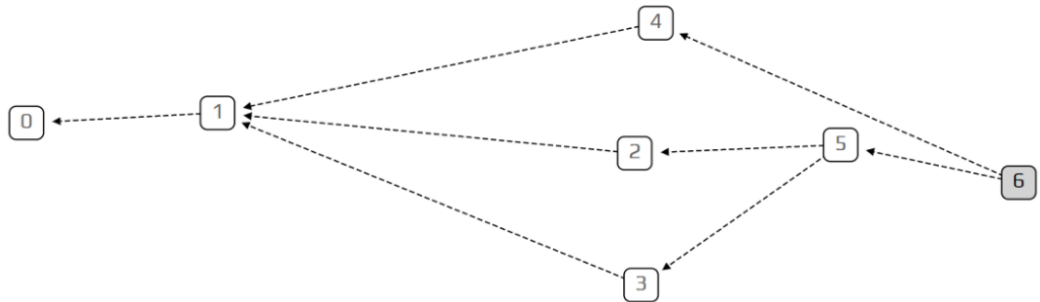
Şekil 2.3.2.3. Blok Zinciri ve Arapsacı Karşılaştırılması



Kaynak: IOTA, ERIŞİM TARİHİ: 10 MAYIS 2020. (Çevrimiçi) <https://www.iota.org/get-started/what-is-iota>, 10 Mayıs 2020.

Arapsacı uygulamasında yeni bir işlemin gerçekleşmesi için her işlemin kendisinden önce gelen 2 işlemi doğrulaması gerekmektedir. Örneğin şekil 2.3.2.4.’de görüldüğü gibi 5 numaralı işlemin arapsacı ağına dahil olabilmesi için 2 ve 3 numaralı işlemleri onaylaması gerekmektedir. Blok zincirinde ise tüm işlemler bütün kullanıcılar tarafından onaylanmakta ve kaydedilmektedir. Arapsacı uygulaması, tezin ilerleyen bölümlerinde blok zincirindeki risklerde bahsedilen enerji, ölçeklenebilirlik ve kuantum bilgisayarlar sorunu için bir alternatif olarak geliştirilmiştir (IOTA: erişim tarihi: 10 Mayıs 2020).

Şekil 2.3.2.4. Arapsacı Yapısında İşlemlerin Onaylanması



Kaynak: GAL, A.:2018.The Tangle: an Illustrated Introduction, Jan 31, 2018, (Çevrimiçi) <https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4>, 10 Mayıs 2020

DDT'lerin temel amaçlarından biri, birbirlerine güvenmesi gerekmeyen kullanıcıların güvenilir bir üçüncü tarafa ihtiyaç duymadan iletişim kurmalarına izin vermektir. Her bir DDT'nin kullandığı veri modelleri ve teknoloji farklılaşsa da DDT uygulamalarının sahip olduğu üç temel özellik vardır, bunlar **dağıtık eşler arası ağ, mutabakat mekanizmaları** ve **açık anahtar şifrelemesidir** (El Ioini ve Pahl, 2018:2).

2.3.3. Kriptoloji

Bilgi, günümüzdeki rekabet ortamında hem bireyler hem de kurumlar için gittikçe daha değerli ve önemli bir konu haline gelmiştir. İletişim teknikleri ve araçlarının gelişmesi ve değişmesi, bilginin saklanması ve iletilmesini zorlaştırmaktadır. Özellikle internet üzerinden yapılan alışverişlerin, internet bankacılığı kullanımının artması ve internet üzerinden haberleşme ve mesajlaşmanın kaçınılmaz olması internetin daha güvenli bir ortam olmasını zorunlu kılmıştır. Bu yüzden haberleşme ve bilişim teknolojisinin temel sorunu bilgi güvenliğidir. Bu bilgi ve haberleşme güvenliğini sağlayacak olan ise şifre bilimi yani kriptolojidir. Şifre bilim özellikle, tezin 1.4. bölümünde de bahsedilen, bilginin gizliliğini ve bütünlüğünü sağlamak amacı ile kullanılmaktadır.

2.3.3.1.Şifreleme

Kriptoloji, eski Yunancadaki kryptos (gizli saklı) ve logos (yazı, sözcük, bilim) kelimelerinden oluşmaktadır. Kriptolojinin temelinde zor matematik problemleri ve algoritmaları vardır. Kriptolojinin iki alt kolu bulunmaktadır. Bunlar kriptografi ve kriptanalizdir. Kriptografi en az iki tarafın güvenli bir şekilde bilgi alışverişi yapmasını sağlayan aynı zamanda paylaşılan bu bilgilerin istenmeyen kişiler tarafından anlaşılamayacak bir şekle dönüştürülmesinde kullanılmaktadır. Kriptografi gizlilik, bütünlük, kimlik denetimi, inkâr edememe gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemleri içermektedir (Akleyek, Yıldırım ve Tok, 2011).

Kriptolojinin diğer alt kolu ise kriptanalizdir. Kriptanaliz şifrelenmiş yani anlamsız metinden doğru metni bulma yöntemidir (Akleyek, Yıldırım ve Tok, 2011).

Şifrelenmiş metinlerin açık metin halini elde edebilmek için kullanılan gizli anahtarların tamamının veya belli bir kısmı elde edilmesi gerekmektedir.

Gönderilen mesajın şifrelenmemiş haline açık metin ya da düz metin (plaintext) denir. Gönderici tarafından alıcıya mesaj gönderilmek istenildiğinde bu mesaj üçüncü kişiler tarafından dinlenebilir veya değiştirebilir. Bu mesajın içeriğini üçüncü kişilerden saklamak amacı ile yapılan işleme şifreleme (encryption) denmektedir. Şifreleme, iletilen açık metnin içeriğinin üçüncü kişiler tarafından anlaşılamayacak hale getirilmesidir. Şifrelenmiş metnin tekrardan açık metne çevirme ya da anlaşılabilir hale getirme işlemine şifre çözümü (decryption) denmektedir. Şekil 2.3.3.1.1.'de şifreleme ve şifre çözme işlemleri gösterilmiştir.

Şekil 2.3.3.1.1. Şifreleme ve Şifre Çözme İşlemleri



Kaynak: KODAZ, H., BOTSALI, F. M.:2010. "Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması". Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu, Teknik - Online Dergi, 9(1), 10-23.

Şifrelenmiş bir mesajın güvenliği kadar şifrelenirken kullanılan yöntem ve tekniklerin gizliliğe de aynı derecede önemlidir (Yılmaz ve Ballı, 2016). Şifreleme işlemi şifrelenecek veri kümesi ve şifrelemede kullanılacak bir anahtar veri yapısı ile yapılmaktadır. Şifreleme yöntemleri istenmeyen kişiler tarafından öğrenilse bile, bu yöntemleri çalıştırmak için gerekli olan kelime/anahtar bilinmiyorsa mesaj çözülemeyecektir (Yılmaz ve Ballı, 2016). Sadece ilgili anahtara sahip olanlar mesajı orijinal haline dönüştürebilir, yani şifreyi çözebilirler (Usta ve Doğantekin, 2017).

Kullanılan anahtarların çeşidi ve özelliklerine göre temel olarak iki çeşit şifreleme vardır (İTÜBİDB, 2013). Bunlar simetrik ve asimetrik şifrelemedir.

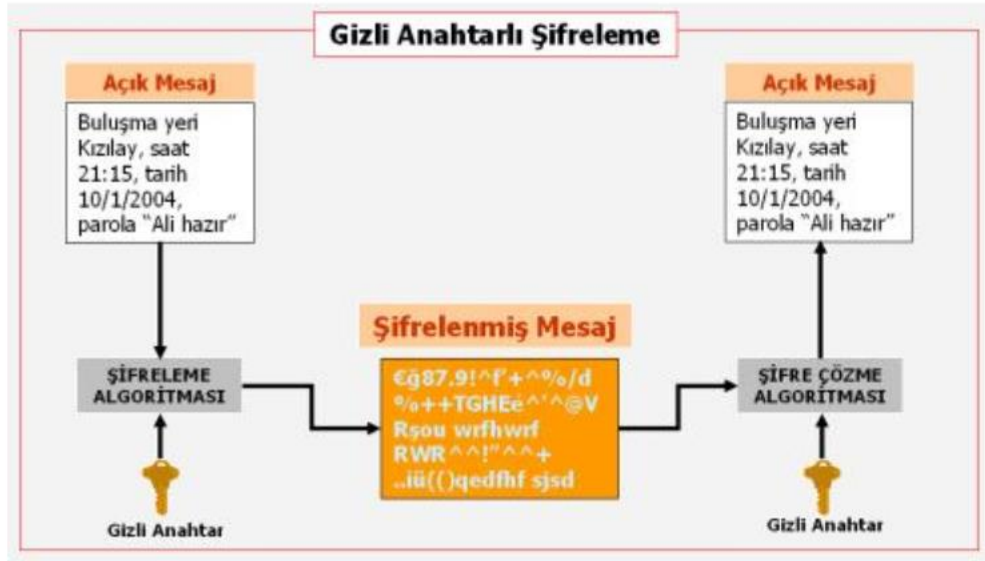
2.3.3.1.1. Simetrik Şifreleme

Simetrik şifreleme yönteminde mesajı gönderen taraf iletiyi şifrelerken, iletiyi alan tarafı ise şifreyi çözerken bir tane gizli anahtar kullanmaktadır. Yani hem bilginin şifreleme işlemi için hem de bilginin şifresinin çözülmesi işlemi için aynı anahtar

kullanılmaktadır. Simetrik şifreleme gizli anahtarlı şifreleme olarak da adlandırılmaktadır.

Kullanılan anahtar şifreleme yapan ile şifrelemeyi çözecek kişiler arasında anlaşılmalı ortak bir anahtardır ve başkalarından gizlidir (İTÜBİDB, 2013). Simetrik şifrelemede, şifreleme işlemi gerçekleştirildikten sonra şifreli metin alıcıya gönderilirken gizli anahtar da şifreli metinle birlikte alıcıya güvenli bir şekilde gönderilmesi gerekmektedir (Kodaz ve Botsalı, 2010). Hem şifreleme işleminde hem de şifreyi çözme işleminde aynı anahtar kullanıldığı için anahtarın sadece ilgili taraflar arasında paylaşılması gerekmektedir. Simetrik şifreleme Şekil 2.3.3.1.1.1.'de görüldüğü gibi tek bir gizli anahtar ile hem açık metin şifrelenmiş hem de mesajı alan kişi tarafından yine aynı gizli anahtarla şifre çözülmüştür.

Şekil 2.3.3.1.1.1. Simetrik Şifreleme



Kaynak: MGSCODE: 2016, Şifreleme Yöntemleri, 18 Haziran, 2016, (Çevrimiçi)
<https://mgscodet.blogspot.com/2016/06/sifreleme-yontemleri.html>, 3 Ocak 20200

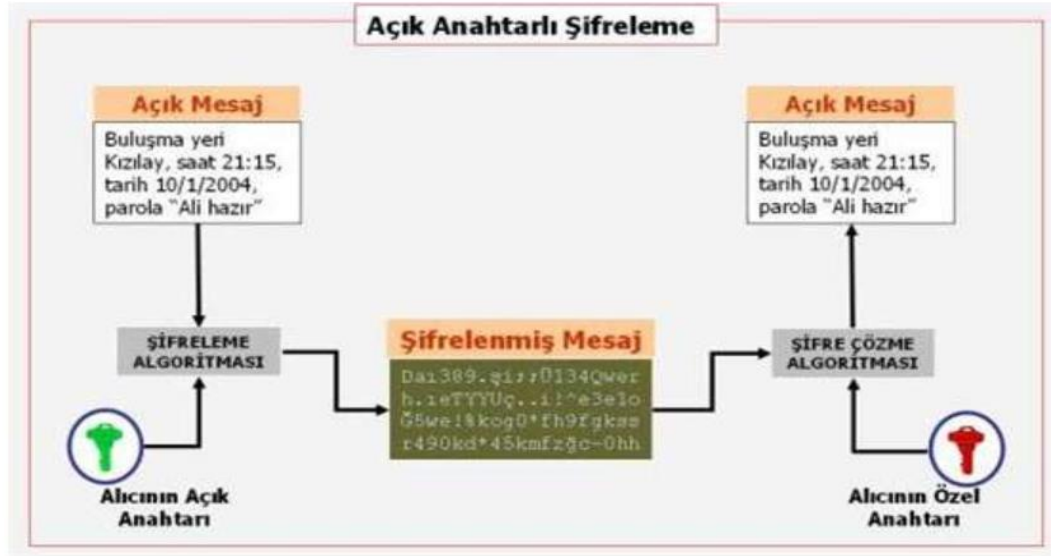
2.3.3.1.2. Asimetrik Şifreleme

Asimetrik şifreleme yönteminde iletiyi şifrelemek için kullanılan anahtar ile şifreyi çözmek için kullanılan anahtar birbirinden farklıdır. Asimetrik şifreleme literatürde açık anahtar şifrelemesi olarak da bilinmektedir. Bu yöntemde bir özel bir de açık olmak üzere her bir kullanıcının bir anahtar çifti vardır. Açık anahtar (public key) herkese dağıtılabılırken özel anahtar (private key) sadece ona sahip kişide kalır.

Açık anahtar iletilerin şifrlenmesinde kullanılırken, özel anahtar şifreyi çözmede kullanılmaktadır.

Şekil 2.3.3.1.2.1’de görüldüğü gibi asimetrik şifrelemede kullanıcının bir tane açık anahtarı bir tanede gizli anahtarı bulunmaktadır. Gönderilmek istenen mesaj alıcının açık anahtarı ile şifrlenir. Alıcı sadece kendisinde olan özel anahtarı ile şifreyi çözüp mesajı okuyabilmektedir. Mesaj şifrlenirken kullanılan anahtar mesaj çözülürken kullanılamaz. Şifrelenmiş ileti başka kişiler tarafından ele geçirilse bile özel anahtar sadece alıcı tarafından bilindiği için şifrelenmiş iletinin çözülüp, orijinal veriye ulaşılması mümkün değildir. Asimetrik şifreleme, simetrik şifrelemeye göre daha güvenlidir (Yılmaz ve Ballı, 2016: 20)

Şekil 2.3.3.1.2.1. Asimetrik Şifreleme



Kaynak: MGSCODE: 2016, Şifreleme Yöntemleri, 18 Haziran, 2016, (Çevrimiçi)
<https://mgscode.blogspot.com/2016/06/sifreleme-yontemleri.html>, 3 Ocak 2020

Blok zinciri teknolojisinde asimetrik şifreleme kullanılmaktadır. Bu yöntem blok zinciri teknolojisinde işlemlerin özel anahtar ile imzalanması, hesap adreslerinin açık anahtar olarak kullanımı, özel anahtar ile imzalanmış işlemlerin açık anahtarla doğrulanması gibi işlemlerde kullanılmaktadır.

2.3.3.2.Özetleme Fonksiyonu

Blok zinciri teknolojisinde kullanılan ve İngilizcede Hash Function olarak geçen terim Türkçede Özetleme ya da Özet Fonksiyonu olarak kullanılmaktadır.

Özetleme fonksiyonları şifreleme biliminde sıklıkla kullanılan matematik formülleridir. Bu fonksiyonların amacı veri güvenliğini sağlaması ve veri bütünlüğünü korumasıdır. Özetleme fonksiyonları çok uzun olan verilerin özet halini oluştururlar. Özetleme fonksiyonları farklı uzunluktaki dijital mesajlardan, sabit uzunlukta bir mesaj özet bilgi çıkarırlar. Bu özet bilgi genellikle “hash” veya “hash digest” olarak adlandırılmaktadır.

Şifreleme biliminde en fazla kullanılan özetleme fonksiyonları MD5 (Message Digest) ve SHA fonksiyonlarıdır. Kısaltması SHA olan Secure Hash Algorithm, Türkçede Güvenli Özetleme Algoritması olarak kullanılmaktadır. Üç çeşit SHA vardır: SHA-0, SHA-1 ve SHA-2. Bunlar birbirinin devamı olan sürümlerdir. Bitcoin üretiminde ise SHA-256 özetleme fonksiyonu kullanılmaktadır. Ancak neden SHA fonksiyonunun kullanıldığını anlamak için MD ve SHA fonksiyonları arasındaki temel fark kısaca Tablo 2.3.3.2.1.’de gösterilmiştir.

Tablo 2.3.3.2.1. Özetleme Fonksiyonları ve Üretilen Toplam Özetleme Sayısı

Özetleme Fonksiyonu	Çıktı Uzunluğu	Üretilen Özetleme Sayısı
MD5	128 bit	2^{128}
SHA1	160 bit	2^{160}
SHA2	256 bit	2^{256}

Tablo 2.3.3.2.1.’de özetleme fonksiyonları sonucunda ortaya çıkan sabit özetleme değerlerinin uzunluğu ve her bir özetleme fonksiyonu için ortaya çıkabilecek birbirinden farklı özetleme değerlerin sayısı verilmiştir. Bir bit değerinde, 0 ve 1 olmak üzere iki olası değer bulunmaktadır. Benzersiz özetleme değerlerinin sayısı da, olası değerlerin bit haliyle ölçülmektedir (Cheapssl, 2017). Bu durumda SHA-256 için 2^{256} farklı olasılık bulunmaktadır. Yani, SHA-256 fonksiyonuyla 2^{256} tane benzersiz özetleme değeri üretebilmektedir.

Özetleme fonksiyonlarında farklı girdiler aynı çıktıyı üretmemelidir. Eğer, özetleme fonksiyonun sonucunda ortaya çıkan özetleme değerleri aynı ise buna *çarpışma* denmektedir ve bu istenmeyen bir durumdur. Özetleme fonksiyonları ne kadar farklı olasılıkta özetleme değeri verebiliyorsa çarpışma olma olasılığı o kadar düşük olur, özetleme fonksiyonun güvenilirliği de aynı oranda yüksek olur. SHA-256

algoritmasından özet bir değer üretmek, 1 ile 2^{256} arasında rastgele bir tam sayı üretmek olarak da görülmektedir (Çarkacıoğlu, 2016). 2^{256} yaklaşık olarak 1.15×10^{77} 'ye eşittir. Teoride aynı çıktının üretilmesi mümkün olsa da, gözlemlenebilir evrendeki atom sayısı yaklaşık olarak 10^{80} oluğu düşünüldüğü için, bu ihtimal göz ardı edilebilir olarak kabul görülmüştür (Usta ve Doğanekin, 2018:113). Bu durum SHA-256 fonksiyonunun ne kadar güvenilir olduğunu açıklamaktadır.

Verinin büyüklüğü ne olursa olsun özetleme fonksiyonu kullanıldığında çıkacak olan özetleme değerinin büyüklüğü her zaman sabittir. SHA-256 fonksiyonundan çıkan özetleme değer 256 bit uzunluğundadır.

Güvenli özetleme algoritmasında, her bir girdi için birbirinden farklı çıktılar üretilmelidir. Aynı girdi de her zaman aynı çıktıyı (özeti) üretmelidir. Şekil 2.3.3.2.1.'de, aynı kelimenin sadece ilk harfi büyük harfle yazıldığında tamamen farklı bir özet oluşmuştur. Her "Serkan" yazıldığında ise verinin özeti her zaman "508B4498D3A57B759CC171A541CA4F2BBB2DC2B18442665E5EE1E50AF37F7F7A" olmalıdır.

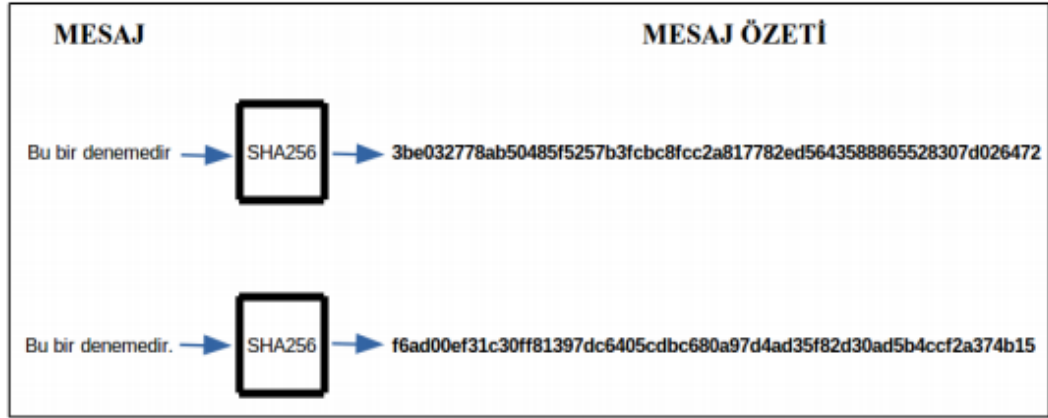
Şekil 2.3.3.2.1. Verinin SHA-256 Karşılığı Örneği

Örnek Veri	SHA-256 Karşılığı (okunabilirlik açısından 16'lık sayı düzeninde gösterilmiştir)
erkan	A7C3962E7BD1F5C65FDD9D97CC993B231CFF60C8296E D9F9590EAD5B0813D1D0
serkan	37B081FA6506D4B937F5A9EB893B45823BDBA49 D5DF840B24AF4122BA29E540D
Serkan	508B4498D3A57B759CC171A541CA4F2BBB2DC2B18442665E 5EE1E50AF37F7F7A

Kaynak: USTA, A., DOĞANTEKİN, S.:2018, Blockchain 101 v2. *Bankalararası Kart Merkezi*, s.113.

Şekil 2.3.3.2.2.'de ise ikinci mesaja, birinci mesajdan farklı olarak nokta ilave edilmiştir ve görüldüğü üzere mesajda ya da girdi üzerinde yapılan ufak bir değişiklik özetleme değerini yani çıktıyı tamamen değiştirmektedir.

Şekil 2.3.3.2.2. SHA-256 Özet Fonksiyonu Örneği



Kaynak: ÇARKACIOĞLU, A.:2016.Kripto-Para Bitcoin. Sermaye Piyasası Kurulu Araştırma Dairesi Araştırma Raporu.,3 Nisan 2020, syf.21

Kısaca özetleme fonksiyonlarının sahip olması beklenen 5 temel özelliği vardır (Güven ve Şahinöz, 2018:50):

1. Aynı girdi her zamana aynı çıktıyı üretmeli
2. Fonksiyon çok hızlı çıktı üretmeli
3. Çıktıyı kullanarak girdiyi hesaplamak mümkün olmamalı
4. Mesajdaki, girdideki ufak bir değişiklik bile çok farklı özetleme değeri üretebilmeli
5. Farklı girdiler aynı sonucu üretmemeli

Blok zincirinde depolanan veriler kriptografik özetleme değerleri ile korunmaktadır. Özetleme değeri alınmış bir veri, verinin doğruluğunu onaylayan bir parmak izine benzetilebilmektedir. Orijinal verilerin değiştirilmesi, değiştirilen verilerin özetleme değerinin artık orijinal parmak izi ile eşleşmemesine sebep olmaktadır (Beck, 2018).

Özetleme fonksiyonları, mesaj doğrulama kodu, parolaların saklanması, verilerin bütünlüğü ve gizliliğinin korunması ve özellikle dijital imzalar kimlik doğrulaması için iletilen mesajın bütünlüğünü kontrol etmek için sıklıkla kullanılmaktadırlar.

2.3.3.3.Dijital İmza

Islak imzalar ile imzalanan belgeler, belgenin imzalayan kişi tarafından oluşturulduğunu, imzalayan kişinin kimliğini, imzalayan kişi tarafından belgenin

içinde yazılanların kabul edildiğini, belgenin bu şekilde doğru ve gerçeği yansıttığını ifade etmektedir. Dijital imzalar da ıslak imzalar ile aynı amacı taşımaktadır.

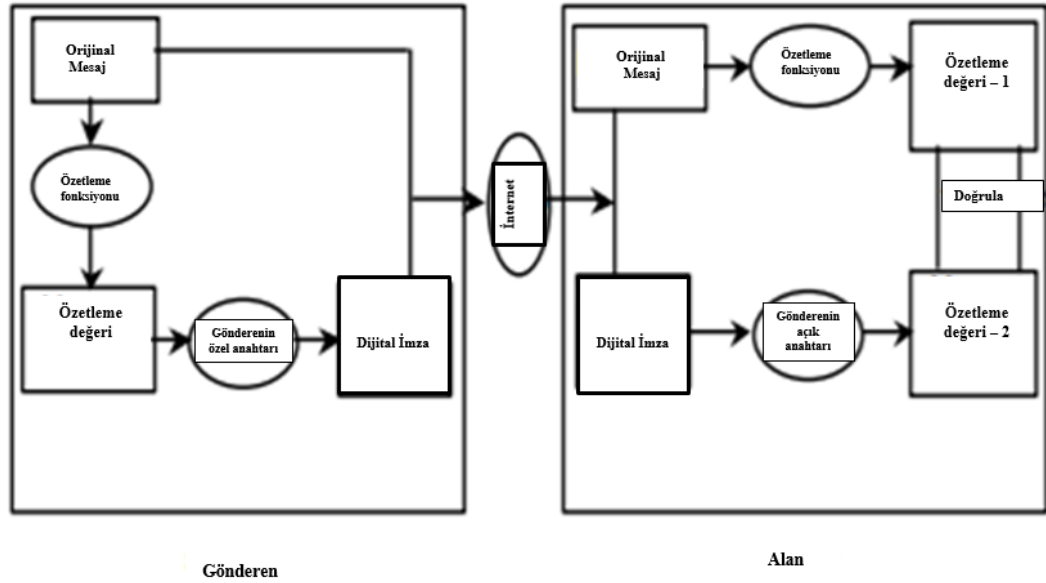
Dijital imzalara duyulan ihtiyaç ve dijital imzaların özellikleri aşağıdaki gibi sıralanabilir (Altundağ, 2006):

- İletilecek bilgi, veri veya mesajın içeriği istenmeyen kişiler tarafından öğrenilmesini önlemek. Diğer bir ifade ile iletilen mesajın gizliliğini korumak.
- İletilen bilgi/verilerin istenmeyen kişiler tarafından değiştirilmesi ve bilgi/verilerin gideceği yere varıncaya kadar yolda değiştirilmemesi ve bozulmamasını önlemek. Mesajın içeriğini korumak.
- İnternet ortamında yapılan işlemlerde, tarafların kimliklerini güvenli bir şekilde doğrulayamamasının önüne geçmek. Dijital imza, bilginin/verinin istenen alıcıya gittiğini ve alıcı tarafından okunabileceğine güvence verir.
- İşlemi yapan tarafın ile mesajı alan tarafın işlemi inkâr edememesi, inkâr etmesi halinde ispat aracı olarak kullanılması sağlanır.

Dijital imzalarda asimetrik şifreleme yönetimi kullanılmakta ve dijital imzalar kriptografik algoritmalar kullanılarak oluşturulmaktadır. Dijital imzalarla mesajı imzalamadan önce mesaja kriptografik özetleme fonksiyonları uygulanır. Uygulanan bu fonksiyondan bir özetleme değeri elde edilir. Bu özetleme değeri daha sonra özel anahtar kullanılarak şifrelenir ve dijital imza oluşur.

Islak imzalarda imza belgeden bağımsızdır. Farklı belgeler imzalanırken ıslak imza hep aynı kalır ve değişiklik göstermez. Dijital imza ise imzalanan belge ile ilişkilidir. Belgedeki metnin değişmesi halinde farklı bir dijital imza oluşur. Dijital imzalar, imzalama ve doğrulama sürecinden oluşmaktadır. Şekil 2.3.3.3.1. dijital imzalama örneği anlatılmıştır.

Şekil 2.3.3.3.1. Dijital İmza Algoritması



Kaynak: ZHU, H., LI, D.:2008. Research on Digital Signature in Electronic Commerce. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1).

İki kişi arasında bir mesaj göndermektedir. Mesajı göndermek isteyen kişinin bir anahtar çifti vardır: özel ve açık anahtar. Mesajı gönderecek olan kişi özel anahtarı kendinde saklar ve açık anahtar bilgisini mesajı alacak olan taraf ile paylaşır. Mesaj hazırlanır ve bir özetleme algoritması uygulanarak mesajın özetleme değeri elde edilir. Gönderenin özel anahtarı ile özetleme değeri şifrelenir ve dijital imza oluşur. Bu şifre gönderilecek mesaja eklenir. Şifrelenmiş mesaj (dijital imzalı) mesajın orijinali ile birlikte alıcıya gönderilir. Doğrulama sürecinde ise; alıcı mesajı gönderen kişinin açık anahtarı ile şifreyi çözer ve mesajın özetleme değerini elde eder. Aynı zamanda alıcı orijinal mesajın tekrardan özetleme değerini alır. Elde edilen bu iki özetleme değeri karşılaştırılır. Eğer bu iki özetleme değeri aynı ise mesajın ve imzanın doğruluğu ispatlanmış olur. Eğer özetleme değerleri aynı çıkmaz ise ya mesajı imzalayan kişi farklıdır ya da mesajın içindeki bilgiler değiştirilmiştir.

Örnekte de görüldüğü üzere geçerli bir dijital imza, mesajı alan tarafa mesajın iddia edilen kaynaktan/kişiden geldiğini, mesajı gönderen kişinin mesajı gönderdiğini reddetmesine imkân vermemekte ve mesajın yolda değiştirilmediğini doğrulamaktadır.

Dijital imza, blok zinciri üzerinden gönderilen ve kaydedilen verilerin güvenliğini sağlamanın yöntemlerinden biridir. Dijital imzalar kullanılarak sadece verinin bütünlüğü değil mesajı gönderenin kimliği de doğrulanmaktadır. Blok zinciri teknolojisi kimlik tanımlaması, verinin bütünlüğü ve inkâr edememe problemlerine dijital imzaları kullanarak çözüm getirmiştir (Di Pierro, 2017). Dijital olarak imzalanan bilgiler blok zinciri ağındaki tüm kullanıcılara yayınlanmakta ve bilgiler açık anahtarlar ile ağıdaki herkes tarafından görülebilmektedir.

2.3.4. Mutabakat Mekanizması ve Algoritmaları

Blok zinciri gibi dağıtık bir ağda fikir birliğine varmak zordur. Dağıtık sistemler veya birbirinden bağımsız çalışan sistemler arasındaki ilişkilere, çıkar çatışmalarına ve mutabakata varılmasının zorluğuna Bizanslı Generaller Problemi denmektedir. Bizanslı Generaller Problemi ilk kez 1982 yılında L.Lamport, R.Shostak ve M.Pease tarafından yazılmış ve bu durum Bizanslı generallerin bir şehri kuşatma planı örnek vererek açıklanmıştır. Bizanslı generaller bir şehri kuşatmak için hazırdır ve her general ordunun bir kısmını kontrol etmektedir. Generaller ya şehre saldıracaklar ya da geri çekileceklerdir. Ortak bir karara vardıkları müddetçe saldırmaları ya da geri çekilmeleri önemli değildir. Burada önemli olan ordudaki generallerin vereceği karardır. Tüm generaller aynı kararı almalıdır. Ancak generaller birbirlerini görmemekte ve ulaklar aracılığı ile birbirlerine haber yollamaktadır. Mesajlar yolda gecikebilir, bazı ulaklar yolda mesajı değiştirebilir, ihanet edebilirler ya da yolda giderken ölebilirler. Ulaklar tarafından mesaj başarılı bir şekilde generallere iletilmiş olsa bile generallerin arasında hain biri olup olmadığı da kesin değildir. Saldırının gerçekleşmesi için herkesin aynı kararı alması ve toplu bir şekilde hareket edilmesi gerekmektedir. Generaller arasında mutabakata varılamaması ve herkesin aynı kararı almamasının sonucu, topluca geri çekilmekten daha kötü olabilir. Ayrıca ordudaki yapının tüm generallere eşit mesafede olduğu da kesin değildir.

Burada generallerin bir sonraki hamlesinde alacakları kararlar konusunda bir iletişim sorunundan bahsedilmiş ve birbirini görmeyen ve güvenmeyen kişiler arasında nasıl fikir birliğine varılabilir konusu tartışılmıştır. Bizanslı Generaller Problemini çözmek için ise Bizans Hata Toleransı sistemleri kullanılmıştır. Bizans hata toleransı

Bizans generalleri problemindeki hatalara karşı dayanıklı olan sistemlerin özelliğidir. Bizans hata toleransı bir ağdaki bazı düğümler arasında iletişim sağlanamasa ya da bazı düğümler kötü niyetli davranışlar bile sistemin çalışmaya devam etmesidir. Böylece bir ağda kötü niyetli düğümlerin bulunması durumunda bile blok zincirin çalışması ve verilerden oluşan blokların doğrulanabilmesi mümkün de olmaktadır.

Bizanslı generaller probleminde anlatılmak istenen ilk olarak merkezi otorite olmayan bir toplumun üyelerinin ortak bir noktada buluşabilmeleri, ikincisi kötü niyetli kişilere rağmen uzlaşma sağlanabilmesi, üçüncüsü bir ya da birkaç kişi hata verdiğinde bile sistemin aksaklık olmadan çalışmaya devam edebilmesidir (Güven ve Şahinöz, 2018). Sistemin hata toleransı olmalı ve doğru ya da doğruya yakın sonuçlar verebilmelidir.

Generaller blok zinciri üzerindeki düğümlere benzetilebilirler. Blok zincirinde blok oluşturmak için düğümlerin çoğunluğunun ortak bir karar vermesi gerekmekte ve dağıtık ağdaki düğümlerin çoğunluğunun hatalardan kaçınmak için aynı şeyi yapmaları gerekmektedir. Bu durum blok zincirindeki mutabakat algoritmalarına götürmektedir.

Blok zincirinde birbirini tanımayan ve birbirinden uzakta olan düğümlerin ya da bilgisayarların aynı deftere sahip olabilmesi, sistemin bütünlüğünün korunması, kayıtlarda tutarlılık olması ve herkesin ortak bir noktada anlaşmaya varabilmesi için belli kurallara uyulan bir yapı gerekmektedir. Belirlenen kurallar çerçevesinde veriler blok zinciri ağına kaydedilmektedir. Ağın geneli tarafından kabul edilen bu kuralları sağlama, kuralların uygunluğunun kabul edilmesi ve fikir birliğine varma işine mutabakat denilmektedir (Usta ve Doğantekin, 2017:45). Ağ üzerindeki herkesin aynı deftere sahip olabilmesi için ağ genelinde mutabakat yapılması şarttır. Bu kurallar genel olarak blokların zincire nasıl ve ne zaman ekleneceğine ilişkin kurallardır.

Blok zincirinde güveni sağlayan şey kriptoloji ve en başta belirlenen mutabakatı sağlayacak olan kurallardır. Sonraki aşamada ise mutabakat sürecinde bu kurallar çerçevesinde üretilen blokların zincirdeki herkese dağıtılmasıdır.

Fikir birliğini sağlamak dağıtık bir sisteme sahip olan blok zinciri teknolojisinde zordur. Blok zincirinde bu fikir birliğini sağlamak ve düğümlerin

güvenli bir şekilde eş zamanlı çalışması için mutabakat algoritmaları kullanılmaktadır. Farklı blok zinciri platformları farklı mutabakat yaklaşımları benimsemiştir. Kullanılan mutabakat algoritmaları farklı olsa da, algoritmaların amacı aynıdır, ağdaki bilgisayarların işlemlerin doğrulanmasındaki yetki dağılımı ve ödüllendirmesi farklılık göstermektedir. En çok kullanılan mutabakat algoritmaları ise İş İspatı ve İş Payı'dır.

2.3.4.1. İş İspatı (Proof of Work –PoW)

Proof of Work (PoW) Türkçede iş ispatı, iş kanıtı, emek kanıtı gibi isimlerle de kullanılmaktadır. Bir bilgisayarın bir iş için çalıştığının kanıtlanmasında kullanılan iş ispatı algoritması, ilk olarak 1997 yılında Adam Back tarafından spam e-postalar ve DoS saldırılarının önüne geçmek için kullanıldığı tezin 2.1. Blok Zinciri Teknolojisinin Tarihsel Gelişimi bölümünde bahsedilmiştir. Örneğin; bilgisayarlar e-posta atmak gibi birçok işlemi çok hızlı bir şekilde yapabilirler. Ancak bu hız milyonlarca e-postanın aynı anda atılmasını da mümkün kılmaktadır. Bunu engellemek için, e-posta sunucusu, e-posta atan bilgisayardan, biraz çalışmasını ve bunu ispatlamasını isteyebilir (Çarkacıoğlu, 2016). Böylelikle e-posta atmak isteyen bilgisayarın milyonlarca e-posta atması engellenmiş ve çalışarak sadece birkaç e-posta atabilecek kadar zaman bulması sağlanmıştır.

İş ispatı algoritması Bitcoin blok zincirinde kullanılmaktadır. Burada mutabakat süreci ve blok üretimi madencilik (mining) olarak adlandırılmaktadır. Blok üretimi yapan veya blok eklemek için çalışan kişilere de madenci (miner) denmektedir. Burada da amaçlanan, tıpkı e-posta örneğinde olduğu gibi, madencilerin üst üste sürekli blok oluşturmalarına engel olmaktır. Madencilerin zincire blok ekleyebilmeleri için bir matematik problemi (mathematical puzzle) çözmeleri gerekmektedir. Bu problemi çözen ilk madenci bloğu zincire ekleme hakkını elde eder ve problemi en hızlı çözen bu madenciye ödül verilmektedir. Yani madencilerin birbirleri ile yarışarak iş ispatı yapması beklenmektedir. Bu mutabakat algoritmaları blok üretimlerinin belirli aralıklarla yapılmasını sağlamak amacıyla uygulanmaktadır. Aksi takdirde madenciler her saniyede onlarca blok üretecek ve zincirin tek olması mümkün olmayacaktır (Güven ve Şahinöz, 2018).

İş ispatı mutabakat algoritmasında madencilerin problemleri çözebilmesi için çok kısa bir sürede çok fazla deneme yapmaları gerekmektedir, bu durum çok yüksek miktarda enerji tüketimine sebep olmaktadır. Bitcoin blok zinciri ağında yeni blokların eklenmesi için madenciler tarafından harcanan işlem gücünün tükettiği elektrik, dünya üzerindeki bazı ülkelerin tükettiği elektrik miktarını geçmektedir. 2014 yılındaki bir çalışmada tüm Bitcoin ağında harcanan elektriğin İrlanda'daki elektrik tüketimine eşit olduğu tahmin edilmektedir (O'Dwyer ve Malone, 2014).

2.3.4.2.İş Payı (Proof of Stake-PoS)

İş payı algoritmasında Türkçede hisse kanıtı olarak da isimlendirilmekte İngilizcede ise Proof of Stake olarak kullanılmaktadır. Bu mutabakat algoritmasında amaç iş ispatı algoritmasında olduğu gibi işlemleri onaylamak ve mutabakatı sağlamak olmakla beraber, burada süreç farklı çalışmaktadır. Amaca ulaşma yöntemi ve hedefe ulaşırken harcanan süre farklıdır.

Bu yöntemde blokların üretimi sırasında bir matematik problemi çözülmesi gerekmemektedir. Blokları zincire ekleme olasılığı, blok zinciri ağı üzerinde sahip olunan pay ile ilişkilidir. Burada sahip olunan pay kişinin ilgili kripto paraya sahip olduğu miktar ile doğru orantılıdır. Örneğin bir kişinin 10 başka bir kişinin ise 50 adet kripto parası varsa, 50 kripto parası olan kişinin bir sonraki bloğu doğrulayan kişi olarak seçilme olasılığı beş kat daha fazla olacaktır (Schumann, 2018). Daha fazla parası olan kişilerin ağa saldırma olasılığının az olduğu düşüncesi vardır (Fernández-València, Caubet ve Vila, 2018). Bu sistemlerde sistem içerisinde üretilebilecek maksimum kripto para miktarı en başta üretilmekte, sistemdeki kullanıcılar yatırımlarına göre paylarına düşen kripto parayı almakta ve sonradan ekleme yapılamamaktadır (Usta ve Doğantekin, 2018:123).

İş ispatı algoritmasında madenci olarak isimlendirilen kişiler burada forger olarak tanımlanmıştır. Bu yaklaşımda blok üretimi sürecine madencilik yerine para basma (minting veya forging) denmektedir.

Burada iş ispatı yönteminde olduğu gibi gelişmiş bilgisayarlara ihtiyaç olmadığı için iş ispatı yönteminde göre çok daha az enerji tüketilmektedir. Bitcoin'den

sonra dünyanın en büyük ikinci kripto parasına sahip olan Ethereum platformu 2018 yılında İş İspatı yöntemini bırakıp iş payı yönteminde geçmiştir.

2.3.5. Blok ve Blok Yapısı

Değer içeren her türlü veri, varlık ve işlemlerin kaydedildiği yapılara “blok” denmektedir. Bu değerlerin ve işlemlerin kaydedildiği bloklar, zincirin esas parçasını oluşturmaktadırlar. Her bir blok kendisinden önce gelen blokların özetini içermektedir. Böylelikle bir zincirin halkası gibi bloklar birbirine bağlanmaktadır. Blok zinciri kavramı ve benzetmesi de buradan gelmektedir.

Blok zincirindeki ilk bloğa *Başlangıç Bloğu (Genesis Block)* denmektedir. Herhangi bir bloktan geriye doğru gitmek istenirse, ulaşılacak en son blok bu başlangıç bloğu olacaktır. Bu başlangıç bloğu ilk olarak 2009 yılında bitcoinin ortaya çıkışıyla üretilmiştir.

Tablo 2.3.5.1’de görüldüğü gibi bir blok, blok boyutu, blok başlığı, işlem sayacı ve işlemler olmak üzere 4 alandan meydana gelmektedir (Antonopoulos, 2014).

Tablo 2.3.5.1. Blok Yapısı

Boyut	Alan	Tanım
4 Byte	Boyutu	Bir bloğun byte cinsinden büyüklüğünü gösterir
80 Byte	Başlık	Çeşitli alanlardan oluşmaktadır (aşağıda anlatılacaktır)
1-9 Byte	İşlem Sayacı	Kaç tane işlem olduğunu gösterir.
Değişir	İşlemler	Kaydedilen tüm işlemleri ifade eder.

Kaynak: ANTONOPOULOS, A. M.:2014, Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc."

2.3.5.1.Blok Boyutu

Bir bloğun tamamının boyutunun ne kadar ya da diğer bir ifadeyle kaç byte olduğunu göstermektedir.

2.3.5.2.Blok Başlığı

Blok başlığı 6 alandan oluşmaktadır (Antonopoulos, 2014). Bunlar Tablo 2.3.5.2.1.’de gösterilmiştir.

Tablo 2.3.5.2.1. Blok Başlığı

Boyut	Alan	Tanım
4 Byte	Sürüm	Blok sürüm numarası
32 Byte	Önceki Blok Özeti	Bir önceki blokun özet değeri
32 Byte	Merkle Kökü Özeti	Bloktaki yer alan tüm işlemlerin merkle ağacı özet değeri
4 Byte	Zaman Damgası	Bloğun oluşma zamanı
4 Byte	Zorluk Hedefi	İş ispatında hedeflenen zorluk derecesi
4 Byte	Nonce	İş ispatı yapılmasında kullanılan sayaç

Kaynak: ANTONOPOULOS, A. M.:2014. Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc."

2.3.5.2.1. Sürüm

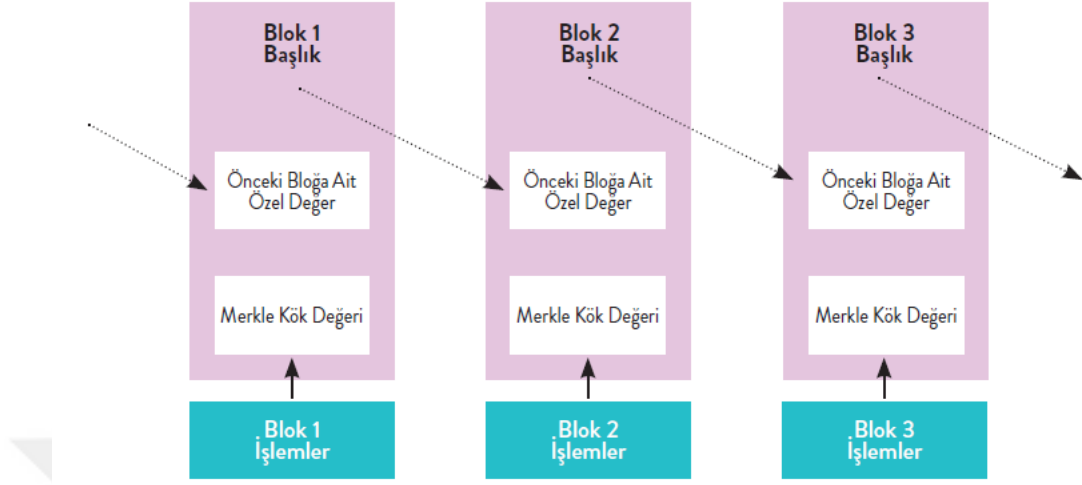
Bir blok oluşturulurken uyulması gereken kurallar vardır. Bu kurallar bloğun yapısını, uzunluğunu, kayıtların şeklini, alanların sırasını gibi uyulması gereken kurallardır (Güven ve Şahinöz, 2018). Bu kurallar zaman içinde değiştirilebilmektedir. Bu kural değişikliğinin zincirin en başından ya da ilgili bloktan sonra geçerli olup olmayacağı sürüm numarasına göre uygulanır. Güncellemelerin takip edilmesini sağlamaktadır.

2.3.5.2.2. Önceki Blok Özet Değeri

Her bir blok kendinden önceki bloğun özet değerini içermektedir. Bu sayede bloklar birbirine bağlanmış olmaktadır. Blokların birbirlerine zincir şeklinde bağlanmasını sağlayan blok başlığında yer alan bu önceki blok özet değeridir.

Bir blokta, hem mevcut bloğun kendi verileri hem de kendinden önce yer alan bloğun özet bilgileri yer almaktadır. Şekil 2.3.5.2.2.1.'e bakıldığında, 3.blok hem kendi verilerini hem de 2.bloğun özet verilerini, 2. blok hem kendi verilerini hem de 1.bloğun özet verilerini içermektedir. Bu yapı bu şekilde devam etmekte ve bloklar bu yapı ile birbirine bağlanmaktadır. Sadece başlangıç blok kendi verilerini içermektedir.

Şekil:2.3.5.2.2.1. Blok Zinciri Yapısı



Kaynak: USTA, A.,DOĞANTEKİN, S.:2018. Blockchain 101 v2. *Bankalararası Kart Merkezi*.

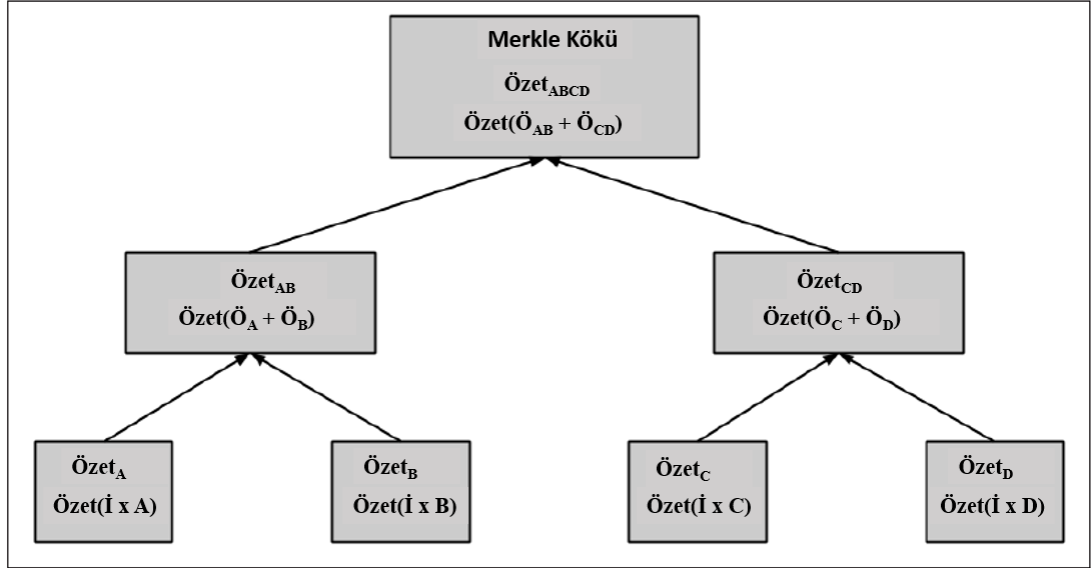
Bir bloğun özet değeri bulunurken, kendinden önceki bloğun özet değeri de dikkate alınır. Bu sebeple kötü niyetli bir kişinin bir bloğu değiştirebilmesi için kendinden önceki tüm blokları değiştirmesi gerekmektedir. Bu da pratikte mümkün görülmemektedir. Özetleme değeri bir bloğun dijital parmak izi olarak kabul edilmektedir. Her blok birbirine bağlandığı için, bloklardaki veriler değiştirilmek istendiğinde kendinden önceki blokların da değiştirilmesi gerektiği için bu durum neredeyse imkânsıza yakındır.

2.3.5.2.3.Merkle Kökü

Merkle ağacı, büyük veri kümelerini güvenli ve hızlı bir şekilde doğrulamak için kullanılan, güvenli özetleme yapısı üzerinde geliştirilmiş bir yaklaşımdır (Usta ve Doğanterkin, 2018). Tüm işlemler için tek bir parmak izi üreterek, bir işlemin ilgili bloğa dahil olup olmadığını hızlı bir şekilde doğrular (Antonopoulos, 2014). Kısaca merkle ağaçları bir blokta bulunan tüm işlemleri özetlemek için kullanılmaktadırlar. Merkle ağacı ismi adını 1979’da patentini alan Ralph Merkle’den almıştır.

Merkle ağaç yapısında ilk olarak, bir blokta yer alan tüm işlemler için ayrı özetleme değerleri bulunur. Her bir işlem için bulunan bu özetleme değerleri ikili şekilde eşleştirilir. Eşleştirilen her iki işlem için yeniden bir özetleme değerine ulaşılır. En tepede tek bir özetleme değeri kalana kadar bu yapı devam eder. En son tek kalan bu özetleme değerine de merkle kökü denmektedir (Credit Suisse, 2016).

Şekil 2.3.5.2.3.1. Merkle Ağacı



Kaynak: ANTONOPOULOS, A. M. :2014. Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc."

Şekil 2.3.5.2.3.1.'de merkle kökünün nasıl hesaplandığı bir örnekle gösterilmektedir. Bir blok içerisinde yer alan işlemlerin (işlem A, B, C ve D) özet değerleri (Ö_A , Ö_B , Ö_C ve Ö_D) ikişerli olarak gruplanmış, bu ikişerli gruplanan özet değerlerin tekrardan özet değeri (Ö_{AB} ve Ö_{CD}) alınmıştır. Bu ikişerli gruplama tek bir özet değer (Özet_{ABCD}) kalıncaya kadar devam etmiştir. En sona kalan bu Özet_{ABCD} özet değeri ile merkle kökü bulunmuştur. Eğer bloğun içindeki işlem sayısı tek ise, bu durumda sonda tek kalan işlem kendisiyle çift olarak özet değeri alınır. Şekil 2.3.5.2.3.1.'de görüldüğü gibi merkle ağacının aşağıdan yukarıya doğru olan bir yapısı vardır.

İşlem sayısı ne olursa olsun süreç aynı şekilde devam etmektedir. İster 4 işlem olsun ister 1000 tane işlem olsun, en sonunda ulaşılan merkle kökünün boyutu hep aynıdır (32 byte). Elde edilen bu merkle kökü blok başlığında depolanır ve blokta bulunan tüm işlemleri özetlemiş olur. Böylelikle bir blok tamamlandığında bloğun tamamının özet değeri alınmaz. Bunun yerine sadece bloğun başlığının özet değeri hesaplanır. Tüm bu özet değerleri hesaplanırken ise kriptolojik özetleme fonksiyonu olan hash fonksiyonu kullanılmaktadır.

Blok zincirindeki her yeni işlem ağdaki binlerce katılımcı tarafından doğrulandıktan sonra zincire eklenir. Merkle ağacı bu doğrulama işleminin daha hızlı ve verimli olmasını sağlamaktadır. Tablo 2.3.5.2.3.1.'de görüldüğü gibi bloğun boyutunun büyüklüğü arttıkça, bir işlemin ilgili bloğa dahil olduğunu ispatlamaya yarayan merkle doğrulama yolunun büyüklüğü de artmaktadır. Ancak merkle doğrulama yolunun büyüklüğü blok boyutunun büyüklüğüne göre daha yavaş bir şekilde ilerlemektedir (Görmez, 2017).

Tablo 2.3.5.2.3.1. Merkle Ağacı Verimliliği

İşlem Sayısı	Blok Boyutu	Merkle Doğrulama Yolu Büyüklüğü (özetleme değeri cinsinden)	Merkle Doğrulama Yolu Büyüklüğü (byte cinsinden)
16 tane işlem	4 kilobayt	4 tane özetleme değeri	128 bayt
512 tane işlem	128 kilobayt	9 tane özetleme değeri	288 bayt
2048 tane işlem	512 kilobayt	11 tane özetleme değeri	352 bayt
65.535 tane işlem	16 megabayt	16 tane özetleme değeri	512 bayt

Kaynak: ANTONOPOULOS, A. M. :2014. Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc."

İşlemlerin sayısı arttıkça blokların boyutu çok hızlı bir şekilde artmaktadır. Ancak buna karşılık özet değerlerin boyutu aynı hızda artmamıştır. İşlemlerin sayısı ve büyüklüğü arttıkça, merkle ağacının çalışma verimliliği de artmaktadır.

2.3.5.2.4. Zaman Damgası

İngilizcede timestamp olarak geçen zaman damgası Bloğun üretildiği zamanı göstermektedir. Zaman damgası, bir belgenin oluşturulma veya değiştirilme zamanını güvenli bir şekilde izlemek için kullanılan bir yöntemdir (Joshi, Han ve Wang, 2018).

2.3.5.2.5. Zorluk Hedefi

Bir bloğun özet değeri hesaplanması, o bloğun artık üretildiği ya da oluştuğu anlamına gelmektedir. Ancak bir bloğun oluşturulma süresinde bazı kısıtlamalar vardır. Örneğin; Bitcoin blok zincirinde bloklar her 10 dakikada bir üretilmektedir. Bu süreyi aşmamak ve bu süreden daha az bir zamanda blok üretilmemesi için bir hedef konulmuştur. İstenilen ortalama 10 dakikada bir blok oluşturmaktır. Eğer uygun

özetleme değeri 10 dakikadan daha kısa bir sürede oluşturulursa bu özet değeri bulunurken zorluk derecesi arttırılır, ya da tam tersi 10 dakikadan uzun sürüyorsa özet değeri bulmadaki zorluk derecesi düşürülür. İlgili blok için zorluk derecesi blok başlığında belirtilir.

2.3.5.2.6. Nonce

Nonce, iş ispatı algoritmalarında, iş ispatı için gerekli sayıyı ifade etmektedir. Uygun özetleme değeri oluşana kadar, nonce alanındaki sayılar deneme yanılma yapılarak değiştirilir (Güven ve Şahinöz, 2018).

2.3.5.3.İşlem Sayacı

Bir bloğun içinde kaç tane işlem olduğunu gösterir. Bloğun içinde yer alan işlem sayısı işlemlerin büyüklüğüne, karmaşık algoritmaları çözmek için gereken hesaplama gücüne bağlı olarak değişmektedir (Ortman, 2018).

2.3.5.4.İşlemler

Bir bloğun içinde kaydedilen tüm işlemleri ifade etmektedir.

2.3.6. Madencilik

Bitcoin merkezi bir otorite tarafından üretilmez veya yönetilmez, bunun yerine madencilik adı verilen bir süreçte oluşturulur (O'Dwyer ve Malone, 2014). Madencilik, bitcoin blok zincirindeki kripto para üretimidir. Kripto para üretiminin yanında ayrıca madencilik hileli işlemleri engeller, olmayan bitcoinleri harcamanın önüne geçer ve aynı bitcoinin birden fazla kez harcanmasına (double spending) karşı korur (Çarkacıoğlu, 2016).

Bitcoin ağında blokları üreten ya da kripto para üreten kişilere madenci denmektedir. Madenciler yeni işlemleri onaylarlar ve onayladıkları bu işlemleri deftere kaydederler. İşlemlerin blok zincirin bir parçası olması bunların “teyit edildiğini” gösterir. Madenciler yapmış oldukları bu madencilik işine karşılık iki çeşit ödül alırlar (O'Dwyer ve Malone, 2014). Birincisi üretmiş oldukları her bir yeni blok için aldıkları bitcoin, ikincisi ise işlemlerden aldıkları komisyondur. Ancak bu ödülü alabilmek için madenciler zor bir matematik problemini ilk önce çözebilmek için yarışır. Tezin 2.3.4.1.bölümünde belirtildiği gibi bu matematik probleminin çözümüne iş ispatı denmektedir. Bu iş ispatı algoritmasını çözmek için yarışmak bitcoinin güvenlik modelinin temelini oluşturmaktadır.

Madencilikğin esas amacı sisteme yeni bitcoin üretmek ya da madencileri ödüllendirmek değildir. Madencilik bitcoin sisteminin güvenliğini sağlamakta ve ağ genelinde merkezi bir otorite olmadan mutabakatın ortaya çıkışını gerçekleştirmektedir. Madencilikğin en önemli özelliği blok zinciri içine kaydedilecek işlemleri ve oluşturulan blokları doğrulaması ve dağıtık ağın sürekliliğini sağlamasıdır.

Bitcoin ağında çok fazla madenci bulunmaktadır. Bu madencilerin hepsinin amacı blok başlığının özetleme değerini ya da o zorluk hedefini bulmaya çalışmaktır. Bu madencileri teşvik eden şey ise, oluşturdukları bloklar için belli bir sayıda bitcoin almalarıdır. Aynı blok üzerinde birden fazla madenci çalışabilir ancak bloğu kim ilk oluşturduysa yani özet değeri ilk kim bulduysa ödülü o almaktadır. Madenciler arasındaki bu yarış yeni bloğun ağa iletilmesi ile sona ermektedir.

Bitcoin ilk üretilmeye başlandığı zamanda madencilik kişisel bilgisayarlarda yapılabilmiştir. Ancak bitcoinin popülerliği arttıkça bitcoin madenciliği yapan insan sayısı artmış ve bu da beraberinde geçerli bloğu oluşturmak için artan zorluk derecesi ile madenciliği zorlaştırmıştır. Bu sorunların üzerinden gelebilmek ve aynı başarı oranına ulaşmak için daha güçlü donanımlara ihtiyaç duyulmuştur (O'Dwyer ve Malone, 2014). Sonrasında sırası ile, kişisel bilgisayarların yetersiz kalması sebebi ile matematik işlemlerinde daha hızlı olan grafik kartlar kullanılmaya başlanmış ve günümüzde ise madencilik için özel tasarlanmış entegre devreler (Application Specific Integrated Circuit-ASIC) kullanılmaktadır. Örneğin, Intel tabanlı bir kişisel bilgisayarın özetleme kapasitesi ortalama 10-30 M/s'dir, ancak bu oran ASIC donanımı kapasitesinin milyonda birini oluşturmaktadır (Çarkacıoğlu, 2016:49). Ancak madencilik çok enerji tüketimine sebep olduğu için yeni donanımların daha yüksek bir özetleme oranına ve daha düşük enerji alanına sahip olması gerekmektedir.

2.3.7. Akıllı Sözleşmeler

Akıllı sözleşmeler (smart contracts), blok zincirine kodlanmış belirli şartlar ve koşullar karşılandığında otomatik olarak kendi kendini uygulayan bilgisayar kodlarıdır. Akıllı sözleşmeler, temeldeki dağıtık deftere yazılan ve ağdaki düğümler tarafından otomatik olarak yürütülen programlardır. Bir bilgisayar tarafından uygulanabilecek herhangi bir talimat teorik olarak akıllı bir sözleşme ile yürütülebilir. Dağıtılmış deftere kaydedilen işlemler veya veriler akıllı sözleşmeyi tetikler ve alınan işlemler de deftere kaydedilir (Natarajan, Krause ve Gradstein, 2017:29). Akıllı sözleşmeler hukuki anlamda bir sözleşme olmaktan ziyade, bir sözleşmenin kanıtı veya bir sözleşme veya sözleşmenin uygulanmasına yönelik teknolojik bir araç olabilirler (Rauchs ve ark., 2018).

Akıllı sözleşmeler kavramı ilk olarak 1994 yılında Nick Szabo isimli bir bilgisayar mühendisi ve kriptograf tarafından kullanılmıştır. Szabo, akıllı sözleşmeleri yaygın olarak karşımıza çıkan basit otomatlara benzetmiştir (Szabo, 1994).

Örneğin, bir kişi bir cips almak için otomata para verir ve ürünü seçer. Fiyatı 3 TL olan bir cips almak için 5 TL otomata verilirse, akıllı sözleşme devreye girecek ve

otomat ürünü ve ürünün fiyatını arayacaktır. Ürün bulunduktan sonra ise otomat, istenilen ürünü ve 2 TL para üstünü kullanıcıya verecektir. Ürün bulunamazsa veya kullanıcı tarafından verilen para ürünü satın almak için yeterli değilse, işlem tamamlanamayacaktır (Rozario ve Vasarhelyi, 2018).

Burada otomat önceden belirlenen kurallar doğrultusunda ürünü vermektedir. Bu durum basit bir akıllı sözleşmeyi temsil etmektedir. Sözleşmenin bir tarafı parayı ödemekte, diğer taraf da (otomat) parayı alınca ürünü teslim etmektedir. Otomatın kilitli kutusu ve diğer güvenlik mekanizmaları makinenin içindeki paraları ve ürünleri hırsızlardan ya da saldırganlardan korumakta ve bu durum otomatların farklı yerlerde yerleştirilmesine izin vermektedir (Szabo, 1997). Buradaki sözleşmeyi “akıllı” yapan, sürecin bir insan ya da üçüncü bir taraf olmadan işlemesi ve tamamen otomatik çalışmasından ileri gelmektedir (Ahi, 2018). Szabo’nun geliştirmiş olduğu akıllı sözleşmeler güvenilir aracı kurumlar olmadan da iki taraf arasındaki sözleşmelerin otomatik olarak kendi kendini gerçekleştirebileceğini savunmuştur.

İlk kez 1994 yılında literatüre girmesine rağmen, akıllı sözleşmelere blok zinciri teknolojisi ortaya çıkana kadar ihtiyaç duyulmamıştır. Bunun nedeni, Szabo’nun geliştirdiği modelde sözleşmedeki kuralların taraflar arasında uygulanıp uygulanmadığı üçüncü bağımsız bir kişi ya da kurum tarafından izlenmesine duyulan ihtiyaçtır. Bu düşünce ortaya çıktığı dönemde akıllı sözleşmelerin üçüncü taraf olmadan güvenilir bir şekilde kendi kendini yürütmesi mümkün değildir. O dönem için bunun için gerekli olan teknoloji henüz mevcut değildir.

Bitcoinin ortaya çıkışı ile birlikte, blok zinciri teknolojisinin dağıtık yapısı ile merkezi otoritelere ihtiyacın kalmadığı görülmüş ve akıllı sözleşmelerin de blok zincire kodlanarak hayata geçirilebileceği anlaşılmıştır. Gözetim sorumluluğu blok zinciri ağına dahil olan bilgisayarlara dağıtıldığı için akıllı sözleşmelerin yürütülmesi artık uygun hale gelmiştir. Blok zincire kodlanan bir sözleşme blok zincirin sahip olduğu özellikler sayesinde değiştirilememektedir.

Akıllı sözleşmeler içinde “eğer bu olursa şunu yap” tarzı mantıksal akışların önceden yazılmış olduğu bir bilgisayar kod bloğudur (Usta ve Doğanterkin, 2018). Akıllı sözleşmeler farklı taraflar arasındaki sözleşmelerin dijital olarak blok zincire

tanımlanmasını sağlamaktadır. Bu sözleşmelerde taraflar arasında müzakere edilmiş ve anlaşılmış şartlar sağlandığında sözleşme içerisinde belirtilen durumlar meydana geldiğinde sözleşme hükümleri otomatik olarak gerçekleşmektedir. Buradaki amaç günümüzdeki mevcut sözleşmelere göre hile ve hatayı azaltarak daha güvenli bir yapı sağlamak ve maliyetleri azaltmaktır.

Bitcoin blok zinciri üzerinde başka uygulamaların gelişmesine uygun olarak tasarlanmamıştır. Uygulama geliştirmek isteyenler bu blok zincirdeki kodlama dilini bilmeleri gerekmektedir. Ancak zaman içinde bu teknolojinin sadece para transferleri için değil, aracı kurumun bir güven mekanizması olarak kullanıldığı diğer alanlarda, başka amaçlar ve ihtiyaçlar doğrultusunda da kullanılabileceği düşünülmüştür. Akıllı sözleşmeler Ethereum platformu ile adını duyurmuş ve çeşitli sektörlerde kullanılmaya başlanmıştır. Ethereum'un Bitcoin blok zincirinden en büyük farkı ise burada kullanılan kodların farklı uygulamaları geliştirmeye uygun olmasıdır.

Akıllı sözleşmelerin hızlı, şeffaf, doğrulanabilir, değiştirilemeyen ve kendi kendini uygulayabilme gibi olumlu tarafları olduğu gibi zayıf yanları da vardır. Örneğin; akıllı sözleşmelerin değiştirilemeyen bir yapısı olduğu için, sözleşme üzerinde değişiklik gerekebilecek olası tüm senaryoları önceden düşünülmeli ve sözleşmeye eklenmelidir. Diğer bir zayıf noktası ise blok zinciri platformları çok yeni, sürekli gelişen teknolojik ürünler oldukları için akıllı sözleşmelerde yeterince karmaşık modeller tasarlanamamakta ve otomatik test yapıları oluşturulması gibi konularında geliştiricilerine mevcut olan yazılım geliştirme platformlarında bulunun kolaylıkları sağlayamamaktadır (Usta ve Doğantekin, 2018). Ayrıca akıllı sözleşmeleri blok zincire kodlayanlar tarafından yapılacak hatalar ciddi sorunlara yol açabilecektir. Şekil 2.3.7.1.'de örnek bir Ethereum akıllı sözleşmesi gösterilmektedir.

Şekil 2.3.7.1. Örnek Bir Ethereum Akıllı Sözleşmesi

```
contract BasicBank {
    mapping(address => uint) private balances;
    address public owner;
    event LogDepositMade(address accountAddress, uint amount);

    function BasicBank() public {
        owner = msg.sender;
    }

    function deposit() public payable returns(uint) {
        balances[msg.sender] += msg.value;
        emit LogDepositMade(msg.sender, msg.value);
        return balances[msg.sender];
    }

    function withdraw(uint withdrawAmount) public returns(uint) {
        require(balances[msg.sender] >= withdrawAmount);
        balances[msg.sender] -= withdrawAmount;
        msg.sender.transfer(withdrawAmount);
        balances[msg.sender] += withdrawAmount;
        return balances[msg.sender];
    }

    function balance() public view returns(uint) {
        return balances[msg.sender];
    }
}
```

Kaynak: USTA, A.,DOĞANTEKİN, S.:2018. Blockchain 101 v2. *Bankalararası Kart Merkezi*.

Günümüzde, imzalanması gereken bir sözleşme, sözleşmeye dahil olan taraflarca anlaşılabilmelidir. Hiç kimse anlamadığı bir sözleşmeye imza atmak istemez. Bu yüzden, günden güne gelişen akıllı sözleşmelerin daha güvenli ve günlük hayattaki herhangi biri tarafından okunabilir hale gelmesi için çalışmalar yapılmakta, insanlar tarafından okunabilen aynı zamanda da makineler tarafından da anlaşılabilen akıllı sözleşmeler geliştirilmektedir. İkinci nesil akıllı sözleşmeler olarak da kabul edilen bu sözleşmelere Ricardian Sözleşmeler (Ricardian Contracts) denmektedir (Özgür, 2019). Ricardian sözleşmelerinin amacı insanlar tarafından okunabilen ve aynı zamanda makineler tarafından da kullanılabilen sözleşmeler yaratmaktır.

Blok zinciri ve akıllı sözleşmeler blok zinciri ağının dışındaki bilgilere erişememektedir. Blok zincire kodlanmış bir akıllı sözleşmedeki şartların gerçekleşip gerçekleşmediği konusunda blok zinciri ekosisteminin dışından gelecek verilere ihtiyaç var ise bu verilere blok zinciri kâhinleri (oracle) olarak tanımlanan araçlar ile erişilmektedir. Örneğin, malların nakliyesi, depolanması ve teslimatı, ürünlerin uygun sıcaklıkta saklanıp saklanmadığı gibi bilgiler, nesnelerin interneti gibi iletişim araçları ile edinilebilmektedir (Cong ve He, 2019). Blok zinciri kâhinleri akıllı sözleşmelerde önceden belirlenmiş kuralların çalışması için dış bilgileri alıp blok zincire yerleştirerek akıllı sözleşmeleri beslemektedir (Hileman ve Rauchs, 2017; Hewett, Gogh, Pawczuk, 2020). Blok zinciri kâhinleri blok zincirin dışından gelen bu bilgiler ile blok zinciri

arasında bir ara yüz görevi görmektedir. Bu sebeple, blok zinciri kâhinleri akıllı sözleşmelerin işlemesi için gerekli doğrulamayı sağlayacağı için üçüncü bir kaynaktan gelen veriler güvenilir olmalıdır.

Akıllı sözleşmeler, iki taraf arasında şartlar ve koşullar üzerinde anlaşılmış ve blok zincirine programlanmış dijital sözleşmelerdir (Brown, 2015). Bir kere blok zincirine programlandıklarında hiçbir taraf bu sözleşmenin koşullarını blok zincirin değiştirilemez yapısından dolayı manipüle edemez. Sözleşmede yazan koşullar sağlandığında sözleşme hükümleri otomatik olarak yürütüleceği için bu sözleşmeler akıllı sözleşmeler olarak adlandırılmışlardır.

2.4.Blok Zincirinin Karakteristik Özellikleri

Blok zinciri aşağıdaki temel özelliklere sahiptir:

- **Merkezi Olmayan (Decentralization):** Geleneksel merkezi sistemlerde, her bir işlemin güvenilen merkezi bir kurum (merkez bankası gibi) tarafından doğrulanması gerekmektedir, bu da kaçınılmaz olarak merkezi sunucularda maliyet ve performans açısından bir darboğaz oluşturmaktadır (Zheng ve ark., 2017). Blok zinciri ağındaki bir işlem ise, merkezi bir kurumun kimlik doğrulamasına gerek kalmadan herhangi iki eş arasında gerçekleştirebilmektedir. Bu sayede, blok zinciri tabanlı uygulamaları kullanan kişiler, hesaplarına bağlı bir anahtar aracılığı ile kendi hesapları üzerinde doğrudan kendi kontrolü bulunmakta ve bu durum kullanıcıların varlıklarını istedikleri herhangi birine aktarma gücü vermektedir (Kibet ve Karuma, 2018). Mutabakat algoritmaları dağıtık ağdaki verilerin tutarlılığını sürdürmek için kullanılmaktadır (Zheng ve ark., 2017). Böylelikle veriler eş zamanlı kaydedilip güncellenebilmektedir. Merkezi yapıların aksine, blok zincirinde üçüncü taraflara ihtiyaç kalmamıştır. Blok zincirinde verileri kaydetmek, saklamak ve güncellemek için merkezi bir bilgisayar yoktur, dağıtık bir yapı vardır.
- **Anonimlik (Anonymity):** Her kullanıcı, gerçek kimliğini ortaya çıkarmayan, blok zincirinde oluşturulan bir adresle işlem yapabilmektedir (Zheng ve ark., 2017). Hatta bir kullanıcı, kimliğinin açığa çıkmasını önlemek için birden fazla

adres de oluşturabilmektedir (Kibet ve Karuma, 2018). Blok zincirinde kullanıcıların özel bilgilerini saklayacak merkezi bir otorite olmadığı için anonimlik, blok zincirine kaydedilen işlemlerde önemli ölçüde gizliliği korumaktadır (Zheng ve ark., 2018).

- **Şeffaflık (Transparency):** Blok zincirde kayıtlı olan her işlem ve bu işlemlerle ilgili detaylar herkes tarafından görülebilmektedir. İşlemlerin ağdaki herkes tarafından görülmesi, blok zincirini güvenilir yapmaktadır. Geçmişte kaydedilen işlemler ve yeni işlemler hakkında ortak bir görüş olduğu için, ağdaki katılımcılar blok zinciri sisteminde yapılanlar hakkında tam bir açıklamaya sahiptir.
- **Değişmezlik (Immutability):** Değişmezlik bir şeyin zaman içerisinde değiştirilememesidir. Bir işlem bir kez blok zinciri ağına kaydedildiğinde bir daha değiştirilmesi neredeyse mümkün değildir. Blok zincirinde işlemler kronolojik olarak sıralıdır ve her işlem kendinden önce kaydedilen işlemler ile bağlantılıdır. Bu yüzden kendin önceki bloğu değiştirmeden işlemleri değiştirmek imkânsızdır. Blok içerisindeki işlem değiştirilirse bu durum ağdaki kullanıcılar tarafından görülebilmektedir. Matematik algoritmaları ve mutabakat mekanizmaları sayesinde blok zincirine kaydedilen verilerin bütünlüğü korunmakta ve veriler kronolojik sıra ile kaydedilmektedir. Değişmezlik özelliği kaydedilen işlemlerin denetlemesinde çok yararlıdır. Ayrıca, ağda yayınlanan her bir blok ağdaki diğer bilgisayarlar tarafından doğrulanacağı ve işlemler kontrol edileceği için, değişiklikler kolayca tespit edilecektir (Zheng ve ark., 2018). Blok zinciri ağına dahil olan biri saldırı gerçekleştirip kendi bilgisayarındaki verileri değiştirse bile, ağdaki diğer bilgisayarda veriler orijinal hali ile kalmaktadır. Bu sebeple teoride blokların değiştirilmesi imkânsızdır. Tezin 2.9. Blok Zinciri Teknolojisinin Karşılaştığı Zorluklar bölümünde açıklanan %51 saldırısında olduğu gibi, birileri ağdaki düğümlerin %51'inden fazlasının kontrolünü aynı anda ele geçirmediği sürece kayıtlar değiştirilemeyecektir.
- **Açık-kaynaklı (Open source):** Birçok blok zinciri ağı herkese açıktır ve kayıtlar kontrol edilebilmektedir. Katılımcılar blok zinciri kodlarını

değiştirerek yeni uygulama yaratabilmektedirler (Lin ve Liao, 2017). Örneğin, tezin 2.7. Blok Zinciri Platformları bölümünde anlatılan Bitcoin, Ethereum ve Hyperledger açık kaynak kodlu uygulamalara örnek olarak gösterilebilir.

- **Denetlenebilirlik (Auditability):** Blok zinciri üzerindeki işlemlerin her biri zaman damgası ile onaylandığı ve kaydedildiği için, kullanıcılar dağıtık ağdaki herhangi bir düğüme erişerek önceki kayıtları kolayca doğrulayabilir ve takip edebilmektedir (Zheng ve ark., 2018). Denetlenebilirlik blok zincirinde kaydedilen verilerin izlenebilirliğini ve şeffaflığını arttırmaktadır.

2.5.Blok Zinciri Ağ Çeşitleri

Blok zinciri teknolojisinin kullanımı yaygınlaştıkça, insanlar bu teknolojinin Bitcoin'in ötesinde kullanım alanları olabileceğini fark etmiştir. Günümüzde sadece finans sektörü değil sağlık, emlak, enerji, tedarik zinciri gibi diğer sektörler de bu teknolojiyi kendi iş modellerine adapte etmeye çalışmaktadır. Ancak her sektörün çalışma yapısı birbirinden farklıdır. Bu sebeple tek tip bir blok zinciri ağının birbirinden farklı çalışma yapısına sahip olan sektörlerin taleplerini karşılaması mümkün olmamaktadır. Bu durum, farklı türde blok zinciri ağ yapılarının ortaya çıkmasını zorunlu hale getirmiştir.

Blok zinciri teknolojisinin özellikleri temel alınarak ağ yapıları için çeşitli sınıflandırmalar yapılmıştır. Blok zincirinde yer alan verilere erişim durumuna göre açık (public) ve özel (private) blok zinciri olarak ayırım yapılmaktayken, ağdaki düğümlerin onay ve doğrulama süreçlerine dahil olabilmesi için yetkilendirmenin gerekip gerekmediğine göre izin gerektirmeyen (permissionless) ve izin gerektiren (permissioned) blok zinciri ağları olarak sınıflandırma yapılabilmektedir (Peters ve Panayi, 2015). Ayrıca özel ağların bir çeşidi olarak konsorsiyum (consortium) blok zinciri ağ yapıları da mevcuttur.

Açık ve özel blok zincirleri kendi içinde izin gerektiren ve izin gerektirmeyen blok zinciri olarak sınıflandırılabilir (Usta ve Doğantekin, 2018).

2.5.1. Açık (Public) Blok Zinciri

Açık blok zinciri ağları herkese açıktır ve ağa dahil olacak katılımcılar konusunda hiçbir kısıtlama yoktur. Açık blok zincirlerinin faydası, kullanıcı anonimliğinin ve tutulan defterin tam şeffaflığının sağlanmasıdır. Bunun sebebi ise ağdaki herhangi birinin işlemleri ve işlemlerin detaylarını inceleyebilmesidir. Açık blok zinciri ağı üzerinde hiç kimse ya hiçbir kuruluş tam kontrole sahip değildir. Bu durum, ağdaki verilerin tek bir kişi ya da kurum tarafından manipüle edilmesini önlemektedir.

2.5.1.1. Açık ve İzin Gerektirmeyen (Public Permissionless) Blok Zinciri

Bu ağ yapılarında dileyen herkes izin almadan ağa dahil olabilir. İzin gerektirmeyen blok zinciri ağlarında ağdaki herhangi biri mutabakat sürecine dahil olabilir, blok oluşturmak ve işlemleri doğrulamak için izne gerek yoktur. Bu ağa dahil olan katılımcı sayısı, mutabakat sürecine katılacak kişi sayısı ile doğru orantılı olduğu için, açık blok zincirleri son derece güvenli bir hale gelmektedir. Ağdaki herkes veri güvenliğinin sağlanmasına, kayıtların değişmezliğine ve bütünlüğüne katkıda bulunmaktadır. Ancak, ağa dahil olan kişi sayısının artmasının getirdiği bir olumsuzluk da bulunmaktadır. Yüksek sayıda kişinin ağda bulunması işlemlerin doğrulanması için gereken süreyi uzatmakta ve mutabakat sürecini yavaşlatarak verimsiz hale getirmektedir. Her bir işlemi doğrulamak için gereken elektrik gücü devasıdır ve ağa eklenen her düğüm ile de çarpıcı biçimde artırmaktadır (Joshi, Han ve Wang, 2018).

Açık ve izin gerektirmeyen blok zincirinin en büyük örneği ise Bitcoin blok zinciri ağıdır. Bu ağ yapısı bilinmeyen kişiler tarafından faaliyet göstermektedir bu yüzden katılımcıları dürüst davranmaya teşvik etmek için insanların bu sistemde bir çıkarı olmalıdır (Hileman ve Rauchs, 2017). Örneğin geçerli işlemleri doğrulamaları için madenciler bitcoin ile ödüllendirilerek teşvik edilmektedir (Miller ve ark., 2019). Bu yüzden bu tarz blok zinciri yapılarında ağın kendisi bir değer ifade etmektedir.

2.5.1.2.Açık ve İzin Gerektiren (Public Permissioned) Blok Zinciri

Bu ağ yapılarında sisteme dahil olan kişilerin kayıtlı olan verileri okuması için izin alması gerekmez. Ancak ağda yeni bloklar oluşturmak ve mutabakat sürecine dahil olabilmek için izin gerekmektedir. İzin gerektiren blok zinciri ağlarında mutabakat sürecine dahil olabilmek için önceden yetkilendirilmiş olmak gerekmektedir. İzin gerektiren blok zincirleri belli bir amaç için oluşturulmaktadır, bu yüzden mevcut olan uygulamalarla uyumluluğu sürdürebilmek için tasarlanmışlardır. (Peters ve Panayi, 2015). Tezin 2.6. Blok Zinciri Platformları bölümünde bahsedilen Ripple uygulaması açık ve izin gerektiren ağ yapılarına örnektir. Ağa dahil olan herkes verilere erişebilir ancak mutabakat sürecinde eşlerin izin alması gerekmektedir.

2.5.2. Özel (Private) Blok Zinciri

Bitcoin gibi açık blok zinciri ağ yapıları, finans kurumları gibi belli regülasyona tabi olan kurumlar için çok uygun görülmemektedir. Çünkü bu ağ yapılarında kullanıcıların gerçek kimlikleri görülmemekte ve anonimlik ön plana çıkmaktadır. Bu sebeple büyük ölçekli ve regülasyona tabi olan firmalar bu teknolojinin kendi ihtiyaçları doğrultusunda nasıl kullanılabileceğini araştırmaya başlamıştır (Hileman ve Rauchs, 2017).

Özel blok zinciri ağlarında sadece izin verilen kişiler ya da organizasyonlar ağa dahil olabilmektedir (Peters ve Panayi, 2015). Özel blok zinciri ağları bilginin kimler ile paylaşılacağını belirlemekte ve sadece ağdaki kişiler bilgilere erişebilmektedir (Usta ve Doğantekin, 2018:14). Özel blok zincirleri şirketlerdeki ya da organizasyonlardaki sadece belli kişilerin kullanması ve bilmesi gereken hassas bilgileri depolamak için kullanılmaktadır. Tüm işlemlerin kamuya açıklanması, çoğu kuruluş için önemli bir güvenlik ve gizlilik riski oluşturmaktadır. Bu nedenle, bazı firmalar blok zinciri protokolünü özel blok zinciri olarak adlandırılan güvenli ve kapalı bir ağ içinde dağıtmaya çalışmıştır. Özel blok zincirler yalnızca yetki verilen tarafların işlemlere erişmesine izin veren, yetki verilmeyen kişilerin ise bu işlemleri veya bilgileri okuyamadığı ve değiştiremediği blok zinciri protokolüne dayanmaktadır. Çünkü bu tür blok zinciri ağında veriler sadece organizasyon içinde kalır ve dışarıdan herhangi bir kurum bu bilgilere ve verilere erişimi

sağlayamamaktadır. Buradaki işlemler sadece bu ekosistemdeki katılımcılara açıktır. Eğer yeni kullanıcılar için erişim izni verilecekse ya da bir kullanıcı ağdan çıkarılacaksa ağ yöneticisi bu durumla ilgilenir. Özel blok zincirlerin tek önemli eksikliği ise, açık blok zincirlerin sağlamış olduğu güvenliği sağlayamaması ve merkezi otoriteye yatkın bir yapıya sahip olmasıdır. Özel blok zinciri yapıları, merkezi bir otoritenin daha güvenli, daha verimli ve daha hızlı bir teknolojiyle buluşmasına izin verdiği için devlete bağlı kurumlar veya özel sektör şirketleri tarafından kabul edilebilirliği açık blok zinciri yapılarına göre daha fazladır (Joshi, Han ve Wang, 2018).

2.5.2.1.Özel ve İzin Gerektirmeyen (Private Permissionless) Blok Zinciri

Bu ağ yapısına dahil olabilmek ve kayıtlı verileri okuyabilmek için izin alınması gerekmektedir. Ancak ağa dahil olan tüm katılımcılar aynı zamanda mutabakat sürecine de dahil olurlar. Mutabakat sürecinde ağdaki katılımcıların özel bir izin almalarına gerek yoktur. LTO Network bu ağ yapılarına örnek olarak gösterilebilmektedir (LTO, 2019).

2.5.2.2.Özel ve İzin Gerektiren (Private Permissioned) Blok Zinciri

Bu ağ yapılarında sadece izin verilen kişiler ağa dahil olabilmekte ve gerçekleşen işlemlerin mutabakatı ve onaylanması sadece işlemin tarafları arasında yapılmaktadır. Ağa dahil olan herkes mutabakat sürecinde yer almaz. Ağ yöneticisi tarafından mutabakat sürecine dahil olunması için izin alınması gerekmektedir. İzin gerektiren ağdaki tüm katılımcılar işlemlerin doğrulanmasına ve onaylanmasına dahil olamazlar. Bunun yerine, belli bir şirket veya kuruluş her bir işlemi başlatır, doğrular ve onaylar.

Ağdaki kişilerin isimleri belli olacağı için yapacakları işlemde yasal olarak sorumludurlar. Bu yüzden açık ve izin gerektirmeyen blok zinciri ağındaki gibi kripto para almak için teşviklendirilmelerine gerek yoktur, yanlış bir hareketlerinde karışılacakları yasal yaptırımlar onları dürüst davranmaya teşvik etmektedir (Hileman ve Rauchs, 2017). Tezin 2.6. Blok Zinciri Platformları bölümünde anlatılan Hyperledger Fabric uygulaması bu ağ yapılarına örnektir.

Şekil 2.5.1.'de farklı blok zinciri ağ türlerinde faaliyet gösteren bazı uygulamalar gösterilmiştir.

Şekil 2.5.1. Blok Zinciri Ağ Türlerinde Faaliyet Gösteren Uygulamalar



Kaynak: LTO:2019, Permissionless Private Blockchain, December 23, 2019, (Çevrimiçi)
<https://blog.ltonetwork.com/permissionless-private-blockchains-lto-network/>, 11 Nisan 2020.

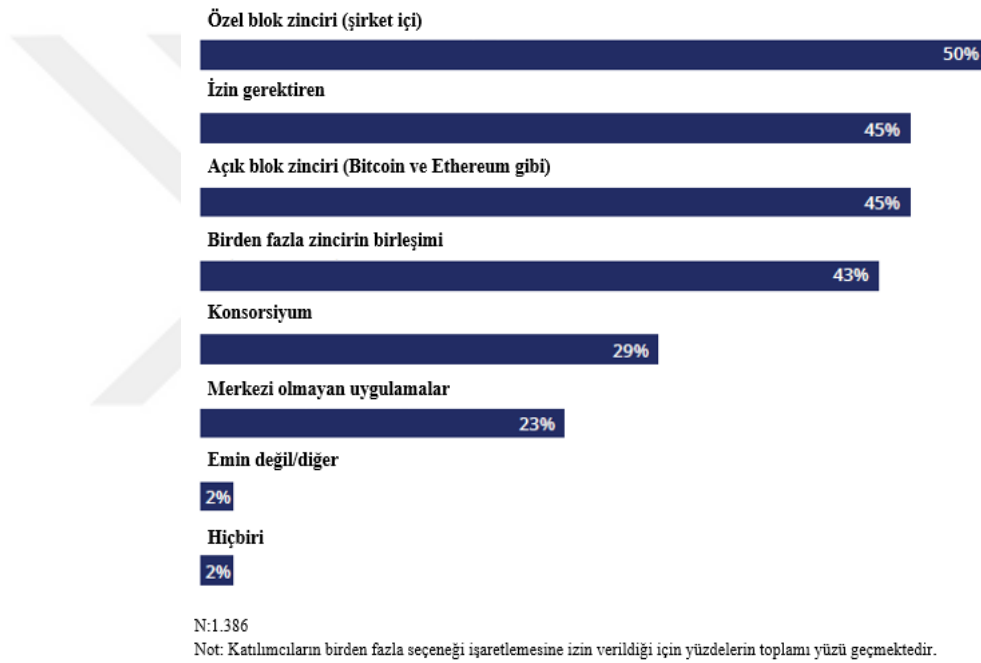
2.5.1. Konsorsiyum Blok Zinciri

Konsorsiyum blok zincirler belirli amaçlar çerçevesinde bir araya gelmiş şirketler ve kurumlar arasında kurulan blok zinciri ağlarıdır. Ağa katılım özel blok zinciri yapılarında olduğu gibi yine herkese açık değildir. Konsorsiyum blok zinciri yapılarında kimlerin işlemlerin doğrulanmasında kimlerin mutabakat sürecini kontrol edeceğine birlikte yer alan şirketler ortak karar vermektedir (Dib ve ark., 2018). Konsorsiyum blok zincirlerde ağ, dışarıdaki katılımcılara kapalı ve resmi olarak birbirini tanıyan kurumlar arasında olduğu için işlemlerin doğrulanması daha hızlı ve verimli şekilde gerçekleşmektedir (Zheng ve ark., 2018). Konsorsiyum blok zinciri ağları, açık ve özel blok zincirlerin karışımı olarak da kabul edilmektedir.

Dünyanın en büyük dört danışmanlık ve denetim firmalarından olan biri olan Deloitte, 2019 yılında yayınlamış olduğu Küresel Blok Zinciri Anketinde (Global Blockchain Survey) katılımcılara şirketlerinde ya da projelerinde hangi blok zinciri modelini uygulamayı düşündüklerin sormuştur. Anket çalışmasına ABD'den 304;

Kanada'dan 103, Birleşik Krallık'tan 150, Brezilya'dan 103, İsrail'den 53, Singapur'dan 100, Hong Kong'dan 101, Çin'den 200, Almanya'dan 131, İsviçre'den 52, Lüksemburg'dan 51 ve Birleşik Arap Emirlikleri'nden 38 üst düzey yönetici katılmıştır. Anket sonuçlarına göre katılımcıların %50'si özel blok zincirlerini %45'i izin gerektiren blok zincir yapılarını yüzde %45'i açık blok zinciri ağ yapısını ve %29'u konsorsiyum tercih ettiğini belirtmiştir (Pawczuk, Massey ve Holdowsky, 2019).

Şekil 2.5.2. Şirketiniz Hangi Blok Zinciri Modeline Odaklanmaktadır?



Kaynak: PAWCZUK, L., MASSEY R., HOLDOWSKY J.: 2019. Deloitte's 2019 Global Blockchain Survey: Blockchain gets down to business'. Deloitte Insights.

2.6.Blok Zinciri Platformları

İnsanların hayata geçirmek istedikleri projeler için çeşitli blok zinciri platformları bulunmaktadır. Yeni yazılım geliştirip, yeni bir platform da kurulabilir ancak bunu yapmak çok zaman alan bir süreçtir. Bu bölümde en çok kullanılan blok zinciri platformları anlatılmıştır.

2.6.1. Bitcoin

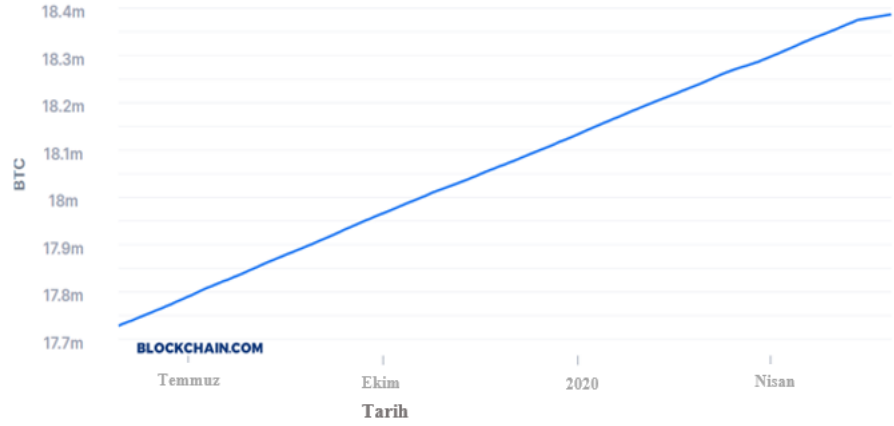
Günümüzde para transferi yapabilmek için aracı kurumlara ihtiyaç duyulmaktadır. Ancak aracı kurumlar ile gerçekleşen bu işlemler hem maliyete sebep olmakta hem de işlem süresini uzatıp, gecikmelere sebep olabilmektedir. Bitcoin bu konuya bir çözüm olarak geliştirilmiş bir uygulamadır. Bitcoin sahibi ve merkezi olmayan bir uygulama ve para birimidir. 2008 Satoshi Nakamoto'nun yayınlamış olduğu makale ile bitcoin ilk kripto para olarak kabul edilmektedir. Bitcoinin, kendi içsel değeri yoktur, onun değerine karar verenler alım satımını yapan kişilerdir. 2009 yılında faaliyete geçen Bitcoin platformunda kullanılan kripto para Bitcoin'dir ve BTC olarak kısaltılmaktadır.

Daha önce tezin 2.3.6. Madencilik bölümünde belirtildiği üzere bitcoinde madencilik çok yüksek işlem gücü gerektiren ve enerji harcayan makinelerle yapıldığı için, madencilerin bu sistemde kalmaları ve yeni madencilerin de bu sisteme dahil olmasını sağlamak için madencilere ödül verilmektedir. Bu bilgisayarlar ya da cihazlar madencilerin yapmış olduğu işlem doğrulama ve yeni işlemlerin bloklara eklenmesi gibi işlerin maliyetinin fazla olmasına sebep olmaktadır. Madencilerin bu yüksek maliyetli işleri yapıp, ağda kalmaları için onları teşvik edecek bir ödül sistemi bulunmaktadır.

Bitcoin'de her 10 dakikada bir blok doğrulanmakta ve bitcoin üretimi yapılmaktadır. Madencilere doğrulanan blok karşılığında verilen bu ödül her dört yılda bir azalmakta ve buna yarılanma (halving) denmektedir. Her 210.000 blok üretildiğinde bitcoin yarılanması meydana gelmektedir, dört yıllık süre bu üretim için gerekli ortalama zamandır. Sistemin ilk faaliyete geçtiği 3 Ocak 2009 tarihinden sonra ilk yarılanma 28 Kasım 2012'de gerçekleşmiş ve madencilerin aldığı ödül 50 bitcoin'den 25 bitcoine düşmüştür. İkinci yarılanma 9 Temmuz 2016'da gerçekleşmiş ve blok ödülü 12.5 bitcoine düşmüştür. Dördüncü yarılanma ise 11 Mayıs 2020'de gerçekleşerek 12.5 bitcoinden 6.25 bitcoine düşmüştür (Partz, 2020). Böylelikle Bitcoinde en fazla 21 milyon adet bitcoin üretimi yapılabilecektir.

Şekil 2.6.1.1.'de Mayıs 2020 itibari ile dolaşımdaki bitcoin sayısı gösterilmektedir.

Şekil 2.6.1.1. Dolaşımdaki Bitcoin Sayısı, Mayıs 2020



Kaynak: Dolaşımdaki Toplam Bitcoin, 2020, (Çevrimiçi)
<https://www.blockchain.com/charts/total-bitcoins>, 19 Mayıs 2020

19 Mayıs 2020 tarihi itibarıyla işlem gören 5.487 kripto para birimi ve 22.324 tane kripto para piyasası mevcuttur. Kripto paraların piyasa değeri 267 milyar dolar 24 saatlik hacmi ise 126 milyar dolardır. Bu piyasalarda bitcoinin hâkimiyeti ise %67.1'dir (Blockchain.com, erişim tarihi: 19 Mayıs 2020). Bu kripto para birimlerinin hepsi güvenliği sağlamak için DDT kullanılmaktadırlar.

2.6.2. Ethereum

Ethereum, bitcoin gibi açık kaynak kodlu bir açık blok zinciri ağıdır. Dünyada bitcoinden sonra en bilinen ve en çok kullanılan para birimi olan Ether (ETH) Ethereum'un para birimidir. Ethereum ağındaki kullanıcıları teşviklendirmek için Ether verilmektedir (Pongnumkul, Siripanpornchana ve Thajchayapong, 2017). Ethereum'un yaratıcısı olan Vitalik Buterin blok zinciri teknolojisini sadece para transferi için kullanılan bir teknoloji olarak görmeme ve bu teknolojinin para transferi dışında başka uygulamalar için de kullanılabileceğini düşünmekteydi. Bitcoin geleneksel ödeme işlemlerine alternatif, merkezi bir otorite olmadan, eşten eşe para transferini sağlarken, Ethereum merkezi bir otorite olmadan, uygulamaların geliştirilmesi ve çalıştırılması üzerine kullanılmaktadır. Ethereum, ağda gerçekleşen işlemlerin programlanabilir bir şekilde yapılmasına olanak sağlamıştır.

Vitalik Buterin, Ethereum’u petrole benzetmiş ve Ether’i şu şekilde tanımlamıştır: *“Eğer kripto paralar ile dünyada bulunan değerli kaynakları karşılaşıyorsak ve Bitcoin’i altın, Litecoin’i gümüş olarak kabul ediyorsak, Ethereum petroldür. Çünkü Ethereum’un altında yatan teknoloji dünyanın internet sistemindeki enerji kaynağı olacaktır. Dünyada petrol nasıl birçok sektör ve teknolojide kullanılıyorsa Ethereum teknolojisi için de aynı şey geçerlidir. Bu nedenle biz Ether’i ‘kripto yakıt’ olarak adlandırıyoruz. Ethereum platformunun ihtiyaç duyduğu enerji bu para ile sağlanacak.”*(Küçük, 2017).

Ethereum ağında her makine Ethereum Virtual Machine (EVM) isimli bir sanal makine ile çalışmaktadır. Bu sanal makine sayesinde teorik olarak gözlenebilen her şey Ethereum içinde program olarak hazırlanabilmektedir ve bu programlara da akıllı sözleşmeler denmektedir (Usta ve Doğantekin, 2018).

Ethereum platformundaki en temel yenilik ise akıllı sözleşmelerdir. Ethereum’un ortaya çıkması ile çok çeşitli akıllı sözleşmeler ortaya çıkmış ve bu sayede farklı amaçlara hizmet edilebilmiştir. Bunların bir kısmı merkezi olmayan uygulamalar (decentralized applications) bir kısmı ise merkezi olmayan kuruluşlar (distributed autonomous organization) olarak yer almaktadır. Tezin 2.3.6 bölümünde detaylıca anlatılan akıllı sözleşmeler sayesinde blok zincirin kullanım alanları oldukça genişlemiştir. Akıllı sözleşmelerin kullanılması blok zinciri teknolojisinin gelişmesinde atılan çok büyük bir adım olmuştur. Bu sebeple Ethereum için Blok Zinciri 2.0 da denilmektedir.

Ethereum platformu bir açık blok zinciri ağı olsa da, yazılımı açık kaynaklıdır ve yazılım geliştiricilerin bu ağı indirmesine ve özel bir ağ tasarlamasına izin vermektedir (Pongnumkul, Siripanpornchana ve Thajchayapong, 2017). Microsoft, Intel, J.P. Morgan gibi kurumlar tarafından kurulan “Ethereum Kurumsal Birliği (Enterprise Ethereum Alliance)” ile birlikte Ethereum, kurumsal dünya içerisinde özel blok zinciri yapılarının oluşturulması adına önemli bir potansiyel sunmaktadır. Ethereum üzerinde geliştirilen ve geliştirilmeye devam eden oldukça fazla proje bulunmakta ve her geçen gün büyümekte olan Ethereum Kurumsal Birliği ile birlikte

özellikle iş dünyasındaki uygulamaların çeşitlenmesi ve artması beklenmektedir. (Usta ve Doğatekin, 2018).

2.6.3. Hyperledger

Hyperledger, Aralık 2015'te Linux Vakfı tarafından duyurulan açık kaynak kodlu bir blok zinciri girişimidir (Hyperledger, 2018). Hyperledger, Bitcoin ve Ethereum platformlarından farklı olarak kurumlara ve iş dünyasına, şirket seviyesindeki ağlara dağıtık sistemlerin alt yapısını kurmayı amaçlamaktadır. Bitcoin ve Ethereum blok zinciri platformları açık blok zinciri ağ yapıları üzerinde çalıştığı için herkes ağdaki işlemleri görebilmektedir ve bu platformlar kripto para işlemleri için kullanılmaktadır. Kurumsal firmaların esas faaliyetleri ise kripto para alım satımı odaklı değil, bilginin değişimi odaklı çalışırlar. Bu yüzden Hyperledger genellikle izin gerektiren özel blok zinciri ağ yapılarını kullanmaktadır. Bu platformdaki uygulamaları kullananlar için gizlilik önemlidir. Hyperledger projelerinin ortaya çıkışının arkasında da bu düşünce yatmaktadır. Hyperledger'in kesinlikle bir kripto projesi olmadığı Hyperledger'in kurucuları tarafından açıkça dile getirilmiştir. Bu yüzden Hyperledger'in kendine ait bir kripto para birimi yoktur. Hyperledger finans, tedarik zinciri, bankacılık, nesnelerin interneti ve teknolojiye lider olan firmaların üye olduğu bir işbirliğidir. Sektörler arası işbirliği sağlanarak blok zinciri teknolojisinin geliştirilmesi amaçlanmıştır.

Kurumların farklı istekleri ve ihtiyaçları olabileceği için Hyperledger bu değişen isteklere cevap verebilmek ve adapte olabilmek için çeşitli uygulamalar ve araçlar geliştirmiştir. Bu yüzden Hyperledger'ın tek bir tane standart blok zinciri uygulaması yoktur. Hyperledger Fabric, Hyperledger Burrow, Hyperledger Besu, Hyperledger Indy, Hyperledger Iroha ve Hyperledger Sawtooth günümüzde kullanılan Hyperledger uygulamalarıdır (Hyperledger, 2020).

En çok kullanılan uygulamalardan olan ve IBM öncülüğünde geliştirilen Hyperledger Fabric'de modüler yapısı ile mutabakat ve üyelik servisleri gibi ihtiyaçlara göre değişiklik yapılabilir. "Herkesi uyandıran (one-size-fits-all)" tek bir

özüm olmaması gerekesi ile, esnek bir yapıda tasarlandığı için son gelişmelerin çoğunu içeren ve ekleyebilen yapıya sahiptir (Hyperledger, 2018).

2.6.4. Ripple

Ripple uluslararası para transferini (para gönderme/ödeme) gerçekleştirmek üzere kurulmuş bir platformdur. Kurumun internet sayfalarında yaptığı açıklamaya göre uluslararası düzeyde para gönderimi sırasında aracı kuruluşlardan dolayı katlanılan maliyet ve yavaşlıktan dolayı bu soruna çözüm getirebilmek için blok zinciri teknolojisi kullanılmıştır. Bitcoin aracı kurumlar olmadan kişiler arası para transferini mümkün kılarken Ripple aracı kurumlar olmadan bankalar arası bir sistem geliştirmiştir (Zimakosov, 2018). Ripple bir ödeme platformu olmasının yanında bünyesinde bir kripto para birimi de bulundurmaktadır. Ripple platformunun kripto para biriminin kısaltması XRP olarak belirlenmiştir. Ripple’in Teknolojiden Sorumlu Başkanı David Schwartz, üç harften oluşan para birimi kodlarının, düzenleyen ülkenin iki harfli ülke koduna bir karakter eklenerek oluşturulduğunu belirtmiştir. Örneğin ABD’nin ülke kodu US (Unites States) olduğundan para birimi olan Amerikan Dolarının kodu USD’ (United States Dollar) dir. Ancak hiç bir ülke tarafından çıkarılmayan varlıkların kodlarının ise X ile başladığını belirtmiş ve altını buna örnek göstermiştir. Altını çıkaran ya da ona sahip olan bir ülke yoktur ve kimyadaki sembolü AU olduğu için para birimi kodu XAU’dur. Ripple para birimini de çıkaran bir ülke olmadığı için kripto para birimi kodunun XRP olarak kısaltıldığını belirtmiştir (Schwartz, 2020).

Ancak kendi para birimi dışında bitcoin, ether gibi diğer kripto paraları ve yabancı ülke paralarının transferini de gerçekleştirebilmektedir. Hatta yolcu mil puanları gibi değer ifade eden herhangi bir birim ile de işlem yapılabilir. (Usta ve Doğantekin, 2018).

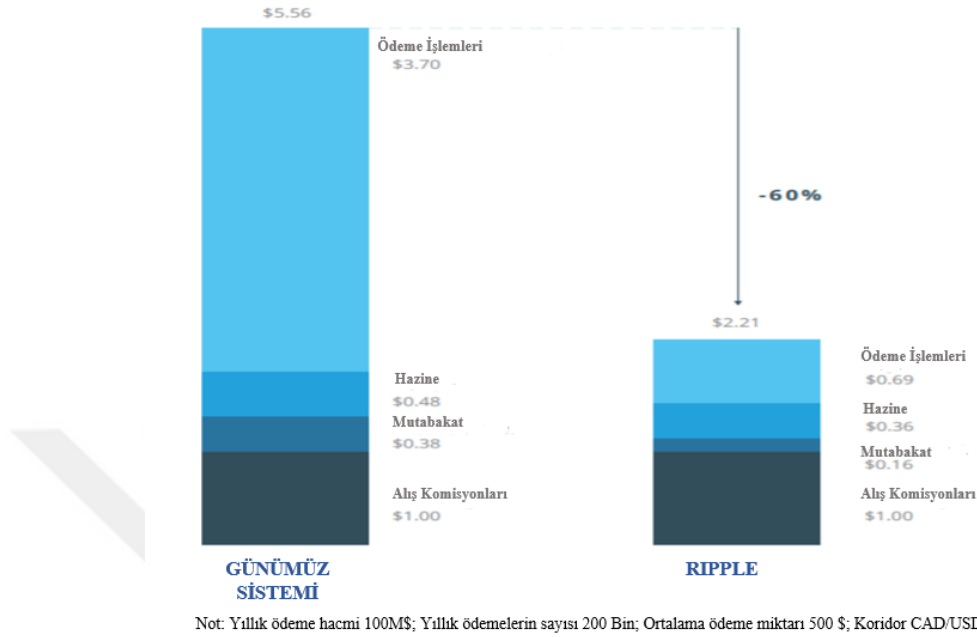
Ripple, bankalar arası iletişimi, ödeme ve takas işlemlerini daha hızlı, şeffaf ve verimli bir şekilde gerçekleştiren ilk küresel gerçek zamanlı brüt ödeme (real-time gross settlement–RSGT) sistemidir. Ripple bankalar arası iletişimi gerçekleştirebilmek için xCurrent isimli bir uygulama geliştirmiştir. Dağıtık ve eşler arası ağ kullanıldığı

için işlemler daha hızlı, gerçek zamanlı ve daha az maliyet katlanılarak gerçekleştirilebilmektedir. Bankalar arası para transferi için kullanılan geleneksel yöntem, “Dünya Bankalar Arası Finansal İletişim Topluluğu” olarak Türkçe’ye çevrilebilecek “Society for Worldwide Interbank Financial Telecommunications” sözünün baş harfleri ile SWIFT olarak ifade edilmektedir. Ripple, bu yönetime alternatif olarak geliştirilmiştir. SWIFT kullanılarak gerçekleşen işlemler nihai yere varmadan önce birkaç aracı kurumdan daha geçmektedir. Bu durum SWIFT’i zaman harcayan, maliyetli ve daha az şeffaflık sunan bir sistem haline getirmektedir. Ripple gibi sistemlerin 5-10 yıl içerisinde ülkeler arası para transferi sistemini değiştireceği beklenmektedir. (Qui, Zhang ve Gao, 2019) .

Ripple ağında olan bankalar hem kendi aralarında ödemeler hakkında bilgi alışverişinde bulunabilmekte hem de ödemeleri gerçek zamanlı gerçekleştirebilmektedir. Ripple’ın kullanmış olduğu Interledger Protokolü (ILP), bankaların farklı sistemlere sahip olmasından kaynaklanan sorunlar aşıl原因arak, farklı defterlerin ve ödeme ağlarının birlikte çalışabilmesine olanak sağlamaktadır.

Ripple tarafından hazırlanan rehberde günümüz bankacılık sistemi ve Ripple sistemi karşılaştırılarak 500\$ değerindeki örnek bir işlemde katlanılan maliyetler Şekil 2.6.4.1.’de gösterilmiştir.

Şekil 2.6.4.1. Ödeme Sistemlerinin Maliyetlerinin Karşılaştırılması



Kaynak: RIPPLE, ERİŞİM TARİHİ: 12 MAYIS 2020. Solution Overwiev, (Çevrimiçi),
:https://ripple.com/files/ripple_solutions_guide.pdf, 12 Mayıs 2020.

Gerçekleşen işlemde günümüz sistemlerinde toplam ödenmesi gereken tutar 5.56\$ iken Ripple'ın kullanıldığı ödeme sisteminde bu tutar 2.21\$ olarak gerçekleşmiştir. Yüzde 60'lık bir azalma ile para transferinin daha verimli bir şekilde yapıldığı görülmektedir. Ayrıca anında doğrulama ve gerçek zamanlı izleyebilme özelliğinden dolayı mutabakat ücretlerinin de azaldığı görülmektedir.

16 Haziran 2016 tarihinde söz konusu maliyet ve zaman tasarrufunun ispatlanmasına yönelik Ripple platformu üzerinde yapılan testte, normalde 2 ile 6 iş günü arasında gerçekleşen bir işlemin Ripple ile 8 saniyede gerçekleştiği saptanmıştır (Ripple, erişim tarihi: 13 Mayıs 2020). Bu denemede bir Kanada bankası olan ATB Financial ile Alman bankası olan Reisebank arasında 1.000 Kanada doları transferi gerçekleşmiştir.

Ripple ödeme platformu üyeleri arasında American Express, MoneyGram, PNC, Santander, SBI Remit gibi önemli uluslararası finans kuruluşları bulunmaktadır. Türkiye'den Akbank da bu platformun 2017 yılından itibaren üyesidir (Ripple, 2017). Akbank Direkt Bankacılıktan Sorumlu Genel Müdür Yardımcısı Tolga Ulutaş, Şubat 2018'de Avrupa'nın en büyük bankalarından biri olan İspanyol Bankası Santander'in

iştiraki Santander UK'e Ripple üzerinden blok zinciri altyapısı ile GBP (Sterlin) para transferlerine başladıklarını belirtmiştir (Akbanklab, 2018).

2018 yılında yaklaşık olarak 100 finansal kuruluşun bulunduğu Ripple platformunda 2019 yılında bu sayı 200'e çıkmıştır. Aynı zamanda 2019 yılında Ripple platformu üzerinde gerçekleşen ödemelerde ise yüzde 350 artış görüldüğü şirketin yaptığı açıklama ile belirtilmiştir (Ripple, 2019).

2.6.5. Corda

Bir başka blok zinciri platformu, bu alanda yazılımları bulunan bir teknoloji firması olan R3 tarafından geliştirilen Corda platformudur. Finans kuruluşları arasındaki yasal sözleşmeleri, kaydetmek, yönetmek ve otomatikleştirmek üzere geliştirilmiş olan bir dağıtık defter platformudur.

Corda'nın geliştiricilerinden olan Richard Gendal Brown, günümüzde finans sektöründe kurumlar arasında gerçekleşen sözleşmelerde, sözleşmedeki tarafların sözleşmeyi birbirinden bağımsız olarak kendi sistemlerinde, farklı şekillerde kaydettiğini ve bu durumdan kaynaklı ortaya çıkabilecek farklılıkları ve uyumsuzlukları düzeltmenin ise oldukça maliyetli bir işlem gerektirdiğini belirtmiştir (Brown, 2016). Corda finans sektöründeki bu sorunları ortadan kaldırmak üzere tasarlanmıştır.

Corda'da akıllı sözleşme yaklaşımı uygulanmakta ve bu yaklaşım ile tekrarlama (duplications), mutabakat (reconciliations), hatalı eşleme (failed matches) ve ihlal (breaks) gibi durumları ortadan kaldırmak hedeflenmektedir (Brown ve ark., 2016).

Corda'da işlemler sadece sözleşmeye dahil olan taraflar arasında görülebilmektedir. Ağdaki diğer kişiler tarafından bu bilgilere erişilmesi mümkün değildir. İşlemlerin doğrulanması da yine sadece sözleşmeye dahil olanlar arasında yapılabilmektedir. Corda da Hyperledger gibi izin gerektiren özel blok zinciri ağ yapılarını kullanmaktadır ve kurumsal firmalar için tasarlanmıştır. Hyperledger platformundan farklarından en önemlisi sadece finans kuruluşlarına hizmet etme amaçlı olmasıdır. Corda'nın kendi kripto para birimi yoktur.

Türkiye’de ilk kez İş Bankası 30 Mart 2020 tarihinde R3 Corda platformuna üye olmuştur. İş Bankası Genel Müdür Yardımcısı Yalçın Sezen blok zinciri teknolojisinin finans sektörü ve bankacılığın geleceğini şekillendireceğini ve bunu yeni bir iş modeli olarak gördüğünü belirtmiştir. Ayrıca Corda platformundaki üyeliği ile R3 üye ağındaki bulunan 300’den fazla paydaş ile işbirliği ve fikir alışverişi yapma imkânından faydalanacaklarını ve blok zincirini entegre ederek geliştirecekleri hizmetler ile Türkiye’de bu alanda öncü banka olmayı hedeflediklerini söylemiştir (İşbankası, 2020).

27 Mayıs 2020 tarihinde İş Bankası, Şişecam, Kuraray Europe GmbH ve Commerzbank arasında ilk pilot işlem gerçekleşmiştir. Corda teknolojisi kullanılarak Marco Polo ağı üzerinden gerçekleşen bu işlemle, dış ticaret finansmanında ödeme güvencesi sağlanarak Almanya’dan Türkiye’ye lamine cam ara katman ticareti gerçekleşmiştir (Marco Polo, 2020). Kuraray, dünya çapında faaliyet gösteren bir özel kimyasallar şirkettir ve endüstrinin birçok dalı için polimerler ve sentetik mikrofiberler alanında en büyük ürün sağlayıcılardan biridir.

2.7.Blok Zinciri Teknolojisinin Karşılaştığı Zorluklar

Her ne kadar günümüzde blok zinciri teknolojinin getirdiği ve getireceği yenilikler konuşuluyor olsa da, bu teknolojinin yüzleşmesi ve çözmesi gereken bazı problemler de mevcuttur. Blok zinciri teknolojisinin getirmiş olduğu avantajlardan faydalanılırken, aynı zamanda, onun etkilerine ve olabilecek güvenlik sorunlarına da dikkat edilmesi gerekmektedir. Blok zinciri teknolojisi, büyük potansiyeline rağmen, geniş çapta kullanımını sınırlayan birçok zorlukla karşı karşıyadır.

Blok zincirinin benimsenmesini engelleyen zorluklardan biri, firma yöneticilerinin finansal gizlilik ve iş sırlarından endişe duymasıdır. Bu endişenin kaynağı, açık ağ yapısındaki bir blok zincirindeki tüm katılımcıların her işlemin tam bir kopyasına sahip olmasıdır. Bir ağa daha fazla düğümün dahil olması ile, kaydedilen veriler güvenilir hale gelmektedir. Ancak bunu sağlayan dağıtık yapı ile verilerin gizliliği azalmaktadır. Zaman içinde özel blok zincirlerin gelişmesine yol açan da bu gizlilik endişesidir. Özel blok zincirleri yalnızca izin verilen bölümlerin bulunduğu daha sınırlı bir dağıtık yapıdır. Özel bir blok zinciri nispeten kapalı, güvenli bir iş

ortamı sağlasa da, yöneticiler ağ üzerinde tam kontrole sahiptir. Bu da saldırılara karşı direnci zayıflatmakta ve kamu katılımını da sınırlandırdığı için zincirin şeffaflığını da azaltmaktadır. Bu nedenle, yönetim kişisel çıkarları için işlemleri ve verileri manipüle edebiliyorsa, özel blok zincirlerin kurcalamaya karşı direnci garanti edilemez (Wang ve Kogan, 2018).

Blok zinciri ağındaki kullanıcı sayısı arttıkça ölçeklenebilirlik (scalability) problemi ortaya çıkmaktadır. Kaydedilen verilerin her geçen gün artmasıyla blok zinciri ağı büyümektedir. Blok zinciri ağı büyüdükçe verilerin kaydedilmesi ve işlemlerin hesaplanması zorlaşmakta ve ağdaki tüm verilerin senkronize olması uzun zaman almaya başlamaktadır. Sürekli artan blok zinciri kullanımı ve günlük işlemlerin sayısındaki artış ile blok zincirin boyutu devasa hale gelmektedir. Kısıtlı blok boyutu ve yeni bir blok üretmek için kullanılan zamanın göz önüne alındığında, blok zincirinin gerçek hayatta aynı anda milyonlarca işlemi gerçekleştirilmesi gerekliliği yerine getirilememektedir. Dünya’da yaygın olarak kullanılan kredili ödeme sistemleri olan Visa ve Mastercard ağında, saniyede binlerce, sadece VISA sisteminde günde yaklaşık 150.000.000 işlem gerçekleştirmektedir ve saniyede 24.000 işlem gerçekleştirme kapasitesi vardır (Li 2019; Visa, erişim tarihi: 9 Mayıs 2020). Bitcoin ağında saniyede 3-4 tane işlem gerçekleştirilmekte ve bir blok büyüklüğü 1MB olmaktadır. Bu blok büyüklüğü ve yeni bir blok oluşturmak için kullanılan zaman aralığı göz önüne alındığında saniyede milyonlarca işlem gerçekleştirilememektedir. Bitcoin ağında her 10 dakikada bir blok onaylanmakta, ethereum ağında ise bir işlemin onaylanması için 15 saniye gerekmektedir (Bambrough, 2019).

Blokların kapasitesi çok küçük olduğu için, madencilerin daha büyük işlem ücretleriyle işlemleri doğrulamayı tercih etmeleri nedeniyle blok zincirindeki blokların boyutu, küçük işlemlerde gecikmeye sebep olabilmektedir (Joshi ve ark., 2018).

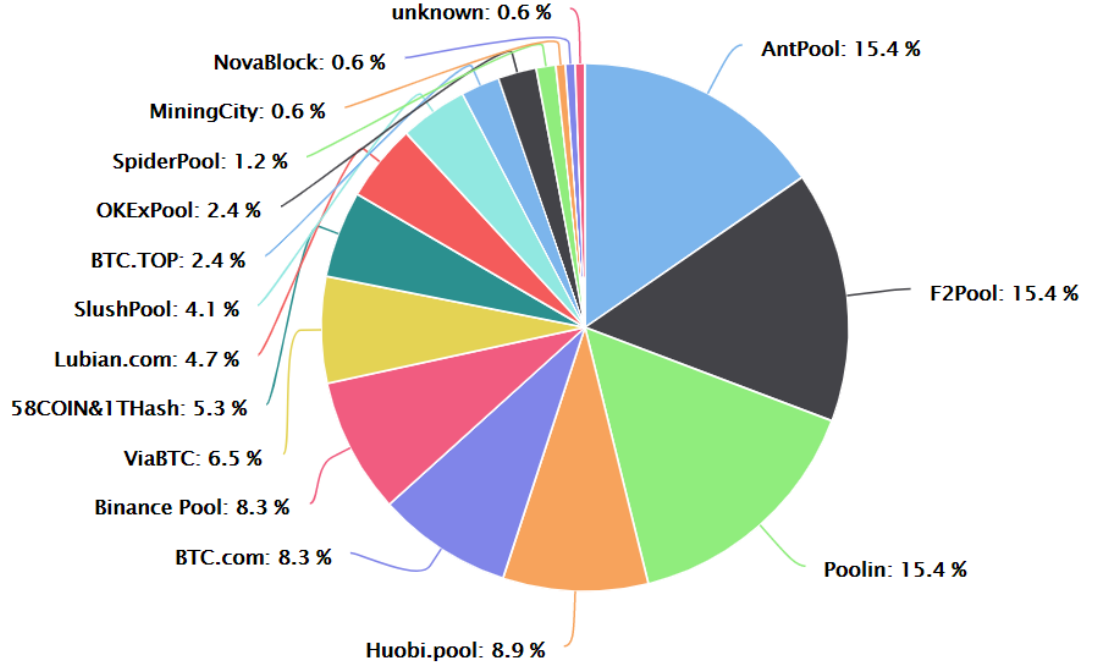
Bir blok zinciri ağındaki kullanıcı sayısı artması ağın güvenliğini ve kaydedilen işlemlerin sayısını artırmaktadır. Kaydedilen işlemlerin sayısı arttıkça büyük depolama kapasitesi gerekme ve tüketilen enerji miktarı artmaktadır. 30 Mart 2019 tarihi itibarıyla Bitcoin ağı ile ilgili tahmin edilen yıllık elektrik tüketimi 77.78 terawatt/ saattir. Bu miktar yaklaşık olarak 7 milyon Amerikan hanesinin ve Şili gibi bazı ülkelerin elektrik tüketimine ve dünyanın elektrik tüketiminin %0,35’üne eşittir (Digiconomist, 2019). Bu yüzden uygulamaların Bitcoinde kullanılan iş ispatı (PoW)

mutabakat algoritması yerine daha az enerji tüketimine sebep olan mutabakat algoritmaları kullanmalarına ihtiyaç duyulmaktadır.

Ağdaki işlem gücünün %51'ine ve daha fazlasına sahip olan kişi veya kişiler blok zincirin kontrolünü ele geçirebilirler. Ağda kötü niyetli kişiler tarafından ağın hesaplama gücünün yarısından fazlasına sahip olunması durumuna %51 saldırısı denmektedir. Ağın %51 ve daha fazla işlem gücünü elinde bulunduran kişi veya kişiler hangi bloğun geçerli olup olmadığına karar verebileceklerdir. Bu kişiler zinciri manipüle edebilir, hileli işlemleri ekleyebilir, mükerrer harcama yapabilir hatta ağdaki diğer kişilerden varlık çalabilirler (Xu, 2016:5). Kötü niyetli madenciler eski bloklardaki verileri değiştiremeseler bile, böyle bir durumun meydana gelmesi blok zincirin bütünlüğünü etkileyecek ve ağa olan kamuoyu güveni sarsılacaktır.

Teknolojideki endişe unsurlarından biri diğeri merkezi olmayan yapısı ile ters düşen madenci havuzlarının oluşumudur. İş ispatı algoritmasında, bir madencinin blok üretebilmesi madencinin çalışmasına veya hesaplama gücüne bağlıdır. Bu yüzden madenciler daha fazla blok üretebilmek için birlikte hareket edip hesaplama gücünün en fazla olduğu madenci havuzlarını oluşturmak isteyeceklerdir (Lin ve Liao, 2017). Hesaplama gücünü artırmak, blokların doğrulama zamanını etkilemek ve daha fazla ödül kazanmak için madenciler tarafından oluşturulan yapılara madenci havuzları denmektedir (Taş ve Kiani, 2018). Şekil 2.7.1.'de 2 Temmuz 2020 tarihi itibarıyla bitcoin ağındaki madenci havuzlarının dağılımı gösterilmektedir.

Şekil 2.7.1. Bitcoin Madenci Havuzları Dağılımı



Kaynak: BTC.COM, ERİŞİM TARİHİ: 2 TEMMUZ 2020. Havuz Dağılımı, 2020, (Çevrimiçi)
https://btc.com/stats/pool?pool_mode=day, 2 Temmuz 2020

Yukarıdaki dağılıma bakıldığında ağın %50'den fazlasının 4 madenci havuzu tarafından yönetildiği görülmektedir. Bu durum blok zincirinin merkezi olmayan yapısına uygun değildir. Ayrıca elektriğin ucuz olması sebebi ile Antpool, BTC.com gibi madenci havuzları ve pek çok madenci Çin'de yer almaktadır (Young, 2019; Çarkacıoğlu, 2016). Açık ve izin gerektirmeyen ve merkezi olmayan bir ağ olarak, coğrafi olarak daha fazla dağıtılmış hesaplama gücüne sahip olmasının daha olumlu olacağı düşünülmektedir. (Young, 2019).

Blok zinciri teknolojisi için gelecekte tehdit oluşturacak bir unsur ise kuantum bilgisayarların gelişimidir. Blok zincirinde güvenliği sağlayan en önemli unsur kullandığı şifreleme algoritmalarıdır ve günümüzde blok zincirde kullanılan şifreleme algoritmaları çok güçlü olarak kabul edilmektedir. Ancak ileride kuantum bilgisayarların kullanımının yaygınlaşması ile bugün kullanılan şifreleme yöntemlerinin kırılabileceği düşünülmektedir (Federov, Kiktenko ve Lvovsky, 2018). Bu durum şuan için bir problem ya da risk arz etmese de ileride blok zinciri uygulamaları için önemli risk taşıyacağı öngörülmektedir.

Karşılaşılan bir diğer zorluk ise anahtar yönetimidir. Blok zinciri teknolojisi asimetrik şifreleme yöntemini kullandığı için, kullanıcıların açık ve kapalı olmak üzere iki anahtarı bulunmaktadır. Bu özel anahtarlar verilerin gizliliğinin koruduğu için çok iyi bir şekilde saklanması gerekmektedir. Özel anahtar saklama sorumluluğu ise tamamıyla kullanıcıya aittir. Ancak bu özel anahtarın kaybedilmesi ya da şifresinin unutulması durumunda işlemlerin kime ait olduğunu doğrulayacak bir bilgiye de erişim mümkün değildir. Bu nedenle bu anahtarların kaybedilmesi ilişkili varlığın da kaybedilmesi anlamına gelmektedir (Usta ve Doğantekin, 2018:96).

Teknolojinin bir başka sorunu, günümüzde blok zinciri teknolojisi ile ilgili bir yasa ya da standart bulunmamasıdır. Bu sebeple merkezi bir otoritesi olmayan bu ağda hatalı bir işlem yapıldığından ya da gizli anahtar şifreleri unutulduğunda kime başvurulacağı, ya da nasıl bir yol izleneceği konuları belirsizdir.

Teknolojinin içerdiği deneyselliğin getirdiği risk bir başka sorunu oluşturmaktadır. Blok zincirinin çalışması için güvenilir kurumların varlığı gerekmesede, blok zincirin altında yatan kodlara ve bu kodları yazan kişilere olan güvene gerçekten ihtiyaç vardır (Al-Saqaf ve Seidler, 2017). Blok zinciri çok yeni bir teknoloji olduğu için yapılan her çalışma genel olarak “deney” olarak adlandırılmakta ve özellikle açık blok zinciri platformlarında öngörülemeyen yazılım hataları siber saldırılara davetiye çıkarmaktadır. Bu açıklar tespit edildiğinde ciddi ekonomik kayıplar yaşanabilmektedir. (Usta ve Doğantekin, 2018:98)

Blok zinciri teknolojisinden maksimum verim elde edilebilmesinin önündeki, bir başka engel, farklı ekosistemlerdeki blok zinciri uygulamalarının birlikte çalışabilmesindeki güçlüttür. Birlikte çalışılabilirlik (interoperability) farklı blok zinciri sistemleri veya ağlarının aralarında bilgi paylaşımı yapabilmesidir. Blok zinciri teknolojisinin kullanımı arttıkça ve geliştikçe farklı blok zinciri uygulamaları da artmaya başlamıştır. Örneğin, GitHub’da, farklı platformların yanı sıra çeşitli programlama dilleri, mutabakat mekanizmaları, protokoller ve gizlilik özellikleri kullanan 6.500'den fazla aktif blok zinciri projesi bulunmaktadır (Monrat, Schelen ve Andersson, 2019). Başka bir deyişle bir blok zinciri içinde yaratılan bir varlığın başka bir blok zinciri içinde de değeri olması demektir. Interoperability, bir blok zinciri için kullanılan para birimini kripto para borsalarında satın sonra başka bir blok zinciri üzerindeki para birimini almak yerine, blok zinciri sistemleri arasında geçiş yapmak

anlamına gelmektedir (Sert, 2019). Bir kişini bitcoinlerini ether ile değiştirmek istemesi buna örnek gösterilebilir. Blok zinciri teknolojisi kabul edilen bir teknoloji olmaya başladıkça birlikte çalışılabilirlik konusu dikkat edilmesi gereken bir konu olmuştur (Koens ve Poll, 2019). Birlikte çalışılabilirlik aracı kurumlar olmadan insanların farklı blok zinciri ağlarındaki bilgileri görebilmesini ve erişebilmesini kolaylaştırmaktadır. Bu durum tam anlamıyla merkezi olmayan sistemlerin gelişimi ile sonuçlanmaktadır. Birlikte çalışabilirlik, kullanıcının tek bir platformda ve platformlar arasında 'Gördüğüm şeyin senin gördüğün ile aynı olduğunu biliyorum' konusunda güvenmesini sağlamaktadır (Hewett, Gogh ve Pawczuk, 2020).

Birlikte çalışılabilirlik, blok zinciri çözümleri oluşturmakla ilgilenen karar vericiler için en büyük endişe kaynağıdır. Kuruluşlar, gelecekte işbirliği seçeneklerini sınırlandırabilecek bir blok zinciri platformunda kendilerini bulmak istememektedir. Gerekirse hem işletme hem de genişletilmiş ekosistemle birlikte büyüyecek ölçeklenebilir çözümler oluşturmak istemektedirler. Birçok kuruluş, farklı çözümleri değiştirme veya bunlara bağlanma konusunda esnek kalmak istemektedir (Hewett, Gogh ve Pawczuk, 2020). Dört büyük denetim firmasından bir diğeri olan PwC'nin yaptığı bir araştırmaya göre, ankete katılan kişilerin %41'i farklı blok zincirlerin birlikte çalışılabilirliği olmadığı için bu teknolojinin kabul görmesinin önündeki engellerden biri olarak görmektedir (PwC, 2018).

2.8.Blok Zinciri Teknolojisinin Günümüzdeki Durumu ve Geleceği

Harvard Üniversitesi profesörlerinin (Iansiti ve Lakhani, 2017) yapmış olduğu araştırmaya göre günümüze kadar gelen sürede yaşanan yıkıcı ya da devrimsel nitelikte sayılabilecek teknolojik gelişmelere bakıldığında, temelde iki ortak özellik bulunmaktadır. Bunlardan ilki yenilik (novelty) diğeri ise karmaşıklılıktır (complexity). Yenilik, bir uygulamanın dünya için yenilik derecesidir. Geliştirilen uygulama kullanıcılar için ne kadar yeni ise, o uygulamanın hangi sorunları çözeceğini ya da neler getireceğini anlamak için harcanan çaba da o kadar fazla olmaktadır. İkinci özellik olan karmaşıklık ise, söz konusu teknoloji ile değer üretebilmek için birlikte çalışması gereken tarafların sayısını ve çeşitliliğini ifade etmektedir.

Şekil 2.8.1. Teknolojilerin Adaptasyon Süreci



Kaynak: Lakhani, K. R., & Iansiti, M. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), 119-127.

Şekil 2.8.1.'de temel teknolojilerin adaptasyon süreci 4 aşamadan oluşmakta ve her bir aşama yenilik ve karmaşıklık boyutları ile tanımlanmaktadır. İlk önce yenilik ve karmaşıklık seviyesi düşük olan uygulamalar kabul görmekteyken, yenilik ve karmaşıklık seviyesi yüksek olan uygulamaların gelişmesi on yılları almaktadır. Adaptasyon sürecinin aşamaları ise sırası ile singel use (tek uygulama), localization (tek bir alan), transformation (dönüşüm) ve substitution (yerini alma, ikame etme)'dir.

İlk aşama olan tek uygulama, teknolojinin sadece tek bir uygulama ile kullanıldığı aşamayı ifade etmektedir. Bu aşamada yeniliğin ve karmaşıklığın daha az olduğu uygulamalar yer almaktadır. Örneğin blok zinciri teknolojisindeki Bitcoin uygulaması bu aşamada yer almaktadır. Çünkü bu teknoloji bitcoinin ortaya çıkışı ile dünyanın ilgisini çekmeye başlamıştır. Bitcoinin uygulama alanı ise alternatif bir ödeme aracı olarak kullanılmasıdır. Bu uygulama internetin ilk çıktığı zamanlarına benzetilebilmektedir. İnternet teknolojisi de ilk ortaya çıktığı zamanlarda e-posta uygulamasını kullanarak telefon, faks gibi iletişim araçlarına alternatif olarak, tek uygulama alanına yönelik bir uygulama olarak karşımıza çıkmıştır.

İkinci aşama olan tek alan ise yenilik açısından yüksek ancak hemen bir değer yaratabilmek açısından sınırlı sayıda kullanıcıya ihtiyaç duyan teknolojik gelişmeleri temsil etmektedir. İhtiyaç duyulan katılımcı sayısı az olduğu için bu aşamada yer alan

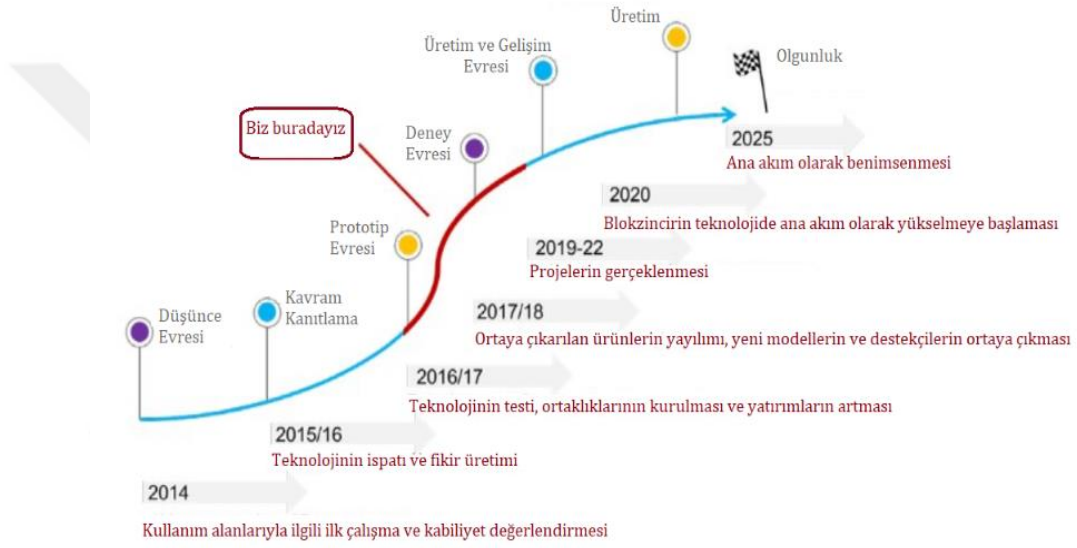
uygulamaların benimsenmesini sağlamak kolaydır. Blok zinciri teknolojisi bitcoin uygulamasından sonra finans sektöründe yaygınlık göstererek tek kullanımlık bir uygulamadan çıkıp artık belirli bir sektöre yönelmiştir. Blok zincirin, finans sektöründe sadece ödeme işlemlerine alternatif olarak değil bankalar ve ülkeler arası mutabakat, menkul kıymet alımı, ticaret finansmanı ve döviz gibi kâğıt kullanımı ve manuel olarak gerçekleştirilen işlemlerin yerini alması beklenmektedir.

Üçüncü sırada olan yerine geçme aşamasındaki uygulamalar daha önceki tek bir alana veya sektöre yönelik olan uygulamaların üzerine inşa edildiği için yenilik derecesi düşükken, bu uygulamaları kullanan kişi sayısı arttığı için katılımcılar arasında ihtiyaç duyulan koordinasyon ve uygulamalardaki karmaşıklık fazladır. Bu aşamadaki uygulamalar mevcut iş yapış şekillerini tamamiyle değiştirmeyi hedeflemektedir. Bu aşamadaki uygulamalar için verilecek en belirgin örnek ise kripto para birimleridir. Kripto paralar sadece ödeme işlemleri ya da finans sektörü için değil, parasal işlem yapmak zorunda olan tüm tarafların kripto paralara uyum sağlamasını gerektirmektedir. Bu durumda devletlerin ve diğer kuruluşların da buna uyum sağlaması beklenmektedir. Bu durum günümüzde bu işlemleri yapan kuruluşlara ve devletlere bir meydana okuma olarak da görülmektedir. Aynı zamanda tüketicilerin de davranışlarını değiştirmesi ve bu kripto paraların fonksiyonlarını, nasıl çalıştığını ve nasıl uygulanacağını anlaması gerekmektedir.

Dördüncü aşama ise dönüşümdür. Bu aşamadaki uygulamalar yüksek derecede yenilik ve katılımcı sayısının oldukça fazla olması sebebiyle karmaşıklığın ve koordinasyona olan ihtiyacın fazla olduğu uygulamalardır. Bu uygulamalar tamamiyle sosyal ve politik sistemlerin yapısını değiştirebilecek uygulamalardır. Blok zinciri teknolojisinde ise bunun en belirgin örneği akıllı sözleşmelerdir. Akıllı sözleşme uygulamasında daha önceden taraflar arasında müzakere edilmiş koşullara göre otomatik ödemelerin ve para veya diğer varlık transferlerinin gerçekleşmesi sağlanmaktadır. Akıllı sözleşmeler gerçekleşirse geleneksel şirket yapıları kökten bir değişime uğrayacak, iş süreçleri, avukatların, muhasebecilerin ve aracı kurumların rolleri değişecektir.

Şekil 2.8.2.'de Blok zinciri teknolojisinde günümüzde hangi aşamada olduğumuz görülmektedir. Credit Suisse'nin 2018 yılında hazırlamış olduğu rapora göre blok zinciri teknolojisinin gelişimi doğrusal bir yapıdan oldukça uzaktır. Günümüzde bulunduğumuz nokta ise blok zinciri projeleri ile ilgili haberlere ve başarılarla olan bakış açısının, özellikle bitcoin ve kripto para uygulamaları ile karşılaştırıldığında, yumuşadığı görülmektedir.

Şekil 2.8.2. Blok Zinciri Gelişim Süreci-Mevcut Durum



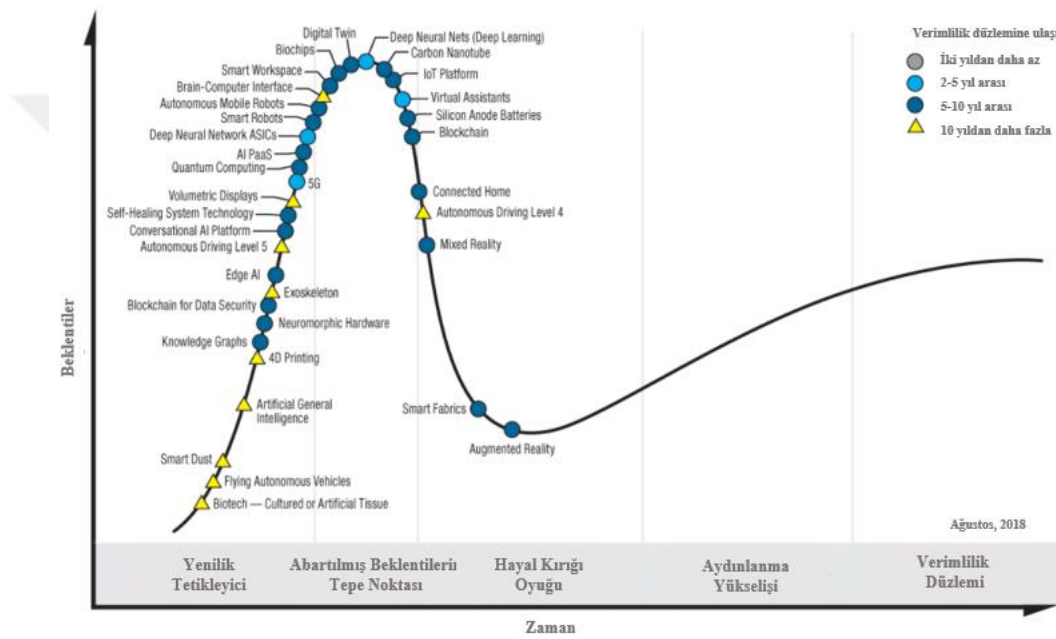
Kaynak: TÜBİTAK BİLGEM BLOK ZİNCİR ARAŞTIRMA LABORATUVARI:2018, Blokzincir, (Çevrimiçi) <https://blokzincir.bilgem.tubitak.gov.tr/bz-calistay/blok-zincir.html>, 25 Mayıs 2020

Dünyanın en büyük araştırma, danışmanlık ve bilgi teknolojisi şirketinden biri olan Gartner tarafından her yıl yeni çıkan teknolojilerin olgunluk, benimsenme ve sosyal uygulama sürecini anlatan bir grafik hazırlanmaktadır. Bu grafiğe göre hayatımıza yeni giren teknolojilerin 5 aşamadan oluşan bir kabul süreci vardır. Bunlar sırasıyla yenilik tetikleyici (innovation trigger), abartılmış beklentilerin tepe noktası (peak of inflated expectations), hayal kırıklığı oyuğu (trough of disillusionment), aydınlanma yükselişi (slope of enlightenment) ve verimlilik düzlemidir (plateau of productivity).

Şekil 2.8.3.'te Gartner tarafından hazırlanan 2018 yılına gelişmekte olan teknolojilerin gelişim grafiği (Hype Cycle for Emerging Technologies) yer almaktadır.

Bu grafiğe göre önümüzdeki 5 ile 10 yıl içinde blok zinciri beklentilerin en tepede olduğu noktadan verimlilik düzlemi aşamasına doğru ilerleyecektir. Bu durum blok zinciri teknolojisi ile ilgili gerçek hayat uygulamalarının oluşturma çabalarının devam ettiğini göstermektedir. Ayrıca Gartner, 2025'e gelindiğinde, blok zinciri tarafından yaratılan iş değerinin 176 milyar dolardan biraz daha fazla olacağını, 2030'a kadar ise 3.1 trilyon doları aşacağını öngörmektedir (STAMFORD, C.:2019a).

Şekil:2.8.3. Gelişmekte Olan Teknolojilerin Gelişim Grafiği, 2018



Kaynak: Panetta K.:2018, 5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018, August 16, 2018, (Çevrimiçi) <https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/>, 21 Mayıs 2020.

Tablo 2.8.1.'de ülkelerin ve uluslararası örgütlerin blok zinciri teknolojisine karşı olan tutumları kripto paralar ile karşılaştırılmıştır. Kripto paralara karşı genel olarak olumsuz ya da tarafsız bir yaklaşım vardır. Ancak, Türkiye dahil olmak üzere, ülkelerin genel olarak blok zinciri teknolojisine karşı olumlu bir tavır sergilediği görülmektedir. Sadece Rusya olumlu ya da olumsuz bir görüş vermemiş, tarafsız kalmıştır. Finansal İstikrar Kurulu (Financial Stability Board- FSB), Uluslararası Menkul Kıymet Komisyonları Örgütü (International Organization of Securities Commissions- IOSCO), Uluslararası Para Fonu (International Monetary Fund- IMF), Dünya Bankası ve Dünya Borsalar Federasyonu (World Federation of Exchanges- WFE) blok zinciri teknolojisine olumlu yaklaşırken, Uluslararası Ödemeler Bankası

(Bank for International Settlements-BIS), Mali Eylem Görev Gücü (Financial Action Task Force-FATF) ve Uluslararası Standartlar Teşkilatı (International Organization for Standardization- ISO) ise tarafsız kalmışlardır.

Tablo 2.8.1. Kripto Paralar ve Blok Zinciri Teknolojisine olan Yaklaşım

Ülkeler	Kripto Paralar	Blok Zinciri Teknolojisi
Çin	Olumsuz	Olumlu
Hindistan	Olumlu	Olumlu
Japonya	Olumlu	Olumlu
Birleşik Krallık	Tarafsız	Olumlu
Fransa	Tarafsız	Olumlu
Avustralya	Tarafsız	Olumlu
Rusya	Olumsuz	Tarafsız
Orta Doğu ve Kuzey Afrika	Olumlu	Olumlu
Türkiye	Tarafsız	Olumlu
Singapur	Tarafsız	Olumlu
Kanada	Tarafsız	Olumlu
Uluslararası Örgütler	Kripto Paralar	Blok Zinciri Teknolojisi
FATF	Olumsuz	Tarafsız
FSB	Tarafsız	Olumlu
IOSCO	Tarafsız	Olumlu
BIS	Olumsuz	Tarafsız
IMF	Olumlu	Olumlu
Dünya Bankası	Tarafsız	Olumlu
ISO	Tarafsız	Tarafsız
WFE	Olumlu	Olumlu

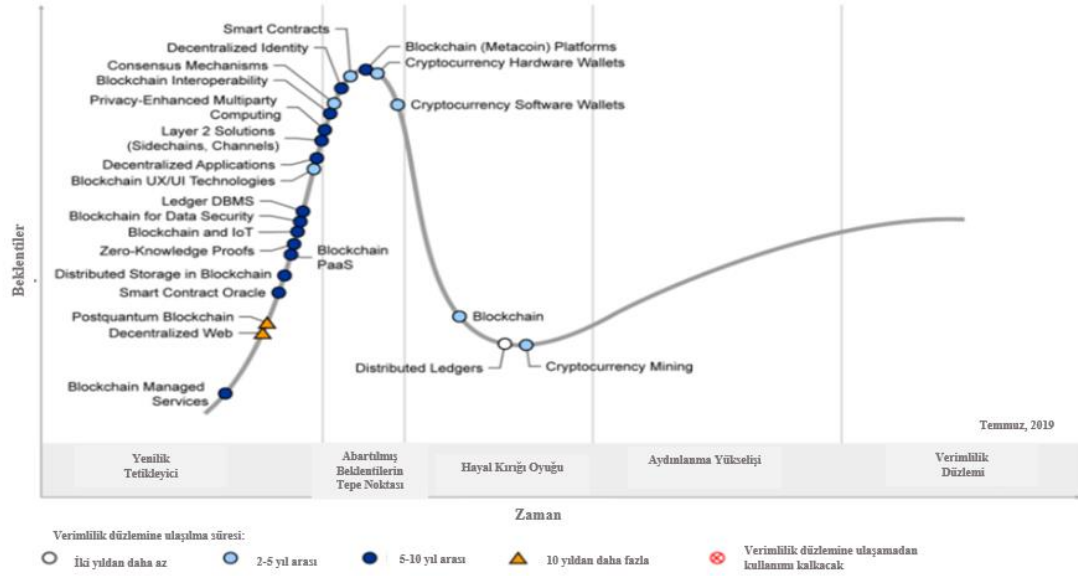
Kaynak: AKGİRAY, V.:2019. The Potential for Blockchain Technology in Corporate Governance. OECD Corporate Governance Working Papers No.21.

Dünya'nın önde gelen danışmanlık şirketlerinden biri olan Accenture'nin 2019 yılında yayınladığı rapora göre şirketlerin uzmanlaşması gerektiği 4 teknoloji

bulunmaktadır, bunlar dağıtık defter teknolojisi, yapay zekâ (Artificial Intelligence-AI), genişletilmiş gerçeklik (extended reality- XR) ve kuantum bilişimdir (quantum computing). Yapılan araştırmaya göre blok zinciri alanında pilot uygulamaya başlayanların ya da başlamayı düşünen şirketlerin oranı %50'dir. Dağıtık defter teknolojisine yapılan yatırımlarda patlama olduğunu, blok zinciri ve kripto para birimi odaklı yeni girişimlerin sadece 2018'in ilk üç çeyreğinde yaklaşık 3,9 milyar dolarlık yatırım topladığını belirtmiştir. Bu rakam 2017 yılındaki toplamının neredeyse üç katıdır (Accenture, 2019).

Şekil 2.8.4.'teki Gartner'ın 2019 yılında Blok Zinciri Teknolojileri Beklenti Döngüsü Grafiği 'ne göre blok zinciri teknolojilerinin dönüştürücü bir etkisinin olması için 5 ile 10 yıl gerekmektedir. Gartner'da analist ve araştırma başkan yardımcısı olan Avivah Litan, blok zinciri teknolojilerinin henüz beklentilere ulaşmadığını, birçok kurumsal blok zinciri projesinin deneme aşamasında kaldığını ve blok zincirinin henüz kurumsal bir ekosistemde dijital iş devrimini sağlayamayacağını belirtmiştir. Ayrıca Gartner blok zinciri teknolojisini teknik ve operasyonel olarak tamamen ölçeklenebilir olmasını en az 2028 yılına kadar beklememektedir. Blok zinciri teknolojisinin ana akım haline gelmesi için kullanıcıların doğru platformu, doğru akıllı sözleşme dilini, doğru sistem ara yüzlerini ve doğru mutabakat algoritmalarını seçme konusunda endişelerinin olmaması gerekmektedir. Bununla birlikte kullanıcıların, projeleri için farklı blok zinciri platformları kullanan iş ortaklarıyla birlikte nasıl çalışacağı konusundaki endişeler giderilmelidir (STAMFORD, C.:2019b).

Şekil 2.8.4. Blok Zinciri Teknolojileri Beklenti Döngüsü Grafiği, 2019



Kaynak: STAMFORD, C.:2019b Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact, October 8, 2019, (Çevrimiçi) <https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-fromtransformational-impact>, 21 Mayıs 2020.

Gartner gibi bir araştırma şirketi olan, bilgi teknolojisi, telekomünikasyon ve tüketici teknolojisi pazarları için danışmanlık hizmetleri sunan International Data Corporation (IDC), 2018 ve 2022 yılları arasında blok zinciri harcamalarının %76 beş yıllık bir bileşik yıllık büyüme oranını ve 2022 yılında toplam 12.4 milyar dolar harcama ile hızlı bir şekilde büyüyeceğini tahmin etmektedir (Framingham, 2019).

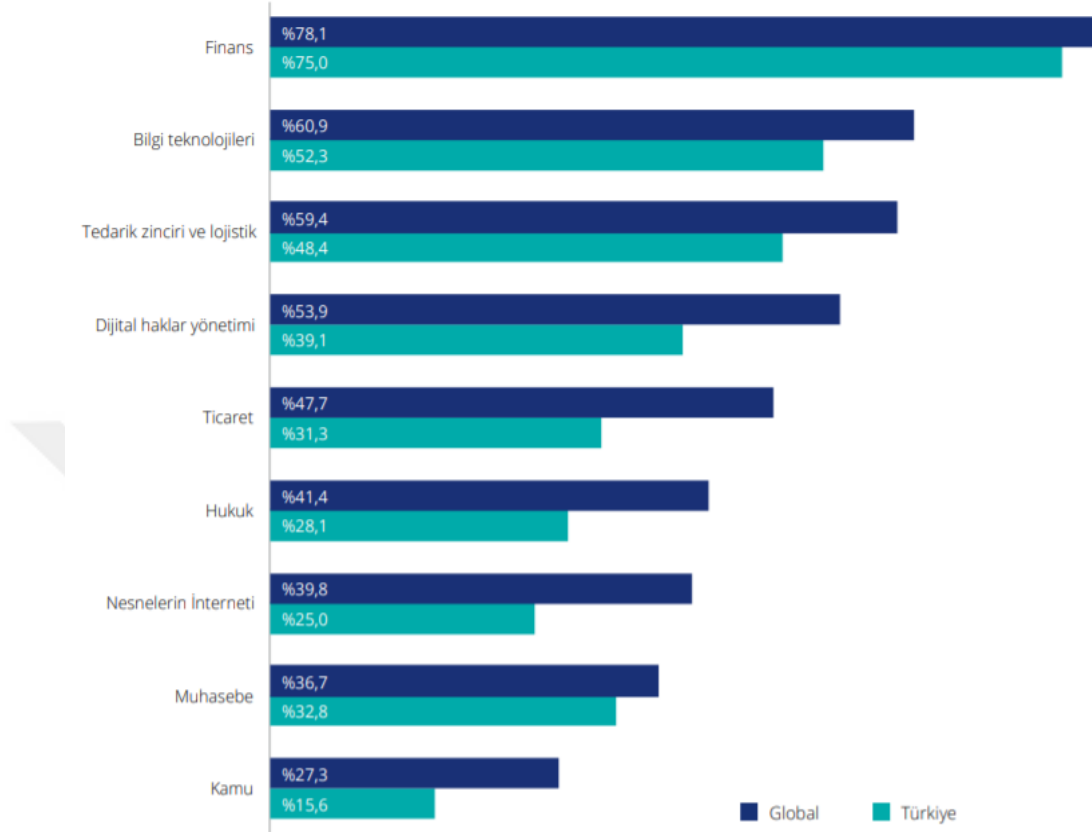
Blok zinciri teknolojisinin 2009 yılından günümüze kadar geçirmiş olduğu evreler üç alanda kategorize edilmiştir. Bunlar Blok Zinciri 1.0, Blok Zincir 2.0 ve Blok zinciri 3.0'dır (Swan, 2015). Blok zincir 1.0. paranın ve ödemelerin merkezi olmayan halini temsil etmektedir. En önemli uygulaması ise Bitcoin'dir. Blok zinciri 2.0. ise ödeme ve para transferleri dışındaki kredi işlemleri, vadeli işlemler ve sözleşmeler gibi daha karmaşık finansal işlemleri ve faaliyet alanlarını kapsamaktadır. Ödeme takas sistemi ve banka kredi bilgi sistemleri, blok zinciri uygulamasının uygun senaryoları olarak gösterilmektedir. Bunları gerçekleştirebilmek için akıllı sözleşmeler kullanılmıştır. En bilinen platform ise Ethereum'dur. Blok zinciri 3.0. ise sektörlerin ya da pazarların merkezi olmayan halini temsil etmektedir. Finans sektörü dışında, sağlık, eğitim, emlak, enerji gibi diğer alanlarda da blok zinciri kullanımını ifade etmektedir.

2.9.Blok Zinciri Teknolojisinin Uygulama Alanları

Blok zinciri teknolojisinin sahip olduğu özellikler sebebi ile birçok sektörün iş yapış şeklini değiştireceği öngörülmektedir. Kripto paraların ortaya çıkışı ile ilk olarak bankalar ve finans sektörünün ilgisini çekse de, günümüzde birçok sektör blok zinciri teknolojisinin gelecekteki potansiyeli ile ilgilenmeye başlamıştır. Bu teknolojinin kurumlar tarafından kullanılma talebi arttıkça IBM, Microsoft, Amazon ve Hewlett Packard (HP) gibi şirketler müşterilerine “Blockchain as-a-Service (BaaS)” hizmetlerini verme konusunda yetkinlikleri arttırmaktadır (Deloitte ve TÜSİAD, 2018).

Şekil 2.9.1.’de, Deloitte ve Türk Sanayicileri ve İş İnsanları Derneği (TÜSİAD)’nin (2018) “Blokzincir Potansiyelinin Keşfi” konulu hazırlanan rapor ve araştırma sonuçlarına göre araştırmaya katılan yöneticiler %78,1 gibi oranla blok zinciri teknolojisinin en çok finans alanında etki göstereceğini öngörmektedir. Yapılan anket sonuçları ile Deloitte’in yine 2018 yılında küresel blok zinciri anketi karşılaştırıldığında Türkiye’deki araştırma sonuçları ile benzer olduğu görülmüştür. Ancak bununla birlikte Türkiye’deki sektörlerin blok zinciri teknolojisinden daha az etkileneceği görülmüştür.

Şekil 2.9.1. Blok Zinciri Teknolojisinden En Fazla Etkileneceği Düşünülen Alanların Dağılımı



Kaynak: DELOITTE, TÜSİAD.:2018,Blokszincir Potansiyelinin Keşfi 2018 Yılı Türkiye Blokszincir Araştırması., (Çevrimiçi)

<https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/consulting/blokszincirpotansiyelinin-kesfi.pdf>, 1 Mayıs 2020.

Özellikle aracı üçüncü taraflara ihtiyaç olmaması, şeffaflık ve işlemlerin takibi, düşük işlem maliyetleri ve geçmişte kaydedilen işlemlerin değiştirilememesi blok zincirin sunmuş olduğu temel faydalarıdır. Bankacılık ve finans sektörünün dışında, sağlık, lojistik, emlak sektörü ve muhasebe blok zinciri teknolojisi ile değişmesi beklenen başlıca sektörlerdir.

2.9.1. Lojistik ve Tedarik Zinciri

Günümüz tedarik zinciri yapısında üreticiden tüketiciye giden ürünlerin akışında karmaşık bir yapı bulunmaktadır. Çiftçi (üretici), dağıtıcı firmalar, satış yapan firmalar kendi iş akışında yoğunlaşmış ve birbirinden bağımsız sistemlerde çalışmaktadırlar. Bu durum birbirleri ile iletişim kurarken hem çok fazla zaman

kaybına hem de kullanılan dokümantasyonu artırmaktadır. Bu yüzden günümüz tedarik zinciri yapısı firmalar için verimliliği azaltan, kontrolü zor bir süreçtir. Blok zinciri teknolojisi kullanılarak, ürünün üretiminden satışına kadar geçen sürede her el değiştirmesi kalıcı bir şekilde blok zincirinde takip edilebilir ve belgelenebilir.

Blok zinciri teknolojisini kullanarak tedarik zincirindeki şeffaflığı ve takip edilebilirliği en iyi kullanan uygulamalardan biri IBM'in geliştirmiş olduğu IBM Food Trust (IBM Gıda Güvenliği) blok zinciri uygulamasıdır. Bu uygulama Hyperledger Fabric kullanılarak hayata geçirilmiştir. IBM'in gıda güvenliğinin takibini yapabilmek için geliştirdiği bu blok zinciri uygulaması birçok büyük şirket ile iş birliği yapmıştır. Walmart, Nestle, Unilever, and Tyson. Carrefour, Dole Food, Driscoll's Inc. Golden State Foods, Kroger ve Tyson Foods gibi büyük gıda marketleri bu uygulamanın üyelerindendir.

Walmart'ın gıda güvenliğinden sorumlu önceki başkan yardımcısı Yannis (2018) durumu şu şekilde açıklamıştır: *Satın aldığımız bir gıdadan dolayı zehirlendiğimiz zaman bunun sebebinin neyden kaynaklandığını anlamamız çoğu zaman bir günden fazla sürebiliyor. Eğer bu olayı araştıranlar bunun hangi toptancıdan ya da çiftçiden kaynaklandığını bulamazlarsa ya o bölgedeki satılan gıdalardan uzak durulmasını ya da komple o ürünün alınmamasını tavsiye etmektedirler. Böyle bir durum söz konusu olduğu zaman ilgili ürün tüm mağazalardan kaldırılmakta ve çöpe atılmaktadır. Tüketicilerin de o ürüne dair güvenleri kalmamaktadır. Ancak satılan ürünler daha iyi bir şekilde izlenebilirse zararlı ürünü üreten üreticiyi tespit ederek diğer üreticileri koruyabilir ve çözümler konusunda hızlı hareket edebiliriz.*

Amerika'da 2018 yılında ıspanaklarda koli basili bakterisi bulunmuş ve çok sayıda kişi gıda zehirlenmesine yakalanmıştır. Blok zinciri teknolojisi ile bakterinin nerden geldiği tespit edilebilecek ve o bölgedeki diğer sebzeler de inceleme altına alınabilecektir. Walmart sadece yeşil yapraklı sebzelerin takibini değil diğer ürünlerin de takibi konusunda blok zinciri teknolojisini kullanmaktadır. Bunlardan bir tanesi Amerika'daki marketlerinde satılan mango meyvesinin takibi, diğeri ise Çin'deki marketlerinde satılan domuz etinin takibidir.

Yannis, Walmart'ta satılan bir mangonun nerede üretildiğini öğrenmek istemiş ve bunu ekibinden rica etmiştir. Çalışanlar tedarikçileri ve dağıtıcı firmaları arayarak ve e-posta ile ulaşarak yedinci günün sonunda cevap alabilmişlerdir. Blok zinciri teknolojisi kullanılmaya başlandığından beri mangonun takibi 7 günden 2 saniyeye düşmüştür (Hyperledger, 2019). Walmart, yeşil yapraklı sebzeleri satın aldıkları 100'den fazla tedarikçiden ürünleri ile ilgili detayları blok zincirine yüklemelerini istemiş ve ilerleyen yıllarda da izlenebilir ürün sayısını arttırmayı planlamaktadır.

2.9.2. Emlak ve Tapu Kayıtları

Gayrimenkul işlemleri, komisyoncular, devlet veri tabanları, tapu ve kadastro işlemleri, müfettişler ve değerlendirme uzmanları, noterler gibi çeşitli araçların katılımı nedeniyle hantal, şeffaflıktan uzak ve pahalıdır. Blok zinciri, her mülkün, her yerde, iskânını, mali durumunu, yasal durumunu, bina performansını ve fiziksel özelliklerini içeren ve tüm geçmiş işlemlerini sürdüren ilgili bir dijital adrese sahip olmasını sağlayacaktır (Puthal ve ark., 2018). Ayrıca fiziksel ortamda saklanan belgelerin kaybolması durumunda sahip olunan taşınmazlar üzerinde kimin hak sahibi olduğu bir bilinmeze girmektedir. Her ne kadar günümüzde e-devlet sisteminde bu bilgiler kaydedilip takip edilse de kayıtların merkezi bir yerde saklanması kayıtlar üzerinde oynanması ve onay dışı değişiklik yapılması günümüzde rastlanan durumlardandır (Usta ve Doğanekin, 2017).

Blok zincirin taşınmazların sahipliğini devretmede daha etkili bir kayıt yöntemi olacağı düşünülmektedir (Veuger, 2018). Alıcı ve satıcı arasındaki devir işlemleri blok zinciri sayesinde daha hızlı gerçekleştirilebilecektir. Alım satım işlemleri blok zinciri teknolojisi ile kaydedilip takip edildiğinde kayıtların birer kopyası ağdaki herkeste olacağı için taşınmazlar üzerinde sahiplik değiştirilemeyecektir. Ayrıca taşınmazın geçmişi hakkında, daha önce kimler tarafından kullanıldığı da sorgulanıp takip edilebilecek ve bu bilgilerin doğruluğundan da emin olunabilecek, tapu kayıtları güvence altına alınacaktır.

Honduras hükümeti, Teksas merkezli olan Factom adlı bir şirketle, Honduras'taki arazi kayıt sistemi ile ilgili kayıt tutma sorunlarını ele almak, kalıcı ve

güvenli bir kayıt sistemi oluşturmak için blok zinciri teknolojisinin kullanımı için anlaştığını bildirmiştir (Chavez-Dreyfuss, 2015).

Brezilya, blok zinciri tapu sicili girişimi olan Ubitquity şirketi ile 2017 yılında Brezilya Tapu Sicili Dairesi ile ortaklaşa bir pilot proje yapacağını duyurmuştur (Suberg, 2017). Projenin amacı, arazi kayıtlarının doğruluğunu, güvenliğini ve şeffaflığını artırırken maliyetleri düşürmeye yardımcı olmak amacıyla bölgenin resmi arazi kayıtları için bir pilot program oluşturmaktır (Lemieux, 2017).

İsveç'te haritalama, tapu ve kadastro otoritesi olan Lantmäteriet (Swedish mapping, cadastre and land registration authority) 2016 yılında, blok zinciri ve akıllı sözleşmelerin gayrimenkul işlemleri için nasıl kullanılabileceğini araştırmaya başlamıştır (Campbell, 2016). Bu çalışma kapsamında danışmanlık firması Kairos Future, telekomünikasyon firması Telia Şirketi ve bir İsveç blok zinciri teknoloji şirketi olan ChromaWay ile de ortaklık kurmuştur. Mülk satın alma süreci, ipotek tapu devirleri ve kayıtları korumak için blok zinciri teknolojisini kullanarak, gerçek zamanlı güncellemeler yapabilecek ve arazi mülkiyeti doğrulamayı basitleştirerek, emlak sahtekârlığını ve yasadışı arazi elde etmeyi durdurabilecektir.

2.9.3. Sağlık Hizmetleri

Hastaneler, doktorlar, hastalar, eczaneler, ilaç tedarikçileri gibi birden fazla tarafın olduğu sağlık sektöründe blok zinciri kullanımının bilgilerin gizliliğini, güvenliğini ve şeffaflığını attıracağı beklenmektedir. Günümüzde, hastalar için önemli sağlık kayıtları farklı kurumlarda farklı sistemler arasında kaydedilmektedir. Kayıtların farklı sistemlerde tutulması hasta bilgilerinin kurumlar arası entegrasyonuna engel olmakta, aynı tetkiklerin farklı kurumlarda defalarca yapılmasına sebep olmaktadır. Ayrıca bu merkezlerin hastaların verilerini yeterince koruyamadığı için, hasta mahremiyetinin ihlali de meydana gelmektedir (Kıyak, Coşkun ve Budakoğlu, 2019). Tüm bunların yanı sıra, ilaç sahtekârlığı da sağlık sektöründeki önemli konuların başında gelmektedir. Sağlık verilerinin birlikte çalışılabilirliği, tıbbi sonuçların incelenmesi, ilaç sahtekârlığının tespiti ve önlenmesi ve maliyetlerin düşürülmesi için blok zinciri kullanımını arttırması beklenmektedir.

Medicalchain uygulaması İngiltere’de hastaların sağlık verilerini kaydedebileceği bir blok zinciri uygulamasıdır. Uygulamanın amacı hastaların sağlık kayıtlarının kendileri ve doktorlar tarafından güvenli, hızlı ve şeffaf bir şekilde değişiminin sağlanmasıdır. Hyperledger platformunu kullanan uygulama, hastaların kendi sağlık kayıtları üzerinde tam kontrole sahip olmasını amaçlamaktadır. Doktorların, hastanelerin, laboratuvarların hastanın sağlık kayıtlarına ulaşabilmeleri için izin almaları gerekmektedir (Medicalchain, 2018a). John Hopkins Üniversitesi tarafından 2016 yılında yapılan bir araştırmaya göre ABD’de hastaların sağlık kayıtlarındaki hatalardan dolayı ölüm oranının, kalp krizi ve kanserden sonra üçüncü olduğu görülmüştür. Bu yüzden Medicalchain’in amaçlarından biri de doktorların hastanın sağlık kayıtlarına ve geçmişine ulaşmasını sağlayarak yanlış tanının önüne geçebilmektir (Medicalchain, 2018b).

MedRec firması sağlık verilerine erişimi blok zinciri üzerinden yapmaya başlamıştır. MedRec, Etheruem akıllı sözleşmeleri kullanarak, sağlık sektöründe hizmet sunan kişileri bir araya getirerek verilerin paylaşımını ve yetkilendirmeyi blok zinciri üzerinden yapılmasına imkân sağlamıştır (Ekblaw ve ark., 2016).

2019 Haziran ayında, Uganda hükümeti sahte ilaçların takibini yapmak ve ilaç sahteciliğinin önleyebilmek için MediConnect blok zinciri şirketi ile işbirliği yapmaya başlayacağını duyurmuştur.

2.9.4. Finans ve Bankacılık

Blok zinciri teknolojisinin finansal hizmetler ekosistemini değiştirme potansiyeli faaliyetleri basitleştirme, düzenleyici ve düzenlenmeye tabi kuruluşlar arasındaki finansal faaliyetlerin gerçek zamanlı izlenmesi, yapılan anlaşmaların dağıtık ve değişmez bir şekilde yürütülerek karşı taraf riskinin azaltılması, takas işlemleri için aracılıktan kaçınma ve varlıkların sahipliği ve sermaye artırımında şeffaflık ve yolsuzluğun en aza indirilmesi konuları dahil olmak üzere geniş çapta tartışılmıştır (Niforos, 2017). Ödeme işlemleri, uluslararası para transferleri, takas yönetimi, hisse senedi alım-satımı, dijital kimlikler yönetimi ve doküman yönetimi gibi alanların finans sektöründe değişim göstereceği öngörülmektedir. Danışmanlık

şirketi olan Capgemini tüketicilerin blok zinciri tabanlı uygulamalarla her yıl bankacılık ve sigorta ücretlerinden 16 milyar dolara kadar tasarruf edebileceğini tahmin etmektedir (Tapscott ve Tapscott, 2017a).

Finansal kuruluşlar bir takım yasal düzenlemelere tabi oldukları için birbirleri ile yaptıkları işlemlerde hem süreler hem de masraflar artmaktadır. Tüm işlemleri kendi merkezi sistemlerinden takip edip kaydetmektedirler. Blok zinciri ile işlem maliyetlerinin düşmesi ve para transfer hızının artması ile birlikte bankalar ve diğer finansal kurumlar bir takım blok zinciri ağlarına dahil olmuştur. Tezin 2.6. Blok Zinciri Platformları bölümünde anlatılan Ripple ve Corda platformu bankacılık ve finans sektörü için kullanılan yaygın uygulamalardandır.

Finans sektörünün içinde dikkati çeken alanlardan birisi de muhasebe ve denetim mesleğidir. İşlemlerin bu yeni deftere kaydedilmesi ile muhasebecilerin ve finansal tablolarını hazırlayan şirketler ile bu tablolardan faydalanan kişiler arasında **“güven”** boşluğunu dolduran denetçilerin blok zinciri teknolojisinden etkileneceği oldukça açıktır. Tezin üçüncü bölümünde blok zinciri teknolojisinin muhasebe ve denetim mesleğine olan etkileri detaylı bir şekilde anlatılmaktadır.

ÜÇÜNCÜ BÖLÜM

MUHASEBE VE DENETİMDE VERİ GÜVENLİĞİ VE BLOK ZİNCİRİ TEKNOLOJİSİNİN BU ALANDA KULLANIMI

Blok zinciri teknolojinin muhasebe mesleğine ve güvence hizmetlerine büyük fayda sağlayacağı ve bu sektörde mevcut olan sistemleri temelden değiştireceği öngörülmektedir. Blok zinciri teknolojisi ile muhasebecinin rolü değişecektir, ancak bu teknoloji muhasebecileri ortadan kaldırmayacaktır. Bilgilerin blok zincirine dahil edilmeden önce doğru şekilde yorumlanması ve sınıflandırılması gerekmektedir. Bunları yapmak, blok zincirini uygulamak ve korumak için muhasebeciye ihtiyaç duyulacaktır. Alacak hesaplarının denetlenmesi; mal ve hizmet ödemelerine ilişkin sözleşmelerin denetlenmesi; fatura hazırlanması; gelir ve giderlerin takip edilmesi gibi işler işletme tarafından yapılmak zorundadır. Blok zinciri teknolojisi ile bile işletmenin sözleşmeleri, satın alma siparişlerini ve ödemeleri bloklara girmesi gerekmektedir. Bu yeni teknolojinin sağladığı, bir muhasebecinin hayali olan verimlilik, kayıtların kalıcı olması ve şeffaflıktır. Bu yüzden bu teknoloji muhasebe mesleği için bir tehdit değil, bir fırsat sunmaktadır (Arnold, 2018).

Merkezi bir mimaride düzenlenen sistemlerden farklı olan blok zinciri, işlemleri doğrulamayı, verileri depolamayı ve organizasyon gücünü bir grup bilgisayara dağıtmaktadır. Blok zinciri teknolojisi, işletmelerin gerçekleştirdikleri işlemleri blok zincirine kaydetmesine izin vererek, değiştirilemeyen muhasebe kayıtlarının oluşmasına imkân sağlamaktadır. Bu işlemler kriptografik yöntemler ile imzalandığı ve dağıtıldığı için işlemlerle oynamak veya onları yok etmek mümkün değildir (Schmitz ve Leoni, 2019).

Açık ya da izin gerektirmeyen blok zincirleri, tüm işlemlerin açıkça erişilebilir olmasını sağlayarak daha fazla şeffaflık sağlayabilirken, müşteri bilgilerinin gizli kalması gereken ortamlar için uygun bulunmamaktadır. Özel ve izin gerektiren blok zincirleri ise, genellikle muhasebe bilgileri için farklı ihtiyaçları olan paydaşlar için farklılaştırılmış erişim oluşturma olanağı sunmaktadır. Muhasebe ve denetimde blok

zinciri teknolojisinin benimsenmesi, bilginin gizliliği ve şeffaflığı arasındaki dengeyi bulmaktan geçecektir (Wang ve Kogan, 2018).

İşletmeler, blok zinciri teknolojisini kullanarak, doğrulanan işlemleri güvenli bir defterde kaydederek yeni muhasebe bilgi sistemlerini üretebileceklerdir. Bu işlemler, yalnızca müşterilerden yapılan tahsilat, bankalara yatırılan nakit gibi iki taraf arasındaki para transferlerini değil aynı zamanda bir şirket içindeki muhasebe veri akışını da içerecektir. Bu tür sistemler, muhasebe bilgilerini yöneticiler, denetçiler, alacaklılar ve paydaşlar gibi ilgili taraflara anında yayınlayarak gerçek zamanlı raporlamaya olanak sağlayacaktır. Ayrıca akıllı sözleşmeler, hesap bilgilerini anında güncelleyerek ve tedarik zincirlerini gerçek zamanlı izleyerek kayıt sürecini hızlandırmada önemli bir rol oynayacaktır (Karajovic, Kim ve Laskowski, 2019:319).

Bir şirketteki insan faktörünün olumsuz etkileri, insanların şirket faaliyetlerindeki karar alma süreçlerine dahil oldukları sürece hep devam edecektir. İnsan faktörünün bu istenmeyen etkileri ise şirket sahipleri ve yöneticilerin çıkar çatışmasını devam ettirecektir. Ancak teknolojideki son gelişmeler ile birlikte insan faktörünün bu olumsuz etkileri ile baş etme fırsatı sağlanmaktadır. Günümüzdeki defter tutma sistemi muhasebeciler için asil-vekil problemi yaratmakta ve işletme yönetiminin amaçlarını en üst düzeye çıkarmak üzere karar almak için kamuoyuna güvenilir bilgi sunma açısından çıkar çatışmasına sebep olmaktadır. Blok zinciri teknolojisi geleneksel merkezi yönetim yapılarındaki asil-vekil ikilemine ve asil-vekil arasındaki iletişimin sağlanması için katlanılan yüksek işlem maliyetlerine çözüm getirerek merkezi olmayan ve anlık olan yapısını güçlendirmektedir. Blok zinciri teknolojisinin getirdiği şeffaflık ile vekâlet probleminin azalacağı, aynı zamanda bilgi asimetrisinin ve ahlaki tehlikenin denetçilerin sürekli güvence sağlama faaliyetleri ile oldukça azalacağı öne sürülmektedir (Chedrawi ve Howayeck, 2018).

Blok zinciri teknolojisinin sermaye piyasaları ve raporlama üzerindeki etkisinin kapsamı, teknolojinin geniş çapta kabul edilmesine ve benimsenmesine bağlı olacaktır. Blok zinciri teknolojisi yaygınlaştıkça hükümetler, düzenleyiciler, finansal kurumlar, işletmeler, muhasebeciler, avukatlar ve teknoloji uzmanları dahil olmak üzere tüm ilgili piyasa katılımcılarının dahil edilmesi gerekecektir (Wunsche, 2016).

Ayrıca, blok zinciri teknolojisinin ortaya çıkışı finansal muhasebeye yeni fikirler getirmektedir. Finansal muhasebede kayıtlara ilk kez alma, ölçme, sunum ve açıklama üzerinde çok ciddi bir etkisi olabilir, dipnot açıklamalarında ve kâr yönetiminde hataları azaltabilir ve buna bağlı olarak bilginin kalitesini arttırabilir ve bilgi asimetrisi sorununu azaltabilir (Yu, Lin ve Tang, 2018).

Blok zinciri teknolojisi bir şirketin muhasebe kayıtlarını doğrulamak için gereken süreyi önemli ölçüde kısaltarak, muhasebecilerin katma değeri olan çalışmalara odaklanmalarına olanak tanımaktadır (Karajovic, Kim ve Laskowski, 2019).

En önemlisi, blok zinciri teknolojisi muhasebede üç taraflı kayıt sistemi için bir fırsat yaratmaktadır. Bu sistem defter tutma güvenilirliğini sağlamak için bir işlemde her taraf tarafından kaydedilen borç ve alacak girişlerini otomatik olarak onaylamaktadır (Karajovic, Kim ve Laskowski, 2019:319).

Tüm bu anlatılanlar çerçevesinde blok zinciri teknolojisinin muhasebe ve denetimde olası kullanım alanları aşağıdaki gibi sıralanabilir (Baron, 2017):

- Takip edilebilen denetim izleri
- Otomatik denetim süreçleri
- İşlemlerin doğruluğunun kanıtlanması
- Varlıkların sahipliğinin izlenebilmesi
- Akıllı sözleşmelerin geliştirilmesi
- Ham maddeden fikri mülkiyet haklarına kadar herhangi bir varlık için kayıt ve stok sistemi

Şekil 3.1.'de ise Dai ve Vasarhelyi (2017)'nin önermiş olduğu Blok Zinciri Tabanlı Muhasebe Ekosistemi gösterilmektedir.

Şekil 3.1. Blok Zinciri Tabanlı Muhasebe Ekosistemi



Kaynak: DAI, J., VASARHELYI, M. A.:2017, “Toward Blockchain-Based Accounting and Assurance”. Journal Of Information Systems, 31(3), 5-21.

3.1.Finansal Raporlama ve Blok Zinciri Teknolojisi

Bu bölümde blok zinciri teknolojisinin ve akıllı sözleşmelerin muhasebe kayıt düzenine etkisi, finansal tabloların raporlanmasındaki olası etkileri ve konu ile ilgili olan test aşamasındaki bazı uygulamalar anlatılmaktadır.

3.1.1.Muhasebede Kayıt Düzeni

Antik medeniyetlerden günümüze kadar gelen sürede finansal olayları kayıt altına alma ihtiyacı hep var olmuş, toplumların gelişmesi, iş yapış biçimlerinin karmaşıklaşması ve teknolojik gelişmelerin artması ile finansal olayları kayıt altına alma ihtiyacı artarak gelişim ve değişim göstermiştir. İlk olarak muhasebede tek taraflı kayıt düzeni ile başlayan bu süreç, sonrasında yerini, günümüzden yaklaşık olarak 600 yıl önce çift taraflı kayıt düzenine bırakmıştır. Günümüzde ise blok zinciri teknolojisinin ortaya çıkması ile muhasebede üç taraflı kayıt düzeni konuşulmakta ve muhasebede çift taraflı kayıt düzenindeki bazı eksiklerin azaltılabileceği düşünülmektedir.

3.1.1.1.Tek Taraflı Kayıt Düzeni

Muhasebe dünyadaki en eski mesleklerden bir tanesidir. Ticaret hayatına dair en eski kayıtların milattan önce Mezopotamya uygarlığına ait olduğu bilinmektedir. Antik medeniyetlerde kullanılan tek taraflı kayıt sistemi hiç gelişim göstermeden bin yıl boyunca varlığını sürdürmüştür (Cai, 2019). Tek taraflı (single entry) kayıt düzenine göre varlıklar bir liste şeklinde yazılarak girişler oluşturulmakta ve her bir girişte tarih, tutar, olayla ilgili bir yorum eklenebilmektedir.

13. yüzyıla kadar yaygın olarak kullanılan tek taraflı kayıt düzeni, olayları tek taraflı kaydetmekteydi. Şekil 3.1.1.1.1.'deki örnekte, 1525 yılına ait bir ders kitabından alınan tek taraflı kayıt sistemi örneği görülmektedir. Sol taraftaki giriş 15 Ocak (15 gennaio) tarihinde 50 kilo (pound) tarçın (Canella) satışı için yapılmıştır. Sağ taraftaki giriş ise borçlu olan Francesco di Giovanni'nin, Antonio Cappello e Luca Vendramin bankasına son ödeme tarihi 20 Ocak olan bir tutarın kısmi ödemesini (10 dukat) göstermektedir. Defter sadece borçlu ve alacaklı hesaplarını içerdiğinden tarçın, nakit veya banka gibi hesaplar kullanılmamaktaydı.

Şekil 3.1.1.1.1. Kontra Giriş için Bir Hesap Göstergesi Olmayan Tek Taraflı Defter

Ser Francesco di Giovanni deve dare addì 15 gennaio, lire 125, soldi 0, per libbre 50 di cannella, al prezzo di soldi 50 la libbra.	L 125	s 0	d 0	Ser Francesco di Giovanni al riscontro deve avere addì 20 gennaio, ducati 10 che egli fece registrare a mio nome nel banco di ser Antonio Cappello e Luca Vendramin per parte delle contrascritte mercanzie.	L 62	s 0	d 0
---	-------	-----	-----	--	------	-----	-----

Kaynak: SANGSTER, A.:2016, The Genesis Of Double Entry Bookkeeping. The Accounting Review, 91(1), syf.304

Bu kayıt düzeninde, kayıt sırasında tutarlarla ilgili bir yanlışlık olduğunda ya da hırsızlık yapıldığında bunun tespit edilmesi oldukça zordur. Meydana gelen olaylar arasında bir bağ kurulamaması ve yararlı bilgi sunmamasından dolayı zaman içerisinde bu kayıt düzeni yerini çift taraflı kayıt düzenine bırakmıştır.

3.1.1.2. Çift Taraflı Kayıt Düzeni

13. yüzyıldan itibaren İtalya’da ticaretin gelişip yaygınlaşması ve sonrasında yaşanan ekonomik ve sosyal gelişmeler ile işletmelerin yapısının karmaşık hale gelmesi, insanların sahip oldukları nakitten daha fazlasını görmek istemelerine sebep olmuştur. Şirket sahipleri, şirketlerin finansal durumu ve performansı ile ilgili daha detaylı bilgilere ihtiyaç duymuş ve işlemlerini takip edebilmek için çift taraflı (double entry) kayıt düzenini kullanmaya başlamışlardır. Bu kayıt düzenine göre her bir finansal işlemi kaydetmek için borç (debit) ve alacak (credit) olmak üzere iki giriş yapılması gerekmektedir. Her bir işlem borç ve alacak olmak üzere iki tarafa kaydedileceği için borçların toplamı ile alacakların toplamı birbirine eşit olmalıdır.

Çift taraflı kayıt düzeni ile işlemler arası ilişki kurulabilmiş, hile ve hırsızlığın önüne geçilmeye çalışılmış, borç ve alacak tarafına yapılan kayıtlarla hesapların eşitliği sağlanmıştır. Eğer kaydedilen işlemlerde hata yapılmamışsa tüm hesapların borç ve alacak tarafının toplamının birbirine eşit çıkması gerekmektedir.

Muhasebe kayıtlarının doğruluğunu artırmak için, günümüz finansal muhasebe sistemi çift taraflı kayıt düzenine dayanmaktadır. Her ne kadar çift taraflı kayıt düzeni basit ve verimli bir yöntem olsa da, bu yöntemde hataları takip etmek ve düzeltmek zahmetli bir iştir. Ayrıca kayıtlarla oynama, hata ve hile riski oldukça fazladır. Çift taraflı kayıt düzeni, işlemlerin yanlışlıkla silinmesi gibi insandan kaynaklı hata riskini azaltabilir, ancak şirketler tarafından hazırlanan finansal tablolar için yine de kapsamlı bir güvence sağlandığı söylenememektedir.

3.1.1.3. Üç Taraflı Kayıt Düzeni

Çift taraflı kayıt düzeninde bakiyelerin birbirine eşit çıkması işletme içi hırsızlığın ya da hilenin engellendiği anlamına gelmemektedir. İşlemler bilinçli olarak değiştirilebilir, yanlış kaydedilebilir ya da hayali işlemler eklenerek bu kayıt düzeninde eşitlik sağlanmaya devam edilebilir (Cai, 2019). Özellikle 2000’li yılların başında yaşanan muhasebe skandalları ile çift taraflı kayıt düzeninin de bu konuda yetersiz kaldığı görülmüştür. Konu ile ilgili yasal düzenlemeler yapılsa da hilenin önlenmesi ve raporlanan bilginin güvenilirliği halen istenen seviyeye getirilememiştir.

Günümüz muhasebe ve denetim uygulamaları maliyetli, yoğun iş gücü gerektiren ve zaman alan uygulamalardır. Ancak bu çalışmalar yine de hileyi önlemekte ya da tespit etmekte yetersiz kalmaktadır. Bağımsız denetçiler, şirketlerin muhasebe kayıtları üzerinde bir dizi test yapan ve finansal tabloların doğruluğu hakkında görüşlerini veren üçüncü taraf olarak görev yapmakta olsalar da, mevcut raporlama ve güvence sistemindeki iyileştirmelere hala ihtiyaç duyulmaktadır.

Hileyi önlemenin ya da tespit etmenin yolu ise muhasebe bilgi sisteminin şeffaflığını arttırmaktır. Bu sebeple, blok zinciri teknolojisinin muhasebe ve denetim alanında, şirketlerin kayıtlarının ve finansal tablolarının güvenilirliğini ve şeffaflığını arttırmak için kullanılması fikri ön plana çıkmaktadır.

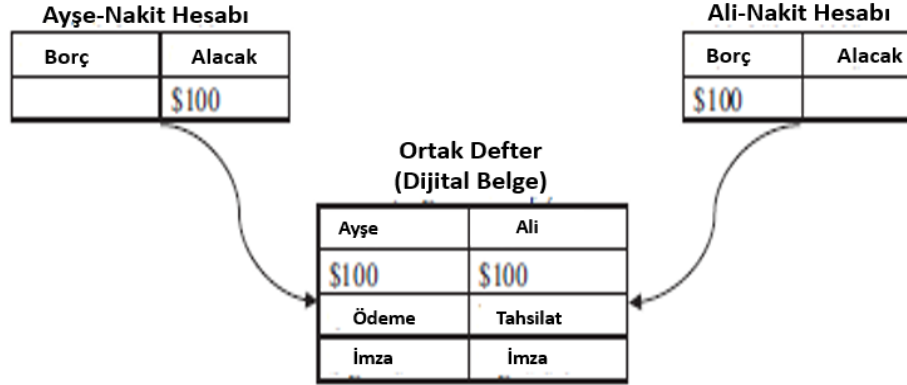
Blok zinciri teknolojisi ile birlikte muhasebe literatüründe üç taraflı kayıt düzeni (triple entry accounting) kavramı sıklıkla kullanılmaya başlanmıştır. Bu kavram her ne kadar blok zinciri teknolojisi ile adından söz ettirmeye başlasa da, üç taraflı kayıt düzeni blok zinciri ile ilk kez duyulan bir kavram değildir. Carnegie-Mellon Üniversitesi'ndeki profesör Yuji Ijiri tarafından 1982 yılındaki "Triple-Entry Bookkeeping and Momentum Income" ve 1986 yılındaki "A Framework for Triple Entry Accounting" başlıklı çalışmalarda ele alınan ve ilk kez kullanılan üç taraflı kayıt düzeninde, Borç (Debit), Alacak (Credit)'in yanında yeni bir Üçüncü Giriş (Tredit)'ten bahsedilmektedir. Çalışmalarında işletmenin gelirlerinin "ne oranda" yaratıldığını anlamının gerekli olduğundan bahsetmiş ve bu kavrama "ivme (momentum)" demiştir. Bu konu Melse (2008) tarafından araç kullanımı örnek verilerek açıklanmıştır: Üç taraflı kayıt muhasebesinin amacı, araç ile kat edilen mesafeyi değil, aracın gittiği hızı ölçmek istemektir. Ijiri'ye göre önemli olan, işletmenin gelirlerinin dönemler arasındaki farklılıkları ya da iki statik nokta arasındaki değişimi ölçmek değil, gelirlerin seviyelerine göre değerlendirilmesidir. Bir görüşe göre Ijiri'nin önerdiği sistemin performans analizi, risk analizi ve stratejik muhasebe gibi çeşitli uygulama alanlarında kullanılmasının faydalı olacağı düşünülmektedir. Ancak Ijiri'nin önermiş olduğu sistemin kullanım alanının olmaması, uygulamasının zor ve riskli olması sebebi ile çokça eleştiri almış ve bu sistemi uygulamak için yeterli talep oluşmamıştır (Carlin, 2018).

Finansal şifrelemede uzman olan Ian Grigg ise, 2005 yılında “Triple Entry Accounting” başlıklı yazdığı makale ile üç taraflı kayıt düzenine bambaşka bir anlam getirmiştir. Grigg “belge işlemdir (the receipt is the transaction)” bakış açısını makalesinde konu almış, muhasebedeki hata ve hilelere karşı bir çözüm önerisi sunmuş ve işletmelerin kayıtları yapan tek taraf olmamaları gerektiğini savunmuştur. Blok zinciri teknolojisinde anlatılan üç taraflı kayıt düzeni de bu makaleye dayanmaktadır.

Blok zincirinde üç taraflı kayıt sistemi ya da düzeni ifadesi ile, muhasebe kaydındaki borç ve alacak tarafı gibi **üçüncü bir girişten bahsedilmemektedir**. Anlatılmak istenen iki taraf arasında yapılan çift taraflı kayıt düzenine göre tutulan muhasebe defterlerinin blok zinciri teknolojisi kullanılarak aynı kayıtları eş zamanlı olarak ortak küresel defterde kaydedilmesi ve aynı bilgilerin tüm taraflarda birer kopyasının olmasıdır. Kriptografik olarak güvenli olan bir kayıt, **üçüncü taraf olarak** iki işletme arasındaki işlemleri eş zamanlı olarak kaydedecektir. Bu üçüncü kayıt, bir işletme tarafından kaydedilen borç kaydı ile karşı işletme tarafından yapılan alacak kaydını içermektedir.

Çift taraflı kayıt düzeninde hem alacaklı hem de borçlu tarafından birbirinden bağımsız bir şekilde, farklı defterlerde kaydedilen işlem Grigg’in önerdiği modelde şekil 3.1.1.3.1.’de görüldüğü gibi ortak bir defterde taraflar arasında aynı anda kaydedilecek ve kendi iç sistemlerinde bir daha değiştirilemeyecektir (Cai, 2019). Blok zinciri teknolojisi kullanılarak, işlemler, farklı defterlerde değil aynı olan açık defterde (public ledger), birbirine bağlı muhasebe kayıtları seti olarak blok zincirinde yer almaktadır. (Potekhina ve Riumkin, 2017). Bu da sistemin üçüncü tarafını meydana getirmektedir. Yani, blok zincirinde saklanan işlem çift taraflı kaydın **üçüncü tarafını** dağıtık defter yapısı ile tek bir blokta oluşturmaktadır (Uysal ve Kurt, 2018:474). Blok zinciri teknolojisinde anlatılan üç taraflı kayıt düzeni bir kayıt tekniği değildir. Günümüzde yapılan çift taraflı kaydın güvenliğini sağlayacak üçüncü bir kayıttır.

Şekil 3.1.1.3.1. Üç Taraflı Muhasebe Sistemi Örneği



Kaynak: CAI, C. W.:2019 ,“Triple-Entry Accounting with Blockchain: How Far Have We Come?”. Accounting & Finance. syf.6.

Kayıtların üçüncü bir tarafça onaylanması bir örnekle açıklanabilir. Borçlu, alacaklı ve bankadan oluşan *üç taraflı* rutin bir ödeme işleminde, borçlu parayı alacaklıya gönderir. Ancak bu para transferinin yapılabilmesi için aracı kuruluş olan bankanın onayı gerekmektedir. Burada aracı olan banka işlemin doğrulanmasından sorumlu olan taraftır. Banka parayı alacaklıya transfer eder ve tarafların bu işlemi defterlerine kaydedebilmeleri için bir belge imzalayıp işlemin gerçekleştiğini ispatlar (Simoyama ve ark., 2017). Bu örnekteki her bir işlemin bağımsız ve güvenilir bir aracı kuruluş tarafından doğrulanması gerekmektedir. Ancak böyle bir durumda para transferinde tüm kontrol ve güç bankada olacağı için banka, hile yapma, işlemi veya tutarları değiştirme olasılığı fazla olan taraf olmaktadır. Bu durumda, iç sahtekârlık (insider fraud) için güçlü bir aday olacak bankaya çok fazla merkezi bir güç verilmektedir (Grigg, 2005). Her ne kadar bankanın buradaki görevi, taraflar arasında gerçekleşen ödeme işleminde güveni sağlamak olsa da kontrol ve güç bankada olacağı için tam anlamıyla hilenin veya hatanın önüne geçildiği söylenememektedir. Bununla birlikte, aracı kuruluş tarafından depolanan ve saklanan verilerin siber saldırılara bağlı olarak kayıp veya yetkisi olmayan kişiler tarafından değişiklik yapılma riskine de maruz kalabilmektedir (Dai ve Vasarhelyi, 2017:10).

Grigg'in önerdiği modelde ise farklı taraflar arasında gerçekleşen ve üçüncü bir tarafça saklanan işlemleri doğrulamak için kriptografik olarak korunan dijital bir belgenin kullanılma olasılığı açıklanmakta ve kayıtlardaki herhangi bir detayın değiştirilip değiştirilmediği veya silinmediği gösterilmektedir (Inghirami, 2019).

Dijital imza ile imzalanmış bir belge kriptografi ile sağlamlaştırılınca taraflar arasındaki işlemler ortak üçüncü bir kayıt gibi görülebilecek ve işletmelerin iç kayıt sistemlerindeki yanlışlıklardan ve hilelerden uzak tutulabilecektir. Hiçbir taraf yetkilendirilmemiş bir işlemi gerçekten meydana gelmiş gibi kendi sistemine kaydedemeyecektir. Buradaki üçüncü kayıt ise kriptografik olarak güvenli bir kayıttır ve bu güvenli kayda da “belge” denmiştir. Çalışma ile “belge işlemdir (the receipt is the transaction)” ilkesi getirilmiş ve böylelikle dağıtık defterde bu belgelerin toplamından oluşmuştur (Simoyama ve ark., 2017).

Grigg 2005 senesinde üç taraflı kayıt düzeni (triple entry accounting) önerisinde bulunduğunda, bu ortak kaydı kontrol edecek güvenilir ve tarafsız üçüncü tarafın kim olacağı konusu belirsizdi (Cai, 2019). 2008 senesinde bitcoinin ortaya çıkışı ile aslında kayıtların kontrolü için üçüncü bir tarafa duyulan güvene ihtiyaç olmadığı, blok zinciri teknolojisi kullanılarak merkezi olmayan, değiştirilemeyen, güvenli ve otomatik hale gelebilen ortak bir üçüncü defterin oluşturulabileceği konuşulmaya başlandı. Blok zincirine dahil olan tüm katılımcılarda aynı kopya olacağı için tarafların işlemleri takip etmek için merkezi bir otoriteye ihtiyacı kalmamaktadır.

Blok zinciri, 2005 yılında Grigg tarafından geliştirilen bu mekanizmayı geliştirme ve muhasebe sisteminde karşılaşılan sorunları azaltma potansiyeline sahip bir teknolojidir. Blok zinciri işlemlerin depolama ve doğrulama sürecini dağıtarak ve otomatik hale getirerek, muhasebe kayıtlarının değiştirilmesini önleyen güvenli bir altyapı sağlayarak aracı kuruluşların yerini alabilir (Dai ve Vasarhelyi, 2017). Blok zincirinin yapısından dolayı, bir muhasebe kaydı onaylanıp zincire eklendiğinde, bu kaydın değiştirilmesi veya ortadan kaldırılması imkânsıza yakındır. Blok zinciri tabanlı muhasebe sistemini tanımlamak için de kullanılan üç taraflı kayıt düzeni, ilgili tarafların muhasebe kayıtlarının **üçüncü taraf olarak blok zinciri tarafından** kriptografik olarak mühürlendiği çift taraflı kayıt düzeninin geliştirilmiş hali olarak görülmektedir (Potekhina ve Riumkin, 2017).

Blok zinciri teknolojisi ile üçüncü bir girdi oluşturulmadığı için üç taraflı kayıt sistemi ifadesi kafa karıştırıcı olabilmektedir. Burada borç ve alacak gibi yeni bir giriş yaratılmamakta sadece birbirinden bağımsız bir şekilde tutulan iki muhasebe defteri

birbirine bağlanmaktadır. Bu bağlantı, ayrı tüzel kişilikleri olan işletmelerde çift kayıtlı muhasebe tekniğine göre kaydedilen işlemlerin, her zaman aynı olmasını sağlamak için çalışan akıllı bir sözleşme ile oluşturulmaktadır.

Blok zincirine kodlanan akıllı sözleşmeler muhasebe standartlarını veya önceden belirlenmiş kuralları takip ederek kayıtların hızlı bir şekilde doğrulanmasını sağlayabilir. Üçüncü muhasebe kaydını blok zincirine kodlayarak, iş ortakları arasında güvenilir veri paylaşımını ve hissedarlar için sürekli raporlamayı kolaylaştıracak şeffaf, kriptografik olarak güvenli ve kendi kendini doğrulayan bir muhasebe bilgi sistemi oluşturulması sağlanır (Dai ve Vasarhelyi, 2017). Denetim kuruluşları, blok zinciri teknolojisi ile uygulamaya geçecek olan üç taraflı kayıt tekniğinin muhasebe mesleğinde dengeleri ve mesleğin gidişatını değiştirecek bir uygulama olduğunu savunmaktadır.

Üç taraflı kayıt düzeni ile ilgili akademik çalışmalar devam ederken, bu kayıt düzeni ile ilgili model önerileri ve kayıt düzenini hayata geçirme amacı ile kurulmuş projeler de ortaya çıkmaya başlamıştır. Dai ve Vasharleyi (2017) günümüz çift taraflı kayıt düzenini geliştirerek üç taraflı kayıt düzeni ile ilgili bir model önerisinde bulunmuştur. Günümüzde blok zinciri teknolojisinde bahsedilen üç taraflı kayıt düzeni ile ilgili en somut projeler ise Ledgerium ve zkLedger uygulamalarıdır.

3.1.1.3.1.Dai ve Vasarhelyi (2017)- Üç Taraflı Kayıt Düzeninde Muhasebe Bilgi Sistemi

Dai ve Vasarhelyi (2017), Girgg'in geliştirmiş olduğu üç taraflı kayıt düzenini esas alarak bir model önerisi sunmuştur. İzin gerektiren blok zinciri ağ yapıları için geliştirdikleri modelde, işletme kendine ait bilgiler hakkında kontrol sahibi olmaya devam ederken, ilgili olmayan tarafları da bu ağın dışında tutmuştur. Modelde, basit bir mal alım ve satım işlemi ele alınmıştır. Bu sistemde çift taraflı kayıt düzeninin üzerine inşa edilen blok zinciri teknolojisi, olayların hem işletme içinde hem de işletme dışı taraflarla kaydedilmesini anlatmaktadır.

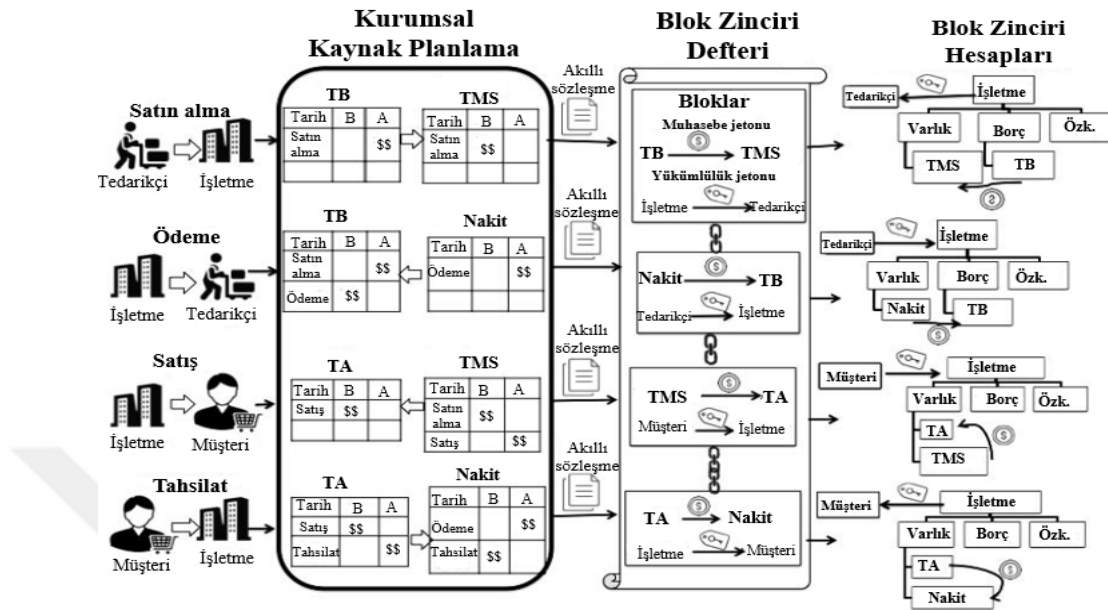
Şekil 3.1.1.3.1.1. basitleştirilmiş bir örnek ile bir üç taraflı muhasebe bilgi sistemi görülmektedir. Bir işletme tedarikçisinden mal satın alır. Bu satın alma işlemi sonucunda hem işletme hem de tedarikçi bu olayı kendi muhasebe defterlerine

bağımsız olarak kaydeder. Bu işleme ilişkin kayıt yine sadece iki tarafın muhasebe defterlerinde yer alır. Üçüncü bir tarafın bu kaydı bilebilmesi ya da görebilmesi mümkün değildir. Ancak, vergi denetimi ya da bağımsız denetim süreci gibi özel bir durum olması halinde üçüncü bir taraf tarafından defterlere bakılabilmektedir. Blok zinciri teknolojisinin kullanıldığı bir ortamda ise bu finansal olaya ait kayıt hem işletmenin (alıcı) hem tedarikçinin (satıcı) defterlerinde gözükürken aynı zamanda ortak defter olan blok zincirine de kaydedilir. Her bir işlem blok zinciri defterinde kaydedilip saklanırken, aynı zamanda işletmelerin kendi muhasebe defterlerinde çift taraflı kayıt düzeni ile de kaydedilmeye devam edilir. Böylelikle alıcının ve satıcının kendi defterlerinde ve Kurumsal Kaynak Planlama sisteminde tutulan kayıttan ayrı olarak üçüncü bir kayıt oluşmuş olur. Bu sistem, hem birlikte iş veya ticaret yapan farklı taraflar arasındaki işlemleri hem de bir işletmenin kendi içindeki veri akışlarına dair bilgileri kaydetmektedir.

Bu örnekte, günümüzde kullanılan çift taraflı kayıt tekniğindeki her bir hesap uygun bir blok zinciri hesabına karşılık gelmektedir. İşletme içindeki veri akışlarını blok zinciri defterine yansıtmak için, işlemler, blok zinciri defterindeki hesaplar arasında bir jeton (token)² aktarımı biçiminde kaydedilmiş ve birbirine bağlı değiştirilemeyen muhasebe kayıtları oluşturulmuştur. Blok zinciri kayıt defterindeki hesaplar hem muhasebenin temel eşitliğinin anında sağlanması hem de farklı kullanıcılar için ilgili bilgilerin görüntülenmesini sağlamak amacı ile veriler çeşitli seviyelerde toplanarak hiyerarşik bir yapıda düzenlenmiştir. Blok zinciri defterinde bulunan jetonlar, taraflar arasındaki yükümlülükleri veya varlıkların sahipliğini kanıtlamak için belge olarak da kullanılmaktadır.

² Kripto paralar para (coin) ve jeton (token) olmak üzere ikiye ayrılmaktadır. Para (coin)'nin kendine ait bir blok zinciri platformu bulunurken, jeton (token) için aynı şey söz konusu değildir. Jetonlar başka hazır bir blok zinciri üzerinde bir varlığın karşılığı bir değerdir. Aynı tür olan ve alım satımı yapılan herhangi bir varlığı temsil edebilirler (Güven ve Şahinöz, 2018).

Şekil 3.1.1.3.1.1. Üç Taraflı Kayıt Düzeninde Muhasebe Bilgi Sistemi



Kaynak: DAI, J., VASARHELYI, M. A.:2017, "Toward Blockchain-Based Accounting and Assurance". Journal Of Information Systems, 31(3), 5-21.

İşletme, tedarikçisinden kredili mal satın aldığı anda, kendi muhasebe sistemini kullanarak bu işlemi Ticari Borçlar (TB) ve Ticari Mal Stoku (TMS) hesaplarına kaydeder. İşletme bu finansal olayı eş zamanlı olarak, iki blok zinciri hesabı arasındaki bir dijital jeton aktarımı biçiminde blok zinciri defterine sunmaktadır. Muhasebe jeton'u (accounting token), blok zinciri defterinde işlemlerin kayıt altına alınması ve takip edilmesi için basit bir simge olarak kullanılmıştır. Kredili mal satın alımı karşı tarafa bir yükümlülük getirdiği için bu işlemi kaydetmek için yükümlülük jetonu (obligation token) kullanılmıştır. Yükümlülük jetonu bir varlığın yükümlülüğünü ve sahipliğini, bununla birlikte varlığın miktarını veya tutarını, zamanı gösteren ve bir kez çıkarıldıktan sonra silinemeyen ve itiraz edilemeyen bir belgedir.

İşletme, aynı prosedürü takip ederek, satış ve tahsilat süreçlerinde üretilen muhasebe verilerini de blok zinciri defterine kaydedebilir. Ödeme işlemi tamamlandığında muhasebe jetonu nakit hesabından ticari borçlar hesabına aktarılır. Aynı zamanda tedarikçi de yükümlülük jetonunu işletmeye geri gönderir.

Blok zinciri hesapları, muhasebe kayıtlarını üç düzeyde toplayan hiyerarşik bir yapıda oluşturulmaktadır: en altta hesaplar ayrı ayrı yer almaktadır; orta seviyede

toplam varlıklar, borçlar ve özkaynaklar ve en tepede ise şirket bir bütün olarak yer almaktadır. Bu yapı, akıllı sözleşmeleri kullanarak bilanço denklemini otomatik olarak doğrulayabilmektedir. Hesapların hiyerarşik yapıda olmasının yararı ise çeşitli düzeylerde veri görüntülemesine izin vermesidir. Farklı seviyedeki bilgi tüketicilerinin, muhasebe verilerini elde etmek için çeşitli talepleri ve kısıtlamaları bulunmaktadır. Bu nedenle, kullanıcıların pozisyonlarına göre farklı veri görünümeleri verilebilecektir. Ayrıca, örneğin, iskontolu satışlarda erken ödeme yapıldığında indirim yapılması ya da son ödeme tarihi geldiğinde akıllı sözleşmenin ödemeyi kendiliğinden gerçekleştirmesi gibi diğer iş kuralları da, gelecekteki koşullara ve faaliyetlere göre önceden belirlenen şartların otonom bir şekilde yürütülmesini sağlayan akıllı sözleşmeye kolayca kodlanabilir (Dai ve Vasarhelyi, 2017).

Bir jeton işlemi blok zinciri ağına gönderildikten sonra, ağdaki bilgisayarlar bu işlemi doğrulamak üzere çeşitli prosedürler uygularlar. Örneğin, şirketin muhasebe sistemi tarafından kaydedilen işlemin blok zincirine kaydedilmesi; varlık transferi; tutarların ve hesapların doğruluğu; işlemi yapan tarafın geçerliliği doğrulamayı gerektiren işlemler arasında yer almaktadır. Doğrulama işlemi blok zinciri teknolojisi ile otomatikleştirilmesine rağmen, bu doğrulama işlemi muhasebeciler, yönetim, denetçiler vb. gibi belirli taraflarla sınırlandırılmalıdır. Bu nedenle, bu senaryodaki blok zinciri defteri izin gerektiren blok zinciri ağ kategorisine girmektedir. Ayrıca, burada her bir tarafın doğrulama sürecinde belirli bir rolü vardır. Geçerli olan onaylanmış işlemler blok zincirinde yer alır ve sonrasında bu işlemleri görmek ve incelemek üzere sadece yetkisi olanlar bakabilir (Dai ve Vasarhelyi, 2017). Şirketin özel bilgilerinin gizliliğini korumak için, işlemler blok zinciri defterine kaydedilmeden önce şifrelenebilir ve sadece şifre çözme anahtarı olan kullanıcılar işlemlerin içeriğini görüntüleyebilir.

Dai ve Vasarhelyi'nin önermiş olduğu bu modelde blok zinciri mevcut olan Kurumsal Kaynak Planlama sisteminin yerini almamakta, mevcut sistemin üzerine blok zinciri tabanlı bir sistem geliştirilmektedir.

3.1.1.3.2. Ledgerium Uygulaması

2018 yılında Avustralya’da başlatılan bir girişim olan Ledgerium uygulaması, blok zinciri teknolojisini muhasebe ve denetim endüstrisine getiren şirket olduğunu söylemiş ve üç taraflı muhasebe sistemi ile merkezi olmayan bir defter oluşturmayı ve geleneksel denetim prosedüründe yenilik yaratmayı amaçladıklarını dile getirmiştir (Ledgerium, 2019).

İnternet sayfalarında yayımladıkları izahatnameye göre defter tutma ve işlem onayları gibi güvene dayanan tüm düşük katma değerli, yüksek maliyetli ve zaman alıcı işleri nasıl aradan çıkarabiliriz sorusuna cevap olarak geliştirdikleri Ledgerium uygulaması, akıllı sözleşmeler ile üç taraflı kayıt sistemini hayata geçirmeyi planlamaktadır. Bu uygulamadaki üçüncü kayıt olan ortak deftere Luca+ ismi verilmiş ve ismini çift taraflı kayıt tekniğinin kurucusu olarak kabul edilen Luca Pacioli’dan almıştır (Lucaplus, 2019a).

Şekil 3.1.1.3.2.1.’te görüldüğü gibi Luca+, e-faturalamada işletmelerin muhasebe yazılımı ile müşterilerin veya tedarikçilerin muhasebe yazılımları arasında bir bağ oluşturarak, yeni bir fatura ağı meydana getirmektedir. Böylelikle faturayı ödeyen ile ödeme yapılan taraf arasında şifrelenmiş bir iletişim kanalı kurulmakta ve faturalamada hileyi önlemektedir. Luca+, şeffaf bir denetim izi sağlarken rutin işleri otomatikleştirerek tüm işletmeler, muhasebeciler ve denetçiler için defter tutmayı kolaylaştırmaktadır.

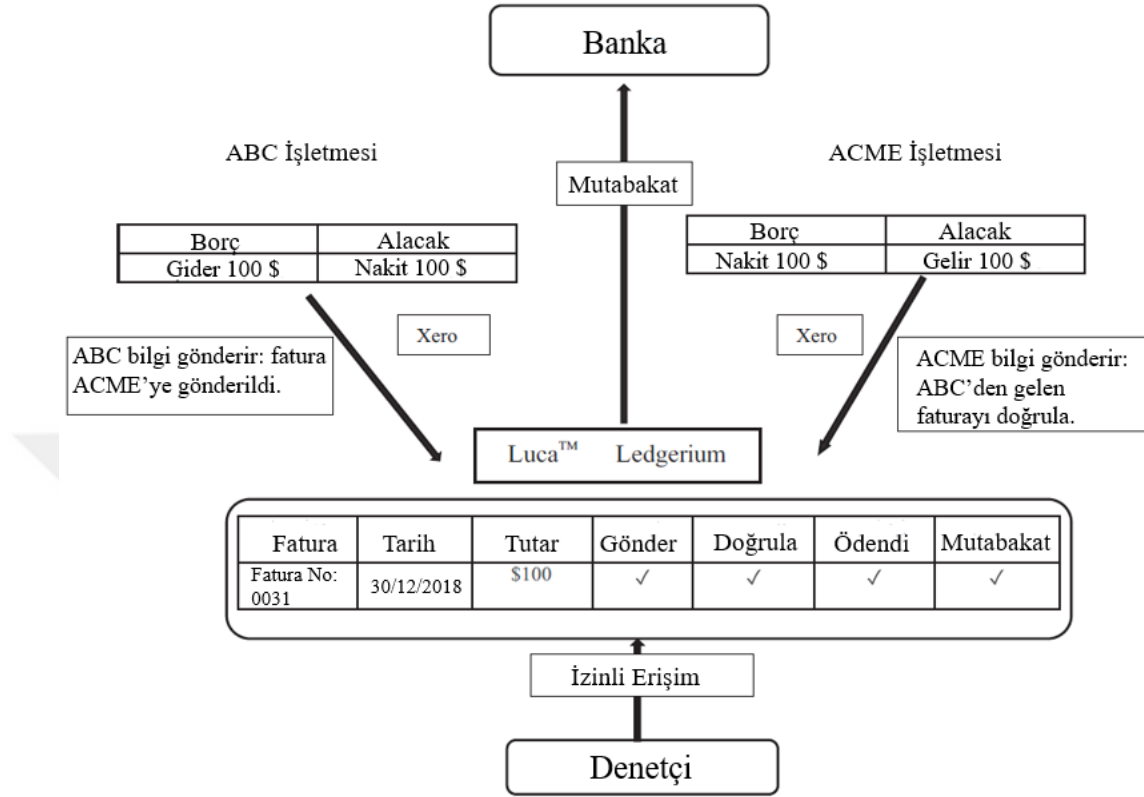
Şekil 3.1.1.3.2.1. Luca+



Kaynak: LUCAPLUS: 2019B, HOW LUCA+ WORKS. (Çevrimiçi)
<https://www.lucaplus.com/#whyus>, 23 Haziran 2020.

Şekil 3.1.1.3.2.2.'de gösterilen Luca+ Ledgerium uygulaması örneğinde ABC İşletmesi'nin, satın almış olduğu hizmet için ACME İşletmesi'ne 100 Avustralya Doları ödemesi gerekmektedir ve ABC İşletmesi kendi kullanmış olduğu Zero yazılımını kullanarak bir fatura düzenlemektedir. Bu faturanın özetleme değeri ile işleme ilişkin detaylar ve şart ve koşullar Luca+ (ortak defter)'ya gönderilir ve ACME'nin açık anahtarı ile şifrelenir. ACME işlemi onayladığında blok zinciri güncellenir ve iki taraf arasındaki ortak defter tamamlanır. Luca+, ödeme işlemi için banka ile doğrulama sürecini yönetir. Ödeme işlemi gerçekleştiğinde de ortak defterdeki bakiyelerde mutabık kalınır. Denetçiler de gerekli izni alarak ortak deftere erişebilmektedir (Cai, 2019).

Şekil 3.1.1.3.2.2. Luca+ Ledgerium Örnek Uygulama



Kaynak: CAI, C. W.:2019 ,“Triple-Entry Accounting with Blockchain: How Far Have We Come?”. Accounting & Finance.

Luca+ ticari alacaklar ve ticari borçlar olmak üzere iki ana hesabı kullanma amacı ile tasarlanmış bir dağıtık defterdir, bu yüzden ana hedef kitle veri tabanlarında alıcıların ve satıcıların çok olduğu müşterilerdir. Luca+ dağıtık defteri ile bu hesapların döngüsündeki şeffaflık ve verimlilik ciddi şekilde artırılabilir (Cai, 2019).

Şirket, 2019 yılında isim değişikliğine gitmiş ve Block Ledger ismini almıştır (Blockledger, 2019). Ancak uygulamalarda Ledgerium ismi kullanılmaya devam etmektedir.

3.1.1.3.3. zkLedger Uygulaması

zkLedger uygulaması, ABD’de Massachusetts Institute of Technology Üniversitesi’nde (MIT) yer alan MIT Media Lab tarafından geliştirilmiş izin gerektiren bir blok zinciri uygulamasıdır. Bu uygulama blok zinciri ağındaki kişilerin

mahremiyetini koruyan ve aynı zaman hızlı ve kanıtlanabilir doğru denetim hizmeti sunan ilk uygulama olduğunu iddia etmektedir.

Üç taraflı kayıt düzeninin uygulanmasındaki ana engel verilerin gizliliğinin endişesidir. Bunun nedeni ise mevcut olan blok zinciri tasarımlarında üçüncü tarafın denetim yapabilmesi için işlemlerin içeriğinin açığa çıkması gerekmektedir (Cai, 2019). zkLedger'in amaçları, doğrulanabilir bir işlem defteri tutarken işlemler arasındaki tutarları, katılımcıları ve bağlantıları gizlemek ve denetçinin sorularına güvenilir cevaplar almasını sağlamaktır. Uygulamada işlemlerin gizliliğini sağlamak için sıfır bilgi ispatı (zero-knowledge proof) algoritması³ kullanılmıştır.

Çalışmanın motivasyonu şu şekilde anlatılmıştır (Narula, Vasquez ve Virza, 2018):

“Kurumlar, kanunlara ve düzenlemelere uyumlu olduklarını ispat etmek için güvenilir üçüncü taraf olan denetçiler ile çalışmaktadırlar. Ancak bu denetim hem çok fazla iş gücü gerektiren hem de zaman harcayan bir iştir, bu yüzden düzenleyiciler ve yatırımcılar kurumların finansal durumunu gösteren gerçek zamanlı verilere ulaşamamaktadırlar. Ayrıca Arthur Anderson'ın Enron'un 100 milyar dolarlık muhasebe sahtekârlığını yakalayamaması sonrasında 2002 yılındaki çöküşü, üçüncü tarafların da hata yapabildiğini göstermektedir.

Dağıtık defterler finansal kurumların, kurumlar arası yaptıkları işlemlerde etkin bir şekilde mutabık kalınmasını sağlamaktadır. Ancak bu defterlerin tamamı tüm katılımcılara açık olup kurumların stratejik ve ticaret bilgilerinin içeriğini açığa çıkarmaktadır. Ya da bu defterler özel defter olup, işlemlerin denetlenebilmesi için, işlemlerin içeriğinin üçüncü taraf olan denetçiler tarafından açığa çıkarılmasını gerektirmektedir.

zkLedger, güçlü işlem gizliliğini, herkese açık doğrulanabilirliği ve pratik denetimi destekleyen ilk dağıtık defter sistemidir. zkLedger güçlü işlem gizliliği

³ Sıfır bilgi ispatı algoritması “Bir bilgiyi bildiğimi, karşı tarafa bu bilgiyi vermeden nasıl ispat edebilirim?” sorusunu cevaplamaktadır. Sıfır bilgi ispatında olması gereken üç özellik: tamlık (completeness), doğruluk (soundness) ve sır vermemek (zero knowledge)'tir. Bu algoritma, bilgileri gizli tutarak doğruluğunun ispatlanmasını sağlamaktadır.

sağlamakta ve kötü niyetli birine, bir işleme kimlerin dahil olduğunu veya ne kadar işlem yapıldığını söylememektedir. zkLedger işlem grafiğini veya işlemler arasındaki bağlantıları göstermez. İşlemlerin süresi ve devredilen varlık türü ise herkese açıktır.”

Konu, bankalar arasındaki dijital varlıkların transferi örnek verilerek anlatılmıştır. Verilen örnekteki olaylar hem açık defterde (public ledger) hem de zkLedger uygulamasında kaydedilmiştir. İki uygulama karşılaştırılarak zkLedger uygulamasının amaçları açıklanmıştır.

Örneğe göre, Goldman Sachs’ın dönemin başında 30 milyon Eurosu bulunmaktadır. Goldman Sachs dönem boyunca JP Morgan’a 10 milyon Euro göndermiş, JP Morgan ise Barclays’e toplamda 3 milyon Euro göndermiştir. Bu işlem açık bir defterde kaydedildiği zaman şekil 3.1.1.3.3.1.’deki gibi, işlemin tutarları, işlemin kimler tarafından gerçekleştirildiği ve kaç tane işlemin gerçekleştiği deftere erişimi olanlar tarafından görülebilmektedir. Ayrıca, işlemin ne zaman ve hangi türdeki varlıkların transferinin gerçekleştiği de deftere erişimi olan herkes tarafından görülebilmektedir.

Şekil 3.1.1.3.3.1. Açık Defter (Public Ledger) Uygulama Örneği

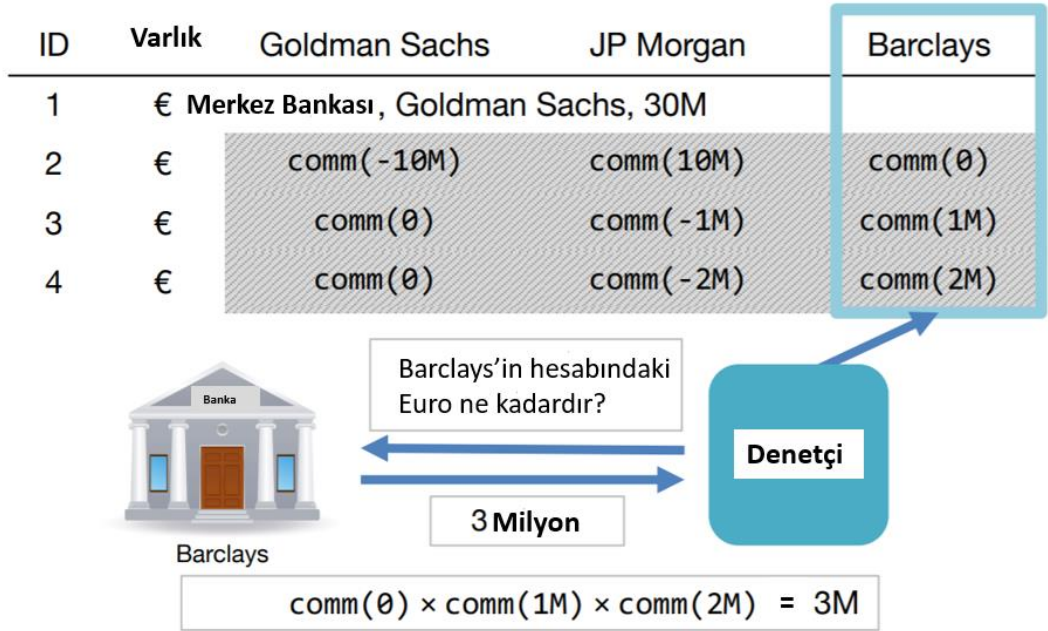
ID	Varlık	Gönderen	Alan	Tutar
1	€	Merkez Bankası	Goldman Sachs	30.000.000
2	€	Goldman Sachs	JP Morgan	10.000.000
3	€	JP Morgan	Barclays	1.000.000
4	€	JP Morgan	Barclays	2.000.000

Kaynak: NARULA, N., VASQUEZ, W., VIRZA, M.:2018, zkLedger Privacy-preserving auditing for distributed ledgers, (Çevrimiçi) https://www.usenix.org/sites/default/files/conference/protected-files/nsdi18_slides_narula.pdf, 3 Nisan 2020., s.19.

Yukarıdaki örnekte meydana gelen aynı olaylar, şekil 3.1.1.3.3.2.’deki zkLedger uygulamasında kaydedilmiştir. Açık defter uygulamasında kullanıcılar tarafından görülebilen işlem bilgileri zkLedger uygulamasında görülememekte ve işlem bilgileri gizli tutulmaktadır. İşlemin zamanı ve varlık türü ise yine deftere erişimi olan herkes tarafından görülebilmektedir.

Örneğin devamında ise denetçi, raporlama dönemi sonunda Barclays Bankası'nın hesabındaki Euro tutarını doğrulamak istemektedir. Denetçiler de bu blok zinciri ağına dâhildir ve defterin bir kopyası denetçilerde bulunmaktadır. Denetçi raporlama dönemi sonunda Barclays'e hesabındaki Euro tutarının ne kadar olduğunu sorduğunda Banka'nın vermesi gereken cevap 3 milyon Euro'dur. Denetçi de defterin bir kopyası olduğu için banka ile iletişime geçip gereken hesaplamaları yaparak, kriptografik olarak bakiyenin doğruluğunun güvencesini alır. Ayrıca denetçi, toplamlar, hareketli ortalamalar, varyans, eş varyans, standart sapma ve oranlar dahil olmak üzere yapılan hesaplamaların doğruluğunu sorgulayabilir. Şekil 3.1.1.3.3.2'te görüldüğü gibi aynı örnek zkLedger uygulaması kullanılarak kaydedildiğinde denetçiler işlemlerin içeriğini görmeden de işlemlerin doğruluğunu ispat edebileceklerdir.

Şekil 3.1.1.3.3.2. zkLedger Uygulama Örneği



Kaynak: NARULA, N., VASQUEZ, W., VIRZA, M.:2018, zkLedger Privacy-preserving auditing for distributed ledgers, (Çevrimiçi) https://www.usenix.org/sites/default/files/conference/protected-files/nsdi18_slides_narula.pdf, 3 Nisan 2020., s..28

zkLedger, bankaların diğer tüm katılımcılar tarafından kamuya açıklanabilen gizli transfer işlemleri yapmalarına izin verir. zkLedger'in amaçları, doğrulanabilir bir

işlem defteri tutarken işlemler arasındaki tutarları, katılımcıları ve bağlantıları gizlemek ve denetçinin sorgularına güvenilir cevaplar almasını sağlamaktır.

Çalışmada işlemlerin gizliliği Pedersen commitment kullanılarak korunmuştur. Daha önceki gizliliği sağlayan blok zinciri sistemlerinde de Pedersen commitment uygulanan çalışmalar vardır; ancak bunlar işlemler arasındaki bağların ortaya çıkması ile sonuçlanmış ve mahremiyeti sağlayan denetim desteklenmemiştir (Narula, Vasquez ve Virza, 2018).

Tüm bunların yanında zkLedger'in, daha önce tezin 2.7. Blok Zinciri Teknolojisinin Karşılaştığı Zorluklar bölümünde bahsedilen, ölçeklenebilirlik sorunu bulunmaktadır. zkLedger'da kaydedilen her işlemin her bir banka için büyüklüğü 4.5 kilobayttır ve bir kaydı yaratmak 8 milisaniyeyi alırken bu kaydı doğrulamak ise 7 milisaniyeyi almaktadır. Ancak zkLedger uygulamasına dâhil olan banka (katılımcı) sayısı arttıkça bir işlemi yaratma ve doğrulama süresi de artmaktadır (Narula, Vasquez ve Virza, 2018).

3.1.2. Gerçek Zamanlı Muhasebe

Blok zinciri teknolojisinin muhasebede kullanılması, yatırımcılara ulaşan bilginin kalitesini iki şekilde arttırabilmektedir. Bunlardan birincisi, işletmelerin finansal bilgilerini blok zincirine kaydetmesi ile muhasebe ile ilgili manipölasyonlar ve hileler için fırsatların azaltılabilmesidir. İkincisi ise, manipölasyonlar ve hileler için fırsatları azaltarak, muhasebe bilgilerini daha güvenilir yapmasıdır. Ayrıca firma içi işlemler daha şeffaf olacaktır. Muhasebe kayıtlarının blok zincirinde tutulması firmanın defterlerinde yer alan her bir işlemi anında erişilebilir yapacağı için muhasebe bilgilerinin gerçek zamanlı olarak güncellenmesi mümkün olmaktadır (Byström, 2019).

Yermack (2017), bir işletmenin ticari işlemlerinin blok zinciri üzerinden yayınlanması ile, ilgili tarafların işletme ile ilgili doğru finansal bilgilere anında erişebileceklerini düşünmektedir. Ayrıca, herhangi birinin blok zincirindeki verileri kullanarak, bağımsız denetçilerin kararına ve yöneticilerin dürüstlüğüne güvenmeden kendi finansal tablolarını hazırlayabileceğini savunmaktadır.

Blok zinciri platformlarının gerçek zamanlı olması özellikle güvence sağlayan taraflar, danışmanlar ve kurumsal paydaşlar için oldukça önemlidir. Kayıtları, meydana geldiği anda görebilmek ağı dahil olan herkes için bütünlük ve şeffaflık sağlamaktadır (Karajovic, Kim ve Laskowski, 2019). Gerçek zamanlı yapılan kayıtların getirdiği bu şeffaflık gizli hesaplara ve başka şekilde göz ardı edilmiş olabilecek küçük ayrıntılara dikkat çekmeye yardımcı olabilir (Tapscott ve Tapscott, 2017b). Blok zinciri teknolojisini kullanan şirketler, finansal durumlarını ve performanslarını yönetmek ve iletmek için tam işlem görünürlüğü ile tamamlanan yeni ve güçlü bir raporlama araçları setine sahip olabilir.

Duke Üniversitesinde finans profesörü olan Campell Harvey blok zincirinin finansal tablolar için esas faydasını tek bir kelime ile açıklamıştır: gerçek-zamanlı. Günümüzde finansal tablolardaki rakamlar bir yıllık, 6 aylık veya çeyrek dönemlik raporlara, yani geçmişten gelen verilere dayanmaktadır. Blok zincirinin izin verdiği şey ise, iç denetim ekibi tarafından tutulan ve iş kollarından anında ve güvenli veri alan bir defter oluşturmak ve bu defterin bağımsız denetçiler tarafından gerçek zamanlı olarak doğrulanabilmesidir (FERF ve Deloitte, 2018).

Kripto varlıklar ile geleneksel finansal ekosistemleri arasındaki boşluğu doldurmak için bir kripto varlık teknolojisi ve veri hizmetleri şirketi olan Lukka'nın Ticari Faaliyetlerden Sorumlu İcra Kurulu Üyesi (Chief Commercial Officer-CCO) Jeremy Dane'in 2016 yılında yazmış olduğu bir yazıda denetim mesleğinin ortadan kalkacağı düşüncesini tümüyle reddetmiş ve amaçlarının denetimde sunulan hizmetin zamanında bir değişim yaratmak olup, denetçilerin geriye dönük değil gerçek zamanlı denetim yapabilmeleri için yazılım geliştirme olduğunu dile getirmiştir (Drane, 2016). Gerçek zamanlı denetim ile anlatılmak istenen işlemleri, meydana geldikleri anda incelenebilecek durumda olunabileceğidir (PWC, erişim tarihi:10 Mayıs 2020). Günümüzde, blok zinciri teknolojisinin henüz çok başında olduğu için, gerçek zamanlı denetime tam anlamıyla geçiş yapılamayacaktır. Bunun sebebi ise işletmelerde meydana gelen işlemlerin tümünün değil henüz sadece belli bir kısmının blok zincirine kaydedilebilmesidir.

Gerçek zamanlı muhasebenin finansal raporlama üzerindeki etkisi, muhasebeci ve aracı kurumlar; kâr yönetimi ve ilişkili taraf işlemleri olmak üzere üç başlık altında toplanabilmektedir (Yermack, 2017).

3.1.2.1. Muhasebeciler ve Aracı Kurumlar

Günümüzde finansal tablolar belli zaman aralıklarında hazırlanmakta ve bu finansal tablolar belli bir dönemde bir işletmenin muhasebe defterine kaydedilen finansal olayların toplamı alınarak oluşturulmaktadır. Daha sonra denetçi bu tabloların doğruluğu hakkında bir görüş bildirmektedir. Yatırımcılar ve finansal tablodan yararlanacak olan diğer kişiler ise denetçinin görüşüne ve yargısına güvenerek finansal tabloların doğru bir şekilde hazırlandığına ve finansal tablolarda yanlış bir bilgi sunulmadığına güvenmek zorundadırlar. Bu sebeple güven duygusu hem finansal tabloların hazırlanma sürecinde hem de denetim sürecinde çok kritik bir yer almaktadır (Brystöm, 2019). Blok zinciri defterine kaydedilen işlemler değiştirilemez olduğu için finansal tablolara olan güvensizlik duygusu da ortadan kalkmaktadır. Eğer ki bir işletme muhasebe verilerini blok zincirine kaydederse her bir işlemin zaman damgası olacak ve kayıtlar değiştirilemeyecektir. İşletmenin defteri tümüyle, hissedarlar, kredi verenler, tedarikçiler veya diğer ilgili taraflarca anında görülebilir olacaktır. Herhangi biri blok zinciri defterinde kaydedilen işlemleri bir araya getirerek herhangi bir anda gelir tablosu ve bilançoyu oluşturabilecektir. Buna bağlı olarak işletmelerin çeyrek dönemler halinde hazırladıkları finansal tablolara ve bu finansal tablolara güvence sunan bağımsız denetçilere duyulan ihtiyaç artık ortadan kalkacaktır (Yermack, 2017). Blok zinciri defterleri, finansal raporları gerçek zamanlı olarak hızlı bir şekilde oluşturacağı için, ay sonu raporlama gecikmelerini azaltacaktır. Şirket genelinde konsolidasyon gerektiren yönetim kurulu raporlaması için finansal tablolar büyük ölçüde blok zincirinde otomatikleştirilebilecektir (Wunsche, 2016).

Gerçek zamanlı muhasebede muhasebe bilgisini kullanacak olan kişiler, denetçinin yargısına ve yöneticilerin dürüstlüğüne güvenmek zorunda değildirlir. Bunun yerine, blok zincirinde yer alan verilerin kesinliğine güvenerek, amortisman veya stokların yeniden değerlemesi gibi parasal olmayan kalemler ile ilgili ayarlamaları kendi muhasebe yargıları ile belirleyebileceklerdir (Yermack, 2017).

Yermack (2017)'e göre ABD'deki potansiyel tasarruflar ülkedeki muhasebe sektörünün toplam gelirine eşittir ve bu da senede 50 trilyon doları aşmaktadır. Bu tutar işletme hesaplarının doğruluğunun üçüncü taraflarca onaylanmasının sosyal maliyetini ya da diğer bir ifade ile işletme yöneticilerine olan güvensizliğin sosyal maliyetini göstermektedir. Davidson, Novak ve Potts (2018), “Güvenin Maliyeti (Cost of Trust)” konulu makalelerinde ABD ekonomisinin kilit sektörleri için güvenin maliyeti hakkında sayısal tahminlerde bulunmuşlardır. Yaptıkları çalışmada güvenin maliyetinin yüksek olduğu faaliyetlerde temsil edilen meslekler arasında avukatlar ve hâkimler, vergi uzmanları, muhasebeciler ve denetçiler bulunmakta ve genel olarak güvenin maliyetinin 2010 yılı ABD istihdamının yüzde 35'ini oluşturduğu tahmin edilmektedir. Güvenin maliyeti, blok zincirini geleneksel yöntemlere göre ekonomik açıdan daha uygulanabilir yapmaktadır.

3.1.2.2. Kâr Yönetimi

Gerçek zamanlı muhasebe ile işletmelerin finansal performansları hakkında finansal tablo kullanıcılarını yanlış yönlendirme ve finansal sonuçları değiştirebilme imkânları çok ciddi bir şekilde azalacaktır. Değiştirilemeyen ve zaman damgalı işlemler sayesinde yöneticiler artık bir satış işlemini gerçekleştirdiği dönemden önceki bir dönemde raporlayamayacaklardır. Ya da ilgili dönemde gider olarak yazılması gereken faaliyet giderlerini ileriki bir döneme aktarmak gibi stratejileri kullanamayacaklardır (Yermack, 2017).

Bu durumda kâr yönetiminin gerçekleşmesi için işletme yönetiminin finansal raporlama süreci üzerindeki yargılarının (kararlarının) değerlendirilmesi gerektiği sonucu ortaya çıkmaktadır. İşletme yönetiminin ister gerçek işlemlerle olsun, ister muhasebe standartlarındaki takdir haklarından kaynaklansın çeşitli güdülerle kâr yönetimi uygulamalarına kalkışması mümkündür (Sakin, 2016). Blok zincirindeki tüm işlemler meydana geldikçe doğrulanıp kaydedildiği için, teorik olarak, özel gerçek zamanlı bir defter oluşturmak kâr yönetimi riskini finansal raporlamada ortadan kaldıracaktır. Gerçek zamanlı raporlamada “bir çeyreğin sonu” olmadığı için, çeyrek dönemin sonunda sayıların iyi görünmesi için var olan tüm olumsuz teşvikler ortadan kaldırılacaktır. Örneğin, birçok işletme, işletme için alınan doğru bir karar olsa bile,

bir çeyrek dönemin sonunda işe alım yapmaz, reklam vermez ve yeni projeleri erteler. Gerçek zamanlı raporlama ile bu teşvikler ortadan kalkacaktır. Gerçek zamanlı raporlama ile şirketler kârlarını yönetmeye daha az; değer kazanmak için uzmanlıklarını yönetmeye daha fazla odaklanacaklardır (FERF ve Deloitte, 2018).

Eğer kullanıcılar blok zincirindeki veriler ile kendi hazırlamış oldukları finansal tablolara güvenirlerse, günümüzde raporlanan veriler ve bunların raporlanma sıklıkları daha az önemli hale gelecektir. İşletmeler tarafından raporlanan verilerin önemi azalacağı için de, veriler yöneticiler tarafından daha az manipüle edileceklerdir.

3.1.2.3. İlişkili Taraf İşlemleri

İlişki taraf açıklamalarının amacı, işletmenin finansal durumu ile kâr veya zararının, ilişkili tarafların mevcudiyetinden, söz konusu taraflarla gerçekleştirilen işlemlerden ve işletme ile ilişkili tarafları arasındaki taahhütler dahil olmak üzere, mevcut bakiyelerden etkilenebileceği olasılığına dikkat çekmek için gerekli olan açıklamaların, işletmenin finansal tablolarında yer almasını sağlamaktır (TMS 24). Gerçek zamanlı muhasebe ile blok zinciri ağındaki kişiler şüpheli varlık transferlerini ya da çıkar çatışmasını gösterecek diğer işlemleri anında fark edebileceklerdir. İlişkili taraf açıklamalarının, dünyanın birçok ülkesinde olduğu gibi, Türkiye’de de finansal tablo dipnotlarında açıklanması zorunludur. Ancak çoğu zaman bu açıklamalarda yer alacak tutarların önemliliği konusunda tartışmalar yaşanmaktadır. Bu konudaki şeffaflık, yöneticilerin aldığı performans primlerini ya da teşviklerini doğrudan etkileyecektir. Bunun sebebi ise blok zinciriyle birlikte işletme içindeki kişilerin işletmenin varlıklarını kendi kişisel çıkarları ve kazançları doğrultusunda yönetemeyecek ve finansal açıdan kötü durumda olan firmaların, yöneticileri tarafından hileli bilgi sunulmasına karşı kredi verenlere gerçek zamanlı gözetim imkânı sunacak olmasıdır (Yermack, 2017).

Özetle, blok zinciri teknolojisinin ortaya çıkışı, finansal muhasebede ölçüm, sunum ve açıklama üzerinde çok ciddi bir etkiye sahip olacak, bu da dipnot açıklamalarındaki ve kâr yönetimindeki hataları azaltacak, niteliksel bilgi üretiminde önemli katkısı olacak ve bilgi asimetrisi sorununu azaltacaktır (Yu, Lin, ve Tang, 2018).

3.2.İç Denetim ve Blok Zinciri Teknolojisi

Blok zinciri teknolojisinin kullanıldığı bir ortam söz konusu olduğunda iç denetçilerin karşılaşacağı sorunlar farklılaşmaktadır. Herhangi yeni bir teknolojinin benimsenmesi ve uygulanması, o teknoloji ile ilgili risklerin uygun bir şekilde yönetilmesine bağlıdır. Özellikle söz konusu olan yeni teknoloji, blok zinciri teknolojisi gibi bir uygulamadan çok kurumun alt yapısının bir parçası ise bu durum daha da önem arz etmektedir (Santhana ve Biswas, 2017).

Blok zinciri teknolojisi, mevcut kayıt tutma, raporlama, güvence ve yönetim uygulamalarını derinden etkileyebilecek finansal ve finansal olmayan bilgilerin şeffaflığını ve erişilebilirliğini arttırmaktadır. Kontroller de dahil olmak üzere sistemler ve süreçler blok zinciri ile farklı bir forma dönüşebilirler, ancak önemli ve gerekli olmaya devam edeceklerdir (Wunsche, 2016).

İç Denetim Enstitüsü Denetim İcra Merkezi, İç Denetim Vakfı ve bir uluslararası denetim ve danışmanlık şirketi olan Crowe, iç denetim mesleğinin blok zinciri teknolojisine ne kadar hazır olduğunu ölçmek amacıyla İç Denetim Enstitüsü üyeleri arasında sınırlı bir anket gerçekleştirmiştir (Kloch ve Simon, 2019). Anket sorularından olan “İşletmeniz blok zinciri teknolojisini kullanıyor mu?” sorusuna katılımcıların %76.6’sı hayır derken, anketteki başka bir soru olan “Blok zinciri teknolojisinin benimsenmesinin önündeki en büyük engel nedir?” için katılımcılar %65.3 oranı ile teknolojinin tam anlaşılması cevabını vermiştir.

Yönetim kurulları hızlı bir şekilde blok zinciri ile kripto paralar arasındaki farkları ve blok zinciri ağ türleri arasındaki farkları öğrenmelidirler. Hatta teknoloji risk komitesi oluşturulmalı veya blok zinciri teknolojisi ve ortaya yeni çıkan teknolojiler konusunda yetkin yeni yöneticilerin yönetim kurullarında yer alması konusunun düşünülmesi gerekmektedir (Kelly, 2019). Blok zinciri teknolojisinin teknolojik riskleri, veri güvenliği riski, birlikte çalışılabilirlik riski ve tedarikçi riski gibi doğal riskleri olduğu için denetçiler bu risklerin müşteriye, iş çevresine ve iç kontrollere olan etkisini değerlendirmek için hazır olmalıdırlar (White, King ve Holladay, 2020). İç denetim birimlerinin blok zinciri kavramları hakkında yeterli bilgi sahibi olarak ortaya yeni çıkan riskleri ve teknolojinin detayları konularında üst

yönetime eğitim ve danışmanlık vermek üzere hazırlıklı olmaları hem denetim mesleği hem de hizmet verilen kuruluş için önemli bir fırsattır (Karahana ve Tüfekçi, 2019:68).

İç denetçiler, bugün rutin olarak gerçekleştirdikleri bazı işlemleri, blok zinciri teknolojisinin özellikleri sayesinde artık yapmayacaklarını anlamalıdır. Örneğin, blok zinciri ortak bir defter olduğu için sistemler arasındaki farklılıkların mutabakatına gerek kalmayacaktır (Rooney, Aiken ve Rooney, 2017). Doğru olan tek bir sistem olacaktır ve tüm paydaşlar bu sisteme erişebilecektir. Ayrıca iç denetçiler hizmet sundukları tarafların blok zinciri teknolojisinin her sorunun çözümü olmadığı konusunda uyarmalıdır (Sheldon, 2019).

İç denetim, blokların yapısının gerçekten değiştirilemez olduğunun, açık ve özel anahtarlar ve dijital imzalar gibi gerekli şifreleme özelliklerinin çalıştığının ve güvenli olduğunun doğrulamasını sağlayabilecek kaynaklara erişebilmelidir. Bu yüzden iç denetçiler, blok zinciri tabanlı uygulamalara planlama aşamasında sürece dâhil olmalıdırlar. Yeterli yönetim, risk yönetimi ve kontrolleri en başta inşa etmek bir sorun ortaya çıktıktan sonra bunları onarmaktan daha kolaydır (Chalker, 2018). Hem iç denetçiler hem de bağımsız denetçiler blok zinciri uyum sürecine erkenden dâhil olmalıdırlar.

Blok zinciri teknolojisi kullanımının iç denetime olumsuz etkileri olabileceği de düşünülmektedir. Blok zinciri iş süreçlerini doğrulayan standardize olmuş bir yol ya da ilgili kontrol ortamı bulunmamaktadır. Her bir blok zinciri ortamının kendine özgü yazılımları vardır ve standardizasyon eksiktir. Bu yüzden her bir şirket kullandığı blok zinciri uygulamasına göre kendine ait kontrol ortamı tasarlamalıdır. Ancak kontrol ortamlarını tasarlayabilecek blok zinciri uzmanları işletmelerde mevcut değildir ve konu ile ilgili çok az bilgi mevcuttur. İşletme yönetimi ise, teknolojik riskleri en aza indirmekten sorumludur. Bu nedenle denetçiler, blok zincirinin benimsenmesinde yeterli gözetimi sağlamak için teknolojik risklerle ilgili yönetim politikalarını ve prosedürlerini kapsamlı bir şekilde gözden geçirmelidir (White, King ve Holladay, 2020).

İç denetçiler için dikkat edilmesi gereken hususlar aşağıdaki gibidir (Kloch ve Simon, 2019):

- *Yönetişim:* Yönetişim, özel anahtarın güvenlik esasları, standart faaliyetlerin tanımı, düğüm ekleme ve çıkarma kuralları ve çeşitli dijital imzaların bileşenleri ve doğrulama algoritmaları gibi konuları içermektedir.
- *Risk yönetimi:* Risk yönetimi, özel anahtarların saklanması ve güvenliği, kod hataları ve kurcalama için akıllı sözleşmelerin izlenimi, blok zinciri dışındaki varlıklarla etkileşim ve zincir dışı veri depolama gibi riskleri kapsamaktadır.
- *Kontrol prosedürleri:* Kontrol prosedürlerinde, ağ erişiminin yönetilmesi, düğümlerin anlaşmaya varması, işlemlerin sıralanması ve yürütülmesi ile mevcut blok sürümlerinin ve içeriğinin bakımı yer almaktadır.

Tüm bu gelişmeler çerçevesinde iç denetçiler sadece muhasebe alanında değil, teknolojik yenilikler ve stratejik konular gibi işletmenin tüm faaliyetleri hakkında bilgi sahibi olup, yeterli donanımı ve bilgiyi edinip, kendilerini geliştirmelidirler. İç denetçiler değişen koşulları takip edip, bu koşullara göre iş yapılarını değiştirmeli ve üst yönetime bunları bildirmeli, yönetimin zamanında ve hızlı bir şekilde sorunlara çözüm üretmesini sağlamalıdır. (Karahana ve Tüfekçi, 2019).

Deloitte, 2017 yılında hazırladığı Blok Zinciri Risk Yönetimi raporunda işletmelerin blok zinciri teknolojisini uygulamaları durumunda karşılaşılabilecekleri riskleri üç ana başlıkta açıklamış ve blok zinciri risk yönetimi çerçevesi hazırlamıştır. Şekil 3.2.1.'de görülen Etkin Bir Blok Zinciri Risk Yönetimi Çerçevesinde yer alan bu üç ana risk ise standart risk faktörleri, değer transferi risk faktörleri ve akıllı sözleşme risk faktörleridir.

Şekil 3.2.1.Etkin Bir Blok Zinciri Risk Yönetimi Çerçevesinin Bileşenleri

Risk yönetimi çerçevesi								
İş hedefleri	Büyüme/yenilik		Müşteri tecrübesi		Maliyet tasarrufu		Pazara daha iyi sunma süresi	Risk ve uygunluk yönetimi
	Bilgi teknolojisi		İnsan kaynakları		Uygunluk		Finans	Diğer
Temel süreçler, yardımcı fonksiyonlar	Standart risk faktörleri				Değer transferi risk faktörleri		Akıllı sözleşme risk faktörleri	
	Stratejik	İtibar	İşletme sürekliliği	Güvenlik	Mutabakat protokolü	Veri gizliliği	İş ve yasa	Yasal yükümlülük
	Yasal	Operasyonlar ve Bilgi teknolojisi	Sözleşme	Tedarikçi	Anahtar yönetimi	Likidite	Sözleşmenin yürütülmesi	Yönetişim
İşletme modeli bileşenleri								
Yönetişim ve gözetim		Politikalar ve standartlar		Yönetim süreçleri		Araçlar ve teknoloji	Risk ölçümü ve raporlama	Risk kültürü

Kaynak: SANTHANA, P., BISWAS, A.:2017 Blockchain Risk Management–Risk Functions Need to Play an Active Role in Shaping Blockchain Strategy. *Deloitte Development LLC*.

3.2.1. Standart Risk Faktörleri

Blok zinciri teknolojisi işletmeleri mevcut iş modellerindeki benzer risklerle karşı karşıya bıraksa da, işletmelerin dikkat etmesi gereken bazı yeni noktalar da bulunmaktadır. Standart risk faktörleri stratejik risk, işletmenin sürekliliği riski, itibar riski, bilgi güvenliği riski, yasal risk, operasyonel ve bilgi teknolojileri riski, tedarikçi riski ve sözleşme riskini kapsamaktadır.

Stratejik risk: İşletmeler stratejik riskleri değerlendirirken üç noktaya dikkat etmelidirler. Birincisi, işletmeler blok zinciri teknolojisinin benimsenmesinde lider konumunda olmayı mı yoksa teknoloji tam olgunlaşınca kadar onu benimsemek için beklemek isteyip istemediklerini değerlendirmelidirler. İkincisi, blok zinciri teknolojisi eşten eşe yapıya sahip olduğu için, işletmelerin doğru ağda bulunması çok önemlidir. İşletmeler içinde bulundukları zincirdeki farklı kurumlardan etkilenebilecekleri için dahil olmak istedikleri ağı seçerken çok dikkatli olmalıdırlar. Üçüncüsü, dahil oldukları blok zincirinde kullanılan platformun seçimi bazı hizmet ve ürünleri sunarken kısıtlamalar getirebilmektedir (Santhana ve Biswas, 2017).

İç denetim, risk ve uyumluluk, teknoloji, iş süreçleri, veri analizi ve finans konularında çözümler sunan danışmanlık şirketi Protiviti, 2019 yılında kurumsal

riskler konusunda bir anket düzenlemiştir. Yapılan anket çalışmasının sonuçlarına göre, yönetim kurulu başkanlarının ve diğer üst düzey yöneticilerin en büyük endişesi yeni gelişen teknolojilere ayak uyduramamak ve rekabette yer bulamamaktır (Protiviti, 2019). Bu durumda yöneticilerin yeni teknolojiler konusunda karşılaştıkları en önemli risk, temkinli davranıp gelişmeleri izlemeleri durumunda teknolojinin gerisinde kalmaları ve fırsatları kaçırmalarıdır. Diğer risk ise, erken davranıp bu fırsatları yakalama stratejisini seçerek olumsuz bir senaryo ile karşılaşılması durumunda gereksiz yatırım yapıp, kaynakların israf edilmesidir (Karahan ve Tüfekçi, 2019). Bu sebeple iç denetim departmanlarının blok zinciri teknolojilerinden kaynaklı riskleri değerlendirebilecek yeterli kaynağa ve bu departmanda çalışanların yeterli bilgiye sahip olması gerekmektedir. Bu kaynaklar yeni işe alınan kişiler veya dışarıdan kaynak kullanma, bilgi teknolojileri bölümünde çalışan veya siber güvenlik ekibindeki kişilerle daha sık iletişim halinde olma veya mevcut çalışanları blok zinciri ile ilgili eğitim ve toplantılara gitmelerini teşvik ederek bunlara ek bütçe ayırma olabilir (Kelly, 2019).

İşletmenin sürekliliği riski: Diğer tüm teknoloji uygulamalarında olduğu gibi, işletmelerin blok zinciri uygulamasına ilişkin iş sürekliliği ve felaket risklerini ele almak için bir planı olması gerekmektedir. Blok zincirindeki bir bileşenin herhangi bir potansiyel faktörden etkilenmesi durumunda blok zincirine ne olacağına dair somut bir anlayış olmalıdır (Maguire ve ark., 2018). Blok zinciri üzerine inşa edilen iş süreçleri, siber saldırıların yanı sıra teknolojik ve operasyonel hatalara karşı savunmasız olabilir. İşletmelerin bu tür riskleri azaltmak için sağlam bir iş sürekliliği planı ve yönetim çerçevesi olması gerekmektedir (Santhana ve Biswas, 2017).

Ayrıca, blok zinciri çözümlerinin birçok iş sürecinin süresini kısaltma potansiyeli bulunmaktadır, bu yüzden iş sürekliliği planlarında daha kısa vadeli kurtarma planları ve iyileştirme süresi hesaba katılmalıdır. İşletmeler, bir blok zinciri ağına dahil olmanın iş sürekliliği planlarını nasıl etkileyebileceğini ve ağın uğrayacağı önemli bir zarardan etkili bir şekilde kurtulmak için uygun önlemlere sahip olup olmadığını düşünmelidirler (Santhana ve Biswas, 2017).

İşletme yönetiminin iç denetim bölümünden beklentisi sadece süreçlerin etkinliği hakkında bilgi vermek değil aynı zamanda süreçlerin geliştirilmesi için tavsiyelerde bulunarak işletmeye değer katmasını sağlamaktır (Turner, 2010). Bu bağlamda, iç denetçiler şirket içinde blok zinciri ile ilgili çalışmaların yapılıp yapılmadığını, üzerinde çalışılan ya da kullanılmakta olan blok zinciri uygulamaları varsa bunları da yönetime bildirmelidir. Ayrıca iç denetçi risk değerlendirmesi yaparken, blok zinciri ile ilgili yapılan çalışmalarda yavaş gidilip gidilmediği, ya da hedeflenenden daha hızlı gidildiği, fırsatları yakalamak isterken tehditleri gözden kaçırma durumu olup olmadığını da üst yönetime sunmalıdır (Kelly, 2019). İç denetçiler yeterli seviyede şeffaflık sağlandığını ve blok zincirinin ve diğer uygulamaların amaçlandığı gibi çalıştığını doğrulamalıdır.

İtibar riski: Blok zinciri teknolojisi işletmelerin temel altyapılarından birisidir, bu yüzden işletmenin önceki altyapıları ile sorunsuz bir şekilde çalışmak zorunda kalacaktır. İşletmelerin bu konuda başarısız olması durumunda müşteri memnuniyeti olumsuz yönde etkilenecek ve yasal sorunlar ile karşılaşacaklardır (Santhana ve Biswas, 2017).

Denetçiler, blok zinciri altyapısının planlanması, uygulanması ve sürdürülmesinde yer alanların niteliklerini düzenleyen kurallara ilişkin yönetim politikalarını değerlendirmelidirler. Denetçiler, müşterinin blok zinciri ile ilgili iş sürecini, eski sistem konularının ilk risk değerlendirmesini tamamladıktan sonra, belirlenen farklılıkların veya çatışmaların çözümüne ilişkin müşterinin politikalarını ve prosedürlerini araştırmalıdır (White, King ve Holladay, 2020). Ayrıca denetçiler, müşterinin iş süreçlerinin ve mevcut bilgisayar sistemlerinin özel blok zinciri ekosistemindeki diğer katılımcıların süreçleri ve sistemleri ile uyumlu olup olmadığını sorgulamalıdır.

Bilgi güvenliği riski: Blok zinciri teknolojisi işlemler için güvenlik sağlarken, hesap ve/veya cüzdanların güvenliğini sağlamamaktadır. Dağıtık bir veri tabanı ve kriptoloji kullanılarak imzalanan bu defter verinin değiştirilmesini önlemektedir. Ancak hesapların içinde olan değerlerin çalınıp çalınmaması konusunda hala şüpheler mevcuttur. Ayrıca, özellikle özel ve izin gerektiren blok zinciri türlerinde, blok zinciri

ağındaki kötü niyetli kişilerin ağdaki düğümlerin kontrolünün %51'ini belli bir süreliğine ele geçirebilmesi durumu gibi, siber güvenlik riskleri mevcuttur (Santhana ve Biswas, 2017).

İç kontrol, örgütün planı ile işletmenin varlıklarını korumak, muhasebe bilgilerinin doğruluğunu ve güvenilirliğini sağlamak, faaliyetlerin verimliliğini arttırmak, tespit edilmiş yönetim politikalarına bağlılığı özendirmek amacıyla kabul edilen ve uygulamaya konulan tüm önlem ve yöntemleri içerir (Güredin, 2014). Bu sebeple, hem bağımsız denetçiler hem iç denetçiler blok zinciri içindeki kontrolleri bilmek ve anlamak durumunda kalacaktır. Blok zinciri ağındaki hangi düğümlerin mutabakat sürecinde yetkilendirildiği, ağa dahil olan düğümlerin hesaplama gücünün dağılımı ve ilgili blok zincirinde hangi mutabakat mekanizmasının (PoW ve PoS gibi) kullanıldığının belirlenmesi ve bu mutabakat protokolünün değerlendirilmesi denetçiler tarafından yapılmalıdır (Bible ve ark., 2017). Böylelikle denetçiler, hesaplama gücünün tek bir düğümden ya da belli düğümlerde toplanıp toplanmadığını anlayıp, %51 saldırısı ile oluşabilecek hile ya da kötü niyetli faaliyetleri dikkate almalıdırlar (Rückeshäuser, 2017).

Yasal riskler: Günümüzde, dünya genelinde blok zinciri teknolojisi ile ilgili yasal gereklilikler konusunda belirsizlikler söz konusudur. Ayrıca her bir kullanım alanı ve blok zinciri uygulaması için de yasal riskler olabilecektir çünkü ağa dahil olan katılımcıların türü, ağın sadece ülke içi işlemlere ya da ülkeler arası işlemlere izin verip vermeyeceği de önemlidir. Bu aynı zamanda sınırlar arası mevzuatlardaki gizlilik ve bilginin korunması ile de ilgilidir (Santhana ve Biswas, 2017). Örneğin ABD'de, hasta kayıtlarının paylaşılmasına ve kaydedilmesine yönelik blok zinciri çözümleri, ABD Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasasına (Health Insurance Portability and Accountability Act - HIPAA) tabi iken, Avrupa'da kişisel veriler için gereksinimler Genel Veri Koruma Yönetmeliği (General Data Protection Regulation- GDPR) ile korunmaktadır. GDPR, kişisel verilerin Avrupa Birliği dışına çıkarılması için gereksinimleri içermektedir (Caron, 2017). Blok zinciri defterleri farklı konumlarda bulunan düğümlerde saklandığı için farklı uluslararası yargı alanlarına tabi olabilir, bu nedenle mevcut yasal tanımlar ve vergi yasaları ile çatışabilirler (Wiatt, 2019).

Blok zincirleri, mali düzenleyiciler ve hükümetler tarafından yeterince güvenli veya şeffaf kabul edilmemektedir (Wunsche, 2016). Aktif bir şekilde uygulamaya geçilmeden önce bu teknolojinin yasalarla ya da mevzuatla ilgili açıklaması ve yönlendirmesi olması gerekir. Her ne kadar blok zinciri yeni bir teknoloji olsa da, bu durum yeni bir teknoloji ile ilk kez karşılaşıldığı anlamına gelmemektedir. Bu yüzden iç denetim bölümleri tarafından yeterli güvencenin sağlanabilmesi için yeni standartlar yazılmalıdır. PwC'nin 2018 yılında gerçekleştirdiği ankette blok zinciri teknolojisinin benimsenmesinin önündeki engeller sorulmuş ve katılımcıların %48'i yasal belirsizlik olduğunu belirtmiştir (PwC, 2018). Blok zinciri teknolojisine ait bir takım risk yönetimi, iç kontrolle ilgili soru işaretleri mevzuatlarla giderilemezse bu teknolojiden büyük ölçüde yararlanabilmek şuan için çok mümkün gözükmemektedir.

Operasyonel ve bilgi teknolojileri riski: Mevcut olan politika ve prosedürler yeni iş süreçlerini yansıtmaması için güncellenmelidir. Ek teknolojik kaygılar arasında hız, ölçeklenebilirlik ve blok zinciri teknolojisinin uygulanmasında eski sistemlerle ara yüz oluşturması sayılabilir (Sanhtana ve Biswas, 2017).

Blok zincirleri henüz mevcut sistemler kadar ölçeklenebilir değildir ve blok zincirlerini korumak için gereken maliyet ve hesaplama gücü (computing power) ile ilgili sorular vardır (Wunsche, 2016). İşletme kaynakları, bugünün ve yarının hesaplama gücüne yatırım yapmak için yeterli olmalıdır (White, King ve Holladay, 2019).

İşletmelerin güçlü ve sağlam bir bilgi teknolojisi yönetişimine duydukları ihtiyaç blok zinciri teknolojisi ile değişmeyecek, hatta bu yönetişim, blok zinciri ile daha karmaşık bir hale gelecektir (Sheldon 2019:3). Yine Sheldon (2019), özel ve izin gerektiren blok zinciri denetimlerini yaparken dikkate alınacak olan bilgi teknolojileri genel kontrollerini “program geliştirme ve değişim yönetimi”, “bilgisayar işlemleri” ve “programlara ve veriye erişim” olmak üzere üç başlıkta sınıflandırarak incelemiştir.

Mevcut sistemlerin tasarımında değişiklik yapılması belli bir süreç gerektirmektedir. Bu süreç değişiklikle ilgili bir talepte bulunma, yeni sistemi geliştirme, test etme, yetkilendirme ve güncel olan sistemi yürürlüğe koyma aşamalarından oluşmaktadır. Süreçteki her bir aşama için kontrol mekanizması

gerekmektedir. Denetçiler özellikle konsorsiyum blok zincirinde yapılabilecek bu değişikliklerin önemini anlamalı ve konsorsiyum blok zincirinde bulunan kişilerin tümünün bu değişiklikleri kabul edip etmediğini veya ağdakilerin bu değişiklikleri uygulamama riskini ve buna bağlı olarak zincirde çatallanma⁴ riskini göz önünde bulundurmalarıdır. Ayrıca, konsorsiyumda bulunan üyeler tarafından bu değişikliklerin kabulünden sonra bu değişikliklerin uygulanması konusu da denetçiler tarafından dikkat edilmesi gereken bir konudur (Sheldon, 2019:5).

Denetçilerin aynı zamanda mevcut sistemde depolanan verilerin blok zincirine aktarımı sırasında da dikkat etmeleri gereken hususlar vardır. Müşteri işletmenin kuruluşundan bugüne kadar kaydetmiş olduğu tüm geçmiş verileri blok zinciri sistemine aktarması mümkün değildir. Bunun yerine işletmeler mevcut sistemlerindeki geçmiş verilerini saklarken bir yandan da meydana gelen yeni işlemleri blok zincirine kaydedecektir. İşletmeler eski sistemlerini bırakıp özel ve izin gerektiren blok zincirleri kullanmaya başladıkça verinin toplanmasında ve işlenmesinde bir geçiş dönemi yaşanacaktır. Böyle bir geçiş yaşandığı zaman mevcut politika ve prosedürlerin devam ettirilmesi hatta daha da geliştirilmesi önem arz etmektedir. Bunun sebebi ise bu politika ve prosedürler doğrultusunda oluşacak verilerin en sonunda blok zincirine kaydedilecek olmasıdır. Hem bağımsız olarak hem de sistemler arasındaki bağlantıların korunması için blok zinciri için kontroller geliştirilmelidir. Her ne kadar blok zincirine kaydedilen veriler değiştirilemez özellikte olsa da, zincirin dışındayken hala bir takım bilgi teknolojisi risklerine karşı savunmasız kalacaktır (Sheldon, 2019:5-6).

Ayrıca, eski sistemler blok zinciri teknolojisi ile bir ara yüz oluşturacaktır. Verilerin blok zincirine geçişindeki ara yüz değişimi bu yeni ortamdaki en önemli kontrol noktalarından biri olacaktır. Denetçiler bu değişimin en kontrollü bir şekilde nasıl gerçekleşebileceği konusunda müşterileri ile birlikte hareket etmelidirler. Her ne kadar blok zinciri iş sürekliliğinde ve felaket kurtarma planlarında birçok endişeyi gidermede yardımcı olsa da, denetçiler, blok zinciri ara yüzü görevi gören eski

⁴ Özet değerler takip edilerek en son bloktan ilk bloğa kadar geri gidilebilmektedir. Bir bloğa bağlı birden fazla blok olmamalıdır. Böyle bir durum meydana gelirse bu duruma çatallanma (fork) adı verilir. Çatallanmanın olduğu yer tespit edilerek kısa zincir yok edilir ve blok zinciri oluşumuna uzun zincir üzerinden devam edilir (Kırbaş, 2018).

sistemlerin erişilemez olması durumunda hangi prosedürlerin takip edileceğini görmek için iş sürekliliği ve felaket kurtarma planlarını değerlendirmelidirler (Sheldon, 2019:7).

Blok zincirinin bilgi teknolojileri altyapısının bir parçası olduğu unutulmamalı ve düzgün çalışan bilgi teknolojileri genel kontrolleri desteklenmelidir. Etkin olmayan bir bilgi teknolojileri genel kontrolleri ile blok zinciri tarafından üretilen verilerin güvenilirliği tam olarak sağlanamayacaktır.

Tedarikçi riski: Blok zinciri teknolojisinin önemli bir kısmı işletme dışı taraflardan temin edileceği için, işletmeler önemli bir üçüncü taraf riski ile karşılaşacaktır (Santhana ve Biswas, 2017).

Blok zinciri teknolojisi karmaşık bir yapıya sahiptir ve çok az sayıda kuruluş başarılı bir uygulama geliştirebilmek için kurum içi yeteneğe sahiptir. Blok zinciri hizmetlerine olan potansiyel talep ile kurum içi yetenekler arasındaki boşluğu doldurmak üzere üçüncü taraf sağlayıcılar için gelişen bir pazar oluşmaktadır (Martin, 2018). Talep edilen bu hizmetler blok zinciri mimarisi ve gelişimi, ödeme platformları, akıllı sözleşme gelişimi, blok zinciri teknolojisi entegrasyonu, yasal hizmetler, muhasebe hizmetleri, kripto para değişimi ve kripto değerlendirme servisleri olmakla beraber sadece bunlarla sınırlı değildir (Prewett, Prescott ve Phillips, 2020). Henüz emekleme aşamasında olan bu pazardaki tedarikçilerin çoğu yeni gelişen ve hızlı büyüyen şirketler olduğu için kendi stratejik gelişimi, regülasyonlarla uyumluluk, istikrarlı olmayan finansal durumları ve yetersiz personel gibi kendine ait sorunları da bulunmaktadır (Caron, 2017). Örneğin, 2015 yılında Ripple platformu kendi kripto parasını kara para aklayanlar veya terörist finansörleri tarafından kullanılmasına karşı korumak için tasarlanmış yeterli bir kara para aklama karşıtı (Anti Money Laundering-AML) programı uygulayamaması gerekçesi ile ABD Hazine Bakanlığı'na bağlı Mali Suçlar Takip Ağı (Financial Crimes Enforcement Network-FinCEN) tarafından 700.000\$ para cezasına çarptırılmıştır (FinCEN, 2015). Ayrıca blok zinciri servisleri sağlayacak olan bu üçüncü taraf tedarikçilerin güvenlik zafiyetleri ve kodlamada yapacakları hatalar, sözleşmeye taraf işletmeleri büyük bir risk ile karşı karşıya bırakacaktır.

Bazı yazılım sağlayıcıları, örneğin, şüpheli ani artışları veya iş hacmindeki düşüşleri yöneticileri uyarmak için akıllı sözleşmelerin gerçek zamanlı olarak izlenmesini sağlayan ürünlerle birlikte, blok zinciri kabinleri güvenliğini değerlendirmek için teknoloji yaratmaya odaklanmıştır. Bu tür yazılımları değerlendirme, seçme ve uygulama yeteneği, iç denetim yöneticisinin yeni yetenekler alırken veya mevcut personeli eğitirken araması gereken yeni bir teknik özellik olacaktır (Kloch ve Simon, 2019).

Ayrıca işletmeler üçüncü tarafın mevcut durumu, kontrolleri ve hizmetleri hakkında iç ve dış denetim güvencesi talep etmeli ve üçüncü taraf bir tedarikçiye başvurmadan önce denetçiye, tedarikçinin güvenlik incelemesine dair kapsamlı bir araştırma işletmeler tarafından sağlanmalıdır. Bu araştırma bağımsızlığı, olası çıkar çatışmalarını ve oluşturulmuş bir geçmiş kaydını ele almalıdır. Oluşturulan geçmiş kaydı, üçüncü taraf satıcının hizmetlerinden yararlanan diğer şirketlerden gelen güvenilir referanslarla doğrulanmalıdır. Bunun yanında müşteri, üçüncü taraf ilişkilerinin sürekli izlenmesini sağlamak için gereken kontrollere sahip olmalıdır (White, King ve Holladay, 2020).

Planlama, durum tespiti, üçüncü taraf seçimi ve fesih aşamaları dahil olmak üzere üçüncü taraf ilişkilerinin sürekli yaşam döngüsünü kapsayan risk yönetimi stratejilerinin uygulanması; sözleşme sonrası uyumluluk değerlendirmeleri ve sürekli izleme programları yürütmek; üçüncü tarafın uzun vadeli stratejik hedefleri hakkında bilgi edinmek için üçüncü taraf ilişkilerini etkin bir şekilde yönetmek ve satıcı için önemli bir risk oluşması durumunda kullanılabilecek resmi iletişim hatlarının oluşturulması blok zinciri yazılım sağlayıcıları ile ilgili riskleri yönetmek için uygulanabilecek bazı faaliyetlere örnek olarak gösterilebilir (Caron, 2017).

Sözleşme riskleri: Tedarikçi riski ile kısmen ilişkili olan sözleşme riski, blok zinciri uygulamalarının dağıtımında bulunan tüm ilişkileri yönetmek için sözleşmelerin geliştirilmesi ve yürütülmesi riskidir (Prewett, Prescott ve Phillips, 2020).

Blok zinciri ağındaki düğümlerin hakları ve ayrıcalıkları değişiklik gösterebildiği için her bir ilişki için farklı hizmet seviyesi anlaşması gerekebilecektir. Hizmet sağlayıcılarıyla yapılan uygunluk açısından izlenmesi gereken hizmet seviyesi

anlaşmalarına (service level agreement-SLA) ek olarak, ağdaki düğümler ile ağın yöneticisi arasında birkaç hizmet seviyesi anlaşması olması beklenmektedir (Santhana ve Biswas, 2017). Etkin hizmet seviyesi anlaşmaları izlenmesi ve yürütülmesi başarılı blok zinciri deneyimi için kritik bir noktadır (Prewett, Prescott ve Phillips, 2020).

3.2.2. Değer Transferi Risk Faktörleri

Blok zinciri merkezi aracı bir kurum olmadan eşten eşe değer değişimi ya da transferi yapmayı mümkün kılmaktadır. Bu değerler varlıklar, kimlikler veya herhangi bir bilgi olabilir. Bu yeni iş modeli daha önce aracı kurumlar tarafından yönetilen bir takım riskleri, birbiri ile iş yapan taraflara maruz bırakmaktadır. Bu bölümdeki riskler mutabakat protokolü riskini, anahtar yönetimi riskini, veri gizliliği riskini ve likidite riskini kapsamaktadır.

Mutabakat protokolü riski: Bir blok zincirinde değer aktarımı, blok zinciri defteri kaydını güncellemek için katılımcı düğümler arasında fikir birliğine ulaşan bir şifreleme protokolünün kullanılmasıyla gerçekleşmektedir. Kullanılan her bir mutabakat protokolü blok zinciri çerçevesi, uygulama alanı ve ağ katılımcısı gereksinimleri bağlamında değerlendirilmelidir (Santhana ve Biswas, 2017).

Bir blok zinciri ağıyla ilişkili doğal risk, ağdaki düğümlerin sayısına, yedek düğümlerinin varlığına veya yokluğuna ve bu tür yedekleme sistemlerinin gerekli olup olmadığına ilişkin yönetim kararına bağlı olarak önemli ölçüde değişebilir. Bir tedarik zincirindeki bir düzine satıcıdan oluşan özel bir blok zinciri, binlerce hastanın tıbbi kayıtlarını içeren büyük bir sağlık blok zincirinden çok farklı bir risk profili sunmaktadır (Kloch ve Simon, 2019)

Ayrıca ağ katılımcılarının işlemlerini yapılandırmak ve kaydetmek için kullanmayı kabul ettikleri mutabakat algoritmaları blok yapısı, depolama ihtiyaçları ve güvenlik riski gibi diğer birçok faktörü doğrudan etkilemektedir (Kloch ve Simon, 2019).

Anahtar yönetimi riski: Mutabakat protokolü bir blok zinciri defterini değiştirilmez bir şekilde mühürlenirken ve geçmiş işlemlerde herhangi bir bozulma mümkün olmazken, özel anahtar hırsızlığına ve genel adreslerle ilişkili varlıkların ele

geçirilmesine hala açıktır. Özellikle tek bir denetleyicinin veya blok zinciri içindeki potansiyel bir üst yönetimin bulunmaması nedeniyle, yanlışlıkla anahtarın kaybolması veya özel anahtar hırsızlığı durumunda dijital varlıklar, telafi edilemez hale gelebilir (Santhana ve Biswas, 2017).

Örneğin, bir konsorsiyum blok zinciri yeni bir banka olan Banka Y'yi kabul etmekte ve bu durumda Banka Y'ye özel bir anahtar verilmesi gerekmektedir. Bu özel anahtar bundan sonra Banka Y tarafından gelecekteki işlemleri imzalamak için kullanılacaktır. Bu durum, blok zinciri ağında bulunan diğer katılımcılara Banka Y'nin işlemi usulüne uygun olarak yetkilendirdiğine dair güvence sağlamaktadır. Eğer Banka Y bu özel anahtarı kaybederse ve kötü niyetli bir kişi bu anahtarı ele geçirirse, bu kötü niyetli kişi işlemleri Banka Y'nin yerine imzalayabilecek, "Banka Y" adına yetkisiz işlemleri kabul edebilecek ve/veya blok zinciri konsorsiyumundaki diğer üyelere sahte belge düzenleyebilecektir. Bu sebeple özel anahtarın kaybolması ağıdaki diğer katılımcılara ciddi hasarlar verebilmektedir. Her bir kişinin özel anahtarlarının güvenliği ve korunması blok zincirinin başarılı olmasında önemli bir noktadır (Deloitte, 2019).

Denetçiler, blok zinciri ağında dijital varlık transferlerinde kullanılan açık ve gizli anahtarların saklanma sürecini ve özel anahtarın çalınması durumunda bu anahtarla ilişkili varlığın kontrolünün yeniden ele alınma sürecini dikkate almalıdır. Bir çalışanın, daha önce anahtarla ilişkilendirilmiş varlığa erişme izni artık mümkün değilse bu varlıkların güvenliği de denetçiler tarafından dikkate alınması gereken bir konudur (Sheldon, 2019).

Veri gizliliği riski: Mutabakat mekanizması, izin gerektiren bir blok zinciri ağında tüm katılımcılara belli bilgilere erişebilme imkânı sağlamaktadır. Bilgiye erişim sınırlandırılıp şifrelenebilirken, yine de bilgilerin açığa çıkma konusunda bazı zayıflıklar vardır. Bu nedenle, blok zinciri ağındaki kuruluşların, kişisel tanımlanabilir bilgilerin (personally identifiable information-PII) tehlikeye atılmamasını veya çalınmamasını sağlamak için veri mahremiyeti ve gizliliği ile ilgili riskleri ele alması gerekmektedir (Deloitte, 2019).

İzin gerektiren bir blok zinciri ağındaki işlemler, içeriği açığa çıkarmamak için özetleme değerleri ile saklanabilirken, belirli üst veriler (metadata) her zaman ağ katılımcıları tarafından kullanılabilir olacaktır. (Prewett, Prescott ve Phillips, 2020).

Örneğin; “Satıcı A” sevk öncesi finansman için bir banka ile işlem yapmaktadır. Bu işlemin bir parçası olarak Satıcı A aynı zamanda “Nakliye Şirketi X” ile de çalışmaktadır. Bu işlemin detayları belki şifrelenmekte ve bu yüzden “Alıcı B” gizli tutulan işlem bilgilerini görememektedir. Ancak “Alıcı B” ağıdaki belirli bir katılımcının banka ve nakliye şirketi ile işlem yaptığını görebilmektedir. Bu bilgi tek başına anlamlı olmasa da binlerce başka işlemle birleştirilirse, bu veriler uygulamanın tasarımında amaçlanmayan şekilde ilgili bilgileri “Alıcı B” ye sağlayabilir (Deloitte, 2019). Şirketlerin bu değer zincirinin katılımcıları arasındaki veri paylaşımı ile ilişkileri riskleri düşünmeleri gerekmektedir.

Likidite riski: Uluslararası Ödemeler Bankası, blok zinciri gibi DDT'nin benimsenmesinin yeni likidite riskleri getirebileceği konusunda uyarmıştır. Mevcut iş modellerinde araçlar tipik olarak karşı taraf risklerini üstlenir ve anlaşmazlıkların çözülmesine yardımcı olur. Dağıtılmış bir güven ortamında uyuşmazlıkların çözümü, önceden belirlenmiş düzenlemelere dayanan bir gerekliliktir (Santhana ve Biswas, 2017).

3.2.3.Akıllı Sözleşme Risk Faktörleri

Akıllı sözleşmeler, potansiyel olarak karmaşık iş, finansal ve yasal düzenlemeleri blok zincirine kodlayabilir ve bu düzenlemelerin fiziksel dünyadan dijital dünyaya bire bir eşleştirilmesiyle ilişkili riskle sonuçlanabilir. Ayrıca, akıllı sözleşmeler sözleşmenin yürütülmesini tetiklemek için blok zinciri kâhinlerine bağlı oldukça siber güvenlik riskleri artacaktır. Bu bölümdeki riskler iş ve hukuki riski, sözleşmenin yürütülmesi riskini, yasal yükümlülükler riskini ve bilgi güvenliği riskini kapsamaktadır.

İş ve hukuki risk: Akıllı sözleşmeler, taraflar arasında tanımlanan ticari, ekonomik ve yasal düzenlemeleri doğru bir şekilde temsil etmelidir. Bir blok zinciri ağında tanımlanan akıllı sözleşmeler, ağıdaki tüm katılımcılara tutarlı bir şekilde

uygulanacaktır. Bu nedenle, bu akıllı sözleşmelerin istisna durum yönetimi yeteneğine sahip olması ve bu istisnaların blok zinciri çerçevesindeki sonuçlarının, ağdaki diğer tüm akıllı sözleşmelerin iş ve yasal düzenlemelere uyma ve mevzuata uygunluk açısından test edilmesi gerekecektir (Santhana ve Biswas, 2017).

İster özel, ister açık, ister konsorsiyum blok zinciri ağ yapısı kullanılsın, iş mantığı⁵ akıllı sözleşmelerle kodlanmaktadır. Akıllı sözleşmeler genel olarak siber saldırılar için en zayıf noktadır.

Sözleşmenin yürütülmesi: Günümüzde, fiziksel bir sözleşmenin yerine akıllı bir sözleşmenin uygulanması konusunda yasal bir emsal bulunmamaktadır ve akıllı sözleşmeleri düzenleyen herhangi bir düzenleme yoktur. Ayrıca, bir blok zinciri üzerindeki veriler değişmez olduğundan, finansal düzenlemeye ilişkin yasal sınırlar içinde olmayan blok zincirinde geçmişten gelen veriler üzerinde hareket ederek mevcut düzenlemelerin ihlallerinden kaçınmak için akıllı sözleşmeleri değiştirmeye dikkat edilmelidir (Santhana ve Biswas, 2017).

Akıllı sözleşmelerin düzenlenmesinde, kodlar programlandığı gibi yürütülür, ancak istenildiği gibi yürütülmez. Eğer sözleşme mantığı düzgün bir şekilde geliştirilmemiş, kodlanmamış ve test edilmemişse veya akıllı sözleşme blok zincirinde yürütülmeye başladıktan sonra koşullar değişmişse, istenmeyen sonuçlar ortaya çıkabilir. Bu gibi durumlarda, çözüm için başvurulacak bir avukat veya mahkeme gibi bir aracı yoktur. Akıllı sözleşmedeki boşluklardan yararlanılabilir ve kod yanlışlıkla veya kötü niyetli kişiler tarafından hiçbir cezaya tabi tutulmadan manipüle edilebilir (Prewett, Prescott ve Phillips, 2020).

Denetçiler, birden fazla kuruluşun katılımıyla oluşturulmuş olan konsorsiyum blok zinciri ağlarındaki akıllı sözleşmelerde kimlerin değişiklik yapma yetkisi olduğunu, kimlerin verileri manipüle edebilme imkanı olduğunu ve ayrıca kimlerin bu ağa artık erişme hakkı olmadığını değerlendirmelidirler (Sheldon, 2019).

Yasal Yükümlülükler: İzin gerektiren bir blok zinciri ağındaki yasal sorumluluk, bir akıllı sözleşmenin ağdaki iki veya daha fazla kuruluş ile uygunsuz, hatalı veya kötü

⁵ İş mantığı, bilgisayar yazılımında, verilerin nasıl oluşturulabileceğini, saklanabileceğini ve değiştirilebileceğini belirleyen gerçek dünya iş kurallarını kodlayan parçasıdır.

niyetli bir şekilde yönetilmesi nedeniyle sonuçlanan bir işlemle, varlıkların bu işlemi yapan kuruluşlar aracılığıyla ağdan çıkmasına neden olması nedeniyle belirsizliğini korumaktadır (Santhana ve Biswas, 2017).

Gerçek zamanlı akıllı sözleşme izlemeye ek olarak, çoğu kuruluş - özellikle de büyük hissedar gruplarına cevap vermesi gerekenler - aynı zamanda sistemlerin amaçlanan bir şekilde çalıştığını göstermek için düzenli olarak denetim ve raporlama gerektirecektir. Bu faaliyetlerin de uzun vadeli iç denetim stratejisi ve planına dahil edilmesi gerekmektedir (Kloch ve Simon, 2019).

Bilgi güvenliği riski: Katılımcı kuruluşlar veya ağ yöneticisi, yeni akıllı sözleşmeleri dağıtmak veya mevcut akıllı sözleşmeleri değiştirmek için güçlü bir yönetim ve değişiklik kontrol sürecine ihtiyaç duyacaktır. Ayrıca akıllı sözleşme operasyonlarındaki aksaklıkları tespit etmek ve bunlara yanıt vermek için sağlam bir olay yönetimi sürecine ihtiyaç duyulacaktır (Santhana ve Biswas, 2017).

Tezin 2.3.7. Akıllı Sözleşmeler bölümünde bahsedildiği gibi blok zinciri kâhinleri, blok zinciri içindeki akıllı sözleşmelerin yürütülmesini tetiklemektedir. Blok zinciri kâhinleri blok zinciri ağının dışında olan ancak ağa veri besleyen cihazlardır. Herhangi bir bilgisayar donanımı veya yazılımı gibi blok zinciri kâhinleri de blok zincirindeki verileri bozmak veya yok etmek için kötü niyetli saldırılara maruz kalabilir ve bozulabilir (Prewett, Prescott ve Phillips, 2020). Bir blok zincirindeki en büyük risk blok zinciri kâhinleridir.

Örneğin, tedarik zinciri ile ilgili bir blok zinciri ağı, belirli ürünler ayrıldığında veya istenilen konuma ulaştığında akıllı sözleşmeleri bilgilendirmek için donanım araçları olarak hizmet etmek üzere fiziksel varlıklara bağlı radyo frekansı ile tanımlama (Radio Frequency Identification-RFID) etiketlerine güvenebilir. Böyle bir durumda denetçi, blok zinciri kâhinlerinin blok zincirine girmeden önce verilerin bütünlüğünü tehlikeye atabilecek hatalardan veya gömülü kodlardan arınmış olup olmadığını belirlemek için müşteri tarafından kullanılan prosedürleri değerlendirmek isteyecektir. Denetçiler ayrıca blok zinciri kâhinleri donanımı olarak kullanılan nesnelerin interneti cihazlarının fiziksel kontrolünü ve özellikle bu cihazları

uygulamak, deęiřtirmek veya kullanımdan kaldırmak için kullanılan prosedürleri deęerlendirmelidirler (Sheldon, 2019).

Blok zinciri kâhinleri ile ilgili her türlü risk akıllı sözleşmelere gömülebilir. Eęer blok zinciri kâhinleri yanlış bilgi sunarsa, tüm blok zinciri bozabilirler. Blok zincirine baęlı herhangi bir cihaz, kod dizesi veya insan etkileřimi deęerlendirilmesi ve yönetilmesi için yeni bir riski ortaya çıkarır (Prewett, Prescott ve Phillips, 2020). Blok zinciri kâhinleri ile ilgili risklerin belirlenmesi ve ölçülmesi, iç denetimin en zor risk deęerlendirme alanlarından birine dönüşebilir (Kloch ve Simon, 2019).

3.3.Baęımsız Denetim ve Blok Zinciri Teknolojisi

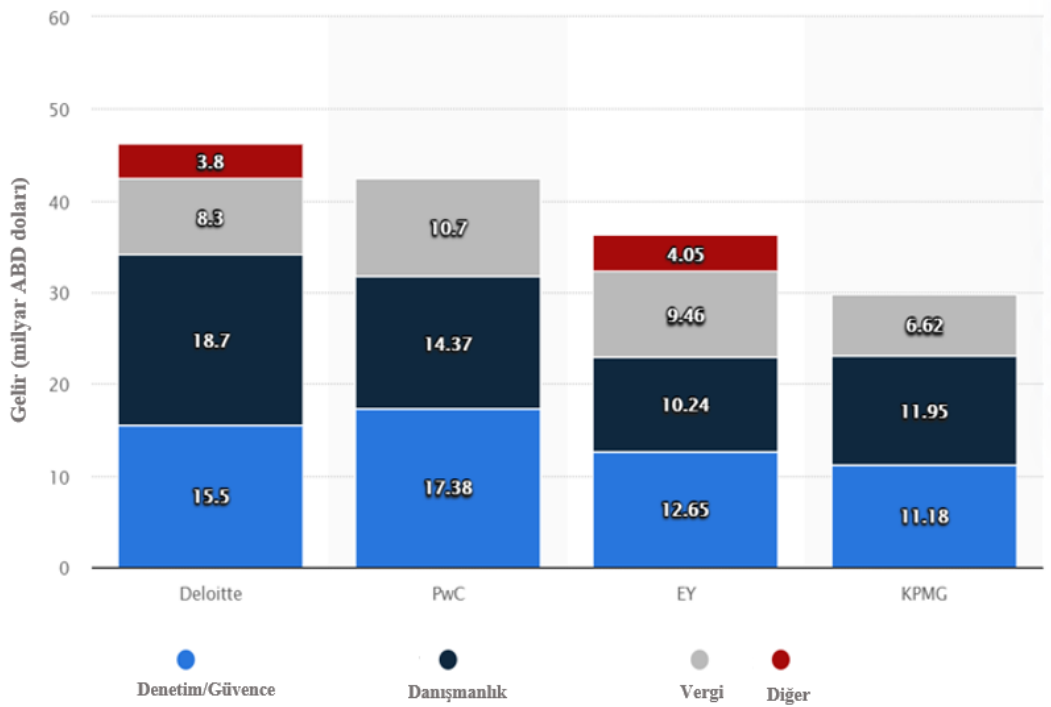
Son yıllarda günümüz denetim mesleęi meydana gelen teknolojik gelişmelerle yeni bir döneme girmiřtir. Geleneksel, insan iş gücüne dayanan denetim mesleęi, çok kısa bir zaman dilimi içerisinde organizasyonların bütünü hakkında makul bir güvence sunabilmesinde denetçilerin yükünü oldukça arttırmaktadır.

1970'lere kadar denetçiler sırasıyla hesap makinelerini, yazılımları ve veri tabanlarını elektronik verileri incelemek için kullanmışlar ve bu araçlar hesaplama yapmada ve işlemlerin takibinde denetçinin iş yükünü ciddi bir şekilde azaltmıştır. 1970'li yıllardan sonra baęımsız denetim mesleęinin etkinlięini ve verimlilięini ve baęımsız denetimin kalitesini arttırmak için yeni çıkan teknolojiler denetim mesleęinde kullanılmıştır (Dai, 2017). Son on yılda ise baęımsız denetim süreçlerini etkileyen ya da etkileyeceęi öngörülen teknolojiler yapay zekâ, dronelar, nesnelerin interneti, büyük veri analizleri, akıllı sözleşmeler ve blok zinciri teknolojisidir (ACCA, 2019).

Muhasebe ve denetim günümüzün en önemli ve büyük sektörlerinden biri olup, her geçen sene önemi ve büyüklüęü daha da artmaktadır. 2019 yılında dört büyük denetim firmaları olarak adlandırılan Deloitte, Ernst & Young (EY), KPMG ve PwC'nin toplam çalışan sayısı dünya genelinde 1 milyonu geçmiştir (Mazareanu, 2019). Dört büyük denetim firmaları sadece 2019 yılında 155 milyar dolar gelir elde etmiş ve bunların 57 milyar dolarını denetim ve güvence hizmetleri oluşturarak denetim řirketleri için en önemli hizmet kolu haline gelmiştir. 2018 yılında ise bu

firmaların elde ettikleri gelir yaklaşık olarak 135 milyar dolar olduğu göz önüne alınırsa %14.8 oranı ile ciddi bir büyüme kaydetmiştir. Tablo 3.3.1.'de ABD'de dört büyük denetim firmalarının 2019 yılında elde ettikleri gelirlerin faaliyet kolu bazında dağılımları gösterilmektedir. Bu dağılıma göre dört firmanın hepsi en fazla geliri bağımsız denetim/güvence hizmetlerinden ve danışmanlık faaliyetlerinden elde etmiştir.

Tablo 3.3.1. ABD'de Dört Büyük Denetim Firmalarının 2019 Yılında Elde Ettikleri Gelirlerin Faaliyet Kolu Bazında Dağılımları

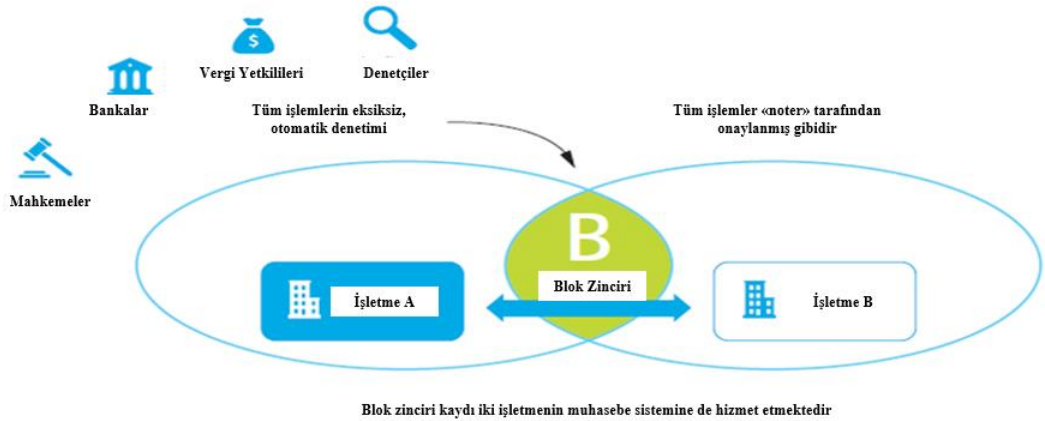


Kaynak: MAZAREANU, E.: 2019. Revenue of the Big Four accounting / audit firms worldwide in 2019, by function, Dec 12, 2019, (Çevrimiçi) <https://www.statista.com/statistics/250935/big-four-accounting-firms-breakdown-of-revenues/>, 17 Mayıs 2020.

Blok zinciri teknolojisi ve muhasebe mesleğini konu alan bazı makale ve gazete yazılarında blok zinciri teknolojisinin denetim mesleğini ortadan kaldıracağı düşünülmektedir (Casey ve Vigna, 2018). İşletmeler işlemleri kaydetme metodunu blok zinciri tabanlı bir yazılıma döndürdüklerinde, değiştirilemeyen denetim izleri oluşturulacaktır. Tüm işlemler ağ tarafından doğrulanacak ve değiştirilemeyecektir. Savunulan iddia ise, blok zincirine kaydedilen tüm işlemlerin tamamıyla takip edilebilen denetim izleri fikrine dayanması ile bağımsız denetimi tümü ile otomatikleştirecek yazılımların geliştirilebilecek olmasıdır. Deloitte Almanya'da

sorumlu ortak baş denetçi olan Nicolai Andersen, 2016 yılında yayınlanan raporda, bütün günlük defter kayıtlarının dağıtık bir ortamda ve kriptografik bir şekilde mühürlenmiş olması sebebi ile gerçekleşen bir olayı gizlemek için kayıtlar üzerinde oynamak ya da kayıtları yok etmenin neredeyse imkânsız olduğunu dile getirmiştir. Bu sebeple, şekil 3.3.1.'de görüldüğü gibi, blok zincirinde kaydedilen işlemleri noter tarafından onaylanmış işlemlere benzetmiştir. Kayıtlarda herhangi bir hile yapılması blok zinciri ağını bu hileli davranışın varlığından haberdar edecektir. Ancak her ne kadar blok zincirin değiştirilemez özelliği olsa da, teknolojinin sunmuş olduğu bazı çözümler risklere açıktır. Bu yüzden yeni bir denetim yaklaşımı gerekmektedir.

Şekil 3.3.1. Blok Zinciri Teknolojisinin Güvenilir Bir Taraf Olmadan Eksiksiz Ve Kesin Doğrulama Sağlaması



Kaynak: Andersen, N.:2016. Blockchain Technology: A game-changer in accounting. Deloitte, March.

Her ne kadar bazı çalışmalarda blok zinciri teknolojisinin denetim mesleğinin yerine geçeceği savunulsa da bu düşüncenin tersini savunan yazılar da mevcuttur. Uluslararası denetim firmalarından bir diğeri olan Mazars'ın Denetim Bölümü'nde sorumlu ortak baş denetçi olan Wiehann Olivier, bazı kişilerin blok zinciri teknolojisinin sahip olduğu şeffaflık ve kayıtların değiştirilememe özelliği sebebi ile denetçilere duyulan ihtiyacın ortadan kalkacağını düşündüklerini belirtmiş, ancak işin aslının bu teknolojinin denetçinin denetimini daha verimli bir hale getiren ve görüş bildirirken dayandıkları bilgilerin güvenilirliği artıran bir araç haline getirdiğini söylemiştir (Monzon, 2020).

Blok zinciri teknolojisinin denetim mesleğinin ve denetçinin yerini alacak olması fikri işlemlerin kendisinin güvenilir olması durumunda geçerlidir. Blok zincirin sunmuş olduğu güven, işlemlerin gerçekten gerçekleşip gerçekleşmediğine ya da gerçekten meydana gelmesi ile ilgilidir. İşlemin kendisinin yasa dışı, hileli veya yetkilendirilmemiş olup olmadığı ile ilgili bir bilgi bulunmamaktadır. Yani, her ne kadar işlemin meydana gelmesi blok zincirinde yapılan kayıt ile doğrulansa da, işlemlerin hile ya da bir sınıflandırma hatası içerip içermediğine dair denetçilerin incelemelerine ihtiyaç vardır (Bible ve ark., 2017). Blok zincirine kodlanmış yalanlar hala yalan olacağı için hile blok zinciri teknolojisi ile birlikte de mevcudiyetini koruyacaktır. Bu yalanlar artık değiştirilemez olarak şekil değiştirecektir (Bradbury, 2015). Ayrıca blok zinciri teknolojisi defter kayıtlarının doğru yapılıp yapılmadığına dair gereken muhasebe bilgisinin yerini dolduramayacaktır. Blok zinciri teknolojisi geçerli olan işlemlerin tahmininde ve ölçümündeki hataları ve varlıkların kötüye kullanımını önleyemeyecektir (Coyne ve McMickle, 2017). Hesaplar hakkındaki değerlemelerinin, sınıflandırmalarının ve varlıkların ve borçların tahmininin değerlendirilmesinde denetçilere ihtiyaç duyulacaktır.

Günümüz denetim mesleğinde, kaydedilen tüm işlemlerin denetimi mümkün olmadığı için denetçiler belirlemiş oldukları risk seviyelerine göre bir örneklem seçmektedirler. Bu örneklem ise tamamen denetçinin kendi yargısına bağlıdır. Ancak blok zinciri teknolojisi ile işlemlerin doğruluğu blok zincirinde sağlanan mutabakat sayesinde onaylanmış olacağı için ve blok zincirin değiştirilemez özelliği sayesinde, denetimde makul güvence verebilmek için örneklem seçimine gerek kalmayacağı öngörülmektedir. Ayrıca blok zincirinde işlemler ağdakilerin mutabakatı halinde deftere kaydedileceği için, denetimde mutabakat en az zaman harcanacağı ve otomasyonun en üst düzeyde olduğu bir noktada olacaktır.

Muhasebe kayıtları bağımsız denetçiler tarafından muhasebe standartlarına uygunluğu ve kayıtların doğruluğu hakkında yatırımcılara makul bir güvence vermek üzere denetlenirler. Bu denetim ve incelemeler çoğu zaman uzun sürmekte ve belge incelemesine dayanmaktadır. Blok zinciri teknolojisinin insan emeğine dayanan iş gücünü ve çeşitli belge incelemesini azaltabileceği öngörülmüştür. Danimarka meşeli nakliye firması olan A.P. Moller-Maersk, malları alıcıya göndermek için yasal süreçte

gereken kağıt işlerinin ve dokümantasyonun sadece malın fiziki olarak gönderilmesi için gerekenden beş katı daha fazla olduğunu belirtmiştir (Moise ve Chopping, 2018).

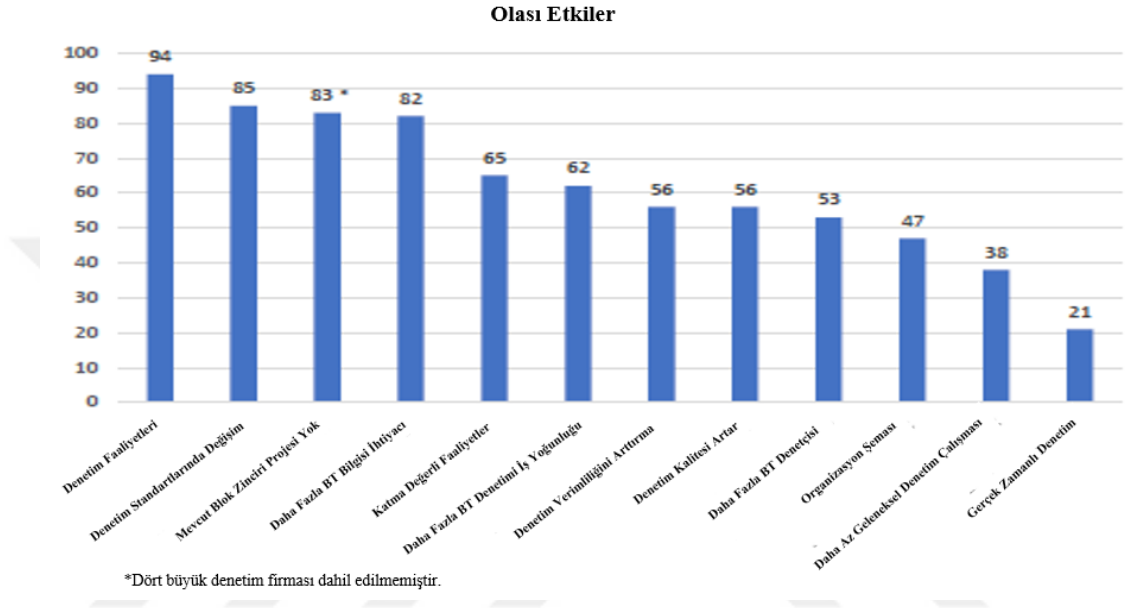
Teknoloji ve otomasyon denetim süreçlerini hızlandırmaktadır. Her ne kadar denetçinin rolü denetimin odağı kayıtların izlenmesi ve doğrulanmasından sistemik değerlendirme, risk değerlendirme, önleyici denetimler ve yolsuzlukların tespiti gibi daha karmaşık analizlere doğru kayacaktır. Bu nedenle denetçilerin temel odak noktaları, zaten teknoloji tarafından yerine getirilmekte olan işlemlerin mevcudiyetini, doğruluğunu ve eksiksiz olmasını ve kanıtların bulunmasını garanti etmek olmayacaktır. Denetçilerin yargılarına, gözetimine ve içgörülerine her zamandakinden daha çok ihtiyaç duyulacaktır (Dai, 2017:76).

Günümüz denetim metodolojisi, önemli yanlışlık riskine ilişkin denetim kanıtı toplayabilmek için örneklem seçimi, geriye doğru denetim yaklaşımı ve bir yıllık, çok kısa bir süre içinde, bir denetim görüşü vermektedir. Binlerce işlemi kaydeden veri tabanları siber güvenlik saldırılarına maruz kalabilirken, geleneksel denetim modellerinin zamanla otomatik hale gelmesi ve öngörmeye dayalı bir yapıya dönüşmesi ise oldukça gereklidir. Bu sebeple, bağımsız denetçiler için akıllı sözleşmeler ve blok zinciri teknolojisi gibi gelişmekte olan teknolojileri ve karmaşık denetim analizlerinin etkisini dikkate almak mesleklerini kaybetmemek, kamuya bir yarar sağlamaya devam edebilmeleri ve kaliteli denetim hizmeti sunabilmeleri açısından önem arz etmektedir (Rozario ve Vasarhelyi, 2018).

Tablo 3.3.2.'de İsviçre'de 23 denetim firması ve 34 denetçi arasında yapılan bir araştırmanın sonuçları gösterilmektedir. Mülakat yöntemi ile bir takım sorular sorularak yapılan araştırmanın amacı İsviçre'de farklı büyüklükteki denetim firmalarında çalışan mali denetçilerin ve bilgi teknolojileri (BT) denetçilerinin, blok zinciri teknolojisi kullanımının denetim mesleğindeki uygulamaları nasıl etkileyebileceği konusundaki algısını araştırmaktır. Buna göre araştırmaya katılanların %62'si denetim mesleğinin daha BT odaklı olacağını düşünmekte, mali denetiminin amacının finansal tabloların doğruluğu ve mevzuatlara uygunluğu açısından güvence vermek olmayacağı, bunun yerine bilgi sistemlerinin incelenmesi ve blok zincirinin doğru bir şekilde kurulması ve uygulanması olduğunu beklemektedir. Bu nedenle,

denetçilerin rolü, bugün olduğu gibi işletmelerin finansal tablolarının doğruluğunu onaylayan finansal tablo denetçileri olmak yerine, blok zincirini onaylayan “BT mühendisi denetçileri” olacaktır (Brender ve ark., 2018).

Tablo 3.3.2. Blok Zinciri Teknolojisinin Denetim Mesleğine Olası Etkileri



Kaynak: BRENDER, N., GAUTHIER, M., MORIN, J. H., & SALIH, A.:2018. The Potential Impact of Blockchain Technology on Audit Practice.

Ayrıca ileride denetim firmalarının yapısının da değişmesi beklenmektedir. Araştırmaya katılanların %53’ü denetim firmalarının ileride daha fazla BT denetçisi alacağını beklediklerini söylemiştir. Denetim ekipleri BT denetçileri ve diğer uzmanlarla yakın ilişkiler içinde çalışabilecek, muhasebe ve finansal bilgisinin yanında bilgisayar becerilerinin de olduğu denetçiler tarafından yönetilecektir. Denetim firmaları, daha fazla BT denetçisi ve daha fazla beceriye sahip kişileri işe alırsa, denetim ekiplerinin bileşimi değişecektir (Brender ve ark., 2018).

Blok zinciri teknolojisi ile denetim faaliyetlerindeki hızı arttırmak işlemlerin meydana geldiği ve onaylandıkları tarihi arasındaki süreyi azaltacaktır. Yönetimin ve denetçilerin daha riskli ve karmaşık yapıda olan işlemlere yoğunlaşıp, rutin olarak yapılan denetim işlemlerinin gerçek zamanlı yapılmasını sağlayarak daha doğru ve etkin finansal raporlama ve denetim hizmeti sunulmasına olanak sağlayacaktır.

Günümüzde yeni mezun üniversite öğrencileri farklı iş sektörlerini tanımak veya işletme büyüklüğü açısından çok çeşitli müşterilerle çalışıp tecrübe edinebilmek için bağımsız denetçi olarak kariyerlerine başlamakta ve daha deneyimli olan denetçilerin koçluğu altında bir nevi okul sonrası eğitimlerine devam etmektedirler. Birkaç yıl bağımsız denetim mesleğinde tecrübe kazandıktan sonra ise denetim sektöründen ayrılıp, yeni sektörlerde çalışmaya başlamaktadırlar. Belirli teknik beceriler gerektirmeyen ve günümüzde daha az tecrübeli olan bu genç denetçiler tarafından yapılan bazı testler ve görevler, uzmanlık ve deneyim gerektiren analizlerin karşısında kaybolacaktır. Bu nedenle, denetim firmalarının yeni mezunlar yerine daha deneyimli profesyonellere ihtiyacı olacaktır. Stajyer, asistan, kıdemli asistan, senior, müdür, direktör, sorumlu ortak baş denetçi şeklindeki hiyerarşik yapıda, yukarıya çıktıkça daha az sayıda çalışanın bulunduğu piramitsel organizasyon yapısı güçlü bir şekilde bu durumdan etkilenecektir. Bununla birlikte, muhasebe şirketleri daha genç kişileri işe almak yerine, bu piramitsel yapının küçüleceği, hatta tersine döneceği düşünülmektedir. Gelecekte, yeni mezunlar uzmanlıklarını geliştirmek için önce sektörde çalışacak ve daha sonra bir denetim firmasına katılacaklardır (Brender ve ark., 2018).

Blok zinciri teknolojisi ile karşılaşılabilecek yeni riskler beraberinde denetçiler için fırsatlar da sunmaktadır. Örneğin, *akıllı sözleşmeler ve blok zinciri kâhinleri denetçisi*, konsorsiyum blok zincirlerinde sistemin sağlamlığı hakkında bağımsız bir güvence verebilmek için *konsorsiyum blok zincirleri denetçisi*, katılmak için izin gerektiren blok zincirlerine erişim izninin verilmesi için *erişim izni veren yönetici* ve blok zincirinde katılımcılar arasında anlaşmazlık olması durumunda anlaşmazlıkların çözümünde *arabulucu* olması gibi denetçilerin yeni rollere sahip olacağı düşünülmektedir (Bible ve ark., 2017).

Bir diğer yaklaşım ise özellikle büyük işletmeler tarafından blok zinciri teknolojisine geçiş sürecinin hemen olmayacağıdır. İşletmeler için alışık oldukları, mevcut sistemlerinden blok zinciri sistemine geçiş yapmak çok maliyetli bir iş olarak görülmektedir. Katlanılacak olan bu maliyetin telafisi denetçilere ödenecek ücretlerde azalma ile giderilebilecektir.

Ayrıca blok zinciri tabanlı sürekli denetim, denetçilerin müşterinin iş yapışını ve çevresini anlamasını geliştirecektir. Bunun sebebi ise denetçiler ile işletmeler arasındaki ilişkilerin artık dönem sonu raporlama dönemi ile sınırlı olmayacak olmasıdır. Bu durum da denetçinin trendleri ve gelecek riskleri tespit etme yeteneğini kolaylaştıracaktır (Vaidyanathan, 2017).

Bununla birlikte teknolojik karmaşıklık, önemli miktarda finansal yatırım ve zaman gereksinimi, teknolojinin diğer paydaşlara yaygınlaştırılmasındaki güçlükler ve süreçlerde değişiklik gerekliliği gibi unsurlar bu yeni teknolojilerin benimsenmesini engelleyebilmektedir (Dai, 2017). Blok zinciri teknolojisi bağımsız denetimi ve bağımsız denetim firmalarının iş yapışını değiştirmesi bekleniyorsa bu teknolojinin müşteri işletmenin kullandığı blok zinciri alt yapısı ile de doğrudan ilgili olmak durumundadır. Denetim mesleği her ne kadar kamuya bir güvence sunma hizmeti olsa da gerçekleşen denetim, müşteri işletmenin kullandığı sistem çevresinde gerçekleşmektedir. Denetim firmalarının denetimini yaptıkları müşteri işletmelerin blok zinciri teknolojisini kullanıp kullanmadıkları ya da yakın gelecekte kullanmaya niyeti olup olmadığı, denetim firmalarının da bu teknolojiye olan tutumunu şekillendirecektir. Ancak izin gerektiren ve izin gerektirmeyen blok zincirleri kullanan şirketlerin sayısı arttıkça, burada yer alan bilgiler finansal tablolar için yeni bir bilgi kaynağı olacağı için denetçilerin denetimlerinde bu durumun etkisinin de farkında olmalıdırlar.

Denetçilere izin gerektiren blok zinciri ağına erişim hakkı verildiğinde işlemler meydana geldiği anda onları inceleyebileceklerdir. Bu durum ise, yılsonu geldiğinde daha karmaşık ve zor yapıda olan işlemleri incelemek için denetçilere ekstra zaman yaratacaktır. Bu karmaşık işlemler değerlendirme ve sınıflandırma ya da daha önce hiç karşılaşmadıkları bir olay da olabilir.

3.3.1.Blok Zinciri Teknolojisinin Denetim Kanıtları Üzerine Etkisi

Bir işlemin gerçekleştiğini doğrulamak, finansal tablo denetimindeki önemli hususlardan sadece biridir. Finansal tablo denetimi, kaydedilen işlemlerin ilgili, güvenilir, objektif, doğru ve doğrulanabilir kanıtlarla desteklendiğini değerlendirmeyi

de içermektedir (Bible ve ark., 2017). Blok zinciri teknolojisi ile verinin (kanıtların) güvenilirliği, güvenliği ve işlemlerin şeffaflığı denetimi etkileyecek önemli noktaların başında gelmektedir (Appelbaum ve Nehmer, 2017).

Denetçiler finansal tablolar hakkında bir görüş bildirebilmek için yeterli ve uygun denetim kanıtı toplamakla yükümlüdürler. Denetim kanıtının uygunluğu kanıtın kalitesinin bir ölçüsüdür. Uygun denetim kanıtı ihtiyaca uygun ve güvenilir olmalıdır. Kanıtın yeterliliği ise toplanacak kanıtın miktarının ölçüsüdür. Toplanacak kanıt miktarı, kanıtın kalitesine göre değişiklik gösterebilmekte ve önemli yanlış risklerini değerlendirirken etkilenmektedir.

Denetçiler, müşteri işletmenin blok zincirinde işlenen işlemlerin tamamını test edebilecekleri için, yeterli kanıt toplanmasının bir blok zinciri ortamında zor olması beklenmemektedir. Buna bağlı olarak denetçiler, denetim kanıtlarının ilgili ve güvenilirlik gerekliliklerine odaklanacaklardır (Rozario ve Thomas, 2019).

Kanıtların güvenilirliği kanıtın kaynağı ile niteliğinden etkilenir ve kanıtın elde edildiği şartlara bağlıdır (BDS 500, 2019). Denetim kanıtı bir denetçinin görüşüne dayanak olacak her türlü bilgiyi içermektedir. Kanıtların kaynağı işletme içi veya işletme dışı olabilir. İşletme dışı elde edilen kanıtların işletme içi elde edilen kanıtlardan daha güvenilir olduğu varsayılmaktadır. Bunun nedeni ise kaynağı işletme dışı olan bu verilerin direkt olarak denetim ekibi tarafından elde edilmesi, işletme içinden herhangi birinin müdahalesinin olmamasıdır.

Blok zincirinin özelliklerinden olan merkezi olmama, değiştirilememe ve izlenebilirlik sayesinde satış emirleri ve faturalar gibi finansal bilgiler güvenli ve şeffaf bir şekilde blok zinciri defterine kaydedilerek işletme içi ve işletme dışı bilgilerin güvenilirliğini artırabilir (Rozario ve Thomas, 2019). Blok zincirinde yer alan bir bilgi ağdaki katılımcılarla birlikte üretildiği için blok zincirindeki verilerin kaynağının işletme dışı olduğu kabul edilmektedir (Appelbaum ve Nehmer, 2017). Ancak denetçi yine de blok zincirindeki bir bilgiyi incelerken bilginin güvenilir olup olmadığını göz önünde bulundurmalıdır. Aynı zamanda, blok zincirinden elde edeceği bilgilerin güvenilirliğini incelerken de mutabakat mekanizmasının güvenilirliğini de değerlendirmelidir. Daha önce Tezin 3.2.1.Standard Risk Faktörleri bölümündeki

Bilgi Güvenliđi Riskinde bahsedildiđi gibi, bilginin güvenilirliđinin deđerlendirmesi mutabakat mekanizmasının manipüle edilip edilmediđinin deđerlendirilmesini de içermelidir.

Veri güvenliđi, verinin manipölasyondan ya da hileli bir şekilde deđiştirilmesinden korunduđuna güvence verilmesidir. Veri güvenliđi yetkilendirilmemiş kiřilerin bilgisayar, veri tabanları ve internet sayfalarına eriřimin önlemesini sađlayan kontrolleri ifade etmektedir. Veri güvenliđi verinin güvenilirliđinin diđer bir tarafıdır. Yani verinin güvenliđinin sađlanması verinin ilk halinin deđiřmeden güvenilirliđini sürdürdüđu anlamına gelmektedir. Bađımsız denetimde, kanıtların elde edilme süreci řeffaf, gözlemlenebilir ve dođrulanabilir olmalıdır. Bu dođrultuda kanıtlardan elde edilen verilerin řeffaflıđı raporlanan bilgilerin dođruluđu ve esas kaynaklardan meydana geldiđi hakkında güvence verecektir.

Blok zinciri teknolojisinin bađımsız denetimi etkileyeceđi konulardan biri de denetim prosedürleri ya da kanıt toplama teknikleridir. Denetçiler blok zincirinden dođrudan denetim kanıtı elde edebilmeleri için yeni denetim prosedürleri geliřtirebilirler (Appelbaum ve Nehmer, 2017) .

500 numaralı bađımsız denetim standardında belirtilen denetim prosedürlerinin, geriye dönük (ilk olarak finansal tablolar, sonra defter kayıtları ve en son belgeler) bir yapısı vardır. Kurumun finansal verilerinin ufak bir kısmı örneklem olarak alınarak dođrulama sađlanır. Daha sonra örneklem alınmış bu veri seti için bir anlam çıkartılır. Denetim prosedürleri denetim faaliyetinin gerçekteřtiđi an uygulanırsa da örnekleme ele alınan işlemler bir yıl öncesine aittir.

Blok zinciri teknolojisi sürekli denetimleri mümkün kılarak, yoğun iş gücü gerektiren ve zaman harcayan denetim faaliyetlerini azaltacaktır. Bu durumda denetçilerin strateji danışmanlıđı, derinlemesine analizler ve veri madenciliđi gibi faaliyetlere odaklanmalarına imkân tanıyacaktır (Schmitz ve Leoni, 2019). Sürekli kanıt toplama (continuous evidence gathering) ise, olayın meydana geliři ile denetim prosedürlerinin uygulanması arasındaki süreyi azalttıđı için denetimin kalitesini arttırmaktadır (Appelbaum ve Nehmer, 2017). Sürekli kanıt toplama ile trend

analizleri, zaman serisi analizleri ve karşılaştırılmalı değerlendirmelerin yapılabileceği öngörülmektedir. Böyle bir durumda ise Tablo 3.3.1.1.'de görüldüğü gibi blok zinciri ile denetim kanıtının sürekli toplandığı bir çevredeki denetim prosedürleri, günümüzde kullanılan denetim prosedürlerine göre daha teknik olmaktadır.

Tablo 3.3.1.1. Geleneksel Prosedürler İle Blok Zinciri Destekli Prosedürlerin Karşılaştırılması

Denetim Prosedürleri	Geleneksel Kanıt Toplama Yöntemi	Blok Zinciri Destekli Sürekli Kanıt Toplama Yöntemi
Kayıt ve Belgelerin Tetkiki	Kayıtlardan örneklem seçilir ve kayıtlar kaynağına doğru takip edilir, doğrulanır ve eşleştirilir	Blok zinciri teknolojisini kullanarak işletmenin muhasebe sisteminde kaydedilen tüm verileri değerlendirme
Maddi Varlıkların Tetkiki	Fiziki stoklar, inceleme	RFID ile etiketleme
Gözlem	İşletme personeli tarafından uygulanan prosedürleri izlemek ve gözlemlemek	Blok zinciri madenciliğini kullanarak iş akışlarını doğrulama
Dış Teyit	Hesap bakiyelerini doğrulamak	Blok zinciri uygulamalarını kullanarak veri akışlarını birbirine bağlama
Yeniden Hesaplama	Kayıtların matematiksel doğruluğu için bağımsız denetçi tarafından yeniden hesaplanması	Tüm verilerin izlenmesi ve belirli aralıklarda otomatik olarak hesaplamaların yapılması

Yeniden Uygulama	İşletme tarafından uygulanan prosedürleri doğrulamak için aynı prosedürlerin bağımsız olarak yeniden yürütülmesi	Tüm işlemlerin otomatik olarak tekrarlanması ve kural dışı olanların tespit edilmesi
Analitik Prosedürler	Finansal ve finansal olmayan veriler arasındaki ilişkilerin analiz edilmesi, istatistiksel analizler	Süreklilik denklemleri ve istatistiklerle gerçek zamanlı verileri filtreleme
Sorgulama	İşletme çalışanlarından yazılı ve sözlü olarak bilgi alınması	Süreçleri ve kontrolleri izleme, inceleyebilmek için süreçleri ihlal edenleri tespit etme

Kaynak: APPELBAUM, D., NEHMER, R.:2017, Designing and Auditing Accounting Systems Based on Blockchain and Distributed Ledger Principles. **Feliciano School Of Business.**

Blok Zinciri Teknolojisinin Gözlem/Sorgulama Üzerindeki Etkisi

Gözlem, başkaları tarafından gerçekleştirilen bir işlemin veya prosedürün izlenmesini ifade etmektedir. İşletme çalışanı tarafından gerçekleşen stok sayımının veya kontrol faaliyetlerinin izlenmesi gözleme örnek olarak gösterilebilmektedir (BDS 500, 2019:10). Denetçiye denetim sürecine doğrudan bağlayacak herhangi bir süreç daha güvenilirdir. Her ne kadar denetçi tarafından doğrudan elde edilen denetim kanıtlarının daha güvenilir olduğu kabul edilse de, gözlem yoluyla elde edilen kanıtlar sadece gözlemin yapıldığı zamanla sınırlıdır. Gözlemlendiğini bilmek süreçlerin ve prosedürlerin uygulanma şeklini etkileyebilir (BDS 500, 2019:11).

Sürekli gerçek zamanlı bir denetim ortamı, blok zincirinin kendisi çok fazla gözlem kanıtı sağlayacağı için denetçilerin gözlem yapma görevini oldukça azaltacaktır. Blok zincirinde işlemlerin ne zaman gerçekleştiğini belirtmek için zaman damgası bulunmakta ve tüm işlemlerin zincirine eklenmeden önce özetleme değerleri alınmaktadır. Zaman damgası ve özetleme değeri oluşturulmuş işlemler mevcut olan zincire eklenebilmektedirler. Bu durumda denetçiler, bloğa eklenen işlemlerin zaman damgasının oluşmasını ve bloğun özetleme değerinin oluşup oluşmadığını gözlemleyebilirler (Appelbaum ve Nehmer, 2017). Ayrıca, gözlem kanıt toplama

tekniki meydana gelme, var olma ve deęerleme ynetim iddiaları iin kanıt toplanmasına yardım edebilmektedir.

Ayrıca ağıın hesaplama gcnn oęunluęu iyi niyetli kiřiler tarafından ynetildięi srece, blok zinciri istenen řekilde alıřmaktadır. Bu durumda ağıın hesaplama gcnn oęunluęu dięer herhangi bir gruptan daha hızlı srede zetleme deęeri retmelidir. Bu sebeple, zetleme fonksiyonlarının alıřıp alıřmadıęını doęrulayabilmek iin zincirin uzunluęunun zaman iinde artıp artmadıęını da gzlemleyebilirler (Appelbaum ve Nehmer, 2017).

Deneti, sorgulama teknięi ile ağıdaki katılımcıların blok zinciri ve ağıın ynetiřim zelliklerinden neyi anlayıp anlamadıęı konusunda bilgi edinebilir. Bu da blok zinciri ile elde edilen bilginin gvenlięi ve gvenilirlięi hakkında kanıt elde edilmesini saęlayacaktır. Bu durum aynı zamanda, blok zincirindeki katılımcıların zinciri bozmak niyetiyle birlikte hareket etmediklerini, belli bir grup katılımcının ağıdaki iřlem gcnn yzde 51 ve fazlasına sahip olmadıęı konusunda kanıt sunacaktır (Appelbaum ve Nehmer, 2017).

Blok Zinciri Teknolojisinin Dıř Teyit zerindeki Etkisi

Alacak hesapları iin dıř teyitler her zaman uygulanan bir kanıt toplama teknięi olmuřtur. Dıř teyitler, genellikle var olma ve haklar ve ykmllkler iddialarına kanıt saęlamaktadır. Yani alacaklar hesabının bakiyesinin gerekten mevcut olup olmadıęı ve alacaklardaki haklar ve ykmlklere iliřkin kořullar nelerdir bunun iin kanıt toplanmaktadır. Dıř teyit mektupları iřletme tarafından nc tarafa gnderilse bile, cevaplar direkt olarak denetiye gnderilmelidir. Ayrıca dıř teyit mektuplarının olmaması durumunda ise denetiler bakiyeleri doęrulamak iin tahsilat fiřlerini, satıř emirlerini, satıř faturalarını, irsaliye faturalarını ve dięer ilgili belgeleri de inceleyebilirler.

Blok zinciri teknolojisinin kullanıldıęı bir ortamda, yukarıda belirtilen belgelerin kaynaęı blok zinciri ile kayıt altına alınmıř olacaęı iin, denetim szleřmesindeki dıř teyit srelerinin deneti zerindeki yk byk lde azalacaktır. Bu durumda, blok zincirinin alıřma bileřenlerinden olan iř ispatı (proof of work) iin gereken zet fonksiyonunun tasarımı ve iřleyiři konusunda ağı yeleri ile

de dış teyit yolu ile kanıt toplanması gerekecektir. Ayrıca, denetçiler dış teyit yöntemi ile iş ispatının hesaplanmasında ağdakilerin bu hesaplama katıldığını doğrulamak için de kullanabilirler (Appelbaum ve Nehmer, 2017).

Blok Zinciri Teknolojisinin Kayıt ve Belgelerin Tetkiki Üzerindeki Etkisi

Kayıtların ve belgelerin incelenmesi temel denetim prosedürlerinden biridir. İncelenen belgeler müşteri firma tarafından oluşturulmuş da olabilir veya işletme dışından da gelebilir. Belgelerin tetkiki ileriye veya geriye doğru yapılabilir. İleriye doğru yapılan belge incelemesi, belgelerden defter kayıtlarına sonrada finansal tablolara doğru yapılan incelemeyi ifade ederken, geriye doğru yapılan denetimde inceleme finansal tablolardan başlayarak, defter kayıtlarına oradan da kayıtların dayanağı olan belgelere doğru ilerler.

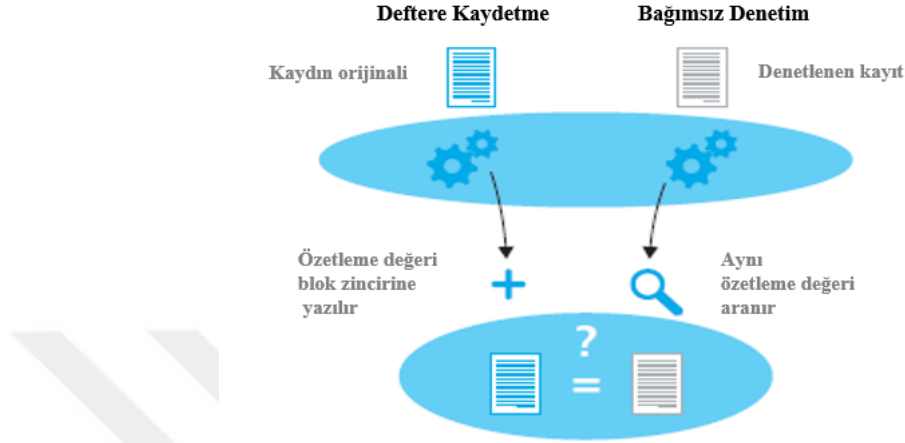
Bir blok zinciri uygulamasında ise denetçi, blok zincirindeki işlemleri yürüten ağın yapılandırmasını ve yönetişimini destekleyen belgeleri inceleyebilir. Bu durum, meydana gelen işlemlerin doğrulanmasında güvenilir bir üçüncü tarafa ihtiyaç olmadığını, blok zincirindeki eşler arası ağın yeterli olduğuna dair kanıt sağlayacaktır (Appelbaum ve Nehmer, 2017).

Blok Zinciri Teknolojisinin Yeniden Hesaplama Üzerindeki Etkisi

Yeniden hesaplama, kayıtların doğruluğunun denetçi tarafından kontrol edilmesini ifade etmektedir. Bir blok zincirindeki özetleme değeri, olması gerektiği doğrulanabilirlikte tasarlanırsa, ağdaki katılımcılar ve denetçi, blok zincirinde kaydedilen işleme ait özet değerini yeniden hesaplamadığı sürece değiştiremeyecektir. Böylelikle denetçi blok zincirin bu özelliği sayesinde özet değerini yeniden hesaplanmasını doğrulamış olacaktır. Denetçiye blokta yer alan işlemlerin akışının hatasız bir şekilde gerçekleştiğine dair kanıt sağlayacaktır. Bu durum aynı zamanda doğruluk iddiasını destekleyecektir.

Blok zinciri teknolojisinde verilerin değiştirilmeden bütünlüğünün korunup korunmadığı özetleme fonksiyonları kullanılarak sağlanmaktadır. Şekil 3.3.1.1.'de bağımsız denetimde blok zincirine kaydedilen bir belgenin bozulmadan bütünlüğünün korunması açıklanmaktadır.

Şekil 3.3.1.1. Blok Zinciri Kullanarak Kayıtların Bütünlüğünü Doğrulamak İçin Bir Yaklaşım



Kaynak: ANDERSEN, N.:2016, Blockchain Technology: A Game-Changer In Accounting. Deloitte, March.

Buna göre, orijinal kaydın özetleme değeri alınır ve kayıt blok zincirinde bu özetleme değeri ile saklanır. Sonraki herhangi bir anda, denetçi tarafından yine özetleme değeri oluşturularak ve blok zincirinde depolanan özetleme değeri ile karşılaştırılarak dosyanın bütünlüğünün korunduğu kanıtlanabilir. Özetleme değerlerinin aynı olması durumunda, özetleme değerinin blok zincirine ilk olarak yazıldığından beri belgenin değişmeden kaldığı ispatlanacaktır.

Finansal ve finansal olmayan bilgilerin denetim kanıtı olarak kullanılması denetim prosedürlerinin doğruluğunu artırmaktadır. Ancak denetçiler çeşitli kaynaklardan gelen bilgilerin birleştirilmesini zor bulabilmekte, farklı kaynaklardan gelen denetim kanıtı hazırlanmasının maliyetinin ise beklenen faydayı aşma olasılığı da bulunmaktadır. Blok zinciri ise çeşitli kaynaklardan denetim kanıtı saklanabilmesini mümkün kılmakta ve böylelikle dışarıdan ve işletme içi elde edilen finansal ve finansal olmayan bilgilerin toplanmasındaki zorlukların üstesinden gelmeye yardımcı olmaktadır (Rozario ve Thomas, 2019).

3.3.2.Blok Zinciri Teknolojisinin Yönetimin İddiaları Üzerindeki Etkisi

Bir denetçinin ana görevlerinden bir tanesi de yönetimin iddialarının doğruluğunu test etmektir. Denetçi, blok zincirinin güvenliğine ve blok zincirindeki verilerin güvenilirliğine kanaat getirdikten sonra yönetimin iddialarının doğruluğunu değerlendirebilecektir (Schulman ve Wilson, 2019). Blok zinciri teknolojisinin sahip olduğu özellikler sayesinde yönetimin iddialarının doğruluğunun test edilmesi kolaylaşabilmektedir. Blok zinciri teknolojisinin yönetimin iddialarından meydana gelme, eksiz olma ve doğruluk iddiasının değerlendirilmesine daha fazla etkisi olacağı düşünülmektedir (Psaila, 2017).

Meydana gelme (var olma): Meydana gelme ve var olma birbirinin yerine kullanılabilir, varlıkların bilanço tarihinde gerçekten var olup olmadığı ve bir işlemin veya fiziksel kontrollerin gerçekten meydana gelip gelmediği sorularına cevap vermektedir. Ortak defterde açık ve özel şifreleme anahtarlarının kullanılması, hem bir işlemin kaynağını (kim tarafından geldiğini) hem de işlemin varacağı yeri doğrulamaktadır. Ayrıca, yeni işlemler yalnızca kullanıcıların büyük çoğunluğu tarafından doğrulanırsa zincire eklenebilmektedir, bu da kötü niyetli kişileri etkisiz hale getirmektedir (Vaidyanathan, 2017). Ağdaki kişilerin tanıklığında işlem ispatının tamamlanmış olması gerektiği için meydana gelme iddiası için kanıt sağlanacaktır (Appelbaum ve Nehmer, 2017). Eğer ağdaki kişiler tarafından işlem onaylanmamışsa, işlemin gerçekleştiği söylenemeyecektir ancak ağdakiler tarafından doğrulamalar gerçekleşirse, denetçi işlemin gerçekleştiğinden emin olabilecektir (Kuhn, 2018).

Eksiksiz olma (tam olma): Yönetimin iddialarından biri olan eksiksiz olma iddiasına göre, bir dönem içerisinde meydana gelen tüm işlemlerin ve olayların eksiksiz bir şekilde kayıtlara alınmış ve kayıt dışı bırakılan hiçbir işlemin olmaması gerekmektedir. Blok zinciri gibi dağıtık defterler mutabakat gerektiren kayıtların birden fazla, birbirinden ayrı tutulan işletme içi ve dışındaki veri tabanlarını ortadan kaldırmakta ve zamanlama uyumsuzlukları veya kaydetme hataları yoluyla yanlışlıkla yapılan eksik işlem riskini azaltmaktadır (Vaidyanathan, 2017). İşlemlerin sırası

konusunda ağdakilerin birbirleri ile mutabık kalmaları gerektiği için işlemlerin eksiksiz olduğu konusunda kanıt sağlanacaktır.

Sınıflandırma ve anlaşılabilirlik: Bir dijital varlığın blok zinciri ile sınıflandırılması zordur. Bu konuyu anlatan muhasebe kaynakları ve emsalleri yeni yeni gelişmektedir. Bu tür varlıkların sınıflandırılmasını belirlemek için şirketlerin varlığın amacını ve kullanımı tarafsız olarak değerlendirmesi gerekecektir (Burns ve Steele, 2020). Anlaşılabilirlik açısından - işlem bilgilerinin veya hesap bakiyelerinin toplanması (daha büyük resmi kaçırmamak için) veya ayrıştırılması yararlı olabilir. Kodda bu esnekliğe izin veren bir yol belirtmek zordur.

Doğruluk: Yönetimin doğruluk iddiası, meydana gelen işlemlerin doğru tutarlarla ve doğru şekilde kaydedildiğini ifade etmektedir. Blok zinciri kullanımının faydalarından biri birden fazla tarafın işlemleri görmesi ve doğrulamasıdır. İşlemlerin şeffaf bir şekilde ve araçlar dahil edilmeden deftere kaydedilmesi, işlemlerin doğruluğunun korunmasına yardımcı olabilecektir. Ancak şeffaflık, doğru olmayan bir durum olduğunda da bu durumun herkes tarafından görülmesini sağlamalıdır (Vaidyanathan, 2017). Blok zinciri mimarisi işlemlerin silinmesine izin vermediği için, geçmiş kayıtları kaldırmak veya değiştirmek yerine, kaydın ilk hali değiştirilmeden aynı kalacak, doğru muhasebe kaydı ise iki işlem arasındaki doğru miktarı yansıtacak şekilde ilk kaydı telafi edecek ve denetim izi korunmaya devam edilebilecektir (Kuhn 2018; Vaidyanathan, 2017).

Değerleme: Varlık değerlemeleri işletme ve çalışma koşulları, gelecekteki beklentiler ve teknoloji gibi çeşitli faktörlere bağlı olabilmektedir. Değerleme kesin bir yargı içermediği için, dağıtık defterler bu tür analizlerde denetçiye yardımcı olmak için tasarlanmamıştır. Bu yüzden blok zinciri teknolojisinin değerlendirilmesinde doğrudan bir faydası olacağı düşünülmemektedir (Vaidyanathan, 2017). Ek olarak, dijital varlıkların değerinin belirlenmesi, bu varlıkların değerini desteklemek için gözlemlenebilir piyasa verilerinin çok az olması veya hiç olmaması veya piyasa verilerinde büyük değişim olması durumunda zor olabilir (Burns ve Steele, 2020).

Dönemsellik: Dönemsellik iddiası, işlemlerin ve olayların tahakkuk ettikleri tarihte ve dönemde kayda alındığını ifade etmektedir. Blok zincirindeki tüm işlemler zaman damgasına sahip olacağı için kalıcı bir şekilde deftere kaydedilecektir. Blok zincirinde, işlemin kaydı ile işlemin kendisi aynı anda gerçekleşmektedir bu yüzden işlem ve işlemin kaydı birbirine çok sıkı bir şekilde bağlıdır. Bu sebeple, bir hesap dönemine ait olmayan bir işlemin o döneme ait kayıtlara dahil edilebilmesi durumunu oldukça zorlaştırmaktadır (Vaidyanathan, 2017). Meydana gelen işlemler daha sonra değiştirilemediğinden denetçi işlem tarihine göre işlemin uygun dönemde kaydedildiğinden emin olabilecektir (Kuhn, 2018). Ancak bununla birlikte, örneğin, gelecekte alınacak olan bir hizmetin karşılığının önceden ödenmesi durumunda bu hizmet zaman içerisinde gerçekleştikçe giderleşecektir veya raporlama döneminde ticari mal satımı gerçekleşmesi durumunda yolda olan malların haklarının ve yükümlülüklerinin transferinde işlemin gerçekleştiği anda kaydedilmesi muhasebe standartlarındaki değerlendirme hükümleri ile uyuşmamaktadır (Schulman ve Wilson, 2019). Bu sebeple, blok zincirindeki zaman damgası denetçinin dönemsellik iddiasını test etmesini ortadan kaldırmayacağı düşünülmektedir.

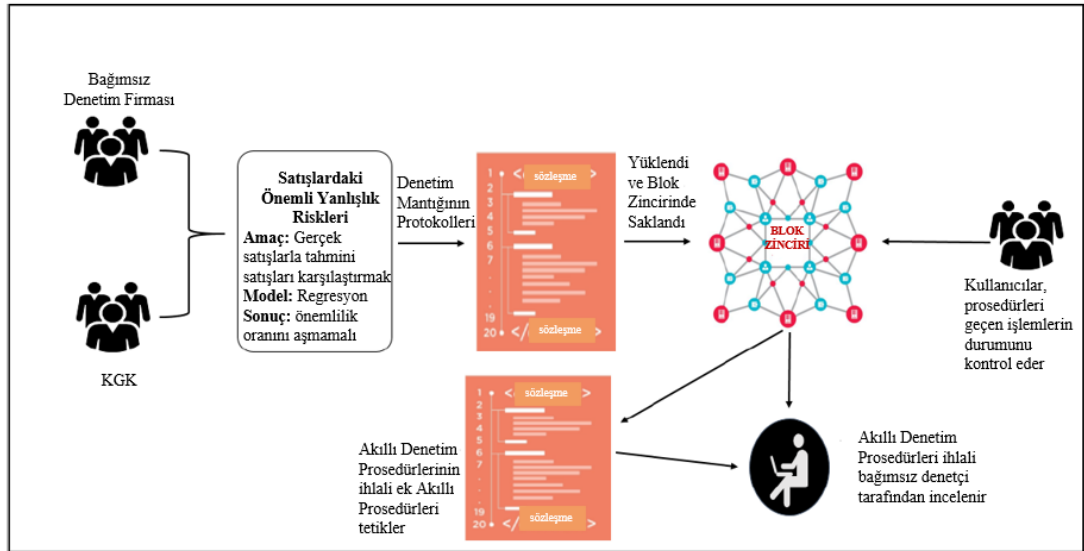
Denetçilerin odak noktası doğrudan işlemleri test etmek olmayacak, bunun yerine blok zincirinde yer alan işlemlerin doğru olduğundan emin olmak için kontrolleri test etmek olacaktır.

3.3.3.Akıllı Sözleşmeler ile Denetim

Rozario ve Vasarhelyi (2018) yaptıkları çalışmayla, akıllı sözleşmelerin bağımsız denetim sektöründe olası kullanım alanına dair bir örnek vermiş ve akıllı denetim prosedürleri kavramını kullanarak bağımsız denetimin kapsamını genişletmişlerdir. Bağımsız denetçinin blok zincirine yüklenen akıllı denetim prosedürleri, bağımsız denetçi adına otonom bir şekilde yürütülen denetimin verimliliğini, etkinliğini ve farklı paydaşların bilgi ihtiyaçlarını karşılayabilmek için daha zamanlı ve daha şeffaf bir denetim raporlamasıdır. Akıllı denetim prosedürleri kendi kendini yürüten denetim prosedürleri olup, akıllı iç kontrol testlerini (kendi kendini yürüten iç kontrol testleri) ve akıllı analitik prosedürlerini (kendi kendini yürüten analitik prosedürleri) içermektedir.

Örneğin; bağımsız denetimde, bağımsız denetçi ile Kamu Gözetim Kurumu (KGK), nakliyesi yapılan malların kayıtlara doğru bir şekilde kaydedilmeme riskini daha önceden belirledikleri denetim prosedürleri ile tespit edip takip edebilirler. Önceden belirlenen bu prosedürler eğer bu olursa şunu yap (IF-THEN) kuralları ile denetim firması tarafından akıllı denetim prosedürleri içine gömülür ve bağımsız denetçinin blok zincirine yüklenir. Ancak her durum akıllı sözleşmeler ile denetlenemeyeceği için bir taraftan da geleneksel denetim yöntemleri kullanılmaya devam edilmektedir. Böylelikle, çalışmada hem akıllı sözleşmeler ile denetim hem de geleneksel denetim yöntemleri kullanılması önerilerek melez bir model kurulmuştur. Akıllı denetim prosedürlerinin satışlara ilişkin önemli yanlışlık riskini tespit etmesi Şekil 3.3.3.1.'de tasvir edilmektedir.

Şekil 3.3.3.1. Satışlardaki Önemli Yanlışlık Riskinin Tespitinde Akıllı Denetim Prosedürlerinin Kullanılması



Kaynak: ROZARIO, A.M., VASARHELYI, M.A :2018, 'Auditing with Smart Contracts', International Journal of Digital Accounting Research, 18 (1): 1–27.

Örnekteki denetim riskine değinmek için akıllı analitik prosedürüne iki konu tanımlanabilir. Bunlardan ilki finansal ve finansal olmayan verileri içeren regresyon modeline dayanarak haftalık satış gelirini tahmin etmek, ikincisi ise regresyon modeline dayanarak tahmin edilen satışların gerçek satışlar ile karşılaştırılmasıdır. Akıllı sözleşmelerdeki “eğer bu olursa şunu yap” mantığı ile, gerçek satışlar toplam

önemlilik seviyesinin %5'ine eşittir, daha azdır veya daha fazladır şeklinde açıklama yapılabilir ve denetçi ek denetim prosedürlerine gerek kalmadan satış geliri hesabı için önemli yanlışlık riskini ölçebilir. Akıllı denetim prosedürlerinin sonuçları, denetim firmasının erişim izni verdiği herhangi bir blok zinciri kullanıcısı tarafından doğrulanabilir. Gerçek satışların programlanan kurallar ile eşleşmemesi durumunda bir hata mesajı görülecek ve detaylı inceleme yapılabilecektir.

Daha sonra, akıllı denetim prosedürleri ile tespit edilen kalemlerin işlenmesini yönetebilmek için denetçi, önemli kalemleri ya manuel olarak araştırarak ya da daha fazla araştırma gerektiren kayıtlara öncelik veren bir ek akıllı denetim prosedürü programlanabilecektir. Ayrıca bu akıllı denetim prosedürlerinin, denetçiler tarafından gerçekleştirilen denetim prosedürleri ile bu denetim prosedürlerinin uygulanmasını bekleyen KGK ve yasa koyucular arasındaki beklenti boşluğunu azaltmada fayda sağlaması beklenmektedir.

Bir satış işlemine ilişkin akıllı denetim prosedürleri geliştirildiği gibi başka konularda da yeni denetim prosedürleri geliştirilebilir. Örneğin, blok zinciri nesnelerin interneti cihazlarının takibini ve izlenmesini mümkün kıldığı için, malların yanlış yere nakliye edilme riskini değerlendirmek için denetim firması malların gerçek konumunu doğrulama ve malların olması gereken konumu ile karşılaştırma yapmak için bir iç kontrol testi tasarlayabilir (Rozario ve Vasarhelyi, 2018). Ayrıca akıllı kontrol prosedürleri müşteri siparişinin, sevkiyat belgelerinin ve satış faturalarının eşleştiğini ve doğru sırada gerçekleştiğini kontrol etmek için basit kurallara dayalı bir sistem olarak da tanımlanabilir (Rozario ve Thomas, 2019).

Tezin 3.2.3 Akıllı Sözleşme Risk Faktörleri bölümünde akıllı sözleşmelerle ilgili risklerden bahsedildiği üzere muhasebecilerin ve denetçilerin akıllı sözleşmelerin oluşturulmasında, yürütülmesinde ve kontrolün çok kritik bir yeri vardır. Güvenilir kişiler olarak görülen muhasebeciler ve denetçiler akıllı sözleşmelerin izlenmesi ve kontrolü ve yürütülen kodlanmış olan standartların veya diğer mevzuatlar için gereken kapsamlı bir muhasebe ve denetim uzmanlığına sahip olmalıdırlar (Schmitz ve Leoni, 2019). Blok zinciri kâhinleri de akıllı sözleşmelerde dikkat edilmesi gereken önemli konulardan biridir. Akıllı sözleşmeler yeni denetim riskleri yaratacağı için akıllı

denetim prosedürleri hem yeni risklere hem de mevcut olan risklere cevap verecek şekilde tasarlanmalıdır.

3.3.4.Küresel Faaliyeti olan Denetim Firmaları ve Uygulamaları

Blok zinciri teknolojisi ile ilgili girişimler ve uygulamalar arttıkça ve teknoloji benimsenmeye başlandıkça denetim firmaları müşterilerine danışmanlık verebilmek için çeşitli girişimlerde bulunmuşlardır. Yapılan çalışmalarda genellikle danışmanlık hizmetleri ve kripto paralar üzerinde durulmuştur. Küresel faaliyeti olan denetim firmaları yaptıkları çalışmalar ve hazırladıkları raporlarla blok zinciri teknolojisini yakından takip etmektedir ve teknoloji geliştikçe kendi uygulamalarını da aynı doğrultuda geliştirmişlerdir.

3.3.4.1.Deloitte

Deolitte 2015 yılında, Deliotte Rubix ismi verilen bir yazılım platformunu oluşturmuştur. Bu platformda hem kendi çalışma takımlarının hem de müşterilerinin ihtiyaçları doğrultusunda blok zinciri uygulamaları geliştirmeyi hedeflemiştir. Hizmet verdikleri müşteriler, herhangi bir uygulama için bu platformu kullanabiliyorken, Deliotte ise vermiş oldukları bağımsız denetim hizmetinin otomasyon sürecinde kullanmak istemektedir. Deloitte'in Rubix Projesinin liderlerinden Matthew Spoke'un daha önce yapmış olduğu bir röportajda hayata geçirdikleri Rubix Projesi ile blok zinciri altyapısını kullanarak denetim izlerinin takibinin zor olan süreçler için geliştirmeyi hedeflediklerini belirtmiştir (Allison, 2015).

Deloitte, 2016 yılında Kanada'nın Toronto şehrindeki ofislerine Bitcoin ATM'si kurmuştur (FinTech İstanbul, 2016). Bu ATM'yi sadece kendi çalışanlarının değil halkın da yararlanabilmesi için ofisin girişine yerleştirmişlerdir. Rubix'in kurucusu ve strateji lideri olan Iliana Oris Valiente Bitcoin ATM'sinin amacını şu şekilde açıklamıştır: *“Blok zinciri teknolojisinin geniş kitleler tarafından kabul edilmesi için ilk adım bilgidir ve bu teknolojiyi anlamının ilk aşaması Bitcoin'in nasıl çalıştığını anlamaktır. Amacımız bitcoini daha erişilebilir hala gelmesini sağlamak. Böylelikle kullanıcılar blok zinciri teknolojisini kullanmayı direkt kendileri tecrübe*

edinecekler, konuya olan anlayışları derinleşecek ve teknolojinin kabullenilmesi hızlanacaktır” (Leung, 2016).

Şekil 3.4.1.1. Deloitte Tarafından Kurulan Bitcoin ATM’si.



Deloitte Mayıs 2016’da, İrlanda’nın Dublin şehrinde Blockchain Lab (blok zinciri laboratuvarını) kurarak blok zinciri teknolojisi ile ilgili danışmanlık faaliyetini hayata geçirmiş ve müşterilerinin dağıtık defter teknolojisini iş süreçlerine entegre edebilme konusunda danışmanlık sunmayı amaçlamaktadır. Blockchain Lab, şirketlerin blok zinciri teknolojisinde başarı elde edebilmeleri için plan geliştirmesine yardımcı olmak için tasarlanmıştır. Burada blok zincirini öğrenen yeni biri de olabilirsiniz, blok zinciri uygulamalarını kullanmaya başlamış olan bir şirket de olabilirsiniz.

Ağustos 2019’da, Blockchain in a Box (BIAB) ismini verdikleri yeni bir platform kurduklarını duyurdular (Deloitte, 2019b). Bu platformun amacı müşterilerin blok zinciri tabanlı uygulamalarının gerçek hayatta nasıl kullanıldıklarını anlayabilmelerini sağlamaktır. Böylelikle müşterilerine kendi blok zinciri çözümlerini deneme fırsatı sunmaktadır. Deloitte, müşterilerin blok zinciri teknolojisine dair meraklarını, endişelerini ve sorularını bu platformda gerçekleşen uygulamalar sayesinde giderebilecektir. Deloitte ABD Blok Zinciri Lideri Linda Pawczuk’a göre bu platform müşteriler için pratik ve en önemlisi somut bir seçenek sunmaktadır.

Deloitte aynı zamanda Amazon ile birlikte blok zinciri hızlandırıcı programı olan Starup Studio'yu⁶ da desteklemektedir. Hukuk, mühendislik, finans, işe alım ve akıllı sözleşmeler gibi blok zinciri girişimlerinin çeşitli alanlarda kendilerini geliştirmek isteyenler için olanak sağlamaktadır.

Kripto paralar ve blok zinciri ile ilgili gelişmeleri ele alan Cointelegraph'ın sayfasındaki habere göre Deloitte Lüksemburg Ofisi, çalışanlarının kantinde yapacağı harcamalar için bitcoin kullanmalarına izin vermiştir (Zmudzinski, 2019). Amaçlarının bitcoin kullanımının nasıl gerçekleştiğini ve çalışanları tarafından blok zinciri teknolojisinin işleyişinin görülmesi olduğunu vurgulamışlardır. Çalışmanın sadece şirket içinde test edildiğini söylemişlerdir.

3.3.4.2.KPMG

Kpmg 2017 yılında Wall Street Blok Zinciri Birliği'ne (Wall Street Blockchain Alliance-WSBA) katılarak bu oluşumun bir üyesi olmuştur (WSBA, 2017). Wall Street Blok Zinciri Birliği blok zinciri, kripto varlıklar ve akıllı sözleşmelerin uygulama alanlarında bankacılık, yatırım yönetimi, hukuk, muhasebe gibi çeşitli sektörlerden dünya genelindeki çalışanların gelişmesini sağlamak amacı ile kurulmuş kâr amacı gütmeyen bir organizasyondur. Bu yüzden sermaye piyasaları ile çalışan çeşitli şirketlerin üyeliği ile yasal düzenlemelere de uyarak değer katmayı amaçlamışlardır. Ayrıca, dünyanın en saygın ve en büyük muhasebe örgütlerinden biri olan Amerikan Mali Müşavirler Enstitüsü (American Institute of Certified Public Accountants- AICPA) de bu birliğin üyelerinden biridir.

Yine 2017 yılında Microsoft ile birlikte dijital dönüşüm sürecinde müşterilerine danışmanlık faaliyetlerini vermeye devam edeceklerini duyurmuşlardır. Hatta 2019 yılında, bu birlikteliklerini beş yıl daha uzattıklarını dile getirmiş ve dijital dönüşüm strateji hedeflerini hızlandırabilmek için 5 milyar dolar yatırımda bulunacaklarını açıklamışlardır (Walters, 2019). Amaçları dijital dönüşümü en üst noktaya getirmektir.

⁶ Start up Studio IDEO CoLab Ventures tarafından başlatılmış olan ve çeşitli konularda uzmanların ve servis sağlayıcıların tek bir çatı altında toplandığı bir programdır.
<https://www.ideocolab.com/startupstudio/>, 25 Mart 2020.

Şubat 2019 yılında, müşterilerine blok zincirinde etkin iş süreçleri sağlamak için yeni dijital ürün ve hizmetler oluşturma konusunda uzman olan Guardtime ile bir işbirliğine girdiğini duyurmuştur (Kpmg, 2019a). Kpmg Amerika Blok Zinciri Lideri Arun Ghosh, Kpmg'nin derin iş ve teknik deneyimi ile Guardtime'ın blok zinciri platformunun, manuel işlemlerle dolu ve veri doğruluğunun, güvenin ve güvenliğin çok önemli olduğu alanlarda iş dönüşümünü teşvik ettiğini belirtmiştir.

Kpmg, Haziran 2019 yılındaki bir başka gelişme ile, reçeteli ilaçların takibi için Amerikan Gıda ve İlaç Kurumu (Food and Drug Administration-FDA), IBM, Walmart ve dünyanın en eski ilaç firmalarından olan Merck ile birlikte çalışacağını duyurmuştur. İsmi geçen şirketler arasında bir blok zinciri konsorsiyumu oluşturulmuştur. Merck ilaç şirketi, IBM teknolojik ortak ve Walmart eczaneler ve klinikler aracılığı ile dağıtıcı olurken Kpmg ise uyumluluk konuları ile ilgilenecektir. Bu pilot çalışmanın amacı ABD İlaç Tedarik Zinciri Güvenlik Yasasına (U.S. Drug Supply Chain Security Act) uymaya yardımcı çözümler bulmaktır (Kpmg, 2019b). Mayıs 2020'de biten pilot çalışmanın sonuçlarına göre, blok zinciri teknolojisinin sağladığı izlenebilirlik ve şeffaflık ile ilaç geri çekme işlemi üç gün yerine saniyeler içinde gerçekleştirilebilmiştir (IBM, 2020).

Yine 2019 yılında Microsoft, Tomia ve Corda platformunun kurucu şirketi R3 ile işbirliğine girmiştir. Amaçları blok zinciri teknolojisini kullanarak telekom firmaları arasındaki gerçek zamanlı ödemeler ve taşıyıcı firmalar ile mobil operatörler arasındaki anlaşmazlıkları azaltmak için bir çözüm önerisi geliştirmektir (Ghosh, 2019). Kpmg akıllı sözleşmelerin kullanıldığı bu uygulama ile telekomünikasyon şirketlerinin daha düşük maliyetlere katlanacaklarını ve ödemelerle ilgili anlaşmazlıkların giderileceğini düşünmektedir.

3.3.4.3.Ernts & Young

2017 yılında Ernts & Young (EY) tarafından hizmete sunulan EY Ops Chain platformu, şirketlerin iş ortakları, müşterileri ve tedarikçileri ile açık veya özel blok zincirleri üzerinden iletişim kurmasını sağlamaktadır. Stok veya sözleşmeler gibi önemli ticari varlıkların tokenlaştırılmasını kolaylaştırmayı ve bunları bir blok zincirinde, jeton, sözleşme veya ödemeler olarak temsil etmeyi amaçlamaktadır. Daha

sonra bu platformu bir adım öteye götürmüş ve 2018 yılında EY Ops Public Edition hizmetini hayata geçirdiklerini duyurmuştur.

2018’de, EY Ops Chain’in devamı olarak hayata geçirilen EY Ops Public Edition uygulamasında sıfır bilgi ispatı kullanılarak açık blok zinciri ağlarının daha güvenli hale getirilmesi amaçlanmıştır. Böylelikle açık blok zinciri ağları üzerindeki gizlilik endişeleri ortadan kaldırılacaktır (EY, 2018a). Yani hem açık blok zinciri ağlarının tüm olumlu özelliklerinden faydalanılabilecek hem de verilere gizlilik getirilebilecektir. Bu uygulamayı kullanarak işlemlere ilişkin bilgiler, bunları görmeye yetkisi olanlar hariç tüm blok zinciri kullanıcılarına gizli tutulacaktır. Şirketler, işlemlerin içeriklerini açıklamadan denetçilere ve yasa düzenleyicilere işlemlerin izlenebilirliği ve geçmişini sunmaya devam edebileceklerdir. Bu uygulamanın açık Ethereum blok zincirinde sıfır bilgi ispatının kullanıldığı ilk uygulama olduğu belirtilmiştir.

EY, 2018 yılında, blok zinciri teknolojisini denetim mesleğinde kullanmak için Blockchain Analyzer isimli bir yazılım geliştirmiştir (EY, 2018b). Bu uygulama kripto para kullanan şirketlerin denetiminde, denetim ekiplerine yardımcı olması için tasarlanmıştır. EY Blockchain Analyzer, denetim ekiplerinin bir şirketin tüm işlem verilerini birden fazla blok zinciri defterinden almasını kolaylaştırmak için tasarlanmıştır. Daha sonrasında denetçiler bu verileri sorgulayabilecek, işlemlerin analizini yapabilecek ve müşterilerin defterindeki kayıtlardan aykırılık gösteren işlemleri tanımlayabileceklerdir. Bu uygulama BitCoin, Ether, BitCoin Cash, LiteCoin gibi birden fazla kripto para birimlerini veya varlık yönetimi firmaları tarafından yönetilen veya ticareti yapılan diğer kripto varlıkların test edilmesini destekleyecek şekilde tasarlanmıştır. Ayrıca şirketler blok zinciri teknolojisini benimsedikçe, bu uygulama işletmenin blok zinciri varlıklarını, borçlarını ve özsermayesini ve akıllı sözleşmeleri test etmek için de bir temel oluşturacaktır. EY bu yazılı denetim ekiplerine işletmenin kayıtları ve defterleri ile dağıtık defterin mutabakatını yapabilmek için tasarlamış olup, denetim ekiplerinin müşterilerin blok zincirinde ne yaptıklarını ve işlerinin bu çevrede nasıl şekillendiğini anlamalarına yardımcı olması beklenmektedir. 2019 senesinde ise bu uygulamayı geliştirerek bir adım öteye götürmüşlerdir. Uygulamanın ilk sürümü kripto varlık ağırlıklı denetimleri ve

işlemleri esas almıştı. Ancak teknolojinin gelişmesi ile birlikte uygulamanın ikinci sürümü denetim, vergi ve işlemlerin izlenmesi gibi müşterilerin ihtiyaçlarına göre çeşitli amaçlar için tasarlanmıştır. İşlemlerin analizinin yanı sıra Blockchain Analyzer uygulamasının ikinci sürümü kripto varlıklar için vergi hesaplamasında da müşterilere destek sağlayacaktır.

Mart 2019’da vergilendirme için Crypto-Asset Accounting and Tax (CAAT) isimli bir araç geliştirmiştir (EY, 2019). EY kripto varlıklarını elinde tutan ve ticaret yapan müşteri sayısında önemli artış gördüğünü belirtmiştir. EY CAAT, bilançolarında kripto varlığı olan kurumsal müşterilerine ve bu tür varlıkların daha küçük ölçekte ticaretini yapan kurumsal ve bireysel müşterilere hizmet etmek için kullanacaktır. Bu araç, kripto varlıklardan elde edilen kazançları ya da kayıpları Amerika Gelir İdaresine (Internal Revenue Service-IRS) beyan hazırlanmasında yardımcı olmak için tasarlanmıştır.

3.3.4.4.PWC

2017 Yılında PwC Hong Kong Ofisi sundukları hizmetler için bitcoini ödeme aracı olarak kabul ettiklerini duyurmuştur. İlk olarak dijital paralar ve blok zinciri teknolojisi ile ilgilenen yerel firmalarda buna başlayacaklarını söylemişler ve amaçlarının bu uygulama ile blok zinciri teknolojisini anlamak olduğunu belirtilmiştir.

2018 yılında, kendi çalışanlarının blok zinciri ve diğer gelişen teknolojiler hakkında bilgilerini artırma ve kendilerini geliştirme amacı ile Digital Accelerators programını hayata geçirmişlerdir. PwC’de Dijital Yetenekler lideri ve Dijital Accelerators programının müdürü olan Sarah McEnaney masa başında oturan çalışanların daha fazla teknolojik beceriye sahip olmaları gerektiğini belirtmiş ve rekabette yer alabilmek ve müşterilerinin ihtiyaçlarına cevap verebilmek için bu eğitim gerekli olduğundan bahsetmiştir. 2 yıl sürecek olan programa 1,000 PwC çalışanı seçilmiştir (Liffreing, 2018).

PwC İsviçre Ofisi, Temmuz 2018’de Tezos şirketini denetleyeceğini duyurmuştur. Tezos, 2014 yılında Arthur and Kathleen Breitman tarafından tasarlanan

merkezi olmayan uygulamaları ve akıllı sözleşmeleri destekleyen çok amaçlı bir blok zinciri ve bir kripto para projesidir. Tezos İsviçre’de kâr amacı gütmeyen bir vakıf kuran Amerika merkezli bir şirkettir (Mendelson, 2019). Tezos projesinin yatırımcıları, girişimler için yatırım toplama aracı olan ve "ilk para teklifi"⁷ olarak bilinen bir kitle fonlaması yöntemi ile Bitcoin ve Ethereum kullanarak jeton satın almış ve Tezos, 232 milyon değerinde para toplamıştır (Dinzeo, 2020). Yatırımcıların karşılığında satın aldıkları bu jetona ise “tezzie” denmektedir (Ortolani, 2019). Tezos, federal menkul kıymetler düzenlemesinden endişe duyarak, Tezos jetonları alımlarının bağış olduğunu iddia ederek kâr amacı gütmeyen bir vakıf oluşturup yasal gerekliliklerden kaçınmaya çalışmıştır (Mendelson, 2019). Ekim 2017’de, bir medya kuruluşu Breitman’lar ve Tezos Vakfı başkanı Johann Gevers arasında çıkan söylentiler hakkında bir haber yapmış ve kurucular arasında bir anlaşmazlık olduğu ortaya çıkmıştır. Herkes projenin çok başarılı olduğunu düşünüp lansman yapmasını beklerken, bu durum yatırımcıların aklında soru işaretleri bırakıp tedirgin etmeye başlamıştır. Yatırımcılar, blok zinciri projesinin erteleneceğinden ve bekledikleri kadar kâr elde edemeyeceklerinden endişe duymaya başlamıştır. Ayrıca ilk para teklifinin bir yatırım mı yoksa bağış mı olduğu konusunda da bir yanlış anlama bulunmaktaydı. Breitman’lar ise, ilk para teklifinin bir yatırım planı olmadığını ve katkıda bulunanlara Tezos jetonları sağlama yükümlülüğü olmadığını iddia etmekteydi. Ancak yatırım yapanlar ise, yaptıkları katkının Tezos’un parayı kabul etmeden önce, ABD Menkul Kıymetler ve Borsa Komisyonu’na (U.S. Securities and Exchange Commission) kaydolmalarını gerektiren yatırımlar olduğunu savunmaktaydı. Yatırımcılar ayrıca, Bitcoin ve Ethereum’larını da geri istemekteydi (Dinzeo, 2020). PwC, iç karışıklar ve toplu davaları olan bu şirketin bağımsız denetimini üsteleneceğini açıklamıştır (Marshall, 2018).

2019 yılında, kripto para birimleri ile işlem yapan kurumlara güvence hizmeti sunabilmek ve kripto para birimlerinin denetimi için, mevcut olan Halo denetim

⁷ Bir projeyi hayata geçirmek için girişimciler tarafından başlangıç yatırımların bir dijital para (coin) veya jeton (token) satışı ile sağlanan kitle fonlamasına İlk Para Teklifi (ICO-Initial Coin Offering) denmektedir. Yeterli fon toplanıp proje hayat geçirildikten sonra yatırımcılar isterlerse bu jetonları satabilir ve projeden çıkabilir ya da isterlerse projede kalıp jetonların sağladığı haklardan yararlanabilirler (Güven ve Şahinöz, 2018).

takımına ek bir denetim aracını hayata geçirdiklerini duyurmuştur. PwC bu aracı ile, Bitcoin, Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond, LiteCoin, Ethereum, ERC20 - OAX jetonu ve Ripple kripto para birimlerini elinde tutan veya işlem gerçekleştiren müşterileri için güvence hizmeti sunmaktadır (PwC, 2019).

Cointelegraph'ın sayfasındaki habere göre dünya çapında bir işe alım platformu olan Indeed'in Mart 2019 tarihi itibari ile yer alan ilanlarına göre, dört büyük denetim firmaları arasında blok zinciri ile ilgili en fazla alıma sahip şirket 40 iş ilan ile PwC'dir. Bunu sırası ile 17 ilan ile EY ve 10 ilan ile Deloitte takip etmektedir. Kpmg'nin ise bu platformda bir işe alım ilanı bulunamamıştır (Zmudzinski, 2019).

3.3.4.5.Diğer

Dört büyük denetim firmasının haricinde küresel faaliyet gösteren diğer denetim firmalarından BDO ve Grant Thornton'un da blok zinciri konusunda girişimleri bulunmaktadır.

BDO'nun Avustralya ofisi 2019 yılında, blok zinciri ve kripto varlıklara denetim ve güvence hizmetleri getirmek için kurumsal düzeyde dijital varlıklar ve hizmetler geliştiren uzman bir blok zinciri şirketi olan Decentralized Capital ile ortaklık kurmuştur. Ortaklık kapsamında BDO, blok zinciri şirketleri ve kripto para birimleri, ticaret platformları ve İlk Para Teklifi ve fonlar gibi varlıklar için kapsamlı denetim ve güvence hizmetleri sağlayacaktır. BDO, Finansal Tablo Denetimi, Varlık Denetimi ve Akıllı Sözleşme Denetimi olmak üzere üç tür blok zinciri merkezli denetim hizmeti sunmaktadır (BDO, 2019). Bu ortaklığın ise daha fazla kurumsal yatırımcıyı cezbedeceğini düşünülmektedir.

Bir diğer büyük denetim firması olan Grant Thornton ise, 2020 yılı Nisan ayında işletmelerin aynı gruptaki şirketler arasındaki işlemleri yönetmesine yardımcı olmak için *inter.x* isimli bir blok zinciri çözümünü açıklamıştır. Şirketin yapmış olduğu açıklamaya göre genellikle şirketler arası işlemler olarak bilinen, bir şirket grubu içindeki ticari varlıklar arasındaki finansal ilişkiler, küresel ekonominin %30 ile %40'ını oluşturmakta ve bu oranda yılda yaklaşık 40 trilyon dolara denk gelmektedir. Grant Thornton'un amaçlarından biri, bu şirketler arası işlemlere grup düzeyinde

görünürlük sağlamaktır (Grant Thornton, 2020). Uygulama, transfer fiyatlandırması ve hazine yönetimi ile ilgili iki noktaya değinmektedir.



SONUÇ

Günümüzde dijitalleşme ile birlikte işletmelerin iş yapış şekilleri değişmekte ve işletmelerin değişime ayak uydurması gerekmektedir. Yeni teknolojilerin mevcut iş süreçlerine dahil edilmesi artık bir tercih değil, bir zorunluluk haline gelmektedir. İşletme yönetiminin bu teknolojilerin gerektirdiklerini anlayarak ve yasa koyucuların da bu teknoloji ile ilgili düzenlemeleri ile birlikte blok zinciri teknolojisinden en üst düzeyde verim sağlanabilecektir.

Teknolojinin yeni yeni gelişmesi ve çok fazla teknik bilgi içermesi sebebi ile yeterince anlaşılamamakta ve bu yüzden de benimsenememektedir. Özellikle Bitcoinin ortaya çıkışı ile birlikte konuşulmaya başlanan blok zinciri teknolojisinin, kripto paralardan farklı olduğu, bitcoin ile blok zincirinin aynı şey olmadığı henüz tam anlamıyla anlaşılamamıştır.

Gün geçtikçe artan blok zinciri teknolojisi ile mevcut olan riskler hem devam etmekte hem de yeni teknoloji beraberinde yeni riskler de getirmektedir. İşletmeler bu risklerin tespitini yapmalı ve gerekli önlemleri almalıdır. İç denetim departmanları kendilerini blok zinciri konusunda geliştirmeleri, işletmeler de bu departmanda çalışanlar için ek bütçe ayırıp bu konu ile ilgili eğitim almalarını sağlamalıdır. İç denetim departmanlarının bu teknolojinin getireceği faydaları anlamaları gerekmektedir beraber, her sorun için bir çözüm önerisi olmadığını da yönetimi bildirmelidir.

Blok zincirinin sahip olduğu değiştirilememe, merkezi olmayan, şeffaflık ve zaman damgası sağlayan özellikleri sayesinde veri güvenliği sağlanmakta ve verilerin manipülasyonunu ciddi bir şekilde önlemektedir. Muhasebe mesleğinde blok zinciri teknolojinin kullanılması, finansal raporlamada sürekli ve gerçek zamanlı raporlama gibi fırsatlar sunmaktadır. Özellikle taraflar arasında bir güvence hizmeti sunan bağımsız denetim için de çok büyük değişimler gerçekleşmesi beklenmektedir. Kaydedilen bilgilerin değiştirilememesi ve silinememesi sebebi ile muhasebe kayıtlarının güvenilirliğinin artması, örneklem seçimini ortan kaldırarak tüm ana kütlenin denetlenmesi ve mutabakatların azalması, blok zinciri teknolojisinin denetim mesleğine sunduğu fırsatlar olarak sıralanabilir. Denetçilerin ise bilgi teknolojileri ve teknik bilgilerini arttırmaları gerekmektedir. Blok zincirinin yapısını anlayıp,

mutabakat mekanizmalarını, blok zinciri ağ türlerini ve anahtar yönetiminin önemini, akıllı sözleşmelerle ilgili riskleri öğrenmelidirler. Giderek bilgi teknolojisi ağırlıklı denetim anlayışına dönüşen denetim mesleğinde, günümüzde ilk işe alırken personel seçimi de değişim göstereceği alanlardan biridir.

Sonuç olarak, güveni sağlayan aracı kurumlara karşı olan ihtiyacın sorgulanması ve aracı kurumlara olan güvene ihtiyaç olunmadığını göstermek üzere ortaya çıkan blok zinciri teknoloji ile bankacılık ve finans sektöründe, lojistik ve tedarik zinciri, sağlık sektörüne kadar birçok sektörün etkilenecek, özellikle maliyetten ve zamandan tasarruf edilmesi beklenmektedir.

KAYNAKÇA

ACCA.: 2019	Audit And Technology. ACCA And CA ANZ.
ACCENTURE:2019	<i>The post-digital era is upon us are you ready for what's next.</i> Technical report, Accenture Technology Vision 2019.
AHİ, G.: 2018	Akıllı sözleşmeler, 2 Mayıs 2018, (Çevrimiçi) https://digitalage.com.tr/makale/akilli-sozlesmeler/ , 15 Nisan 2020
AKBANKLAB: 2018	Akbank'ta Ripple Üzerinden Sterlin Transferleri Başladı!, 13 Aralık 2018, (Çevrimiçi) https://www.akbanklab.com/tr/guncel/basinda-biz/akbankta-ripple-uzerinden-sterlin-transferleri-basladi , 13 Mayıs 2020
AKGİRAY, V.:2019	The Potential for Blockchain Technology in Corporate Governance. OECD Corporate Governance Working Papers No.21 2019.
AKLEYLEK, S., YILDIRIM, H. M., TOK, Z.:2011	“Kriptoloji Ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta”. Akademik Bilişim . 713-718.
AL-SAQAF, W., SEIDLER, N. :2017	Blockchain technology for social impact: opportunities and challenges ahead. <i>Journal of Cyber Policy</i> , 2(3), 338-354.
ALLISON, I.:2015	Deloitte, Libra, Accenture: The work of auditors in the age of Bitcoin 2.0 technology, August 18, 2015, (Çevrimiçi) https://www.ibtimes.co.uk/deloitte-libra-accenture-work-auditors-age-bitcoin-2-0-technology-1515932 , 25 Mart 2020.

ALTUNDAĞ, S.:2006	“Dijital İmzanın Ticari Hayatta Kullanılması ve Düzenlenmesi”. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 10(1), 55-76.
ANDERSEN, N.:2016	Blockchain Technology: A Game-Changer In Accounting. <i>Deloitte, March</i> .
ANDERSON, R.:1996	Information Hiding: First International Workshop, Cambridge, Uk, May 30-June 1, 1996. Proceedings (Vol. 1). Springer Science & Business Media.
ANTONOPOULOS, A. M.:2014	Mastering Bitcoin: Unlocking Digital Cryptocurrencies. " O'Reilly Media, Inc."
APPELBAUM, D., NEHMER, R.:2017	Designing and Auditing Accounting Systems Based on Blockchain and Distributed Ledger Principles. Feliciano School Of Business .
ARNOLD, A.:2018	Blockchain Is Not A Threat To Accounting, It's An Opportunity, 28 Ağustos 2018, (Çevrimiçi) https://www.forbes.com/sites/andrewarnold/2018/08/28/blockchain-is-not-a-threat-to-accounting-its-an-opportunity/#3d71adc868d0 , 27 Haziran 2020.
ASTRI:2016	Whitepaper on Distributed Ledger Technology, November 2016, (Çevrimiçi) https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf , 9 Mayıs 2020.
AYTAÇ, H.:2017	“Bitcoin Nedir? Ne İşe Yarar? Bitcoin Hakkında Bilinmesi Gerekenler”, 6 Ekim 2017, (Çevrimiçi) www.hasanaytac.net/genel/bitcoin/bitcoin-nedir-ne-ise-yarar-bitcoin-hakkinda-bilinmesi-gerekenler/ , 11 Mayıs 2020

BACK, A.:2002	Hashcash-a denial of service counter-measure. (Çevrimiçi) file:///C:/Users/Hp/Downloads/hashcash.pdf, 13 Ağustos 2019
BAMBROUGH B.:2019	PayPal And Visa Warned Bitcoin Presents A 'Ludicrous' Existential Challenge, March 4, 2019, (Çevrimiçi) https://www.forbes.com/sites/billybambrough/2019/03/04/paypal-and-visa-warned-bitcoin-presents-a-ludicrous-existential-challenge/#21d7699d3e22 , 9 Mayıs 2020
BARAN, P.:1964	On Distributed Communications Networks. IEEE Transactions On Communications Systems, 12(1), 1-9.
BARON, J.:2017	Blockchain, accounting and audit: What accountants need to know. Accounting Today, March 27, 2017, (Çevrimiçi) https://www.accountingtoday.com/opinion/blockchain-accounting-and-audit-what-accountants-need-to-know#:~:text=Like%20most%20forms%20of%20technology,owners%20of%20the%20accounting%20system , 28 Haziran 2020
BDO: 2019	Blockchain, 2019, (Çevrimiçi) https://www.bdo.com.au/en-au/industries/financial-services/blockchain , 25 Mart 2020
BDS 500: 2019	Bağımsız Denetim Standardı 500, Bağımsız Denetim Kanıtları, 31/12/2019 tarihli ve 30995 (4.Mükerrer) sayılı Resmi Gazete.
BECK, R.:2018	Beyond Bitcoin: The Rise of Blockchain World. Computer , 51(2), 54-58.
BIBLE, W., RAPHAEL, J., TAYLOR, P., VALIENTE, I. O.:2017	Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession. CPA Canada and AICPA. Aicpa. Org

BIS: 2017	Distributed ledger technology in payment, clearing and settlement. An analytical framework., Bank for International Settlements, February, 2017, (Çevrimiçi) https://www.bis.org/cpmi/publ/d157.pdf , 10 Mayıs 2020
BLOCKCHAIN.COM , ERİŞİM TARİHİ: 19 MAYIS 2020	Dolaşımdaki Toplam Bitcoin, 2020, (Çevrimiçi) https://www.blockchain.com/charts/total-bitcoins , 19 Mayıs 2020
BLOCKLEDGER: 2019	REBRAND OF LEDGERIUM TO BLOCK LEDGER AND INAUGURAL PRODUCT LAUNCH (LUCA), 13 June, 2019, (Çevrimiçi) https://www.theblockledger.net/rebrand-of-ledgerium-to-block-ledger-and-inaugural-product-launch-luca/ , 23 Haziran 2020.
BRADBURY, D.:2015	How the Blockchain Could Stop Firms Cooking the Books, Feb 7, 2015, (Çevrimiçi) https://www.coindesk.com/how-the-blockchain-could-stop-firms-cooking-the-books , 11 Şubat 2020.
BRENDER, N., GAUTHIER, M., MORIN, J. H., SALIHI, A.:2018	The Potential Impact of Blockchain Technology on Audit Practice.
BROWN, R.G.:2015	“A Simple Model for Smart Contracts”. Richard Gendal Brown, 10.
BROWN, R.G.:2016	INTRODUCING R3 CORDA™: A DISTRIBUTED LEDGER DESIGNED FOR FINANCIAL SERVICES, April 5, 2016, (Çevrimiçi) https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financialservices/ , 13 Mayıs 2020

BROWN, R. G., CARLYLE, J., GRIGG, I., HEARN, M.:2016	Corda: an introduction., R3 CEV, August, 1, 2015, (Çevrimiçi) https://blockchainlab.com/pdf/corda-introductory-whitepaper-final.pdf , 13 Mayıs 2020
BTC.COM, ERİŞİM TARİHİ: 2 TEMMUZ 2020	Havuz Dağılımı, 2020, (Çevrimiçi) https://btc.com/stats/pool?pool_mode=day , 2 Temmuz 2020
BUTERIN V.: 2015	Visions, Part 1: The Value of Blockchain Technology, April 13, 2015, (Çevrimiçi) https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/ , 11 Mayıs 2020
BYSTRÖM, H.:2019	Byström, H. (2019). Blockchains, real-time accounting, and the future of credit risk modeling. <i>Ledger</i> , 4, pp.40-47.
CAI, C. W.:2019	“Triple-Entry Accounting with Blockchain: How Far Have We Come?”. Accounting & Finance .
CALLAHAN, A.:2019	“How Fund Transfers, Direct Deposits and Electronic Banking Trace Back to the Telegraph”, December 18, 2019, (Çevrimiçi) https://www.cpapracticeadvisor.com/accounting-audit/news/21118625/how-fund-transfers-direct-deposits-and-electronic-banking-trace-back-to-the-telegraph , 25 Nisan 2020
CAMPBELL, R.: 2016	Sweden Tests Blockchain Smart Contracts for Land Registry, June 22, 2016, (Çevrimiçi) https://cointelegraph.com/news/sweden-tests-blockchain-smart-contracts-for-land-registry , 7 Mayıs 2020
CANBEK, G., SAĞIROĞLU, Ş.:2006	“Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme”. Gazi Üniversitesi Politeknik Dergisi , 9(3), 165-174.

CARLIN, T.:2019	“Blockchain and The Journey Beyond Double Entry”. Australian Accounting Review , 29(2), 305-311.
CARON, F.:2017	Blockchain: Identifying Risk On The Road to Distributed Ledgers. <i>ISACA Journal</i> , 5.
CASEY, M. J., VIGNA, P.:2018	“In Blockchain We Trust”. MIT Technology Review , 121(3), 10-16.
CHALKER, A.:2018	Why Internal Auditors Must Care Blockchain, June 12, 2018, (Çevrimiçi) https://blog.protiviti.com/2018/06/12/internal-auditors-must-care-blockchain/ , 18 Nisan 2020
CHAVEZ-DREYFUSS G.:2015	Honduras to build land title registry using bitcoin technology, May 15, 2015, (Çevrimiçi) https://in.reuters.com/article/usahonduras-technology/honduras-to-build-land-title-registry-using-bitcoin-technologyidINKBN0O01V720150515 , 7 Mayıs 2020
CHEAPSSL: 2017	SHA-1, SHA-2 ve SHA-256 Hash Algoritmaları Arasındaki Farklar, 12 Eylül 2017, (Çevrimiçi) https://www.cheapssl.com.tr/blog/sha-1-sha-2-ve-sha-256-hash-algoritmaları-arasindakifarklar.html , 3 Ocak 2020.
CHEDRAWI, C., HOWAYECK, P.:2018	Audit in The Blockchain Era Within A Principal-Agent Approach. <i>Information And Communication Technologies in Organizations and Society (ICTO 2018): “Information and Communications Technologies For An Inclusive World</i> .
COINMARKETCAP, ERİŞİM TARİHİ: 19 MAYIS 2020	Toplam Piyasa Değeri Yüzdesi (Hâkimiyet), 2020, (Çevrimiçi) https://coinmarketcap.com/charts/#dominance-percentage , 19 Mayıs 2020

CONG, L. W., HE, Z.:2019	“Blockchain Disruption and Smart Contracts””. The Review of Financial Studies , 32(5), 1754-1797.
COYNE, J. G., MCMICKLE, P. L.:2017	“Can Blockchains Serve An Accounting Purpose?”. Journal of Emerging Technologies in Accounting , 14(2), 101-111.
CREDIT SUISSE:2016	Blockchain-The Trust Disrupter. 3 August, 2016, (Çevrimiçi) https://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf , 2 Şubat 2020.
CREDIT SUISSE:2018	Blockchain 2.0. <i>Connections series</i> , 11. (Çevrimiçi) https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&sourceid=csplusresearchcp&document_id=1080109971&serialid=pTkp8RFIoVyHegdQM8EllLNi1z%2Fk8mInqoBSQ5KDZG4%3D , 25 Mayıs 2020.
CROSBY, M., PATTANAYAK, P., VERMA, S., KALYANARAMAN, V.:2016	“Blockchain Technology: Beyond Bitcoin”. Applied Innovation , (2), 6-10.
ÇARKACIOĞLU, A.:2016	Kripto-Para Bitcoin. Sermaye Piyasası Kurulu Araştırma Dairesi Araştırma Raporu, 3 Nisan 2020
DAI, J., VASARHELYI, M. A.:2017	“Toward Blockchain-Based Accounting and Assurance”. Journal Of Information Systems , 31(3), 5-21.
DAI, J.:2017	<i>Three Essays On Audit Technology: Audit 4.0, Blockchain, And Audit App</i> (Doctoral Dissertation, Rutgers University-Graduate School-Newark).

DAI, W.:1998	B-Money. (Çevrimiçi) http://www.weidai.com/bmoney.txt , 20 Mart 2020.
DAVIDSON, S., NOVAK, M., POTTS, J.:2018	The Cost of Trust: A Pilot Study. The JBBA. 1(2). 1-7. <i>Available At SSRN 3218761.</i>
DELOITTE, TÜSİAD.:2018	Blokzincir Potansiyelinin Keşfi 2018 Yılı Türkiye Blokzincir Araştırması., (Çevrimiçi) https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/consulting/blokzincirpotansiyelinin-kesfi.pdf , 1 Mayıs 2020.
DELOITTE:2019A	An Internal Auditor's Guide to Blockchain. Risk Considerations In Blockchain Technology. Deloitte Development LLC.
DELOITTE: 2019B	Deloitte Debuts 'Blockchain In a Box' (BIAB), August 20, 2019, (Çevrimiçi) https://www2.deloitte.com/us/en/pages/about- deloitte/articles/press-releases/blockchain-in-a-box.html , 25 Mart 2020
DEMİREL, C.:2018	Mors Kodu Hakkında Bilmeniz Gereken Her Şey, 18 Haziran, 2018 (Çevrimiçi) http://blog.milliyet.com.tr/mors-kodu-hakkinda-bilmeniz- gereken-her-sey/Blog/?BlogNo=589773 , 30 Nisan 2020
DI PIERRO, M.:2017	"What is the Blockchain?". Computing in Science & Engineering , 19(5), 92-95.
DIB, O., BROUSMICHE, K. L., DURAND, A., THEA, E., HAMIDA, E. B.:2018	Consortium Blockchains: Overview, Applications and Challenges. International Journal On Advances in Telecommunications , 11(1&2).

DIGICONOMIST: 2019	Bitcoin Energy Consumption Index, (Çevrimiçi) https://digiconomist.net/bitcoin-energy-consumption , 9 Mayıs 2020
DINZEO, M.:2020	Tezos Cryptocurrency Founders Settle With Investors for \$25 Million, March 20, 2020, (Çevrimiçi) https://www.courthousenews.com/tezos-cryptocurrency-founders-settle-with-investors-for-25-million/?utm_source=rss&utm_medium=rss&utm_campaign=tezos-cryptocurrency-founders-settle-with-investors-for-25-million , 25 Mart 2020.
DOĞAN, K., ARSLANTEKİN, S.:2016	“Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum”. Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi , 56(1).
DOĞANTEKİN, S.: 2016	“Yeni Sihirli Kelime: Bitcoin”, 30 Eylül 2016, (Çevrimiçi) https://medium.com/@sdogantekin/yeni-sihirli-kelime-blockchain-68864a30fee9 , 19 Mart 2020
DRANE, J.:2016	Wait, blockchains need audited?!?, 21 Aralık 2016, (Çevrimiçi) https://www.linkedin.com/pulse/wait-blockchains-need-audited-jeremy-drane/ , 19 Mayıs 2020
DWORK, C., NAOR, M.:1992.	Pricing via processing or combatting junk mail. In <i>Annual International Cryptology Conference</i> (pp. 139-147). Springer, Berlin, Heidelberg.
ECLECTICA, ERİŞİM TARİHİ: 19 NİSAN 2020	Jacquard's Loom and the stored programme concept, (Çevrimiçi) http://addiator.blogspot.com/2011/10/jacquards-loom-and-stored-programme.html , 19 Nisan 2020.
EKBLAW, A., AZARIA, A., HALAMKA, J. D., LIPPMAN, A.:2016.	A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data. Whitepaper, August, 2016, (Çevrimiçi) https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5a6fd2f7e2c48387dff12676/1517278000381/

	blockchain-medical-records-patient-data-medrec-eckblaw.pdf, 8 Mayıs 2020.
EL IOINI, N., PAHL, C.:2018	A review of distributed ledger technologies. In <i>OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"</i> (pp. 277-288). Springer, Cham.
ESSINGER, J.:2004	<i>Jacquard's Web: How A Hand-Loom Led to The Birth of The Information Age</i> . OUP Oxford.
EY: 2018A	EY launches the world's first secure private transactions over the Ethereum public blockchain, 30 Oct, 2018, (Çevrimiçi) https://www.ey.com/en_gl/news/2018/10/ey-launches-the-world-s-first-secure-private-transactions-over-the-ethereu-public-blockchain , 25 Mart 2020
EY: 2018B	EY announces blockchain audit technology, 24 Aprl, 2018, (Çevrimiçi) https://www.ey.com/en_gl/news/2018/04/ey-announces-blockchain-audit-technology , 25 Mart 2020.
EY:2019	New EY CAAT technology facilitates cryptocurrency reporting and compliance, 4 Mar, 2019, (Çevrimiçi) https://www.ey.com/en_us/news/2019/03/new-ey-caat-technology-facilitates-cryptocurrency-reporting-and-compliance , 25 Mart 2020.
FEDOROV, A. K., KIKTENKO, E. O., LVOVSKY, A. I.:2018	Quantum computers put blockchain security at risk. Nature.
FERF, DELOITTE:2018	BLOCKCHAIN FOR FINANCIAL LEADERS: OPPORTUNITY VS. REALITY. (Çevrimiçi) https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-fei-blockchain-report-future-hr.pdf , 13 Mayıs 2020.

FERNÁNDEZ-VALÈNCIA, R., CAUBET, J., & VILA, A.: 2018	Cryptography Working Group Introduction to Blockchain Technology.
FinCEN:2015	FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger, May 5, 2015, (Çevrimiçi) https://www.fincen.gov/sites/default/files/2016-08/20150505.pdf , 20 Haziran 2020
FİNTECH İSTANBUL, :2016	Deloitte Bitcoin ATM'si kurdu., 8 Eylül 2016, (Çevrimiçi) https://fintechistanbul.org/2016/09/08/deloitte-bitcoin-atmsi-kurdu/ , 25 Mart 2020.
FRAMINGHAM, M.: 2019	Worldwide Blockchain Spending Forecast to Reach \$2.9 Billion in 2019, According to New IDC Spending Guide, March 4, 2019, (Çevrimiçi) https://www.idc.com/getdoc.jsp?containerId=prUS44898819 , 18 Mayıs 2020.
FRANCIS-POULIN, M., ERİŞİM TARİHİ: 30 NİSAN 2020.	Electronic Payments: A Brief History, (çevrimiçi), https://blog.forte.net/electronic-payments-history/ , 30 Nisan 2020
GAL, A.:2018	The Tangle: an Illustrated Introduction, Jan 31, 2018, (Çevrimiçi) https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4 , 10 Mayıs 2020
GIBLIN, M.:1991	<i>The impact of electronic data interchange (EDI) on Irish foreign trade and transport</i> (Doctoral dissertation, Dublin City University).
GIFFORD, E. A.:1988	Electronic Information Security. IEEE Potentials , 7(4), 26-30.
GHOSH, A.:2019	KPMG is working with TOMIA and Microsoft to create a near real-time settlement network for telecom companies, July 16, 2019, (Çevrimiçi)

	https://info.kpmg.us/news-perspectives/technology-innovation/blockchain-streamlining-settlements-between-telecom-companies.html , 25 Mart 2020.
GODA, K., KITSUREGAWA, M.:2012	The History of Storage Systems. <i>Proceedings of the IEEE, 100(Special Centennial Issue)</i> , 1433-1440.
GÖRMEZ, B.:2017	Finansal Sektörde Yıkıcı Yenilik: Dağıtılmış Defter Teknolojisi Ve Türkiye Sermaye Piyasalarının Durumu (Distributed Ledger Technologies/Blokchain). Sermaye Piyasası Kurulu Aracılık Faaliyetleri Dairesi, Yeterlik Etüdü.
GRANT THORNTON: 2020	Grant Thornton moves intercompany transactions to the blockchain, 30 April, 2020, (Çevrimiçi) https://www.grantthornton.com/library/press-releases/2020/april/GT-moves-intercompany-transactions-blockchain.aspx , 20 Mayıs 2020.
GRIGG, I.:2005	Triple Entry Accounting. Systemics Inc. 25/12/2005, (Çevrimiçi) https://iang.org/papers/triple_entry.html , 6 Mayıs 2020.
GUPTA, M.:2017	Blockchain For Dummies®, IBM Limited Edition, John Wiley & Sons, Inc. <i>Hoboken, NJ</i> .
GÜMÜŞHAN, H.:2018	Yazının Tarihsel Gelişim Ve Bu Süreçte Yazının Çeşitli Yüzeylere Uygulanabilirliği. 6. ULUSLARARASI MATBAA TEKNOLOJİLERİ SEMPOZYUMU. İstanbul Üniversitesi - Cerrahpaşa / 01-03 Kasım / November 2018.
GÜREDİN, E.:2014.	"Denetim ve Güvence Hizmetleri." <i>SMM ve YMM'lere Yönelik İlkeler ve Teknikler, Türkmen Kitabevi.</i>
GÜVEN, V., ŞAHİNÖZ, E.:2018	Blokzincir Kripto Paralar Bitcoin. İstanbul, Kasım.

HABER, S., STORNETTA, W.:1991	How to Time-Stamp A Digital Document, Crypto'90, LNCS 537. pp. 437-455. Springer-Verlag Berlin Heidelberg.
HAKAN, 2017:	Blok Zinciri(Blockchain) Teknolojisine Giriş- 2, 27 Eylül 2017, (Çevrimiçi) https://www.getrevue.co/profile/Hakan/issues/blok-zinciri-2-merkezi-olmayan-75090 , 20 Mart 2020.
HEWETT, N., GOGH V.M, PAWCZUK L, Y. :2020)	Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability. World Economic Forum.
HILEMAN, G., RAUCHS M.:2017	Global Cryptocurrency Benchmarking Study. Cambridge Centre for Alternative Finance , 33, 33-113.
HUGHES, E.:1993	A Cypherpunk's Manifesto. URL (accessed 3 August 2004): http://www.activism.net/cypherpunk/manifesto.html , 28 Nisan 2020.
HYPERLEDGER: 2018	An Introduction to Hyperledger. Hyperledger Whitepaper. (Çevrimiçi) https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf , 18 Mayıs 2020.
HYPERLEDGER: 2019	How Walmart brought unprecedented transparency to the food supply chain with Hyperledger fabric. (Çevrimiçi) https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf , 5 Mayıs 2020.
HYPERLEDGER: 2020	(Çevrimiçi) https://www.hyperledger.org/use , 19 Mayıs 2020.
IANSTITI, M., LAKHANI, K.:2017	The truth about blockchain. <i>Harvard Business Review</i> , 95(1), 119-127.

IASA, ERİŞİM TARİHİ: 29 NİSAN 2020.	Magnetic Tape Alert Project (Çevrimiçi) http://www.mtap.iasa-web.org/ , 29 Nisan 2020
IBM: ERİŞİM TARİHİ: 19 NİSAN 2020	The IBM Punch Card, (Çevrimiçi) https://www.ibm.com/ibm/history/ibm100/us/en/icons/punchcard/transform/ , 19 Nisan 2020.
IBM, ERİŞİM TARİHİ: 21 NİSAN 2020	The Floppy Disks, (Çevrimiçi) https://www.ibm.com/ibm/history/ibm100/us/en/icons/floppy/transform/ , 21 Nisan 2020
IBM CLOUD EDUCATION: 2019	Cloud Storage, 24 June, 2019, (Çevrimiçi), https://www.ibm.com/cloud/learn/cloud-storage , 30 Mayıs 2020
IDEOCOLAB, ERİŞİM TARİHİ: 25 MART 2020.	https://www.ideocolab.com/startupstudio/ , 25 Mart 2020.
IJIRI, Y.:1982	Triple-Entry Bookkeeping and Income Momentum. American Accounting Association.
IJIRI, Y.:1986	“A Framework For Triple-Entry Bookkeeping”. Accounting Review , 745-759.
INGHIRAMI, I. E.:2019	AIS In The Time of Blockchain. <i>Living In The Digital Ecosystem: Technologies, Organizations And Human Agency</i> , 122.
IOTA: ERİŞİM TARİHİ: 10 MAYIS 2020.	(Çevrimiçi) https://www.iota.org/get-started/what-is-iota , 10 Mayıs 2020.
İŞBANKASI: 2020	İş Bankası R3 Blockchain Birliği'ne katılan ilk Türk bankası oldu, 29 Nisan 2020, (Çevrimiçi) https://www.isbank.com.tr/bankamizi-taniyin/is-bankasi- r3-blockchain-birligine-katilan-ilk-turk-bankasi-oldu , 13 Mayıs 2020

İTÜBİDB:2013	Şifreleme Yöntemleri, İTÜ Bilgi İşlem Daire Başkanlığı, 7 Eylül 2013, (Çevrimiçi) https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri , 5 Mart 2020.
JOSHI, A. P., HAN, M., WANG, Y.:2018	“A Survey On Security And Privacy Issues Of Blockchain Technology”. Mathematical Foundations Of Computing , 1(2), 121.
KARAHAN, Ç., TÜFEKÇİ, A.:2019	“Blokzincir Teknolojisinin İç Denetim Faaliyetlerine Etkileri: Fırsatlar ve Tehditler”. Denetışim , (19), 55-72.
KARAJOVIC, M., KIM, H. M., LASKOWSKI, M.:2019	“Thinking Outside The Block: Projected Phases of Blockchain Integration in the Accounting Industry”. Australian Accounting Review , 29(2), 319-330.
KELLY, M.:2019	Boards Look to Harness Blockchain Disruption. Tone at the Top. The Institute Of Internal Auditors. Issue 91, February 2019.
KIBET, A., KARUME, S. M., K.:2018	A Synopsis of Blockchain Technology. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) , 7(11), ISSN: 2278 – 1323.
KIRBAŞ, I.:2018	“Blokzinciri Teknolojisi ve Yakın Gelecekteki Uygulama Alanları”. Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi , 9(1), 75-82.
KIYAK, Y. S., COŞKUN, Ö., & BUDAKOĞLU, I. İ.:2019	Blokzinciri, Akıllı Kontratlar ve Sağlık Alanındaki Üç Uygulama Örneği. Hacettepe Sağlık İdaresi Dergisi , 22(2), 457-466.

KLOCH R.C. & SIMON J LITTLE.:2019	Blockchain and Internal Audit. Internal Audit Foundation And Crowe, 2019, ISBN 978-1-63454-065-0.
KODAZ, H., BOTSALI, F. M.:2010	“Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması”. Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu, Teknik - Online Dergi , 9(1), 10-23.
KOENS, T., POLL, E.:2019	Assessing interoperability solutions for distributed ledgers. <i>Pervasive and Mobile Computing</i> , 59, 101079.
KPMG: 2019A	KPMG Forms Strategic Alliance with Guardtime, February 20, 2019, (Çevrimiçi) https://home.kpmg/us/en/home/media/press-releases/2019/02/kpmg-forms-strategic-alliance-with-guardtime.html , 25 Mart 2020
KPMG: 2019B	KPMG, IBM, Merck and Walmart Are Piloting Blockchain for Medicine Distribution, June 13, 2019, (Çevrimiçi) https://home.kpmg/us/en/home/media/press-releases/2019/06/kpmg-ibm-merck-and-walmart-are-testing-blockchain-for-medicine-distribution.html , 25 Mart 2020
KUHN, B. D.:2018	The Impact of Blockchain Technology on Business, Financial Auditors and Accounting Professionals. Honor Thesis. <i>NORTHERN ILLINOIS UNIVERSITY</i> .
KUMARI, S.:2013	Recurrent Sequences and Cryptography (Doctoral Dissertation, National Institute of Technology Rourkela, India).
KÜÇÜK, E.: 2017	"Sanal paraların en hızlısı ‘Ethereum’", 14 Haziran 2017, (Çevrimiçi) https://www.dunya.com/finans/haberler/sanal-paralarin-en-hizlisi-ethereum-haberi-367684 , 19 Mayıs 2020.

LEDGERIUM: 2019	Ledgerium Whitepaper. (Çevrimiçi) https://whitepaper.ledgerium.io/untitled/history-and-vision , 23 Haziran 2020.
LEMIEUX, V. L.:2017	Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective. European Property Law Journal , 6(3), 392-440.
LEUNG, A.:2016	Deloitte Sets Good Example, Installs Bitcoin ATM in Toronto Office, September 20, 2016(Çevrimiçi) https://cointelegraph.com/news/deloitte-sets-good-example-installs-bitcoin-atm-in-toronto-office , 25 Mart 2020.
LI, K.:2019	The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed, 30 June, 2019, (Çevrimiçi) https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44 , 9 Mayıs 2020.
LIFFREING, I.:2018	PwC launches 2-year digital skills course to train 1,000 employees on everything from drones to blockchain, August 30, 2018, (Çevrimiçi) https://digiday.com/marketing/pwc-launches-two-year-digital-skills-course-train-1000-employees-everything-drones-blockchain/ , 25 Mart 2020.
LIN, I. C., LIAO, T. C.:2017	“A Survey Of Blockchain Security Issues and Challenges””. IJ Network Security , 19(5), 653-659.
LTO: 2019.	Permissionless Private Blockchain, December 23, 2019, (Çevrimiçi) https://blog.ltonetwork.com/permissionless-private-blockchains-lto-network/ , 11 Nisan 2020.
LUCAPLUS: 2019A	Luca+. About Us. (Çevrimiçi) https://www.lucaplus.com/about/ , 23 Haziran 2020.
LUCAPLUS: 2019B	HOW LUCA+ WORKS. (Çevrimiçi) https://www.lucaplus.com/#whyus , 23 Haziran 2020.

MAGUIRE E., NAGARAJ K, VIRESD., WYNER S.:2018	Realizing Blockchain's Potential. Introducing Kpmg Blockchain Technology Risk Assessment Solution. KPMG International Cooperative.
MAIWALD, E.:2003	Network Security: A Beginner's Guide.2
MARCO POLO: 2020	First Turkish-German trade finance transaction on Marco Polo blockchain network with İşbank and Commerzbank, June 3, 2020, (Çevrimiçi) https://www.marcopolo.finance/first-turkish-german-trade-finance-transaction-on-marco-polo-blockchain-network-with-isbank-and-commerzbank/ , 15 Haziran 2020.
MARSHALL, A.:2018	Controversial Blockchain Project Tezos to Be Audited by 'Big Four' PwC., Jul 24, 2018, (Çevrimiçi) https://cointelegraph.com/news/controversial-blockchain-project-tezos-to-be-audited-by-big-four-pwc , 25 Mart 2020.
MARTIN, R.:2018	5 blockchain security risks and how to reduce them.Ignite Outsourcing, November 29, 2018, (Çevrimiçi) https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/ , 22 Haziran 2020
MAZAREANU E.: 2019	Revenue of the Big Four accounting / audit firms worldwide in 2019, by function, Dec 12, 2019, (Çevrimiçi) https://www.statista.com/statistics/250935/big-four-accounting-firms-breakdown-of-revenues/ , 17 Mayıs 2020.
MEDICALCHAIN:2018A	Medicalchain announces a partnership with The Groves Medical Group, London, March 6, 2018, (Çevrimiçi) https://medium.com/medicalchain/medicalchain-announces-a-partnership-with-the-groves-medicalgroup-london-98c30372998b , 25 Nisan 2020

MEDICALCHAIN:2018B	Medicalchain Whitepaper 2.1., (Çevrimiçi) https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf , 25 Nisan 2020.
MELSE, E.:2008	“Accounting in Three Dimensions: A Case for Momentum Revisited”. The Journal Of Risk Finance . 9(4), 334-350.
MENDELSON, M.:2019	From Initial Coin Offerings to Security Tokens: A US Federal Securities Law Analysis. <i>Stan. Tech. L. Rev.</i> , 22, 52.
MGSCODE: 2016	Şifreleme Yöntemleri, 18 Haziran, 2016, (Çevrimiçi) https://mgscod.blogspot.com/2016/06/sifreleme-yontemleri.html , 3 Ocak 2020.
MGSCODE: 2016	Şifreleme Yöntemleri, 18 Haziran, 2016, (Çevrimiçi) https://mgscod.blogspot.com/2016/06/sifreleme-yontemleri.html , 3 Ocak 2020.
MILLER, D., MOCKEL, P., MYERS, G. I., NIFOROS, M., RAMACHANDRAN, V., REHERMANN, T., SALMON, J.:2019	<i>Blockchain: Opportunities for Private Enterprises in Emerging Markets</i> . No. 134063, pp. 1-88. The World Bank.
MOISE I., CHOPPING, D.:2018	Maersk and IBM Partner on Blockchain for Global Trade, Jan 16, 2018, (Çevrimiçi) https://www.wsj.com/articles/maersk-and-ibm-partner-on-blockchain-for-global-trade-1516111543 , 25 Mayıs 2020.
MONRAT, A. A., SCHELÉN, O.,	A Survey of Blockchain from The Perspectives of Applications, Challenges, and Opportunities. <i>IEEE Access</i> , 7, 117134-117151

ANDERSSON, K.:2019	
MONZON, L.:2020	How Blockchain Can Change the Audit Profession, May 1, 2020, (Çevrimiçi) https://www.itnewsafrika.com/2020/05/how-blockchain-will-disrupt-the-audit-profession/ , 25 Mayıs 2020
NAKAMOTO, S.:2008	A Peer-to-Peer Electronic Cash System., 2008, (çevrimiçi) http:// bitcoin.org/bitcoin.pdf , 12 Ağustos 2019,.
NARULA, N., VASQUEZ, W., VIRZA, M.:2018	Zkledger: Privacy-Preserving Auditing For Distributed Ledgers. In <i>15th {USENIX} Symposium On Networked Systems Design And Implementation ({NSDI} 18)</i> (Pp. 65-80).
NARULA, N., VASQUEZ, W., VIRZA, M.:2018	zkLedger Privacy-preserving auditing for distributed ledgers, (Çevrimiçi) https://www.usenix.org/sites/default/files/conference/protected-files/nsdi18_slides_narula.pdf , 3 Nisan 2020.
NATARAJAN, H., KRAUSE, S., GRADSTEIN, H.:2017	Distributed Ledger Technology (DLT) and Blockchain. FinTech Note; No. 1. Washington, DC: World Bank Group.
NIFOROS, M.:2017	Blockchain in Financial Services in Emerging Markets Part One: Current Trends (No. 120261, pp. 1-8). The World Bank
NONNENMACHE, T.:2001	History of the US Telegraph Industry. EH. Net Encyclopedia, edited by Robert Whaples, 2001, (Çevrimiçi) https://eh.net/encyclopedia/history-of-the-u-s-telegraph-industry/ , 19 Nisan 2020
O'DWYER, K.J., MALONE, D.:2014	Bitcoin Mining and Its Energy Footprint. In: Proceedings Of The 2014 IET Irish Signals & Systems Conference

OĞUZ, H.:2013	ELEKTRONİK ORTAMDA KİŞİSEL VERİLERİN KORUNMASI, BAZI ÜLKE UYGULAMALARI VE ÜLKEMİZDEKİ DURUM. Uyuşmazlık Mahkemesi Dergisi , (3), 1-38.
ORTMAN, C.:2018	Blockchain and the Future of the Audit. <i>MC Senior Theses</i> . 1983. http://scholarship.claremont.edu/cmc_theses/1983
ORTOLANI, P.:2019	“The Impact of Blockchain Technologies and Smart Contracts on Dispute Resolution: Arbitration And Court Litigation At The Crossroads”. Uniform Law Review , 24(2), 430-448.
ÖZGÜR, D.: 2019	Akıllı Sözleşme 2.0 = Ricardian, 17 Temmuz, 2019, (Çevrimiçi) https://bctr.org/akilli-sozlesme-2-0-ricardian-9754/ , 15 Nisan 2020
PANETTA K.:2018	5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018, August 16, 2018, (Çevrimiçi) https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/ , 21 Mayıs 2020.
PARTZ, H.:2020.	It Happened: Bitcoin Just Experienced Third Halving in Its History, May 11 2020, (Çevrimiçi) https://cointelegraph.com/news/it-happened-bitcoin-just-experienced-third-halving-in-its-history?_ga=2.32897341.2012875521.1599681205-1557701812.1580649889 , 19 Mayıs 2020.
PAWCZUK, L., MASSEY, R. HOLDOWSKY, J.:2019	Deloitte's 2019 Global Blockchain Survey: Blockchain gets down to business'. <i>Deloitte Insights</i> .
PONGNUMKUL, S., SIRIPANPORNCHA	Performance Analysis of Private Blockchain Platforms in Varying Workloads. In 2017 26th International

NA, C., THAJCHAYAPONG, S.:2017	Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE.
POTEKHINA, A., RIUMKIN, I.:2017	Blockchain–A New Accounting Paradigm: Implications For Credit Risk Management. Master Degree Thesis. (Çevrimiçi), https://www.diva-portal.org/smash/get/diva2:1114333/FULLTEXT01.pdf , 6 Mayıs 2020.
PREWETT, K. W., PRESCOTT, G. L., PHILLIPS, K.: 2020	“Blockchain Adoption is İnevitabl—Barriers And Risks Remain”. Journal Of Corporate Accounting & Finance , 31(2), 21-28.
PROTIVITI:2019	Executive Perspectives on Top Risks 2019, (Çevrimiçi) https://www.protiviti.com/sites/default/files/united_states/insights/nc-state-protiviti-survey-top-risks-2019-executive-summary.pdf , 13 Mayıs 2020.
PSAILA, S.:2017	Blockchain: A Game Changer for Audit Processes. <i>Deloitte Malta</i>
PUTHAL, D., MALIK, N., MOHANTY, S. P., KOUIGIANOS, E., DAS, G.:2018	Everything You Wanted to Know about The Blockchain: Its Promise, Components, Processes, and Problems. IEEE Consumer Electronics Magazine , 7(4), 6-14.
PWC: 2018	Pwc’s Global Blockchain Survey 2018. Hong Kong: Pricewaterhousecoopers (Pwc) Ltd.
PWC: 2019	PwC launches solution supporting audit of cryptocurrency, 2019, (Çevrimiçi) https://www.pwc.com/gx/en/news-room/press-releases/2019/cryptocurrenc-audit.html , 25 Mart 2020.

PWC, ERİŞİM TARİHİ: 10 MAYIS 2020.	https://www.pwc.com/us/en/industries/financial-services/research-institute/blog/blockchain-audit-a-michael-smith.html , 10 Mayıs 2020
QIU, T., ZHANG, R., GAO, Y.:2019	Ripple Vs. SWIFT: Transforming Cross Border Remittance Using Blockchain Technology”. Procedia Computer Science , 147, 428-434.
RAUCHS, M., BLANDIN, A., KLEIN, K., PIETERS, G. C., RECANATINI, M., ZHANG, B. Z.:2018	2nd Global Cryptoasset Benchmarking Study. Available At Ssrn 3306125.
RAUCHS, M., GLIDDEN, A., GORDON, B., PIETERS, G. C., RECANATINI, M., ROSTAND, F., VAGNEUR K., ZHANG, B. Z.:2018	Distributed Ledger Technology Systems: A Conceptual Framework. Available at SSRN 3230013.
RIPPLE, ERİŞİM TARİHİ: 12 MAYIS 2020.	Solution Overwiev, (Çevrimiçi), https://ripple.com/files/ripple_solutions_guide.pdf , 12 Mayıs 2020.
RIPPLE, ERİŞİM TARİHİ: 13 MAYIS 2020.	ReiseBank integrates Ripple to make payments faster and cost-effective, (Çevrimiçi) https://ripple.com/files/case_study_reisebank.pdf , 13 Mayıs 2020.
RIPPLE: 2017	Ten New Customers Join Ripple’s Global Payment Network, April 26, 2017, (Çevrimiçi)

	https://ripple.com/insights/ten-new-customers-join-ripples-global-payment-network/ , 13 Mayıs 2020
RIPPLE: 2019	RippleNet Reaches Milestone, Surpasses 200 Customers, January 9, 2019, (Çevrimiçi) https://ripple.com/ripple_press/rippletnet-reaches-milestone-surpasses-200-customers/ , 13 Mayıs 2020
ROONEY, H., AIKEN, B., ROONEY, M.:2017	“Q. Is Internal Audit Ready For Blockchain?”. Technology Innovation Management Review , 7(10), 41-44.
ROZARIO, A. M., THOMAS, C.:2019	“Reengineering The Audit with Blockchain and Smart Contracts”. Journal Of Emerging Technologies In Accounting , 16(1), 21-35.
ROZARIO, A. M., VASARHELYI, M. A.:2018	“Auditing With Smart Contracts”. International Journal of Digital Accounting Research , 18.
RÜCKESHÄUSER, N.:2017	Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls. In: 13th International Conference On Wirtschaftsinformatik, St. Gallen. AIS, Pp 16–30
SAKİN, T.:2016	Kâr Yönetimi ve Türkiye’deki Kâr Yönetimi Çalışmalarının Değerlendirilmesi. İÜ İşletme Fakültesi Muhasebe Enstitüsü, İstanbul, 181-192.
SANGSTER, A.:2016	The Genesis Of Double Entry Bookkeeping. The Accounting Review , 91(1), 299-315.
SANTHANA, P., BISWAS, A.:2017	Blockchain Risk Management–Risk Functions Need to Play an Active Role in Shaping Blockchain Strategy. Deloitte Development LLC.

SCHMITZ, J., LEONI, G.:2019	“Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda”. Australian Accounting Review , 29(2), 331-342.
SCHNEIER, B., KELSEY, J.:1999	Secure Audit Logs to Support Computer Forensics. <i>ACM Transactions on Information and System Security (TISSEC)</i> , 2(2), 159-176.
SCHOLLMEIER, R.:2001	A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In <i>Proceedings First International Conference on Peer-to-Peer Computing</i> (pp. 101-102). IEEE.
SCHULMAN, J., WILSON S.:2019	How blockchain technology will affect the audit, November 13, 2019, (Çevrimiçi) https://rsmus.com/what-we-do/services/assurance/how-blockchain-technology-will-affect-the-audit.html , 28 Mayıs 2020.
SCHUMANN, T.: 2018	Consensus Mechanisms Explained: PoW vs. PoS, April 5, 2018, (Çevrimiçi) https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10 , 5 Nisan 2020
SCHWARTZ, D.: 2020	What do the letters 'XRP' stand for, or why does Ripple Labs call it 'XRP'?, January 23, 2020, (Çevrimiçi) https://www.quora.com/What-do-the-letters-XRP-stand-for-or-why-does-Ripple-Labs-call-it-XRP , 20 Haziran 2020
SENGEL, B.:2020	“Bitcoin’in Temelleri”, 14 Ocak 2020, (Çevrimiçi), https://bctr.org/bitcoinin-temelleri-13374/ , 13 Nisan 2020
SERT, T.:2019	Sorularla Blockchain, (Çevrimiçi) https://bkm.com.tr/wp-content/uploads/2015/06/Sorularlablockchain.pdf , 10 Mayıs 2020.

SHELDON, M. D.:2019	“A Primer for Information Technology General Control Considerations on A Private and Permissioned Blockchain Audit”. Current Issues In Auditing , 13(1), A15-A29.
SIMOYAMA, F. D. O., GRIGG, I., BUENO, R. L. P., OLIVEIRA, L. C. D.:2017	“Triple Entry Ledgers With Blockchain For Auditing”. International Journal of Auditing Technology , 3(3), 163-183.
STAMFORD, C.:2019A	Gartner Predicts 90% of Current Enterprise Blockchain Platform Implementations Will Require Replacement by 2021, June 3, 2019, (Çevrimiçi) https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain , 20 Mayıs 2020.
STAMFORD, C.:2019B	Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact, October 8, 2019, (Çevrimiçi) https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-fromtransformational-impact , 21 Mayıs 2020.
SUBERG, W.:2017	US-Based Startup Ubitquity Brings Blockchain To Brazil’s Real Estate, April 6, 2017, (Çevrimiçi) https://cointelegraph.com/news/us-based-startup-ubitquity-brings-blockchain-to-brazils-real-estate , 7 Mayıs 2020
SWAN, M.:2015	Blockchain: Blueprint For A New Economy. " O'Reilly Media, Inc."
SZABO, N.:1994	Smart contracts. <i>Unpublished Manuscript</i> .

SZABO, N.:1997	The Idea of Smart Contracts. <i>Nick Szabo's Papers and Concise Tutorials</i> , 6.
SZABO, N.:2005	Bit Gold, (Çevrimiçi) http://unenumerated.blogspot.de/2005/12/bit-gold.html , 20 Mart 2020
TAPSCOTT, A., TAPSCOTT, D.:2017A	How blockchain is changing finance. Harvard Business Review , 1(9), 2-5.
TAPSCOTT, D., TAPSCOTT, A.:2017B	How blockchain will change organizations. MIT Sloan Management Review , 58(2), 10-13.
TAŞ, O., KİANİ, F.:2018	Blok zinciri teknolojisine yapılan saldırılar üzerine bir inceleme. Bilişim Teknolojileri Dergisi , 11(4), 369-382.
TAŞYÜREK, G.:2020	Enigma Nedir?, 16 Ocak, 2020, (Çevrimiçi) https://www.iienstitu.com/blog/enigma-nedir , 19 Nisan 2020
TRIKHA, B.:2010	“A Journey from Floppy Disk to Cloud Storage”. International Journal on Computer Science and Engineering , 2(4), 1449-1452.
TÜBİTAK BİLGEM BLOK ZİNCİR ARAŞTIRMA LABORATUVARI:2 018	Blokszincir, (Çevrimiçi) https://blokszincir.bilgem.tubitak.gov.tr/bz-calistay/blokszincir.html , 25 Mayıs 2020
TYSIAC, K.:2017	Blockchain: An opportunity for accountants? Or a threat. <i>Journal of Accountancy</i> . (Çevrimiçi), 18 Mayıs 2020
UNDERWOOD, S.: 2016	Blockchain beyond bitcoin. Communications of the ACM . 59(11), 15-17.
US CENSUS BUREAU: ERİŞİM TARİHİ: 30 NİSAN 2020	The Hollerith Machine, (Çevrimiçi) https://www.census.gov/history/www/innovations/technology/the_hollerith_tabulator.html , 30 Nisan 2020

USTA, A., DOĞANTEKİN, S.:2017	Blockchain 101. İstanbul: Kapital Medya Hizmetleri A.Ş
USTA, A., DOĞANTEKİN, S.:2018	Blockchain 101 v2. <i>Bankalararası Kart Merkezi.</i>
UYSAL, T.U., KURT G.:2018	“Muhasebede ve Denetimde Blok Zinciri Teknolojisi”. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi , 23(2), 467-481.
VAIDYANATHAN, N.:2017	Divided We Fall, Distributed We Stand. <i>The Professional Accountant's Guide to Distributed Ledgers and Blockchain.</i> London, UK: Association of Chartered Certified Accountants.
VASTERS, C. F.:2001	<i>Biztalk Server 2000: A Beginner's Guide.</i> McGraw-Hill Osborne Media
VBAP, ERİŞİM TARİHİ: 30 NİSAN 2020	EDI-Elektronik Veri Değişimi (Electronic Data Interchange), (Çevrimiçi) https://www.vbap.com.tr/blog/edi-elektronik-veri-degisimielektronic-data-interchange/ , 30 Nisan 2020
VEUGER, J.:2018	Trust in a viable real estate economy with disruption and blockchain. Facilities .36(1/2), pp. 103-120 © Emerald Publishing Limited.
VISA, ERİŞİM TARİHİ: 9 MAYIS 2020	Visa acceptance for retailers, (Çevrimiçi) https://usa.visa.com/run-your-business/small-business-tools/retail.html , 9 Mayıs 2020.
VİKİPEDİ: 2020A	Veri kayıt ortamı, 12 Mart 2020, (Çevrimiçi) https://tr.wikipedia.org/wiki/Veri_kay%C4%B1t_ortam%C4%B1 , 20 Nisan 2020

VİKİPEDİ: 2020B	Sezar şifrelemesi, 5 Şubat 2020, (Çevrimiçi) https://tr.wikipedia.org/wiki/Sezar_%C5%9Fifrelemesi , 19 Nisan 2020.
VİKİPEDİ: 2020C	Telex, (Çevrimiçi) https://en.wikipedia.org/wiki/Telex , 30 Nisan 2020.
WANG, Y., KOGAN, A.:2018	“Designing Confidentiality-Preserving Blockchain-Based Transaction Processing Systems”. International Journal of Accounting Information Systems , 30, 1-18.
WHITE, B. S., KING, C. G., HOLLADAY, J.:2020	“Blockchain Security Risk Assessment and The Auditor”. Journal Of Corporate Accounting & Finance , 31(2), 47-53.
WIATT, R.G.:2019	From the mainframe to the blockchain. <i>Strategic Finance</i> , 100(7), 26-35.
WIKİTARİH, ERİŞİM TARİHİ: 30 NİSAN 2020.	Matbaanın İcadı, (Çevrimiçi) https://www.wikitarih.com/matbaanın-icadi/#:~:text=Johannes%20Gutenberg%20ve%20Modern%20Matbaan%C4%B1n%20%C4%B0cad%C4%B1&text=Gutenberg'in%20icat%20etti%C4%9Fi%20matbaa,da%20Gutenberg%20%C3%B6nemli%20yenilikler%20getirmi%C5%9Ftir. , 30 Nisan 2020
WILD, J., ARNOLD, M., STAFFORD, P.: 2015	Technology: Banks Seek the Key to Blockchain-FT. com., November 1, 2015, <i>Financial Times</i> . Np, 1. (Çevrimiçi) https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64 , 11 Mayıs 2020.
WSBA:2017	Wall Street Blockchain Alliance Adds KPMG as Corporate Member., November 15, 2017, (Çevrimiçi) file:///D:/Drive/Cryptocurrency%20&%20Blockchain%20Infographics/Big4%20Raporlar/wsba%202017.pdf , 25 Mart 2020.

WUNSCHE, A.:2016	Technological Disruption Of Capital Markets And Reporting? An Introduction to Blockchain'. <i>Chartered Professional Accountants Canada (CPA)</i> .
XU, J. J.:2016	Are blockchains immune to all malicious attacks?. <i>Financial Innovation</i> , 2(1), 1-9.
YERMACK, D.:2017	"Corporate Governance and Blockchains". Review of Finance , 21(1), 7-31.
YILDIRIM, H.:2019	"Blokzincir mi, blok zincir mi, blok zinciri mi?", 14 Şubat 2019, (Çevrimiçi) https://medium.com/@hakany/blokzincir-mi-blok-zincir-mi-blok-zinciri-mi- , 7 Mayıs 2020
YILMAZ, M., BALLI, S.:2016	"Veri Şifreleme Algoritmalarının Kullanımı İçin Akıllı Bir Seçim Sistemi Geliştirilmesi". Uluslararası Bilgi Güvenliği Mühendisliği Dergisi , 2(2), 18-28.
YOUNG, J.:2019.	"New Report Shows China Dominates Bitcoin Mining, Is This a Sign of Worry?", December 12, 2019, (Çevrimiçi) https://www.forbes.com/sites/youngjoseph/2019/12/12/new-report-shows-china-dominates-bitcoin-mining-is-this-a-sign-of-worry/#40ca60e442e1 , 2 Temmuz 2020.
YU, T., LIN, Z., TANG, Q.:2018	"Blockchain: The Introduction and its Application in Financial Accounting". Journal of Corporate Accounting & Finance , 29(4), 37-47.
ZHENG, Z., XIE, S., DAI, H., CHEN, X., WANG, H.:2017	An Overview of Blockchain Technology: Architecture, Consensus, And Future Trends. In <i>2017 IEEE International Congress On Big Data (Bigdata Congress)</i> (Pp. 557-564). IEEE.
ZHENG, Z., XIE, S., DAI, H. N., CHEN, X., WANG, H.:2018	"Blockchain Challenges and Opportunities: A Survey". International Journal of Web and Grid Services , 14(4), 352-375.

ZHU, H., LI, D.:2008	Research on Digital Signature in Electronic Commerce. <i>In proceedings of the International MultiConference of Engineers and Computer Scientists</i> (Vol. 1).
ZIMAKOSOV, V.:2018	Usage of IBM Blockchain Technology to Improve Clearing and Settlement Processes in the Banking Sector.
ZMUDZINSKI, A.:2019	Big Four Auditing Firm Deloitte Lets Staff Pay for Lunch in Bitcoin, September 17, 2019, (Çevrimiçi) https://tr.cointelegraph.com/news/big-four-auditing-firm-deloitte-allows-staff-to-pay-lunch-in-bitcoin , 25 Mart 2020.