



**T.C.
ERCIYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI**

**KRİPTO PARA: MUHASEBELEŞTİRİLMESİ VE
KRİPTO PARA DOLANDIRICILIĞININ
TESPİTİNDE ADLİ MUHASEBENİN ROLÜ**

**Hazırlayan
Al-Fahad Tareq Atiyah AL-DULAIMI**

**Danışman
Prof. Dr. Azzem ÖZKAN**

Yüksek Lisans Tezi

Haziran 2021, KAYSERİ

**T.C.
ERCIYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI**

**KRİPTO PARA: MUHASEBELEŞTİRİLMESİ VE KRİPTO
PARA DOLANDIRICILIĞININ TESPİTİNDE ADLİ
MUHASEBENİN ROLÜ
(Yüksek Lisans Tezi)**

**Hazırlayan
Al-Fahad Tareq Atiyah AL-DULAIMI**

**Danışman
Prof. Dr. Azzem ÖZKAN**

Haziran 2021, KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Al-Fahad Tareq Atiyah Al-Dulaimi

İmza:



T.C.

ERCIYES ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Anabilim Dalı : İşletme

Program Adı : Yüksek Lisans

Tez Başlığı : Kripto Para: Muhasebeleştirilmesi Ve Kripto Para Dolandırıcılığının
Tespitinde Adli Muhasebenin Rolü

Yukarıda bilgileri verilen tez çalışmasının a) Giriş, b) Ana bölümler ve c) Sonuç kısımlarından oluşan (Kapak, Önsöz, Özet, İçindekiler ve Kaynakça hariç) toplam 120 sayfalık kısmına ilişkin 12/07/2021 tarihinde **Turnitin** intihal programından aşağıda belirtilen filtreleme uygulanarak alınmış olan özgünlük raporuna göre tezin benzerlik oranı: **%3**'dür.

Filtrelemeye **alıntılar dahil** edilmiştir. Filtrelemede **yedi (7) kelimedenden daha az** örtüşme içeren metin kısımları hariç tutulmuştur.

Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Tez İntihal Raporu Uygulama Esaslarını inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına göre tez çalışmasının herhangi bir intihal içermediğini, aksinin tespit edilmesi durumunda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim. 12/07/2021

Danışman: Prof. Dr. Azzem ÖZKAN Öğrenci: Al-Fahad Tareq Atiyah AL-DULAIMI

İmza

İmza

KILAVUZA UYGUNLUK

“Kripto Para: Muhasebeleştirilmesi Ve Kripto Para Dolandırıcılığının Tespitinde Adli Muhasebenin Rolü” başlıklı Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Lisansüstü Tez Yazım Kılavuzuna uygun olarak hazırlanmıştır.

Hazırlayan

Al-Fahad Tareq Atiyah AL-DULAIMI

Danışman

Prof. Dr. Azzem ÖZKAN

İşletme ABD Başkanı

Prof. Dr. Faik BİLGİLİ

ÖN SÖZ

Tez konusunun belirlenmesinden tezin son aşamasına gelene kadar bana yol gösteren, yoğun iş temposu arasında, çok değerli vakitlerini ayırarak bana destek ve yardımlarını esirgemeyen ve tecrübeleriyle bana ışık tutan, tez danışmanı saygıdeğer hocam Prof. Dr. Azzem ÖZKAN'a teşekkür ederim. Türkiye'ye, Devletine, Halkına ve Toprak'ına minnettarım.

Hayatım boyunca yanımda olan ve emeklerin en büyüğüne sahip olan anneme ve babama, akademik hayatıma adım attığım ilk günden bu yana her koşulda bana inanan ve her daim yanımda olan sevgili eşime ve kızıma yürekten teşekkür ederim.

Al-Fahad Tareq Atiyah AL-DULAIMI

Kayseri, 2021

KRİPTO PARA: MUHASEBELEŞTİRİLMESİ VE KRİPTO PARA DOLANDIRICILIĞININ TESPİTİNDE ADLİ MUHASEBENİN ROLÜ

Al fahad Tareq Atiyah ALDULAIMI

**Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü,
Yüksek Lisans Tezi, Haziran 2021
Danışman: Prof. Dr. Azzem ÖZKAN**

ÖZET

Kripto paralar ve Blockchain teknolojisi, finans sektöründe, muhasebe kurallarının ve standardizasyonlarının ciddi bir dönüşümüne yol açan büyük bir etkiye sahiptir. Dijital para ticaretinde oldukça büyük ölçekli bir pazar ortaya çıkarmıştır. Öte yandan, bu alandaki kanunların henüz yetersiz olmasından dolayı, bu teknolojiler, dolandırıcılar ve kötü niyetliler tarafından büyük bir fırsat olarak değerlendirilmektedir. Denetim sistemleri ve güvence hizmetleri ne kadar düzenli bir şekilde sağlanırsa sağlansın, bu dolandırıcılık vakalarına karşı istenen etki gösterilememektedir. Worldcom skandalından sonra, adli muhasebe ortaya çıkmıştır.

Bu çalışmada, adli muhasebenin işlevleri ve yöntemleri açıklanmakta adli muhasebenin gelişim serüveninin kısa bir tarihçesine yer verilmektedir. Ayrıca, Blockchain teknolojisinin ne olduğu ve nasıl çalıştığı üzerinde durulmakta, kripto para birimleri ve kripto varlık muhasebesi açıklanmaktadır. Çalışmamızda, kripto varlık dolandırıcılığı ile mücadelede etkili olabilecek adli muhasebe tekniklerinin ve araçlarının işlevselliği açıklanmaktadır. Sonuç olarak, adli muhasebe tekniklerinin kripto varlık işlemlerinde ve bu işlemlerin kamuoyu nezdindeki etkileşimlerinde tespit edilen bulgular içerisinde en önemli ve dikkate değer noktalardan bahsedilmektedir.

Anahtar Kelimeler: Adli Muhasebe, Blockchain, Kripto Para/varlıklar, Dolandırıcılık, Muhasebe

ACCOUNTING FOR CRYPTOCURRENCY AND THE ROLE OF FORENSIC ACCOUNTING IN CRYPTOCURRENCY FRAUD DETECTION

Al fahad Tareq Atiyah ALDULAIMI

Erciyes University, Graduate School of Social Sciences

M.Sc. Thesis, June 2021

Supervisor: Prof. Dr. Azzem ÖZKAN

ABSTRACT

The Cryptocurrencies and Blockchain technology have a big effect to the financial sector leading a real transformation in accounting rules and standardizations and also it opened a huge market for digital money trading. On the other hand, it seems to be a good chance for the fraudsters and scammers to hit on taking advantage of gaps in the laws. A regular audit and assurance service would not be effective with these high intelligent fraud cases and after Worldcom scam a high level type of investigatory accounting and auditing methods has been more known than before named Forensic accounting and it starts to get a wide range role now.

This work, tried to explore the Forensic accounting functions and methods and provided a brief history of its beginning and development journey. Then discussed what is the Blockchain and simply explained how it works, the uses of it and especially the Cryptocurrency with focusing on Cryptoassets accounting. Explaining the ability of Forensic accounting techniques and tools that could be well affective in fighting the Cryptoassets fraud. Overall in conclusion has been mentioned the most important and valued points within the findings of the interact of Forensic accounting and its techniques in Cryptoassets operations and to the publics.

Key Words: Forensic accounting, Blockchain, Crypto-currency/asset, Fraud, Accounting

İÇİNDEKİLER

KRİPTO PARA: MUHASEBELEŞTİRİLMESİ VE KRİPTO PARA DOLANDIRICILIĞININ TESPİTİNDE ADLİ MUHASEBENİN ROLÜ

BİLİMSEL ETİĞE UYGUNLUK	i
TEZ ÖZGÜNLÜK ONAYI	ii
KILAVUZA UYGUNLUK	iii
KABUL VE ONAY TUTANAĞI	iv
ÖNSÖZ	v
ÖZET	vi
ABSTRACT	vii
İÇİNDEKİLER	viii
SİMGELER VE KISALTMALAR LİSTESİ	xii
TABLolar LİSTESİ	xiv
ŞEKİLLER LİSTESİ	xv
GİRİŞ	1

BİRİNCİ BÖLÜM

ADLİ MUHASEBE

1.1. Adli Muhasebeye Genel Bakış	4
1.1.1. Adli Muhasebenin İlk Düşümü	5
1.1.2. Adli Muhasebenin Tanımı	6
1.2. Adli Muhasebecilerin Rolü	7
1.2.1. Adli Muhasebeciler İçin Gerekli Olan Yetkinlikler	10
1.3. Dolandırıcılık Risk Yönetimi	15
1.3.1. Dolandırıcılık Türleri	15
1.3.2. Hile Üçgeni	16
1.3.3. Dolandırıcılık Riskinin Değerlendirilmesi	18
1.3.4. Dolandırıcılık Faaliyetlerinin ve Yolsuzlukların Tespiti ve Önlenmesine Yönelik Adli Muhasebe Soruşturma Teknikleri	20
1.4. Bağımsız Denetçi Ve Adli Muhasebeci Arasındaki Farklar	25

1.5. Adli Muhasebecilerin Rolü	27
--------------------------------------	----

İKİNCİ BÖLÜM

BLOCKCHAIN VE KRİPTO PARA

2.1. Blockchain Tanımı	34
2.2. Blockchain Kullanım Alanları	36
2.2.1. Bitcoin ve Blockchain	36
2.2.2. Akıllı Sözleşmeler ve Blockchain	39
2.2.3. Finans Sektöründe Blockchain Kullanımı	40
2.2.4. Gayrimenkul Sektöründe Blockchain Kullanımı	41
2.3. Blockchain'in Muhasebe Sistemleri Üzerindeki Etkisi	41
2.3.1. Blockchain Çağında Muhasebe	41
2.3.2. Blockchain Çağında Denetim	45
2.4. Blockchain'in Avantajları ve Dezavantajları	47
2.4.1. Blockchain Avantajları	47
2.4.1.1. Dağımlılık (Dağıtım)	47
2.4.1.2. Kararlılık (İstikrar)	48
2.4.1.3. Güven Gerektirmeyen Sistem	48
2.4.2. Blockchain Dezavantajları	48
2.4.2.1. %51 Saldırıları	48
2.4.2.2. Veri Modifikasyonu	49
2.4.2.3. Özel Anahtarlar	49
2.4.2.4. Yetersizlik (Verimsizlik)	50
2.4.2.5. Depolama (Saklama)	50
2.5. Kripto Para Türleri ve Yasallığı	50
2.5.1. Kripto Para	50
2.5.2. Dijital Para Biriminin Niteliği ve Türleri	52
2.5.3. Kripto Para Türleri	55
2.6. Kripto Paranın Muhasebeleştirilmesi	56
2.6.1. Muhasebe ve UFRS Açısından Kripto Para	57
2.6.2. Nakit ve Nakit Benzerleri / Eşdeğerleri	59
2.6.2.1. Nakit	59

2.6.2.2. Nakde Eşdeğer Varlıklar	61
2.6.3. Finansal Araç	61
2.6.3.1. Sözleşmeden Haklar	62
2.6.3.2. Öz Kaynağa Dayalı Finansal Araçlar	64
2.6.3.3. Sözleşmeden Doğan Nakit veya Başka Bir Finansal Varlık Hakkı.....	64
2.6.3.4. Türev Araçlar.....	65
2.6.4. Stoklar.....	67
2.6.4.1. Maliyet veya Net Gerçekleşebilir Değerden Düşük Olanıyla Değerleme	68
2.6.4.2. Satış Maliyetleri Düşülmüş Gerçeğe Uygun Değer.....	68
2.6.5. Avanslar (Ön Ödeme).....	69
2.6.6. Maddi Olmayan Duran Varlıklar.....	70
2.6.6.1. UMS 38'in Kapsamı	70
2.6.6.2. Maddi Olmayan Duran Varlığın Tanımı	70
2.6.6.3. Muhasebeleştirme Gereksinimleri	71
2.6.6.4. İlk Muhasebeleştirme (İlk Ölçüm).....	72
2.6.6.5. Sonraki Ölçüm (Dönemsonu Değerleme)	72
2.6.6.5.1. Maliyet Yöntemi	72
2.6.6.5.2. Yeniden Değerleme Yöntemi	73
2.7. Kripto Paranın Muhasebeleştirilmesinde Yönelik IASB Kararı	74

ÜÇÜNCÜ BÖLÜM

KRİPTO PARA DOLANDIRICILIĞI ve ADLİ MUHASEBE ÇÖZÜMLERİ

3.1. Şirketlerde ve İşletmelerde Kripto Para Riskleri.....	78
3.2. Kripto Para: Risk Yönetimine Genel Bakış.....	79
3.3. Kripto Para Riskleri	80
3.4. Dolandırıcılık ve Kara Para Aklama	87
3.5. Kripto Para Birimleri Kara Para Aklama ve Terörizmin Finansmanında Kullanımı	93
3.6. Kripto Para Sahtekarlığı ile Mücadelede Adli Muhasebe	103
3.7. Soruşturmalar (Araştırmalar).....	106
3.7.1. Ağ Analizi	106

3.7.2. İşlem Analizi	107
3.7.3. Cüzdan Analizi	107
3.8. Kripto Para Cüzdanları İle Kimliklerin İlişkilendirilmesi.....	111
3.8.1. Dusting (Tozlanma) Saldırısı.....	112
3.8.2. Paket Korsanlığı (Packet Sniffing) Ve Gizli Dinleme (Eavesdropping) Saldırısı	113
SONUÇ VE ÖNERİLER	119
KAYNAKÇA.....	122



SİMGELER VE KISALTMALAR LİSTESİ

ACFE	: The Association of Certified Fraud Examiners
AICPA	: The American Institute of Certified Public Accountants
AML	: Anti-Money Laundering
ANOVA	: Analysis of Variance
APR	: Annual Percentage Rate
ASAF	: The Accounting Standards Advisory Forum
ATM	: Automated Teller Machine
BTC	: Bitcoin (Currency)
CAR	: Computer Assisted Reviews
CIA	: Central Intelligence Agency
CIMA	: The Chartered Institute of Management Accountants
COSO	: The Committee of Sponsoring Organizations of the Tredway Commission
CPA	: Certified Public Accountant
DBC	: Digital Bearer Certificate
DFRWS	: Digital Forensic Research Workshops
DLT	: Distributed Ledger Technology
ECB	: The European Central Bank
ETN	: Exchange-Traded Notes
FBI	: Federal Bureau of Investigation
FinCEN	: The Financial Crimes Enforcement Network
FTC	: Federal Trade Commission
GAO	: Governmental Accountability Office
GB	: Gigabyte
IAS	: International Accounting Standards
IASB	: International Accounting Standards Board
ICO	: Initial Coin Offering

IEO	: Initial Exchange Offering
IFAC	: International Federation of Accountants
IFRS	: International Financial Reporting Standard
IMF	: The International Monetary Fund
IRS	: Internal Revenue Service
ISA	: The International Standard on Auditing
ISO	: International Organization for Standardization
KYC	: Know Your Customer
LLCs	: Limited liability companies
MMORPGs	: Massively Multiplayer Online Role Playing Games
MSB	: Money service Businesses
P2P	: Peer to Peer
PDA	: Personal Digital Assistants
POW	: Proof of Work
QR	: Quick Response
RSF	: Relative Size Factor
SAS	: The Statement on Audit Standards
SEC	: The U.S Securities & Exchange Commission
SHA	: Secure Hash Algorithms
SPPI	: The Solely Payment of Principal and Interest
STO	: Security Token Offering
TOR	: The Onion Router
UFRS	: Uluslararası Finansal Raporlama Standartları
UTXO	: Unspent Transaction Output
VCE	: Virtual Currency Exchanges
XBT	: Bitcoin (Currency)

TABLÖLAR LİSTESİ

Tablo 2.1: Kripto Paraların En Önemli Türleri	56
---	----



ŞEKİLLER LİSTESİ

Şekil 2.1: Bitcoin işlem hareketi	38
Şekil 3.1: Bitcoin Volatile Grafiği.....	83
Şekil 3.2: Trezor Kripto Para Cüzdanı One/T Modeli.....	98
Şekil 3.3: Karıştırma Hizmeti Çalışma Prensibi.....	101



GİRİŞ

Kripto para, oluşumlarında kriptografik ve zaman damgası gibi çeşitli teknolojilere bağlı olan en yaygın ve modern teknolojilerden biridir. Kripto para, yaygınlaşmasının ardından birçok halk ve kurumlar tarafından da kabul görmüştür. Gerçekte, birçok şirket kripto paraları operasyonlarının ana faaliyeti olarak veya nakit yerine ödeme aracı olarak kabul edilmektedir.

Günümüzde, ihraç yöntemlerine ve para birimini oluşturma ve çalıştırma sürecinde güvenilen teknolojinin türüne bağlı olarak farklı türlerde birçok kripto para birimi bulunmaktadır. En çok öne çıkan kripto para birimlerinden biri de diğer kripto para birimlerinden ayrılan hususiyeti ve özellikleriyle adından söz ettiren Bitcoin'dir. Bitcoin, üzerine inşa edildiği Blockchain teknolojileri sayesinde günümüzde hem fiyat hem piyasa değeri açısından en büyük hacmi işgal etmektedir.

Bitcoin, büyük hırs ve ihtiraslara sahip gençler için zenginliğe giden hızlı ve kolay bir yolun kapılarını açmıştır. Ayrıca, kripto para piyasası, piyasa değerindeki hızlı ve büyük değer kazanımları ile kripto para birimlerinin sayısındaki hızlı artış nedeniyle yatırımcılar için eşsiz bir pazar sağlamıştır. Bitcoin, ilk olarak 2009 yılında Satoshi Nakamoto tarafından yayınlanan bir makalede, Blok Zincirinin yeni ve merkezi olmayan bir hesap defteri teknolojisi olarak tanıtılması ile bilinirlik kazanmıştır. Satoshi ismi ise halen bir kişiye ya da bir varlığa atıfta bulunan anonim bir karakter olarak kalmaktadır. Satoshi'nin açıkladığı fikirlerden biri, yeni bir teknoloji olan bu Blockchain teknolojisinin, parasal varlıklara sahip olmak ve para transferlerini hükümet kontrol ve kurallarını dışında gerçekleştirebilecek finansal bir özgürlük sağlamasıdır.

Blockchain, her bir kayıt için kriptografik zaman damgası teknolojisi özelliği nedeniyle yeni muhasebe teknolojisi olarak kabul edilmiş ve küçük depolama boyutuyla da herhangi bir defter girişini sorunsuz hale getirmiştir. Bu özellikler, birçok şirketi, sözleşmelerin devamlılığını sağlama, para transferlerinin ve para hareketlerinin

gerçekleştirilmesi, e-fatura işlemlerinin sağlanması, tedarik zinciri finansmanının sürdürülmesi ve şirketler arasında muhasebe girişlerinin kaydedilmesi gibi birçok sayıda ve çeşitli amaçlara yönelik olarak Blockchain ağ hizmetlerini kullanmaya teşvik etmiştir ki bu üç taraflı muhasebe yönteminin ve benzer diğer yaklaşımların başlangıcı olarak kabul edilebilmektedir.

Amerika Birleşik Devletleri ve Kanada gibi büyük ve gelişmiş ekonomilere sahip ülkeler kripto paraların kullanıldığı işlemlerin yapılmasına izin vermektedir. Bununla birlikte, her ne kadar çoğu ülkede kripto para birimlerinin kullanımının yaygınlaştırılmasına yönelik çabalar söz konusu olsa da bunların günlük işlemlerde kullanılması tamamen veya kısmen yasak olarak kalmaya devam etmektedir. Ayrıca belirtmek gerekir ki bazı ülkeler kendi kripto para birimlerini oluşturmaya karar verme yoluna gitmektedir. Muhasebe işlemlerinde ve finansal faaliyetlerde kripto varlıklara yer vermeye yönelik bir düzenleme ihtiyacı ortaya çıkmaktadır ve bu ihtiyaca karşılık olarak Dört Büyükler (Big-4) ve Uluslararası Muhasebe Standartları Komitesi gibi Dünya'nın en büyük muhasebe toplulukları ve şirketleri tarafından genel bir eylem planı oluşturulmuştur. Bu bağlamda, kripto varlıkların nasıl hesaplanacağı, bu varlıklarla yapılan işlemlerin defter kaydının nasıl gerçekleştirileceği, şeffaf bir şekilde nasıl açıklanacağı üzerinde durulmuş ve gerekli raporlamalar yapılmıştır.

Değerli metaller ve emtialar ile aynı şekilde bir yatırım aracı olarak değerlendirilen dijital para birimleri hem finansal yatırım beklentilerinden hem de yasadışı faaliyetlerde kullanılabilme gerçeğinden dolayı diğer yatırım araçları ile benzer risklerle karşı karşıya kalmaktadır. Kripto para birimlerinin kullanılması muhtemel olan yasadışı faaliyetlerin çoğu iki farklı türde incelenebilmekte ve işleme dahil olan farklı tarafları da olumsuz şekilde etkileyebilmektedir. Dolandırıcılık, sahtekarlık ve hırsızlık gibi meseleler kişileri etkilemekteyken, kara paranın aklanması ve terörizmin finansmanı gibi meseleler ülkelerin ulusal güvenliğini tehdit etmektedir.

21.Yüzyıl'ın başlarında, Worldcom ve Enron gibi büyük şirketler, yalnızca standartlar çerçevesinde geliştirilen denetim unsurlarının yeterli olmayacağını fark etmiştir. Öyle ki adli muhasebenin önemini ortaya koyan ve kurumları adli muhasebe etkinliklerine yönelten çok sayıda skandala tanık olunmuştur. Genel bir çerçeveden bakıldığında, Blockchain, yapay zekâ ve nesnelerin interneti gibi teknolojilerin yeni

nesil dolandırıcılık vakalarında iz sürmeyi çok daha zor hale getirdiğini belirtmek mümkündür. Buna bağlı olarak, denetim prosedürleri de alışlagelmiş yöntemlerin dışına çıkarak çok daha karmaşık bir hal almaktadır. Bu nedenle, adli muhasebe ile sağlanabilecek bu yeni ve zorlu değişiklikleri ortaya çıkarabilecek ve bunlarla baş etmeye imkân tanıyacak üst düzey becerilere, tekniklere ve yöntemlere yönelik bir ihtiyaç da ortaya çıkmaktadır. Adli muhasebeyi düzenli denetim ve güvence hizmetlerinden farklı kılan husus, adli muhasebe uzmanlarının özel olarak eğitilmiş ve yetiştirilmiş olmaları ve faaliyetlerini alışlagelmişin dışında sıra dışı yöntemlerle gerçekleştiren dolandırıcılarla ve dolandırıcılık suçlarıyla mücadele etmelerini sağlayan farklı uygulamalı eğitimlere sahip olmalarıdır. Genel olarak, gerekli finans ve muhasebe eğitimlerini alan, sertifikalı kamu muhasebecileri (CPA) ve sertifikalı adli finans uzmanı (CFA) gibi sertifikalara sahip olan adli muhasebe uzmanları, suçla mücadele eden adli ve hukuki kurumlar, avukatlık firmaları ve devlet kolluk kuvvetleri tarafından işe alınmaktadır. Adli muhasebe uzmanlarının başlıca görevleri, takip ettikleri davalarla ilgili olarak ihtiyaç duyulan kanıtları bulmak ve toplamak, gerekli tanımlamaları yapmak, elde ettiği sonuçları sunmak ve olayı açıklığa kavuşturmadır.

Bu çalışmada, açıklayıcı bir yöntem benimsenerek, Blockchain teknolojisine ve kripto para birimlerinin ardında saklı olan mantığa ışık tutmak, adli muhasebe yöntemleri ile mücadele edilen, kripto para birimlerinin kullanıldığı modern dolandırıcılık vakalarının nasıl gerçekleştirilebileceğini açıklamak ve ayrıca muhtemel defter girişlerini tanımlamak ve açıklığa kavuşturmak amaçlanmaktadır.

Bu çalışma üç bölümden oluşmaktadır. Çalışmanın ilk bölümünde, adli muhasebe kavramına ve adli muhasebenin tarihsel gelişim sürecine yönelik genel bir incelemeye yer verilmekte, ilgili yöntem ve teknikler açıklanmaktadır. İkinci bölümde, Blockchain ve kripto varlıklar üzerinde durulmakta, bunların nasıl işlediğine ve kullanımlarına yer verilmekte, ayrıca bazı muhtemel muhasebe uygulamalarına değinilmektedir. Son olarak, üçüncü bölümde, bilhassa kripto varlıkların bilgisayar korsanlığı ile manipüle edilmesi (hacklenmesi) ve dolandırıcılık faaliyetinde kullanılacak yöntemlerin incelenmesi, siber güvenlik risklerinin değerlendirilmesi ve dolandırıcılıkta mücadelede adli muhasebe yöntemlerinin nasıl etkin bir şekilde kullanılabileceği üzerinde durulmaktadır.

BİRİNCİ BÖLÜM

ADLİ MUHASEBE

Son 30 yılda, çalışanlar tarafından yapılan mesleki dolandırıcılık, genellikle en yaygın dolandırıcılık şekli olan varlıkların çalınması ve zimmetine geçirilmesini içerir. Sürekli değişen ekonomik, sosyal ve teknolojik ortam ve artan sosyal ve finansal terörizm nedeniyle işletme sahipleri, soruşturma yapılırken adli soruşturmalara başvurma nın neredeyse gerekli olduğuna inanmaktadır. Ancak bilirkişiler tarafından ele alınabilmesi için olayın mevcut yasa ve yönetmeliklere uygun olarak mahkemeye sunulması gerekmektedir. Adli muhasebe mesleğinin artan önemi ile mesleki eğitim sadece özel kurum / kuruluşlar tarafından verilmemekle birlikte üniversiteler ve meslek kuruluşları tarafından çeşitli kurslar da düzenlenmektedir. Günümüzde çeşitli üniversitelerin lisansüstü derslerinde adli muhasebe dersleri açıldığını görebiliriz (Aksu vd., 2008, s. 63).

1.1.Adli Muhasebeye Genel Bakış

Adli muhasebe, her ne kadar son yıllarda rağbet görmeye başlamış olsa da yeni bir kavram değildir. Bu alanın temeli, dolandırıcılık suçunun neden işlendiğini anlamak için dolandırıcıların zihnini ve düşünce yapısını anlamak üzerine kuruludur. Bir sosyolog ve suçbilimci olan Donald Cressey, 1940'lı yıllarda yaptığı çalışmalarla adli muhasebenin öncüsü olmuştur. Cressey, La Cosa Nostra üzerine bir inceleme niteliğinde olan “Theft of The Nation” adlı eserini kaleme almış ve organize suçlar alanındaki çalışmaları ile tanınmıştır. Cressey, Indiana Üniversitesi'nde, zimmetine para geçiren kimseler üzerine yazdığı doktora tezini tamamlayarak bu alanda öne çıkan ilk akademisyen olmuştur. Cressey, doktora çalışması kapsamında, zimmetine para geçiren 200 tutuklu ile yüz yüze görüşme gerçekleştirmiştir. Cressey çalışmasının neticesinde, “Hile Üçgeni” teorisini geliştirmiştir (Karancher vd., 2011, s. 62).

Hile Üçgeni yaklaşımı, dolandırıcılık suçunun işlenmesi için üç faktörün gerekli olduğunu öne sürmektedir. Bu faktörler şunlardır: Baskı, fırsat ve rasyonalizasyon. Acil finansal ihtiyaçlarla karşı karşıya kalan çalışanlar, karşılaştıkları finansal yükleri hafifletmek için **baskı** hissedebilmektedirler. Bu finansal ihtiyaçlar genellikle gizlidir ve çalışanlar finansal sorunlarını hızlı ve sessiz bir şekilde çözmeye yönelik endişe içerisinde bulunabilmektedirler (The Center for Audit Quality, 2010, s. 3).

Çalışanlar içine düştükleri böylesi vahim bir durumu algıladıktan sonra, çalıştıkları yerde herhangi bir yakalanma korkusu duymaksızın bir dolandırıcılık yapma **fırsatı** kollamaya başlayabilmektedir. Çalışanlar, dolandırıcılık suçunu işlemelerine bir neden olarak, ihtiyaçlarının, işverenin zararından daha önemli olduğunu ya da haksız bir muameleye maruz kaldıklarını ve haklarının yenildiğini öne sürerek, bu suçu **rasyonelleştirebilmektedirler**. Suçu gizleme ihtiyacı büyüdükçe, dolandırıcılık faaliyetleri de kontrolden çıkmaya başlamaktadır (Golden vd., 2006, s. 56).

1.1.1. Adli Muhasebenin İlk Düşümü

Bilinen en eski Adli muhasebe vakası 1824 yılına kadar uzanmaktadır. 1824 yılında İskoçya'nın Glasgow kentindeki bir gazete ilanı bu alanda bilinen ilk suç olarak karşımıza çıkmaktadır. Bu vakada, mahkeme, hakimler ve avukatlar ilk kez bir dolandırıcılık faaliyetinin araştırılmasına yönelik olarak adli muhasebe uzmanlarının yardımına başvurmuşlardır. Ancak, adli muhasebe uzmanlarının bilirkişi olarak mahkemelerde görevlendirilmesi 1900'lü yılların başlarında Amerika Birleşik Devletleri ve İngiltere'de gerçekleştirilmeye başlanmıştır (Crumbley D. L. vd., 2003, s. 9).

Zaman içerisinde, düzenleyici kuralların ve ceza kanunlarının değişimi ile birlikte adli muhasebeye yönelik ihtiyaç da bir artış göstermiştir. Örneğin, 1900'lü yılların başında, Federal Gelir Vergisi kabul edilmesi ile birlikte gelir vergisi kaçakçılığının önlenmesine yönelik çabalar adli muhasebe uzmanlarına olan talebi artırmıştır. Bunun için Amerika Birleşik Devletleri Milli Gelirler İdaresi (IRS), vergi kaçakçılarının tespit edilmesi amacıyla kullanılan adli tekniklerin büyük bir kısmını geliştirme hususunda başarılı olmuştur. Adli muhasebe uzmanlarınca ortaya çıkarılan ilk vergi kaçakçılığı vakalarından biri kötü şöhretli bir gangster olan Al Capone tarafından işlenen suçtur. Ayrıca, II.Dünya Savaşı esnasında finansal işlemleri

incelemek ve takip etmek için Amerika Birleşik Devletleri Federal Soruşturma Bürosu (FBI) 500'den fazla adli muhasebe uzmanı istihdam etme yoluna gitmiştir (Nunn vd., 2006, s. 1).

Adli Muhasebe alanı ve adli muhasebe uzmanlığı mesleği zaman içerisinde geliştikçe ve büyüdükçe, adli muhasebe uzmanlarına rehberlik sağlamak üzere çok sayıda çalışmalar gerçekleştirilmiş ve çeşitli yayınlar sunulmuştur. Bu bağlamda, New Yorklu bir muhasebe uzmanı olan Maurice Peloubet, 1946 yılında “Adli Muhasebe: Bugünün Ekonomisindeki Yeri” başlıklı bir makale kaleme almıştır. 1982 yılında Francis C. Dykeman tarafından yayınlanan “Adli Muhasebe: Bir Bilirkişi Olarak Muhasebeci” adlı kitap da bilinen bir örnek teşkil etmektedir. Ayrıca, 1986 yılında Amerikan Serbest Muhasebeci Mali Müşavirler Enstitüsü (AICPA) tazminatlar, antitröst, muhasebe, değerlendirme, genel danışmanlık ve analizler başlıklarını içeren, altı adet hukuk davası hizmet alanını özetleyen “Uygulama Yardımı - 7” adlı çalışmayı yayınlamıştır. Ayrıca, adli muhasebe alanında büyük bir literatür kaynağı olan, “Journal of Forensic Accounting: Auditing, Fraud & Taxation” adlı bir süreli yayın da bulunmaktadır. Bu uzmanlık alanının büyümesi ve adli muhasebe uzmanlığının profesyonel bir meslek haline gelmesi ile birlikte 1997 yılının Mart ayında, Amerikan Adli Muhasebeciler Kurulu adlı bir meslek teşkilatı kurulmuştur (Crumbley D. vd., 2015, s. 12).

1.1.2. Adli Muhasebenin Tanımı

Adli muhasebe, adli muhasebecilik ya da **adli finans** terimi, fiili ya da muhtemel anlaşmazlıklar ya da davaya konu olan sözleşmelere dayanan durumları tanımlayan bir muhasebe dalıdır ve uzmanlık gerektiren bir uygulama alanıdır. “Adli” terimi, “bir mahkemede kullanımı uygun olan” anlamına gelmektedir ve adli muhasebe uzmanları genellikle bu standart çerçevesinde çalışmaktadır ve üzerinde çalıştıkları vakaların sonucu da mahkemelerde sonuçlanmaktadır. Adli muhasebe uzmanları, aynı zamanda adli denetçiler ya da soruşturmacı/araştırmacı denetçiler olarak da adlandırılmaktadır ve genellikle adli duruşmalarda bilirkişi görüşü sunmaktadırlar. Neredeyse bütün büyük muhasebe firmalarında, çok sayıda orta ölçekli ve özel firmalarda, çeşitli kolluk kuvvetlerinde, polis teşkilatlarında ve devlet kurumlarında adli muhasebe uzmanlarının istihdam edildiği özel birimler vardır. Bu birimlerde çeşitli alt

uzmanlık alanları olabilmektedir. Bunlara örnek olarak; sigorta talepleri, kişisel yaralanma talepleri, dolandırıcılık, kara para aklamayı önleme, hukuki yorum, telif hakkı denetimleri gibi alanlarda uzmanlaşmış adli muhasebe uzmanları sayılabilmektedir (Manning, 2005, s. 6).

Adli muhasebe, "mali sorunların, mahkemelerin gerektirdiği standartları karşılayacak şekilde çözülmesi amacıyla, soruşturma becerilerinin ve analitik becerilerin uygulanması" olarak tanımlanmaktadır. Adli muhasebe uzmanları, vakalara dair kanıtları toplamak, analiz etmek ve değerlendirmek, bulguları yorumlamak ve sonuçları ilgili makamlara iletmek için muhasebe, denetim ve finans alanlarında bilgilerini ve niceliksel yöntemleri kullanarak, hukukun ilgili alanlarında ihtiyaç duyulan özel araştırma ve soruşturma becerilerini uygulamaktadır (Singleton ve Singleton, 2010, s. 12).

“Adli” terimi, tanımından da anlaşılacağı üzere “mahkemeye uygun” anlamına gelmektedir. Adli muhasebe, adli bir merciiye sunulabilecek nitelikte bilgiler üzerine odaklanmış bir muhasebe türüdür. Adli muhasebe, ilgili finansal verileri tanımlama, yerleştirme, sıralama, çıkarma, kaydetme, raporlama ve doğrulamanın yanı sıra, cezai gözlem altına giren finansal konuların durumu hakkında uygun sonuçlar elde etmek için açıkça düzenleme ve analiz etme etkinliği olarak tanımlanabilmektedir (The Association of Certified Accountants (ACCA), 2010).

1.2.Adli Muhasebecilerin Rolü

Adli muhasebeci, yasal çözüm de dahil olmak üzere dolandırıcılık döngüsü ile ilgili becerilere, yeteneklere ve bilgiye sahiptir. Dolandırıcılık, kapsamı nedeniyle birçok farklı alanda gerçekleşebilen bir suçtur. Bu nedenle, adli muhasebe uzmanları çok sayıda farklı alanda hizmet sağlamaktadır.

Adli muhasebeciler ya da bir başka ifade ile dolandırıcılık denetçileri, bu işi yapmalarını sağlayan çeşitli beceriler ile donatılmış uzmanlardır. Bu uzmanlar çoğunlukla, görevlerini yapmak için ihtiyaç duydukları becerileri edinmelerine ve geliştirmelerine katkıda bulunan sertifikalı kamu muhasebecileri (CPA) ve sertifikalı adli finans uzmanı (CFA) gibi sertifikalara sahiptir. Adli muhasebe uzmanlarının sahip olduğu niteliklerden biri de profesyonel şüpheciliktir. Öyle ki, bu nitelikleri sayesinde dolandırıcılık denetçileri, ilgili mali suçları tespit edebilmektedir. Bir nakdin

kaybolduğu hallerde, bir denetçi, kullanılacak uygun araştırma tekniklerini belirlemek için organizasyon içerisinde meydana gelmesi muhtemel dolandırıcılık planlarını tespit edebilmeli ve ortaya çıkarabilmelidir. Denetçi, araştırma teknikleri ve keşif yöntemleri hakkında bilgi sahibi olmalıdır. Yürütülen bir soruşturmada çok sayıda ve farklı türlerde belgeye ihtiyaç vardır ve denetçi neyin kimden talep edilmesi gerektiğini belirleme hususunda yetkin olmalıdır. Ayrıca, yürütülen soruşturmalar sırasında, mevcut mesele hakkında bilgi sahibi olan kimselerle görüşmek yararlı olmaktadır. Denetçinin, görüşülen kişilerin güvenini kazanmak ve bu kişilerden mümkün mertebe fazla bilgi edinmek için gerekli olan görüşme tekniklerinde yetenekli olması gerekmektedir. Çoğu durumda, bir adli muhasebe uzmanı, çalışmaları esnasında edindiği bilgileri mahkemeye sunmaktadır ve bu nedenle adli muhasebe uzmanının kanıt kurallarını bilmesi önemlidir. Bir kanıt elde edildiğinde, gizliliğin korunması için uygun bir delil güvenlik zincirinin sürdürülmesi ve kanıtların uygunluğun sağlanması önemlidir (Crumbley D. L., 2009).

Dolandırıcılık denetçisi, ayrıca edindiği mali bilgileri yorumlama kabiliyetine sahip olmalıdır. Muhasebe defterlerinden, faturalardan ve hatta üçüncü taraflardan edinilen bilgi ve belgeler, ilgi düzeylerinin ve önemlerinin belirlenmesi için dikkatle analiz edilmelidir. Bir soruşturma tamamlandığında, adli muhasebe uzmanının bulguları açıkça sunamaması halinde hizmeti alan kişi ya da makam için yararlı olması mümkün değildir. Raporlar, hizmeti alan kişi ya da kuruma, incelenen belgeleri, soruşturma sırasında atılan adımları ve soruşturma süresince edinilen bulguların neler olduğunu açıklayacak şekilde dikkatle yazılmalıdır. Bu raporlar genellikle hakimlere, avukatlara ve uzmanlara sunulmaktadır. Dolayısıyla, raporda tüm gerçekler açık, anlaşılır ve ikna edici bir şekilde sunulmalıdır. Bir adli muhasebe uzmanının, bir soruşturmadaki en önemli rolü, bilirkişi olarak hizmet sağlaması ve bu bilirkişi sıfatı ile duruşmalarda ifade vermesidir. Bir adli muhasebe uzmanı, soruşturma için gerekli olan tüm bilgileri ve kanıtları hâkime, mahkeme heyetine ve avukatlara anlaşılır bir şekilde ifade etmelidir. Adli muhasebecilerin çalışmaları ve faaliyet alanları tıpkı onların hizmetlerine ihtiyaç duyan kişiler ve kurumlar gibi büyük bir çeşitlilik göstermektedir. Adli muhasebe uzmanları, nakit ve gayrimenkul gibi çeşitli varlıkların takibi için görevlendirilebildikleri gibi açıklanmayan ya da gizli tutulan varlıkların tespit ve takibi ile de ilgilenebilmektedirler. Ayrıca, alacak ve iflas gibi mali davalar üzerinde çalışabilmektedirler. Adli muhasebecilere çoğu zaman, davaya konu olan zarar tutarının

hesaplanması veya bir davaya konu olan mali anlaşmazlıkların çözülmesi gibi hususlarda danışılmaktadır. Adli muhasebeciler, şüpheli dolandırıcılık faaliyetlerini araştırabildikleri gibi bir işletmede dolandırıcılığı önleme yöntemlerinin uygulanmasını da sağlayabilmektedir. Adli muhasebecilerin hizmetlerine genellikle davacılar tarafından başvurulmaktadır, ancak şirketler veya bireyler tarafından da sıklıkla danışılmaktadır. Adli muhasebeciler, yürütülen soruşturmalar esnasında vergi uzmanları, denetçiler ve ekonomistler gibi farklı uzmanlıklara sahip çeşitli kişilere birlikte çalışma imkânı bulmaktadırlar. Adli muhasebe uzmanları, bazı soruşturmalarda, soruşturmanın tamamlanması için veya mahkeme heyetine sunulacak bilgilerin toplanması için, nihai amaçları doğrultusunda, kolluk kuvvetleri ve devlet kurumları ile birlikte çalışabilmektedirler (Hechat, 2010). Adli muhasebecilerden yararlanılan alanlar şöyle özetlenebilir:

a) Kurumsal inceleme: Şirketler veya kurumlar, kendi çalışma ortamlarının içinden ya da dış kaynaklardan kendilerine yönelik olarak gerçekleştirilebilecek muhtemel istenmeyen durumlardan ve eylemlerden endişe duymakta ve önlemek üzere tepki göstermektedirler. Hoşnutsuz çalışanlardan ve üçüncü şahıslardan gelen isimsiz telefon çağrıları veya anonim e-postalar gibi sorunlar şirketlerde veya kurumlarda rahatsızlık uyandırmaktadır. Bu tür sorunların ivedilikle ve etkili bir şekilde ele alınması, şirketlerin ve kurumların hedeflerine ulaşmalarında sürekliliğin sağlanması için önemlidir. Daha spesifik bir şekilde belirtmek gerekirse, bir adli muhasebeci, kayıt dışı komisyonlar, rüşvet, iş akdinin haksız bir şekilde sonlandırılması, şirket yönetiminin veya personellerinin yanlış eylemleri gibi çeşitli iddiaların söz konusu olduğu durumlarda şirkete veya kuruma yöneltilen iddiaların ele alınmasına yardımcı olmaktadır. Böyle hallerde, soruşturmayı yürüten adli muhasebeci, ortaya atılan iddialardan, söylentilerden veya doğrudan soruşturmanın kendisinden etkilenen kişilerle görüşebilmektedir. Söz konusu kişiler, adli muhasebeciyi bağımsız ve tarafsız bir aktör olarak görebilmekte ve dolayısıyla adli muhasebeci ile konuşmaya ve görüşmeye daha istekli olabilmektedirler (Gray, 2008, s. 115).

b) Dava desteği: Dava desteği, kâr veya zarar, hukuki yorum iddiaları, ürün ve hizmet sorumluluğu, hissedarlar arasındaki anlaşmazlıklar, iflas ve sözleşme ihlali gibi alanlarda, davaya konu olan mali unsurların bütünlüğünün ve miktarlarının araştırılması ve değerlendirilmesi için avukata yardımcı olmayı içermektedir. Dava

desteđi, davanın cezai ya da hukuki olmasına bakılmaksızın bir tür yasal talebe yanıt veren bir avukat tarafından başlatılmaktadır.

c) Cezai konular: Adli muhasebeciler ve denetçiler bilhassa beyaz yakalı çalışanlar tarafından işlenen suçların araştırılmasında ya da suçların önlenmesinde, ayrıca bireylere ve şirketlere yöneltilen iddialara dair ilgili mali işlemlerin düzenlenmesi, değerlendirilmesi ve raporlanmasında sürekli olarak başvurulanan kimselerdir. Burada ilgili suçlar şu şekilde sıralanabilmektedir: Kundakçılık, sahtekarlık, dolandırıcılık (örneğin; zimmete para geçirme, rüşvet ya da gayri resmî komisyon), satıcı dolandırıcılığı, müşteri dolandırıcılığı, yatırım dolandırıcılığı ve borsa manipölasyonu. Mahkemeler tarafından adli muhasebe uzmanları ve denetçilerin bilirkişi görüşlerine yönelik ihtiyaçları günden güne önem kazanmaktadır (Karancher vd., 2011, ss. 36-39).

d) Sigorta talepleri: Sigortalılar ve sigortacılar adına sigorta tazminat taleplerinin hazırlanması ve değerlendirilmesi, bir tazminat talebinin hem bütünlüğü hem de miktarının değerlendirilmesi gibi hususlarda bir adli muhasebecinin yardımına başvurulması gerekebilmektedir. Ayrıca, iş kesintisi, kefalet senedi ve kişisel yaralanma gibi durumlardan kaynaklanan zararın hesaplanması gibi daha önemli konularda da adli muhasebeci yardımı talep edilebilmektedir. Bu vakalardan bir kısmı mali öngörüler gerektirse de birçoğu tarihsel analizlere ve diğer muhasebe ve denetim odaklı hizmetlere ihtiyaç duymaktadır (Karancher vd., 2011, ss. 36-39).

e) Yasal düzenlemeler: Adli muhasebeciler, şirketlere yönelik uygunluk yasaları, kanun hükümleri ve sözleşme hükümlerinin takibini sağlayarak kuruluşların mevzuata ve sözleşmelere uygunluğunu sağlamaya yardımcı olabilmektedir. Hibe ve sübvansiyon soruşturmaları ve kamu soruşturmaları ise hükümete yönelik sağlanan hizmetlerin bir parçasını oluşturmaktadır (Singleton ve Singleton, 2010, ss. 21-22).

1.2.1. Adli Muhasebeciler İçin Gerekli Olan Yetkinlikler

Günümüzde, iş dünyasında adli muhasebecilere olan ihtiyaç önemli bir hal almıştır. Ancak herkesin yüksek nitelikli bir adli muhasebecinin sahip olduđu bilgi ve özelliklere sahip olduğunu belirlemek mümkün değildir. Adli muhasebeciler yüksek yazılı ve sözlü iletişim becerilerine sahip olmalıdır. Bu meslekte güçlü bir muhasebe alt yapısına sahip olmak zorunluluk arz etmektedir. Adli muhasebeci, denetim, risk değerlendirmesi, kontrol, dolandırıcılık tespiti gibi hususlarda kapsamlı bilgi sahibi

olmalı ve ayrıca hukukun temel ilkeleri hakkında yeterli bilgi sahibi olmalıdır. Adli muhasebeciler için, doğru cevapları vermekten kaçınabilecek kimselerle yüz yüze görüşmeler yapmak ve bu kimselerden etkili bir şekilde bilgi alma becerisine sahip olmak önemlidir. Bu nedenle adli muhasebeciler, bir soruşturma kapsamında inceledikleri kişilere şüpheyle yaklaşmalıdırlar. Mali planlama ve yönetim tekniklerindeki bilgi ve deneyimin yanı sıra çeşitli bilgi teknolojilerini ve muhasebe sistemlerini anlama ve uygulama becerisi de dahil olmak üzere gelişmiş bilgisayar becerileri de bir adli muhasebecinin temel nitelikleri arasında yer almaktadır. Başarılı bir adli muhasebeci için gerekli olan çeşitli beceri ve nitelikler vardır. Etkili bir adli muhasebecide olması gereken nitelikler şu şekilde sıralanabilmektedir (Davis vd., 2010, s. 10):

- Eğitim ve öğretim
- Uygun disiplinlerde üst düzey ve sürekli eğitim
- Çeşitlendirilmiş muhasebe ve denetim tecrübesi
- Sözlü ve yazılı iletişim becerileri
- Uygulamalı iş deneyimi
- Çeşitlendirilmiş adli denetim deneyimi
- Ekip ortamında çalışma becerisi
- İnsan ilişkileri ve esneklik konusunda beceriler.

Adli muhasebeci için, en önemli beceri deneyimdir. Deneyim, meslekte doğal olgunlaşma yoluyla kazanılmaktadır. Bir adli muhasebeci deneyim kazandıkça, muhasebe ve denetim, vergilendirme, iş operasyonları ve yönetimi, iç kontroller, kişiler arası ilişkiler, iletişim ve insanlarla ilgili beceriler kazanmaktadır. Bir işletmenin nasıl çalıştığını ve etkili iç kontrol türlerini bilmek, adli muhasebeci için kritik öneme sahiptir. Dolandırıcılık suçları üzerinde uzmanlaşmak isteyen bir muhasebecinin bir kolluk kuvvetinde çalışması da tavsiye edilmektedir. Bir adli muhasebecinin sahip olması gereken temel ve en önemli kabiliyetler şunlardır (Nunn vd., 2006, s. 2):

Dolandırıcılığı Tespit Etme Kabiliyeti: Bir dolandırıcılık soruşturması genellikle potansiyel bir dolandırıcılık suçuna ilişkin kısıtlı ve düşük seviyede bilgi ile

başlamaktadır. Adli muhasebeci, muhtemel suç dolandırıcılık teorisi yaklaşımı gibi yöntemler bağlamında belirleyebilmelidir. Muhtemel suçun işlenme şekli ve muhtemel dolandırıcılığın kanıtlanması ya da çürütülmesi için yukarıda bahsedilen teori gibi potansiyel olarak etkili prosedürlerden yararlanılması gerekmektedir.

Görüşme (Mülakat): Kanıt toplama ve bilgi edinme sürecinde adli muhasebecinin bir dizi görüşme gerçekleştirmesi gerekmektedir. Bu işlev, adli muhasebecinin ustalaşmasını gerektiren bir sanattır. Adli muhasebeci, vakanın tarafları ile görüşmeler gerçekleştirirken, bu görüşmelerin hangi sıra ile yapılacağı da dahil olmak üzere görüşme ile ilgili çok sayıda bilgi ve yeteneğe sahip olmalıdır. Burada en önemli husus, adli muhasebecinin mahkeme tarafından kabul edilebilecek nitelikte ve bir delil özelliği taşıyabilecek itirafları edinmesi ve süreci bu şekilde ele almaya hazırlıklı olmasıdır (Singleton ve Singleton, 2010, ss. 23-25).

Düşünce Yapısı (Zihniyet): Bir adli muhasebecinin yürüttüğü soruşturmada başarılı olmasını sağlayan en kritik faktörlerden biri de düşünce yapısıdır. Bu, tanımlanması ve ölçülmesi en zor olan faktördür. Başarılı bir adli muhasebeci, çeşitli yetenekleri içine barındıran belirli bir düşünce yapısına sahiptir. Adli muhasebecinin dolandırıcı gibi düşünmesi gereklidir. Bu özellik, temelde dürüst bir hayat süren ve dürüstlüğü sıkı sıkıya bağlı ortalama bir denetçiye oldukça aykırı bir tutumdur. Başarılı bir adli muhasebeci, istenmeyen bir durumu neredeyse içgüdüsel olarak sezebilmelidir. Bir denetçi bazen sıra dışı bir durumun doğasını gerçekten bilmeden de bu sıra dışı durumun varlığını hissetmektedir. Böyle bir adli muhasebecinin daima sağlıklı bir şüphecilğe sahip olduğunu söylemek mümkündür ve belirmek gerekir ki bu niteliğe sahip bir denetçi insanlara tam olarak güvenmediği gibi tamamen güvensiz bir yaklaşım da sergilememektedir. Ayrıca, adli muhasebeciler düşünce yapılarını etkileyen birtakım faktörlerin farkındadır ve bunlara sahiptir. Söz konusu faktörler şu şekilde sıralanabilmektedir (Davis vd., 2010, s. 12):

- Dolandırıcılık, denetçi tarafından tespit edilebileceği gibi bir kaza sonucunda ya da bir ihbar ile de ortaya çıkarılabilmektedir.
- Finansal denetim metodolojileri, dolandırıcılık suçunu tespit etme amacından ziyade, daha önemli olduğu kabul edilen bir takım finansal hataları ve yanıltıcı beyanları tespit etmek üzere hazırlanmıştır.

- Dolandırıcılık tespiti, bir bilimden ziyade bir sanattır. Öyle ki yenilikçi ve yaratıcı düşüncenin yanı sıra bilimin katılığını ve hassasiyetini de gerektirmektedir.
- Kararlılık, ısrarcılık ve özgüven gibi nitelikler bir dolandırıcılık denetçisi için istihbarattan ve bilgi toplamaktan daha önemlidir.
- Mantık, problem çözme kabiliyeti ve dedektiflik becerileri, dolandırıcılık denetçileri ve adli muhasebeciler için en kritik başarı faktörleri arasında yer almaktadır.

Kanıt Bilgisi: Bir adli muhasebeci, nelerin kanıt teşkil ettiğini, “en iyi” ve “birincil” kanıtların anlamını ve çeşitli muhasebe verilerinin özetlerinin mahkemelerce kabul edilebilir nitelikte birleştirilmek için alabileceği şekli bilmeli ve anlamalıdır. Bir adli muhasebeci, mahkemedeki kanıt kurallarını ve soruşturmayı en başından itibaren nasıl yürüteceğini bilmeli, tüm delillerin sanki mahkemeye sunulacakmış gibi hazırlamalı ve bunları anlamalıdır. Bu kurallar dikkate alınmaz ve göz ardı edilirse, kanıtlar tehlikeye atılabilmekte mahkeme tarafından geri çevrilebilmektedir (Davis vd., 2010, s. 14).

Bulguların Sunumu: Bir adli muhasebeci, soruşturma sonucunda açığa çıkan bulguları, meslekten olmayan kimselerin de anlayabileceği bir tarzda, açıkça ve anlaşılır bir şekilde iletme yeteneğine sahip olmalıdır. Sunum, sözlü veya yazılı olabilmekte, destekleyici ve açıklayıcı nitelikte uygun yardımcı unsurları da içerebilmektedir. Mahkeme önünde tanık ya da bilirkişi olarak bulunan adli muhasebecinin sunumu, soruşturma kapsamında edinilen bulguların son kez test edilmesi anlamına gelmektedir. Bununla birlikte, adli muhasebecinin aktardığı muhasebe bilgilerinin ve finansal bilgilerin ortalama bir insan tarafından anlaşılması hayli zordur. Bu nedenle, bir bilirkişi olarak, adli muhasebeci, kesin ve eksiksiz bir sonuca ulaşmak üzere, finansal bilgileri ortalama bir vatandaşın anlayabileceği ve değerlendirebileceği şekilde aktarabilmeli, bunun için de ortalamanın üzerinde bir iletişim becerisine sahip olmalıdır (Crumbley D. L. vd., 2003, s. 625).

Araştırma (Soruşturma) Teknikleri Bilgisi: Bir sorun tespit edildiğinde, bu soruna dair iddiaların ve suçlamaların desteklenmesi ya da çürütülmesine yardımcı olacak daha fazla kanıt elde etmek adına daha fazla bilgi ve belge edinilmesi zorunludur. Bu, yalnızca ilgili finansal ve mali belgelerin nerede bulunduğunu bilmekle sınırlı kalmamakta, Genel Kabul Görmüş Muhasebe İlkeleri (GAAP) ve Uluslararası

Finansal Raporlama Standartları (IFRS/UFRS), mali tablo açıklamaları ve iç kontrol sistemlerinin karmaşık unsur ve yapılarının bilinmesini gerektirmektedir. Bununla birlikte, bir adli muhasebeci, dolandırıcılık suçlarında, müdahil olan insan unsurunun da farkında olmalıdır (Nunn vd., 2006, s. 2).

Araştırma (Soruşturma) Becerileri: Adli muhasebeciler, bir soruşturma esnasında, genellikle sahip oldukları soruşturma becerilerini kullanmaktadırlar. Örneğin, cezai bir durumun söz konusu olduğu soruşturmalarda, adli muhasebecinin asıl endişesi, neden, fırsat ve fayda unsurları kapsamındaki kanıtları geliştirmektir. Bir o kadar da endişe verici olan husus, işlemlere uygun yorumların yapılması için vakanın diğer tarafına da şüphe ile yaklaşmaktır. Bir soruşturma esnasında, çalışma yöntemi ve ekonomik risk sorunları gibi diğer endişe uyandıran hususlar da dikkatle ele alınmalıdır.

Araştırmacı Düşünce Yapısı (Soruşturma Anlayışı): Adli muhasebeciler, muhasebe bilgilerinin yanı sıra muhasebe veya denetim standartları ile belirlenen sınırların ötesine geçmelerine olanak tanıyan bir soruşturma anlayışı geliştirmektedirler. Soruşturma anlayışı, adli muhasebecinin deneyimi ile doğru orantılı bir şekilde gelişmektedir. Bu süreç ile birlikte adli muhasebecinin algısı gelişir. Öyle ki, mahkeme önünde, karşı tarafın avukatı, adli muhasebecinin o güne dek dikkate almadığı sorunları ve olasılıkları gündeme getirebilmektedir. Bir adli muhasebecinin, bilirkişi deneyiminin artması, vaka ile ilgili olan hususların daha detaylı tespitine ve dikkate alınması gereken noktalara dair daha kapsamlı bir farkındalığın gelişmesine imkân sağlamaktadır. Böylece bilirkişi, durumun gerçekliğini yansıtmak ve vakayı aydınlatmak için gerekli olan mali kanıtları bağımsız ve tarafsız bir şekilde sunma kabiliyetine sahip olmaktadır (Davis vd., 2010, s. 17).

Finansal Sorunların Tanımlanması: Adli muhasebecilerin, bir şikâyet, iddia, söylenti, soruşturma ya da suçlama ile ortaya çıkan bir durumla karşılaşmaları halinde, vaka için önemli olan finansal meseleleri hızlı ve net bir şekilde tanımlamaları hayli önemlidir. Adli muhasebeciler, deneyimlerine ve bilgi birikimlerine dayanarak karar vermektedirler. Dolayısıyla, ortaya çıkan her bir öneri hem sağduyu içermeli hem de iş gerçekliğini yansıtmalıdır. Örneğin, yabancı bir yargı merciinden gelecek belgelere yönelik bir gereksinim söz konusu ise en net ve anlaşılır öneri bu kayıtların edinilmesi yönünde olacaktır. Ancak bu öneri genellikle pratik bir çözüm sağlamamaktadır.

Dolayısıyla, bu noktada, adli muhasebeci diğer alternatif çözümleri düşünmelidir (Crumbley D. L. vd., 2003, s. 176).

Finansal Bilgilerin Yorumlanması: Bir işlemin ya da bir olaylar silsilesinin yalnızca tek bir yorumla sınırlandırılması alışılmadık bir durumdur. Bir adli muhasebeci, yorumlama sürecinde var olması muhtemel, doğal bir önyargı hususunda uyanık ve bilinçli olmalıdır. Elde edilen bilgilerin nihai yorumunun sağduyu ve iş gerçekliğine uygun olması gerekmektedir. Adli muhasebecinin bu durumdan emin olması için vakaya dair işlemleri her yönüyle incelemesi oldukça önemlidir. Bilginin doğru bir şekilde yorumlanması, ancak herhangi bir kapsam sınırlaması olmaksızın, söz konusu işlemin etraflıca ele alınmasıyla mümkündür. Bilhassa, bir adli bilirkişi olarak mahkemeye davet edilen bir adli muhasebecinin, alternatif ve farklı muhasebe ve mali formülleri bilmesi, farklı kurallardan ve yorumlardan haberdar olması gerekmektedir (Singleton ve Singleton, 2010, ss. 23-25).

1.3.Dolandırıcılık Risk Yönetimi

Bu kısımda dolandırıcılık türleri, hile üçgeni ve dolandırıcılık riskinin değerlendirmesi ele alınacaktır.

1.3.1.Dolandırıcılık Türleri

Dolandırıcılık terimi, kullanıldığı yere göre farklı anlamlara gelebilmektedir. Dolandırıcılık, bir hukuki kavram olarak geniş kapsamlı bir şekilde ele alındığında, başka kişi ya da kişileri mülklerinden veya haklarından mahrum bırakma amacıyla gerçekleştirilen her türlü kasıtlı aldatma eylemi olarak tanımlanmaktadır. Ancak, dolandırıcılık terimine mali açıdan bakıldığında farklı tanımlar karşımıza çıkmaktadır. ACFE* tarafından 2015 yılında yayınlanan Dolandırıcılık İnceleme Uzmanları El Kitabı adlı yayında, muhasebe dolandırıcılığı “mali ve finansal tabloların kullanıcılarını aldatmak için tablolardaki tutarların veya açıklamaların kasıtlı olarak yanlış beyan edilmesi veya ihmal edilmesi yoluyla, bir işletmenin mali durumunun kasıtlı olarak yanlış beyan edilmesi” olarak tanımlanmaktadır. (Jofre, 2017, s. 9) Ayrıca bir muhasebe dolandırıcılığı “mali ve finansal tabloların denetiminde hile yapılması ve finansal tablolarda kasıtlı olarak yanlışlık yapılması” şeklinde de tanımlanmaktadır. Bu

* Uluslararası Dolandırıcılık İnceleme Uzmanları Birliği (ACFE), Dünya çapında dolandırıcılıkla mücadele eğitimi ve öğretimi sağlamaktan sorumlu olan en büyük dolandırıcılıkla mücadele organizasyonlarından biridir.

bağlamda muhasebe dolandırıcılığının iki temel unsurunun, hileli finansal raporlama ve varlıkların kötüye kullanılması olduğunu belirtmek mümkündür (Arens vd., 2016, s. 298).

ACFE'ye göre, kurum ve kuruluşları etkileyen üç temel dolandırıcılık kategorisi vardır. Bunlardan ilki varlık dolandırıcılıkları, ikincisi hileli ifadeler ve üçüncüsü ise yolsuzluktur.

Bu sınıflandırma, finansal ve mali raporlama dolandırıcılıklarını inceleyen ve halka açık şirketlere yönelik bir sınıflandırma geliştiren Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (COSO) tarafından desteklenmektedir. COSO raporu, şu durumları tanımlamaktadır: Hatalı gelir muhasebeleştirilmesi, varlıkların fazla gösterilmesi, giderlerin/borçların (yükümlülüklerin) eksik gösterilmesi ve uygunsuz beyan. Öte yandan, mali raporlama dolandırıcılığının iki temel kategoride ele alınabilecektir. Bunlardan ilki, bir şirketin düzenleyici çerçevede bağlamında izin verilenin dışında muhasebe uygulamalarını kullanması, ikincisi ise hayali satışlar veya hayali envanter gibi işlemlerin deftere kaydedilmesidir (Committee of Sponsoring Organizations of The Treadway Commission, 2016, s. 8).

1.3.2. Hile Üçgeni

Amerikan Serbest Muhasebeci Mali Müşavirler Enstitüsü (AICPA) tarafından yayınlanan Denetim Standartları Tebliğleri/Beyanları (SAS-99) (Ramos, 2003, s. 1) ve IFAC tarafından yayınlanan Uluslararası Denetim Standartları (ISA-240) standardı, dolandırıcılığın kullanımına ilişkin üç koşul bildirilmektedir. Bu koşullara, hile üçgeni adı verilmektedir. Bu koşullar şu şekilde sıralanabilmektedir:

- (1) Motivasyon (teşvik) ya da baskı
- (2) Fırsat
- (3) Tutumlar ya da rasyonalizasyon.

Bir dolandırıcılık suçunun işlenmesi için üç koşulun mevcut olması gerekmektedir. Dolandırıcılık yapan kişinin motivasyonu veya kişiyi dolandırıcılık yapmaya yönelik bir teşvikin yada baskının varlığı, kişinin dolandırıcılık yapmaya yönelik bir fırsat elde etmesi ve son olarak da kişinin dolandırıcılık suçunu rasyonalize etmesi. İlk olarak Dr.Donald Cressey tarafından gerçekleştirilen kriminoloji

alışmalarında ne srlen hile geni yaklařımı, bilhassa dolandırıcıların davranıřlarını dikkate almaktadır. Baskı, genellikle bir kiřinin dolandırıcılık suunu iřlemesine neden olan motivasyondur. Baskı, tıbbi bir durumun varlıęı olabileceęi gibi, faturalarını deyememe gibi mali bir durum da olabilmektedir. Ayrıca, uyuřturucu, alkol ve kumar baęımlılıęı ya da pahalı ve lks eřyalara ynelik istekler de baskı unsuru olarak kabul edilmektedir. Bununla birlikte, bazı durumlarda baskı unsuru yalnızca aęzllk ve servet dřknlę dıřında herhangi bir baskı unsuru grlmemektedir (Arens vd., 2016, s. 305).

1. Motivasyon (Teřvik) / Baskı: řirketlerin mali tablolarını maniple etmeleri iin ortak bir teřvik / baskı unsuru, řirketin mali beklentilerinde grlen bir dřř olarak karřımıza ıkmaktadır. Bir řirketin, faaliyetlerine devam etmek iin krediye ihtiyacı olması halinde ancak finansal beklentilerinin kt olduęu durumlarda, řirket ynetimi, řirket kazanlarını olduęundan daha fazla gstererek maniplasyon yoluna gitmeye alışabilmektedir. Ynetimin kazanları maniple etmesi iin bir bařka teřvik unsuru da hisse senedi fiyatlarını řiřirme isteęi olabilmektedir. řirket ynetimi, řirkette opsiyon ve/veya hisse senedi aısından yksek mali ilgiye sahip olduęunda, hisse senedi fiyatlarını yapay olarak artırma yoluna gidebilmektedir. Ayrıca, uyuřturucu madde ve kumar baęımlılıęı gibi byk mali ykmllkleri de beraberinde getiren zararlı alışkanlıklara sahip olan alışanlar da gelirlerini artırmak iin ikramiyelerini alma ya da maniple etme baskısıyla karřılařabilmektedir.

2. Fırsat: Fırsat baęlamından bakıldıęında, dolandırıcılıęın zayıf bir i kontrol sistemine sahip olan řirketlerde, řirket mlkləri zerinde gvenlięin zayıf olduęu durumlarda, ifřa korkusunun etkili olmadıęı ve yakalanma olasılıęının az olduęu zamanlarda ve bu tr davranıřlara ynelik politikaların belirsiz olduęu řirketlerde daha muhtemel olduęu grlmektedir. Yapılan alışmalar ve arařtırmalar, bazı alışanların tam anlamıyla drst olduęunu ancak bazı alışanların ise drstlk hususunda gvenilir olmadıęını ve fırsat olarak sayılan durum ve kořullardan etkilenebildięini ortaya koymaktadır.

3. Rasyonalizasyon: İnsanların oęunluęu yasalara inandıklarından dolayı ve/veya yakalanmaları halinde nemsedikleri kiřilerin kendilerini ayıplamalarından veya toplum tarafından reddedilip dıřlanmaktan korktukları iin yasalara itaat etmektedir.

1.3.3. Dolandırıcılık Riskinin Değerlendirilmesi

Bir dolandırıcılık riskinin değerlendirilmesi, genellikle bir kuruluşun mevcut yerleşik kontrollerinin ve prosedürlerinin, dahili riskleri ölçmek için mevcut organizasyon yapısı içinde nasıl işlediğini ve sektörün harici risklerini nasıl ele aldığını anlamakla başlamaktadır. Bu anlayış, daha sonra, organizasyon içerisinde belirli bir pozisyonda görev yapan bir çalışanın, belirli bir dolandırıcılık olayını zamanında tespit edilmeksizin başarma olasılığını değerlendirmek için kullanılmaktadır. Prosedürler ve kontroller hiçbir zaman bir boşlukta test edilmez, aksine, daima kontroller ve prosedürlerle etkileşime giren pozisyonlar bağlamında değerlendirilmektedir (Okoye ve Gbegi, 2013, s. 80).

Bir kuruluşun dahili ve harici risklerinin belirli pozisyonlara göre tespit edilmesini takiben, bir sonraki adımda ise en kolay şekilde gerçekleştirilebilecek muhtemel dolandırıcılık planlarının bir listesi derlenmektedir. Bu süreç, kuruluşa yönelik geniş kapsamlı riskler yerine belirli dolandırıcılık planlarının tanımlanması ile sonuçlandırılmalıdır. Örneğin, gelirin muhasebeleştirilmesini bir dolandırıcılık riski olarak tanımlamaktansa, düzgün ve uygun bir şekilde yürütülen bir dolandırıcılık riski değerlendirmesi ile kuruluşun teşvik ücretini üçer aylık gelir performansına bağlama riskinden yola çıkarak sözleşmeler için gelir tahakkukunun zamanlamasıyla ilgili daha spesifik bir dolandırıcılık riski olarak belirlenebilmektedir.

Burada, dolandırıcılık riskinin değerlendirilmesi bağlamına odaklanılması uygun görülmektedir. Bu nedenle, bu bölümde yalnızca dolandırıcılık riskinin değerlendirilmesi süreci hakkında bilinmesi gereken temelleri ve bilhassa denetim standartlarının dikkate alındığı aksaklıklar üzerinde durulacaktır. Denetçiler, dolandırıcılık riskini belirlemek ve bunlara karşı gereken önlemleri almak için dolandırıcılık risk faktörleri de dahil olmak üzere geniş bir bilgi kümesini dikkate almakla birlikte profesyonel şüphecilik niteliklerini de makul düzeyde korumalıdır. Bir denetçi, dolandırıcılıktan veya hatalı bildirimlerden kaynaklanan önemli yanlışlıkların ve aksaklıkların tespit edildiğine dair makul bir güvence elde etmek için, denetimi dikkatli bir şekilde planlayarak uygulamaya koymalıdır. Öyle ki denetçi, dolandırıcılık riskine yönelik karşı tedbirlerin yürürlüğe konması sorumluluğuna sahiptir (Arens vd., 2016, s. 303).

Risk yönetimi, “kurumun, kurumsal hedeflerine ulaşma çabasında, kaçınılmaz olarak maruz kaldığı risklerin anlaşılma ve yönetilme süreci” olarak tanımlanmaktadır. (Doody, 2009, s. 13) Denetçiler, dolandırıcılık risklerini değerlendirmek için en ilgili ve gerekli bilgi kaynaklarından, şirketin durumu hakkında bilgi toplayarak işe koyulmalıdır.

Bir kurum ya da şirketin finansal tablolarında var olan önemli yanlışlıkların gözden kaçırılma riskini azaltmak için denetim prosedürleri tasarlanmalıdır. Bu doğrultuda denetçinin mesleki niteliklerinden biri olan şüphecilikten yararlanması gerekmektedir. Dolayısıyla denetçi, müşterinin halihazırdaki yöntemleri ve önceki deneyimlerinden bağımsız bir şekilde muhtemel bütün kanıtlara karşı uyanık olmalı ve yönetim dolandırıcılığı olasılığını artıran faktörlerin de farkında olmalıdır. Bununla birlikte, uzmanlarla yapılan istişarelerin büyük bir mali yük doğuracağı da göz önünde bulundurularak, denetçiler mevcut görevlerinde önemli ölçüde yüksek bir dolandırıcılık riskinin söz konusu olduğundan emin olmadıkları sürece sorunları adli muhasebecilere iletmekten kaçınma eğilimindedirler. Böylesi bir durumda denetçiler, bir sözleşmeden kaynaklı dolandırıcılık risklerini olduğundan daha az düzeyde gösterme eğilimi sergileyerek kendilerini kandırma yoluna gidebilirler. Bununla birlikte denetçiler, adli muhasebecilere danışmanın kendilerini denetim programı tasarımındaki zayıflıklardan koruyacağına inanarak kendilerini yanlış yönlendirebilmektedirler. Oysa belirlemek gerekir ki adli muhasebeciler, denetim programı tasarımında sınırlı bir yetkinliğe sahip olabilmektedirler (Elliott, 2016).

Adli muhasebe, risk yönetimini yeni ve farklı bir bakış açısı ile ele almaktadır. Bu nedenle, bilhassa dolandırıcılık riskleri ve yönetsel riskleri değerlendirilirken, risk yönetim süreçlerine adli muhasebecilerin dahil edilmesi ciddi bir problem olarak değerlendirilmektedir.

Dolandırıcılık ve yolsuzluk, çoğu kuruluş için süregelenleşmiş bir risk halini almıştır. Dolandırıcılık, mali kayıplara neden olmakta, marka itibarını ve şöhretini zedelemekte, değerli müşterileri ve tedarikçileri uzaklaştırmakta, piyasa güvenini ve saygınlığını azaltmaktadır.

Kuruluşlar ve şirketler, günümüzde, dolandırıcılığı ve yolsuzluğu önlemek ve bunların etkilerini en aza indirmek için giderek daha fazla proaktif bir yaklaşım benimsemektedir (Graham, 2005, s. 53).

1.3.4. Dolandırıcılık Faaliyetlerinin, Yolsuzlukların Tespiti ve Önlenmesine Yönelik Adli Muhasebe Soruşturma Teknikleri

Bu başlık altında, en önemli adli muhasebe tekniklerinin üzerinde durulmaktadır. 2013 yılında Enorfe, Okpako ve Atube tarafından gerçekleştirilen bir çalışmada, Nijeryalı şirketlerde, adli muhasebenin dolandırıcılık tespiti üzerindeki etkisi incelenmiş ve dolandırıcılık tespiti ile adli muhasebe arasındaki ilişki açık bir şekilde ortaya konmuştur. Söz konusu çalışmada, adli muhasebe hizmetlerinin şirketlere sunulması ve uygulanmasının dolandırıcılık faaliyetlerin düzeyini etkilediği bildirilmektedir. (Enorfe, Okpako, & Atube, 2013, s. 65) Günümüzde çeşitli teknikleri ve araçları içinde bulunduran ve bu teknik ve araçlar temelinde çeşitli raporlar oluşturan farklı yazılımların varlığından söz etmek mümkündür. Bu yazılımlar, hem profesyonel hem de teknolojik dolandırıcılık vakalarına yönelik oldukça yararlı, kapsamlı ve başarılı raporlar üretmektedir. Bankacılık ve sigortacılık sektörlerinde olduğu kadar diğer sektörlerde de faaliyet gösteren finans kuruluşları, bilhassa internet üzerinden bağlanan, ofis dışındaki çok fazla sayıda müşteriye hizmet vermektedir ve bu durum kuruluşlar için büyük bir risk oluşturmaktadır. Dolayısıyla, bu kuruluşları ve şirketlerin güvenliğinin sağlanması ve kaynaklarının korunması için adli muhasebe araçları ve teknikleri hususunda iyi eğitilmiş uzmanlardan yardım alınması hayli önemlidir. Dolandırıcılığın tespit edilmesine yönelik etkili teknikleri şu şekilde sırlamak mümkündür:

- a. **Dolandırıcılığın Tespitinde İstisnai Durumlar:** Yeminli Yönetim Muhasebecileri Enstitüsü (CIMA), 2008 yılında dolandırıcılıkla mücadelede dolandırıcılıkla mücadele uzmanları (adli muhasebeciler) için mantıklı düşünme ve hareket etme becerisine dayanan iki temel araç belirlemiştir. Bu temel araçlar, eğitim – deneyim ve ihtiyaç duyulan düşünce yapısıdır (zihniyet). CIMA, ayrıca dolandırıcılık olarak nitelendirilebilecek usulsüzlüklerin tespitine yardımcı olacak günlük uygulamalara dayalı teknikler önermiştir. Buna ek

olarak daha fazla önlem alınıp alınmayacağına karar vermek için sıra dışı durumun anlaşılması ve araştırılması önerilmiştir.

Veri eşleştirme analizi gibi denetim araçları hayli yararlı olabilmektedir. Diğer araçlar ise gerçek zamanlı işlem değerlendirmesi, hedefli işlem sonrası inceleme veya yönetim hesaplarının stratejik analizi gibi çeşitli analizlerin gerçekleştirilmesini mümkün kılmaktadır. Çok sayıda sistem, önceden belirlenmiş eşik değerlerinin (istisnalar) dışında kalan sonuçlar için otomatik raporlar oluşturarak normdan sapan sonuçların anında tanımlanmasını sağlamaktadır. Günümüz teknolojisiyle, istisnalar belirlendiğinde e-posta veya metin uyarısı şeklinde bir bildirimin doğrudan bir yöneticiye gönderilmesi mümkündür. CIMA'ya göre bu tanımlama uyarı tekniklerinin büyük çoğunluğu, süreci daha verimli hale getirmek için otomatikleştirilebilmektedir (Doody, 2009, s. 41).

- b. **Bilgisayar Destekli İncelemeler (CAR) ve Belge İncelemeleri:** Losey'e (2016) göre, belgelerin bilgisayar yardımı ile incelenmesi ve özel olarak tasarlanmış hukuki araştırma ve inceleme yazılımlarının kullanılması oldukça iyi ve yararlı bir yaklaşımdır. Bilgisayar Destekli İnceleme terimi ve aynı anlama sahip alternatif bir ifade olan Teknoloji Destekli İnceleme terimi, bir bilgisayar aracılığı ile belgeleri incelemek ve kodlamaktan çok daha fazlasını ifade etmektedir. Bu yaklaşım, büyük bir veri ortamında, ilgili kanıtları aramak ve bulmak için bilgisayar yazılımlarının vazgeçilmez araçlar olarak kullanıldığı bir süreçtir. (Losey, 2016) En iyi CAR uygulamaları şunlardır: i. Hibrit Çokdorukslu (Hybrid Multimodal), ii. Tahmine Dayalı Kodlama (Predictive Coding), iii. Alt Satıra Dayalı Orantılı İnceleme (Bottom Line Driven Proportional Review), iv. Kalite Kontrol İncelemesi (Review Quality Controls).
- c. **Veri Madenciliği:** Galvanize'e (2018) göre veri madenciliği, verileri keşfetmek için tasarlanmış önemli bir analitik süreçtir. Dünyadaki elmas veya altın madenciliğinin gerçek hayat sürecine çok benzer şekilde, veri madenciliğindeki en önemli görev, büyük miktarda veriden önemsiz olmayan külçeleri çıkarmaktır. Veri madenciliği, karar verebilmeniz veya yargılayabilmeniz için verileri işlemek ve bu bilgilerdeki kalıpları ve eğilimleri tanımlamakla ilgilidir.

Veri madenciliğinin temel ilkeleri üzerinde uzun yıllardır tartışılmaktadır, ancak büyük verilerin ortaya çıkarılması ile bu temel ilkeler daha da yaygınlaşmakta ve bilinir hale gelmektedir. Veri madenciliği, bilgisayar biliminin disiplinler arası bir alt alanıdır. Veri madenciliği, yapay zekâ, makine öğrenimi, istatistik ve veritabanı sistemlerinin kesişme noktasındaki yöntemleri içeren büyük veri kümelerindeki kalıpları keşfetmede etkili bir hesaplama süreci olarak ifade edilmektedir (Galvanize, 2018).

- d. **Benford Yasası:** Rakamlar, mali tabloların kalitesini değerlendirmek de dahil olmak üzere, şirketlerin (mali tablolarının) gücünü belirlemekten daha fazlası için kullanılabilir. Yöntemlerden biri, birçok sayı kümesinin Benford dağılımı olarak bilinen bir logaritmik dağılımı izlemesi gerektiğini belirten Benford Yasası'nın uygulanmasına dayanmaktadır. Coleman'a (2014) göre, 1930'larda General Electrics'te fizikçi olan Frank Benford, logaritma kitaplarının ilk sayfalarının sonraki sayfalardan önemli ölçüde daha fazla yıprandığını fark ettikten sonra, kendi adı ile anılan bir dağılım kuralı varsayımında bulunmuştur. Benford, çeşitli kaynaklardan derlenen 20.000'den fazla sayıyı araştırmış ve dağılımı 1938'de yayınlanan bir araştırma makalesinde tanımlamıştır. Makalede, araştırılan sayıların yaklaşık %30'unun 1 rakamıyla, %18'inin 2 ile başladığını ve yaklaşık %5'inin 9 ile başladığını ifade etmiştir. (Coleman, 2014) Benford Yasası ister yazım hataları ister rastgele şans veya doğrudan manipülasyon olsun, verilerdeki anormallikleri tespit etmek için kullanılabilir. Dağılıma uyması beklenen bir dizi sayı dağılıma uygun olmadığında, bu durum, verilerde bir sorun olduğuna dair bir işaret olarak değerlendirilebilir. Bir modelin belirlenmesi ve oluşturulması için tarihsel süreçteki verileri derinlemesine analiz eden ve bu şekilde veri toplayan adli muhasebeciler için Benford Yasası, adli muhasebe görevlerinde kullanılabilecek nitelikte bir tekniktir. Birinci basamak yasası olarak da adlandırılan Benford Yasası, gerçek hayattaki birçok sayısal veri kümesinde önde gelen basamakların frekans dağılımı hakkında bir gözlem sunmaktadır.
- e. **Oran (Rasyo) Analizi:** Oran analizinin kullanılması, mali tablo dolandırıcılıklarını tespit etmede en güvenilir yöntemlerden biridir. Dolandırıcılık eylemi, payı ve paydayı normal (uygun şekilde belirtilmiş)

orandan farklı bir oranda etkilediği durumda Oran (Rasyo) Analizi yöntemi söz konusu dolandırıcılığı tespit etmede büyük olasılıkla başarılı olmaktadır. Örneğin, gerçeğe uygun değerdeki mevcut olmayan artışlarla bağlantılı olarak hileli kazançların kaydedilmesi sonucunda cari yatırımların defter değerinin olduğundan yüksek gösterilmesi durumunda, işletmenin cari oranı (cari varlıkların cari borçlara bölünmesi) yapay olarak şişirilmektedir veya beklenen bozulma oluşmamaktadır. Elbette, çoğu dolandırıcılık içermeyen, iyileştirilmiş bir cari oran için çok sayıda başka açıklamaların varlığı da söz konusu olabilmektedir. Ancak, önemli oranlardaki açıklanamayan değişiklikler, özellikle birden fazla önemli oranla ilgili olarak ortaya çıktığında, bu bir finansal raporlama dolandırıcılığının ilk uyarı işareti olabileceğinden, her zaman araştırılmalıdır. Bloomenthal (2020) yılında gerçekleştirdiği çalışmasında, karşılaştırmalı oran analizinin analistlerin ve denetçilerin bir firmanın mali tablolarındaki farklılıkları tespit etmesini de mümkün kıldığını belirtmektedir. Oranlar analiz edilerek tutarsızlıklar açısından bir analiz gerçekleştirilebilmektedir. Beneish Modeli olarak bilinen matematiksel bir yaklaşım, sekiz farklı oranı değerlendirerek, kazanç manipülasyonu olasılığını tespit etmektedir (Bloomenthal, 2020).

- f. **Veri Eşleştirme:** Veri Eşleştirme, aynı varlığa işaret eden kayıtları bulma görevidir. Normalde, bu kayıtlar birden çok veri kümesinden gelmektedir ve ortak bir varlık tanımlayıcısına sahip değildir, ancak veri eşleştirme teknikleri tek bir veritabanı içinde yinelenen kayıtları tespit etmek için de kullanılabilir (Garcia, 2018). Garcia'ya (2018) göre Veri Eşleştirme, kayıt bağlantısı, nesne tanımlama veya varlık çözünürlüğü olarak da bilinmektedir. Birden çok veri kümesinde kayıtları belirleme ve eşleştirme yeteneğinin, birçok nedenden dolayı çok zor bir görev olduğunu belirtmek mümkündür. Her şeyden önce, kayıtların genellikle aynı varlığa atıfta bulunanları tanımlamayı kolaylaştıran hiçbir özelliği yoktur, bu nedenle isimler ve doğum tarihleri (insanlar için) ya da markalar (ürünler için) veya unvan gibi kısmi tanımlama sağlayan nitelikleri analiz etmek gerekmektedir. Bu nedenle, veri eşleştirme algoritmaları veri kalitesine karşı çok hassastır, bu da en azından anahtar tanımlayıcı öznitelikleri için asgari bir kalite standardı sağlamak için bağlanan

verilerin önceden işlenmesini gerekli kılmaktadır. Okoye ve Gbegi tarafından (2013) yılında yapılan bir çalışmada, profesyonel adli muhasebecilerin hem kamu sektörüne hem de özel sektöre sağladığı katkıların önemi vurgulanmış ve bu katkının asla göz ardı edilemeyeceği ifade edilmiştir. Söz konusu çalışmada, Nijerya'nın Kogi Eyaletinde yer alan kamu kurumlarında dolandırıcılık suçlarının tespiti ve önlenmesinde adli muhasebe işlevsel bir araç olarak kullanılmış ve önemi ortaya konulmuştur. Bu bağlamda, hem birincil hem de ikincil veri kaynakları kullanılmıştır. Nijerya'nın Kogi Eyaletinde seçilen beş adet bakanlıktan 370 adet personele anket uygulanmış ve bu bakanlıklarda gerçekleştirilen görüşmelerde toplam 350 adet geri dönüş kaydedilmiştir. Verileri analiz etmek için tablolar ve basit yüzdeler kullanılmış ve araştırma hipotezlerini test etmek için Varyans Analizi (ANOVA) kullanılmıştır. Çalışmada, adli muhasebenin kullanımının kamu sektöründe dolandırıcılık vakalarını önemli ölçüde azalttığı ve profesyonel adli muhasebeciler ile geleneksel dış denetçiler arasında önemli bir fark olduğunu belirtilmiş ve bu nedenle adli muhasebecilerin hizmetlerinin kamu sektörü kuruluşlarındaki dolandırıcılık vakalarının tespiti ve önlenmesinde etkili bir şekilde yardımcı olabileceği ortaya konulmuştur (Okoye ve Gbegi, 2013, ss. 11-13).

- g. **Göreceli Boyut Faktörü Teorisi – RSF (Benzer Boyut Faktörü / İlişkili Tutar Faktörü):** Özel tekniklerden biri olan RSF teorisi, bir denetçinin, sistem üzerinden yaygın olmayan işlemleri tespit etmesine yardımcı olmaktadır (Nigrini, 2011, s. 212). Bu uygulama, dönem boyunca gerçekleştirilmiş çeşitli işlemlerin karşılaştırılmasına dayanmaktadır. Örneğin, kayda geçirilmiş seyahat giderleri, 2019 – 2020 mali yılı için 55.000 \$, 2018 – 2019 mali yılı için 25.000 \$ ve 2017 – 2018 mali yılı için 23.000 \$ olarak görülüyor ise böyle bir durumda 2019 – 2020 mali yılındaki seyahat giderlerinin artışı dikkat çekmektedir. Bu bilgi, denetçinin araştırmasını daha da ilerletmesi ve daha ayrıntılı bir soruşturma gerçekleştirmesi adına yarar sağlamaktadır. Böyle bir durumda, normal şartlar altında tek beklenti çalışan sayısının artması nedeniyle seyahat giderlerinin artması olabilmektedir. Dolayısıyla, söz konusu tutarın son birkaç yıla göre yüksek olması bir dolandırıcılık vakasına işaret etmeyebilmektedir. Bu

yaklaşım, denetçinin belirli bir listeden, belirli öğeleri seçmesini kolaylaştırmaktadır (Goldrick ve Gerson, 2002, ss. 5-6).

1.4.Bağımsız Denetçi Ve Adli Muhasebeci Arasındaki Farklar

Bir bağımsız denetçi, esasen, finansal tabloların hazırlanmasında kabul edilebilir muhasebe ve denetim uygulamalarının kullanıldığını doğrulamak için muhasebe ilkeleri ve standartlarından önemli sapmaları ortaya çıkarmayı amaçlamaktadır. Adli muhasebeci, sadece mali tablolarda ne olduğunu doğrulamakla kalmayıp, dolandırıcılığı ortaya çıkarmak için çok daha şüpheli ve proaktif bir yaklaşım benimsemektedir (Crumbley ve Apostolou, 2002).

Bağımsız denetçi ile adli muhasebeci arasındaki fark, esas olarak bu iki görevlinin amaçlarına bağlı olarak ortaya çıkmaktadır. Bağımsız denetçi, genellikle müşterilerinin muhasebe standartlarına uygun hareket ettiğini varsaymakta, denetim standartları tarafından belirlenen yönergeleri takip etmekte ve denetimden sonra, finansal raporlamayı daha adil bir hale getirmek için çeşitli düzenlemeler önermektedir (Rouse ve Conway Jr., 2002, ss. 23-24).

Adli muhasebeciler ise müşterileri ya da süreç hakkında herhangi bir varsayımda bulunmamaktadır. Bir adli muhasebeci, şirketlerin finansal işlemlerinin meşruiyetini ve muhasebe ilkelerine uygunluğunu değerlendirirken sürece eleştirel bir bakış açısı ile yaklaşmaktadır. Dolandırıcılık ya da suiistimal iddiası söz konusu olduğunda bir adli muhasebeci ile çalışmak önem arz etmektedir çünkü diğer denetçiler muhtemel içsel çatışmalarla karşı karşıya kalabilmektedir. Meslek grubu haricindeki birçok kişi, denetçilerin adli muhasebe soruşturması ve soruşturma becerileri hakkında kapsamlı bir eğitim aldığı yanılgısına düşme eğilimindedir. Böyle bir eğitim süreci, denetçilerin çoğu için geçerli değildir. Lisans düzeyinde eğitim veren muhasebe programlarında bu konuda yeterli eğitim verilmemektedir. Her ne kadar bu konuda bazı seçmeli derslerin verildiği biliniyor olsa da adli muhasebe araştırmaları hakkında kapsamlı derslere gereksinim duyulmaktadır. Geleceğin muhasebecileri için umut edilen şey, onların alacakları eğitimin geliştirilmesi, soruşturma ve algılama teknik ve yaklaşımları konusunda farkındalıklarını artıran bir müfredatın hazırlanması ve adli muhasebe uzmanlarının sahip olması gereken yetenekleri kazandıran bir öğretim sisteminin olmasıdır. Böylelikle, muhasebe bölümünden mezun olan genç muhasebeciler, iş

dünyasında, operasyon, yönetim ve iç denetim gibi birimlerde çalışabildikleri gibi ayrıca bağımsız denetçiler olarak da dolandırıcılık suçunun izlerini keşfetme konusunda etkin olabilecekler ve adli muhasebe uzmanlarını ne zaman davet edeceklerini de daha iyi bilme imkanına kavuşabileceklerdir (Golden vd., 2006, s. 244).

Adli muhasebecilik, denetçilik ve özel dedektiflik mesleklerinin bir kombinasyonu gibi görülebilmektedir. Bir adli muhasebecinin sahip olması gereken bilgi ve beceriler şu şekilde sıralanabilmektedir: Soruşturma becerileri, araştırma, hukuk, sayısal yöntemler, finans, denetim, muhasebe ve kolluk kuvvetleri gibi düşünebilme kabiliyeti. Ayrıca, örgütsel davranış ve uygulamalı psikoloji bilgi ve becerileri de oldukça önemlidir. Amerika Birleşik Devletleri'nde adli muhasebeciler, FBI, CIA, IRS, FTC, HOMELAND, ATF ve GAO gibi resmi federal kuruluşlarda istihdam edilmektedir. Adli muhasebecinin odak noktası beyaz yakalı suçu olarak adlandırılan suçlardır, bu nedenle adli muhasebecilerin finansal ve diğer ilgili becerilere sahip olması gerekmektedir (Gray, 2008, s. 115).

Adli muhasebeciler, devlet kurumları haricinde bankalar ve sigorta şirketleri gibi büyük işverenler veya ilgili davalara bakan hukuk büroları tarafından da istidam edilebilmektedirler. Adli muhasebeciler genellikle hukuk ve ceza mahkemelerinde bilirkişi sıfatıyla görev almakta, uzman görüşü bildirmektedirler. Adli muhasebeciler herhangi bir dolandırıcılık suçunun olup olmadığına dair tanıklık yapmazlar zira bu yönde bir kararı mahkeme verebilmektedir. Adli muhasebeciler mahkemeye kanıt sunarlar ve tanık çıkarırlar. Adli muhasebeciler mesleklerini ve çalışmalarını destekleyen çok sayıda mesleki organizasyona ve kuruluşa sahiptir (Gottschalk, 2018, s. 59).

İyi bir adli muhasebeci daima mahkeme önünde bilirkişi sıfatıyla görüş bildirecekmiş gibi çalışmalarını yürütmelidir. Adli muhasebeci, karmaşık konuları, basit, sade ve anlaşılması kolay bir şekilde açıklayabilmelidir. Adli muhasebeci daima tarafsızlığını muhafaza etmeli ve bu yönde itibarını sürdürmelidir (Crumbley D. vd., 2015, s. 193).

Adli muhasebe, finansal muhasebenin aksine, rutin bir temelde değil yalnızca daha önce belirtilen özel koşullar gerektirdiğinde icra edilen bir yaklaşımlar bütünü sunmaktadır. Sonuç olarak, bir adli muhasebeciye ne zaman ihtiyaç duyulduğunu veya

ne zaman danışılması gerektiğini bilmek müşteri, hak sahibi ve üst yönetim kadrosu için önemlidir. Adli muhasebecinin yürüttüğü soruşturma, davanın daha erken bir aşamasında başlatılırsa, genellikle daha az bir zaman gerektirmekte ve daha az bir ücrete mal olmaktadır. Bir vaka kapsamında, adli muhasebecinin hizmetlerinden kısmen ya da tamamen yararlanılması her halükârda süreci daha olumlu bir düzleme taşımaktadır (Gray, 2008, s. 115).

1.5.Adli Muhasebecilerin Rolü

Şirketlerin ya da bireylerin, adli muhasebecinin hizmetlerinden yararlanmasının çeşitli nedenleri vardır. Adli muhasebeciler, soruşturma denetimi için onları mükemmel kılan özel becerilere sahiptir ve bu beceriler çoğu vakanın aydınlatılmasında birer gereklilik olarak karşımıza çıkmaktadır (DiscoverAccounting, 2019). Şirketlerin ve bireylerin adli muhasebecilerin hizmetlerine yönelmesine neden olan durumlardan en bilinen sekiz tanesi şunlardır:

a) Boşanma & Mal Paylaşımı

Boşanma davalarında, konu mal paylaşımına gelince işler karmaşık bir hal alabilmektedir. Yüksek miktarlarda varlıklara sahip olan çiftlerin boşanma davalarında finansal konular özellikle daha zor bir hal alabilmektedir. Yatırım portföyleri, çoklu banka hesapları, uzaktaki gayrimenkuller ve diğer özel yatırımlar daima işlerin daha da karmaşık bir hal almasına neden olmaktadır. Ayrıca taraflardan birinin off-shore banka hesaplarında birikim yapması, mali kayıtları karışık bir hale sokması ya da eşinin varlıklarını farklı şekillerde saklaması söz konusu olabilmektedir (Manning, 2011, s. 223). Boşanma davasının taraflarının sahip oldukları varlıkları saklamak için çok sayıda gizli yöntem kullandığı bilinmektedir. Bu nedenle, evlilik kapsamındaki tüm banka hesaplarının ve mali tabloların kontrol edilmesi için bir adli muhasebeciye ihtiyaç duyulabilmektedir. Adli muhasebeciler, usulsüzlükleri ortaya çıkarabilmekte, fonların nerede saklandığını keşfedebilmektedir (Coenen, 2009, s. 170). Taraflar düzensiz ve anlamsız mali kayıtlar sunduklarında, bir adli muhasebeci, tüm bunları maksimum verimlilikle sırlayabilmekte ve analizi zamanında yapabilmektedir. Boşanma davaları büyük ve karmaşık varlık portföylerini içerdiğinde, saygın bir adli muhasebeci bulmak ve ondan hizmet almak çok önemlidir. Taraflar bir şirkete sahipse veya bir şirket üzerinde karşılıklı iddialarda bulunuyorsa, şirketin mali tablolarındaki dolandırıcılıkla

tutarlı kalıpların ve düzensizliklerin ortaya çıkarılması için özel olarak eğitilmiş bir adli muhasebe uzmanının incelemesine tabi tutulması zorunludur. Adli muhasebecinin nihai raporu tarafların sahibi olduğu şirketler için de faydalı olabilmektedir. Öyle ki bu raporlar, şirketlerin muhtemel sızıntıları ve suiistimal fırsatlarını düzeltmelerine yardımcı olabilmektedir. Esasen, yüksek değerli boşanma davalarında, adli muhasebeciler, takip soruşturmaları yürütmek için davaya dahil edilebilmektedir. Örneğin, taraflardan biri, boşanma kararını etkileyebilecek bir mali değişiklik gerçekleştirmeye ya da bunu talep etmeye çalışabilmektedir. Bununla birlikte nafaka talebi ya da nafaka ödemesi ile ilgili olarak da bir usulsüzlük söz konusu olabilmektedir. Bu tür iddia ve tutumlarda etik olmayan ve yanlış muhasebe uygulamalarının ortaya çıkarılması için bir adli muhasebe denetimi uygulanması ve değerlendirme bu uygulama ışında gerçekleştirilmelidir (Huber ve Glenn, 2009, ss. 3-5).

b) Birleşmeler ve Devralmalar

Bir şirketin diğer bir şirket ile birleşmesi veya bir şirketin devren satın alınması gibi durumlarda ciddi bir finansal analiz ihtiyacı ortaya çıkmaktadır. Eğer eşit düzeyde ve nitelikte şirketlerin birleştiği bir durum söz konusu ise taraflardan her biri diğer tarafın mali kayıtlarının incelenmesini talep ederek herhangi bir dolandırıcılık vakasının olup olmadığını kontrol etmek isteyebilmektedir. Şayet bir şirketin tek taraflı satış işlemi söz konusu ise, satın alan taraf, satın alınmak istenen şirketin tam olarak kapsamlı bir denetime tabi tutulmasını isteyebilmektedir. Bunlara ek olarak, adli muhasebeciler, defterlerin düzgün tutulup tutulmadığını tespit etmek için yatırım bankacıları tarafından da göreve davet edilebilmektedir. Bazı görüşler, adli denetim ve analizin, her birleşme ve devir işleminde, sürecin ayrılmaz bir parçası olması gerektiğini savunmaktadır. Adli muhasebe denetiminin kendine özel araç ve kabiliyetleri vardır ve geleneksel muhasebe yöntemleri ile tespit edilemeyen aksaklıkları ve dolandırıcılıkları bu araç ve yöntemlerle açıklığa kavuşturmaktadır (Grippio ve Ibex, 2008, s. 134). Adli muhasebe çalışmaları ve uygulamaları, tarafların her birinin güvenliğini artırmakta ve sürecin sorunsuz bir şekilde ilerlemesine katkıda bulunmaktadır. Gerçekten de devredilen şirketlerin, çalışanları tarafından devirden hemen önce suiistimal edilmesi görülen bir olgudur. Tam bir adli durum tespiti esnasında, önceki dolandırıcılık vakalarından ya da diğer benzer sorunlardan kaynaklanabilecek muhtemel sorunların belirlenmesi ve gelecekte vergi suçları gibi daha ağır sonuçlara neden olmadan

önlenmesi mümkündür. Bir adli muhasebeci, suç teşkil eden olayları ortaya çıkarmanın yanı sıra şirketlerin tahmini kazançları, mevcut borçları ve varlık değerleri ile ilgili bildirimlerin manipüle edilip edilmediğini ya da hatalı olup olmadığını da açığa çıkarabilmektedir. Böyle durumlar kimi zaman basit bir hatadan kaynaklanıyor olabilir de satış veya devir işleminde alıcı konumunda olan şirket teklifini buna göre düzenlemek isteyebilmektedir. Doğal olarak, satın alınmak istenen şirket, bir şekilde kedi değerini düşürmüş ve alıcı tarafa bir fırsat sunmuş gibi görünme yoluna da gitmek isteyebilmektedir. Bütün bunlara ek olarak, satın alınmak istenen şirket, alıcı tarafa yönelik bir adli muhasebe denetimi talep edebilmektedir. Eğer satın alınmak istenen şirket kaliteli bir ürün grubu ya da hizmet oluşturmak için çok çalıştıysa, şirketin zimmete para geçiren ya da dolandırıcılık suçu işleyen kimseler tarafından zarar görmesini ve hatta yok edilmesini istemeyecektir (Rouse ve Conway Jr., 2001, s. 18).

Sonuç olarak, bir şirket birleşmesi ya da devri söz konusu olduğunda adli muhasebeci durum tespit sürecinin vazgeçilmez bir parçasıdır ve sürece mutlaka dahil edilmelidir. Her iki tarafın selameti için etki olmayan durumlar, dolandırıcılık vakaları ve usulsüzlükler kontrol edilmeli ve böyle bir durum söz konusu ise muhakkak tespit edilmelidir.

c) Şirket Denetimleri

Standart denetimler, yanlış beyanları ortaya çıkarmak ve daha sonra gerek görülmesi halinde bunları raporlamak için tasarlanmıştır. Bu, ufak tefek düzensizliklerin gözardı edilebileceği ya da yok sayılabileceği anlamına gelmektedir. Öte yandan, adli muhasebe denetimi, bu düzensizliklerin doğasını tespit etmeye ve bir örüntü ortaya çıkarmaya çalışmaktadır. Zira, zeki bir dolandırıcı, uzun süre boyunca ufak miktarlarda para çekebilir ya da mal çalabilir ve böylece tipik bir denetimde yakalanmaktan kaçınabilmektedir (Özcan, 2019, s. 1746).

Bir adli muhasebe ekibinin esas amacı hırsızlık ve dolandırıcılık vakasını açığa çıkarmaktır. Bu doğrultuda, standart bir muhasebe denetimi ve analizinden farklı birtakım yöntem ve hedeflere sahiptirler. Adli muhasebeciler, bir şirketin gelecekte karşılaşması muhtemel sorunların önüne geçmek için suiistimal edilen zayıflıklar olup olmadığını tespit etmek adına finans ve BT sistemlerini derinlemesine bir analize tabi tutmaktadırlar. Bir adli muhasebeci, denetim sürecine başladığında birtakım yasadışı ve

etik olmayan uygulamaları araştırmaktadır. Bunlar şu şekilde sıralanabilmektedir (Bhasin, 2007, s. 1008):

- Hayali ya da şişirilmiş maaş bordroları
- Olduğundan daha az bildirilen gelirler
- Şüpheli kişilere, gayri resmî bağlantıları olabilecek alacaklılara yapılan aşırı ödemeler
- Nedensiz ve doğrulanamamış borçlar
- Yerli ve yabancı şüpheli şirketlere yönelik ödemeler veya para transferleri
- Herhangi bir gelir kaydı olmayan taraflarca yapılan şüphe uyandıracak derece büyük satın alımlar.

d) Sözleşme Uyuşmazlıkları (Anlaşmazlıklar)

Bir sözleşme taraflarının, sözleşmeden doğan mali yükümlülüklerini yerine getirmekten kaçındığı durumlar sıklıkla görülmektedir. Taraflar, sattıkları üründen elde ettikleri geliri ya da ürünün satış fiyatını gizleme yoluna gidebilmektedir. Eşit hisselere sahip ortaklar arasında eksik ödeme yapılması gibi durumlar da söz konusu olabilmektedir. Bunların yanında, bir şirket, başka bir şirket tarafından lisanslanmış ürünlerin nasıl kullandığını ve bu ürünlerden nasıl kazanç elde edebileceğini anlamak için çaba harcayabilmektedir. Adli muhasebeciler, sözleşme kapsamında tarafların ne kadar borca sahip olduğunu belirlemek için mali kayıtları ve diğer kayıtları inceleme konusunda etkin uzmanlardır (Menon ve P., 2016, s. 456).

Bu tür anlaşmazlıklar, çok sayıda çeşitli durumda ortaya çıkabilmektedir. Hatta bu anlaşmazlıkların çalışanlara yönelik ödemeler ve tazminatlarda dahi ortaya çıktığı görülmektedir. Öyle ki, bazen çalışanlar yıllık maaşlarının büyük bir kısmını ikramiye olarak almaktadır. Bu ödemeler, çalışanların kendi başarılarına göre belirlenebildiği gibi çalışanların bağlı olduğu departmanın ya da bir bütün olarak şirketin başarısına göre de belirlenebilmektedir. Çalışanlar, görünüşte eksik olan ikramiye çeklerinin, eksik bildirilen şirket gelirlerinin bir sonucu olduğunu düşündüklerinde adli muhasebe denetimi talep ederek bu eksikliğin giderilmesini isteyebilmektedirler (Menon ve P., 2016, s. 456). İkramiye ödemelerini etkileyen dolandırıcılık vakalarının standart muhasebe yöntemleri ile belirlenmesi kimi zamanlarda mümkün olmamaktadır.

Sözleşme uyuşmazlıklarının büyümesi ve mahkeme önüne taşınması halinde, bir adli muhasebeci bilirkişi olarak ayrıntılı ve objektif bir görüş bildirebilmektedir. Bazı durumlarda, taraflar hem adli muhasebeciden hizmet alımına gidebilmekte hem de avukatların mahkeme heyeti önünde görüşülmesi gereken davalarda çelişkili ifadelerde bulunabilmektedir.

Bir adli muhasebeci, sözleşme hukuku ve suç konusunda yeterli bilgi sahibi olduğunda, sözleşme uyuşmazlıklarının asıl nedenlerini açığa çıkarabilmektedir. Örneğin, taraflardan birinin, sözleşmeden doğan yükümlülüklerini yerine getirmekten kaçınmak için fon ve gelirleri eksik ya da fazla rapor etmesi halinde, bir adli muhasebe ekibi bu durumu derinlemesine ele alabilmektedir. Adli muhasebeciler, geleneksel muhasebecilerin sağlamadığı bir yaklaşımı benimseyerek vakaları farklı bir şekilde ele alabilmektedir. Adli muhasebeciler, mali usulsüzlüklerle ilgili kalıpları ve temel unsurları araştırarak, mahkeme heyeti de dahil olmak üzere ilgili tarafları tam ve eksiksiz bir şekilde bilgilendirmektedirler (Dhar ve Sarkar, 2010, s. 98).

e) Sigorta Talepleri

Şirketler ve bireyler, kimi zamanlarda, sahip oldukları fiziksel ve gerçek varlıklarının değerini olduğundan fazla göstererek, bu gerçek dışı rakamları sigorta taleplerine dahil edebilmektedir. Bununla birlikte, taraflar, bir dolandırıcılık davası üzerinden çıkar sağlamaya çalışabilmekte, bir dolandırıcılık ya da hırsızlık vakasından dolayı gerçek değer çok üzerinde bir kayıp ile karşı karşıya kaldıklarını iddia edebilmektedir. Adli muhasebeciler, mali kayıtlardaki desenleri inceleyebilmekte ve iddiaya konu olan gerçek değeri tespit edebilmektedir. Ayrıca, sigorta şirketlerinin tazminat ödemekten kaçındığı haller de söz konusu olabilmektedir. Sonuçta, birincil gayeleri talebe dair ödeme miktarını en düşük düzeye indirmektedir. Örneğin, bir yangın ya da başka bir doğal afet halinde bir kişi ya da bir şirket tüm kayıtlarını kaybedebilmektedir. Böyle bir durumda sigorta şirketleri bu durumdan yararlanmaya çalışabilmekte ve sözleşmeden kaynaklanan yükümlülüklerinin tamamından ziyade bir kısmını ödeme yoluna gidebilmektedir. Adli muhasebeciler, mali belgeleri yeniden oluşturmak ve böylece davacının mahkemeye sunduğu iddiaları desteklemek için avukatlar tarafından danışman olarak işe alınabilmektedir. Adli muhasebecinin elde

ettiği kanıtların sıklığı ve inandırıcılığı doğrultusunda sigorta şirketlerinin kimi zamanlarda davadan çekildikleri de görülmektedir (Baker Tilly, 2018).

Geleneksel muhasebeci, sigorta dolandırıcılığı ya da etik olmayan uygulamalarla ilgili bir soruşturma becerisine ya da eğitimine sahip değildir. Maalesef, bir şirketi ya da bireyi dolandırmaya çalışan ve dezavantajlı durumundan yararlanmaya çalışan kişiler var oldukça, adli muhasebecilere olan ihtiyaç da gerekliliğini sürdürecektir (Silverstone ve Michael, 2007, s. 62).

f) Zimmet (Yolsuzluk) Vakaları

Zimmete para geçirme suçunu işleyen kişiler günden günde bu suçu daha akıllıca işlemektedir ve yakalanmaları da daha zor bir hal almaktadır. Suçların sabit olduğu ve apaçık görüldüğü hallerde dahi standart muhasebe yöntemleri bu suçluları yakalamakta yetersiz kalabilmektedir. Serbest muhasebecilerden bu dolandırıcılık suçlarının açığa çıkarılmasının talep edildiği vakalar olsa da serbest muhasebeciler bu bağlamda profesyonel bir tutum sergileyememektedir. Bu nedenle muhtemel bir dolandırıcılık ya da zimmet suçu ile karşı karşıya kaldığını düşünen bir şirket, bu suçun soruşturulmasına yönelik bir gereksinim duyduğunda mutlaka bir adli muhasebe ekibi ile iletişime geçmeli ve onların sunduğu hizmetlerden yararlanmalıdır. Örneğin, bir yönetici tarafından düzenli bir şekilde çok yüklü meblağları zimmetine geçirdiği ve bunu yapmak için bariz yöntemler kullandığı hallerde bile standart muhasebe ekipleri bu suçu açığa çıkarma konusunda yetersiz kalabilmektedir. Bu yönetici, kendine verilen standart ve vergilendirilmiş bir maaş çeki yerine bir gider hesabından ödeme yapabilmektedir. Ayrıca yönetici, şirket kurallarını ihlal ederek, müşteri ödemelerini nakit olarak kabul edebilir ve belgelendirmediği bu ödemeleri zimmetine geçirebilir ve hatta şirketin hesapları üzerinden bir sanat eseri satın alarak bunu kendi evine taşıyabilir. Israrcı çalışmalar yürüten bir adli muhasebe ekibi, tüm bu suçları belgeleyebilmekte ve soruşturmayı başarılı bir şekilde sonuçlandırabilmektedir (Dorrell ve Gregory , 2012, s. 462).

Şirketlerin hepsi için düzenli bir standart muhasebe denetimi önerilse de bu denetimleri bir adli muhasebe ekibi devraldığında çok daha fazla usulsüzlük tespit edilebilmektedir. Yukarıda verilen örnek her ne kadar kötü bir durum gibi görülsün de söz konusu vaka, gerekli kanıtların adli muhasebe ekibi tarafından bulunduğu, işlenmiş

bir suçtur. Elbette, bundan daha az belirgin bir şekilde gerçekleştirilen usulsüzlükler de vardır. Dijital para transferlerinin, şifreli hesapların ve pek çok sayıda kötü niyetli bilgisayar korsanlığının gerçekleştiği günümüzde, adli muhasebecilere yönelik ihtiyaç da giderek artmaktadır (Golden vd., 2006, s. 41).

g) Hukuk Davaları

Adli muhasebecilerin asli görevi, mahkeme önünde görülen davalara kanıtlar sağlamak ve bilirkişi görüşü bildirmektir. Adli muhasebeciler; vergi kayıtları, borç işlemleri ve yabancı bankalar üzerinden gerçekleştirilen para transferleri de dahil olmak üzere mali kayıtları araştırmak üzere avukatlar ve kolluk kuvvetleri ile birlikte çalışmak için eğitilmiş uzmanlardır. Adli muhasebeciler, zimmete para geçirme, varlık enflasyonu ve kara para aklamadan kaynaklanan mali desenleri tespit etme hususunda bilgi sahibidirler. Adli muhasebeciler, genellikle, bir şirketin genel sağlığını değerlendirebilen ve güvenlikle ilgili tavsiyelerde bulunabilen bağımsız danışmanlık firmaları için çalışmaktadır. Adli muhasebecilerin gerçekleştirdikleri denetlemeler, serbest muhasebeciler tarafından gerçekleştirilen denetlemeler kadar geçerlidir, ancak dolandırıcılık ve diğer suçların söz konusu olduğu hallerde genellikle bir adli muhasebe denetimi gerekli olmaktadır (Oyedokun, 2013, s. 9).

h) Miras Anlaşmazlıkları

Çok büyük mülklerin miras kaldığı durumlarda, ilgili taraflar kendilerine düşen miras paylarından daha fazlasını alma hakkında sahip olduklarını düşünebilmektedir. Ayrıca, ailenin bazı üyeleri, vasiyetname üzerinde belirlenen kimi varlıkları gizlemek için diğer aile üyelerine yönelik usulsüz bir plan kurmuş olabilmektedir. Bu durum, bilhassa mülk üzerinde ismi geçen ancak mirasın tamamı hakkında bilgi sahibi olmayan çocuklara yönelik olabilmektedir. Miras bölüşümü zaman geldiğinde, vefat eden kimsenin mali çizelgeleri, vasiyeti ya da diğer mali bilgileri son derece karmaşık ya da anlaşılmasız bir halde olabilmektedir. Belirli varlıkların değeri, vasiyetnamenin hazırlanmasından sonra miras paylaşımına kadar olumlu ya da olumsuz yönde değişmiş olabilmekte ve bu değerler vasiyetnamede adı geçen kimselerin beklentilerini karşılamayabilmektedir. Ayrıca, vasiyeti uygulayan kimse kötü niyetle hareket edebilmekte ve varlıkları yanlış bir şekilde tanımlayıp tanıtarak kendine çıkar sağlama yoluna gidebilmektedir (Anderson, 2016).

Büyük mülklerin el değıştirmesi esnasında, emlak konusunda uzmanlaşmış avukatların hazır bulunmasının yanı sıra mülkü bir bütün olarak analiz edebilecek ve en adil paylaşım yolunu tespit edebilecek adli muhasebecilerin de sürece dahil edilmesi hayati önem taşımaktadır. Anlaşmazlığın söz konusu olmadığı hallerde dahi, mülk paylaşımı için bir adli muhasebeciden hizmet almak taraflar için çok daha iyi olabilmektedir (Maddox, 2019).

Netice itibarıyla küreselleşen dünyamızdaki teknolojik gelişme dikkate alındığında yeni meslekler ve yeni uzmanlık alanları ortaya çıkmıştır. Bu meslekler ve meslekler bilgi ve tecrübeyi birbirleriyle paylaşmalıdır. Özellikle muhasebe ve hukuk gibi karmaşık disiplinlerde profesyoneller arasında konularda bilgi ve deneyim paylaşımı profesyonellerin bir zorunluluk haline gelmiştir. Bu gereklilik aynı zamanda adli muhasebe ve adli muhasebe mesleklerini de doğurmuştur. "Adli " terimi "mahkemelerde kullanıma uygun" anlamına gelir. Adli muhasebeciler genellikle bu standart dahilinde çalışır ve davalarının sonuçları mahkemelerde karara bağlanır. Adli muhasebeciler, adli denetçileri veya araştırmacılar / soruşturma denetçileri olarak da bilinir ve genellikle adli duruşmalarında uzman görüşleri sunarlar. Adli muhasebe, "mali sorunları mahkemenin gerektirdiği standartları karşılayacak şekilde çözmek için soruşturma ve analitik becerilerin kullanılması" olarak tanımlanır. Adli muhasebeciler ya da bir başka ifade ile dolandırıcılık denetçileri, bu işi yapmalarını sağlayan çeşitli beceriler ile donatılmış uzmanlardır. Adli muhasebeciler güçlü yazılı ve sözlü iletişim becerilerine sahip olmalıdır. Bu meslekte güçlü bir muhasebe alt yapısına sahip olmak zorunluluk arz etmektedir. Adli muhasebeci, denetim, risk değerlendirmesi, kontrol, dolandırıcılık tespiti gibi hususlarda kapsamlı bilgi sahibi olmalı ve ayrıca hukukun temel ilkeleri hakkında yeterli bilgi sahibi olmalıdır.

İKİNCİ BÖLÜM

BLOCKCHAIN VE KRİPTO PARA

Blockchain, (diğer şeylerin yanı sıra) kripto para biriminin varlığını sağlayan teknolojidir. Bitcoin, blockchain teknolojisinin icat edildiği en iyi bilinen kripto para biriminin adıdır. Bir kripto para birimi bir değış tokuş (takas) aracıdır, ancak dijitaldir ve parasal birimlerin oluşturulmasını kontrol etmek ve fon transferini doğrulamak için şifreleme tekniklerini kullanır.

2.1.Blockchain Tanımı

Blockchain kavramı ilk olarak 2009 yılında, ses dosyaları, görüntü dosyaları ve metin belgeleri gibi kolayca değıştirilebilen dijital varlıkların zaman damgalama ile ilgili teknolojik sorununa yönelik bir çözüm ihtiyacı için ortaya atılmış ve kavramsallaştırılmıştır. Blockchain teknolojisi ile bir dosyanın ne zaman oluşturulduğunu ve ne zaman değıştirildiğini izlemek mümkün olabilmektedir (Gupta, 2017, s. 3). Bu teknoloji de tıpkı internet gibi, daha ucuz, daha kolay, daha güvenli ve daha verimli iş süreçlerinin gerçekleştirilmesini sağlamaktadır. “*How to timestamp a digital document (bir dijital belgeye zaman damgası nasıl yapılır)*” başlıklı bir makalede, bu teknolojik soruna yönelik bir çözüm önerilmiş ve bir dosyanın ne zaman oluşturduğunu ve ne zaman değıştirildiğini izlemek için verileri kaydederken yardımcı bir yöntem olarak geliştirilen Blockchain teknolojisi açıklanmıştır (Stornetta ve Haber, 1991, s. 102).

Blockchain’in ilk pratik uygulaması olan Bitcoin adlı elektronik para sistemi 2009 yılında ortaya çıkmıştır. Bitcoin, Satoshi Nakamoto takma adı ile anılan bir kişi veya topluluk tarafından oluşturulmuştur. “Bitcoin: A peer-to-peer electronic Cash System” (Bitcoin: Uçtan uca elektronik nakit sistemi) başlıklı makalede, Bitcoin’in temelinde yatan fikir, Bitcoin kavramı ve Bitcoin’in nasıl kullanılacağı anlatılmış, dijital para

işlemlerini izlemek ve doğrulamak için ise Blockchain bir mekanizma olarak önerilmiştir. Blockchain, dijital bilgileri oluşturan ve paylaşan, halka açık, bir dağıtık defter olarak tanımlanmakta ve esasen gerçekleştirilen dijital işlemlerin bir kaydını oluşturmaktadır. Blockchain'in halka açık bir defter olması, tek bir tarafa ait olmadığı veya kontrol edilemediği anlamına gelmektedir. Bunun yerine, ağ üzerindeki kontrol kullanıcılar arasında dağıtılmaktadır. Bu durum, bilgilerin ağdaki herkes tarafından görülebilmesinden kaynaklanmaktadır (Nakamoto, 2008, s. 3).

Banka veya hükümet gibi resmi bir otorite veya kurum, finansal kurumlar arasında gerçekleştirilen işlemleri kaydetme sorumluluğuna sahiptir. Bir dağıtık hesap defteri olan Blockchain'de ise merkezi bir kontrol ya da kayıt birimi ihtiyacı ortadan kalmaktadır, çünkü işlemler günlük dosyalarında kayıt altına alınmakta ve ağ kullanıcıları tarafından doğru ve kesin bir şekilde doğrulanmaktadır. Burada, güvenilir bir üçüncü taraf yerine bilgilerin depolanması yoluyla kullanıcılara belirli verilerin kanıtını sağlayabilen ve güvenilir bir defter oluşturmaları için birbirini tanımak ya da birbirine güvenmek zorunda olmayan kişilere izin veren bir Blockchain devreye girmektedir (Lazanis, 2015). Underwood'un 2016 yılında gerçekleştirdiği çalışmasında bahsettiği üzere, burada işlemleri onaylayan veya kaydeden merkezi bir birim yoktur. Ancak tüm bilgiler, bütün kullanıcıların erişebildiği Blockchain sisteminde saklanmaktadır. Kullanıcılar bilgiye kendileri erişim sağlayabildiklerinden dolayı artan bir güven oluşmakta ve aracı bir birim dahil etme ihtiyacı tamamen ortadan kalmaktadır (Underwood, 2016, s. 15).

Blockchain, Bitcoin ağında gerçekleşen her işlemi kaydeden, çift harcama problemini ortadan kaldıran, bir aracı birim yerine işlev gören ve sıralı işlem grupları içeren bir dizi bloktan oluşan halka açık bir dağıtık defterdir. Blockchain, "yükseklik" olarak adlandırılan mesafeyle "herhangi bir bloktan ilk bloğa uzanan en uzun yol" olarak tanımlanmaktadır. Çift harcama saldırılarına, işlem gücünün ağ kullanıcıları arasında paylaşıldığını ve çoğunun dürüst olduğunu varsayan dağıtık iş kanıtı tabanlı bir hizmet kullanılarak karşı konulmaktadır. Şu anda Blockchain yaklaşık 285 GB büyüklüğündedir (Blockchain.com, 2020).

Blockchain teknolojisi birçok uygulama içerisinde ayrı ayrı ele alınmaktadır, ancak, içsel işlevi ve değeri "güvenilir bir üçüncü tarafa" gerek kalmaksızın birbirlerine

güvenmek zorunda olmayan taraflar arasında gerçekleştirilen işlemlerin matematiksel olarak kanıtlanabilir olmasını sağlamaktır. Bitcoin'in imgesel (takma ad kullanılan/anonim) doğası, daha kişisel tanımlamaların aksine takma adlardan oluşan Bitcoin adreslerine atıfta bulunan bu dağıtık defter yaklaşımına dayanmaktadır. Bitcoin adresleri, “doğrudan eliptik eğri genel anahtarlardan türetilmiş” yapıdadırlar ve bir kullanıcı rutin olarak tamamı cüzdanları tarafından yönetilen yüzlerce farklı adrese sahip olabilmektedir.

Her bir blok, önceki bloğun bir SHA-256 sağlamasını (hash) içermektedir. Bu, blokları bir diziye bağlamakta ve blok zincirini oluşturmaktadır. Burada, ilk bloğa (genesis) kadar olan tüm yol izlenmektedir.

2.2.Blockchain Kullanım Alanları

Bitcoin'in popülaritesi, blockchain'in finanstaki uygulamasının gösterilmesine yardımcı oldu, ancak girişimciler, teknolojinin çok daha fazla sektörü dönüştürebileceğine inanmaya başladılar. Günümüzde şirketler dijital bilgi ekosisteminde daha fazla şeffaflık ve doğruluk sağlamak için blockchain kullanıyor, altyapıdan kamu politikasına kadar çeşitli sektörlerde teknoloji farkındalığını artırıyorlar. Aşağıda, şirketlerin blockchain'in gücünden yararlanmanın en son yenilikçi yollarından bazıları yer almaktadır.

2.2.1.Bitcoin ve Blockchain

Blockchain'in en yaygın kullanılan uygulaması bir kripto para birimi olan Bitcoin'dir. Bitcoin, merkezi olmayan bir dijital para birimi olarak tanımlanabilmektedir (Nakamoto, 2008, s. 1). Yani, Bitcoin'in çalıştırıldığı merkezi bir sunucu yoktur, bankalar ve hükümetler gibi hiçbir kurum ya da kişi Bitcoin'i desteklememekte ve kontrol etmemektedir (Nofer vd., 2017, s. 185). Franco'nun 2014 yılında yayınladığı çalışmasında belirtildiği üzere, kripto para biriminin en yenilikçi özelliklerinden biri olan Bitcoin, merkezi olmayan bir şekilde inşa edilen ilk dijital para birimidir. Bitcoin, tüm bitcoin işlemlerinin güvenli bir şekilde bir deftere depolanıp, kaydedilip ve doğrulanarak çalıştırıldığı, düğüm adı verilen bağlı bilgisayarın eşler arası uçtan uca oluşturduğu ağ temelinde şekillendiğinden, “tamamen uçtan uca bir elektronik para versiyonu” olarak tanımlanabilmektedir. Geleneksel ödeme yöntemleri ile kıyaslandığında, Bitcoin'in en büyük avantajının, herhangi bir merkezi birim veya

otorite tarafından kontrol edilmediği için, kullanıcıların herhangi bir üçüncü tarafa güvenmek zorunda kalmamaları olduğu söylenebilmektedir (Franco, 2014, s. 96). Geleneksel finansal sistemlerde, finansal kurumlar, değerin / varlığın temsil edildiği veritabanlarını (defterleri) yöneten kurumlardır. Kullanıcılar, bu finans kuruluşlarının veritabanlarının içeriden veya dışarıdan herhangi bir saldırıya maruz kalmadığı müddetçe bu kurumlara güven duymaktadırlar. Öte yandan, Bitcoin, kendi veritabanını halka açık hale getirmekte ve ağa zarar vermek isteyen saldırganlara karşı koyacak bir biçimde tasarlanmış, açık kaynak kodlu bir yazılım protokolü oluşturmakta ve böylece kendini güvence altına almaktadır (Segendorf, 2014).

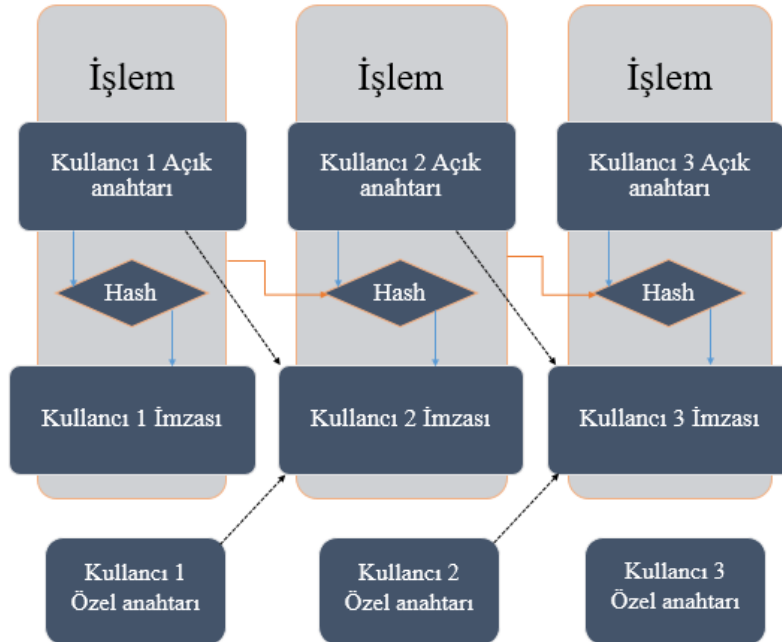
Bitcoin'in bir diğer faydası da para transferi işlemlerinin diğer para birimleriyle yapılan işlemlere veya ödemelere göre daha hızlı ve daha ekonomik olması ve ayrıca kullanıcılara ve işlemlere anonimlik sağlamasıdır (Göbel vd., 2016, s. 1). Bitcoin ağında gerçekleştirilen işlemlerin ardında saklı olan kimlikler dışında, ağdaki bütün bilgiler herkese açıktır. Bitcoin, herhangi bir fon sahibini tanımlamak için kişisel bilgilerini kullanmak yerine onların Bitcoin adreslerini kullanmaktadır. Bitcoin gönderme işleminin gerçekleştirilmesi için yalnızca alıcının Bitcoin adresinin bilinmesi yeterlidir. Bu adresler bir tür takma ad olarak kabul edilebilmektedir. Bu adresler genel – özel şifreleme anahtarının genel kısmıdır. Anahtarın özel kısmı ise kullanıcının kontrolü altındadır ve gizlidir. Ancak, bütün bunlara ek olarak belirtmek gerekir ki, Bitcoin, diğer ödeme sistemlerini düzenleyen yasaların kapsamına dahil olmadığından dolayı, Bitcoin kullanımı birtakım riskleri de beraberinde getirmektedir. Bitcoin üzerinde bir tüketici koruma mekanizmasının etkin olmaması, Bitcoin'in kabul edilebilir ve uygulanabilir bir ödeme aracı olarak görülmemesine yol açabilmektedir (Barski ve Wilmer, 2014, s. 118).

Bitcoin, bir dağıtık veritabanı olan Blockchain üzerine inşa edilmiştir. Bu veritabanı, geçmişte gerçekleştirilen tüm işlemleri ve mevcut fon sahiplerini bünyesinde kayıtlı tutmaktadır. Sistem, fon sahiplerini temsil eden girişleri de tuttuğu için defter olarak da adlandırılabilir. Birkaç kriptografik yapı kullanarak, Bitcoin, dağıtık veritabanı üzerinde bilgileri bir araya getirerek bir bilgi bütünlüğü oluşturabilmektedir. Bu, saldırılara karşı koruma sağlamak ve yeni Bitcoinlerin ihracını gerçekleştirmek için büyük miktarda hesaplama gücü kullanılarak yapılmaktadır. Blockchain'i güvence altına alan kişilere “madenci” adı verilmektedir. Bu kişiler, özel bir yazılım kullanarak, Blockchain'e eklenen işlem bloklarını oluşturmak için birbirleri ile rekabet

içerisindedir. Bir madenci, matematik problemlerini çözerek bu bloklardan birini oluşturduğunda, yeni basılan ve ihraç edilen Bitcoinlerden oluşan bir blok ödülü elde etmektedir (Franco, 2014, s. 16).

Bitcoin ağında bir işlemin nasıl yönetildiğine bir örnek vermek gerekirse: Bir kullanıcının (X), bir diğer kullanıcıya (Y) para transferi yaptığını varsayalım. Ağdaki her kullanıcı, kendi fonlarını kontrol eden bir kriptografik özel anahtara sahiptir. Bu nedenle para göndermek isteyen X kullanıcı öncelikle “1gr6U6... adresine 1 Bitcoin göndermek istiyorum” mesajını imzalamak için kendi anahtarını kullanmaktadır. Bu imzalı mesaj, ağdaki her bir katılımcının bir kopyasını aldığı bir mesaj olarak ağ üzerinde yayınlanır. X’in bu mesajı alındığında, ağdaki düğümler temel olarak üç adım izlemektedir. İmza doğru ise mesaj onaylanır, eğer imza doğru değil ise mesaj reddedilir. Gönderen adresin işlemleri tamamlamak için yeterli paraya sahip olup olmadığı+ kontrol edilmekte ve eğer kullanıcının bakiyesi söz konusu işlemin gerçekleştirilmesi için yeterli değilse işlem geçersiz sayılmaktadır. Son olarak, fon bir adresten çıkarılıp diğer adrese yatırılmaktadır ve son adımda veritabanı bu yeni bilgiler ile güncellenmektedir.

Şekil 02.1: Bitcoin işlem hareketi



Kaynak: (Gültekin ve Bulut, 2016, s. 85)

2.2.2. Akıllı Sözleşmeler ve Blockchain

Akıllı sözleşmelerin birkaç farklı tanımı vardır. Arama, müzakere, taahhüt, yürütme, bakım, performans ve karar (yargı) süreci, sözleşme sürecinin tüm adımlarıdır (Szabo, 1994). Mougyar (2015) yılında yaptığı bir çalışmada, akıllı sözleşmeleri, zaman damgası, iş teslimine dair kanıtlar, emanet, bahisler ve aile mutemetliği gibi bir dizi uygulama alanıyla bir tür ademi merkeziyetçilik ya da yetki dağıtımı olarak tanımlamaktadır. Bir akıllı sözleşmenin temelinde yer alan ana fikir, birkaç taraf arasında yapılan bir anlaşmanın, Blockchain kullanılarak otomatik doğrulanmasıdır. Akıllı sözleşmeler, kanunlara dayanmak yerine, matematik tabanlı oluşturulan sözleşmelerdir ve bu tür sözleşmelerden kaynaklanan ödemeler tamamen bir bilgisayar programı aracılığı ile gerçekleştirilmektedir. Bir akıllı sözleşmenin amacı, bir taraftaki varlıkların diğer tarafa aktarılmasıdır. Burada, sözleşme, otomatik olarak yürütülebilen ve uygulanabilen bir dijital sözleşme olarak hareket etmektedir (Mougayar, 2015).

Akıllı sözleşmelerin amacı, anonim olan iki tarafın, merkezi bir kontrol birimi ya da bir kural koyucu gibi herhangi bir aracıyı sürece dahil etmeksizin iş yapabilmelerine imkân sağlamaktır.

Geleneksel ve basılı sözleşmeler, doğrulama için üçüncü bir tarafın varlığını gerektirmektedir. Dolayısıyla bu tür bir sözleşmenin hazırlanması ve yürürlüğe konulması çok zaman alabilmektedir. Ayrıca, herhangi bir anlaşmazlığın söz konusu olduğu hallerde, çözümün genellikle bir üçüncü taraf aracılığıyla sağlanması gerekli olduğundan, sorunların çözümü maliyetli bir hal almaktadır ve uzun sürmektedir. Sayısallaştırılmış akıllı sözleşmeler, zamanla değişen koşulları, ortaya çıkabilecek olası sorunları ve muhtemel sonuçları tanımlayan kodlara dayanmaktadır. Bu nedenle, tarafların üzerinde mutabık kaldığı sözleşme şartları yerine getirildikçe sözleşmeyi oluşturan kodlar otomatik bir şekilde işlemleri gerçekleştirmektedir (Powazka, 2017) (Szabo, 1994).

Stark, 2016 yılında yayınladığı bir çalışmada, akıllı sözleşmeleri, akıllı sözleşme kodları ve akıllı yasal sözleşmeler olarak ikiye ayrı bölümde ele almaktadır. Akıllı sözleşme kodu, bir Blockchain bloğu üzerinde doğrulanan, çalıştırılan ve saklanan belirli bir teknoloji kodunu ifade etmekten, akıllı yasal sözleşme ise belirli bir

uygulama için yasal sözleşmelerim tamamlayıcısı ya da ikamesi olarak tanımlanmaktadır (Stark, 2016).

Akıllı sözleşmeler, özellikle finansal araçlar için tercih edilebilir sözleşme türleri olduğundan dolayı finans piyasalarında büyük bir ilgi ile karşılanmıştır. Akıllı sözleşmelere yönelik olumlu yaklaşımlara karşın birtakım zorlukları da beraberinde getirdiğini belirtmek mümkündür. ENISA tarafından 2016 yılında yayınladığı bir çalışmada, akıllı sözleşmelerin temelde bir dağıtık defter üzerinde çalışan programlar olduğunu ve dolayısıyla muhtemel kod hatalarından etkilenmeye müsait olduklarını ifade etmiştir. Bir akıllı sözleşme ne kadar karmaşık yapılı ise yazılım hatalarına da o kadar eğilimli olmaktadır. Akıllı sözleşme kodlarının işlevi ve güvenliği genellikle kod yazan kişilerin yeteneklerine bağlıdır (The European Union Agency for Cybersecurity-ENISA, 2016, s. 12).

2.2.3. Finans Sektöründe Blockchain Kullanımı

Blockchain teknolojisi, finans sektöründe, uluslararası işlemlerin güvenliğinin sağlanmasında, verimliliğin artırılmasında ve maliyetlerin düşürülmesinde kullanılabilmektedir. Bu teknoloji ayrıca ödeme işlemleri için kullanılabilmekte, operasyonel verimliliği artırabilmekte ve bankaların maliyetlerini düşürebilmektedir. Blockchain ödemeleri, tam bir şeffaflık, düşük maliyet ve gerçek zamanlı dolandırıcılık analizi ile etkin bir koruma sağlamakta ve işlemlerin gerçek zamanlı olarak gerçekleştirilmesini sağlamaktadır (FinTech Network, 2018). Visa Europe Collab ve BLT Group, finansal hizmet ekosistemi içerisinde Blockchain teknolojisinin potansiyel uygulamalarını keşfetmek üzere çeşitli projeler üzerinde çalışmaktadır. Bu projeler bilhassa bankalar arasında gerçekleştirilen yurtiçi ve uluslararası ödemelerde yaşanan sorunları azaltan Blockchain tabanlı bir uzlaştırma çözümü üzerinde yoğunlaşmaktadır. Böylece, maliyetleri, kredi risklerini ve ödeme süresini azaltarak, yurtiçi ve uluslararası ödemelere yönelik düzenleme ve uyumluluk gerekliliklerinin düzenlenmesi ve otomatikleştirilmesi amaçlanmaktadır (Surane, 2016).

NASDAQ ve İsveç'te bulunan bir Finans Kurumu olan SEB, 2017 yılında Blockchain Teknolojisine dayalı yatırım fonu ticaret platformları için bir prototip geliştirmek ve test etmek için ortak bir proje yürüteceklerini duyurmuştur. Zira, günümüzde kurumlar söz konusu alandaki işlemleri, manuel rutinler, kâğıt üzerinde

gerçekleştirilen süreçler ve uzun yerleşim döngüleri ile gerçekleştirmektedir. Bu projenin amacı, fon birimlerinin alım – satım sürecinde verimlilik artırımının sağlanması ve tek bir birim defterinin oluşturulmasıdır (GlobeNewswire-GN, 2017).

2.2.4. Gayrimenkul Sektöründe Blockchain Kullanımı

Blockchain Teknolojisi, gayrimenkul sektörü ve emlakçılık mesleğinde gerekli belge ve işlemlerin gerçekliğini kanıtlamak ve mülk alım – satım işlemlerinin verimliliğini ve güvenliğini artırmak için uygulanabilmektedir. Mülkiyete dair işlemler, hayli büyük miktarlarda işlemleri içeren ve yüksek güvenlik ile şeffaflık gerektiren bir alandır. Deloitte, 2016 yılında yayınladığı bir çalışmada, gayrimenkul sektöründe Blockchain teknolojisinden yararlanılabilecek üç alan belirlemiştir. Bu alanlar; şeffaflığın artırılması, dolandırıcılık riskinin en aza indirilmesi ve mülk alım – satım süreçlerinin hızlandırılması olarak sıralanmaktadır (The Deloitte Center for Financial Services, 2017, s. 3).

2.3. Blockchain'in Muhasebe Sistemleri Üzerindeki Etkisi

Blockchain iş fırsatlarını keşfeden daha fazla şirket ile birçok muhasebe firması, bu önemli ve çok yönlü teknolojinin sonuçlarını daha da anlamak için Blockchain'in girişimlerini üstlendi. Denetçiler ve muhasebeciler gelişmelerden haberdar olmalı ve blockchain iş uygulamaları, muhasebede blockchain ve blockchain denetim teknolojisi hakkında daha fazla bilgi edinmeye devam etmelidir (Deloitte Consulting GmbH, 2016, s. 2).

2.3.1. Blockchain Çağında Muhasebe

Blockchain, kavramsal olarak bir defterin güvenilirliğinin, onu koruyan merkezi denetçilerden kaynaklandığı bir noktadan, kayıt tutmayı yönlendiren sisteme duyulan güvenden türetildiği bir noktaya doğru gerçekleşen harekettir. Üstelik bunun yanında, işlemleri kendiliğinden yürüten akıllı sözleşmeler için var olan potansiyel, tüm sözleşmelerin işleyişini temelden etkileyebilecek programlanabilir bir defterin oluşturulmasına izin vermektedir (Beck vd., 2017, s. 382).

Olası teknolojik engellerin tamamının aşıldığı varsayılırsa, Blockchain'in büyük bir potansiyele sahip olduğu söylenebilmektedir. Akıllı sözleşme işlevselliği bir yana, yalnızca Blockchain kabiliyetleri göz önünde bulundurulduğunda, tam anlamıyla

gerçekleştirilecek bir Blockchain uygulamasının finansal sistemdeki aracı kurumların büyük bir kısmını saf dışı bırakacağı görülebilmektedir. Birbiri ile karşılıklı işlemler gerçekleştiren gruplar arasındaki özelleştirilmiş Blockchain uygulamaları; bankalar, takas kurumları ve avukatlar gibi merkezi otorite unsurlarının yerini alabilmektedir. Doğrudan etkileşim yeteneği ve asla mutabakat gerektirmeyen tek bir defter aracılığı ile işletmeler, hem genel muhasebe giderlerinden hem de uzlaşma çabalarından tasarruf edebilmektedirler. Böyle durumlarda belirsizliğin ortadan kaldırılması, ekonomiyi daha düzenli bir hale getirmekte ve kararlara yönelik güven artışını destekleyerek ekonomiye büyük bir katkı sağlamaktadır. Dahası, eğer şartlar elverişli ise, vergi dairesine ya da benzer bir gözetim otoritesine bu tür Blockchain uygulamalarını görüntüleme erişimi sağlanarak işlemleri gerçek zamanlı olarak gözlemelerine ve takip etmelerine izin verilebilir. Bu tür bir yaklaşım, maliyetlerde azalmaya, düzenleme ve uyumluluk faaliyetlerinin verimliliğinde ise artışa imkân sağlayabilir. Bir Blockchain uygulamasının kalıcı kaydı, finansal suç olasılıklarını azaltmakta, böylece kayıtları ve işlemleri daha güvenli bir hale getirebilmektedir (Fullana ve Ruiz, 2020, ss. 16-17).

Blockchain bir muhasebe teknolojisidir. Öyle ki, bu teknoloji, varlıkların mülkiyetlerinin devri ve doğru finansal bilgilerin yer aldığı defter kayıtlarının tutulması ile ilgilidir. Muhasebecilik mesleği ise genel olarak finansal bilgilerin değerlendirilmesi, bildirimi ve analizi ile ilgilenen bir alandır. Bu meslek, büyük ölçüde, mülkiyet üzerindeki hak ve yükümlülüklerin tespiti, ölçümü ve finansal kaynakların en iyi şekilde tahsisinin planlamasını ele almaktadır. Blockchain'in muhasebeciler tarafından kullanılması, varlıkların mülkiyeti ve yükümlülükler hususunda netlik sağlayabilmekte ve verimliliği büyük ölçüde artırabilmektedir (Deloitte Consulting GmbH, 2016, s. 3).

Blockchain, muhasebecilerin, şirketlerin mevcut kaynakları ve yükümlülükleri hakkında daha doğru bilgilere sahip olmasını sağlayabilmekte ve ayrıca onların, kayıt tutma yerine planlama ve değerlendirmeye odaklanmak için daha fazla kaynağa sahip olmasına imkân tanıyabilmektedir. Makine öğrenimi gibi diğer otomasyon eğilimlerinin yanı sıra, Blockchain, giderek daha fazla ve daha üst düzey muhasebe işlemlerinin yapılmasına imkân tanıyabilecektir ancak bu kez bu işlemleri yapanlar muhasebeciler olmayacaktır. Muhasebeciler, bunun yerine, Blockchain kayıtlarının reel ekonomik durumlarını değerlendirmek ve yorumlamak, kayıtları gerçek durum ile eşleştirmek ve birleştirmek gibi işlemleri yapan uzmanlar haline geleceklerdir. Örneğin, Blockchain,

bir borçlunun varlığını tespit edip açık ve net bir şekilde tanımlayabilmektedir, ancak, bunun geri kazanım değeri ve ekonomik değeri halen tartışmalıdır. Buna ek olarak, bir varlığın mülkiyeti Blockchain kayıtları ile doğrulanabilmekte ancak varlığın durumunun, konumunun ve gerçek değerinin yine de garanti edilmesi gerekmektedir (Charafeddine ve Barakat, 2018, s. 3).

Blockchain, mutabakatları ortadan kaldırmakta, işlem geçmişi üzerinde kesinlik sağlamakta, muhasebe kapsamını genişletmekte ve kapasitesini artırmakta, ölçülmesi günümüzde çok zor olan, bir şirketin elinde bulundurduğu verilerin değerinin ölçülmesini mümkün kılmaktadır. Bir başka ifade ile, Blockchain'in, defter tutma ve mutabakat çalışmalarının yerini aldığını belirtmek mümkündür. Bu durum, muhasebecilerin işleri ve çalışmaları üzerinde bir tehdit unsuru olabileceği gibi farklı değer kazanımlarına odaklanan muhasebecilere ise destek sağlayabilmektedir. Örneğin, şirket birleşmesi ve devri işlemlerinde gerçekleştirilen durum tespitlerinde, kilit rakamlar üzerinde dağıtılmış fikir birliği, yargılayıcı alanlara ve tavsiyelere daha fazla zaman ayrılmasına ve genel olarak sürecin daha hızlı ilerlemesine izin verebilmektedir (Procházka, 2018, s. 163).

Blockchain, ayrıca, geleneksel defterlerden daha fazla şeffaflığa izin vermektedir. Bu durum, varlıklara yönelik yolsuzluk veya suiistimal risklerinin söz konusu hallerde hayli cazip bir seçenek olarak karşımıza çıkmaktadır. Örneğin, yardım harcamaları veya bağışlar, Blockchain tabanlı varlıklarla sağlanabilir ve böylece sağlanan finansmanın alıcısı kolayca tespit edilebilir. Halihazırda, şirketler arasında gerçekleşen finansal işlemler, her şirketin kendi çift girişini yaptığı ve teorik olarak iki giriş kümesinin değer olarak eşit olduğu bir tür “dörtlü girişli defter tutmaya” yol açmaktadır. Bu model, Blockchain ile büyük ölçüde değiştirilebilmektedir. Bu, grup içi ticaret gibi bir etkinliğe yönelik olarak başlatılabilir ancak zamanla birden fazla varlığı içerecek şekilde büyüyerek bir tür “evrensel giriş muhasebesi” yaratılabilir. Temel olarak, her çeşit varlık defteri, bir Blockchain zincirinin sağladığı gizlilik sınırlamaları çerçevesinde tasarlanmalıdır. Her bir işleme dair veriler ayrı ayrı şifrelenebilirken, varlık kaynakları ya da mülkiyetleri söz konusu olduğunda, bunların doğrulanması için önceki işlemler herkesin erişimine açık olmalıdır. Yetkilerin dağıtımı (merkeziyetten uzaklaşma), gizlilik ve güvenlik konuları birbiri ile eşit derecede önemlidir ve bu unsurlar arasında bir dengenin sağlanması, Blockchain uzmanları arasında hayli revaçta

olan güncel bir çalışma ve araştırma alanı olarak karşımıza çıkmaktadır. Ayrıca belirtmek gerekir ki, günümüzde halen Blockchain teknolojilerinin uyarlanabileceği çok fazla alanın varlığı söz konusudur. Bir Blockchain kümesi, güçlü bir dijital kimlik sistemine bağlandığında, kullanıcıların kimlik bilgilerini depolayabilmekte ve şirketlerle kimlik paylaşımını sağlayarak onların “müşterilerini tanımalarına” ve diğer kimlik süreçlerini kolaylaştırmalarına imkân tanıyabilmektedir. Benzer şekilde, fikri mülkiyet haklarının barındırıldığı veritabanları da fikri mülkiyet sahiplerinin tanımlanması, belirlenmesi, hak taleplerinin karşılanması ve hakların ödenmesi gibi süreçleri basitleştirmek için paydaşlar arasında dağıtılabilmektedir (Daniel ve Green, 2018, s. 6) (Procházka, 2018, s. 163).

Blockchain’in finansal sistemler için önemli bir unsur olduğunu belirtmek mümkündür ve Blockchain’in kullanıldığı bir finansal sisteme geçiş de muhasebecilik mesleği için birçok fırsatı beraberinde getirmektedir. Muhasebeciler; kayıt tutma, karmaşık kuralların uygulanması, iş mantığı ve standart belirleme konularında uzman kabul edilmektedir. Blockchain’in gelecekte sistemlere nasıl entegre edileceği, işlemleri ve uzmanları nasıl etkileyeceği ve yönlendireceği, Blockchain öncülüğünde ne tür çözümlerin ve hizmetlerin üretileceği gibi hususlarda Muhasebeciler rehberlik edecek uzmanlar olarak görülebilmektedir. Blockchain’in, finansal sistemlerin ayrılmaz bir parçası haline getirilmesi için bu teknoloji geliştirilmeli, standartlaştırılmalı ve optimize edilmelidir. Bu sürecin uzun yıllar alması muhtemeldir, öyle ki, Bitcoin’in faaliyete başlamasının üzerinden henüz çok bir zaman geçmedi ve halen bu konuda yapılacak çok şeyin olduğu görülmektedir. Bu alanda, çok sayıda Blockchain uygulaması ve bu işle ilgilenen Start-up şirketlerin varlığı göze çarpmaktadır, ancak, bunların çok azı etkin işlem sağlayabilmekte ve deneme çalışmalarının ötesine geçebilmektedir. Bütün bu süreçlere muhasebeciler de dahil olmaktadır ancak bu meslek grubunun payına düşen işin hayli çok olduğunu belirtmek mümkündür. Muhasebeciler ve muhasebe şirketleri, Blockchain uygulamalarını ve kullanımını kapsayacak düzenleme ve standartlar oluşturmak için uzmanlıklarını kullanma yoluna gidebilmelidir. Bununla birlikte muhasebeciler, Blockchain sistemine dahil olmayı düşünen şirketlere danışmanlık hizmeti verebilmekte ve bu yeni sisteme yönelik maliyetlerin ve avantajların değerlendirilmesi ile raporlanması hususunda tavsiyelerde bulunabilmektedirler. Yeni teknolojinin kullanıldığı alanlarda muhasebeciler şirketlere oldukça önemli konularda

danışmanlık hizmeti sağlama kabiliyetindeki uzmanlar olarak değerlendirilmektedir (Institute of Chartered Accountants in England and Wales (ICAEW), 2018, s. 11).

İşlem güvencesi ve mülkiyet hakları gibi muhasebe konularının, Blockchain ve Akıllı Sözleşme yaklaşımları ile bir dönüşüm geçireceği öngörülmektedir. Uzlaşma ve Anlaşmazlık Yönetimi ihtiyacındaki azalma, haklar ve yükümlülükler konusundaki artan kesinlik ile birleştiğinde, işlemlerin hesaplanmasına ve değerlendirilmesine daha fazla odaklanmak mümkün olmakta ve hangi alanlarda ne tür bir hesap verilebilirliğin söz konusu olacağı daha geniş kapsamlı bir şekilde değerlendirilebilecektir. Mevcut muhasebe süreçlerinin büyük bir çoğunluğu, Blockchain, veri analizi ve makine öğrenimi gibi modern teknolojiler aracılığı ile optimize edilmeye elverişlidir. Böyle bir durumda, muhasebenin işlevsel verimliliğinin ve değerinin artacağı kolaylıkla ifade edilebilmektedir. Bütün bunların bir sonucu olarak, muhasebe sektöründe temsil edilen becerilerin kapsamı da değişecektir. Uzlaşmalar ve veri kaynağı güvencesi gibi bazı alanlarda iş yükleri azaltılabilmekte veya tamamen ortadan kaldırılabilen teknoloji, danışmanlık ve diğer katma değerli faaliyetleri genişleyebilmektedir (El-Sayid, 2018, s. 16).

2.3.2. Blockchain Çağında Denetim

Dış denetim faaliyetinde de Blockchain uygulamalarından söz etmek mümkündür. Bir şirketin mali durumunun doğrulanması, bu durumun temelindeki işlemlerin bir kısmının ya da tamamının Blockchain sisteminde görüntülenmesi halinde onaylarını daha az gerekli olacaktır. Böyle bir durum, denetimlerin çalışma biçiminde köklü bir değişiklik anlamına gelmektedir (Gül, 2018, s. 191). Bir Blockchain çözümü, uygun veri analitiği ile birleştirildiğinde, bir denetim işleminde yer alan işlem seviyelerini azaltmakta ve denetçinin becerileri daha ciddi ve üst düzey sorunların çözümüne yönlendirmesi mümkün olabilmektedir. Örneğin, bir denetim esnasında, yalnızca bir işlemin kimler arasında hangi parasal tutar çerçevesinde gerçekleştiği değil aynı zamanda nasıl kaydedildiği ve sınıflandırıldığı da dikkat çekmektedir. Şayet bir nakit ödemesi varsa, bu çıkışın satış maliyetlerinden mi yoksa giderden mi kaynaklandığı ya da bir alacaklıya mı ödeme yapıldığı yoksa bir varlık mı yaratıldığı gibi sorulara yanıt aranmaktadır. Bu yargılayıcı unsurlar, genellikle halka açık olmayan ve yalnızca iş yerinde gerekli olan bir konuya işaret etmektedir. İşte bu noktada

Blockchain teknolojisi, denetçinin bu tür sorulara odaklanması için daha fazla zaman kazanmasını sağlamaktadır (Kokina vd., 2017, s. 95).

Blockchain teknolojisi tabanlı işlemler gerçekleştiren bir şirketin denetlenmesinde, denetçinin bu denetim sürecini uygun bir şekilde gerçekleştirmesi için kendi odak noktalarını değiştirmesi gerekecektir. Dış kaynaklarla gerçekleştirilen Blockchain işlemlerinin doğruluğunun veya varlığının teyit edilmesine yönelik bir ihtiyaç oldukça azdır ya da hiç yoktur. Ancak bu işlemlerin mali tablolara nasıl kaydedildiği ve değerlendirildiği gibi yargısal unsurların nasıl kararlaştırıldığına hala çok dikkat edilmektedir. Uzun vadede, daha fazla kaydın Blockchain sistemine entegre olabileceği ve buna erişimi olan denetçilerin ve düzenleyicilerin bu işlemleri gerçek zamanlı olarak kontrol edebileceği, ayrıca bu işlemlerin kaynakları üzerinde de kontrol sahibi olabilecekleri öngörülmektedir (McGhee ve Grant, 2019, s. 10).

Günümüzde, bir şirket denetiminde, Blockchain teknolojisinin kullanıldığına dair bir örneğin varlığından söz etmek henüz mümkün değildir. Bununla birlikte, bazı araştırmacılar böylesi bir sistemin nasıl çalışacağı ve Blockchain teknolojilerini kullanan bir şirketin elde edebileceği potansiyel yararlar hususunda önerilerde bulunmaktadır. Blockchain, denetim takibinin oluşturulması için de kullanılabilir. Bir şirkette gerçekleşen her bir işlem, bir Blockchain kümesi oluşturmak üzere birbirine zincirlenmiş gerçek zaman damgalı bloklar oluşturacaktır. Blockchain teknolojisi ile tüm işlem geçmişi bu defterde saklanabilecek, dolayısıyla otomatik bir denetim izi oluşturulabilecektir. Blockchain teknolojisinin uygulanması ile deftere ilk girdilerin kaydedildiği andan itibaren tüm işlemleri içerecek olan ve değiştirilmesi mümkün olmayan bir kayıt oluşturulabilecektir (Schulman ve Wilson, 2019).

Blockchain'in faydalarından biri de gönderilen tüm verilerin Blockchain tarafından güvence altına alınmasıdır. Bu durum, denetçilerin defterler incelerken verilerin bütünlüğüne güvenilebileceği anlamına gelmektedir. Bir işlemin bilgileri deftere girildikten sonra asla silinememekte ve bu da ilişkili tüm işlemlerin ayrıntılı bir denetimine imkân tanıyabilmektedir. Böyle bir ayrıntılı denetim izni ise daima izlenebilir olacaktır. Blockchain kapsamındaki dağıtık defterler, denetim kontrollerinin daha sık ve artan bir güven çerçevesinde sürekli bir şekilde gerçekleştirilmesini

sağlayabilecektir. Blockchain, tüm işlemleri gerçek zamanlı olarak doğruladığından dolayı, denetimden önce işlemlerin değiştirilmesi imkânsız hale gelmektedir. Bir Blockchain kümesinde yapılan işlemler asla değiştirilememektedir (Vaidyanathan, 2017, s. 25). Bir işlem yanlışsa, bu işlemin değiştirildiği yeni bir işlem kaydı oluşturulurken, geçmiş işlem iptal edilmektedir. Bu durum, dolandırıcılığın önlenmesini sağlayabilmekte, dolandırıcılık tespitinin maliyetini azaltabilmekte ve sonuç olarak daha verimli bir denetim süreci ortaya çıkarabilmektedir (CPA Canada, AICPA Ve UWCISA, 2017).

2.4.Blockchain'in Avantajları ve Dezavantajları

Çoğu Blockchain zinciri, bir dağıtık defter olarak işlev gören, merkezi olmayan birer veritabanı olarak tasarlanmıştır. Bu Blockchain defterleri, verileri kronolojik bir sırayla düzenlemekte ve kriptografik kanıtlarla birbirine bağlanmış bloklar halinde kaydetmekte ve saklamaktadır. Blockchain teknolojisinin yaratılması, çeşitli endüstriyel sektörlerde birçok avantajı da beraberinde getirmiş, güvensiz ortamlarda daha fazla güvenlik sağlamıştır. Bununla birlikte, merkezi olmayan yapısı, bazı dezavantajları da beraberinde getirmektedir. Örneğin, geleneksel merkezi veri tabanları ile karşılaştırıldığında, Blockchain, daha sınırlı verimlilik sunmakta ve artırılmış depolama kapasitesi gerektirmektedir (Chuen ve Low, 2018, s. 61).

2.4.1.Blockchain Avantajları

Blockchain teknolojisinin sağlayacağı birçok faydalarından söz edebilir. Bunlardan bazıları aşağıda ele alınmıştır.

2.4.1.1. Dağınıklık (Dağıtım)

Blockchain verileri genellikle (dağınık bir düğüm ağında) binlerce farklı cihazda depolanmaktadır. Böylece sistem ve veriler, teknik arızalara ve kötü niyetli saldırılara karşı oldukça güvencedir. Her bir ağ düğümü, veritabanının bir kopyasını saklayabilir ve depolayabilir. Bu nedenle herhangi bir hata noktasının varlığından söz etmek mümkün değildir. Öyle ki tek bir düğümün çevrimdışı olması, ağın kullanılabilirliğini veya güvenliğini etkilememektedir. Tam tersine, geleneksel veritabanlarının çoğu, bir veya birkaç sunucuda barındırılmaktadır. Bu nedenle geleneksel veritabanları teknik arızalara ve siber saldırılara karşı daha savunmasızdır (Retief, 2018, s. 10).

2.4.1.2. Kararlılık (İstikrar)

Doğrulanmış ve onaylanmış Blockchain bloklarının tersine çevrilmesi mümkün değildir, yani veriler Blockchain sisteminde bir kez kaydedildikten sonra bu işlemi iptal etmek ya da değiştirmek son derece zordur. Bu özellik, Blockchain'in finansal kayıtların veya denetim takibinin gerekli olduğu diğer verilerin depolanması için mükemmel bir teknoloji olması anlamına gelmektedir. Öyle ki, her bir değişiklik izlenebilmekte ve kalıcı olarak dağıtılmış ve halka açık bir deftere kaydedilmektedir. Örneğin, bir işletme çalışanlarının dolandırıcılık riski taşıyan etkinliklerini önlemek için Blockchain teknolojisinden yararlanabilmektedir. Bu örnekte, Blockchain, şirket içinde gerçekleşen tüm finansal işlemlerin güvenli ve kararlı bir kaydını sağlayabilmektedir (Marshall, 2018, s. 25).

2.4.1.3. Güven Gerektirmeyen Sistem

Çoğu geleneksel ödeme sisteminde, işlemler yalnızca ödeme işleminin ilgili iki tarafına değil, aynı zamanda bir banka, kredi kartı şirketi veya ödeme sağlayıcısı gibi bir aracıya da bağlı olarak gerçekleşmektedir. Blockchain teknolojisinin kullanılması ile, bu üçüncü tarafın varlığı gereksiz hale gelmektedir. Çünkü, dağıtık düğüm ağı işlemleri, madencilik olarak bilinen bir süreç aracılığı ile işlemleri doğrulamaktadır. Bu Blockchain genellikle “güven gerektirmeyen” bir sistem olarak tanımlanmaktadır (Bratspies, 2018, s. 2) (Marshall, 2018, s. 15).

Bu nedenle, bir Blockchain sistemi, tek bir kuruluşa güvenme riskini ortadan kaldırmakta, aracıları ve üçüncü tarafları işlevsiz hale getirerek, genel maliyetleri ve işlem ücretlerini azaltmaktadır (Engle, 2016, s. 341).

2.4.2. Blockchain Dezavantajları

Blockchain kullanımı gelişen teknolojiyle birlikte hızlı bir şekilde artıyor ve kesinlikle bazı dezavantajlarını yer alılabilmektedir.

2.4.2.1. %51 Saldırıları

Bitcoin Blockchain'ini koruyan Proof of Work protokolü algoritmasının ne denli verimli olduğu yıllar içerisinde kanıtlanmıştır. Bununla birlikte Blockchain ağlarına yönelik olarak gerçekleştirilebilecek birkaç tane potansiyel saldırı türünden bahsedilebilmektedir. Bunlardan en çok tartışılanı %51 saldırılarıdır. Bu saldırı türü, bir

varlık ağındaki karma (hashing) gücünün %50'sinden fazlasının kontrol altına alınması ile gerçekleştirilebilmektedir. Şayet bu mümkün olursa, işlemlerin sırası kasıtlı olarak dışlanabilmekte veya değiştirilmekte, bunun sonucunda da ağ kesintiye uğratılabilmektedir.

Bu saldırı teorik olarak mümkün görünmesine karşın, bugüne dek Bitcoin Blockchain sisteminde herhangi bir başarılı %51 saldırısı gerçekleştiği görülmemiştir. Bir ağ büyüdükçe, o ağın güvenliği de aynı şekilde artar. Madencilerin dürüst davranışlarının ödüllendirildiği de göz önünde bulundurulduğunda, Bitcoin'e saldırmak için büyük miktarlarda para ve kaynak ayrılması gerekmektedir ki bu durum rasyonel değildir. Bunun dışında, başarılı bir %51 saldırısının gerçekleştirilmesi halinde, yalnızca en son işlemler kısa bir süre için değiştirilebilmektedir. Çünkü, bloklar kriptografik kanıtlarla bağlanmaktadır. Eski blokları değiştirmek, somut ve rasyonel olmayan seviyelerde bilgi işlem gücü gerektirmektedir. Ayrıca, Blockchain sistemi hayli dayanıklıdır ve herhangi bir saldırıya çok hızlı bir şekilde yanıt vererek kolaylıkla adaptasyon sağlayabilmektedir (Cawrey, 2014).

2.4.2.2. Veri Modifikasyonu

Blockchain sistemlerinin bir diğer dezavantajı da verilerin Blockchain'e eklendikten sonra değiştirilmelerinin hayli zor olmasıdır. Kararlılık, Blockchain'in avantajlarından biri olsa da bu her zaman iyi olmayabilir. Blockchain verilerini veya kodunu değiştirmek genellikle çok zahmetlidir ve bir zincirin terk edildiği ve yenisinin alındığı bir "hard fork" işlemi gerektirmektedir (Engle, 2016, s. 343).

2.4.2.3. Özel Anahtarlar

Blockchain, kullanıcılara, kendi sahip oldukları kripto paralar üzerinde veya diğer Blockchain verileri üzerinde sahiplik sağlamak için açık anahtarlı veya asimetrik kriptografi kullanmaktadır. Her bir Blockchain adresine karşılık gelen bir özel anahtar vardır. Adresler paylaşılabilmektedir ancak özel anahtar gizli tutulmalıdır. Kullanıcılar sahip oldukları fonlara erişmek için kendi özel anahtarlarına ihtiyaç duymaktadır. Bu her bir kullanıcının kendi bankalarımış gibi hareket etmesi anlamına gelmektedir. Bir kullanıcının özel anahtarını kaybetmesi halinde, kullanıcının sahip olduğu fon da kaybedilir ve bunun için kullanıcının yapabileceği hiçbir şey yoktur (European Central Bank, 2015, s. 10).

2.4.2.4. Yetersizlik (Verimsizlik)

Blockchain oldukça verimsizdir. Madencilik son derece yüksek bir rekabete dayanmaktadır. Her on dakikada yalnızca bir madenci kazanmaktadır. Dolayısıyla diğer tüm madencilerin emekleri boşa gitmektedir. Madenciler, hesaplama güçlerini sürekli olarak artırmaya çalışmaktadırlar. Geçerli bir blok hash bulma şansları daha yüksek olduğu için, Bitcoin ağı tarafından kullanılan kaynaklar son birkaç yılda önemli ölçüde artış göstermiştir. Öyle ki Bitcoin ağı günümüzde, Danimarka, İrlanda ve Nijerya gibi ülkelerden çok daha fazla enerji tüketmektedir (Chuen ve Low, 2018, s. 42).

2.4.2.5. Depolama (Saklama)

Blockchain defterleri zaman içerisinde daha da büyüyerek, daha çok depolama alanı işgal edebilirler. Bitcoin Blockchain Sistemi şu anda yaklaşık 285 GB depolama alanı gerektirmektedir (Blockchain.com, 2020). Blockchain boyutundaki mevcut büyüme, sabit disklerdeki depolama kabiliyetini aşmaktadır ve eğer defter, bireylerin indirmesi ve bunu depolaması için çok büyük bir hale gelirse ağ düğümlerini kaybetme riski söz konusu olabilmektedir. Blockchain teknolojisi bütün bu dezavantajlarına rağmen bazı benzersiz avantajlar sunduğundan varlığını sürdüreceği tahmin edilmektedir. Bu teknolojinin kabul görmesi ve tam olarak benimsenmesi için uzun bir süreye ihtiyaç vardır. Ancak çok sayıda endüstriyel sektörde Blockchain sistemlerinin avantaj ve dezavantajları bilinir haldedir. Yakın gelecekte, büyük olasılıkla, şirketler ve hükümetler, Blockchain teknolojisinin hangi alanlara katma değer sağladığını görmek için yeni uygulamalar denediği görülecektir (European Central Bank, 2015, s. 13).

2.5.Kripto Para Türleri ve Yasallığı

Türleri çok olduğunu için, kripto paraların yasallığı ülkeden ülkeye değişmektedir. Bazılarında yasallık durumu hala belirsiz ya da değişkenken, bunu farklı farklı faktörlere dayalı değişebilmektedir.

2.5.1.Kripto Para

Kripto para, dijital bilginin kıt hale getirilmesi için kriptografi, dağıtık bilgi işlem yazılımı, dünya çapında bir bilgisayar ağı, ekonomik saikler ve çeşitli protokol algoritmalarının bir kombinasyonundan oluşturulan, alınıp satılabilen dijital paradır. Dijital kıtlık, kripto para biriminin temel niteliklerinden biridir. Şayet dijital kıtlık

olmasaydı, para birimini temsil eden verilerin sınırsız sayıda kopyalanabilmesi mümkün olabilirdi. Dijital paranın sınırsız sayıda kopyalanması dijital para birimini değersiz hale getirmektedir. Dijital kıtlık yalnızca bir ağ içerisinde çalışmaktadır. Bu ağ içinde kripto para birimi işlemlerinin geçerliliği konusunda bir uzlaşya varmak mümkündür. Bu uzlaşya fikir birliği ya da konsensüs adı verilmektedir. Kullanılan konsensüs yöntemi ile kripto paranın sahtesinin üretilmesi engellenmekte ve dijital paranın iki kez harcanamaz hale getirilmesi sağlanmaktadır. Çoğu kripto para birimi, sahipliğin izlenmesi, dijital kıtlığın yaratılması ve çifte harcamanın önlenmesi için genellikle Blockchain teknolojisini kullanmaktadır. ABD Merkez Bankası, parayı, hanehalkı ve işletmeler tarafından ödeme yapmak veya kısa vadeli yatırımlar için saklamak amacıyla kullanılabilen bir grup güvenli varlık olarak tanımlamaktadır. Bitcoin ve diğer kripto para birimleri bu temel tanımı karşılamaktadır. Bitcoinde nakit parada olduğu gibi kendine özgü bir değer söz konusu değildir. Bitcoin'in arzı sınırlıdır ve ağdaki diğer katılımcılarla değişim için bir aracı kurum gerektirmemektedir. Bununla birlikte, ABD Gelir İdaresi (IRS), kripto para birimlerini varlık olarak ele almakta ve geçerli sermaye kazancı vergilerine konu etmektedir (Hileman ve Rauchs, 2017, s. 87).

Akıllı telefonların ve internet teknolojilerinin gelişmesi ile birlikte hayatımıza giren dijital depolama kartları ile birlikte piyasalarda çeşitli yenilikçi ödeme sistemleri de geliştirilmeye başlanmıştır. Bu dijital ödeme sistemleri sınıfının ortaya çıkması, varlıkların ve değerlerin aktarım biçimlerine yönelik bir devrim yaratmıştır. Değer aktarımının en son ve en ilginç biçimi 2008 yılında Satoshi Nakamoto tarafından oluşturulmuştur (Nakamoto, 2008). Satoshi'nin Bitcoin'i artık merkezi bir otoritenin varlığı gerekmeksizin birbirine güvenmeyen taraflar için iyi bilinen bir sınır aşırı değer transfer sistemi haline gelmiştir. Bitcoin; bir değişim aracı, bir değer deposu ve bir hesap birimidir. Geleneksel olarak büyük harflerle yazılmış "Bitcoin" ağ ve teknolojiyi ifade ederken, küçük harfle yazılmış "bitcoin(ler)" para birimini ifade etmektedir. Para birimi de yaygın bir şekilde BTC olarak kısaltılmaktadır. Ancak bazı borsalarda ISO 4217 standardıyla uyumlu bir şekilde önerilen para birimi kodu olan XBT ifadesi tercih edilmektedir. Bitcoin ve diğer kripto para birimlerinin alternatif para birimleri olup olmadıklarına ilişkin tartışmalar hala devam etmektedir. Kripto para birimi kavramının ne olduğunu anlamak için, merkezi olmayan kripto para biriminin temelindeki felsefeyi

iyi anlamak ve merkezi dijital para biriminin tarihini ve gelişimini anlamak önemlidir (Hennessy, 2014, ss. 222-223).

2.5.2. Dijital Para Biriminin Niteliği ve Türleri

Devlet tarafından basılan ve dağıtılan resmi para birimi dışında çok sayıda ve çeşitli alternatif para birimi türü vardır. Hileman, (2009) yılında yayınladığı bir çalışmada bunları genel olarak iki kategoriye ayırmıştır: 1) Somut (Maddi) para ve 2) Dijital para. “Emtia Parası” ile yakından ilişkili olan maddi para birimleri, değerlerini görece kıtlıktan ve parasal olmayan faydadan almaktadır. Dijital veya sanal ifadesi, elektronik bir ortama dayalı para birimlerini tanımlarken birbirlerinin yerine kullanılabilen kavramlar olarak karşımıza çıkmaktadır. Ancak bu iki kavram eş anlamlı değildir. “Sanal” terimi, bir şeyin “görünüşte gerçek” olduğunu ancak tam anlamıyla “gerçek olmadığını” ifade ettiği için olumsuz bir çağırışa yol açmaktadır. Bu ifadenin bir para biriminden bahsederken yaygın olarak kullanılması söz konusu değildir. Bunun yerine daha nötr bir ifade olan dijital para birimi ifadesi genellikle daha yaygın olarak kullanılmaktadır (Goldfeder vd., 2016, s. 14).

Değer transferini genel olarak dört kategoriye ayırarak incelemek mümkündür:

(a) Merkezi, Coğrafi Olarak Sınırlandırılmamış:

Bunlara örnek olarak; finans, telekomünikasyon veya perakende sektörlerinde faaliyet gösteren şirketlerden gelen sadakat programı puanları, havayollarından alınan ve mil olarak adlandırılan seyahat puanları. Bu para birimleri ayrıca sınır aşırı ön ödemeli telefon kartlarını ve bir dereceye kadar nakit değerine sahip akıllı kartları, ön ödemeli banka kartlarını ve kredi kartlarını da içermektedir. Bu kartlar mobil cihazlar üzerinde, sanal ya da fiziki olarak bulunabilmekte veya kullanılabilmektedir. Diğer sistemlere örnek vermek gerekirse, farklı ülkelerde, QR (Hızlı Yanıt) kodu veya yüz tanıma yöntemleri ile vergi iadeleri için dahi kullanılabilen bir sistem olan Alipay RMB cüzdanı sayılabilmektedir. Çevrimiçi (online / e-cüzdan) ve Çevrimdışı (offline / fiziki, kartlı cüzdan) gibi dijital ödemeler bu kategoriyi uygun bir şekilde örnekleyebilmektedir. Bu sınıftaki unsurlar, resmi para biriminin aksine, hükümet yetkisinden bağımsız olabilmekte ve hatta daha da önemlisi coğrafi olarak herhangi bir sınıra da tabi tutulmamaktadır (Floris, 2020).

(b) Merkezi, Coğrafi Olarak Sınırlı:

Bunlar, dijitalleştirilmiş ulusal para birimidir. Bu para birimleri belirli bir topluluğa ait olabildikleri gibi yerel ölçekli para birimleri olarak da karşımıza çıkmaktadır. Bunlara örnek olarak; İngiltere’de kullanılan e-Brixton Pund ve Bristol Totnes ve Almanya’da kullanılan eChiemgau verilebilir. Bu para biriminin kullanım amacı daha spesifik ve genellikle birtakım sosyal sözleşmelere dayanmaktadır. Mal alışverişinde kişileri ödüllendirmek ya da mal arzını sınırlandırmak gibi hususları içeren anlaşmalar vasıtasıyla kullanım çerçeveleri belirlenmektedir. Bu para biriminde yönetim merkezleştirilmiş ve değer transferi yerleştirilmiştir (Calvo ve Morales, 2014, ss. 34,29).

(c) Merkezi, Çapraz Platform:

Bunlara örnek olarak; açık piyasa sistemleri olan ve diğer kuruluşlarla işlem yapılmasına imkân tanıyan Flooz ve Beenz girişimleri örnek olarak verilebilmektedir. TenX gibi kripto banka veya kredi kartlarının, merkezi olmayan bir kripto para birimi ve jeton (itibari para/token) sistemi üzerine inşa edildiğini de göz önünde bulundurmak gerekmektedir. Bu para birimlerinde, akıllı sözleşmeler, farklı dijital para birimleri arasında ve ağ genelinde değer alışverişini mümkün kılmaktadır. Yönetim yapısı, aslında merkezi olmayan bir yapı üzerinde merkezleştirilmiştir ve bu merkezleştirme çoğu zaman akıllı sözleşmelerle gerçekleştirilmektedir. Değer, platform genelinde dijital olarak işlenmektedir ve bu işleme çevrimdışı veya çevrimiçi olabilmektedir (Grant, 2018) (Higgins, 2014).

(d) Hiçbir Şekilde Merkezi Olmayan veya Tam Olarak Dağıtılmış Para Birimi:

Bu para birimlerine örnek olarak; Bitcoin, Ethereum, Qtum, Zcash, Dogecoin ve diğerleri sayılabilmektedir. Bu para birimleri herhangi bir dış aracı ile işlem görebilmektedir. Hem yönetim hem de teknoloji, açık kaynaklı yazılımlarla merkezi bir yapıdan hayli uzaklaştırılmaktadır. Genellikle, faaliyetlerden sorumlu olan hiçbir tüzel kişilik yoktur ve bu nedenle geleneksel düzenlemelerin tamamen dışındadırlar. Değer transferi tamamen çevrimiçi gerçekleştirilmektedir (Massad, 2019, s. 18).

Kripto para birimi, uçtan uca (peer-to-peer / P2P) programlanabilir bir dijital para birimidir. Kripto para birimi, çevrimiçi ödemelerin bir araçtan geçmeden doğrudan doğruya bir taraftan diğerine gönderilmesine olanak tanımaktadır. Kripto para

birimi ile gerçekleştirilen işlemlerde ağ zaman damgası kriptografik olarak bütün işlemleri gerçekleştirmektedir. Bitcoin için bu durum Proof of Work (PoW / Emek İspatı) olarak bilinmektedir. PoW, bir Bitcoin protokolüdür ve esasen bir kod çözme yarışmasıdır. Öyle ki, PoW, katılanları ödüllendirmek için bir tür teşvik işlevi görmektedir. Kodu kıran ilk katılımcı yeni Bitcoinler ile ödüllendirilmektedir. Yaklaşık her 10 dakikada bir kez yeni bir işlem bloğu oluşturulur. İşlem kaydının değiştirilmesi neredeyse imkansızdır veya altı onay bloğundan sonra değiştirilmesi hayli maliyetlidir. Alternatif bir para birimi veya ücretsiz bir jeton (token) olarak bir kripto para birimi oluşturmak kolaydır, çünkü bunların hemen hemen hepsi açık kaynaklıdır. Bitcoin'in sorunsallarını çözmek için çok sayıda çeşitli altcoin oluşturulmuştur (BDO, 2019, s. 3).

Teknolojideki ilerlemelerin yoğun olması nedeniyle birçok alternatif kripto para birimi veya altcoin ortaya çıkmakta, sıkı düzenlemeler ve yetersiz taleplerden ötürü bu girişimlerin çoğu başarısızlık ile sonuçlanmakta ve yalnızca birkaç tanesi küresel olarak benimsenmektedir.

Kripto para birimi, işlemlerin güvenliğini sağlamak, doğrulamak ve ayrıca yeni para birimlerinin oluşturulmasını kontrol etmek için kriptografi adı verilen oldukça karmaşık bir şifreleme türünün kullanıldığı soyut, dijital para birimi olan bir dijital varlık türüdür. Kripto para, bir finans kurumundan ya da herhangi bir merkezi otoriteden bağımsız olarak, merkezi olmayan bir değişim aracı olarak çalışmak üzere tasarlanmıştır (Horowitz vd., 2018, s. 15). Bitcoin en çok bilinen kripto para birimi olsa da tek kripto para birimi değildir. Diğer önemli kripto para türleri arasında; Ethereum, Ripple, Bitcoin Cash ve Litecoin gibi kripto para birimlerini saymak mümkündür. Bu sayılanların dışında başka dijital varlıklar ya da bir başka ifade ile “kripto varlıklar” da vardır. Bunlar genellikle, dijital tokenler olarak adlandırılmaktadır. Örneğin, bir şirket genellikle ilk dijital para arzı (ICO) olarak adlandırılan bir “token satışı” ya da “token lansmanı” başlatabilmektedir. Bir ICO’da, bir şirket yeni bir ürün yaratmakta ve ürünü erken satın almaktan fayda sağlayacak bir kullanıcı tabanı oluşturmak istemektedir. Ayrıca, ICO, şirketin ürününü geliştirmek için gelir elde etmesini sağlamaktadır. Bu, şirketler için cazip bir çözümdür, çünkü risk sermayedarlarının veya bankaların gerektirdiği titiz ve düzenlenmiş sermaye artırma sürecini bu şekilde hızlı bir şekilde geçiştirmektedirler. Bu nedenle, bu tür dijital varlıklar etrafında düzenleyiciler tarafından öne sürülen karışık koşullar ve önemli tartışmalar göz önünde

bulundurulduğunda, şirketler hukuk, muhasebe ve vergi danışmanlarına danışmaya teşvik edilmektedir (International Securities Services Association (ISSA), 2018, s. 22).

Yeni bir kripto para biriminin “tokenlerini” oluşturma süreci, yeni bir Blockchain blok zinciri oluşturmayı, yeni bir varyant veya “fork (çatal)” oluşturmayı içeren mevcut bir süreci baştan aşağı değiştirmeyi içerebilmektedir. Bu sözde “altcoinlerin” çoğu aslında Bitcoin protokolünün çatallarıdır. Mevcut bir kripto paranın daha fazla “tokeninin” yaratılması için tek yol, kriptografik bir bulmaca olan algoritmayı çözen ve temeldeki Blockchain algoritmasına katkıda bulunan madenciye bir işlem ücreti olarak yeni bir “tokenin” verilmesidir. Madencilik, kriptografik bir bulmaca çözme sürecidir. Madencilik son derece rekabetçidir ve önemli bir hesaplama ve işlem gücü gerektirmektedir (Quest, 2018, s. 164).

Bitcoin gibi bazı kripto para birimleri arz açısından sınırlıdır yani dolaşımda bulunabilecek en yüksek Bitcoin sayısı belirlenmiştir. Diğerlerinin ise bir üst sınırı yoktur, ancak her yıl oluşturulabilecek yeni “token” sayısı sınırlanabilmektedir.

2.5.3. Kripto Para Türleri

CoinMarketCap’e göre toplam kripto para türü sayısı 5112’dir (CoinMarketCap, 2020). Coinlore’de ise toplam 3623 adet farklı kripto para türü listelenmektedir (Coinlore, 2020). Piyasada 3600’den fazla kripto para türü olduğu tahmin edilmektedir. Ancak günümüzde var olan kripto para birimlerinin sayısını tam olarak belirlemek mümkün değildir.

Kripto para birimleri, finans dünyasında bir fırtına etkisi yaratmıştır. “Kripto para” teriminden bahsedildiğinde, çoğu kimse bu terimi finansal özgürlük ve fırsatla ilişkilendirmektedir. Bu alanda meydana gelen pek çok teknolojik gelişme ve yeniliklerle birlikte, kripto para projeleri ve şirketlerinin de sayısı her geçen gün artmaktadır. Bir zamanlar kripto para birimlerinin türlerini ve sayısını kolaylıkla bilmek mümkün görünmekteyken, günümüzde bu mümkün değildir. Bilhassa son beş yıllık süreçte kripto para pazarının hızla büyüdüğü görülmektedir. Tüm bu kripto para birimleri, IEO’lar, ICO’lar, STO’lar, coinler, dolandırıcılar, Blockchain şirketleri ve çatallar gibi kavram ve aktörlerin var oluşu kripto para dünyasını anlamlandırmak ve anlamak günümüzde oldukça zor bir hal almıştır. Kripto para projelerinin hepsinin sonsuza kadar varlığını sürdüreceğini düşünmek mümkün değildir. Bazıları birer şaka

ya da test amacıyla yaratılmakta ve kısa bir süre içerisinde unutulup kaybolmaktadır (Şen ve Akarslan, 2018, ss. 189-190).

Kripto paraların listelenmesi için farklı kaynaklarda farklı listeleme yöntemleri kullanılmaktadır ve bunun sonucunda kripto paralarının sayılarına yönelik farklı bilgilendirmeler yapılmaktadır. CoinGecko'ya göre kayıtlarda 6788 adet kripto para birimi vardır. Bu, diğer kaynaklardan büyük ölçüde farklı bir veri olarak karşımıza çıkmaktadır. Dolayısıyla, bu durum, binlerce kripto paranın çoktan tarihe karıştığını, bir başka ifade ile “öldüğünü” göstermektedir. Aşağıda en önemli kripto para birimlerine yer verilen bir tablo sunulmaktadır:

Tablo 02.1: Kripto Paraların En Önemli Türleri

No.	Simge	Ad	Kodu	Fiyat/TL	Piyasa Değeri/TL
1		Bitcoin	BTC/XBT	89,998.23	1,666,741,824,333
2		Ethereum	ETH	2,920.40	330,127,234,574
3		Tether	USDT	7.94	125,513,016,099
4		Ripple	XRP	1.92	86,754,623,337
5		Bitcoin Cash	BCH	1,984.48	36,806,169,648
6		Litecoin	LTC	375.61	24,672,223,643
7		Monero	XMR	960.10	17,022,730,149
8		Zcash	ZEC	519.40	5,334,231,593
9		Dash	DASH	525.83	5,133,829,515

Kaynak: (coingecko.com, 2020)

2.6.Kripto Paranın Muhasebeleştirilmesi

Kripto paranın muhasebeleştirilmesine ilişkin olarak kavram tartışması yaşanmaktadır. Kripto paranın yasal durumu tam bir şekilde açıklanamadığından nasıl muhasebeleştirilmesine ilişkin çeşitli yorumlar geliştirilmiştir. Bu kısımda kripto para muhasebeleştirilmesi UFRS açısından ele alınacaktır.

2.6.1. Muhasebe ve UFRS Açısından Kripto Para

Şu an, 5000'den fazla farklı kripto para birimi, kripto para ve kripto belirteci, çeşitli kripto borsalarında işlem görmekte veya listelenmektedir. Bu kripto varlıkların şartları ve uygulamaları büyük ölçüde farklılık göstermekte ve zamanla değişebilmektedir. Şartlar değiştikçe muhasebeyi yeniden değerlendirmek önemlidir. Bazı kripto varlıklar, sahibine tanımlanabilmekte ve karşı taraftan bir mal veya hizmet alma hakkı vermektedir. Örneğin, bazı kripto varlıklar, sahibine bir saklama bankasından ya da borsa takas merkezinden belirli bir miktarda altın alma hakkı vermektedir. Böyle durumlarda, kripto paranın sahibi, kripto varlığı kullanarak ekonomik fayda elde edebilmektedir. Kripto varlık bir para olmasa da temsili para ile çok sayıda ortak özeliğe sahiptir (Leopold ve Vollmann, 2018, s. 5).

Bitcoin gibi diğer kripto varlıklar, sahibine temel bir mal veya hizmet hakkı vermemektedir ve tanımlanabilir bir karşı tarafın varlığından söz etmek de mümkün değildir. Kripto varlığın sahibi, bir ekonomik fayda elde etmek için kripto varlığı nakit, mal veya hizmet karşılığında kabul etmeye istekli bir alıcı bulmak zorundadır. Bir şirket, kripto varlıklarını doğrudan kendi cüzdanlarında tutabileceği gibi ortak veya paylaşılan bir cüzdana da bulundurması mümkündür. Şayet, şirket, kripto varlığı kendi cüzdanında tutarsa, kripto varlığın yasal mülkiyetine de sahip olmaktadır. Bununla birlikte, bir emanetçi kuruluşun (örneğin bir kripto varlık komisyoncusu şirketin), bir işletmenin kripto varlıklarını tuttuğu veya borsanın bu kripto varlıkları bir veya daha fazla paylaşılan cüzdana taşıdığı durumlarda, kripto varlıkların yasal mülkiyeti farklı taraflara ait olabilmektedir (Venter, 2018, s. 7). Böyle hallerde, kripto varlıkların asıl sahibinin söz konusu kripto varlıklar üzerinde münhasır hakkı bulunmamakta ve muhasebe, kripto varlıkların tutulma şekli ile ilgili hak ve yükümlülüklerle bağlı olmaktadır. Örneğin, bir kripto varlık borsasının paylaşılan cüzdanındaki kripto varlıklarda ekonomik bir fayda sahibi olan bir şirket, borsadaki bir talep yoluyla kripto varlıkların dolaylı sahibi olabilmektedir. Bu durumda, kripto varlıkların işlem hacmindeki değişikliklere ek olarak, kripto varlıkların sahibi aynı zamanda karşı taraf performans risklerine de maruz kalabilmektedir. Yani, kripto varlıkların asıl sahibi, borsanın tüm müşterilerinin taleplerini karşılayabilecek miktarda yeterli kripto varlık bulundurmama ihtimalinden kaynaklı risklerden de etkilenmektedir. Ayrıca belirtmek gerekir ki, bazı borsalar, kripto varlık sahiplerinin, sahip oldukları kripto varlıkları

başka bir borsaya veya kendi kripto varlık cüzdanlarına aktarma hakkını kısıtlayabilmektedir. Bu sınırlamalar, kripto varlık sahiplerinin, kripto varlıkları üzerindeki kontrollerini ve kripto varlıkların ekonomik fayda üretme potansiyelini etkili bir şekilde sınırlandırabilmektedir. Bu değerlendirmenin yapılması için, kripto varlık sahiplerinin, kripto varlık borsasına ilişkin bilgileri ve iddiaları dikkatli bir şekilde analiz etmeleri oldukça önemlidir (Trimborn vd., 2017, s. 14).

Burada, kripto varlıkların doğrudan doğruya elde tutulması üzerinde durulması uygun görülmektedir.

Kripto varlık bulundurmak, çeşitli hüküm ve koşullara tabidir. Kripto varlık sahiplerinin söz konusu kripto varlıkları ellerinde bulundurma amaçları da farklılık göstermektedir. Bu nedenle, kripto varlık sahiplerinin, mevcut UFRS kapsamında, hangi muhasebe sınıflandırması ve ölçümünün uygulanması gerektiğini belirlemek ve kendi koşullarını ve durumlarını değerlendirmek gereklilik arz etmektedir.

Standartlara bağlı olarak, hak sahibinin uygun sınıflandırma ve ölçümü belirlemek için gerekli olan iş modelini de değerlendirmesi söz konusu olabilmektedir (Fernandes vd., 2018, s. 2). Aşağıda, elde bulundurulan bir kripto varlık ve bununla ilgili ölçüm gereksinimlerine yönelik geçerli çeşitli muhasebe standartları ve bu standartlara dair tanımlar ile diğer gereksinimlere yer verilmektedir.

Bir kripto varlığın doğal bir özelliği de dijital bir temsil olması ve dolayısıyla doğası gereği soyut olmasıdır. Aşağıdaki muhasebe standartları yalnızca maddi varlıklar için geçerlidir ve bu nedenle kripto varlıklar için geçerliliği söz konusu değildir:

- UMS 16 Maddi Tesis ve Ekipman, maddi duran varlıklar için geçerlidir.
- UMS 40 Yatırım Amaçlı Gayrimenkuller arsa, bina (veya bir kısmı) veya her ikisi için de geçerlidir.
- UMS 41 Tarım, canlı varlıklar için geçerlidir (yani, canlı hayvanlar veya bitkiler)

Buna ek olarak, UFRS 6 Maden Kaynaklarının Araştırılması ve Değerlendirilmesi, maden kaynaklarının (mineraller, petrol, doğal gaz ve benzeri yenilenebilir olmayan kaynaklar) araştırılması için yapılan arama ve değerlendirme harcamaları için de geçerlidir.

Bazı kripto varlıklar 'madencilik' adı verilen bir süreçle yaratılsa da UFRS 6 sadece maden çıkarma işleminden önce maden kaynaklarının aranması ile bağlantılı olarak araştırma ve değerlendirme harcamaları için geçerlidir. Bu nedenle, bir işletme kripto varlıkların muhasebeleştirilmesinde UFRS 6'yı uygulamamalıdır. Kripto varlıklar için dikkate alınması muhtemel muhasebe işlemleri aşağıdaki şekilde sıralanabilmektedir.

- Nakit veya nakde eşdeğer varlıklar.
- UFRS 9 Finansal Araçlar
- UMS 2 Stoklar
- Ön Ödeme Varlıkları
- UMS 38 Maddi Olmayan Varlıklar
- UMS 8 Muhasebe politikaları, muhasebe tahminlerinde değişiklikler ve hatalar kapsamında bir muhasebe politikasının geliştirilmesi (McGuire & Massoud, 2018, s. 10).

2.6.2. Nakit ve Nakit Benzerleri / Eşdeğerleri

UMS 7, nakit ve nakit benzerleri, bir işletmenin nakit ile vadesiz mevduatı veya tutarı belirli bir nakde kolayca çevrilebilen kısa vadeli ve yüksek likiditeye sahip ve değerindeki değişim riski önemsiz olan yatırımları tanımlamaktadır.

2.6.2.1. Nakit

UMS 7'de , Nakit Akışı, “kasadaki nakit ve vadesiz mevduat” olarak ifade edilmektedir. Ancak UFRS'de bu terimler daha ayrıntılı bir şekilde tanımlanmamaktadır. AMB (ECB), IMF ve ABD Merkez Bankası, paranın üç farklı işlevi olduğunu belirtmektedir. Bu işlevleri şu şekilde sıralamak mümkündür:

- Değişim ortamı
- Hesap birimi
- Değer deposu

UMS 32 Finansal Araçlar: Sunum, nakit ve para birimini birbirinin yerine kullanır. Uygulamada para birimi, belirli bir yetki alanında dolaşımda olan hem fiziksel hem de elektronik para ile eş anlamlıdır (Humaidat, 2014, ss. 62,436).

UMS 32, ayrıca, nakdin değişim aracını temsil eden bir finansal varlık olduğunu ve bu nedenle, tüm işlemlerin ölçülüp finansal tablolarda muhasebeleştirilmesinin temeli olduğunu not etmektedir.

Vadesiz mevduatlar genellikle önceden haber verilmeksizin veya ceza verilmeksizin talep üzerine çekilebilen mevduatları temsil etmektedir.

Günümüzde mali tablolarda sunulduğu şekliyle, nakit, çeşitli yetki alanlarında yer alan bölgelerin hükümetleri tarafından ihraç edilen veya desteklenen resmi para birimlerinin fiziksel varlığı ve vadesiz mevduatı olma eğilimindedir. Yasal para birimlerinin gerçek değeri çok azdır veya hiç yoktur. Ancak genellikle bir yargı alanında bir değişim aracı olarak kabul edilmektedirler. Çünkü, yasal para birimi, hükümet tarafından desteklenmekte ve kendi yetki alanlarında yasal ödeme aracı olarak kabul edilmektedir (Grant Thornton, 2018, s. 4).

Yasal para statüsü, bir yetki alanında kanunlar doğrultusunda verilmektedir ve genellikle bir merkez bankası veya hükümet tarafından yetkilendirilmiş bir kuruluş tarafından verilen banknotlar ve madeni paralar için ayrılmaktadır. İngiltere Merkez Bankasına göre yasal para çok dar ve teknik bir anlama gelmektedir. Borçlu borcunun tamamını yasal para ile ödemeyi teklif ederse, borçluya ödeme yapmaması nedeniyle dava açılmaz. Ek olarak yasal para olarak sınıflandırılan şey genellikle belirli bir yetki ve yargı alanında bir hukuk meselesi olarak ele alınmaktadır. Bu nedenle, bir kripto varlık, bir yargı alanındaki belirli kuruluşlar tarafından ödeme için kabul edilebilirken, o yargı alanında kendiliğinden bir yasal ödeme aracı haline gelememektedir (Massad, 2019, ss. 15,18). UMS 32, nakdin tüm işlemlerin ölçülmesi ve finansal tablolarda muhasebeleştirilmesi için temel olduğunu belirtmektedir. Günümüzde, bir kripto varlığın bir işletmenin ya da şirketin finansal tablolarında yer alan muhasebe kalemlerini ölçmek ve muhasebeleştirmek için uygun bir temel olarak kabul edilmesi söz konusu değildir.

Bazı hükümetler, kendi kripto varlıklarını çıkarmayı veya başka bir tarafça çıkarılan bir kripto varlığı desteklemeyi düşündüklerini bildirmelerine karşın, bu aşamada kripto

varlıkların yasal para olarak değerlendirilip değerlendirilmeyeceği yani ödeme aracı olarak kabul edilip edilmeyecekleri hala net değildir (Cryptocurrency/Wikipedia, 2020).

Kripto varlıkları ihraç etme lisansına sahip özel şirketler, yasal para statüsü verme yetkisine sahip değildir. Bu nedenle, kripto varlıklar bir ödeme aracı olarak kabul edilse ve kullanılsa dahi UFRS açısından nakit olarak değerlendirilememektedir. Bir dereceye kadar çok çeşitli tüccarlar tarafından kabul edilse dahi, bu kripto varlıklar bir tür hediye kartına benzemektedir (Grant Thornton, 2018, s. 5).

2.6.2.2. Nakde Eşdeğer Varlıklar

UMS 7, nakit benzerlerini ya da bir başka ifade ile nakde eşdeğer varlıkları, yüksek likiditeye sahip, kolaylıkla nakde dönüştürülebilen ve önemsiz bir değer değişikliği riskine tabi olan yatırımlar olarak tanımlamaktadır. UMS 7, nakde eşdeğer varlıkların yatırım veya diğer amaçlardan ziyade vadeli nakit taahhütleri karşılamak amacıyla tutulduğunu ve bir yatırımın normalde edinim tarihinden itibaren üç ay veya daha kısa bir vadeye sahip olması halinde nakde eşdeğer varlık olarak nitelendirilebileceğini bildirmektedir.

Nakde eşdeğer varlıklar, sunum kategorisidir ve bir varlığın muhasebeleştirilmesini veya ölçülmesini belirlememektedir. Bu nedenle, bir kripto varlığın sunum amacıyla nakit eşdeğeri olarak kabul edilebilmesi için geçerli muhasebe standardına göre sınıflandırılması ve ölçülmesi gerekmektedir. O yüzden kripto varlıkların nasıl muhasebeleştirilebileceği varlığın türüne bağlıdır.

Uluslararası Finansal Raporlama Standartları Kurumu Yorumlama Komitesi, 2009 yılında, bir aracın nakit eşdeğeri varlık tanımına uyması için alınacak nakit miktarının ilk yatırım sırasında bilinmesi gerektiğini ifade etmiştir (Alibhai vd., 2018, s. 104).

Bununla birlikte belirtmek gerekir ki, kripto varlık ilk satın alındığında, vade sonunda alınacak nakit miktarı yaklaşık olarak bilinmektedir.

2.6.3. Finansal Araç

UMS 32, bir finansal aracı, bir işletmenin finansal varlığı ile diğer bir işletmenin finansal borcunda ya da özkaynağa dayalı finansal aracında artışa neden olan herhangi bir sözleşme şeklinde tanımlamaktadır.

2.6.3.1. Sözleşmeden Haklar

Finansal araç tanımı öncelikle, taraflar arasında bir sözleşmenin veya sözleşmeye dayalı ilişkinin varlığını gerektirmektedir. Bu durum, yasal gerekliliklerden kaynaklanan varlık veya yükümlülüklerin (örneğin gelir vergileri) finansal araç olmadığını belirten UMS 32'nin uygulama kılavuzunda belirtilmektedir. Benzer şekilde, oldukça likit bir yapıda olmasına karşın, külçe altın bir finansal araç değildir, çünkü nakit veya başka bir finansal varlık almak için sözleşmeye dayalı bir hak sağlamamaktadır (Deloitte, 2005).

UMS 32'de tanımlandığı üzere, bir sözleşme, iki veya daha fazla taraf arasında, genellikle anlaşmanın kanunen icra edilebilir olması nedeniyle, eğer varsa, kaçınılması gereken çok az takdir yetkisine sahip olduğu açık ekonomik sonuçları olan bir anlaşma olarak tanımlanmaktadır. Sözleşmeler çeşitli şekillerde olabilir ve yazılı olmaları şart değildir. Blockchain veya dağıtık defter teknolojisinin kullanılması, taraflar arasında kendiliğinden bir sözleşme ilişkisine yol açmamaktadır. Öte yandan, sahibine tanımlanabilir ve bir karşı tarafça sağlanan temel mal, hizmet veya finansal araçlar için yetki veren kripto varlıklar bir sözleşmenin tamamını karşılayabilmektedir. Diğer taraftan, sahibine, mal, hizmet veya finansal araçlar bağlamında herhangi bir hak ya da yetki tanımayan ve tanımlanabilir olmayan kripto varlıklar ise sözleşme tanımını karşılayamamaktadır. Örneğin, Bitcoin Blockchain'inde yer alan taraflar, diğer herhangi bir katılımcıyla sözleşmeye dayalı bir ilişkiye sahip değildir. Yani, bir kullanıcının Bitcoin sahibi olması nedeniyle Bitcoin madenileri, borsalar, diğer Bitcoin sahipleri veya herhangi bir başka taraf ile uygulanabilir bir sözleşmesi ve herhangi bir hak iddiasında bulunması söz konusu değildir. Bu tür hak sahipleri, ellerinde bulundurdıkları Bitcoinlerden ekonomik bir fayda sağlamak için bu Bitcoinleri almaya istekli alıcıları bulmaları gerekmektedir. (Smith, 2018, s. 3).

Sözleşmeye dayalı olmayan kripto varlıklar yine de bir sözleşmenin konusunu teşkil edebilmektedirler. Örneğin, belirli bir karşı taraftan Bitcoin satın almaya yönelik bağlayıcı bir anlaşma, Bitcoin'in kendisine yönelik bir sözleşme ilişkisini temsil etmese dahi bir çeşit sözleşme oluşturmaktadır. Bu nedenle, kripto varlıkları satın almak veya satmak için Blockchain dışında yapılan anlaşmalar, yukarıda belirtilen sözleşme tanımları kapsamında değerlendirilebilmektedir.

Finansal araç tanımı ikinci olarak, bir finansal aracın bir işletmenin finansal varlığında ve başka bir işletmenin finansal borcunda veya özkaynağa dayalı finansal aracında artışa yol açmasını gerektirmektedir. Dolayısıyla, bir kripto varlığın bir finansal araç olarak değerlendirilmesi, ancak sahibi için bir finansal varlığı temsil etmesi ile mümkün olacaktır.

UMS 32, bir varlığın finansal varlık olarak tanımlanması için aşağıdaki özelliklere sahip herhangi bir varlık olması gerektiğini bildirmektedir:

- Nakit
- Başka bir şirketin özkaynak aracı
- Sözleşmeden doğan bir hak
- Başka bir işletmeden nakit veya benzeri başka bir finansal varlık almak için veya,
- Finansal varlıkları veya finansal borçları, işletme için potansiyel olarak elverişli koşullar altında başka bir işletme ile takas etmek için veya,
- İşletmenin kendi özkaynağına dayalı finansal araçlarına ödenebilecek veya bir başka şekilde oluşturulan sözleşmelerin kriterlerini karşılamak için gerekli özelliklere sahip varlıkla. (SOCPA, 2018, s. 34).

Kripto varlıklar bağlamında, bir finansal varlık şunlardan biri olabilir: Nakit, başka bir işletmenin özkaynağına dayalı finansal aracı, sözleşmeye dayalı nakit veya diğer finansal varlıklara ilişkin bir hak veya potansiyel olarak uygun şartlarda finansal enstrümanlar ticareti yapma hakkı (örneğin bir türev). Bu seçeneklerin her biri göz önünde bulundurularak, bir kripto varlığın nakit dışındaki bir finansal varlık tanımını karşılayıp karşılamayacağı aşağıdaki bölümlerde analiz edilmektedir.

Sahibine, sözleşmeye dayalı olmasına rağmen, tanımlanabilir bir karşı tarafça sağlanan mal ve hizmetlerden yararlanma hakkı tanıyan kripto varlıklar, finansal varlık tanımını karşılamamaktadırlar. Çünkü, gelecekteki ekonomik fayda, nakit veya başka bir finansal varlıktan ziyade bir mal veya hizmetin satın alınması ile elde edilmektedir. Örneğin, sahibine, sözleşmeye dayalı bile olsa, bir bulut (cloud) bilişim hizmetinden yararlanma imkânı sağlayan bir kripto varlık, finansal bir varlık olma özelliğine sahip

olamamaktadır. Öyle ki, gelecekteki fayda, bir finansal varlık hakkı yerine bir hizmettir. Bu tür kripto varlıkların sahipleri, ilgili UFRS standartlarına göre uygun muhasebe yöntemlerini değerlendirmelidirler. Ön ödemeli maddi olmayan varlıklarla ilgili tartışmalar da bu konu ile ilgili olabilmektedir (BDO, 2019, s. 2).

Kripto varlığın sahibinin dayanak varlık teşkil eden mal ve hizmetleri alması için sözleşmeden doğan haklarının var olup olmaması, belirli gerçeklerin ve koşulların yanı sıra sözleşmenin uygulanabilirliğinin dikkatli bir şekilde incelenmesini gerektirebilmektedir.

2.6.3.2. Öz Kaynağa Dayalı Finansal Araçlar

UFRS, özkaynağa dayalı finansal aracı ya da bir başka ifade ile özkaynak aracını, bir işletmenin tüm borçlarını çıkardıktan sonra, varlıklarında kalan paylara kanıt teşkil eden herhangi bir sözleşme olarak tanımlamaktadır. Dolayısıyla, bu tür hakları tebliğ eden bir kripto varlık, özünde bir elektronik hisse senedi ve sonuç olarak bir finansal varlık olarak değerlendirilebilmektedir. Bir kripto varlık, değişken bir nakit akışına yol açsa dahi, bu kendiliğinden özkaynağa dayalı finansal araç tanımını karşıladığı anlamına gelmemektedir. Örneğin, sahibine, maddi olmayan bir varlık (örneğin bir çevrimiçi oyun) üzerindeki brüt telif hakkı akışından pay alma hakkı sağlayan bir kripto varlık, bir özkaynak aracı olarak değerlendirilememektedir. Buna ek olarak, bir kripto varlığı ihraç eden tarafın zımni kabulden doğan bir yükümlülüğü, kripto varlık hamili için bir özkaynağa dayalı finansal araç olarak nitelendirilen bir tutara yönelik faiz için, sözleşmeye dayalı bir hak doğurmamaktadır. Son olarak, bir kripto varlığın değeri, o kripto varlığın kullanıldığı bir platformun bilinirliği ile ilişkilendirilebiliyor olsa da, bu durum tek başına, platformun net varlıklarından sağlanabilecek bir fayda için sözleşmeye dayalı bir hakkı temsil etmemektedir. Bir başka ifade ile özkaynak aracı değildir (KGK, 2018, s. 12).

2.6.3.3. Sözleşmeden Doğan Nakit veya Başka Bir Finansal Varlık Hakkı

Bir Özkaynak aracı ya da türev olmayan bir kripto varlık*, hem sözleşmeye dayalı hem de nakit veya başka bir finansal varlık alma hakkını içermekteyse, finansal varlık tanımını yine de karşılamaktadır. Örneğin, bir kripto varlık, sahibine, nakit ödeme

* Kripto Varlıklar kategorisi altında sadece Kripto Para değil, diğer türleri Token, ICO, STO v.b olarak bulunmaktadır.

veya tahvil ya da hisse senetlerinin teslimi gibi bir hak sağlıyorsa, bu kripto varlık finansal varlık tanımını karşılamaktadır (Leopold ve Vollmann, 2019, s. 9).

Bu gibi durumlarda, kripto varlık esasen sahibini karşı taraftan kaynaklanan risklerle birlikte dayanak varlık üzerindeki ekonomik risklere de maruz bırakabilmektedir. Böyle bir kripto varlık, UFRS 9 sınıflandırma ve ölçüm şartları kapsamında değerlendirilmektedir. Tüm finansal varlıklar, sonradan gerçeğe uygun değer farkı kar veya zarara yansıtılarak ölçülenlerin dışında, başlangıçta gerçeğe uygun değer artı ilişkilendirilebilir işlem maliyetleri üzerinden kaydedilir.

Müteakip ölçüm, varlığın nakit akışı özelliklerine ve elde tutulma amacına bağlıdır. Sadece ana para ve faiz ödemesi nakit akışı özellikleri testini (SPPI testi) geçemeyen Özkaynak araçları dışında finansal varlıklar ve alım – satım amacıyla elde tutulanlar, gerçeğe uygun değerde kâr veya zararın yansıtılması ile ölçülmektedir. Süreçle ilgili iş modeli, SPPI testini karşılayan finansal varlıkların ölçümünü yönlendirmektedir. Finansal varlığın sözleşmeye bağlı nakit akışlarını tahsil etmek amacıyla elde tutulması anlamına gelen “Hold to collect” iş modeli kapsamında, UFRS 9 uyarınca itfa edilmiş maliyet üzerinden bir ölçüm söz konusu olmaktadır. “Hold to collect and sell” modelinde ise diğer kapsamlı gelir yoluyla gerçeğe uygun değer üzerinden bir ölçüm söz konusuyken, daha sonra bilanço dışı bırakılma halinde kâr veya zarara geri dönüştürülme işlemi gerçekleştirilmektedir. Bununla birlikte, muhasebe uyumsuzluğunun azaltılmasına ya da tamamen giderilmesine imkân tanıdığı hallerde, UFRS 9, SPPI nakit akış özelliklerini testinin kriterlerini karşılamasına rağmen, bir hamilin bir finansal varlığı belirlemesine izin vermektedir. Burada temel unsur, gerçeğe uygun değer farkının kâr veya zarara ilk muhasebeleştirme esnasında yansıtılmasıdır (PWC, 2017, s. 22).

2.6.3.4. Türev Araçlar

UFRS 9’de, bir türev araç, UFRS 9 kapsamında aşağıdaki özelliklerin üçüne birden sahip olan sözleşme olarak tanımlanmaktadır. Bu özellikler şu şekilde sıralanabilmektedir:

- Belirtilen faiz oranı, finansal araç fiyatı, emtia fiyatı, döviz kuru, fiyat veya oran endeksi, kredi notu veya kredi endeksi ve diğer değişkenlerde görülebilecek değişikliklere tepki olarak değerinde değişikliklerin

meydana gelmesi. Burada finansal deęiřken, deęiřken sözleşmenin (bazen dayanak olarak da adlandırılır) taraflarından herhangi birine özgü deęildir.

- Piyasa faktörlerinde meydana gelen deęişikliklere benzer bir tepki vermesi beklenen dięer sözleşme türlerine nazaran daha küçük ölçekli bir başlangıç yatırımı gerektirmesi ya da ilk yatırım gerektirmemesi.
- İleri bir tarihte ödenmesi. Böylelikle, bir türev, sözleşmenin UFRS 9 kapsamında olması kaydıyla, bir finansal araçtan ya da bir başka sözleşmeden kaynaklanabilmektedir.

Nakit olarak ödenebilen veya finansal olmayan kalemlerin kolayca nakde çevrilebildięi finansal olmayan kalemleri almaya veya satmaya yönelik bazı sözleşmeye dayalı haklar, finansal araçlar (örneğin bir türev) gibi muhasebeleştirilmektedir. Bu durum, UFRS 9 uyarınca ilk defa finansal tablolara alma sırasında gerçeęe uygun deęer farkı kar veya zarara yansıtılacak olarak belirlenmedikçe, “zati kullanım” sözleşmeleri için geçerli deęildir. Böyle bir hakkın sahibi, yukarıda tartışılan bir türevin üç özellięini de karşılayıp karşılamadığını deęerlendirmeli ve eęer öyleyse, bu hakkı bir türev olarak deęerlendirmelidir (Örten vd., 2018, ss. 338,393).

Kripto varlıkları satmak ya da satın almak için sözleşmeye dayalı bir hak (örneğin, bir aracı kurumla ile gerçekleştirilen ileri vadeli bitcoin işlemi) kripto varlığın kendisi bir finansal araç olmasa bile, kripto varlığın kolayca nakde çevrilebilir olması ya da sözleşme uyarınca nakde çevrilmesi kořuluyla bir türev haline gelmesine imkân tanımaktadır. Bu durum, ticari bir iş modelindeki emtia sözleşmelerinin muhasebeleştirilmesine benzemektedir. Örneğin, petrolün kendisi bir finansal araç olmamasına karşı vadeli petrol sözleşmeleri UFRS 9 kapsamına girebilmektedir.

Türev araçların ölçümü, başlangıçta gerçeęe uygun deęerden kaydedilmekte ve daha sonra satış veya elden çıkarma maliyetleri için herhangi bir kesinti olmaksızın kâr veya zarara yansıtılarak gerçeęe uygun deęerinden ölçülmektedir. Bununla birlikte, nakit akışı riskinden korunma işleminde, riskten korunma aracı olarak belirlenen bir türev için, etkin korunma kısmına ilişkin gerçeęe uygun deęer hareketleri, korunan kalem kâr veya zararı etkileyene kadar dięer kapsamlı gelirlerle birlikte kaydedilmektedir (Aygören ve Kurtcebe, 2019, s. 8).

Sonuçta, kripto varlıklar finansal araçlar olarak türev de dahil UMS7 ve UFRS 32'ine göre muhasebeleştirilebilecektir, bunu kripto varlıkların türlerin ile ilgilidir, bazı ICO'lerin türü bir misal olarak kabul edilebilmektedir.

2.6.4. Stoklar

Stoklar, her ne kadar somut bir varlık olarak varsayılsa da UMS 2, stokların somut olmasını gerektirmemektedir. Bu standart, stokları belirli maddeler kapsamında bir varlık olarak tanımlamaktadır. Bu maddeleri şu şekilde sıralamak mümkündür:

- Olağan bir iş akışı içinde satış için tutulan,
- Satış için üretim sürecinde tutulan,
- Üretim sürecinde veya hizmet sunumunda tüketilecek malzeme veya sarf malzemesi şeklinde tutulan stok.

Kripto varlıklar, işin olağan akışı içerisinde, örneğin bir emtia komisyoncusu ya da tüccar tarafından satılmak üzere tutulabilmektedir. Kripto varlıkların olağan iş akışı içinde satılıp satılmayacağı, sahibi için belirli gerçeklere ve koşullara bağlıdır. Uygulamada, kripto varlıklar genellikle stok üretiminde kullanılmamaktadır ve bu nedenle üretim sürecinde tüketilecek malzeme ve sarf malzemeleri arasında sayılmamaktadır (Örten vd., 2018, s. 42).

UMS 2, finansal araçlara uygulanmamaktadır. Bu nedenle, kripto varlığın finansal araç tanımını karşıladığı hallerde UMS 2 kapsamındaki stok yerine UFRS 9 kapsamında muhasebeleştirilmelidir.

Normalde UMS 2, maliyet veya net gerçekleştirilebilir değerden daha düşük bir ölçüm gerektirmektedir. Bununla birlikte, esas olarak fiyat dalgalanmalarından veya alım – satım makasındaki dalgalanmalardan kâr etmek için kripto varlıkları alıp satan komisyoncular / tüccarlar, kripto varlık stoklarını gerçeğe uygun değerden daha az satış maliyetleri ile ölçme kabiliyetine sahiptir (Procházka, 2018, s. 170).

Yukarıdakilere göre eğer bir işletmenin esas faaliyeti içinde kripto para alım satımı yapıyorsa stok olarak muhasebeleştirilebilecektir.

2.6.4.1. Maliyet veya Net Gerçekleşebilir Değerden Düşük Olanıyla Değerleme

Satın alınan kripto varlık stoklarının maliyetleri, tipik olarak satın alma fiyatı, geri alınmaz vergiler ve doğrudan stokun edinilmesiyle ilişkilendirilebilen diğer maliyetleri (örneğin, Blockchain işletme ücretleri) içermektedir. Diğer maliyetler, stokların maliyetine, yalnızca kripto varlık stoklarının bugünkü konumuna ve durumuna getirilmesine katlanıldığı ölçüde dahil edilmektedir.

Üretim sürecinde, kripto varlıklara yönelik uygulanması söz konusu olmayan çeşitli üretim aşamaları arasında, depolama gerekli olmadığı sürece, stok maliyeti, beklenen satış maliyetlerinin yanı sıra depolama giderlerini de içermemektedir. Depolama maliyetlerine bir cüzdan ya da başka bir kripto para hesabı bulundurma maliyeti örnek olarak verilebilmektedir.

Net gerçekleştirilebilir değer, UMS 2’de işin olağan akışı içindeki tahmini satış fiyatı, tahmini tamamlanma maliyeti ve satışın gerçekleştirilmesi için gerekli tahmini maliyetin çıkarılması ile tanımlanmaktadır. Stok olarak kaydedilen kripto varlıkların maliyeti, bu kripto varlıklar tamamen veya kısmen kullanılmaz hale gelmişse (kripto varlığa veya uygulamasına yönelik ilginin azalması buna neden olabilir) veya satış fiyatları düşüyse geri alınamayabilir. Benzer şekilde, kripto varlık stokunun maliyeti, bunları satmanın tahmini maliyetleri arttıysa tam olarak geri kazanılamayabilir (Güncenme Gençoğlu, 2017, s. 12).

Kripto varlık stokuna sahip bir şirket, her raporlama döneminde net gerçekleştirilebilir değeri tahmin etmek durumundadır. Net gerçekleştirilebilir değer maliyetin altında olduğu durumlarda, stok net gerçekleştirilebilir değeri ile yazılmalıdır ve değer düşüşü kâr veya zarara kaydedilmelidir. Stok değerinde daha önce görülen bir düşüş, koşullar iyileştiğinde tersine çevrilebilmektedir. Ancak tersine çevirme işlemi, asla orijinal maliyetini aşmamalı ve önceden yazılmış olan tutarla sınırlı olmalıdır.

2.6.4.2. Satış Maliyetleri Düşülmüş Gerçeğe Uygun Değer

Daha önce belirtildiği üzere, emtia komisyoncuları, emtia stoklarını satış maliyetleri düşürüşmüş gerçeğe uygun değer üzerinden ölçebilmektedirler. Komisyoncu/tüccarlar, başkaları veya kendi nam ve hesaplarına emtia (mal) satın alan veya satan kişilerdir. Bu emtialar, esas olarak, yakın bir gelecekte satılmak ve fiyat veya

makas aralığındaki dalgalanmalardan bir kâr elde etmek amacıyla elde edildiğinde, satış maliyetleri düşükmüş gerçeğe uygun değer üzerinden emtia stoku olarak sınıflandırılabilir (Alibhai vd., 2018, s. 141).

Bir komisyoncu/tüccar, stokunu satış maliyetleri düşülmüş gerçeğe uygun değer üzerinden ölçtüğünde, muhasebeleştirilen tutardaki herhangi bir değişiklik, dönemin kârına ya da zararına dahil edilmelidir. Bir kripto varlığın bir komisyoncu/tüccar olan sahibi, ilgili Blockchaindeki işlem maliyetlerini ve kripto varlığı nakde dönüştürmek için gereken diğer ücretleri de dikkate almalı ve kripto varlığı satmanın maliyetini her raporlama tarihinde uygun bir şekilde öngörmelidir. Bu ücretler, ilgili Blockchain’de mevcut işlem talebine bağlı olarak dönemden döneme dalgalanabilmekte ve bu dalgalanmalar kimi zaman önemli boyutlara varabilmektedir (Leopold ve Vollmann, 2019, s. 9) (Alibhai vd., 2018, s. 139).

2.6.5. Avanslar (Ön Ödeme)

Ön ödeme, işletmenin ya da şirketin mal veya hizmetlerini teslim etmeden önce gerçekleştirilen ödeme şeklinde kaydedilen bir varlık türüdür. Ön ödemeler, işletmeye ya da şirkete nakit, finansal varlık veya finansal araçların uygun koşullarda alım satım hakkı yerine gelecekteki mal veya hizmetlerin alımına yönelik bir hak sağladığı için finansal varlık olarak değerlendirilmemektedir. Bununla birlikte, bir kripto varlığın, sahibine kolayca nakde çevrilebilen bir dayanak varlığı satın alma veya bunu satma hakkı sağladığı durumlarda, türev kılavuzu uygun olabilmektedir. Sahibine ileri vadede bir mal üzerinde hak sağlayan bir kripto varlık, elektronik bir çeşit ödemeyi ispatlayan elektronik belge niteliğindedir. Bir işletmenin ya da şirketin niyeti ve iş modeli, bu tür bir belge için uygun bir muhasebe etkinliği gerektirmektedir. İşletmenin ya da şirketin, dayanak malı teslim almak için kripto varlığı elinde tutma niyetinde olmaması halinde, bunun bir ön ödeme olarak muhasebeleştirilmesi genellikle uygun görülmemektedir ve maddi olmayan varlık kılavuzu dikkate alınmalıdır (Deloitte, 2015).

Ölçüme ilişkin olarak, UFRS’de, ön ödemelerin muhasebeleştirilmesi konusunda çok sınırlı bir kılavuz olduğu görülmektedir. Uygulamada, ön ödemeler genellikle maliyet üzerinden muhasebeleştirilmekte ve UMS 36 – Varlıklarda Değer Düşüklüğü uyarınca değer düşüklüğü testine tabi olmaktadır. UFRS’deki sınırlı kılavuz dikkate alındığında, bir işletmenin veya bir şirketin, bir muhasebe politikası geliştirmesi, bu

politikayı benzer kalemlere ve raporlama dönemleri boyunca tutarlı bir şekilde uygulaması gerekmektedir (Deloitte, 2015).

2.6.6. Maddi Olmayan Duran Varlıklar

UMS 38, varlığı, “geçmişteki bazı olayların sonucu olarak işletme tarafından kontrol edilen ve işletmeye gelecekte ekonomik fayda sağlaması beklenen bir kaynak” şeklinde tanımlamaktadır. Maddi olmayan duran varlıklar bu grubun bir alt bölümünü oluşturmakta ve “fiziksel niteliği bulunmayan, tanımlanabilir, parasal olmayan bir varlık” şeklinde tanımlanmaktadır.

Parasal varlık, elde tutulan para ile sabit ya da belirlenebilir tutarda bir para cinsinden elde edilebilecek varlıklardır. Nakit veya finansal araç tanımını karşılamayan bir kripto varlık, genellikle parasal olmayan bir varlık olma özelliğine sahiptir (Leopold ve Vollmann, 2019, s. 8).

2.6.6.1. UMS 38’in Kapsamı

Maddi olmayan duran varlıklar, başka bir standardın kapsamına girdikleri durumlarda (örneğin UMS 32 kapsamındaki bir finansal varlık tanımına uyan kripto varlıklar veya UMS 2 kapsamında normal iş akışı dahilinde satış için tutulan kripto varlıklar), UMS 38 kapsamında muhasebeleştirilmemelidir. UMS 38, faaliyetlerin veya işlemlerin farklı bir şekilde ele alınması gerekebilecek muhasebe sorunlarına yol açacak kadar özelleşmiş hallerde, bunların kapsam dışında bırakılabileceğini bildirmektedir. Bu standart, maden çıkarma endüstrilerinde, petrol, gaz ve maden yataklarının araştırılması veya geliştirilmesi ya da bunların çıkarılmasına yönelik harcamaların muhasebesi ve sigorta sözleşmelerinin muhasebeleştirilmesi için geçerli değildir (Örten vd., 2018, s. 242).

2.6.6.2. Maddi Olmayan Duran Varlığın Tanımı

Uluslararası Muhasebe Standartları Kurulu (IASB), maddi olmayan duran varlıkların temel özelliklerini şu şekilde sıralamaktadır:

- İşletme tarafından kontrol edilmektedirler.
- İşletme için gelecekte ekonomik faydalar sağlamaktadırlar.
- Fiziksel varlık söz konusu değildir.

- Tanımlanabilirlik.

Bu özelliklere sahip bir kalem, işletmenin bu varlığı neden elinde tuttuğuna bakılmaksızın maddi olmayan duran varlık olarak sınıflandırılabilir.

Kontrol – Kontrol, başkalarının bu faydalara erişimini kısıtlama ve bir kalemin gelecekteki ekonomik faydalarını elde etme gücüdür. Kontrol, normalde yasal haklarla kanıtlanmaktadır, ancak, UMS 38, işletmenin ekonomik faydalara erişimi başka bir şekilde kontrol edebildiği durumlarda bunun gerekli olmadığını açıklamaktadır.

UMS 38, yasal hakların olmadığı hallerde, benzer sözleşme dışı kalemler için takas işlemlerinin varlığının, işletme ya da şirketin, beklenen ileri vadeli ekonomik faydaları kontrol edebildiğine dair kanıt sağlayabileceğini ifade etmektedir.

Gelecekteki Ekonomik Faydalar – Çoğu kripto varlık, ekonomik faydalara için sözleşmeye dayalı bir hak sağlamamaktadır. Bunun yerine, ekonomik faydaların gelecekteki bir satıştan, istekli bir alıcıya satıştan ya da kripto varlığın mal veya hizmetlerle takas edilmesinden kaynaklanması muhtemeldir.

Fiziksel Varlığın Yokluğu – Kripto varlıklar dijital temsiller olduğu için doğaları itibarıyla fiziksel varlığa sahip değildir.

Tanımlanabilirlik – Bir varlığın tanımlanabilir olması için, maddi olmayan duran varlıktan ayrılabilir olması yani hamilinden ayrı olarak satılabilir ya da devredilebilir olması gerekmektedir. Bununla birlikte, varlığın, sözleşmeden doğan veya diğer yasal haklardan kaynaklanması gerekmektedir. Çoğu kripto varlık, istekli bir alıcıya serbestçe aktarılabilirliğinden, genellikle ayrılabilir olarak kabul edilmektedir. Benzer şekilde, sözleşmeden doğan haklardan kaynaklanan kripto varlıklar da genellikle ayrılabilir olarak kabul edilmektedir (KGK, 2018, ss. 4-7).

2.6.6.3. Muhasebeleştirme Gereksinimleri

Bir maddi olmayan duran varlık, yalnızca gelecekteki ekonomik faydaların işletmeye ya da şirkete girişinin muhtemel olduğu ve maliyetinin güvenilir bir şekilde ölçülebildiği hallerde muhasebeleştirilmektedir. Ayrı olarak elde edilen maddi olmayan duran varlıklar, normal olarak UMS 38'in maliyetinin gelecekteki ekonomik faydaların beklentisini yansıttığını varsaydığı için muhasebeleştirilebilmektedir. Bu nedenle, işletme, zamanlama ve tutar konusunda herhangi bir belirsizlik söz konusu olsa dahi,

her zaman bu maddi olmayan duran varlıklardan gelecekteki ekonomik faydaların sağlanabileceğini beklemektedir (SOCPA, 2018, s. 18).

2.6.6.4. İlk Muhasebeleştirme (İlk Ölçüm)

Maddi olmayan varlıklar, başlangıçta, maliyet değeri ile muhasebeleştirilir. Kripto varlıkları edinmenin maliyeti, tipik olarak, eğer varsa ticari indirimler ve tenzilatların düşülmesinden sonra, satın alma fiyatının ve Blockchain işlem ücretlerin toplamı ile ilgili işlem maliyetlerini içermektedir. Bir maddi olmayan duran varlığın başka bir parasal olmayan varlık karşılığında edinilmesi durumunda, maliyet gerçeğe uygun değer üzerinden ölçülmektedir. İşlem ticari özden yoksun olmadıkça veya edinilen varlığın veya vazgeçilen varlığın gerçeğe uygun değeri güvenilir bir şekilde ölçülemediği sürece. Bu tür durumlarda, maddi olmayan duran varlığın maliyeti, vazgeçilen varlığın defter değeri olarak ölçülmektedir (Grant Thornton, 2018, s. 7).

2.6.6.5. Sonraki Ölçüm (Dönemsonu Değerleme)

UMS 38 kapsamında, maddi olmayan duran varlıklar için, iki adet sonraki ölçüm yaklaşımı vardır. Bunlar:

- Maliyet yöntemi
- Yeniden değerlendirme yöntemi.

Bir şirket ya da işletmenin farklı türdeki kripto varlık türlerini elinde bulundurduğu hallerde, farklı kripto varlıkların sağladığı hakların ve temel ekonomik özelliklerinin büyük ölçüde değişmesinden dolayı, bunların farklı maddi olmayan duran varlık sınıfları oluşturup oluşturmadığının değerlendirilmesi gerekmektedir.

2.6.6.5.1. Maliyet Yöntemi

UMS 38 kapsamındaki maliyet yönteminde, sonraki ölçümün, herhangi bir amortisman ya da değer kaybı kaynaklı maliyetlerin düşülmesinden sonra gerçekleştirilmesi gereklidir.

Faydalı Ömür ve Amortisman: Bitcoin gibi çoğu kripto varlığın bir son kullanma tarihi yoktur ve nakit veya diğer mal veya hizmetlerin edinimi için istekli bir karşı tarafla değiştirilebilecekleri süre için de öngörülebilir bir sınır söz konusu değildir. Bu nedenle bir hamilin, böyle bir kripto varlığın işletme ya da şirketi için net nakit girişi

oluşturmasının beklendiği süre için öngörülebilir bir sınır olup olmadığını göz önünde bulundurması gerekmektedir. Ancak, sınırsız faydalı ömre sahip maddi olmayan duran varlıkların en az yılda bir kez ve değer düşüklüğü belirtisi olduğu anlarda değer düşüklüğü testine tabi tutulması gerekmektedir (ACCA, 2019).

Bir kripto varlığın, sahibi için net nakit girişi oluşturması için öngörülebilir bir sınır varsa, kripto varlığın faydalı ömrüne yönelik bir öngörü geliştirilmeli ve kripto varlığın maliyeti de kalıntı değer tutarı düşülerek, öngörülen faydalı ömür boyunca amortize edilmelidir. Ek olarak, değer düşüklüğüne yönelik herhangi bir belirti söz konusu olduğunda, kripto varlık UMS 36 kapsamında belirtilen değer düşüklüğü testine tabi tutulmalıdır.

Değer Düşüklüğünün Tersine Çevrilmesi: Maddi olmayan duran varlıklara yönelik gerçekleştirilen değer düşüklüğü testi ile bu varlıkların değer düşüklüğüne uğradığı tespit edilirse, hamil, maddi olmayan duran varlığın defter değerini, geri kazanılabilir tutarına getirmeli ve ilgili dönem için kâr ve zarara yansıtması gerekmektedir (ACCA, 2019).

Daha sonraki dönemlerde, hamil, değer düşüklüğü kaybının artık mevcut olmayabileceğine (veya zararın azalmış olabileceğine) dair bir gösterge olup olmadığını değerlendirmeli ve eğer öyleyse, geri kazanılabilir tutarı belirlemelidir. UMS 36, varlık sahibine, güncellenmiş defter değerinin varlığın orijinal maliyetinden daha önce herhangi bir değer düşüklüğünün söz konusu olmaması ve bunun muhasebeleştirilmemesi koşuluyla, kaydedilecek olan amortisman eksikliğini aşmamasını dikkate alınarak, değer düşüklüğünün iptalini kaydetmesine izin vermektedir.

2.6.6.5.2. Yeniden Değerleme Yöntemi

İşletme, yeniden değerlendirme yöntemini ancak gerçeğe uygun değer için aktif bir piyasaya atıfta bulunarak belirlenmesi durumunda uygulayabilmektedir. Aktif piyasa, UFRS 13 – Gerçeğe Uygun Değer Ölçümü kapsamında şu şekilde tanımlanmaktadır: “Varlık veya yükümlülük için işlemlerin, sürekli olarak fiyatlandırma bilgisi sağlamak adına yeterli sıklıkta ve hacimde gerçekleştiği bir piyasa.”

UMS 38’de, maddi olmayan duran varlığın gerçeğe uygun değerinin dolaylı olarak belirlenmesini mümkün kılan herhangi bir hüküm bulunmamaktadır. Örneğin, bir şirket birleşmesinden dolayı edinilen maddi olmayan duran varlıkların gerçeğe uygun

değerinin tahmin edilmesi için uygulananlar gibi değerleme teknikleri ve finansal yöntemlerin kullanılması ile bir belirlemenin yapılmasına izin verilmemektedir (Daniel ve Green, 2018, s. 20).

Sonuç olarak, aktif bir piyasada, özdeş bir varlık için gözlemlenebilir bir fiyat yoksa (yani UFRS 13 kapsamında Seviye – 1 fiyatı), varlık sahibi, tutulan kripto paralara maliyet yöntemini uygulamak durumunda olacaktır. Yeniden değerlendirme modeline göre, maddi olmayan duran varlıklar için yeniden değerlendirme tarihindeki gerçeğe uygun değerinden müteakip amortisman ve değer düşüklüğü zararlarının çıkarılmasıyla ölçüm sağlanmaktadır (McGuire ve Massoud, 2018, s. 8).

Maddi olmayan duran varlığın başlangıç maliyetini aşan gerçeğe uygun değerdeki net artış, diğer kapsamlı gelir yoluyla yeniden değerlendirme hesabına kaydedilmektedir. Maliyetin altında net bir düşüş, kâr veya zarar olarak kaydedilir. Kümülatif yeniden değerlendirme karşılığı (yedeği), bilanço dışı bırakıldıktan sonra ve muhtemelen yeniden değerlendirilmiş tutara ilişkin ek amortismanın varlık kullanıldıkça dağıtılmamış kârlara aktarılması ile doğrudan dağıtılmamış kârlara aktarılabilir. Ancak, UMS 38, yeniden değerlendirme fonunun kâr veya zarar yoluyla transfer edilmesine izin vermemektedir.

2.7. Kripto Paranın Muhasebeleştirilmesinde Yönelik IASB Kararı

Uluslararası Muhasebe Standartları Kurulu'nun (IASB) talebine istinaden, UFRS Yorumlama Komitesi, 2019 yılının Haziran ayında, mevcut UFRS standartlarının kripto varlıkların bir alt kümesi olan kripto paralar üzerinde nasıl uygulanması gerektiği hakkında bir gündem kararı yayınlamıştır. Komite, bir kripto para biriminin, hamilinden ayrılıp, ayrı ayrı satılabilmesi veya devredilmesi ve parasal bir varlık olmaması nedeniyle, yeni sahibine sabit veya belirlenebilir sayıda para birimi alma hakkı sağlamaması nedeniyle, UMS 38 Maddi Olmayan Duran Varlıklar kapsamındaki **maddi olmayan duran varlık tanımını karşıladığını bildirmiştir**. UFRS Yorumlama Komitesi, **kripto para birimlerinin olağan iş akışı dahilinde satış için tutulmadıkları sürece UMS 38 kapsamında muhasebeleştirilmesi gerektiği sonucuna varmıştır**. Bu durumda UMS 2 Stoklar kapsamı da geçerli olmaktadır. Gündem kararı, ayrıca, kripto para birimleri ile ilgili olabilecek mevcut UFRS

standartları kapsamında açıklama gereklilikleri hakkında da yol göstermektedir (IFRS Interpretations Committee - IFRIC, 2019, s. 2).

IASB'nin Muhasebe Standartları Danışma Forumu (ASAF), Avustralya Muhasebe Standartları Kurulu tarafından hazırlanan bir makaleye dayanarak ilk olarak Aralık 2016'da "dijital para birimleri" konusunu ele almıştır (Venter, 2018, s. 4). Ocak 2018'deki IASB toplantısında Kurul, araştırma gündeminin bir parçasını oluşturabilecek belirli emtia türlerini, dijital para birimlerini ve emisyon tahsisatlarını içeren bazı işlemleri tartışmıştır. Nisan 2018'de ASAF, diğerlerinin yanı sıra, ASAF üyelerinin yargı alanlarında dijital para birimlerinin yaygınlığını değerlendirmiş ve dikkate alınması gereken potansiyel standart belirleme projeleri hakkında IASB'ye tavsiyelerde bulunmuştur. 2018 yılının Temmuz ayında, IASB, UFRS Yorumlama Komitesinden, bir işletmenin kripto para birimleri ve İlk Para Arzı (ICO) sahipliklerine ilişkin muhasebe uygulamalarının belirlenmesinde mevcut UFRS Standartlarının nasıl uygulanabileceği konusunda bilgi vermesini istemiştir. 2018 yılının Eylül ayında ise Komite, mevcut UFRS standartlarının kripto para ve ICO varlıklarına uygulanmasının yanı sıra IASB tarafından standart belirleme etkinliği olasılığını ele almıştır. Kasım 2018'de IASB, çalışma planına kripto para varlıklarına veya ilk madeni para tekliflerine ilişkin bir proje eklememeye, bunun yerine kripto varlıklarının gelişimini izlemeye karar vermiştir. IASB, Komiteden, kuruluşların mevcut UFRS standartlarını kripto para birimlerine nasıl uyguladıklarına dair bir gündem kararı yayınlamayı düşünmesini istemiştir (IASB, 2018, ss. 14-17). Komite, daha fazla tartışmanın ardından, Mart 2019'da geçici gündem kararını yayınlamış ve Haziran 2019'da, alınan görüş yazışmalarını değerlendirdikten sonra, bu konuda bir gündem kararı yayınlamıştır.

Gündem Kararının Kapsamı

Yorumlama Komitesi, mevcut UFRS standartlarının kripto para birimlerine nasıl uygulanacağını kapsamlı bir şekilde ele almıştır. Komite, bir dizi kripto varlık tanımlamıştır. Bu bağlamda gerçekleştirilen çalışmaların amacı doğrultusunda, UFRS Yorumlama Komitesi, günden kararında, kripto varlıkların bir alt kümesi olarak ele aldığı “kripto paraların” aşağıdaki özelliklerin tümüne sahip olması gerektiğini bildirmiştir. Bu özellikler şu şekilde sıralanmaktadır:

- Güvenlik açısından kriptografinin kullanıldığı, bir dağıtık deftere kaydedilen dijital veya sanal para birimi olması,
- Bir yetkili otorite tarafından veya yargısal olarak yetkilendirilmiş bir başka kurum tarafından verilmemiş/sağlanmamış olması,
- Hamili ile başka taraf arasında bir sözleşmeye yol açmamış olması.

Kripto para birimleri için hangi UFRS standartlarının geçerli olduğu konusuna gelince; UFRS, UMS 2 kapsamındaki stoklar, maddi olmayan duran varlıkları içermektedir. Çünkü bu standart, stok öğelerini varlıklar olarak tanımlamaktadır. UFRS Yorumlama Komitesi bu sonuca varırken şu hususları dikkate almıştır: (Yatsyk, 2018, s. 57)

- Olağan iş akışı içinde satış için tutulan,
- Satış için üretim sürecinde tutulan,
- Üretim sürecinde veya hizmet sunumunda tüketilecek malzeme veya sarf malzemesi şeklinde tutulan kripto paralar.

Kripto Para Birimi Varlıklarının Tutulması (Bulundurulması): UFRS Yorumlama Komitesi, bir işletmenin olağan iş akışı dahilinde satış için kripto para birimleri bulundurabileceğini bildirmektedir. Bu durumda, **bir kripto para birimi varlığı, şirket ya da işletme için stoklar olarak kabul edilmekte** ve buna göre UMS 2 kapsamında bulunmaktadır.

Yorumlama Komitesi, ayrıca, bir işletmenin kripto para komisyoncusu/tüccarı olarak hareket edebileceğini ifade etmiştir. Bu durumda, işletme, kripto para stoklarını satış maliyetleri düşülmüş gerçeğe uygun değerinden ölçen emtia komisyoncusu/tüccarı için geçerli olan UMS 2 hükümlerini dikkate almak durumundadır (Venter, 2018, s. 14).

Komisyoncu/tüccarlar, başkalarının ya da kendilerinin nam ve hesabına mal alıp satan kişilerdir. Bahsedilen stoklar, esas olarak yakın gelecekte satış yapmak ve fiyat dalgalanmaları, makas aralıkları değişiklikleri gibi durumlardan kâr elde etmek amacıyla edinilmektedir. Maddi olmayan duran varlık tanımı UMS 38 kapsamında, “fiziksel nitelikleri olmayan, tanımlanabilir, parasal olmayan bir varlık” olarak bildirilmektedir. Bir varlık, ayrılabilir nitelikteyse veya sözleşmeden doğan veya diğer

yasal haklardan kaynaklanan özellikte ise tanımlanabilir olarak nitelendirilmektedir. Bir varlık, işletmeden ayrılabilir, bölünebiliyorsa, tek başına veya ilgili bir sözleşme kapsamında tanımlanabilir varlık ya da borçla birlikte satılabilir, devredilebilir, lisanslanabilir, kiralanabilir veya takas edilebilir o varlığın ayrılabilir olduğunu belirtmek mümkündür. UMS 21 – Döviz Kurlarındaki Değişikliklerin Etkisi başlığı altında parasal olmayan bir kalemin temel özelliğinin sabit veya belirlenebilir sayıda para birimi alma hakkının ya da teslim etme yükümlülüğünün olmadığını bildirmektedir. **UFRS Yorumlama Komitesi, bir kripto para biriminin birtakım gerekçelerle UMS 38’de bildirilen maddi olmayan duran varlık tanımını karşıladığını bildirmiştir.** Bu gerekçeler şu şekilde sıralanabilmektedir:

- (a) Hamilinden ayrılıp, ayrı ayrı satılabilir veya devredilebilir,
- (b) Hamiline sabit veya belirlenebilir sayıda para birimi alma hakkını veremez.

UMS 38’in kapsamı, aşağıdakiler dışında tüm maddi olmayan varlıkların muhasebeleştirilmesinde geçerlidir:

- Başka bir UFRS standardı kapsamında olanlar,
- UMS 32 – Finansal Araçlar başlığı altında, Sunum kapsamında tanımlanan varlıklar,
- Arama ve değerlendirmeye tabi varlıkların muhasebeleştirilmesi ve ölçülmesi (UFRS 6 – Maden Kaynaklarının Araştırılması ve Değerlendirilmesi Kapsamındaki varlıklar),
- Minerallerin, petrolün, doğal gazın ve benzeri yenilenebilir olmayan kaynakların geliştirilmesi ve çıkarılması için yapılan harcamalar.

Buna göre, UFRS Yorumlama Komitesi, bir kripto para biriminin, UMS 32 kapsamında bildirilen bir finansal varlık tanımını karşılamadığını veya başka bir standart kapsamında olup olmadığını da tartışma gereği görmüştür (EY, 2019, s. 3).

Bu kararın nedenleri; kripto paranın nakit olmaması, başka bir işletmenin Özkaynak aracı olmaması, hamili için sözleşmeye dayalı bir hak doğurmaması ve hamilinin kendi Özkaynak araçlarında ödenecek bir sözleşme olmamasıdır.

UFRS, bazı kripto para birimlerinin, belirli mal veya hizmetler karşılığında kullanılabileceğini belirtmektedir. Ancak, mal veya hizmetlerin fiyatlandırılmasında bir değişim aracı ve para birimi olarak tercih edilen herhangi bir kripto para biriminin, tüm işlemlerin ölçülmesinde ve finansal tablolarda muhasebeleştirilmesinde esas teşkil edecek ölçüde dikkate alındığını söylemek mümkün değildir.

Bir kripto para birimi, maddi olmayan duran varlık tanımını karşıladığından ve ilgili kapsam istisnaları geçerli olmadığından, kripto para birimi varlıkları, olağan iş akışı içinde satış için tutulmadıkları sürece UMS 38 kapsamında muhasebeleştirilmelidir, diğer halde UMS 2 geçerli olmaktadır (EY, 2018, s. 21).

UFRS standartları tarafından aksi yönde gerekli kılınan açıklamalara ek olarak, bir işletmenin, UMS 1 - Finansal Tabloların Sunumu kapsamı uyarınca, finansal tablolarının anlaşılmasıyla ilgili her türlü ek bilgiyi açıklaması gerekmektedir. Özellikle, Yorumlama Komitesi, kripto para birimleri bağlamında birtakım açıklama gerekliliklerine dikkat çekmektedir. Bu gereklilikleri şu şekilde sıralamak mümkündür:

- Bir işletme, aşağıdaki gereklilikler doğrultusunda ilgili açıklamaları sağlamalıdır:
 - (a) İşin olağan akışı dahilinde satış için tutulan kripto para birimleri için UMS 2,
 - (b) Uygulanabilir hallerde UMS 38.
- Bir şirket ya da işletme, kripto para varlıklarını satış maliyetleri düşülmüş gerçeğe uygun değer üzerinden ölçüyorsa, UFRS 13 - Gerçeğe Uygun Değer Ölçümü kapsamında geçerli açıklama gerekliliklerini belirtmelidir.
- UMS 1'in 122'nci paragrafını uygulayan bir işletme, finansal tablolarda muhasebeleştirilen tutarlar üzerinde en önemli etkiye sahip olan yetkili otoritelere tabi ise, yönetiminin kripto para varlıklarının muhasebeleştirilmesine ilişkin olarak aldığı kararlar ve sahip olduğu yetkiler doğrultusunda gerekli açıklamaları yapmalıdır.
- UMS 10 - Raporlama Döneminden Sonraki Olaylar, bir işletmenin, olayın niteliğine ilişkin bilgiler ve bunun finansal etkisinin bir tahmini (veya böyle bir tahminin yapılamayacağına dair bir açıklama) dahil olmak üzere,

düzeltilme gerektirmeyen önemli olayların ayrıntılarını açıklamasını gerektirmektedir. Örneğin, kripto para birimleri bulunduran bir şirket ya da işletme, raporlama döneminden sonra, bu varlıkların gerçeğe uygun değerinde meydana gelen değişikliklerin, finansal tablo kullanıcılarının ekonomik kararlarını etkileyebilecek kadar önemli olup olmadığını değerlendirmek durumundadır (IFRS Interpretations Committee - IFRIC, 2019).

Sonuç olarak kripto varlık çok geniş bir terimdir ve kripto para kripto varlıkların bir türüdür. Kripto para muhasebeleştirme için iki kavram ile bağlıdır. İlkisi işletmenin esas faaliyeti nedir? İkincisi ise işletme hangi standartlarına göre defterlerini tutulur. Eğer bir işletme GAAP (Genel Kabul Görmüş Muhasebe İlkeleri)ne tabii olansa her daima kripto para maddi olmayan varlık olarak muhasebeleştirilecektir. Lakin diğer bakışta eğer bir işletme UFRS standartlarına tabii ise, o zaman işletmenin esas faaliyetini ne olduğunu bakmak gerekir. Bir işletmenin esas faaliyetini kripto parayı alım satımı ise (kripto borsaları ve brokerliği gibi) UMS2 ine göre stok olarak muhasebeleştirilecektir. Öte yandan eğer bir işletmenin kripto para satın almış bu kripto para UMS 38 ine göre maddi olmayan varlık olarak muhasebeleştirilecektir.

ÜÇÜNCÜ BÖLÜM

KRİPTO PARA DOLANDIRICILIĞI ve ADLİ MUHASEBE ÇÖZÜMLERİ

Kripto para birimleri, bankalardan veya geleneksel para hizmeti işletmelerinden daha fazla anonimlik sahiptir. Kripto para biriminin suça ilişkin tarafı anlaşılana kadar alıcı ve satıcının kripto parayı nasıl ve neden kullandığı ile alışverişin taraflarına erişmek hiç de kolay olmamıştır. O yüzden Kara para aklamayı, vergi kaçakçılığı ve saire gibi sahtekarlık işlemlere saha açmıştır. Ancak adli muhasebe ve onun gelişmiş ve özel teknikleri ile kullanıcıların kripto para dolandırıcılığından ve teknolojiye bağlı suçlarından korumada etkin bir rol üstlenmektedir.

3.1. Şirketlerde ve İşletmelerde Kripto Para Riskleri

İlk dijital para birimi olan Bitcoin'in halka tanıtıldığından bu yana kripto para birimleri ile ilgili çeşitli ve çok sayıda risk endişeleri ve risk yönetim problemleri konu olmuştur. Bu bağlamda algılanan riskler esasen genel hatlarıyla spekülatif riskler olarak tanımlanabilmektedir. Dolayısıyla bu risklerin, geleneksel bir sigortacının endişe duyacağı tarzda riskler olmadığını belirtmek mümkün görünmektedir. Sigorta şirketleri, kripto para risklerini kapsamak için ihtiyatlı bir şekilde sigortalama iştahlarını genişletmiştir. Ancak bu bağlamda oluşturulan kripto varlıklara yönelik sözde sigorta poliçeleri hiç de ucuz değildir ve kripto para birimlerinin kararsız ve hatta istikrarsız durumunun yanı sıra tarihsel süreç içerisinde kaydedilemeyen kayıp verilerin eksikliği nedeniyle uygulanmalarının önüne geçilmektedir. Yakın bir tarihte İngiltere'de bulunan Lloyd's of London adlı büyük sigorta borsası, kripto para ile ilgili risklere yönelik bir sigortalama kararı almış olsa da, yöneticiler tarafından "bir dereceye kadar ihtiyatlı hareket edilmesi" ikazında bulunulmuştur. Bitcoin'in asıl amacı, geleneksel bankacılık ve finans ağları üzerinde herhangi bir olumsuz etki yaratmadan kullanıcılar arasında uçtan uca bir değişim aracı sağlamak olarak ifade edilmiştir. Ancak, aradan yaklaşık on

yıl geçtikten sonra, her biri farklı derecede tüketici güvenliğine sahip olan ve genellikle değişken fiyat dalgalanmalarının görüldüğü binlerce farklı kripto para birimi oluşturulmuştur. Risk transferi fırsatlarına yönelik en tutarlı ilgi, kripto para birimlerine odaklanan borsalar, yatırımcılar, geleneksel finans kurumları ve finans teknolojisi girişimcileri tarafından yönlendirilmiştir. Sigorta uzmanları, şu anda kripto para birimlerini ticari bir mal olarak kullanan kişi ya da şirketlere ve bu tür işlemleri gerçekleştiren müşterilerine gözetim hizmeti sağlayan yerleşik düzenleyici ve uyumluluk çerçevelerine sahip geleneksel finans kurumlarına karşı bir açılım süreci başlatmışlardır. Sigorta uzmanları, çok daha büyük bir risk profilinin küçük bir parçası olarak gördükleri kripto para kullanan şirketlere yönelik işlem yapma hususunda gün geçtikte daha istekli hale gelmektedirler (Angotti vd., 2018, ss. 1-2). Kripto para sektörüne yeni girmiş şirketler ya da bu alanda uzun süredir faaliyet gösteren şirketler, her ne kadar sigortacılık sektörünün hizmetlerinden yararlanma imkanına sahip olsalar da bu şirketlere hizmet sağlayan sigorta şirketlerinin ve sigorta uzmanlarının, hizmetlerini daha rahat sürdürebilmeleri için daha detaylı bir durum tespit süreci yürütmeleri gerekmektedir. Bu hususta açıkça bilinen bir gerçek vardır. Gün geçtikçe, iş modellerine kripto para birimlerini dahil eden şirketlerin sayısı hızla artmaktadır ve bu süreçte, bu tür şirketlerin faaliyetlerinden kaynaklanan farklı düzeydeki riskler ya sigortalar tarafından eksik karşılanmaktadır ya da hiçbir şekilde bir sigorta poliçesine karşılanmamaktadır. Bu yeni iş modellerine dayanan ticari faaliyetlerin çoğu, mevcut sigorta poliçelerinin kapsamının yeniden incelenmesini ve kripto para birimleri ile gerçekleştirilen ticari faaliyetlere dair risklerin azaltılmasına yönelik politikaların araştırılmasını gerekli kılmaktadır (Homeland Security Enterprise, 2014, s. 18).

3.2. Kripto Para: Risk Yönetimine Genel Bakış

Geçtiğimiz birkaç on yılda, teknolojik gelişmeler hız kesmeden devam etmektedir. Bu gelişmeler, hayatımızın birçok alanını daha iyi hale getirmektedir. İletişim, sağlık hizmetleri ve iş yönetimi gibi alanlar teknolojik gelişmelerle birlikte gün geçtikçe daha iyi hale gelmektedir. Bu nedenle, teknolojik gelişmelerin daha iyi ve daha kullanışlı bir para birimi fikrine ilham vermesi bir zamanlama meselesi olarak düşünülebilmektedir. Ancak, ortada yeni bir para biriminin olması, onun kusursuz olduğu anlamına gelmemektedir. Bu yeni para birimi her ne kadar şifreleme yoluyla güvenli olacak şekilde tasarlanmışsa da yine de kripto para kullanımının beraberinde

getirdiği riskler vardır. Geleneksel finans kurumlarından piyasa riski, likidite riski, operasyonel riskler gibi çeşitli risk faktörlerini ölçmesi ve değerlendirmesi beklenmektedir (Sloan, 2018).

Bitcoin ve Ethereum gibi dijital para birimlerinin değerinin hızla artması ve diğer birçok varlığın sağladığı kazançları geride bırakmaları ile birlikte kripto para birimleri ana akım ilgi odakları arasında yer almaya başlamıştır. Deneyimli ve fikirlerine saygı duyulan yatırımcıların 2017 yılında en çok konuştukları konu Bitcoin olmuştur. Bu finans sektörünün kripto para birimlerine erişime ve bu yöndeki talebi karşılamaya yönelik çabalarını oldukça fazla düzeyde artırmalarına yol açmaktadır (Bridgers vd., 2019).

Ancak, gayrimenkul piyasasının aksine, kripto para birimleri o kadar yenidir ki, çoğu geleneksel finans şirketi dahi henüz kripto para piyasasına erişim sağlayamamaktadır. Öyle ki, kripto para piyasasındaki hizmetlerin çoğu geleneksel finans şirketleri yerine finans teknolojileri şirketleri tarafından gerçekleştirilmektedir. Finans teknolojileri şirketleri kripto para hesaplarının açılması, kripto para ticaretinin yapılması için gerekli olan uygun kullanıcı deneyimlerinin sağlanması gibi hizmetler sunmaktadır. Bununla birlikte, finans teknolojileri şirketleri de bilgi eksikliği yaşayan müşterilerin kripto para işlemlerine dair riskleri yönetmek hususunda kısmen deneme yanılma yöntemiyle hizmet sağlamaktadırlar. Kripto para ile ilgili hizmet sağlayan şirketler, kripto para birimlerine özgü risklerin tespiti ve yönetimi, kripto paraları saklama ve transfer etme gibi temel finansal hizmetleri nasıl gerçekleştireceklerine yönelik bir öğrenim sürecindedirler (Macwan, 2019).

3.3. Kripto Para Riskleri

Sigorta uzmanları halen kripto para birimlerinden kaynaklanan yeni riskleri tanımaya çalışmaktadır. Bu risklerden en bilinenlerini şu şekilde sıralamak ve açıklamak mümkündür:

1- Belirsiz (Net Olmayan) Düzenlemeler:

Bu grup altında yer alan risklerin şu ana kadar aşıldığını belirtmek mümkündür. Örneğin, ödeme ve alternatif para transfer şirketleri arasında yaygın bir şekilde kullanılan bir kara para aklama önleme yaklaşımı (AML) oluşturulmuştur. Bir kısım sigorta uzmanları, yasal standartların tamamı karşılanana dek, kripto para birimi veya

bununla ilgili işlemlerle uğraşan müşterilere yönelik bir sigorta kapsamı hazırlamaktan kaçınılmaktadır. Bu düzenleme eksikliği, yatırım sermayesini artırmak amacıyla gerçekleştirilen ilk para arzı (ICO) piyasasında oldukça belirgindir. İlk beş yılda gerçekleştirilen ICO faaliyetlerinde yaklaşık 6 milyar dolarlık bir işlem hacmi gerçekleşmiş ve kripto para piyasasının toplam değeri 260 milyar dolara ulaşmıştır. Bu denli büyük rakamlar yatırımcıların hayli ilgisini çekmektedir ancak ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) ve diğer düzenleyici kurumlar, ICO'ların çoğunun dolandırıcılık amaçlı gerçekleştiğini bildirmekte ve ICO etkinliklerindeki potansiyel dolandırıcılık tehlikesine dikkat çekmektedir. Daha genel olarak, SEC'e göre, hisse senedi ve emtia piyasalarına yönelik düzenlemelerin arasında kripto para birimlerine yönelik düzenleme gereksinimlerine şüphe ile yaklaşılmaktadır. ABD dışındaki ülkelerde de farklı hedefler doğrultusunda çeşitli düzenlemelerin yapıldığı görülmektedir. Bazı ülkeler kripto para birimlerinin herhangi bir şekilde kullanımını engellerken Çin gibi bazı ülkeler ise kripto paraların finansal kurumlarda kullanımını kısıtlamaya yönelik adımlar atmaktadır. İsrail ise kripto paraların finansal hizmet sektörünün bir alt alanı olarak ele alınmasına yönelik tasarlanmış, şeffaflığa önem veren ve tüketici haklarını koruyan, kara para aklama ve diğer yasadışı faaliyetleri azaltacak çeşitli kurallar geliştirmektedir (Wijayaa ve Suwarsonob, 2018, s. 12).

2- Muhafaza / Saklama

ABD'de SEC, saklama düzenlemeleri ile ilgilenen düzenleyici kurumlar arasında ilk sırada yer almaktadır. SEC Başkanı Jay Clayton, 2018 yılında gerçekleştirilen yatırım konferansında, kripto paraların saklanmasıyla yönelik çözümlerin genişletilmesi ve geliştirilmesini kabul edilse dahi saklama tekliflerinin hala iyileştirilmesi ve saklama koşullarının sertleştirilmesi gerektiğini ifade etmiştir. Bu çözümler, başlangıçta düzensiz bir şekilde öne sürülmelerine karşın; güvenlik ve diğer taahhütler ile ilgili kaygıları dikkate alarak şekillenmektedir. Köklü şirketler bu özelleşmiş pazara girmeye yönelik faaliyetlerine devam etmektedir. Örneğin çokuluslu bir Amerikan yatırım şirketi olan Fidelity Investments "bu yükselen varlık sınıfını, müşterilerimizin anlaması ve kullanması için daha kolay bir hale getirme yolları geliştirmeye ve uzun vadede yatırımlarını artırmaya yönelik çabalarımızı sürdürmeye devam edeceğiz" diyerek bu alandaki girişiminin ciddiyetini göstermiştir. Ayrıca Japonya merkezli bir finansal holding şirketi olan Nomura ise fon yönetimi, dijital

varlık güvenliği, dijital varlık yönetimi ve bankacılık alanlarında sahip olduğu uzmanlık çerçevesinde kripto para saklama hizmeti sunmaya başlayacağını duyurmuştur. Bunların yanı sıra Citigroup ve diğer büyük finans şirketlerinin de benzer girişimlerini sürdürdüğü bilinmektedir. Artan taleplerden dolayı, sigorta şirketleri de daha önce rafa kaldırdıkları hususları artık standartlaştırmaya yönelik çalışmalara başlamaktadırlar. Sigorta uzmanları, çalışanlar tarafından gerçekleştirilen hırsızlık ve dolandırıcılıklar, gizli anlaşmalar ve gasp olaylarının neden olduğu kayıp ve hasarlara yönelik koruma sağlayabilecek teminatlar hazırlamaya başlamışlardır (Houben ve Snyers, 2018, s. 27).

3- Siber Güvenlik

Japonya merkezli bir yazılım şirketi olan Trend Micro tarafından yayınlanan bir raporda, kripto para birimlerine yönelik yeteneklere ilgi artarken, bu bağlamda yeteri kadar güvenlik uzmanı yetiştirilemediği belirtilmiştir. Kurumsal ve bireysel yatırımcılar büyük kayıplarla, karmaşık yapıdaki fidye yazılımlarıyla, gasp olaylarıyla, yapay zekâ destekli botlarla* ve zayıf internet bağlantılarıyla karşı karşıya kalarak çeşitli problemler yaşamaktadırlar. Farklı sektörlerdeki siber tehditlere benzer şekilde, bu alanda da bilgisayar korsanları kullanıcılara, depolama alanlarına ve ilgili bilişim işlevlerine yönelik tehdit oluşturmaktadırlar. Kripto para şirketleri de çoğu geleneksel finans şirketi gibi merkezi bir şekilde çalışmaya başladıklarında, Blockchain teknolojisinin sunduğu ana güvenlik özelliğini yitirme riski ile karşı karşıya kalmaktadırlar. Blockchain, yüksek derecede güvenlik sağlayabilmektedir, ancak merkezi bir yapı ile çalışmaya başlandığında, bilgisayar korsanların ve diğer veri koruma uygulamaların sızma girişimleri de söz konusu olabilmektedir. Sektörün büyümesi ile birlikte gerekli düzenlemelerin yapılmadığı şirketlerin büyük ölçüde piyasaya baskın olduğu görülmektedir ve bu duruma bir sigorta uzmanının perspektifinden bakıldığında, gözetim seviyesi ve uygun iç kontroller hakkında sorunlar olduğu ortaya çıkmaktadır. Bir kesim sektör gözlemcileri, kripto para birimi sektöründeki büyümenin gelecekte çözüm sağlayıcılar ve güvenlik uzmanlarının hem sıcak (çevrimiçi) hem de soğuk (çevrimdışı) depolamanın iyileştirilmesine yönelik gözetiminin önemine dikkat çekmektedir. Bir kesim siber güvenlik uzmanına göre ise kripto para birimleri ile ilgili

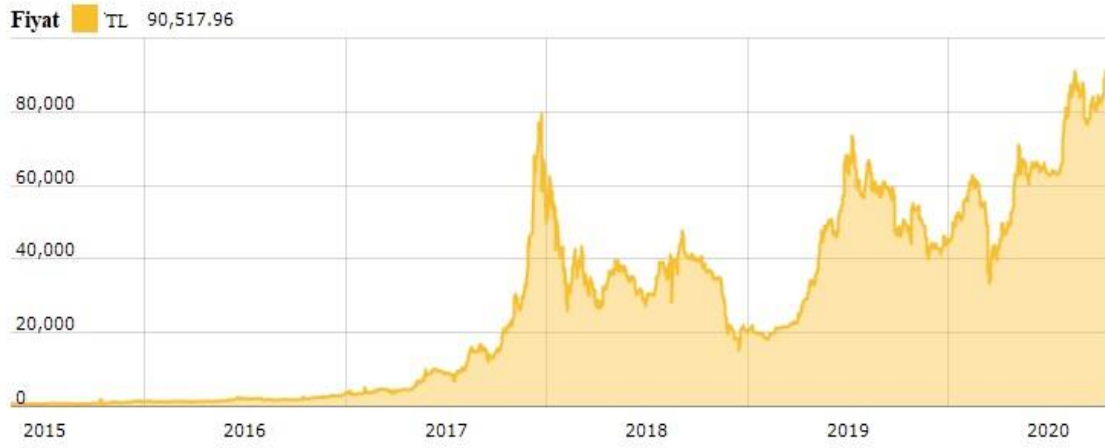
* Web ortamlarında gerçek kullanıcıymış gibi kötü amaçlı faaliyetle bulunan kişi/kurumları verilen isimdir

suçlar, diğer tüm alanlardaki siber saldırılardan daha fazla gerçekleştirilmektedir (Disparte, 2018).

4- Dalgalanma ve Likidite Azlığı

Kripto para borsaları, müşterilerin taleplerini karşılamak üzere kendi fonlarından ödeme yapmaktadır ve daha sonra kripto para piyasasında satış işlemleri gerçekleştirmektedirler. Bu nedenle, kripto para borsalarının göreceli olarak yüksek risk profillerine sahip olduğunu belirtmek mümkündür (European Central Bank, 2015, s. 23).

Şekil 03.1: Bitcoin Volatile Grafiği



Kaynak: (Cointelegraph.com, 2020)

ABD Hazine Bakanlığı tarafından desteklenen, “Kripto Para Birimi Riskleri ve Zafiyetleri” başlıklı bir çalışmada, kripto para birimlerinin büyük ölçekli kullanımının ve finans sektörü ile giderek artan bağlılığının finansal riskler yaratabileceği bildirilmektedir. IMF tarafından sağlanan verilere dayanan bu çalışmada iki örneğe yer verilmektedir. Bu örneklerden ilki daha ucuz ve daha az düzenli faaliyetler yürüten kripto para şirketlerinin yarattığı rekabetten kaynaklanan ve bankacılık gelirine yönelen tehditler ve ikincisi de kriptografik risklere karşı savunmasızlıktır. Kripto para likiditesi, yetersiz işlem gören piyasalarla birlikte piyasaya girişte karşılaşılan düzenleyici ve teknik engeller nedeniyle daha da kötüleşmektedir. Bitcoin ve diğer kripto para birimlerinin oynaklığı, bunların birer para birimi olarak yararlılıklarını büyük ölçüde azaltmakta ve likidite sorunlarının daha da büyümesine yol açmaktadır. Bununla birlikte, IMF, yükümlülüklerini yerine getiremeyecek, borçlarını ödeyemeyecek veya

gerektiğinde kullanıcılara likidite sağlamak hususunda problem yaşayabilecek üçüncü taraf kurumlar tarafından tutulan kripto para birimlerinin kredilendirilebilirlik ve likidite açısından risk oluşturabileceğini ifade etmektedir (Leopold ve Vollmann, 2018, s. 23).

5- İş ve İtibar ile İlgili Riskler

Bilhassa finans kurumları başta olmak üzere şirketler, kripto para birimlerine yönelik bir strateji oluşturma konusunda baskı altındadır. Ayrıca, kripto para birimlerinin ana akım ödeme unsuru haline gelmeye başlaması ihtimaline karşılık, bu şirketlerin gerekli yatırım ölçeği hususunda doğru öngörülerde bulunmaları beklenmektedir. Ayrıca, kripto para birimlerini içeren süreçler, şirketler için itibar ve marka açısından da önemli riskleri beraberinde getirmektedir. Kripto paralar ile ilgili faaliyetlerde bulunan köklü finans kurumları, kripto para işlemlerine yönelik stratejiler oluşturarak ve uygulayarak yeni müşteri kazanımı yoluna gitseler de mevcut müşterilerin geleneksel hizmetlerden ayrılma yönünde bir çekince göstermesi kuvvetle muhtemeldir (Santhana ve Biswas, 2017, s. 5) (Young Entrepreneur Council (YEC), 2018).

6- İşlem Güvenliği (Operasyonel Güvenlik)

Kripto para birimi alanındaki işlemler nihaidir ve geri alınamaz niteliktedir. Bu durum değişmezlik faktörü olarak adlandırılmaktadır. Değişmezlik faktörü başta olmak üzere dikkate alınması gereken belli başlı işlem güvenliği sorunları söz konusudur. Bu sorunları şu şekilde sıralamak mümkündür:

- Kripto para transferinin yanlış bir hesaba gerçekleştirilmesi ya da başka bir ifade ile yanlış bir “cüzdana” gönderilmesi halinde, kripto paralar kaybolur ve bu işlem geri alınamaz,
- Alım – satım işlemi gerçekleştirilen şirketlerde çalışan bir kimse ya da kötü niyetli bir komisyoncu/tüccar, kripto para transferini kurumun cüzdanı yerine kendi cüzdanına yaptığı takdirde bu işlem geri alınamaz ve transfer edilen kripto paraların kurtarılması için yapılacak çok az şey vardır,

- Kripto para işlemleri faaliyetlerinin gerçekleştirildiği bir borsa, bir siber saldırıya maruz kalırsa ve bundan etkilenirse ya da kullanıcılar şifrelerini ve/veya kullanıcı adlarını kaybederse, kripto paralar tamamen yitirilir,
- Kripto paraların saklandığı bir bilgisayarın siber saldırıya uğraması halinde, bu saldırı sonucunda kripto paralar çalınırsa, bu kripto paralar geri çevrilemez şekilde yitirilir (Bodden vd., 2019).

Sayılan bütün bu nedenlerden dolayı, güvenlik unsuru bu alanda oldukça büyük bir öneme sahiptir. Bu nedenle, bir borsadaki kripto paraların yerel bilgisayarlarda ve çevrimdışı olarak saklanması hususunda bir denge gözetilmelidir.

7- Kara Para Aklamanın Önlenmesine Yönelik Sorunlar

Anonim ya da takma isimlerle gerçekleştirilmesi nedeniyle, kripto para işlemleri doğası itibarıyla, suçluların para aklaması için oldukça uygun bir alandır. Bunun için, müşterilere yönelik yasal hususların kapsam ve içeriklerinin iyi bilinmesi, kuruluşların suç faaliyetlerini kolaylaştırmadığından emin olmak adına oldukça önemlidir. Kripto para piyasalarında gerçekleştirilen herhangi bir işlem, kara para aklamak amacıyla kullanılabilir. Bu nedenle, kripto para biriminin fon veya sermaye kaynağı olarak kullanıldığı işlemler genellikle yüksek risk grubunda değerlendirilmektedir. Bir kişinin kripto parayı hangi yolla ve nereden temin ettiğini tespit etmek, yasal paraya göre çok daha zordur (Paul, 2019).

Bütün yeni teknolojilerde olduğu gibi kripto para birimleri ile ilgili teknolojilerin etrafındaki ekosistem de hızla gelişmektedir. Kripto para birimleri ile ilgili işlemleri gerçekleştirmeden önce bir yatırımcının ya da bir şirketin, kripto para birimlerinin doğasını, kripto para ile ilgili teknolojilerin nasıl çalıştığını ve bu teknolojilerle ilgili ekosistemin yapısını anlaması oldukça önemlidir (BIDITEX Exchange; The Startup, 2019).

Günümüzde, kripto para birimleri, modern toplumda giderek daha popüler hale gelmektedir. Batı ülkelerinde, kripto para birimleri ile işlem yapan ATM'ler ortaya çıkmakta, dijital paralar internet üzerinden kolaylıkla alınıp satılmakta ve birçok ciddi finansal analiz şirketi dijital para hareketlerini ve piyasalardaki dalgalanmaları yakından

takip etmekte ve bununla ilgili öngörülerde bulunmaktadır (Holman ve Stettner, 2018, ss. 31-32).

Her ne kadar güvenli bir para birimi olamasa da Bitcoin de diğer tüm ödeme yöntemleri gibi mevcut ekonomiye entegre edilmiştir. Bundan dolayı Bitcoin de diğer ödeme yöntemlerinin her biri gibi birtakım riskler taşımaktadır. Ancak, bugüne kadar geçen sürece dayanarak, kripto para biriminin umut vadeden bir geleceğe sahip olduğunu söylemek mümkündür. Ancak, kripto para piyasasındaki beklenmedik fiyat dalgalanmaları ve bilhassa ani düşüşler, en deneyimli yatırımcıları bile ihtiyatlı olmaya sevk etmektedir (Bodden vd., 2019).

8- Deneysel Aşama Riskleri

Unutulmamalıdır ki kripto para kavramı yenilikçi bir yaklaşım olduğu kadar yeni bir teknolojidir. Bu nedenle, kripto para teknolojilerinin ne denli güvenilir olduğunu değerlendirmek adına yeterli tarihsel veri ve deneyim birikimi mevcut değildir. Bitcoin de diğer kripto para birimleri gibi halen geliştirilme aşamasındadır. Bu nedenle, her an beklenmedik ve istenmedik durumlar söz konusu olabilir. Bu durum sadece ekonomik varlıklarda değil deneysel teknolojilerin tamamında geliştirilme aşamasında sıklıkla karşılaşılan bir durumdur. Bununla birlikte, Bitcoin en aktif şekilde kullanılan kripto para birimi olması nedeniyle, muadillerine göre daha az “deneyseldir”. Ek olarak ifade etmek gerekir ki, geleneksel ve muhafazakâr yatırımcılar için tasarlanmamış olan kripto para birimleri yüksek riskli olarak değerlendirilmektedir (Sloan, 2018).

9- Teknoloji Riskleri

Teknolojik öğeler, daima, çok hızlı ve çoğu zaman kontrolsüz bir şekilde gelişmektedir. Herhangi bir kullanıcı, Bitcoin’in zaten var olduğunu ve ayrıca Bitcoin’in varlığını korumasına ek olarak çok sayıda rakibi olduğunu da bilmektedir. Marka bilinirliği ve büyük risk sermayesi takviyesinden kaynaklanan avantaja rağmen, diğerlerine göre daha gelişmiş bir kripto para biriminin potansiyel görünümü, diğer kripto para birimleri için gerçek bir teknolojik risk teşkil etmektedir. Yatırımcılar, kripto varlıkların ne zaman değer kaybedeceğini önceden kestiremeyebilirler (Macwan, 2019).

10- Tüketicinin Korunması

Bitcoin, tüketicinin korunmasına yönelik herhangi bir etki sağlamamaktadır. Bir Bitcoin işleminin geri alınması mümkün değildir. Başarısız bir işlemden sonra geriye kalan tek seçenek, parayı alan tarafın gönüllü olarak parayı iade etmeye ikna edilmesidir. Bunun nedeni, banka üzerinden yapılan işlemlerde olduğu gibi herhangi bir garantör aracı kurumun olmamasıdır. Bitcoin işlemleri, yalnızca iki tarafın söz konusu olduğu bir nakit işlemine benzemektedir. Bununla birlikte, işlemlerin bu geri döndürülmez olma özelliği, Bitcoin yatırımları üzerinde göreceli olarak düşük düzeyli bir risk oluşturmaktadır. Ancak, yatırımcıların bu tür bir riskin varlığı konusunda bilinçli olmaları gerekmektedir (Price D. , 2018).

11- Saldırı Riski

Geleneksel finans kurumlarının aksine, kripto para işlemleri doğası itibariyle merkezi olmayan bir yapıda gerçekleştirilmektedir. Örneğin, %51 Saldırıları, bu yöndeki risklerin en bilinenlerinden biridir. Bu tür saldırılar başarılı oldukları takdirde, saldırganlar Blockchain ağının operasyonel kontrolünü ele geçirebilmektedir.

Piyasada nispeten yüksek fiyattan işlem gören bir kripto para birimi ağ saldırılarının hedefinde yer alabileceği gibi nispeten düşük bir faaliyete ya da hash* oranına sahip bir Blockchain ağı da ağ saldırılarının hedefi olabilmektedir. Düşük hash oranı saldırıyı daha kolay bir hale getirirken, çalınan kripto para birimleri saldırgana önemli miktarda bir haksız kazanç sağlamaktadır. Bu nedenle, karma oranla ölçülen sistem tabanlı ölçütler ile fiyatla ölçülen finansal piyasa tabanlı ölçütler arasında tutarsızlığın söz konusu olduğu kripto para türlerinin %51 saldırılarına maruz kalma olasılığı çok daha yüksektir (Frankenfield, 2019) (Liquid.com, 2019).

3.4.Dolandırıcılık ve Kara Para Aklama

Geleneksel finans sisteminde, fonlar bankacılık sektöründe gizlilik içerisinde tutulmakta ve bu gizlilik idari ve yargı kanallarınca desteklenmektedir. Ancak bu husus, kripto para birimlerinin kullanıma başlanmasıyla büyük ölçüde değişikliğe uğramaktadır.

* Hash Oranı: Kripto paralarda saniye başına bulunan hash miktarıdır. Buradaki hash doğru şifreyi bulmak için yapılan denemelerdir.

Kripto para birimleri ile gerçekleştirilen işlemlerde, işlem güvenliğinin sağlanması için herhangi bir üçüncü taraf aracı kuruma ihtiyaç duyulmamaktadır. Banka, birinin bilgilerini açıklamaya kanunlarla zorlanabilirken, Bitcoin sisteminde böyle bir durum söz konusu olmamaktadır (Sprenger ve Balsiger, 2018, s. 2).

Bununla birlikte, mevcut dijital para birimlerinin çoğunda halka açık ve kalıcı bir deftere kaydedilerek işlem gerçekleştirilmektedir. Örneğin, Bitcoin, pek çok kişinin inandığının aksine tam anlamıyla anonim değildir. Yetkililerin bir cüzdan adresi ile bir suç arasında bağlantı kurmaları halinde, mevcut ya da gelecekte gerçekleştirilecek her işlem izlenebilir, analiz edilebilir ve işlemler ile hesabın anonimliği ortadan kaldırılabilir (Canellis, 2018).

Kripto para karıştırma hizmetleri, kara para aklayan kripto para hesaplarını parçalayarak diğer adresler ile karıştırmakta ve böylece hesabı temize çıkarmaktadır. Bu tür “karıştırıcı” hizmetlerinin standart kullanım ücretleri, cüzdanda bulunan ve karıştırılmaya konu olan kripto para tutarının %1 - %3’ü arasında değişmektedir. Bu sistem, öncelikle normal internet ağında ya da başka bir ifade ile “Clearnet” üzerinde bulunan Bitcoin cüzdanına erişmekte ve daha sonra yalnızca “DarkWeb” üzerinde çalışan iki veya daha fazla Bitcoin cüzdanına erişerek bu cüzdanlar üzerinde karıştırma işlemi yapmaktadır (Cryptocurrency tumbler/Wikipedia, 2015).

Başlangıç olarak "clearnet" üzerindeki cüzdandan alınan kripto para Tor üzerindeki gizli cüzdanlardan birine gönderilmektedir. Bu tür işleme “atlama” adı verilmektedir. Atlama işlemi, DarkWeb üzerindeki Bitcoin cüzdan adreslerine birden çok kez gerçekleştirilir ve her atlama işlemi ile bir şaşırtma katmanı oluşturulur. DarkWeb üzerinde yer alan bir cüzdanda karıştırma işlemi gerçekleştirilir. Her biri saygın olduğunu iddia eden ve kullanıcı tarafından talep edilen anonimlik düzeyine bağlı olarak çeşitli ücretler talep eden çok sayıda karıştırma hizmeti sağlayıcısı vardır. Karıştırıcı, Bitcoin’i otomatik olarak birden fazla işleme bölmektedir ve rastgele aralıklarla, işlemlerin birbiriyle olan anlamlı bağlantılarını ortadan kaldıran, Tor tarafından barındırılan Bitcoin adresine göndermektedir (Wegberg vd., 2018, s. 423).

Karıştırma işlemi tamamlandıktan sonra, Bitcoin, diğer kripto para birimleri ve hatta yasal para ile takas edilmek üzere bir kripto para borsasına yatırılacak kadar temiz hale getirilmektedir. Bu karıştırma hizmetlerinin ne kadar etkili olduklarının

belirlenmesi üzerine araştırma halen devam etmektedir. Ancak, araştırmacılar, en tanınmış ve en köklü karıştırma hizmet sağlayıcılarının bile ciddi güvenlik ve mahremiyet problemleri taşıdığını tespit etmiş ve bu tür hizmetlerin suç faaliyetleri için kullanılabileceğinin altını çizmişlerdir (Wegberg vd., 2018, s. 429).

Bitcoin, düzenlemelerden uzak borsalarda kolaylıkla aklanmaktadır. Düzenlemeler kapsamında denetlenmeyen Kara Para Aklama ile Mücadele (AML) gibi kimlik kontrollerine dayalı prosedürlerin olmadığı kripto para birimi değişimleri Bitcoin ile kara para aklamaya imkân tanımaktadır (Sprenger ve Balsiger, 2018, s. 3).

Bu işlemler, Bitcoin'in çeşitli borsalarda birkaç kez takas edilmesi ile gerçekleştirilebilmektedir. Örneğin, bir kullanıcı düzenlemeler kapsamında denetlenmeyen bir borsaya Bitcoin yatırabilmekte ve bunu çeşitli altcoinlerle değiştirebilmektedir. Bir komisyoncu/tüccar, bir türdeki kripto para birimini diğer türdeki kripto para birimi ile değiştirdiğinde, cüzdan adresleri arasında atlama işlemine benzer gizlilik dereceleri eklenmektedir. Bunun ne kadar etkili olduğu büyük ölçüde değişim sisteminin altyapısına ve teknolojisine bağlı olsa da bu yaklaşım tam anlamıyla etkili ve sağlam bir çözüm değildir. Böyle bir durumda, kullanıcı, kripto parayı sahip olduğu anonim değişim hesapları aracılığıyla harici bir kripto para birimi cüzdanına aktarabilmektedir. İşlemin gerçekleştirildiği borsaya bağlı olarak, kirli kripto para aklanarak yasal banknotlara dönüştürülebilse de düzenlenmemiş borsalarda yasal para hareketleri zor ve genellikle kısa ömürlüdür (Fanusie ve Robinson, 2018, ss. 4-5).

Ayrıca bu karıştırma hizmetlerinin daha az yasadışı ancak yine şüpheli olan kullanımları söz konusudur. Özellikle, Coinbase gibi düzenlenmiş borsalar, kripto para ile kumar oynatan siteler ile muhtemel etkileşimlere yönelik olarak ağlarını düzenli olarak kontrol etmektedirler. Bu nedenle, Coinbase ve benzeri düzenlenmiş borsalara para yatırmadan önce, Blockchain kumarhanelerine maruz kalan dijital fonlar temizlenmesi, ultra-yasadışı kara para aklamanın ötesinde sıklıkla bahsedilen bir kullanım durumu olarak karşımıza çıkmaktadır. Bitcoin gibi günümüzün önde gelen para birimleri, zaman tespiti geçebilir ya da geçemeyebilir ancak temel teknoloji daima kalıcıdır. Yenilikçi girişimciler, kripto para biriminin heyecan verici ancak kimilerine göre korkutucu olan dünyasına yeni bir kapı açmaktadırlar (Canellis, 2018).

Tarihsel sürece bakıldığında, kara para aklayan suçluların, düzenleyici kurumları, kolluk kuvvetlerini ve AML profesyonellerini daima atlatılabildikleri görülmektedir. Dolandırıcılıkla mücadele uzmanları, kripto para birimlerini içeren kara para aklama faaliyetlerinin geleceğinin nasıl olacağı üzerine ciddi şekilde kafa yormaktadır. Böylece, kendilerinden bir adım önde olan kötü adamları yakalayıp onların önüne geçmek mümkün olacaktır (Engle, 2016, s. 343).

Kripto para ekosisteminde geliştirilen farklı türdeki dijital para birimlerinin ve uygulamalarının incelenmesi, onların kara para aklama ve dolandırıcılık açısından yüksek riskli olmasına yol açan etkenlerin ve nedenlerin daha iyi anlaşılmasını sağlamaktadır.

eCache gibi bazı dijital birimleri tamamen anonimdir. Operatörlerine göre, eCache kişi ile işlemleri birbirine bağlamamakta ve ilişkilendirmemektedir. eCache, internetteki diğer veriler gibi başka bir tarafa aktarılabilen bir Dijital Taşıyıcı Sertifikası (DBC) gibi çalışmaktadır. Öyle ki, daha sonra şifresi çözülmekte ve sahibine sertifikayı destekleyen varlıkların tanımlanmış bir kısmına yönelik hak sağlamaktadır (Sibenik, 2019).

Diğer kripto para birimleri de tıpkı Bitcoin gibi, tüm işlemleri hakla açık bir defter olan Blockchain üzerinde saklamaktadır. Blockchain, kullanıcıların kimliklerini değil yalnızca işlemlerini kaydetmektedir. İnternet Protokolü (IP) adreslerinin Bitcoin işlemleri ile ilişkilendirilmesi mümkündür ancak, TOR ağı ile bir kullanıcının IP adresi gizlenebilmekte ve kullanıcıya tam anonimlik sağlanabilmektedir. Böylece kullanıcı, son hedefe erişmeden önce rastgele seçilen vekil (Proxy) sunuculardan oluşan dağıtılmış bir ağ üzerinden güvenli bir şekilde bağlantı sağlamaktadır (Laurence, 2017, s. 4).

- Dark Wallet

Bu Bitcoin uygulaması, tüm kullanıcı ödemelerini şifreleyerek ve karıştırarak, kripto para biriminin izinin takip edilmesini neredeyse imkânsız hale getirmektedir. “Dark Wallet” adlı uygulama ile Bitcoin işlemleri tamamen izlenemez bir hale gelmektedir.

Dark Wallet’in geliştiricisi Amir Taaki ile yapılan bir röportajda, terörist örgütlerin bu uygulamayı kullanabileceğinin farkında olduğunu ancak yine de bu

uygulamayı desteklediğini belirtmiştir. Taaki şöyle demiştir: “Kişisel önyargılarınız nedeniyle teknolojiyi kullanmaktan vazgeçemezsiniz Kim olursa olsun, herkesin katılabileceği özgür ve açık sistemleri destekliyoruz.” (Taki ve Todd, 2014).

Birden fazla yetki ve yargı alanında hızlı ve anonim işlem gerçekleştirme yeteneği, kripto para birimlerini kara para aklayan suçlular için oldukça çekici bir mecra haline getirmektedir (Greenberg, 2014).

- Online Borç Veren Pazarları

BTC Jam gibi şirketler, para birimi olarak Bitcoin’in kullanıldığı bir alanda, küresel ölçekte borç verenler ile borç alanları buluşturmayı amaçlamaktadır. Kendini dünyanın en büyük uçtan uca borç verme pazarı olarak ilan eden BTC Jam, aynı zamanda bu sistem aracılığı ile kitle fonlaması da sağlamaktadır. Bu durum, suç fonlarının yerleştirilmesi veya katmanlanması için sayısız olasılığa kapı açmaktadır (BTCJam/Wikipedia, 2014).

- Kitle Fonlaması

Kitle fonlaması, kara para aklamak için çeşitli şekillerde kullanılabilir. Örneğin bir ihraççı kuruluş, bir ticari işlem maskesi altında, bir organize suç örgütü ile menkul kıymetler karşılığında para takası yapmak için yatırımcılarla iş birliği yapabilmektedir. Bir FINCEN raporunda bildirildiği üzere (Yerak, 2015), şüpheli faaliyet raporları, kara para aklamak, terörizmin finansmanı, kredi kartı dolandırıcılığı, kimlik hırsızlığı, hesapların ele geçirilmesi, kimlik avı planları ve paravan şirket suiistimleri için kitle fonlaması platformlarının yasadışı kullanıldığını ortaya koymaktadır (Robock, 2014, s. 124).

Bir kitle fonlaması başlangıcı olan Swarm, Kickstarter veya Indiegogo gibi ana kitle fonlaması sitelerine benzemekte, ancak Swarm üzerinde para birimi olarak Bitcoin kullanılmaktadır. Bitcoin’in oldukça büyük bir şekilde kısıtlandığı BitPay, Coinbase ve Circle gibi sistemler üzerinden Bitcoin ile çok az yere ve sınırlı şekilde ödeme sağlanmaktadır. Bu durum, BitPay, Coinbase ve Braintree gibi şirketlerin komisyoncu/tüccar ödemelerini için Bitcoin işlemesi gibi etkilerle hızla değişmektedir. CoinDesk’te yayınlanan bir makaleye göre, BitPay üzerinden her gün yaklaşık 1 Milyon

Dolar hacminde Bitcoin ödemesi gerçekleştirilmektedir. BitPay'in 10000 olan müşteri sayısı yalnızca dokuz ay gibi bir sürede 30000'e ulaşmıştır (Hajdarbegovic, 2014).

Son derece yenilikçi bir şirket olan Circle, müşterilerinin kredi kartı ile Bitcoin almalarına imkân tanımaktadır. Ayrıca Circle'a rakip olan Coinbase adlı platform da benzer bir içerik sunmaktadır. Circle, çok yakında nakit olarak finanse edilebilen ön ödemeli banka kartlarının da kabul edileceği bir girişimi olacağını duyurmuştur (Coinbase.com, 2018).

Burada, örnek bir vaka senaryosundan söz etmek mümkündür. Bu senaryoya göre, Bir suçlu birden fazla ön ödemeli banka kartına, yasadışı yollardan edindiği nakit paraları yükleyerek, bu paralara Bitcoin satın almaktadır. Daha sonra, suçlu, bu Bitcoinleri çevrimiçi mal ve hizmet satın almak için kullanmaktadır. Kara para aklamanın üç aşaması olan yerleştirme, katmanlama ve entegrasyon bu kısa örnekle gösterilmektedir.

Bu alanda soruşturma yapan uzmanların karşılaştığı en ciddi zorluklardan biri kara para aklama sürecinin takibi ve izlenmesidir. Ancak kara para aklama süreci tamamen çevrimiçi şekilde gerçekleştirildiğinde, bu durum geleneksel kara para aklama yöntemlerine kıyasla iz sürmeyi daha kolay hale getirmekte ve cezaya konu olan eylemin izlerini takip etme sürecini hızlandırabilmektedir. Kripto para birimlerinin işlenmesi daha kolay hale geldikçe, bunların kumarhaneler, çevrimiçi müzayedeler, rehin komisyoncuları ve kullanılmış araba satıcıları gibi diğer yüksek riskli sektörlerde giderek daha fazla kullanılacağını öngörmek mümkündür.

- Dijital Sermaye Piyasası

“Colored Coins” olarak bilinen, Türkçe'ye renkli paralar olarak da çevrilmesi mümkün olan katmanlar, diğer potansiyel olarak fiziksel varlıkları temsil etmek için Bitcoinleri kullanan, Bitcoin üzerinde yer alan ek katmanlardır. Örneğin, Bitcoin Blockchain'indeki işlemler, hisse senedi, menkul kıymetler ya da arazi tapusunu temsil etmek için kullanılabilir. Business Insider'da yayınlanan bir makalede, Colored Coins'i geniş kitlelere yaymaya çalışan start-up şirketleri ChormaWay ve Colu sayılmaktadır (Price R. , 2015).

- Dijital Para Hizmeti Şirketleri

Suçlular, kara para aklama sürecinin her aşamasında para hizmeti şirketlerini (MSB) istismar etmektedir. MSB'ler, resmi bankacılık hizmetlerine erişimi olmayabilecek kişilere döviz bozdurma ve para gönderme gibi işlemler de dahil olmak üzere çok çeşitli ve değerli finansal hizmetler sağlamaktadırlar. Ancak, genellikle uygun kayıt veya uyum rejimi olmadan çalıştıkları ve çoğu zaman düzenlemelerin dışında kalan denizaşırı iş ortaklarıyla işlem yaptıkları için önemli bir tehdit oluşturmaktadırlar (Lathrop Gage, 2018). ABD'de, Hazine Bakanlığı, Adalet ve İç Güvenlik Bakanlığı, ABD Merkez Bankası ve ABD Posta Servisi tarafından oluşturulan bir raporda, döviz büroları ile geleneksel müşteri ilişkilerinin kısa süreli doğası ve birden fazla dijital para biriminin anonimliği, kara para aklama olasılığını gündeme getirmekte ve bir tehdit unsuru olarak ortaya çıkmaktadır (DOJ, USDT, DHS, Federal Reserve, USPS, 2005, s. 10).

3.5.Kripto Para Birimleri Kara Para Aklama ve Terörizmin

Finansmanında Kullanımı

Kripto para birimleri, bankalardan veya geleneksel para hizmeti işletmelerinden daha fazla anonimlik sunsa bile, bu yeni para birimi kara para aklamayı kolaylaştırmak için ideal bir platform olma özelliği taşımamaktadır. Suçluların kullandığı sistemler hayli karmaşık olmakla birlikte, ileri düzeyde bilgisayar bilgisinin yanı sıra dolandırıcılık ve kara para aklama deneyimi de gerektirmektedir. Büyük suç örgütleri, suça yönelik işlemlerinin ifşa edilmesinden kaçınmak amacıyla ayrıntılı bir sistem oluşturmak adına yeterli kaynaklara erişebilmektedirler. Bununla birlikte, yeterli bilgi ve kaynaklar olmadan, bireyler, fonları aklamak için ödeme platformları, ön ödemeli banka kartları ve normal banka hesapları gibi geleneksel yöntemleri daha çok kullanmaktadır. Kara para aklama girişimleri uzmanlık ve adanmışlık gerektirmektedir ki bu durum çoğu kullanıcının kaçındığı ya da gözden kaçırdığı bir noktadır. Ayrıca, kripto para birimlerindeki değer dalgalanmaları, para aklama için ek bir risk faktörüdür. Oysa standart ücretli bir ödeme aracı veya ödeme platformunun kullanılması, suçlulara fonlarının ne kadarının aklanabileceğini tahmin etme imkânı sağlamaktadır (Demeter, 2018).

Kara para aklama işlemleri için kripto para birimleri günümüzde, bir zamanlar hayal edildiği kadar istenen bir araç değildir. Ancak, kurumlar yine de bu bağlamda gerekli inceleme ve tespitleri dikkatli bir şekilde gerçekleştirmek durumundadır (Acheson, 2019). Bu yönde halen gelişmiş durum tespiti prosedürleri ve dikkat noktaları söz konusudur. Atlanta Merkez Bankası, kripto para birimi ile ilgili işletmeleri ve kripto para birimi işlemlerine izin veren şirketleri takip etmek amacıyla finansal kurumlara yararlı bir rehberlik hizmeti sağlamaktadır. Atlanta Merkez Bankası, finans kurumlarının diğer yüksek riskli finansal işlemlerin yanında kripto para birimi işlemlerini de izlemesini önermektedir. Kripto para birimi ödeme işlemcileri için sağlanan bu uzmanlaşmış rehberlik hizmeti, finansal kurumların müşterinin kripto para birimi ile gerçekleştirdiği işlemlere izin verme motivasyonunun anlaşılır hale gelmesini sağlamaktadır (King, 2016, s. 8).

Daha önce FinCEN tarafından tespit edilen kara para aklama ve terörizmin finansmanına yönelik olumsuz bulgular, kripto para birimleri için de geçerlidir, ancak kripto para birimi işlemlerine özel olarak olumsuz bulgular tespit edilmiştir. Örneğin, kripto para birimi işlemcileri için bir olumsuz bulgu, bir satıcının diğer elektronik işlemleri işleyememesidir. Çünkü bu satıcının yasadışı ürünler satmasından veya büyük hacimli ters ibrazlara, iadelere veya aldatici satış taktikleri veya düşük ürün kalitesinden kaynaklanan müşteri şikayetlerinden kaynaklanabilmektedir. Bilgisayar sunucularının satın alınması ve kripto para birimi kullanılarak etki alanlarını kaydettirmek için yapılan ödemeler bir tür olumsuz bulgu olarak değerlendirilmelidir (FinCEN, 2019, s. 7).

Yeterli kaynak ve zamanın ayrılması ile en ayrıntılı kara para aklama işlemleri bile takip edilebilmekte ve bu yöndeki planların önüne geçilebilmektedir. Ancak başlangıçta, kripto para birimlerinin anonimlik sağlayabileceğine ve düzenleyicilerin erişemeyeceği bir para transfer sistemi sağlayabileceğine inanılmıştır. Günümüzde ise ilgili otoriteler ve devlet kurumları, bu yeni para birimi ile gerçekleştirilen işlemlerin takibi hususunda hassasiyet göstermektedirler. Genel olarak, kripto para birimlerinin kara para aklama ve suç faaliyetlerini kolaylaştırma amacıyla kullandığı düşünülmektedir. Bu nedenle, finansal kurumlar, kripto para birimleri ile gerçekleştirilen işlemleri izlemeli ve olumsuz bulguları araştırmalıdır. Bununla birlikte, bireyler, anonimliğin azaldığını ve kripto para birimi işlemlerine yönelik takip

ve gözetimlerin arttığını öğrendikçe, suçlular kripto para birimi kullanımını azaltma yoluna gidebilmektedir (FATF, 2019, ss. 20-22).

Kripto para piyasaları, çok çeşitli suç faaliyetlerine ve mali suçlara karşı potansiyel olarak savunmasızdır. Bu tür risklerin çoğu Blockchain kendisinde değil, çevredeki ekosistemde, VCE'lerde ve tüketicinin DLT'ye erişimini destekleyen cüzdanlarda gerçekleşir. Hızla gelişen teknoloji ve yeni kripto paraları oluşturmanın daha kolay hale gelmesi ile birlikte, kolluk kuvvetlerinin ve AML gerekliliklerine tabi olan finansal kurumların suç takibinin zorlaşacağı düşünülmektedir (King, 2016, s. 8).

Bütün bunlara ek olarak, kripto para birimlerinin anonimliği, likiditesi ve sınırsız doğası, kripto para birimlerini potansiyel kara para aklayıcıları için oldukça cazip kılmaktadır (King, 2016, s. 8).

- **Yerleştirme:** Hesapların hızlı ve anonim olarak açılması, suç örgütlerinin yasa dışı parayı dönüştürmesi ve konsolide etmesi için düşük riskli bir yol sağlamaktadır.
- **Katmanlama:** Kripto para birimi, yasadışı gelirleri sınırların ötesine taşımak için ideal bir yol sağlamaktadır. Kripto para birimi, malların fiili veya hayali satışında "geri ödeme" olarak sınır ötesi para transferlerinde kullanılmaktadır. ABD Uyuşturucu ile Mücadele İdaresi, Çin'in sermaye kontrollerinden kaçınmak üzere Bitcoin talebinde bulunduğunu, ABD, Avrupa ve Avustralya'da toplu yasal nakit sağlama amacıyla bir pazar oluşturulduğunu ve lisanslı ya da lisanssız tezgâh üstü Bitcoin borsalarında yoğun yasadışı hareket gerçekleştirildiğini bildirmektedir (Drug Enforcement Administration, 2017, s. 130). Benzer şekilde, 2018 yılının Nisan ayında, Avrupalı yetkililer de uyuşturucu kaçakçılığından elde edilen nakit gelirlerin İspanya'dan Kolombiya ve Panama'ya transferi için Finlandiya'dan faaliyet gösteren bir Borsadan satın alınan Bitcoinler ile gerçekleştirilen bir kara para aklama eylemini tespit etmişlerdir (Europol, 2018). Ayrıca kayıt dışı ICO etkinlikleri de büyük ölçekli katman oluşturma fırsatları sağlamaktadır. Kara para aklayan suçluların kontrol ettikleri ICO'lar ile kripto para cinsinden edinilen yasadışı gelirler, yasal para birimlerine dönüştürülmekte ve hileli bir sermaye artırımını işlemi gerçekleştirilmektedir.

- **Entegrasyon:** Kripto para birimleriyle satın alınabilen malların çeşidi ve sayısı arttıkça, entegrasyon fırsatları da bununla doğru orantılı olarak artmaktadır. Örneğin, İtalyan Ulusal Noterler Konseyi, kripto ödeme kaynağının anonim yapısının, kimliğin tanımlanmasını engelleyebileceğinden dolayı kripto para birimleri aracılığı ile gayrimenkul satın alımında işlemin tarafları için daima şüpheli işlem raporu hazırlanması gerektiğini bildirmektedir. ICO etkinlikleri ile kripto para ticareti yapma istekliliği, bu kapsamdaki şirketlerin farkında olarak ya da olmayarak organize suç örgütlerinin işlerini kolaylaştırabilmektedir (Miggiani, 2020).
- **Terörizmin Finansmanı ve Yaptırımlardan Kaçınma:** Kripto paraların oluşturulma kolaylığı ve anonimliği, kripto para hesaplarını, terörizme finansman sağlama ve yaptırımlardan kaçınma gibi yasadışı işlemler için ideal hale getirmektedir. Terörizmin finansmanında kripto para birimlerinin kullanımı henüz çok yaygın olmasa da, 2014 yılından beri terörist grupların kripto para birimleri üzerine çalışmalar yaptığı bilinmektedir. Bununla birlikte, sosyal medya üzerinden ya da kitle fonlama yöntemiyle çalışan bağış platformları üzerinden yürütülen kampanyalar ile Bitcoin ile yardım kabul ederek, bu gelirleri faaliyetlerinde kullanan terör örgütleri de vardır. Ayrıca, yaptırımlardan kaçınmaya çalışan devletler de kripto para birimleri ile işlem yapma yoluna gitmektedirler. Örneğin, 2018 yılının şubat ayında Venezuela devlet destekli bir kripto para birimi yaratma yoluna gitmiştir (Goldman vd., 2017, s. 15) (Reuters, 2018).

Bütün bu riskler, düzenlemeler kapsamında faaliyet göstermeyen başka bir ifade ile kaçak kripto para piyasalarında artış göstermektedir. Kripto para piyasalarının geleneksel finansal hizmetler sektörüyle etkileşime girdiği her yerde anonimliğin reddedilmesi ve AML kontrollerinin uygulamaya konması için düzenleyici baskı göz önüne alındığında, kripto para piyasasının farklılaştığına dair işaretler görülmektedir. Bazı yeni kripto paralar, mevcut düzenlemelere daha uyumlu olacak şekilde oluşturulmaktadır. Bununla birlikte hala “gizliliğe önem veren” kripto paralar da vardır ve bunlar piyasa dışı işlemleri kolaylaştırmak için işlemlerin ve kimliklerin gizliliğine öncelik tanınmaktadır (Holman ve Stettner, 2018, s. 32).

1- Yatırım Dolandırıcılığı ve Bilgisayar Korsanlığı

Kripto varlık dolandırıcıları, kripto para birimi yatırımlarını teşvik etmek için sıklıkla ünlülerin veya tanınmış kişilerin resimlerini kullanarak sosyal medya üzerinden reklam vermektedirler. Bu reklamlar, profesyonel görünümlü web sitelerine bağlanmaktadır. Bu reklamlar yoluyla ilgili sitelere yönlendirilen kullanıcılar, kripto para birimleri veya geleneksel para birimlerini kullanarak bu dolandırıcı firma ile işlem yapmaya ikna ve teşvik edilmektedir (Actionfraud.police.uk, 2018).

Dolandırıcı firmalar genellikle hedefledikleri ülkenin dışında bir konumda yerleşiktir ancak son derece saygın bir adreste bulunduklarını iddia etmektedirler. Bu firmalar, fiyatları ve yatırım getirilerini bozmak için yazılımlarını manipüle edebilmektedir. Böylelikle insanlar, var olmayan kripto varlıkları satın alarak dolandırıcıların kurbanı olabilmektedirler. Ayrıca kullanıcıların çevrim içi hesapları aniden kapatılabilmekte ve fonlarını aktarmayı reddetmeleri ya da fon transferi gerçekleştirmek istediklerinde fidye niteliğinde yüksek ödemeler talep edilebilmektedir (DeVries, 2016, s. 4).

Kripto para sahipleri dikkatli olmadıkları takdirde kolaylıkla kripto dolandırıcılığı kurbanı olabilmektedir. En büyük dolandırıcılık biçimi ise bir kripto para birimi borsasının bilgisayar korsanlarınca ele geçirilmesi ve borsada depolanan kripto paraların çalınması şeklindedir. Buna dair en iyi bilinen örnek, Dünyanın en büyük Bitcoin Borsası olan Mt.Gox'un bilgisayar korsanları tarafından ele geçirilmesidir. Mt.Gox, kripto madenciliği platformları saldırıya uğradığında yaklaşık 470 milyon dolar tutarına karşılık gelen 850 bin Bitcoin kaybettiklerini bildirmiş ve bunu takiben 2014 yılının Şubat ayında iflas bildiriminde bulunmuştur (Pollock, 2018).

Kripto para birimi sahibi kişiler, elinde kripto para bulundurdıkları sürece muhtemel bir kayıp riski ile karşı karşıya kalmaktadırlar. Bu kişilerin kendilerini bilgisayar korsanlığı tehdidinden korumalarının en iyi yolu, kripto para birimlerini çevrimdışı bir cüzdana saklamalarıdır. Çevrimdışı cüzdanların bilgisayar virüslerine karşı daha güvenli olduğu bilinmektedir. Çeşitli donanım cüzdanları mevcuttur. Bunlara örnek olarak; KeepKey (Büyük boy), Nano Ledger S (Orta boy) ve Trezor (Küçük boy) verilebilmektedir (Hudson intelligence, 2018) (Chainbits.com, 2018).

Şekil 3.2: Trezor Kripto Para Cüzdanı One/T Modeli



Kaynak: (Trezor, 2020)

Kripto para birimi dolandırıcılığının bir başka kaynağı da ICO ya da başka bir ifade ile İlk Para Arzı etkinlikleridir. Bir ICO etkinliğinin arkasındaki bir Start-up şirketi, dijital tokenler oluşturmakta ve yeni işlerini finanse etmek için bunları satma yoluna gitmektedir. Bu tür firmalar genellikle, geleneksel bankalara borçlanmaktan ya da hisse senetlerinin satışından kaçınmaktadırlar. Yatırımcılar ise hisse senetleri yerine, değerinin artacağını umarak kripto tokenleri satın almaktadırlar. Bu tür bir faaliyet, dolandırıcılar için büyük bir fırsattır. Öyle ki, deneyimsiz ve hevesli yatırımcılar değersiz tokenleri alarak, şirket kurucularına büyük miktarda para kazandırmaktadır. Kötü niyetli şirket kurucuları ise sahte bir şirket kurarak, bu sahte şirket aracılığı ile düzenledikleri ICO etkinlikleri ile büyük bir dolandırıcılık faaliyeti gerçekleştirebilmektedirler. Buna dair en bilinen örneklerden biri 2014 yılında yaşanan PonziCoin olayıdır (Jenkinson, 2018).

Oldukça şüphe uyandıran bir isme sahip olmasına rağmen insanlar bu kripto para birimine yatırım yapmıştır ve ICO etkinliğinin ardından dolandırıcılar topladıkları paralarla kayıplara karışmıştır. 2017 yılında Rishab Hegde bir kripto para birimi yaratmış ve bu para birimine PonziCoin adını vermiştir. PonziCoin'in bu versiyonunda benzersiz olan şey, web sitesinde kurucusunun açıkça bunun bir Ponzi Şeması olduğunu söylemesidir. Bununla birlikte, birçok yatırımcı bunun bir aldatmaca olduğunu yönündeki uyarılara rağmen bu kripto para birimini satın almıştır. Hegde, 2018 yılının Ocak ayında yatırımcılara herhangi bir ödeme yapmadan, sistemi kapatmış ve herhangi bir suçlama ile karşılaşmamıştır (FAU - Centre of Forensic Accounting, 2019).

Dolandırıcılık amacıyla gerçekleştirilen ICO etkinliklerinin diğer yeni örnekleri; Bitconnect, OneCoin, Plexcoin, Centrtech, Pitcoin ve iFan olarak sıralanabilmektedir. Sahte ICO etkinliklerinin ve sahte platformlara çok sayıda örnek vermek mümkündür. Kripto para kullanıcıları ve kripto para almak isteyen yatırımcılar bu konuda çok iyi eğitilmiş olmalı, iyi bilinen platformları kullanmalı, yüksek getiri vaatleri ve piramit benzeri planlar gibi şüphe uyandıran durumlardan uzak durmalıdır. Ayrıca ICO etkinliklerindeki olası yatırımcılar, finanse etmek üzere oldukları projeyi etraflıca araştırmalıdır. Bu bir araştırma şunları içermelidir:

- Firmanın teknik raporlarını okumak ve fikrin mantıklı olup olmadığını değerlendirmek.
- Yönetim ekibi ile ilgili bilgileri gözden geçirmek.
- Profesyonellerin ve ICO sunan firmanın lisanslı olup olmadığını kontrol etmek (Investor-SEC, 2017).

2- Vergi Kaçakçılığı

Kripto para birimi ile gerçekleştirilen işlemlerin, kripto para ticaretinin ve madencilik işlemlerinin vergiye tabi olup olmadığı ülkelerin mevzuatlarında açıkça bildirilmektedir. Ancak bazı vergi mükellefleri kasıtlı olarak bu alandaki etkinliklerini ve bu etkinliklerinden elde ettikleri gelirleri bildirmeme yoluna gitmektedir. Bunun çeşitli nedenleri vardır (Marian, 2013, s. 44). En sık görülen nedenlerden ilki kişilerin kripto para birimleri ile gerçekleştirdikleri faaliyetlerin tespit edilemez olduğunu düşünmeleridir. İkincisi de bazı kimselerin, merkezi bir kurum tarafından zorunlu kılınan vergilerin büyük ölçüde merkezi olmaktan uzak kripto para dünyasının özünü uyumsuz olduğuna inanmalarıdır (Chandrasekera, 2020).

3- Kara Para Aklama

Kara para aklama suçunun varlığı kripto para birimlerinden çok daha eskiye dayanmaktadır. Suçluların, mali incelemelerden kaçınmak ve kanuni yaptırımlardan kaçmak için kullandıkları çok sayıda yöntem vardır. Günümüzde de bu yöntemlerin bazıları sıklıkla kullanılmaktadır. Örneğin, kripto para birimleri ile elde edilen kara para, suçlunun kendi banka hesabında aklanabilmektedir. Burada yöntem çok basittir.

Kişi, suçlulardan gelen Bitcoinleri kabul etmekte ve bu Bitcoinleri nakde çevirmek için kendi banka hesabını kullanmaktadır (NLTimes, 2018).

a) Şirinlemek (Smurfing Method)

Kara para aklamada yaygın olarak kullanılan bir diğer yöntem ise ismini Şirinler (The Smurfs) adlı çizgi filminden alan ve Smurfing olarak bilinen bir yöntemdir. Bu yöntem Türkçe'ye “şirinlemek” şeklinde çevrilebilmektedir. Şirinlemek yöntemi, farklı platformlarda küçük işlemler yapan çok sayıda kişinin, çok yüksek miktardaki tutarlarla tek bir işlem yapan kişiden daha az şüphe çekeceğine yönelik inanca dayanmaktadır. Şirinlemek, yeni bir yöntem olmamasına karşın kripto para birimlerinin yerel veya küresel ölçekte kolayca ve hızlı şekilde aktarılabilmesi nedeniyle günümüzde küresel bir sorun haline gelmiştir (Europol, 2018).

b) Çevrimiçi Kumarhaneler Aracılığıyla Kripto Paraların Aklanması

Kara para aklamada yaygın olarak tercih edilen bir diğer yöntem ise kumarhanede kumar oynamaktır. Teoride, suçlu kişi, yasadışı yollarla edindiği para ile kumarhanede fiş satın almakta ve burada birkaç tur çeşitli masalarda kumar oynamaktadır. Suçlu daha sonra fişleri kumarhanede bozdurarak kara para aklama işlemini tamamlamaktadır. Suçlu bu esnada para kaybederse bu kaybı genellikle bir iş yapmanın maliyeti olarak kabullenmektedir. Ancak suçlu kumarda kazandığı takdirde yine para aklama işlemi tamamlanır ve üzerine beklenmedik bir kâr elde eder. Kumarhaneler bu tür faaliyetleri tespit etmek ve önlemek için bir dizi tedbir almış olsalar da denizaşırı konumlardan servis sağlayan çevrimiçi kumarhanelerde bu tür etkinliklerin takip ve tespiti çok daha zor olmaktadır (Chainalysis, 2019, s. 26).

CiperTrace adlı kripto para güvenlik şirketi tarafından 2018 yılında hazırlanan kara para aklama ile mücadele raporuna göre, internet üzerinde kripto para ile kumar oynamaya izin veren çevrimiçi kumarhane sayısı 100 ilâ 200 arasında değişmektedir. Tıpkı normal bir kumarhanede olduğu gibi fonlar bahis aracılığıyla bir çevrimiçi kumarhaneye aktarılmakta ve mümkün olan en az sayıda bahis oynayarak veya mümkün olan en düşük tutarı harcayarak kalan para doğrudan doğruya geri çekilmektedir. Raporda bildirildiği üzere, çevrimiçi kumarhaneler aracılığıyla işlenen kara para aklama suçunun tespit ve takibindeki en büyük zorluk, bu kumar sitelerinin “Müşterini Tanı (KYC)” düzenlemelerine tabi olmamasından dolayı kolluk

kuvvetlerinin sisteme yatırılan ve sistemden çekilen para transferlerinin takibini yapmakta yaşadığı sorunlardır (CipherTrace, 2018, s. 8).

c) Karıştırma Hizmeti (Mixing & Tumbling)

Şekil 3.3:Karıştırma Hizmeti Çalışma Prensibi



Kaynak: (Möser, 2013, s. 2)

Kripto paralar üzerinden kara para aklama işlemleri ile ilgili daha önce verilen örneklere bakıldığında genel olarak geleneksel kara para aklama yöntemlerinin modernize edilmiş versiyonlarının işlendiği görülmektedir. Ancak kripto paraların aklanmasında yeni teknolojilerin de kullanılması mümkündür. Bu doğrultuda kullanılan en aldatıcı yöntemlerden biri “karıştırma hizmeti” adı verilen teknolojik bir süreçtir. Bu kavram, farklı bireylerin, bir grubun nihai yararı için fonlarını toplu olarak bir araya getirebildikleri bir yatırım fonuna benzemektedir (Sprenger & Balsiger, 2018, s. 1).

Ancak, bu kişilerden toplanan paralar bir yatırım ile değerlendirilmek yerine, borsalar arasında taşınmakta ve sonuçta belirli işlemlerin izlerinin takibi son derece zorlaştırılmaktadır (CipherTrace, 2018, s. 8).

d) Kripto Paraların İlk Arzı (ICO) Etkinlikleri

Kripto para kullanılarak gerçekleştirilen çok sayıdaki kara para aklama yöntemine ek olarak, en yaygın kullanılan kara para aklama yöntemi ICO etkinlikleridir. ICO etkinlikleri halka arz etkinlikleri ile karıştırılmamalıdır. Öyle ki ICO etkinliğinde yatırımcılar yeni kurulmuş bir şirkete fon sağlamak adına hisse alma işlemi gerçekleştirmemektedirler. Bunun yerine yatırımcılar ICO aracılığıyla, değer kazanacağı beklentisi ile şirket tarafından sunulan dijital ürünü satın almaktadır (Underhill, 2018).

Bazı ICO etkinlikleri doğaları gereği kesinlikle yasaldır ve kazançlı bir yatırım fırsatı sunabilmektedir. Örneğin, 2014 yılında Ethereum gerçekleştirdiği ICO etkinliği

ile 18 milyon doları fon toplamıştır. Bugün ise Ethereum piyasa değerine bağlı olarak, en büyük ikinci kripto para birimidir (Frankenfield, 2020).

Yeni başlayanlar için, tıpkı kripto para birimleri satın almak veya takas etmek gibi, bir ICO'ya yatırım yapmak da anonim bir işlem olabilmektedir. Çünkü hem ihraç eden hem de alıcı gerçek kimliklerini takma isimler ardına gizleyebilmektedir. Dahası, işlem kaydının halka açık bir deftere kaydedilmesine rağmen, suçluların işlem yapabileceği yüzlerce Blockchain zinciri vardır. Ayrıca belirtmek gerekir ki, günümüzde yetkililerle iş birliğine yanaşmayan kripto para borsalarının sayısında büyük bir artış söz konusudur (Cointelegraph.com, 2018).

Kara para aklama ile ilgili ikinci bir endişe de bir ICO etkinliğinde toplanabilecek muhtemel para miktarıdır. Öyle ki sadece 2017 yılında gerçekleştirilen ICO etkinliklerinde 5 milyar dolardan fazla para toplanmıştır. Üstelik 2018 yılının henüz ilk çeyreğinde toplanan para miktarı 6 milyar doları aşmıştır. Bir ICO danışmanlık firması olan Satis Group tarafından yayınlanan araştırmaya göre, yatırımların bir kısmı finansal açıdan güvenli ve yararlı olsa da 2017 yılında gerçekleştirilen ICO'ların %78'inin dolandırıcılık amaçlı olduğu ortaya çıkmıştır. Sonuç olarak, ICO etkinliklerinin kara para aklamaya yönelik bir araç olarak kullanılması hayli mümkündür (Morse, 2018).

CNBC'de yayınlanan bir makalede yer verilen varsayımsal bir senaryoya göre, süreç endişe verici derecede basittir. Senaryoda, daha önce bir ICO etkinliğinde yatırım yapma kararı alan bir yatırımcı sonunda kripto paralarını satmaya karar vermektedir. Satıcının iki seçeneği vardır: İlki, kripto paralarını büyük bir borsada satmak ve yatırımından daha küçük bir getiri elde etmektir. İkincisi ise, daha yüksek gelir amacı ile potansiyel olarak daha iyi kazanç şansının sunulduğu “pek de tekin olmayan” bir borsada işlem yapmaktır. Büyük borsada işlem yapmak kazançlı bir seçim olmayabilir, ancak hem alıcı hem de satıcı hakkındaki gerekli tüm bilgileri kayıt altına alan bir KYC sistemi kullanmaktadır. Bununla birlikte, bu güvenliği inşa etmek ve sürdürmenin de bir mali külfeti vardır. Bu durum da mümkün olan en yüksek kârı elde etmek isteyen satıcı için pek ilgi çekici olmamaktadır. Sonuçta, kişi, müşterilerin bilgilerini kanun yararına saklamayı taahhüt eden platformun aksine en iyi kazanç oranını sunan tekin olmayan platform üzerinde hesap açma yoluna gitmektedir. Bu esnada bir alıcı, yasadışı yollarla

kazanılan parayı aklama isteği ile, ilgili işlem bilgilerinin kaydedilmediği bir borsaya bir miktar prim ödemesi yapmaya da razı olmaktadır. (Dahası, alıcı, iş yapmanın bilinen bir maliyeti olarak kripto paralar ile fazladan ödeme yapmaya isteklidir). Sonunda, kişi, bir ICO etkinliğinden satın aldığı ve daha sonra başka bir kripto para ile değiştirilebilen veya tekrar nakde dönüştürülebilen kripto paralar şeklinde aklanmış paralara sahip olmaktadır. Burada satıcı dürüst ve yasalara saygılı bir vatandaş olsa bile, alıcının kimliği veya kripto paraları satın almak için kullanılan fonların kaynağı hakkında endişelenmesi pek de olası değildir. Aslında, herhangi bir endişenin söz konusu olması halinde, satıcı muhtemelen borsanın durum tespiti yapmaktan ve kendi müşterilerini doğru şekilde tanımlamaktan sorumlu olacağını varsayma yoluna gidecektir. Tersine, alıcı ICO etkinliğinin, yeni ve gereğinden daha az düzenlenmiş bir yatırım ortamı olduğunu gerçeğini bilmekte ve bir yükten kurtulmaktadır. Ayrıca kara para aklamak için hem potansiyel olarak vicdansız bir takas işleminden hem de hiç şüphe duymayan bir satıcıdan yararlanmaktadır (Choudhury, 2018).

3.6.Kripto Para Sahtekarlığı ile Mücadelede Adli Muhasebe

Adli Muhasebe, kullanıcıları kripto para dolandırıcılığından ve bilgisayar suçlarından korumada etkin bir rol üstlenmektedir. Bitcoin, takibi ve izlemesi hayli zor olan dijital finans ve kripto para çağını başlatmıştır. The Silk Road'un (çevrimiçi bir kara borsa) doruk noktasında olduğu günlerde, Bitcoin ile neredeyse her şeyin alınması ve satılması mümkün idi. Bu ortamda, silah ve uyuşturucu başta olmak üzere her türlü yasa dışı madde düzenli olarak en yüksek teklifi veren kişilere satılmıştır (Greenberg, 2016).

Bitcoin, pratikte, anonim olarak tanıtıldı ve muteber finansal işlemlerin çoğunu meraklı gözlerden koruma yeteneği ile ön plana çıkmıştır. Ancak, The Silk Road adlı platformun kripto paranın kullanıldığı bir pazar haline gelmesi polisin dikkatini çekmiştir. (InspireMalibu.com, 2016) Ancak, kripto para kullanımının sağladığı gizlilik kanun uygulayıcı kurumları büyük bir çıkmaza sokmuştur. Kripto para biriminin suça ilişkin tarafı anlaşılana kadar alıcı ve satıcının kripto parayı nasıl ve neden kullandığı ile alışverişin taraflarına erişmek hiç de kolay olmamıştır (Doran, 2015, s. 12).

Kripto paralar her ne kadar iyi birer sır saklayıcı olsalar da, adli muhasebeciler ve dijital araştırmacılar için ardında çok sayıda iz bırakmaktadır. Birçok kullanıcı,

Bitcoin'i sađladıđı gizlilik iin tercih etmekte ve savunuculuđunu yapmaktadır. Ancak, Bitcoin'in tam olarak izlenemez olduđunu sylemek mmkn deđildir. Her ne kadar kullanıcıların gizliliđini korumak iin tasarlanmış olsa da ardında arařtırmacıların takip edebileceđi bir veri izi bırakmaktadır (businessdegrees.uab.edu, 2019).

Arařtırmacılar, Bitcoin Blockchain'inde halka aık olarak kaydedilen belirli iřlemleri karaborsadaki satıřlara bađlayarak, satıcılara ulařabilmektedir. Darknet (karanlık ađ) zerinde alıcılar ve satıcılar Bitcoin karřılıđında mal ve hizmet alıřveriřinde bulunmaktadırlar. Arařtırmacılar; kimin, kime, ne iin ve ne kadar deme yaptığını ortaya ıkarmak, iřlemleri dođrulamak ve aramayı daraltmak iin Blockchain zerinde arařtırma yapmaktadırlar (Greenberg, 2013).

Burada nihai hedef satıcıların IP adreslerine ulařmaktır. Bylelikle satıcının kendisine ulařmak iin gerekli olan her ařama kaydedilmektedir. Blockchain'in halka aık defteri, bulmacanın en nemli parasıdır. Herhangi bir Bitcoin sahibinin gerek kimliđi bilinmez ancak bunun yerine iřlemler adeta evrimii bir imza gibi davranan bir kodla iliřkilendirilmektedir (Engle, 2016, s. 344).

Bitcoin ve diđer kripto para birimleri geleneksel olarak zel, anonim ve izlenemeyen dijital para birimleri olarak tasarlanmıştıř. Getiđimiz birkaç yıl iinde, daha fazla insan Bitcoin gibi kripto para birimlerinin aslında hi zel olmadığını ve kesinlikle izlenebilir olduđunu fark etmiř, bu durum da kripto para birimine ynelik uzmanlařmıř adli muhasebe firmalarının ykseliřine yol amıřtır. Bitcoin gibi kripto para birimlerinin byk ođunluđu anonim olmaktan ziyade, daha nce bahsedilen nedenlerden tr yalnızca birer "takma ad" sađlamaktadır. Yapılan iřlemlere esas olan czdan adresleri, iřlem yapan kiřilerin kimliđini herkese aık řekilde listelemese bile kimliđin genel adreslerle iliřkilendirilmesi mmkndr (Sibenik, 2019).

Bir bitcoin iřlemi, "toplam girdi" olarak bilinen bir dizi girdiyi ve "toplam ıktı" olarak bilinen bir dizi ıktıyı iermektedir. Toplam ıktıya dahil olmayan iřlem creti nedeniyle toplam ıktı her zaman toplam girdiden biraz daha dřktr. Bir iřlem teorik olarak sınırsız sayıda girdiye sahip olabilir, ancak iřlemlerin ođu yalnızca tek bir girdiye sahiptir. Bir iřlem gerekleřtiđinde, her zaman birden ok ıktı oluřmaktadır. Tipik olarak iki tane vardır, ancak tıpkı girdilerde olduđu gibi varsayımsal olarak herhangi bir iřlemden sonsuz miktarda ıktı adresi vardır. Bitcoin protokolnn dođası

gereği her zaman birden fazla çıktı vardır. Tipik olarak, bir kişinin cüzdanında bir miktar BTC olduğunda, kişi bunların hepsini aynı anda harcamamaktadır. Muhtemelen sadece harcanması amaçlanan nakit çıkarılmakta ve geri kalanı cüzdanda kalmaktadır. Ancak bu, Bitcoin için uygun olmayan bir benzetmedir (Sibenik, 2019).

Bir Bitcoin işleminde, cüzdanda bulunan bütün tutar cüzdandan çıkarılmaktadır. Harcanan tutar bir çıktı adresine gönderilirken, kalan tutar bir “değişim adresine” gönderilmektedir. Değişim adresi varsayımsal olarak fonların gönderildiği adresle aynı olabilmektedir.

Örnek bir Bitcoin işlemi şu şekildedir:

Bu işlemde, 10sbKtBzZjz68PO2fBSp3bveef55948j1k adresine ait 2.86682 BTC olduğu için toplam 2.86682 BTC girdi vardır.

Kişi daha sonra 0.44062860 BTC'yi 66ST5NJpTVyxWFQu2QFooEGUyecdRjFHFV adresine göndermektedir.

İşlem ücreti kesildikten sonra kalan 2.20600082 BTC, daha önce hiç kullanılmamış değişim adresi olan 21dChRuFEm2Evv3muYiX8zucSHBRL74m9F adresine gönderilmektedir.

Burada değişim hesabının daha önce kullanılmamış olması, paranın güvenliğinin sağlanmasıdır. Cüzdan yazılımları değişim adreslerinin daha önce hiç kullanılmamış adresler olmasını sağlamaktadır.

Bir işlem gerçekleştiğinde, bazıları, adresle ilişkili özel anahtar yayınlandığı için, şifrelenmiş bir biçimde de olsa, işlem sırasında ifşa ettiği için adresin bir daha güvenli olmadığını iddia edilebilmektedir.

Bu işlemlerde ayırt edici olan husus; 66ST5NJpTVyxWFQu2QFooEGUyecdRjFHFV ve 10sbKtBzZjz68PO2fBSp3bveef55948j1k adreslerinin aynı kişi veya kuruluşa ait olmasıdır.

21dChRuFEm2Evv3muYiX8zucSHBRL74m9F adresinin kime ait olduğu ise bilinmemektedir (Agrawal, 2020). Aynı kişiye ait olabileceği gibi, bir ödeme veya hizmet için veya bir borsaya gönderilen fonlar da olabilir. Kesin olarak bir şey söylemek mümkün değildir. Ancak bazı cüzdan adreslerinin belirli kişilere, varlıklara, gruplara ve bazı durumlarda organize suç örgütlerine ait olduğu bilinmektedir. Eğer cüzdan adresi

bilinmiyorsa, ilerideki diğer işlemler için bu adresi izlemek yine de mümkündür. Bu durumda, bilinen diğer adreslerle ne kadar yakından ilişkili olduğuna bakılmaktadır (Sibenik, 2019).

Bunlar Bitcoin'e yönelik adli muhasebenin ardındaki temellerdir. Ayrıca bunun, adli takibin nasıl çalıştığını gösteren basitleştirilmiş bir model olduğunu söylemek mümkündür. Çoğu durumda, farklı adresler arasındaki bağlantıları belirlemek için yüzlerce, hatta binlerce işlemin analiz edilmesi ve birbirine bağlanması gerekmektedir. Ayrıca, Ethereum gibi diğer bazı kripto para birimlerinin, Bitcoin ile aynı şekilde UTXO (gerçekleşmemiş işlem çıktısı) oluşturmadıkları için farklı şekilde çalıştığı da unutulmamalıdır (bitcoin.org, 2019).

3.7.Soruşturmalar (Araştırmalar)

Soruşturmalar, adli muhasebenin baş-tekniklerinden birisidir, bu kapsamda kripto para dolandırıcılığın tespit etmek için en sık kullanılan yöntemlerini ele alınacaktır.

3.7.1.Ağ Analizi

Ağ analizi, uçtan uca ya da başka bir ifade ile eşler arası (Peer-to-peer) Bitcoin ağının incelenmesi ve analiz edilmesidir. Bugüne kadar gerçekleştirilen çalışmaların ve araştırmaların büyük çoğunluğu, Bitcoin kullanıcı gizliliğinin test edilmesine ya da iyileştirilmesine odaklanmaktadır. Bu doğrultuda, ağ analizinde veri toplamak üzere, CoinSeer adlı özel bir Bitcoin istemcisi geliştirilmiştir (Koshy, 2013, s. 11).

Bir kullanıcı Bitcoin istemcisini ilk kez açtığında, sabit kodlu bir liste kullanarak eşleriyle bağlantı kurmaya çalışırken aynı zamanda kendi IP adresini ve bağlantı noktasını içeren bir adres mesajı göndererek varlığını duyurmaktadır ve böylelikle diğer düğümlere bağlantı sağlamak üzere izin vermektedir. İstemci ayrıca bağlı bir kullanıcıya, bağlı kullanıcının bilinen eşlerini talep etmek için bir “getaddr” mesajı gönderebilmektedir. Buna bağlı kullanıcı 1.000 adede kadar adres mesajıyla yanıt verebilmekte ve istemcinin ek bağlantılar başlatmasına olanak tanıyabilmektedir (Quadrando vd., 2019, s. 149).

Ağ, işlemin uygunluğunu komşularına bildirerek düğümlerin defter kopyalarını güncellemek ve senkronize etmek için belirli protokolleri takip etmekte ve

uygulamaktadır. Buradaki ilk düğüme “kaynak” adı verilmektedir. Yayındaki her atlama, iletim süresi ve doğrulama süresinden oluşan bir "yayılma gecikmesine" neden olmaktadır. Herhangi bir bloğun ağdaki herkese ulaşmasının yaklaşık iki hafta sürdüğü tespit edilmiştir (Koshy, 2013, s. 11).

3.7.2. İşlem Analizi

İşlem analizi, temel olarak, Blockchain’in incelenmesine dayanan bir çalışmadır. Bitcoin’e yönelik kaleme alınan eski bir makalede, 50 bin BTC’den büyük hacimdeki işlemlere vurgu yapılarak, bu işlemlerin neredeyse tamamının 2010 yılının Kasım ayında gerçekleştirilen 90 bin BTC hacmindeki tek bir işlemin alt kümeleri olduğu bildirilmiştir (Ron ve Shamir, 2019, s. 18).

Bitcoin ağında anonimlik ve mahremiyet üzerine yayınlanan bir başka eski tarihli makalede, gerçek ve potansiyel anonimlik arasındaki boşluğa dikkat çekilmekte ve işlemsel analiz kullanılarak, Bitcoin değişim adreslerine dayalı olarak kümelenmelerini yenmek için önemli bir çaba gerekeceği sonucuna varılmıştır (Meiklejohn vd., 2013, s. 4). Meiklejohn (2013) tarafından gerçekleştirilen bir çalışmada, sınıflandırma ve etiketlemeyi birleştiren, web kazıma yöntemi ile kullanıcıları tanımlamaya çalışan ve birçok gerçek dünya vakasında başarıyla test edilen BitIodine adlı otomatik ve ölçeklenebilir bir modüler çerçeve geliştirilmiştir (Spagnuolo, Maggi, & Zanero, 2014, s. 7).

Kısa süre önce yayınlanan bir makalede, internet alışverişlerinde kripto para kullanımına ilişkin gizlilik riskleri incelenmiştir. Söz konusu makalede, üçüncü taraf web izleyicilerinin, blok zincirindeki işlemi benzersiz bir şekilde tanımlamak ve bunu kullanıcının tanımlama bilgilerine (çerez/cookie) ve gerçek kimliğine bağlamak için genellikle yeterli bilgiye sahip olduğunu göstermiştir. Ayrıca, aynı kullanıcıdan iki satın alma tespit edildiği takdirde, CoinJoin protokolü veya benzeri kullanılmasına rağmen, bu kullanıcının Blockchain üzerindeki tüm işlem ve adres kümeleri belirlenebilmektedir (Goldfeder vd., 2018, s. 3).

3.7.3. Cüzdan Analizi

Bitcoin cüzdanı, özel anahtarların saklandığı yerdir ve kullanıcının Bitcoin işlemlerini güvenli bir şekilde gerçekleştirmesine imkân sağlamaktadır. Cüzdanlar, Bitcoin gönderme ve alma mekanizmasını otomatikleştirmekte ve ağa aktif olarak

katıldıklarında "istemci" olarak adlandırılmaktadır. Hafif cüzdanlar, tam düğüm cüzdanlarının aksine, Blockchain zincirinin kapsamlı bir kopyasını tutmayarak, disk alanından ve bant genişliğinden tasarruf sağlamaktadırlar. Bunun yerine, 2011 yılının ikinci yarısından itibaren, hafif cüzdan kullanımını mümkün kılmak için basitleştirilmiş ödeme doğrulaması (SPV) uygulamaya konmuştur. SPV istemcilerine ilişkin potansiyel gizlilik kaybına ilişkin sıklıkla endişeler dile getirilmektedir (Goldfeder vd., 2016, ss. 94,284).

Çevrimiçi (sıcak) veya çevrimdışı (soğuk) olarak tanımlanan çeşitli ve farklı cüzdan türlerinden bahsetmek mümkündür. Çevrimdışı cüzdanların çok daha güvenli olduğunu apaçık ortadadır. Çevrimdışı cüzdanlar daha ziyade uzun vadeli varlıklar için tercih edilirken, çevrimiçi cüzdanlar genellikle düzenli/günlük kullanım için tercih edilmektedir. Cüzdanlar; masaüstü, mobil, web, fiziksel, donanımsal ya da Bitcoin istemcileri şeklinde olabilmektedir. Web tabanlı cüzdanlar, tüm Blockchain'in indirilmesi ihtiyacını ortadan kaldırmakta, ancak özel anahtarın nerede saklandığına bağlı olarak güvenlik düzeyi farklılık gösterebilmektedir (Cohen, 2015).

Orijinal Bitcoin istemcisinin tam cüzdan analizinde, şifre çözme işleminin gerçekleştirilmesi için cüzdanın (isteğe bağlı) parolasına ihtiyaç duyulmamaktadır. Parola kullanmak yalnızca özel anahtarı şifrelemektedir, bu nedenle parolalar yalnızca işlemleri başlatmak için gerekmektedir.

Dijital kanıt içeren başarılı bir vaka, vakanın içeriğinin yanı sıra vakadan sorumlu araştırmacının bilgisi, deneyimi, uzmanlığı, titizliği ve merakına da bağlıdır. Dijital bir vakanın başarısı, çok yönlü bir araştırmacının yanı sıra, araştırmacının ilerleyebileceği aşamaları sağlayan temel bir modele de dayanmaktadır. Dijital Adli Bilimler için Araştırma Süreci modeli, başarılı bir dijital araştırmanın temelidir.

DFRWS 2001 tarafından piyasaya sürülen bu model, altı temel aşama içermektedir: (Harrell, 2010)

- 1- Tanımlama
- 2- Hazırlık
- 3- Toplama
- 4- İnceleme

5- Analiz

6- Sunum

Bitcoin'in adli çıktıları dikkate alarak bir vaka inşa etmek, Nakamoto'nun işlemleri anonim tutmak için geliştirdiği teknoloji nedeniyle ortalama bir vakadan çok daha zordur. Bu anonimlik nedeniyle, belirli kanıtların elde edilmesi ve yorumlanması da zor bir hal almaktadır. Bununla birlikte, Dijital Adli Bilimler için Araştırma Sürecinin aşamalarının takip edilmesi ile başarılı bir Bitcoin araştırması yapmak mümkün olmaktadır. Tanımlama ve koruma, modelin ayrılmaz aşamaları olsa da, buradaki odak noktası, bir Bitcoin vakasının adli çıktıları ile ilgili olan Toplama, İnceleme ve Analiz aşamalarıdır. Toplama aşamasında, araştırmacının potansiyel olarak dijital kanıt içerebilecek herhangi bir nesneyi veya veriyi araştırması, belgelemesi ve toplaması gerekmektedir. Bitcoin işlemleri bir ağ bağlantısı üzerinden gerçekleştiğinden, bir araştırmacı internete bağlanabilen herhangi bir fiziksel nesneyi ele geçirmelidir. Bu nesneler arasında cep telefonları, PDA'lar, dizüstü bilgisayarlar, tabletler ve masaüstü bilgisayarlar bulunmaktadır. Tanımlama ve Koruma aşamaları sırasında şüphelinin bilgisayarının açık olduğu belirlenirse, araştırmacının sistemin fiziksel belleğini yakalaması zorunludur (Doran, 2015, s. 11). Bitcoin ile ilgili geçici bellekte pek çok kanıt türü bulunabilmektedir. Bu tür kanıtlar şunları içermektedir (Massad, 2019, ss. 28-29):

- Çalışan Bitcoin işlemleri ve hizmetleri
- Sistem bilgisi
- Giriş yapan kullanıcıların bilgileri
- Kayıt bilgileri
- Sosyal ağlarda ve Bitcoin forumlarında gerçekleştirilen sohbet ve iletişim kalıntıları
- Son Bitcoin web tarama etkinlikleri
- Bitcoin içeren e-posta sistemleri aracılığıyla gerçekleştirilen son iletişim bilgileri
- Bulut hizmetlerinden elde edilen bilgiler

- Yakalama sırasında eklenen şifreli birimler için şifre çözme anahtarları
- Kötü amaçlı Bitcoin yazılımları ya da Truva atları.

Soruşturmacı, kanıtları fiziksel olarak veya çıkarma ve görüntüleme gibi yöntemlerle topladıktan sonra, verileri inceleyebilmekte ve her bir parçanın önem düzeyini belirleme sürecine başlayabilmektedir. Bitcoin uzantıları ve ilişkili verilerin şüphelinin sabit diskinde bulunmasına ve AccesData'nın Adli Araç Seti veya EnCase gibi sağlam adli araçlar kullanılarak kurtarılabilmesine karşın, Internet Evidence Finder (İnternet Kanıt Bulucu/IEF), araştırmacının yalnızca Bitcoin uzantılarını görmesine olanak tanımaktadır (Piggott, 2014, s. 15).

Bir soruşturmacının IEF kullanarak Bitcoin kanıtlarını kurtarmasını sağlayan iki seçenek mevcuttur. İlk seçenek, soruşturmacının, şüphelinin sürücüsünde yer alan Bitcoin dosya klasörünü tamamen dışarı aktarması ve IEF ile bu klasörü analiz etmesidir. İkinci seçenek ise soruşturmacının IEF ile yalnızca Bitcoin uzantılarını değil sürücünün tamamını içerecek şekilde internet geçmişini, sohbet geçmişini, e-postaları ve internet aramalarını da geri getirerek analiz etmesidir. Her iki seçenekte de, kurtarılan Bitcoin verileri, soruşturmacının bir vaka oluşturmaya sağlam bir temel teşkil etmektedir. Kullanıcının Bitcoin ile ilgili etkinliklerinin çoğunluğu kullanıcının kendi Bitcoin cüzdanında yer aldığından, adli bulguların çoğu bir tek dosyada yer alabilecektir. IEF, dosyayı kurtararak, Bitcoin cüzdanındaki adreslerin yanı sıra Bitcoin istemci yazılımı tarafından oluşturulan günlük dosyalarından Bitcoin ağına kullanıcı dostu bir formatta yapılan sorguları sunabilmektedir (Piggott, 2014, s. 27).

Soruşturmacı, halihazırda gerçekleştirilmemiş tüm işlemleri görüntülemek için bir zincir durumu alt dizinini inceleyebilme seçeneğine sahiptir. Daha sonra kaydedilen dosyadan kurtarılan adresler ile ilgili olan diğer adresler ve işlemlerin tamamı, Blockchain üzerindeki verilerle karşılaştırılabilmektedir. Soruşturmacı, gerçekleştirilmiş işlemlerle ilgili kurtarılmış adresleri, sorguları ve bilgileri alarak, vakayı yavaş yavaş bir bütün haline getirebilmektedir. Böylelikle, diğer potansiyel şüphelilere ve mağdurlara ulaşabilmenin yanında diğer muhtemel soruşturmalara da kapılar açılabilmektedir (Forensic Focus, 2013).

Açgözlü yatırımcılar, kripto para dolandırıcılarının sunduğu sözde gelecek vaat eden büyük getirilerle karşılaştıklarında büyük bir etki altına girmekte ve bu teklifleri

cazip olarak değerlendirmektedir. Dolandırıcılar, yatırım stratejilerine dair bilgi vermeden, kayda değer bir yatırım getirisi elde etmek için ağlarına düşürdükleri yatırımcıları 95 – 118 gün aralığında bekletmeyi başarmaktadırlar. Bu süre zarfında hiçbir şeyden şüphelenmeyen hırslı yatırımcılar, teşvik edici ve heyecan uyandırıcı mesajlarla tuzağa çekilmektedirler (Saada, 2019).

Elektronik para transfer sistemleri olan kripto para birimleri, geleneksel risk sermayedarlarına ve melek yatırımcılara karşı rekabetçi bir giriş sunmaktadır. Muhasebe muhakemeleri, gerçekte herhangi bir yasal korumaya sahip olmayan yatırımcılar için önemli bir koruma unsuru sağlamaktadır. Kripto para biriminin arkasındaki organizasyon mutlaka bir şekilde finanse edilmektedir. Şayet yatırımcılar ve organizasyon iyi değilse, pompalama ve boşaltma planları işletilmektedir. Adli muhasebe, kullanıcıları kripto para dolandırıcılığından kurtarmanın yegâne anahtarıdır (Kirby, 2017).

Yatırımcılar, kripto para dünyasındaki kötü eylemler ve dolandırıcılık etkinlikleri hakkında mutlaka eğitilmelidir. Paranın gelişimi ile birlikte, muhasebe ihtiyacı da artış göstermektedir. Kripto para biriminin geleceğin para birimine doğru evrilmesi ile birlikte, faiz oranlarının hesaplanıp hesaplanamayacağının, artan faizin değerlendirilip değerlendirilemeyeceğinin, fiyat trendlerindeki, vergilerdeki veya ismi henüz konulmamış muhtemel hususların daima muhasebeleştirilmesi gerekecektir (Fuscaldo, 2018).

Kripto para birimi günlük ödeme aracı haline geldiğinde, muhasebe ihtiyacı da katlanarak artacaktır. Kripto para birimi işlemlerini düzenleme, organize etme, izleme ve yönetme ihtiyacı, yeni fırsatları ve zorlukları beraberinde getirmektedir. Kripto para muhasebesi, kripto para birimi ana akım ödeme sistemi haline geldiğinde, kripto para işlemlerinin meşruiyetini sürdürmenin anahtarıdır (Jacque, 2018).

3.8.Kripto Para Cüzdanları İle Kimliklerin İlişkilendirilmesi

Bir dizi cüzdan adresinin aynı kişi tarafından kontrol edildiğini bilmek, işin sadece yarısıdır. Çoğu durumda bu hesapları kontrol eden kişinin kim olduğunu bulmak gerekmektedir. Cüzdan hesaplarının ardındaki kişilerin kimliğini tanımlamak için kullanılan en yaygın yöntem, kişilerin kullandığı ya da kullanması muhtemel olan kripto para birimi borsaları ile birlikte çalışmaktır (Hrones, 2018). Bireylerin tipik olarak KYC

(müşterini tanı) tanımlamasından geçmeleri gerekli olduğundan dolayı, borsalar genellikle resmi bir talep söz konusu olduğunda, kişilerin para transferi, para yatırma ya da para çekme gibi işlemleri hakkında resmi otoritelere bilgi sağlamaktadırlar (Robinson, 2018).

Tanımlama hususunda en çok dikkat edilmesi gereken husus, para yatırma ve para çekme geçmişidir. Çoğu zaman kişiler para yatırma ve para çekme işlemlerinde borsa dışındaki kişisel cüzdanları üzerinden işlem yapmaktadır ve böylece cüzdanların kime ait olduğunu belirlemek daha mümkün hale gelmektedir. Herkese açık adresler ile bireylerin kimliğini ilişkilendirmek için çeşitli başka tekniklerin de söz konusu olmasına karşın kripto para değişimi en tipik yöntem olarak karşımıza çıkmaktadır. Ayrıca, adli muhasebeciler çok daha gelişmiş farklı yöntemleri de kullanma kabiliyetine sahiptir (Roberts, 2018).

Günümüzde, kripto para birimleri üzerine çalışan adli muhasebeciler, daha temel nitelikli izleme girişimleri başarısız olduğunda, halka açık adresler ile bireylerin kimliklerini ilişkilendirmede iki ana saldırı vektörü kullanmaktadır.

3.8.1. Dusting (Tozlanma) Saldırısı

Dusting saldırısı, anonimleştirmeyi ortadan kaldırmayı ve cüzdanları birbirine bağlamayı amaçlamanın yanı sıra hali hazırda sıklıkla kullanılan saldırı vektörleri arasında en yeni ve en etkili olanlarından biridir. Bu yöntem, bir saldırganın ya da bir adli muhasebecinin, aynı kişiye ait olduğundan şüphelendikleri cüzdanlara “dust” (toz parçacığı) adı verilen çok küçük miktarda, örneğin 0,01 Dolardan daha azına karşılık gelen miktarda Bitcoin göndermesi şeklinde çalışmaktadır. Çoğu Bitcoin işleminde, tipik olarak önceki bir UTXO'dan yalnızca bir giriş vardır, ancak birden çok giriş kolayca birleştirilebilmekte ve bu genellikle cüzdan yazılımı aracılığıyla otomatik olarak yapılmaktadır (Musiala vd., 2020, s. 4).

Örneğin, birine 0,45051 BTC ödemek istiyorsak ve bir cüzdanda 0,00001 BTC'ye sahipsek, cüzdan yazılımımız 0,00001 BTC'yi, toplam 0,45051 BTC'lik bir giriş oluşturmak için birlikte 0,4505 BTC'ye eşit olan diğer girişlerle otomatik olarak birleştirebilmektedir. Bununla birlikte, işlem tamamlandığında, yalnızca 0,00001 BTC tutan cüzdan sahibinin aynı zamanda 0,4505 BTC'yi tutan / ödeyen cüzdan ya da cüzdanların da sahibi olduğu halka açık bir bilgi olarak kaydedilmektedir. Saldırganın

ya da adli muhasebecinin, cüzdanlardan birinin kime ait olduğunu bilmesi ile birlikte, artık diğer tüm cüzdanların kime ait olduğunu da bilmek ve bu yeni cüzdanlarla ilişkili işlem geçmişini de izlemek mümkün hale gelmektedir (Cryptopedia, 2018).

Dusting saldırıları, anonimleştirmenin ortadan kaldırılması dışında başka bir tehdit oluşturmamakta ve yalnızca sahibi saldırıya uğrayan cüzdan adresinden para çıkışı olduğunda gerçekten işe yaramaktadır. Kişinin söz konusu cüzdandan bir daha hiç para çıkışı gerçekleştirmemesi halinde, anonimleştirilmeye dair herhangi bir risk durumu da söz konusu olmayacaktır (Jake, 2018).

3.8.2. Paket Korsanlığı (Packet Sniffing) Ve Gizli Dinleme (Eavesdropping) Saldırısı

Bu saldırı yöntemi, bir bilgisayardan ya da bir sunucudan gerçekleştirilen veri iletimi esnasında, iletilen verilerin yakalanmasını, ağ trafiğinin etkin bir şekilde izlenmesini ve takip edilmesini içermektedir. Halka açık ağlar gibi güvenli olmayan ağlar bu tür saldırılara sıklıkla hedef olmaktadır. Bu tür bir saldırı anonimliği ortadan kaldıracak gibi şifreler ve özel anahtarlar gibi diğer verileri de çalmak için kullanılan bir yöntemdir. Bu nedenle, kripto para varlıklarının da çalınmasında/ele geçirilmesinde etkili bir saldırı yöntemidir (Lagarde, 2019, s. 53).

Adli muhasebeciler, dolandırıcılık eylemlerini ve diğer mali suçları araştırmak için finans, muhasebe ve bilgi işlem sistemlerine dair var olan uzmanlık bilgilerini kullanmaktadır. Adli muhasebecilerin çalışmaları, müşterilerine finansal suç riskleri ve kontrolleri sağlamayı, tespit ve soruşturma hizmetleri sunmayı, davalarda teknik destek sağlamayı ve varlıkların korunmasını içermektedir. Bu çalışmalardaki iki temel yön ise kara para aklama ve varlık takibi olarak karşımıza çıkmaktadır. Kara para aklama, suç gelirlerinin nakit gibi asıl hallerinden, yeni varlıklara ve yeni yerlere, kökenlerini gizlemek ve meşru göstermek amacıyla dönüştürülmesidir (Jacque, 2018).

Varlıklar, tipik olarak, banka hesapları, şirketler, tröstler ve özel amaçlı araçlar gibi karmaşık bir varlık zinciri dahilinde taşınmış olabilmektedir. Genellikle bunlar birden çok yargı alanını kapsamaktadır. Tüm bunlar, izi takip etmenin mümkün olduğunca daha zor bir hale getirilmesi için yapılmaktadır. Varlık izleme, bir varlığın başlangıç noktasından nihai varış noktasına kadar olan izini dikkatli bir şekilde ortaya

ıkarma, yol boyunca her adımı adli aıdan saėlam bir ekilde ve mahkeme nne sunulabilecek ekilde belgeleme srecidir (Sibenik, 2019).

Bitcoin gibi kripto para birimleri, saėlayabildikleri kısmi anonimlik ve merkezi denetim eksikliėi sayesinde kara para aklayan sululara yeni fırsatlar sunmaktadır. Bu zelliklerin her ikisi de, hem gerek mřteriler hem de drst olmayan mřteriler iin oldukça cazip grnmektedir. The Silk Road'un kurucusu Ross Ulbricht'in DarkWeb'deki ilk zel karaborsayı kurması ve 2016 yılındaki ABD Bařkanlık seimlerinde Rus istihbarat grevlilerinin seimlere mdahale etmesi ynndeki sulamalar bu ynde verilebilecek iki kt rnektir (Rosenberg ve Popper, 2018) (Sergison, 2019).

Kripto para birimleri esasen řu drt teknolojinin bileřimidir: (Bonhill Group Plc., 2018) (Serapiglia vd., 2015, s. 46)

1. Daėıtık Defterler: Her katılımcı, Bitcoin ve diėer birok kripto para birimi sistemi iin bir Blockchain eklinde yapılandırılmış olan tm defterin (iřlem kaydı) bir kopyasına sahip olabilmektedir.
2. Merkezi Olmayan Kontrol: Katılımcılar, merkezi bir otorite veya banka gibi bir kontrol birimi aracılıėıyla deėil, birbirleriyle doėrudan doėruya iřlem yapabilmektedir.
3. Kriptografinin Kullanımı: İřlemleri, bakiyeleri ve katılımcıları korumak ve doėrulamak iin kriptografi kullanılmaktadır.
4. Otomasyon: Akıllı szleřmelerde olduėu gibi veya belirli bir olay gerekleřtiėinde bir tahvil faiz demesini tetikleyerek iřlemleri programlı olarak otomatikleřtirme yeteneėidir.

Daha nce de belirtildiėi gibi, kripto para birimleri yalnızca bir dereceye kadar anonimlik sunmakta ve finansal varlıkların hkmet gzetimi ya da dzenlemesi olmadan yetki alanları arasında tařınmasını saėlamaktadır. Bir kiři, kimliėi hakkında hibir bilgi paylařmadan ve herhangi bir aıklamada bulunmadan, sistemde yalnızca basit bir adres olarak grnen bir kripto para czdan hesabı aabilmektedir (Sibenik, 2019). alınan kiřisel veriler, fidye yazılım demeleri, uyulurucu ticareti ve diėer karaborsa alıřveriřleri gibi durumlarda gerekleřtirilen demelerde kripto para en sık

tercih edilen takas aracıdır. Ayrıca ABD Doları gibi resmi para birimlerinin kullanılmasını yasaklayan devlet yaptırımlarından kaçınmak için giderek daha fazla kullanılmaktadır. İran, Rusya, Myanmar ve Kuzey Kore de dahil olmak üzere bazı yaptırımlara tabi ülkeler, kendi kripto para birimlerini geliştirdiklerini bildirmektedirler (Brett, 2020).

Bununla birlikte, kripto para birimleri, suçluların birbiri arasında gerçekleştirdikleri işlemler için güvenli bir alan sağlamaktadır. Ayrıca belirtmek gerekir ki, kripto para birimleri ile satın alınabilecek yasal varlıklar hala oldukça sınırlıdır. Sonuç olarak, haksız kazançlarını faydalı ürünlere harcamak isteyen suçlular en sonunda kripto para birimleri şeklinde tuttukları paralarını gerçek ekonomik araçlarla değiştirmek zorunda kalmaktadırlar. Suçlular, suç gelirlerini ilk etapta kripto para birimine çevirmek zorundadır. Bu durum, suçluların bakış açısından iki temel savunmasızlık alanını vurgulamaktadır: Giriş ve Çıkış Noktaları (Hares, 2020) (Canellis, 2018).

Reel ekonomide, örneğin yatırım sahtekarlığı yoluyla para kazanan suçluların, gelirlerini kripto para birimlerine dönüştürmeleri gerekecektir, bu da karşılığında yasal para birimini kabul etmeye istekli bir taraf bulmak anlamına gelmektedir. Uygulamada - her büyüklükteki işlem için - gerçek (yasal) para biriminin ödemesinin banka gibi bir finans kuruluşundan geçmesi gerekmektedir (Holman ve Stettner, 2018, s. 32). Finans kuruluşunun kara para aklamayı önleme konusunda güçlü kontrolleri varsa, fonların kaynağının ve işlemin yapısının şüpheli görünüp görünmediğini değerlendirmesi ve varsa bunu yetkililere bildirmesi söz konusu olmaktadır. Kripto para birimi yasal para birimine dönüştürüldüğünde de benzer hususlar geçerli olmaktadır. Bu, adli muhasebecilerin, varlıkları izlemeye çalışırken odaklanabileceği bir alandır. Düzenlenmiş finansal kuruluşların sıkı "müşterini tanı (KYC)" kurallarına uyması gerekmektedir ve bu nedenle, düzenlemeler dahilinde faaliyet gösteren finansal kurumların kayıtları, tarafların kimlikleri hakkında yararlı bir bilgi kaynağı olabilmektedir (Perlman, 2020).

Düzenleyici otoritelere göre, kripto para birimi alıp satan, müşterilere giriş ve çıkış noktası sağlayan şirketler ve borsaların kötü bir şekilde düzenlenmesi büyük bir zayıflıktır. Bunlar tipik olarak kara para aklamayı önleme düzenlemelerinin dışında

faaliyet göstermektedirler. Bununla birlikte, kripto para birimlerinin yükselmesi ve buna bağlı olarak kara para aklama riskinin artması da bu durumu değiştirmektedir (Sharma, 2019). 2018 yılının Temmuz ayında yürürlüğe giren AB'nin 5. Kara Para Aklamaya Mücadele Direktifi, üye devletlerin daha sıkı kurallar koymasını, kripto para birimleri ve kripto para birimi borsalarını yasal para birimi ve bankalar için mevcut kurallarla uyumlu hale getirmesini gerekli kılmaktadır. 2018 yılının Aralık ayında ise Birleşik Krallık hükümeti, yeni direktifin gerekliliklerinin önemli ölçüde daha ötesine geçerek, tüm risklerin dikkatle ele alınacağını duyurmuştur (Krais, 2018).

Suçlular, doğal olarak, kara para aklama ile mücadelenin en zayıf olduğu alanlara yönelerek, para değişimini bu mecralarda gerçekleştirmektedir. Bu durum, kara para aklamayı tamamen yok etmenin hayli zor olduğu anlamına gelse de yasadışı faaliyetlerin, yargı alanının etkili olduğu mecraların dışına taşınmasına neden olmaktadır. Bir adli muhasebeci, işlemlerin etkili yargı alanlarının dışına taşınmasını şüphe uyandırıcı bir durum olarak değerlendirmelidir. Böyle bir yaklaşım, soruşturmanın odağını suç faaliyetinin en muhtemel olduğu alanlara doğru daraltmaya yardımcı olabileceği için oldukça yararlıdır (Houben ve Snyers, 2018, s. 79). Dijital para biriminin izlenemez olduğu ve tamamen anonim olduğu yaygın bir yanılgıdır. Cüzdanların, teknik kripto para sistemi içinde, anonim bilgisayar adresleri olarak saklandığı doğru olsa bile cüzdanlar ile kişileri birbiri ile ilişkilendirmenin çok çeşitli yolları vardır. Bunlar, işlem modeli analizi (örneğin varlık transfer kayıtlarını kripto para birimi defterindeki işlemlerle eşleştirme) veya sadece iş birliği yapan taraflardan bilgi alma gibi geleneksel adli araştırma tekniklerini içerebilmektedir. Daha gelişmiş teknikler ise belirli sunucular ve IP adresleri aracılığıyla internet trafiğinin analiz edilmesini içermektedir (Bohannon, 2016).

Esasen, kripto para birimleri adli muhasebecilerin en iyi arkadaşı olabilmektedir. Çünkü, kripto para birimleri ile gerçekleştirilen işlemlerin tam anlamıyla hepsi silinmez bir şekilde Blockchain üzerinde kaydedilmektedir. Üstelik, Bitcoin gibi geleneksel kripto para birimleri için bu Blockchain, halka açık bir dağıtık defterdir. Her işlem kelimenin tam anlamıyla herkesin görmesi ve analiz etmesi için orada kayıtlıdır (Jacque, 2018). Bu durum, adli muhasebecilerin, gelişmiş grafik veritabanı sistemlerinin (matematikte grafik, cüzdanlar gibi düğümler ve cüzdanlar arasındaki işlemler gibi bir bağlantılar ağıdır) yardımıyla kaydedilen işlemleri analiz etmek için grafik teknolojisini

ve ağ teorisini kullanmasına imkân sağlamaktadır (Musiala vd., 2020, s. 6). Bu sistemler, yoğun trafik rotaları ve faaliyet kümeleri gibi faaliyet modellerini veya görünüşte farklı bireysel işlemlerin nihai hedefini belirlemek için farklı cüzdanlar arasındaki yüz binlerce işlemi analiz etmek için kullanılabilir. Tüm işlemler tamamen kaydedildiğinden dolayı akışları ağdaki çok sayıda ara düğümden giriş ve çıkış noktalarına kadar izlemek mümkün olabilmektedir. Soruşturmanın odak noktası buradan, varlıkların kripto ve geleneksel varlıklar arasında dönüştürüldüğü ilgili kripto para birimi değişimine ve ardından normal banka hesaplarına çevrilebilmektedir. Yukarıda bahsedildiği gibi, düğümlerin her birini kimin kontrol ettiğini belirlemek için daha geleneksel teknikler kullanılabilir (Yousaf vd., 2019, s. 846).

Bu nedenle, kripto para teknolojisi, bir kez iyi bir şekilde anlaşıldığında, adli muhasebeciler, açık işlem sırlarını kırmak için bir dizi geleneksel ve yeni nesil araç kullanabilmektedir. Bununla birlikte, anonimlik bir kez ortadan kaldırıldığında, kripto para defteri, tümü düzgün bir şekilde bağlanmış, eksiksiz ve doğru bilgileri içeren bir hazine haline gelebilmektedir ki bu geleneksel adli varlık takibinde nadiren mümkün olan bir durumdur (Paul, 2019).

Netice itibarıyla kripto para ve Blockchain yeni bir teknoloji olduğu için diğer teknolojiler gibi çeşitli risklere maruz kalmaktadır.

Söz konusu riskler aslında iki tür risklere ayrılabilir, birincisi yatırımcıların bu yeni yatırım teknolojilerine hakim olmadıklarına rağmen hızlıca yatırım yapıp kazanç elde etmek peşinde olduklarından kaynaklanırken ikincisi ise bu tür para fiziki varlığı olmayıp dijital para olduğu için suçlular tarafından, yolsuzluk kazanma dolandırıcılığı ve çalınma ihtimali yüksek olduğundan kaynaklanmaktadır.

Kripto para genel olarak hem anonim hem de merkezi olmayan bir para türü olduğu için kara para aklamakta kullanılabildiği gibi terörü finanse etmekte de kullanılabilir.

Örnek olarak Monero ve Zcash paranın anonimlik derecesi tam olmasa da çok yüksek olması, bu paranın takip edilmesini zor kılarken bitcoin paranın anonimlik derecesinin düşüklüğü, takip edilmesini daha kolay hale getirmiştir.

Diğer tarafta adli muhasebenin teknikleri ve adli muhasebecilerin yüksek becerileri, kripto paranın dolandırıcılığının yolunu kesmiştir. Kripto para hareketlerini

takibine ihtiyaç duyulduđu için adli muhasebe teknikleri ortaya çıkmıştır. Söz konusu tekniklerin sayesinde Kripto/Blockchain adli denetim firmaları yeni hizmet sektörü olarak ortaya çıkmaya başlamıştır.



SONUÇ VE ÖNERİLER

Adli muhasebe teknikleri, terör finansmanı, kara para aklama, uyuşturucu kaçakçılığı, vergi kaçırma ve zimmete para geçirme gibi çeşitli dolandırıcılık tespit operasyonlarında kullanılan en iyi yöntem ve tekniklerden biridir.

Sertifikalı adli muhasebeciler aracılığıyla adli muhasebe, tarafsız ve doğru kararlar verebilmek için gerekli tavsiyeleri sunarak çeşitli taraflar arasındaki mali uyumsuzlukların çözümü için mahkemelere gerekli desteği sağlamaktadır. Adli muhasebenin önemi ve hassasiyeti nedeniyle de adli muhasebeciler, en iyi yeminli ve uzman muhasebeciler arasından bir takım özel testlere tabi tutularak seçilmektedir.

Adli muhasebenin ortaya çıkışı yüz yıldan daha uzun bir zamana dayanmasına karşın, şirketlerdeki ve kurumlardaki yolsuzluklarla mücadele de adli muhasebenin sağladığı hizmetlere yönelik ihtiyaç son yirmi yılda anlaşılmıştır. Adli muhasebe henüz hakkettiği ilgiyi görememektedir. Bu nedenle, adli muhasebecilerin, özellikle modern bir şekilde ve yeni teknolojiler yardımıyla ileri düzeyde eğitilmesi gerekmektedir. Böylece, adli muhasebeye yönelik ilgi artabilecektir.

İşlemenin ya da şirketin büyüklüğüne bağlı olarak, dolandırıcılık vakalarının yalnızca düzenli güvence ve denetim hizmetleri ile takibi zorlaşmıştır. Günümüzde şirketler ve kurumlar, dolandırıcılık ile mücadelede adli muhasebe desteğine ihtiyaç duymaktadır. Özellikle kripto para varlıklar üzerinden yapılan yolsuzluklarda adli muhasebenin önemi daha da belirgin hale gelmektedir. Bahse konu kripto varlıklar Blockchain teknolojisi ile oluşturulup izlenmektedir. Söz konusu blockchain dijital bilgileri oluşturan ve paylaşan halka açık bir dağıtık defter sistemidir. Bu sistemde merkezi kayıt birimi ortadan kalkmaktadır günümüzde bu teknoloji konusunda araştırma sınırlıdır. Ancak bahse konu teknolojinin muhasebe ve denetim sistemleri üzerinde büyük bir etkiye sahip olacağı kaçınılmaz gözükmektedir. Bu bakımından

arařtırmaların bu alana yoğunlařmasının muhasebe ve denetim alana katkıda bulunacaktır.

Para biriminin geliřmesiyle birlikte muhasebe talebi de artmıřtır. Kripto para birimlerinin gelecekteki para birimlerini geliřtirilmesiyle, faiz oranlarının hesaplanıp hesaplanamayacađını, yükselen faiz oranlarının, fiyat eğilimlerinin, vergilerin veya potansiyel bilinmeyen sorunların değeriendirilip değeriendirilemeyeceđini her zaman dikkate almak gerekecektir. IASB Komitesi talimatları uyarınca, kripto varlıklar yalnızca bulundurma amacıyla kullanılmadıkları sürece ve daha sonra UMS 2 stok standardına göre iřleme tabi tutulmadıkça, hem muhasebe kayıtlarında hem de açıklamalarda UMS 38 maddi olamayan duran varlıklar standartlarına göre değeriendirilmelidir. Kripto varlıkların kullanıldıđı tüm olası teorilerin ele alındıđı, dođru, kesin ve spesifik bir standarda ihtiya duyulmaktadır. Kripto para teknolojileri ok hızlı bir řekilde geliřtiđi ve sürekli güncellendiđi iin, mevcut standartlar yeterli olmamaktadır.

Kripto para birimleri ile gerekleřtirilen iřlemlerde, iřlem güvenliđinin sađlaması iin herhangi bir üçüncü taraf aracı kuruma ihtiya duyulmamaktadır. Banka, birinin bilgilerini açıklamaya kanunlarla zorlanabilirken, Bitcoin sisteminde böyle bir durum söz konusu olmamaktadır. Kripto para piyasaları, ok eřitli suç faaliyetlerine ve mali suçlara karřı potansiyel olarak savunmasızdır. ek olarak, kripto para birimlerinin anonimliđi, likiditesi ve sınırsız dođası, kripto para birimlerini potansiyel kara para aklayıcıları iin oldukça cazip kılmaktadır Kripto paraların oluřturulma kolaylıđı ve anonimliđi, kripto para hesaplarını, terörizme finansman sađlama ve yaptırımlardan kaınma gibi yasadıřı iřlemler iin ideal hale getirmektedir. Bununla birlikte, internet üzerinden ya da kitle fonlama yöntemiyle alıřan bađıř platformları üzerinden yürütölen kampanyalar ile kripto para ile yardım kabul ederek, bu gelirleri faaliyetlerinde kullanan terör örgütleri de vardır. Ayrıca, yaptırımlardan kaınmaya alıřan devletler de kripto para birimleri ile iřlem yapma yoluna gitmektedirler.

ok sayıda avantajı ve dezavantajı olan blockchain teknolojisi ok uzun süre varlıđını sürdürecektir. Otomasyon teknolojilerinin geliřmesi ile birlikte gelecekte dünya genelinde muhasebeci sayısı azalacaktır. Bu nedenle, muhasebecilerin eđitiminde teknolojik, profesyonel ve etik alanlarda bir etkileřim ortamı yaratılmalıdır. Böylelikle,

muhasebecilerin finansal sektörleri mükemmel bir şekilde sevk ve idare etmek için mesleki eğitim kalitelerinin sürekli olarak artırılması gerekmektedir. Kripto para birimi günlük bir ödeme aracı haline geldiğinde, muhasebe talebi katlanarak artacaktır. Kripto para birimi işlemlerini düzenleme, organize etme, izleme ve yönetme ihtiyacı yeni fırsatlar ve zorluklar getirdi.

Kripto para ana ödeme sistemi haline geldiğinden, kripto para muhasebesi, kripto para işlemlerinin meşruiyetini korumanın anahtarıdır. Kripto para birimleri, yasal para birimlerine karşı daima var olacaktır. Yakın gelecekte kripto para birimlerinin kaderi üç şekilde belirlenecektir: 1) Ya kripto paralar resmi olarak benimsenecektir 2) ya resmi olarak düzenlemeye tabi tutulacaktır 3) ya da hükümetler kendi kripto para birimlerini çıkaracaktır. Kripto para birimlerinin kullanımına ve kripto paralarla gerçekleştirilecek işlemlere yönelik düzenlemelerin yapılmadığı her ülkede kripto para birimlerinin gerçek bir ulusal güvenlik tehdidi olarak değerlendirilmesi kuvvetle muhtemeldir.

Dolandırıcıların çoğu, insanların zengin olma hırsından yararlanmaktadır. Dolayısıyla, dolandırıcılık vakalarını en aza indirmek için, profesyonel olmayan yatırımcılara yönelik farkındalık artırıcı ve bilgi sağlayıcı özel eğitim programları ve kurslar düzenlenmelidir. Öte yandan adli muhasebe teknikleri ve yöntemleri, dolandırıcılıkla mücadelede, risk tahmini ve yönetiminde, soruşturmalarda ve denetimlerde en iyi sonuçları elde etmek için siber teknolojilerle ve bilişim unsurlarıyla birleştirilebilmektedir. Hem adli muhasebe hem de kripto para alanları, ayrı ayrı ve birlikte ele alınarak, her iki alanda da daha fazla çalışma ve araştırma gerçekleştirilmesi gerekmektedir. Her iki alanda da yapılan çalışma sayısı yeterli değildir. Bu alanlarda yapılan çalışmaların ve araştırmaların artması, bu konuda çalışan uzmanlara ve profesyonellere kolaylık sağlayacaktır.

Bu nedenle araştırmacılara bahse konu blockchain teknolojisi, kripto varlık ve adli muhasebe konusunda spesifik çalışmalar yapmaları önerilmektedir.

KAYNAKÇA

- ACCA. (2019). *Accounting for cryptocurrencies*. ACCAGlobal: <https://www.accaglobal.com/in/en/student/exam-support-resources/professional-exams-study-resources/strategic-business-reporting/technical-articles/cryptocurrencies.html>
- Acheson, N. (2019). *The Hidden Effects of Crypto Money Laundering Rules*. Consensus: <https://www.coindesk.com/the-hidden-effects-of-crypto-money-laundering-rules>
- Actionfraud.police.uk. (2018). *Well-known names being used in cryptocurrency scams*. ActionFraud: <https://www.actionfraud.police.uk/news/well-known-names-being-used-in-cryptocurrency-scams>
- Agrawal, G. (2020). *How to trace Bitcoin transactions or address?* Bitquery: <https://bitquery.io/blog/trace-bitcoin-transaction-and-address>
- Aksu, İ., Uğur, A., & Çukacı, Y. (2008). Adli Muhasebe ve Adli Muhasebecilik Mesleğinin Bir Kolu Olarak Bilirkişilik. *Yönetim ve Ekonomi Araştırmaları Dergisi*, 6(9), 63-71.
- Alibhai, S., Bakker, E., Balasubramanian, T. V., Bharadva, K., Chaudhry, A., Coetsee, D., . . . Yeung, P. (2018). *Interpretation and Application of IFRS Standards*. John Wiley & Sons, Inc.
- Anderson, D. (2016). *Arbitrating Inheritance Battles an Important Role for Forensic Accountants*. David Anderson & Associates LLC: <http://davidandersonassociates.com/arbitrating-inheritance-battles-an-important-role-for-forensic-accountants/>
- Angotti, A., Shea, A., & Sisul, E. (2018). *Cryptocurrency Red Flags in U.S. Dollar Transaction Monitoring: A Practical Approach to Assessing Risk*. Navigant Consulting, Inc.
- Arens, A. A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2016). *Auditing and Assurance Services*. Pearson Education Limited.
- Aygören, H., & Kurtcebe, E. (2019). Türev Finansal Araçların Muhasebe Standartlarına Göre Muhasebeleştirilmesi. *Muhasebe ve Finansman Dergisi*, 84, 1-16. <http://doi.org/10.25095/mufad.625644>
- Baker Tilly. (2018). *Forensic accounting: why it's vital and the role it plays in the insurance world*. bakertilly: <https://www.bakertilly.com/insights/forensic-accounting-why-its-vital-and-the-role-it-plays-in-the-insurance-wo>
- Barski, C., & Wilmer, C. (2014). *Bitcoin for the Befuddled*. No Strach Press.
- BDO. (2019). *Cryptocurrency: The Top Things You Need To Know*. BDO USA, LLP.
- Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business & Information Systems Engineering*, 11(10), 381-384. <https://doi.org/10.1007/s12599-017-0505-1>
- Bhasin, M. (2007). Forensic Accounting: A New Paradigm For Niche Consulting. *The Chartered Accountant*, 1, 1000-1010.
- BIDITEX Exchange; The Startup. (2019). *The Risks of Cryptocurrency: The Dangers of Investing In Crypto*. Medium: <https://medium.com/swlh/the-risks-of-cryptocurrency-the-dangers-of-investing-in-crypto-406fad8307e5>

- bitcoin.org. (2019). *Glossary*. Developer.bitcoin:
<https://developer.bitcoin.org/glossary.html>
- Blockchain.com. (2020). *Blockchain Size (MB)*. Blockchain:
<https://www.blockchain.com/charts/blocks-size>
- Bloomenthal, A. (2020). *Detecting Financial Statement Fraud*. Investopedia:
<https://www.investopedia.com/articles/financial-theory/11/detecting-financial-fraud.asp>
- Bodden, A., Schulman, J., & Briggs, T. (2019). *Cryptocurrency: cybersecurity and the operational risks*. Cayman Funds:
<https://www.caymanfundsmagazine.com/contributed-article/cryptocurrency-cybersecurity-and-the-operational-risks>
- Bohannon, J. (2016). *Why criminals can't hide behind Bitcoin*. SienceMag:
<https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>
- Bonhill Group Plc. (2018). *The technologies behind cryptocurrencies*. Information Age:
<https://www.information-age.com/technologies-behind-cryptocurrencies-123470617/>
- Bratspies, R. M. (2018). Cryptocurrency and the Myth of the Trustless Transaction. *Michigan Technology Law Review*, 25(1), 1-57.
- Brett, J. (2020). *Trend Continues For Countries Looking To Evade U.S. Sanctions Using Crypto*. Forbes:
<https://www.forbes.com/sites/jasonbrett/2020/01/29/trend-continues-for-countries-looking-to-evade-us-sanctions-using-crypto/?sh=a80889959ffd>
- Bridgers, A., Kosoff, J., & Lee, H. (2019). *Understanding the Risks of Cryptocurrency in Financial Services*. The Risk Management Association:
<https://www.rmahq.org/understanding-the-risks-of-cryptocurrency-in-financial-services/>
- BTCJam/Wikipedia. (2014). Wikipedia: <https://en.wikipedia.org/wiki/BTCJam>
- businessdegrees.uab.edu. (2019). *What Can You Do in Forensic Accounting with an Accounting Degree?* UAB Collat: <https://businessdegrees.uab.edu/blog/an-overview-of-forensic-accounting/>
- Calvo, S., & Morales, A. (2014). *Exploring complementary currencies in Europe: a comparative study of local initiatives in Spain and the United Kingdom*. Living in Minca.
- Canellis, D. (2018). *Here's how criminals use Bitcoin to launder dirty money*. Thenextweb: <https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/>
- Cawrey, D. (2014). *Are 51% Attacks a Real Threat to Bitcoin?* Coindesk:
<https://www.coindesk.com/51-attacks-real-threat-bitcoin>
- Chainalysis. (2019). *Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams*.
- Chainbits.com. (2018). *Trezor vs Ledger vs Keepkey: Which is The Best Cryptocurrency Hardware Wallet?* Chainbits: <https://www.chainbits.com/wallets/trezor-vs-ledger-vs-keepkey/>

- Chandrasekera, S. (2020). *How The IRS Knows You Owe Crypto Taxes*. Forbes: <https://www.forbes.com/sites/shehanchandrasekera/2020/01/27/how-the-irs-knows-you-owe-crypto-taxes/?sh=37961a14438e>
- Charafeddine, R., & Barakat, W. (2018). *Mihnat Al-Muhasebe fi Asri il-Blockchain: Al-Tahadiyatu ve'el-Aqfak [Blockchain Çağında Muhasebe Mesleği: Zorluklar ve Beklentiler]*. Beyrut Arap Üniversitesi.
- Choudhury, S. R. (2018). *It's a very good time to be a money launderer, and you can thank cryptocurrencies*. CNBC: <https://www.cnbc.com/2017/08/04/icos-may-be-seen-as-securities-by-u-s-and-singapore-regulators.html>
- Chuen, D. L., & Low, L. (2018). *Inclusive FINTECH Blockchain, Cryptocurrency and ICO*. World Scientific.
- CipherTrace. (2018). *Cryptocurrency Anti-Money Laundering Report 2018 Q2*. CipherTrace.
- Coenen, T. L. (2009). *Expert Fraud Investigation: A Step-By-Step Guide*. John Wiley and Sons, Inc.
- Cohen, C. (2015). *Forensics and Bitcoin*. Forensic Focus: <https://www.forensicfocus.com/articles/forensics-bitcoin/>
- Coinbase.com. (2018). *Coinbase and Circle announce the launch of USDC — a Digital Dollar*. Coinbase: <https://blog.coinbase.com/coinbase-and-circle-announce-the-launch-of-usdc-a-digital-dollar-2cd6548d237>
- coingecko.com. (2020). *coingecko*. coingecko: <https://www.coingecko.com/>
- Coinlore. (2020). *Live Cryptocurrency Prices & Coin Market Caps*. Coinlore: <https://www.coinlore.com/>
- CoinMarketCap. (2020). *Today's Cryptocurrency Prices by Market Cap*. CoinMarketCap: <https://coinmarketcap.com/>
- Cointelegraph.com. (2018). *How To Buy ICO Tokens: Beginner's Guide*. Cointelegraph: <https://cointelegraph.com/ico-101/how-to-buy-ico-tokens-beginners-guide>
- Cointelegraph.com. (2020). *Bitcoin Fiyat Endeksi*. Cointelegraph: <https://cointelegraph.com/bitcoin-price-index>
- Coleman, D. (2014). *Benford's Law and Financial Statements*. Audit Analytics: <https://blog.auditanalytics.com/benfords-law-and-financial-statements/>
- Committee of Sponsoring Organizations of The Treadway Commission. (2016). *Fraud Risk Management Guide*. Committee of Sponsoring Organizations of The Treadway Commission (COSO).
- Congress. (2018). *H.R.6411 - FinCEN Improvement Act of 2018*. Congress: <https://www.congress.gov/bill/115th-congress/house-bill/6411/text>
- CPA Canada, AICPA Ve UWCISA. (2017). *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession*. Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf>

- Crumbley, D. L. (2009). So what is forensic accounting? *Accounting Behavior and Organization*, The American Accounting Association. <https://aaahq.org/Portals/0/documents/segments/ABO/fall09.pdf>
- Crumbley, D. L., Heitger, L. E., Smith, S., & Smith, G. (2003). *Forensic and Investigative Accounting*. CCH. INC.
- Crumbley, D., & Apostolou, N. (2002). Forensic Accounting: A New Growth Area in Accounting. *CPA Journal*, 16(3), 16-21.
- Crumbley, D., Heitger, L. E., Smith, S., & Smith, G. (2015). *Forensic and Investigative Accounting*. CCH. INC.
- Cryptocurrency *tumbler/Wikipedia*. (2015). Wikipedia: https://en.wikipedia.org/wiki/Cryptocurrency_tumbler
- Cryptocurrency/Wikipedia. (2020). Wikipedia: <https://en.wikipedia.org/wiki/Cryptocurrency>
- Cryptopedia. (2018). *What Is a Crypto Dusting Attack?* Gemini Cryptopedia: <https://www.gemini.com/cryptopedia/crypto-dusting-attack-bitcoin>
- Daniel, J. G., & Green, A. (2018). *IFRS (#) — Accounting for crypto-assets*. EYGM Limited.
- Davis, C., Farrell, R., & Ogilby, S. (2010). *Characteristics and Skills of the Forensic Accountant*. American Institute of Certified Public Accountants.
- Deloitte. (2005). *TMS 32 : Finansal Araçlar: Sunum*. Verginet: https://www.verginet.net/dtt/1/TMS32FinansalAraclarSunum_10083.aspx
- Deloitte. (2015). *IAS 36 — Impairment of Assets*. IAS Plus: <https://www.iasplus.com/en/standards/ias/ias36>
- Deloitte Consulting GmbH. (2016). *Blockchain Technology: A game-changer in accounting?* Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft.
- Demeter, C. (2018). *Is Cryptocurrency Money Laundering a Real Threat?* AML Right Source: <https://www.amlrightsource.com/news/posts/cryptocurrency-money-laundering-red-flags>
- DeVries, P. D. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. *International Journal of Business Management and Commerce*, 1(2), 1-9.
- Dhar, P., & Sarkar, A. (2010). Forensic Accounting: An Accountant's Vision. *Vidyasagar University Journal of Commerce*, 10, 93-104.
- DiscoverAccounting. (2019). *Top Eight Reasons Forensic Accountants Are Hired*. DiscoverAccounting: <https://discoveraccounting.org/top-8-reasons-forensic-accountants-are-hired>
- Disparte, D. (2018). *Beware Of Crypto Risks - 10 Risks To Watch*. Forbes: <https://www.forbes.com/sites/dantedisparte/2018/07/21/beware-of-crypto-risks-10-risks-to-watch/?sh=798323365f17>
- DOJ, USDT, DHS, Federal Reserve, USPS. (2005). *U.S Money Laundering Threat Assessment*.
- Doody, H. (2009). *Fraud Risk Managment: A Guide to Good Practice*. Chartered Institute of Management Accountants.
- Doran, M. (2015). *A Forensic Look at Bitcoin Cryptocurrency*. SANS Institute.

- Dorrell, D. D., & Gregory, A. (2012). *Financial Forensics Body of Knowledge*. John Wiley & Sons, Inc.
- Drug Enforcement Administration. (2017). *National Drug Threat Assessment*. DEA: https://www.dea.gov/sites/default/files/docs/DIR-040-17_2017-NDTA.pdf
- Elliott, L. C. (2016). *Fraud Risk Assessments: A Key Tool for Organizations, Forensic Accountants and Internal Auditors*. EisnerAmper LLP: <https://www.eisneramper.com/fraud-risk-assessments-1116/>
- El-Sayid, M. H. (2018). Al-Tadkik El-Dahili Val-Mutagayirat Al-Teknolojiya Al-Haditha. *Auditors Magazine*, 1, 14-20.
- Engle, E. (2016). Is Bitcoin Rat Poison? Cryptocurrency, Crime, And Counterfeiting (CCC). *Journal of High Technology Law*, 16, 340-393.
- Enofe, A., Okpako, P., & Atube, E. (2013). The impact of forensic accounting on fraud detection. *European Journal of Business and Management*, 5 (26), 61-72.
- European Central Bank. (2015). *Virtual currency schemes – a further analysis*. European Central Bank.
- Europol. (2018). Illegal Network Used Cryptocurrencies and Credit Cards to Launder More Than EUR 8 Million from Drug Trafficking. <https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking>
- EY. (2018). *Applying IFRS Accounting by holders of crypto assets*. EYGM Limited.
- EY. (2019). *Holdings of cryptocurrencies*. EYGM Limited.
- Fanusie, Y. J., & Robinson, T. (2018). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Elliptic.
- FATF. (2019). Guidance for A Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>
- FAU - Centre of Forensic Accounting. (2019). *Cryptocurrency Fraud*. Florida Atlantic University: <https://business.fau.edu/centers/center-for-forensic-accounting/public-resources-on-fraud/particular-areas-of-fraud/cryptocurrency-fraud/>
- Fernandes, J., Fields, B., Ward, K., Werling, R., & Wildenborg, I. (2018). *Blockchain and Digital Currencies Challenge Traditional Accounting and Reporting Models*. KPMG LLP.
- FinCEN. (2019). Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies.
- FinTech Network. (2018). Four Blockchain Use Cases for Banks. https://germanyfintech.org/wp-content/uploads/2018/01/fintech_blockchain_report_fintech_network.pdf
- Floris, S. (2020). *Mobile Payment Apps in China for International Students*. China Scholar: <https://www.china-scholar.com/mobile-payment-apps-in-china-for-international-students/>

- Forensic Focus. (2013). *Bitcoin Forensics Part II: The Secret Web Strikes Back*. Forensic Focus: <https://www.forensicfocus.com/articles/bitcoin-forensics-part-2-the-secret-web-strikes-back/>
- Franco, P. (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*. John Wiley & Sons Ltd.
- Frankenfield, J. (2019). *51% Attack*. Investopedia: <https://www.investopedia.com/terms/1/51-attack.asp>
- Frankenfield, J. (2020). *Initial Coin Offering (ICO)*. Investopedia: <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>
- Fullana, O., & Ruiz, J. (2020). Accounting information systems in the blockchain era. *International Journal of Intellectual Property Management*, 11(1), 63-80.
- Fuscaldo, D. (2018). *Investors Still Interested In Cryptocurrency But Crave More Education*. Forbes: <https://www.forbes.com/sites/donnafuscaldo/2018/12/20/investors-still-interested-in-cryptocurrency-but-crave-more-education/?sh=1a66ebe0efcc>
- Galvanize. (2018). *4 Data Mining Techniques for Businesses (That Everyone Should Know)*. Galvanize Blog: <https://blog.galvanize.com/four-data-mining-techniques-for-businesses-that-everyone-should-know/>
- Garcia, R. I. (2018). *What is Data Matching?* Infosimples Medium: <https://medium.com/neuronio/what-is-data-matching-9478c80da888>
- GlobeNewswire-GN. (2017). *SEB and Nasdaq to Build Blockchain for Swedish Mutual Fund Market*. Nasdaq: <https://www.nasdaq.com/about/press-center/seb-and-nasdaq-build-blockchain-swedish-mutual-fund-market>
- Göbel, J., Keeler, H. P., Krzesinski, A., & Taylor, P. (2016). Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, 104, 23-41. <https://doi.org/10.1016/j.peva.2016.07.001>
- Golden, T. W., Skalak, S. L., & Clayion, M. M. (2006). *A Guide To Forensic Accounting Investigation*. John Wiley & Sons, INC.
- Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *Proceedings on Privacy Enhancing Technologies*, 4, 179-199.
- Goldfeder, S., Narayanan, A., Bonneau, J., Felten, E., & Miller, A. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
- Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J. (2017). *Terrorist Use Of Virtual Currencies: Containing the Potential Threat*. Center for a New American Security.
- Goldrick, M., & Gerson, R. (2002). *The definitive work on genograms is Genograms in Family Assessment* (3üncü b.). W. W. Norton & Company, Inc.,.
- Gottschalk, P. (2018). *Investigating White-Collar Crime*. Springer International Publishing AG. <https://doi.org/10.1007/978-3-319-68916-6>
- Graham, E. (2005). *Management Accounting Officail Terminology*. CIMA Exam Support Books. Elsevier.

- Grant Thornton. (2018). *IFRS Viewpoint Accounting for Cryptocurrencies - the basics*. Grant Thornton International Ltd.
- Grant, C. (2018). *A decade before crypto, one digital currency conquered the world — then failed spectacularly*. TheHustle: <https://thehustle.co/beenz-pre-bitcoin-digital-currency>
- Gray, D. (2008). Forensic Accounting And Auditing: Compared And Contrasted To Traditional Accounting And Auditing. *American Journal of Business Education*, 1(2), 115-126.
- Greenberg, A. (2013). *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*. Forbes: <https://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/?sh=2f057fb1adf7>
- Greenberg, A. (2014). *'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever*. Wired: <https://www.wired.com/2014/04/dark-wallet/>
- Greenberg, A. (2016). *The Silk Road's Dark-Web Dream Is Dead*. Wired: <https://www.wired.com/2016/01/the-silk-roads-dark-web-dream-is-dead/>
- Grippio, F. J., & Ibex, J. (2008). Forensic Accounting: Should It Be A Required Course For Accounting Majors? *The Journal of Applied Business Research*, 24(1), 129-136.
- Gül, H. (2018). Blokzincir (Blockchain) Teknolojisi ve Muhasebe. *Sosyal, Beşeri ve İdari Bilimler Alanında Yenilikçi Yaklaşımlar*, Gece Akademi.
- GÜLTEKİN, Y., & BULUT, Y. (2016). Bitcoin Ekonomisi: Bitcoin EkoSisteminden Doğan Yeni Sektörler ve Analizi. *Sosyal Bilimler Enstitüsü Dergisi*, 3(3), 82-92.
- Güncenme Gençoğlu, Ü. (2017). Temel Konularda BOBİ FRS ve TMS/TFRS Karşılaştırması. *Muhasebe ve Finansman Dergisi*, (76), 1-24. <https://doi.org/10.25095/mufad.400056>
- Gupta, M. (2017). *Blockchain for dummies*. John Wiley & Sons, Inc.
- Hajdarbegovic, N. (2014). *BitPay Now Processing \$1 Million in Bitcoin Payments Every Day*. Coindesk: <https://www.coindesk.com/bitpay-now-processing-1-million-bitcoin-payments-every-day>
- Hares, S. (2020). *5 ways accountants can track cryptocurrency*. Journal of Accountancy: <https://www.journalofaccountancy.com/newsletters/2020/jun/accountants-track-cryptocurrency.html>
- Harrell, C. (2010). *Overall DF Investigation Process*. Journey Into Incident Response: <http://journeyintoir.blogspot.com/2010/10/overall-df-investigation-process.html>
- Hechat, M. (2010). *Unveiling the Mystery of Forensic Accounting*. Accounting Today: <https://www.accountingtoday.com/news/unveiling-the-mystery-of-forensic-accounting>
- Hennessy, K. (Dü.). (2014). *How Money Works*. Dorling Kindersley.
- Higgins, S. (2014). *3 Pre-Bitcoin Virtual Currencies That Bit the Dust*. Coindesk: <https://www.coindesk.com/3-pre-bitcoin-virtual-currencies-bit-dust>
- Hileman, G., & Rauchs, M. (2017). *Global Cryptocurrency Benchmarking Study*. Cambridge center for alternative finance.

- Holman, D., & Stettner, B. (2018). Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches. *The International Comparative Legal Guide to: Anti-Money Laundering*. Washington, D.C.: Allen & Overy, LLP.
- Homeland Security Enterprise. (2014). *Risks and Threats of Cryptocurrencies*. Virginia: Homeland Security Studies & Analysis Institute.
- Horowitz, J., While, T., & Virgilio, R. (2018). *Compliance with Regulatory Obligations*. KPMG.
- Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain : Legal context and implications for financial crime, money laundering and tax evasion*. Brussels: European Parliament.
- Hrones, M. (2018). *Yes, Your Bitcoin Transactions Can Be Tracked – And Here Are the Companies That Are Doing It*. Bitcoinist: <https://bitcoinist.com/yes-your-bitcoin-transactions-can-be-tracked-and-here-are-the-companies-that-are-doing-it/>
- Huber, E., & Glenn, D. A. (2009). *Forensic Accounting for Divorce Engagements: A Practical Guide*. American Institute of Certified Public Accountants, Inc.
- Hudson intelligence. (2018). *Cryptocurrency Fraud*. Fraud Investigation: <https://www.fraudinvestigation.net/cryptocurrency>
- Humaidat, J. (2014). *Khabir Al-Ma"aiyer Al-Duvvaliya Li I"dad Al kavaym Al-Maliya [Finansal tabloların hazırlanması için UFRS Uzmanı] IFRS EXPERT*. International Arab Society of Certified Accountants (IASCA).
- IASB. (2018). Transactions involving commodities and cryptocurrencies.
- IFRS Interpretations Committee - IFRIC. (2019). Holdings of Cryptocurrencies—Agenda Paper 12.
- InspireMalibu.com. (2016). *Silk Road May Be Gone, But Online Drug Cryptomarkets Still Exist*. Inspire Malibu: <https://www.inspiremalibu.com/blog/drug-addiction/silk-road-may-be-gone-but-online-drug-cryptomarkets-still-exist/>
- Institute of Chartered Accountants in England and Wales (ICAEW). (2018). *Blockchain and The Future of Accountancy*. ICAWE: <https://www.icaew.com/-/media/corporate/files/technical/information-technology/thought-leadership/blockchain-and-the-future-of-accountancy.ashx>
- International Securities Services Association (ISSA). (2018). *Infrastructure for Crypto-Assets: A Review by Infrastructure Providers*. International Securities Services Association.
- Investor-SEC. (2017). *Investor Bulletin: Initial Coin Offerings*. Investor: <https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins-16>
- Jacque, A. E. (2018). *Why Blockchain Technology Won't Replace the Forensic Accountant*. WIPFLI: <https://www.wipfli.com/insights/articles/cons-why-blockchain-technology-wont-replace-forensic-accountant>
- Jake. (2018). *Alert: Crypto Dusting is a New Type of Blockchain Spam that Corrodes Reputations and Impacts Cryptocurrency AML*. Ciphertrace: <https://ciphertrace.com/crypto-dusting/>

- Jenkinson, G. (2018). *Unpacking the 5 Biggest Cryptocurrency Scams*. Cointelegraph: <https://cointelegraph.com/news/unpacking-the-5-biggest-cryptocurrency-scams>
- Jofre, M. (2017). Fighting Accounting Fraud Through Forensic Analytics.
- Karancher, M. J., Riley, R. A., & Wells, J. T. (2011). *Forensic Accounting And Fraud Examination*. John Wiley & Sons. INC.
- KGK. (2018). TMS 32 : Finansal Araçlar : Sunum. https://www.kgk.gov.tr/Portalv2Uploads/files/DynamicContentFiles/T%C3%BCrkiye%20Muhasebe%20Standartlar%C4%B1/TMSTFRS2018Seti/TMS/TMS_32_2018.pdf
- KGK. (2018). TMS 38 : Maddi Olmayan Duran. <https://www.kgk.gov.tr/Portalv2Uploads/files/DynamicContentFiles/T%C3%BCrkiye%20Muhasebe%20Standartlar%C4%B1/TMSTFRS2011Seti/TMS38.pdf>
- King, D. (2016). *Banking Bitcoin-Related Businesses: A Primer for Managing BSA/AML Risks*. Federal Reserve Bank of Atlanta: https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/2016/banking-bitcoin-related-businesses.pdf
- Kirby, D. (2017). *Forensic Accounting and Cryptocurrencies*. AaccountingWeb: <https://www.accountingweb.com/community/blogs/david-kirby/forensic-accounting-and-cryptocurrencies>
- Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent Industry Adoption and Implications for Accounting. *Journal of Emerging Technologies in Accounting*, 14(2), 91-100. <https://doi.org/10.2308/jeta-51911>
- Koshy, P. (2013). *Coinseer: A Telescope Into Bitcoin*. Pennsylvania University Press
- Krais, J. (2018). *EU: 5th EU Anti-Money Laundering Directive published*. Global Compliance News: <https://globalcompliancenews.com/eu-5th-anti-money-laundering-directive-published-20180716/>
- Lagarde, M. J. (2019). Security Assessment of Authentication and Authorization Mechanisms in Ethereum, Quorum, Hyperledger Fabric and Corda. Ecole Polytechnique Federale De Lausanne.
- Lathrop Gage. (2018). *Cryptocurrency, Money Service Businesses and Anti-Money Laundering Laws*. LathropGPM: <https://www.lathropgpm.com/newsroom-alerts-Cryptocurrency-Money-Service-Businesses-and-Anti-Money-Laundering-Laws.html>
- Laurence, T. (2017). Improving the Anonymity of the IOTA Cryptocurrency. <https://www.iota.org/foundation/research-papers>
- Lazanis, R. (2015). *How Technology Behind Bitcoin Could Transform Accounting As We Know It*. BornDigital: <https://bit.ly/3cp2hj7>
- Leopold, R., & Vollmann, P. (2018). *Cryptographic assets and related transactions: accounting considerations under IFRS*. PWC.
- Leopold, R., & Vollmann, P. (2019). *Cryptographic assets and related transactions: accounting considerations under IFRS*. PWC. <https://www.pwc.com/gx/en/audit-services/ifrs/publications/ifrs-16/cryptographic-assets-related-transactions-accounting-considerations-ifrs-pwc-in-depth.pdf>
- Liquid.com. (2019). *What risks are specific to the cryptocurrency sector?* Liquid: <https://blog.liquid.com/what-are-the-risks-specific-to-cryptocurrency-sector>

- Losey, R. (2016). *Computer Assisted Review*. Electronic Discovery Best Practices: <http://www.edbp.com/search-review/computer-assisted-review/>
- Macwan, U. (2019). *The Main Risks Of Investing In Bitcoin*. Finextra: <https://www.finextra.com/blogposting/17390/the-main-risks-of-investing-in-bitcoin>
- Maddox, D. (2019). *A Forensic Accountant's Role in Litigation*. mxvaluations: <https://mxvaluations.com/2019/05/>
- Manning, G. A. (2005). *Financial Investigation and Forensic Accounting*. CRC Press.
- Manning, G. A. (2011). *Financial Investigation and Forensic Accounting* (3üncü b.). CRC Press.
- Marian, O. Y. (2013). Are Cryptocurrencies 'Super' Tax Havens? *Michigan Law Review First Impressions*, 112(38), 38-48.
- Marshall, L. (2018). *Cryptoasset: Taxonomy Report*. CryptoCompare. <https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf>
- Massad, T. G. (2019). *It's Time to Strengthen the Regulation of Crypto-Assets*. The Brookings Institution.
- McGhee, M., & Grant, S. (2019). *Audit and technology*. London: the Association of Chartered Certified Accountants (ACCA). https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/audit-and-tech/pi-audit-and-technology.pdf
- McGuire, R., & Massoud, M. (2018). *An Introduction to Accounting for Cryptocurrencies*. Chartered Professional Accountants of Canada.
- Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. *Internet measurement conference (IMC)* (ss. 127–140). Association for Computing Machinery.
- Menon, G., & P., L. (2016). Forensic Accounting: A Checkmate for Corporate Fraud. *Journal of Modern Accounting and Auditing*, 12(9), 453-460.
- Miggiani, K. (2020). *AMLD 5 and the EU May 2020 AML/CFT Action Plan – where do crypto assets fit into the emerging landscape?* Regulation-Y: https://regulation-y.com/2020/06/14/amld-5-and-the-eu-may-2020-aml-cft-action-plan-where-do-crypto-assets-fit-into-the-emerging-landscape/#_ftnref21
- Morse, J. (2018). *Shocking no one, study finds almost 80 percent of ICOs are scams*. Mashable: <https://mashable.com/2018/07/12/majority-ico-scams/#eZDWhjSulqqT>
- Möser, M. (2013). Anonymity of Bitcoin Transactions: An Analysis of Mixing Services. *Münster Bitcoin Conference (MBC)*. University of Münster.
- Mougayar, W. (2015). *Understanding the blockchain*. O'Reilly: <https://www.oreilly.com/radar/understanding-the-blockchain/>
- Musiala, R. A., Goody, T. M., Reynolds, V., Tenery, L., McGrath, M., Rowland, C., & Sekhri, S. (2020). *Cryptocurrencies: Forensic techniques to meet the challenge of new fraud and corruption risks*. AICPA and CIMA.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

- Nigrini, M. J. (2011). *Forensic Analytics Methods and Techniques for Forensic Accounting Investigations*. John Wiley & Sons, Inc.
- NLTimes. (2018). *Brit held in bitcoin laundering scheme could get 5 years in prison*. NLTimes: <https://nltimes.nl/2018/02/22/brit-held-bitcoin-laundering-scheme-get-5-years-prison>
- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), 183-187. <https://doi.org/10.1007/s12599-017-0467-3>
- Nunn, L., McGuire, B., Whitcomb, C., & Jost, E. (2006). Forensic Accountants: Financial Investigators. *Journal of Business And Economics Research*, 4(2), 1-6. <https://doi.org/10.19030/jber.v4i2.2631>
- Okoye, E. I., & Gbegi, D. O. (2013). An Evaluation of Forensic Accountants to Planning Management Fraud Risk Detection Procedures. *Global Journal of Management and Business Research*, 13(1), 74-90.
- Okoye, E. I., & Gbegi, D. O. (2013). Forensic Accounting: A Tool for Fraud Detection and Prevention in the Public Sector. (A Study of Selected Ministries in Kogi State). *International Journal of Academic Research in Business and Social Sciences*, 3(3), 1-19.
- Örten, R., Kaval, H., & Karapınar, A. (2018). *Türkiye Muhasebe Finansal Raporlama Standartları (TMS - TFRS) Uygulama ve Yorumları*. Gazi yayın evi.
- Oyedokun, G. E. (2013). An Assessment of the Role of Forensic Accountants in Litigation Support Services (An Explanatory Approach). *SSRN Electronic Journal*, 1-24. <http://dx.doi.org/10.2139/ssrn.2410664>
- Özcan, A. (2019). Analyzing the impact of forensic accounting on the detection of financial information manipulation. *MANAS Sosyal Araştırmalar Dergisi*, 8(2), 1744-1760.
- Paul, P. D. (2019). *Crypto Assets, Financial Crime & Forensic Accounting*. The Expert Witness: <https://www.expertwitnessjournal.co.uk/forensics/1085-crypto-assets-financial-crime-forensic-accounting?tmpl=component&print=1&layout=default%E2%80%A6>
- Perlman, N. B. (2020). *What is KYC and Why does it Matter for Cryptocurrency Buyers*. Gemini: <https://www.gemini.com/blog/what-is-kyc-and-why-does-it-matter>
- Piggott, D. (2014). *A Journey into Litecoin Forensic Artifacts*. SANS Institute.
- Pollock, D. (2018). *The Mess That Was Mt. Gox: Four Years On*. Cointelegraph: <https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on>
- Powazka, P. (2017). *Smart contracts are knocking on your door – it's time to answer!* The International Association for Contract & Commercial Management (IACCM): <https://journal.iaccm.com/contracting-excellence-journal/smart-contracts-are-knocking-on-your-door-its-time-to-answer>
- Price, D. (2018). *8 Cryptocurrency Risks to Consider Before Investing in Crypto*. Blocks Decoded: <https://blocksdecoded.com/cryptocurrency-investment-risks/>
- Price, R. (2015). *The 25 most exciting bitcoin startups*. Business Insider: <https://www.businessinsider.com/25-most-exciting-bitcoin-startups-in-the-world-ethereum-21-coinbase-coindesk-2015-3?op=1>

- Procházka, D. (2018). Accounting for Bitcoin and Other Cryptocurrencies under IFRS: A Comparison and Assessment of Competing Models. *The International Journal of Digital Accounting Research*, 18(24), 161-188.
- PWC. (2017). IFRS 9, Financial Instruments ; Understanding the basics. PWC. <https://www.pwc.com/gx/en/audit-services/ifrs/publications/ifrs-9/ifrs-9-understanding-the-basics.pdf>
- Quadrando, J. C., Teixeirao, C., Fronzeco, L., & Ezcudeiro, P. (2019). Futuristic Invisibility for User Identity and Data Protection. *International Research Journal of Management, IT & Social Sciences*, 6(5), 144-157.
- Quest, M. (2018). *Cryptocurrency Investing Success: Your Guide to Maximizing the Investing Potential of Bitcoin, Ethereum, Altcoins and Other Cryptocurrencies*. CreateSpace Independent Publishing Platform.
- Ramos, M. (2003). *Auditors' Responsibility for Fraud Detection. SAS no. 99 introduces a new era in auditors' requirements*. Journal of Accountancy: <https://www.journalofaccountancy.com/issues/2003/jan/auditorsresponsibilityforfrauddetection.html>
- Retief, E. (2018). Accounting for Cryptocurrency. *Professional Accountant*, (38), ss. 10-12. <https://www.saipa.co.za/wp-content/uploads/2019/04/Cryptocurrency-article.pdf>
- Reuters. (2018). *Venezuela says launch of 'petro' cryptocurrency raised \$735 million*. Reuters: <https://www.reuters.com/article/us-crypto-currencies-venezuela-idUSKCN1G506F>
- Roberts, J. J. (2018). *To Catch a Bitcoin Thief, Call These Detectives*. Fortune: <https://fortune.com/2018/06/27/bitcoin-detective-zcash-cryptocurrency/>
- Robinson, T. (2018). *5th AML Directive: EU Regulation Of Cryptocurrency Businesses*. Elliptic: <https://www.elliptic.co/our-thinking/5th-aml-directive-eu-regulation-cryptocurrency>
- Robock, Z. (2014). The Risk of Money Laundering Through Crowdfunding: A Funding Portal's Guide to Compliance and Crime Fighting. *The Michigan Business & Entrepreneurial Law Review*, 4(1), 114-129.
- Ron, D., & Shamir, A. (2019). Quantitative Analysis of the Full Bitcoin Transaction Graph. S. AR (Dü.), *Financial Cryptography and Data Security*. Springer.
- Rosenberg, M., & Popper, N. (2018). How Russian Spies Hid Behind Bitcoin in Hacking Campaign. The New York Times.
- Rouse, R. W., & Conway Jr., A. C. (2002). This Is a Job for Superman: Calling in a Forensic Accountant. *Journal of Corporate Accounting & Finance*, 13 (4), 23-28. <https://doi.org/10.1002/jcaf.10066>
- Rouse, R., & Conway Jr., A. (2001). Protecting yourself: Due diligence in mergers and acquisitions. *Journal of Corporate Accounting & Finance*, 13(2), 17-22. <https://doi.org/10.1002/jcaf.1219>
- Saada, D. (2019). *Forensic Accounting is the Key to Rescuing Users from Cryptocurrency Fraud and Computer Crimes*. The Currency Analytics: <https://thecurrencyanalytics.com/5822/forensic-accounting-is-the-key-to-rescuing-users-from-cryptocurrency-fraud-and-computer-crimes/>

- Santhana, P., & Biswas, A. (2017). *Blockchain risk management Risk functions need to play an active role in shaping blockchain strategy*. Deloitte Development LLC.
- Schulman, J., & Wilson, S. (2019). *How blockchain technology will affect the audit*. RSM US LLP: <https://rsmus.com/what-we-do/services/assurance/how-blockchain-technology-will-affect-the-audit.html>
- Segendorf, B. (2014). *What is Bitcoin?* sveriges riksbank. http://archive.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_art
- Şen, O., & Akarslan, H. (2018). Use of Blockchain Technology in the Financing of DEASH. *International Journal of Information Security Science*, 7(4), 185-197.
- Serapiglia, A., Serapiglia, C., & McIntyre, J. (2015). Cryptocurrencies: Core Information Technology and Information System Fundamentals Enabling Currency Without Borders. *Information Systems Education Journal*, 13(3), 43-52.
- Sergison, D. (2019). *Black Markets, Fraud, and Money Laundering: How Much Are Cryptocurrencies Used For Crime?* Fintechnews: <https://www.fintechnews.org/black-markets-fraud-and-money-laundering-how-much-are-cryptocurrencies-used-for-crime/>
- Sharma, R. (2019). *Should Cryptocurrency Exchanges Self-Regulate?* Investopedia: <https://www.investopedia.com/news/should-cryptocurrency-exchanges-selfregulate-themselves/>
- Sibenik, P. (2019). *Cryptocurrency Forensic Accounting: How Crypto Assets are Tracked*. Cryptforensic: <https://cryptforensic.com/2019/07/04/cryptocurrency-forensic-accounting-how-crypto-assets-are-tracked/>
- Sibenik, P. (2019). *How Anonymous Are Cryptocurrencies?* Cryptforensic Investigators: <https://cryptforensic.com/2019/01/08/how-anonymous-are-cryptocurrencies/>
- Sibenik, P. (2019). *What is Cryptocurrency Forensics?* Cryptoforensic: <https://cryptforensic.com/2019/01/22/what-is-cryptocurrency-forensics/>
- Silverstone, H., & Michael, S. (2007). *Forensic Accounting and Fraud Investigation for Non-Experts*. John Wiley & Sons, Inc.
- Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing And Forensic Accounting*. John Wiley & Sons, INC.
- Sloan, K. (2018). *4 Risks of Using Cryptocurrency*. Business 2 Community: <https://www.business2community.com/tech-gadgets/4-risks-of-using-cryptocurrency-02092258>
- Smith, C. (2018). Transactions involving commodities and cryptocurrencies. IFRS/IASB. www.ifrs.org
- SOCPA. (2018). Muhtasar Al-Ma'ayeer Al-Dualiya Liil' takrir Al-Mali [UFRS özeti]. SOCPA.
- Spagnuolo, M., Maggi, F., & Zanero, S. (2014). BitIodine: Extracting Intelligence from the Bitcoin Network. *Financial Cryptography and Data Security*, ss. 457-468.
- Sprenger, P., & Balsiger, F. (2018). *Anti-Money Laundering in Times Of Cryptocurrencies*. KPMG.ch.

- Stark, J. (2016). *Making Sense of Blockchain Smart Contracts*. Coindesk: <https://www.coindesk.com/making-sense-smart-contracts>
- Stornetta, W. S., & Haber, S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3, 99-111. <https://doi.org/10.1007/BF00196791>
- Surane, J. (2016). *Visa Asks Banks to Participate in Blockchain Pilot for Transfers*. Bloomberg: <https://bloom.bg/31LSCPs>
- Szabo, N. (1994). *Smart Contracts*. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- Taki, A., & Todd, P. (2014). Hiding currency in the Dark Wallet. (J. Copestake, Rōportaj Yapan) BBC.
- The Association of Certified Accountants (ACCA). (2010). *Forensic Accounting*. AccAGlobal: <http://www.accaglobal.com/za/en/student/exam-supportresources/professional-exams-study-resources/p7/technical-articles/forensicaccounting0.html>
- The Center for Audit Quality. (2010). *Deterring and Detecting Financial Reporting Fraud: A Platform for Action*.
- The Deloitte Center for Financial Services. (2017). *Blockchain in commercial real estate*. Deloitte Development LLC. <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/real-estate/real-estate-blockchain-game-changer-immobilienwirtschaft.pdf>
- The European Union Agency for Cybersecurity-ENISA. (2016). *Distributed Ledger Technology*. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/blockchain-security/at_download/fullReport
- Trezor. (2020). *Trezor*. Trezor: <https://trezor.io/>
- Trimborn, S., Li, M., & Härdle, W. K. (2017). Investing with cryptocurrencies - A liquidity constrained investment approach. *SFB 649:ECONOMIC RISK*.
- Underhill, J. (2018). *Initial coin offerings*. Fraud Magazine: <https://www.fraud-magazine.com/article.aspx?id=4295000887&Site=ACFEWEB>
- Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, 59(11), 15-17. <https://doi.org/10.1145/2994581>
- Vaidyanathan, N. (2017). *Divided we fall, distributed we stand*. The Association of Chartered Certified Accountants (ACCA). <https://www.accaglobal.com/gb/en/technical-activities/technical-resources-search/2017/april/divided-we-fall-distributed-we-stand.html>
- Venter, H. (2018). Digital currency – A case for standard setting activity. *EEG Meeting, May 2018, Agenda Paper 2D*, (ss. 1-25). The Australian Accounting Standards Board (AASB).
- Wegberg, R. v., Oerlemans, J.-J., & Deventer, O. v. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419-435. <https://doi.org/10.1108/JFC-11-2016-0067>

- Wijayaa, D. A., & Suwarsonob, D. A. (2018). Cryptaxforensic, when cryptocurrency, taxation, and digital forensic collide: an overview of Indonesian cryptocurrency market. *arXiv, arXiv-1811*.
- Yatsyk, T. (2018). Methodology Of Financial Accounting Of Cryptocurrencies According To The IFRS. *European Journal of Economics And Management*, 4(6), 53-60.
- Yerak, B. (2015). 'Suspicious' crowdfunding activity on the rise, U.S. watchdog says. Chicago Tribune: <https://www.chicagotribune.com/business/ct-crowdfunding-fincen-sars-1015-biz-20151015-story.html>
- Young Entrepreneur Council (YEC). (2018). *4 Important Cryptocurrency Facts Business Owners Should Be Aware Of*. Forbes: <https://www.forbes.com/sites/theyec/2018/05/24/4-important-cryptocurrency-facts-business-owners-should-be-aware-of/?sh=68f45a724e1c>
- Yousaf, H., Kappos, G., & Meiklejohn, S. (2019). Tracing Transactions Across Cryptocurrency Ledgers. *28th USENIX Security Symposium* (ss. 837-850). Usenix Association.