



T.C.
İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

ULUSLARARASI GÜVENLİK VE TERÖRİZM ANA BİLİM DALI

KRİPTO VARLIKLARIN TERÖRİZMİN FİNANSMANINDA KULLANILMASI
VE MALİ EYLEM GÖREV GÜCÜ (FATF) TAVSİYELERİ

HAZIRLAYAN
MERVE AYBÜKE TEKGÜL LEVENT

YÜKSEK LİSANS TEZİ

ŞUBAT 2024



1904

T.C.
İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

KRİPTO VARLIKLARIN TERÖRİZMİN FİNANSMANINDA
KULLANILMASI VE MALİ EYLEM GÖREV GÜCÜ (FATF)
TAVSİYELERİ

YÜKSEK LİSANS TEZİ
ULUSLARARASI GÜVENLİK VE TERÖRİZM ANA BİLİM DALI

HAZIRLAYAN
Merve Aybüke TEKGÜL LEVENT

TEZ DANIŞMANI
J.Alb. Dr. Öğr. Üyesi Bürke Uğur BAŞARANEL

ANKARA-2024
“Her Hakkı Saklıdır”

Merve Ayb ke TEKG L LEVENT tarafından hazırlanan ‘‘KRİPTO VARLIKLARIN TER RİZMİN FİNANSMANINDA KULLANILMASI VE MALİ EYLEM G REV G C  (FATF) TAVSİYELE ’’ adlı tez  alışması aŗağıdaki j ri tarafından OY BİRLİĞİ ile Jandarma ve Sahil G venlik Akademisi G venlik Bilimleri Enstit s  Uluslararası G venlik ve Ter rizm Ana Bilim Dalında Y KSEK LİSANS TEZİ olarak kabul edilmiŗtir.

Danışman: J.Alb. Dr.  ğr.  yesi B rke Uğur BAŞARANEL

Jandarma ve Sahil G venlik Akademisi

Bu tezin, kapsam ve kalite olarak Y ksek Lisans Tezi olduėunu onaylıyorum.

Başkan: J. Alb. Dr. Tarık AK

Jandarma ve Sahil G venlik Akademisi

Bu tezin, kapsam ve kalite olarak Y ksek Lisans Tezi olduėunu onaylıyorum.

 ye: Dr. Mehmet Onur YURDAKUL

Mali Su ları Araŗtırma Kurulu Başkanlığı

Bu tezin, kapsam ve kalite olarak Y ksek Lisans Tezi olduėunu onaylıyorum.

Tez Savunma Tarihi: 07/02/2024

J ri tarafından kabul edilen bu tezin Y ksek Lisans Tezi olması i in gerekli řartları yerine getirdiėini onaylıyorum.

Do .Dr. Naci AKDEMİR

J.Alb.

Enstit  M d r 

ETİK BEYAN

Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Merve Aybüke TEKGÜL LEVENT

07/02/2024

T.C.
İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

KRİPTO VARLIKLARIN TERÖRİZMİN FİNANSMANINDA KULLANILMASI VE
MALİ EYLEM GÖREV GÜCÜ (FATF) TAVSİYELERİ
(Yüksek Lisans Tezi)

Merve Aybüke TEKGÜL LEVENT

Şubat 2024

ÖZET

Finansal teknolojideki gelişmelerin bir yansıması olarak ortaya çıkan kripto varlıklar, terörizmin finansmanına yeni bir boyut kazandırmış olup terörizmin finansmanı ile mücadelede artan bir endişe kaynağı haline gelmiştir. Kripto varlıkların terörizmin finansmanı ile mücadele kapsamında oluşturduğu risklerin anlaşılması, etkili önlemlerin alınabilmesi için büyük öneme sahiptir. Bu kapsamda tez, kripto varlıkların terörizmin finansmanında hangi faktörlerden etkilenerek, hangi yöntemlerle kullanılabileceğinin ve ne derecede kullanıldığının ortaya konulması ile konu bağlamında ilgili Mali Eylem Görev Gücü (Financial Action Task Force-FATF) tavsiyelerinin incelenmesini amaçlamaktadır. Nitel araştırmaya dayanan tezde, doküman incelemesi yöntemiyle çeşitli birincil ve ikincil kaynaklardan veri toplanmış olup toplanan veriler içerik analizi yöntemiyle çözümlenmiştir. Tezin kapsamı, kripto varlıkların terörizmin finansmanında kullanılma potansiyeli, açık kaynaklara yansıyan birtakım kullanım örnekleri ve konuyla daha ilgili olduğu değerlendirilen FATF tavsiyelerinin bu bağlamda incelenmesidir. Teknik detayların ele alınması, terörizmin finansman faaliyetlerinin çoğunlukla gizlilik içinde yürütülmesi ve kripto varlıkların hukuki durumu ve düzenlemeleriyle ilgili küresel bir uyumun henüz sağlanmamış olması gibi konular sebebiyle tezin bazı sınırlılıkları da mevcuttur. Kripto varlıkların ortaya çıkışı ve gelişiminin incelendiği tezin birinci bölümünde; para kavramı ve tarihi, kripto varlıkların dayandığı blokzinciri teknolojisi, kripto varlıklara getirilen tanımlar, kripto varlıkların teknik altyapısı, kripto varlık ekosistemindeki aktörler ve kripto varlık türlerine yer verilmiştir. Kripto varlıkların terörizmin finansmanında kullanımının incelendiği tezin ikinci bölümünde; terör ve terörizm kavramları, terörizmin finansmanı ve aşamaları, kripto varlıkların terörizmin finansmanında kullanılmasını etkileyen faktörler, kripto varlıkların terörizmin finansmanında potansiyel kullanım yöntemleri ve kripto varlıkların terörizmin finansmanında kullanım örneklerine yer verilmiştir. Tezin üçüncü ve son bölümünde; FATF'in tarihçesi, çalışma alanları, kripto varlıklar konusunda yayınladığı raporlar ile rehberlere yer verilmiş ve FATF tavsiyeleri kripto varlıklar bağlamında incelenmiştir. Tezin sonuç bölümünde ise kripto varlıkların terörizmin finansmanında kullanılması potansiyeli ile genel eğilimlere ve FATF'in düzenleme çabalarına ilişkin birtakım değerlendirmeler gerçekleştirilmiştir.

Bilim Kodu : 114111

Anahtar Kelimeler : Kripto Varlıklar, Terörizmin Finansmanı, Mali Eylem Görev Gücü (FATF) Tavsiyeleri

Sayfa Adedi : 197

Tez Danışmanı : J.Alb. Dr. Öğr. Üyesi Bürke Uğur BAŞARANEL

T.R.
MINISTRY OF INTERIOR
GENDARMERIE AND COAST GUARD ACADEMY
SECURITY SCIENCES INSTITUTE

USE OF CRYPTO ASSETS IN THE FINANCING OF TERRORISM AND FINANCIAL
ACTION TASK FORCE (FATF) RECOMMENDATIONS
(M.Sc. Thesis)

Merve Aybüke TEKGÜL LEVENT

February 2024

ABSTRACT

Emerging as a reflection of developments in financial technology, crypto assets have added a new dimension to the financing of terrorism and have become an increasing source of concern in the fight against the financing of terrorism. Understanding the risks posed by crypto assets within the scope of combating the financing of terrorism is of great importance in order to take effective measures. In this context, the thesis aims to reveal the factors affecting use of crypto assets in the financing of terrorism, the methods by which they can be used and to what extent they are used, and to examine the relevant Financial Action Task Force (FATF) Recommendations in the context of the subject. In the thesis based on qualitative research, data was collected from various primary and secondary sources by document review method and the collected data was analyzed by content analysis method. The scope of the thesis is to examine the potential of crypto assets to be used in financing terrorism, some usage examples reflected in open sources, and FATF Recommendations, which are considered to be more relevant to the subject, in this context. The thesis has some limitations due to issues such as the handling of technical details, the fact that terrorism financing activities are mostly carried out in secrecy, and the fact that global compliance regarding the legal status and regulations of crypto assets has not yet been achieved. In the first part of the thesis, which the emergence and development of crypto assets is examined; the concept and history of money, the blockchain technology on which crypto assets are based, the definitions of crypto assets, the technical infrastructure of crypto assets, the actors in the crypto asset ecosystem and the types of crypto assets are included. In the second part of the thesis, which examines the use of crypto assets in terrorism financing; concepts of terror and terrorism, the financing of terrorism and its stages, factors influencing the use of crypto assets in terrorism financing, potential methods of using crypto assets in terrorism financing, and examples of the use of crypto assets in terrorism financing are included. In the third and last part of the thesis; FATF's history, areas of work, reports and guides published on crypto assets are included, and FATF Recommendations are examined in the context of crypto assets. In the conclusion part of the thesis, some evaluations were made regarding the potential of crypto assets to be used in financing terrorism, general trends and FATF's regulatory efforts.

Science Code : 114111

Keywords : Crypto Assets, Financing of Terrorism, Financial Action Task Force
(FATF) Recommendations

Page Number : 197

Supervisor : Gen. Col. Assist. Prof. Bürke Uğur BAŞARANEL

TEŞEKKÜR

Çalışmalarım boyunca değerli katkılarıyla beni yönlendiren ve kıymetli tecrübeleri ile çalışmalarından faydalandığım danışmanım J.Alb. Dr. Öğr. Üyesi Bürke Uğur BAŞARANEL'e, bilgi birikiminden istifade ettiğim ve önemli yardımlarıyla bana yol gösteren jüri üyesi üstadım Dr. Mehmet Onur YURDAKUL'a, çalışmanın geliştirilmesi için katkılarından dolayı jüri üyesi J. Alb. Dr. Tarık AK'a, fikirleri ile ufkumu genişleten üstadım Fatih EMECAN'a, bu çalışmanın gerçek mimarı olan çok değerli eşim Burak LEVENT'e, tüm desteğiyle beni hiçbir zaman yalnız bırakmayan aileme ve arkadaşlarıma teşekkür ve saygılarımı bir borç bilirim. Ayrıca bana bu imkânı sağlayan Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü'ne şükranlarımı sunarım.

İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ŞEKİLLERİN LİSTESİ.....	x
SİMGELER VE KISALTMALAR	xi
GİRİŞ	1

BİRİNCİ BÖLÜM

KRİPTO VARLIKLARIN ORTAYA ÇIKIŞI VE GELİŞİMİ

1.1.	Para Kavramı	13
1.1.1.	Para Nedir?.....	13
1.1.2.	Paranın Özellikleri ve Fonksiyonları	14
1.1.3.	Paranın Tarihi ve Para Sistemleri.....	15
1.1.3.1.	Mal (Meta) para	15
1.1.3.2.	Madeni para	15
1.1.3.3.	Temsili para	16
1.1.3.4.	İtibari para	18
1.1.3.5.	Kaydi para	18
1.1.3.6.	Dijital para	19
1.1.3.7.	Elektronik para.....	21
1.1.3.8.	Sanal para.....	23
1.2.	Blokzinciri Teknolojisi	27
1.3.	Kripto Varlık Kavramı	35
1.3.1.	Getirilen Tanımlar.....	35
1.3.2.	Ortaya Çıkış Süreci ve Benimsenmesi.....	37
1.3.3.	Teknik Unsurları	40
1.3.4.	Kripto Varlık Ekosistemindeki Aktörler.....	42
1.3.4.1.	Kripto varlık kullanıcıları.....	42
1.3.4.2.	Madenciler	42
1.3.4.3.	Kripto varlık hizmet sağlayıcıları	43
1.3.4.4.	Kripto varlık yaratıcıları.....	45
1.3.4.5.	Kripto varlık arz edenler (ihraççıları)	45
1.3.5.	Kripto Varlık Türleri.....	45
1.3.5.1.	Coin kavramı ve türleri	48
1.3.5.1.1.	Bitcoin.....	49
1.3.5.1.2.	Ethereum	52

Sayfa

1.3.5.1.3.	Ripple	54
1.3.5.1.4.	Litecoin	55
1.3.5.1.5.	Gizlilik tabanlı kripto varlıklar (Privacy Coins)	56
1.3.5.2.	Token kavramı ve türleri.....	60
1.3.5.2.1.	Ödeme Token (Payment Token).....	61
1.3.5.2.2.	Fayda Token (Utility Token)	63
1.3.5.2.3.	Menkul Kıymet Token (Security Token).....	64
1.3.5.2.4.	Nitelikli Fikrî Tapu (Non-Fungible Token-NFT)	65
1.4.	Birinci Bölüme İlişkin Değerlendirme.....	66

İKİNCİ BÖLÜM**KRİPTO VARLIKLARIN TERÖRİZMİN FİNANSMANINDA KULLANILMASI**

2.1.	Terör ve Terörizm	69
2.1.1.	Terör Kavramı.....	69
2.1.2.	Terörizm Kavramı.....	70
2.2.	Terörizmin Finansmanı	72
2.2.1.	Terörizmin Finansmanı Kavramı	72
2.2.2.	Terörizmin Finansman Aşamaları.....	75
2.2.2.1.	Toplama	75
2.2.2.2.	Aktarma.....	77
2.2.2.3.	Depolama	77
2.2.3.	Terörizmin Finansmanı ve İnternet.....	78
2.3.	Terörizmin Finansmanı Amacıyla Kripto Varlıkların Kullanılması.....	80
2.3.1.	Kripto Varlıkların Terörizmin Finansmanında Kullanılmasını Etkileyen Faktörler	81
2.3.1.1.	Kolaylaştıran faktörler	81
2.3.1.1.1.	Anonimlik	83
2.3.1.1.2.	Merkeziyetsiz yapı	85
2.3.1.1.3.	Küresel erişim ile sınır ötesi ve hızlı transfer mekanizması	86
2.3.1.1.4.	Düzenleme eksiklikleri	87
2.3.1.2.	Zorlaştıran faktörler	88
2.3.1.2.1.	Örgütsel öğrenim ve kontrol sorunları	90
2.3.1.2.2.	Teknik altyapı eksikliği.....	91
2.3.1.2.3.	Likide dönüştürülemezlik	92
2.3.1.2.4.	Değer oynaklığı.....	93
2.3.2.	Kripto Varlıkların Terörizmin Finansmanında Potansiyel Kullanım Yöntemleri	94
2.3.2.1.	Bağışlar	94
2.3.2.2.	Dark Web içerisinde suç geliri ve malzeme temini	96
2.3.2.3.	Suç gelirlerinin aklanması.....	98
2.3.2.4.	Nitelikli Fikrî Tapu (Non-Fungible Token-NFT)	100
2.3.2.5.	Merkezi olmayan finans (Decentralized Finance-DeFi).....	101
2.3.2.6.	Madencilik (Mining)	102
2.3.2.7.	Kripto varlıkların ilk arzı (Initial Coin Offering-ICO)	103
2.3.2.8.	Karıştırıcı (Mixer) hizmetleri.....	104
2.3.2.9.	Gizlilik tabanlı kripto varlıklar (Privacy Coins)	105

Sayfa

2.3.3.	Kripto Varlıkların Terörizmin Finansmanında Kullanım Örnekleri.....	107
2.4.	İkinci Bölüme İlişkin Değerlendirme	119

ÜÇÜNCÜ BÖLÜM

KRİPTO VARLIKLAR VE MALİ EYLEM GÖREV GÜCÜ (FINANCIAL ACTION TASK FORCE-FATF) TAVSİYELERİ

3.1.	Mali Eylem Görev Gücü'nün Tarihçesi.....	121
3.2.	Mali Eylem Görev Gücü'nün Çalışma Alanları	123
3.2.1.	Yöntem ve Trendlerin Belirlenmesi.....	124
3.2.2.	FATF Tavsiyeleri.....	124
3.2.3.	Karşılıklı Değerlendirme Raporları	125
3.2.4.	Yüksek Riskli ve Artırılmış İzlemeye Tabi Ülkelerin Belirlenmesi.....	126
3.3.	Mali Eylem Görev Gücü'nün Kripto Varlıklar Alanında Yaptığı Yayınlar ...	127
3.4.	FATF Tavsiyelerinin Kripto Varlıklar Bağlamında İncelenmesi	132
3.4.1.	FATF'in 1 Nolu Tavsiyesi	133
3.4.2.	FATF'in 2 Nolu Tavsiyesi	135
3.4.3.	FATF'in 3-8 Nolu Tavsiyeleri	136
3.4.4.	FATF'in 10 ve 11 Nolu Tavsiyeleri.....	138
3.4.5.	FATF'in 15 Nolu Tavsiyesi	140
3.4.6.	FATF'in 16 Nolu Tavsiyesi	143
3.4.7.	FATF'in 19-21 Nolu Tavsiyeleri	145
3.4.8.	FATF'in 24 ve 25 Nolu Tavsiyeleri.....	147
3.4.9.	FATF'in 26 ve 27 Nolu Tavsiyeleri.....	148
3.4.10.	FATF'in 29-31 Nolu Tavsiyeleri	149
3.4.11.	FATF'in 34 ve 35 Nolu Tavsiyeleri.....	151
3.4.12.	FATF'in 37-40 Nolu Tavsiyeleri	152
3.5.	Üçüncü Bölüme İlişkin Değerlendirme	154
SONUÇ VE ÖNERİLER.....		159
KAYNAKÇA.....		167

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 1.1. Dijital Para Kategorileri.....	20
Şekil 1.2. Sanal Paranın Sınıflandırılması	26
Şekil 2.1. Örnek Olay Görsel Analizi	109



SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler

Açıklama

%

Yüzde

Kısaltmalar

Açıklama

AB

Avrupa Birliği

ABD

Amerika Birleşik Devleti

ATM

Automated Teller Machine, Otomatik Vezne Makinesi

BIS

Bank for International Settlements, Uluslararası Ödemeler Bankası

BTC

Bitcoin

BUSD

Binance USD

CBDC

Central Bank Digital Currency, Merkez Bankası Dijital Parası

CEX

Centralized Exchange, Merkezi Borsa

DAO

Decentralized Autonomous Organizations, Merkeziyetsiz Otonom Kuruluşlar

DApps

Decentralized Applications, Merkezi Olmayan Uygulamalar

DEAŞ

Irak Şam İslam Devleti

DeFi

Decentralized Finance, Merkezi Olmayan Finans

DEX

Decentralized Exchange, Merkezi Olmayan Borsa

DLT

Distributed Ledger Technology, Dağıtık Defter Teknolojisi

EBA

European Banking Authority, Avrupa Bankacılık Otoritesi

ECB

European Central Bank, Avrupa Merkez Bankası

ETH

Ether

FATF

Financial Action Task Force, Mali Eylem Görev Gücü

FOBİM

Finansal Olmayan Belirli İş ve Meslekler

FSRB

FATF Style Regional Bodies, FATF Benzeri Bölgesel Kuruluş

HTŞ

Heyet Tahrir el-Şam

ICO

Initial Coin Offering, Kripto Varlıkların İlk Arzı

Kısaltmalar	Açıklama
IMF	<i>International Monetary Fund</i> , Uluslararası Para Fonu
IoT	<i>Internet of Things</i> , Nesnelerin İnterneti
IP	<i>Internet Protocol</i> , İnternet Protokol
LTC	Litecoin
MB	Megabyte
MASAK	Mali Suçları Araştırma Kurulu
MiCA	<i>Markets in Crypto Assets</i> , Kripto Varlık Piyasaları
NFT	<i>Non-Fungible Token</i> , Nitelikli Fikrî Tapu
OECD	<i>Organisation for Economic Co-operation and Development</i> , İktisadi İşbirliği ve Gelişme Teşkilatı
OFAC	<i>Office of Foreign Assets Control</i> , Yabancı Varlıkları Kontrol Ofisi
P2P	<i>Peer to peer</i> , Eşler Arası
PoS	<i>Proof of Stake</i> , Pay İspatı
PoW	<i>Proof of Work</i> , İş İspatı
QR	<i>Quick Response</i> , Hızlı Cevap/Karekod
RingCT	<i>Ring Confidential Transactions</i> , Halka Gizli İşlemler
SEC	<i>Securities and Exchange Commission</i> , Menkul Kıymetler ve Borsa Komisyonu
SHA-256	<i>Secure Hash Algorithm 256-bit</i> , Güvenli Hash Algoritması 256-bit
TracFin	<i>Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins</i> , Yasadışı Mali Hareketlere Karşı Eylem ve Bilgi İşlem Kuruluşu
URD	Ulusal Risk Değerlendirmesi
USD	<i>United States Dollar</i> , Amerikan Doları
USDC	USD Coin
USDT	USD Tether
XMR	Monero
XRP	Ripple

GİRİŞ

Hayatın hemen her alanında büyük dönüşümlere yol açan teknolojik gelişmeler, insan davranışının bir parçası olarak yasa dışı faaliyetleri de etkilemiş ve hız ile anonimlik gibi getirileri sayesinde çeşitli yasa dışı faaliyetlerin araç ve yöntemlerinde değişikliklere yol açmıştır (Dyntu ve Dykyj, 2021, s. 67). Teknoloji, terör örgütlerinin de sosyal medya kullanımından, şifreli internet protokolleri aracılığıyla iletişimine kadar pek çok faaliyetinde önemli bir unsur haline gelmiştir (İbrahim, 2019, s. 2). Finansal teknolojideki gelişmelerin bir yansıması olarak ortaya çıkan kripto varlıklar, terör örgütlerinin finansman faaliyetlerine yeni bir boyut kazandırmıştır.

Kripto varlıkların ilk ve en bilinen örneğinin, Satoshi Nakamoto lakaplı kişi veya kişilerce 2009 yılında kamuya yönelik açık kaynaklı bir yazılım olarak piyasaya sürülen Bitcoin olduğunu söylemek mümkündür (Majumder vd., 2019, s. 126). Aynı zamanda bir kripto para birimi olan Bitcoin'e uzanan süreç, tarihteki para kavramının evrimini yansıtan önemli bir dönemeçtir. Teknolojinin ilerlemesi ve dijitalleşme, paranın fiziksel formunun yanı sıra soyut bir form da kazanmasına ve dijital ödeme sistemleriyle birlikte dijital para birimlerinin ortaya çıkmasına yol açmıştır. Tarafların fiziksel varlığına veya paranın fiziki formuna ihtiyaç duyulmayan dijital ödeme sistemlerindeki maliyet ve güvenlik endişeleri nedeniyle ise merkezi olmayan ve eşler arası elektronik transferlere imkân tanıyan kripto para birimleri ortaya çıkmıştır (Majumder vd., 2019, s. 126). Paranın dijitalleşmesi ve buna bağlı olarak getirilen kontroller, terör örgütleri için gizlilik içerisinde işlem yapmayı zorlaştırırken, kripto paraların ortaya çıkışı, terör örgütlerinin terörizmin finansmanı ve suç gelirlerini aklama faaliyetlerinde yeni girişimlerin yolunu açmıştır (İbrahim, 2019, s. 2). Sürekli olarak değişen paranın tarihine ilişkin olarak değişmeyen tek gerçek ise, her dönüşümün yeni bir suistimal kaynağı olmasıdır (Galbraith, 2017, s. 30). Başka bir deyişle, para ve ödeme sistemleriyle ilgili her gelişme, yasa dışı amaçlarla hareket eden aktörlerin kötüye kullanımları için yeni olanaklar da sağlamaktadır.

Kripto para birimlerini içine alan kripto varlıklar özellikleriyle tanımlanmaktadır; kriptografi ile dağıtık defter teknolojisine (*Distributed Ledger Technology*-DLT) dayanan ve dijital şekilde oluşturularak işlem gören bir dijital varlık sınıfıdır (ECB, 2019, s. 3; Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, 2021). Merkezi bir otoriteye olan güven ihtiyacını ortadan kaldırarak temelde merkeziyetsiz bir yapıda işlem

gören kripto varlıklarda güven, blokzinciri gibi bir dağıtık defter teknolojisine ve kriptografiye dayalı olarak sağlanmaktadır. Kripto varlıkların teknik altyapısı sayesinde, merkezi bir gözetim ve kontrol mekanizması olmadan, kripto varlıkların bulunduğu ağa erişimi olan ve ağ üzerinde gerçek kimlikleri yerine alfanümerik karakterlerle temsil edilen dünya çapındaki taraflar arasında doğrudan işlemler gerçekleşmesi mümkün olmaktadır. Bu sayede kripto varlıklar, finansal sistemi çeşitlendirmek, yenilikçiliği teşvik etmek ve erişilebilirliği artırmak gibi önemli potansiyellere sahip olmakla birlikte, kripto varlıkların doğasından kaynaklanan özellikleri, terörizmin finansmanı gibi yasa dışı faaliyetlerde kullanılması için yeni fırsatlar da yaratmaktadır (FATF, 2020a, s. 3).

Düzenlenmiş finansal sistem dışında edinilebilen, aktarılabilen ve saklanabilen kripto varlıklar terör örgütlerine, küresel şekilde hızlı işlem yapma ile fonların kaynağının ve varış noktasının gizlenmesi konusunda birçok imkân sunmaktadır (FATF, 2020a, s. 3). Kripto varlıklar terör örgütlerinin yanı sıra, terör örgütlerine finansman sağlayan kişi ve gruplara da merkezi otoritelerin tespit ve müdahalesinden kaçınmalarında yeni olanaklar sağlamaktadır (Eisermann, 2020, s. 4). Kripto varlıkların kullanımı, ulusal ve uluslararası terörizmin finansmanı ile mücadele düzenlemeleri tarafından görece daha az kısıtlanabilecek, fonların daha hızlı, anonim ve küresel ölçekte edinilmesi ve aktarılmasına yönelik yeni bir yöntemi temsil etmektedir (Silfversten vd., 2020, s. VII).

Henüz geniş kitlelerce yaygın şekilde kullanılmayan kripto varlıkların, yasa dışı aktörler tarafından, yasa dışı faaliyetlerde kullanımı giderek daha fazla yaygınlaşmıştır. Kripto varlıkların yasa dışı amaçlarla kullanım örneklerinin en fazla, yasa dışı öğelerin kaçakçılığı ve dolandırıcılık suçlarıyla ilgili olduğu görülmektedir. Kripto varlıkların suç gelirlerinin aklanması ve ilgili öncül suçlar kapsamında kullanımı daha yaygın olmakla birlikte, terör örgütleri tarafından finansman faaliyetlerinde kullanılması da son derece dikkat çekicidir (FATF, 2020a, ss. 4-5). Genellikle zayıf yasal ve mali düzenleme rejimlerine sahip ülkelerle ilişkilendirilen terörizmin finansmanı riski, kripto varlıkların bir ödeme yöntemi olarak sunmuş olduğu yenilik ve teknolojik karmaşıklık nedeniyle artmıştır (Salami, 2017, s. 2).

İhtiyaçlarına cevap verdiği ve avantaj oluşturduğu sürece imkân ve yetenekleri dahilinde yeni teknolojilere adaptasyon eğilimi olduğu söylenebilen terör örgütlerinin kripto varlıklara olan ilgi seviyesi son yıllarda yükselmiştir (Dyntu ve Dykyj, 2021, s. 68). Son

kanıtlar, terör örgütlerinin ve finansal destekçilerinin, kripto varlıklara dayalı teknolojilere giderek daha fazla aşına hale geldiklerini ve kripto varlıkları terörizmin finansmanında artan bir şekilde kullanma eğiliminde olduklarını göstermektedir (Eisermann, 2020, s. 4). Kripto varlıklar, terörizmin finansmanında kullanılması bağlamında elverişli özelliklere sahiptir (Teichmann, 2018, s. 519) ve terör örgütlerinin fon sağlamasında, aktarmasında, saklamasında uygun bir araç veya yöntem olarak kullanılabilir. Yapılan araştırmalar, kripto varlıkların terör örgütleri tarafından özellikle fon toplama faaliyetlerinde kullanıldığını; ancak geleneksel finansal araçlarla kıyaslandığında kripto varlıkların terörizmin finansmanı bağlamında kullanımının varsayıldığı kadar yaygın olmadığını göstermektedir (Silfversten vd., 2020, s. VII).

Geleneksel yöntemlerin halihazırda terör örgütlerinin ihtiyaçlarını etkin şekilde karşılamasının, teknolojinin değerinin farkında olmalarına rağmen terör örgütlerinin kripto varlıkları finansman faaliyetlerinde tam anlamıyla kullanmamalarına sebep olduğu söylenebilmektedir (Kfir, 2020, s. 118). Terörizmin finansmanının geleneksel araç ve yöntemlerinin henüz ölümcül bir darbe almadığından dolayı terör örgütlerinin çeşitli finansal ihtiyaçları bağlamında halen etkin bir şekilde çalışması, kripto varlıkların terör örgütleri tarafından kullanımının sınırlı olmasına yol açmaktadır. Mevcut kanıtlar, terör örgütlerinin kripto varlıklara önemli ölçüde bağımlı olmadığını, kripto varlıkların terörizmin finansmanında kullanımının henüz erken bir aşamada olduğunu göstermektedir (Wang ve Zhu, 2021, s. 2337). Bununla birlikte, kripto varlıkların terörizmin finansmanında giderek artan bir şekilde kullanılmaya devam ettiği, konu hakkında yapılan araştırmaların da incelenmesiyle açıkça görülmektedir.

Salami (2017, ss. 1-39) yapmış olduğu “*Terrorism Financing With Virtual Currencies- Can Regulatory Technology Solutions Combat This? (Sanal Para Birimleriyle Terörizmin Finansmanı-Düzenleyici Teknoloji Çözümleri Bununla Mücadele Edebilir Mi?)*” adlı çalışmada, Mali Eylem Görev Gücü (*Financial Action Task Force-FATF*)’ne benzer şekilde kripto para birimlerini merkezi olmayan sanal para birimleri olarak ele almış ve sanal para birimlerinin terörizmin finansmanı ile ilişkisi üzerine genel bir inceleme sunmuştur. Salami, sanal para birimlerinin özelliklerini inceleyerek terörizmin finansmanı için uygun bir araç olduğunu değerlendirmiş ve FATF’in risk temelli yaklaşımının sanal para birimlerine uygulanması ile bu yaklaşımın sınırlamalarını incelemiştir. Ancak Salami’nin,

birçok ilgili FATF tavsiyesini bu kapsamda incelememişti ve sanal para birimlerinin terörizm finansmanında nasıl kullanıldığına dair yeterli örnek sunmadığı görülmektedir.

Hasbi ve Mahzam (2018, ss. 1-3) yapmış oldukları “*Cryptocurrencies: Potential For Terror Financing (Kripto Para Birimleri: Terörün Finansmanı Potansiyeli)*” adlı çalışmada, kripto para birimlerinin terörizmin finansmanında kullanım potansiyelini ideolojik ve pratik açıdan incelemiştir. Yazarlar, terörizmin finansmanında kripto paraların rolüne dair çeşitli vakalar sunarak ve terör örgütleri tarafından finansman faaliyetlerinde ideolojik nedenlerle de kripto para birimi kullanımının tercih edilebileceğini değerlendirerek literatüre katkı sağlamıştır. Ancak çalışmada, kripto para birimlerinin terörizmin finansmanında kullanılmasının önlenmesine yönelik mevcut düzenlemelere değinilmediği ve terör örgütleri tarafından kripto para birimlerinin hangi yöntemlerle kullanıldığının veya kullanılabileceğinin incelenmediği görülmektedir.

Keatinge vd. (2018, ss. 1-87) tarafından yapılan “*Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses (Sanal Para Birimleri ve Terörizmin Finansmanı: Risklerin ve Yanıtların Değerlendirilmesi)*” adlı çalışmada; kripto para birimleri, sanal para birimleri içerisinde değerlendirilmiş ve sanal para birimlerinin terörizmin finansmanı bağlamında oluşturduğu riskler incelenmiştir. Çalışmada, sanal para birimlerinin mevcut ve gelecekteki muhtemel risklerinin değerlendirilmesi amacıyla özellikleri ve terörizmin finansmanında kullanım örnekleri detaylandırılmış ve konu kapsamında düzenleyici otoritelerin almış olduğu önlemlerin etkinliği tartışılmıştır. Pek çok açıdan oldukça kapsamlı bir bakış açısı sunan çalışma yalnızca sanal para birimleri ile sınırlı tutulduğundan, para birimi olarak nitelendirilmeyen Nitelikli Fikrî Tapu (*Non-Fungible Token-NFT*) gibi kripto varlıklara ilişkin herhangi bir inceleme sunulmadığı görülmektedir.

Whyte (2019, ss. 1-24) yayınlamış olduğu “*Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise (Kriptoterörizm: Terörist Girişimler İçin Blokzinciri Teknolojilerinin Faydasının Değerlendirilmesi)*” adlı makalesinde, kripto para birimlerini dijital para birimlerinin bir alt kümesi olarak değerlendirmiş ve kripto para birimlerinin çeşitli benzersiz özelliklerinin, özellikle suç gelirlerini aklama ve gelir elde etme konusunda terör örgütlerine birçok fırsat sağladığını belirtmiştir. Yazar, terör örgütlerinin fon toplama, aktarma ve malzeme temininde kripto para birimlerini kullandığına ilişkin kanıtları da inceleyerek son yıllarda kullanım örneklerinin artmış olduğunu

değerlendirmiştir. Yazar, konu hakkındaki literatür eksikliğine dikkat çekerek ve teknik detayları ele alarak ayrıntılı bir analiz sunmuş olup kripto para birimlerinin terörizmin finansmanı risklerine yönelik ulusal veya uluslararası düzenlemeler konusunda herhangi bir tartışma yürütmemiştir.

Majumder vd. (2019, ss. 125-138) tarafından yazılan “*A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing (Kripto Para Ekonomisinin Ortaya Çıkışı ve Terörizmin Finansmanı ile Bağlantısı Üzerine Kavramsal Bir Çalışma)*” adlı makalede, dünya genelinde popüler hale gelen kripto para birimlerinin, tutarlı düzenlemelerden yoksun ve alternatif bir sanal ekonomi oluşturduğuna dikkat çekilerek terörizmin finansmanı bağlamında kullanılma potansiyeli incelenmiştir. Yazarlar, Bitcoin’in teknik mekanizmasını inceleyerek anonimlik, gizlilik, merkezi gözetleme eksikliği gibi özellikleri sayesinde kripto para birimlerinin potansiyel bir terörizmin finansmanı aracı olduğunu değerlendirmiştir. Makalede yalnızca Bitcoin özelinde inceleme yapılarak genel olarak kripto para birimleri hakkında değerlendirme sunulması, konu hakkındaki çoğu yönün açıkta bırakılmasına sebep olmuştur.

Dion-Schwarz vd. (2019, ss. 1-80) tarafından yapılan “*Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats (Kripto Para Birimlerinin Terörist Kullanımı: Teknik ve Organizasyonel Engeller ve Gelecekteki Tehditler)*” adlı çalışmada, terör örgütleri tarafından finansman faaliyetlerinde kripto para birimlerinin ne derecede kullanıldığı, kullanılmasını etkileyen faktörler ve kullanımını artırma potansiyeli olan gelecekte ortaya çıkması muhtemel özellikler incelenmiştir. Çalışma, odağını Bitcoin dışındaki kripto para birimlerine de yönlendirmesi, özellikle gizlilik özellikleri artırılmış kripto para birimlerinin terör örgütlerinin anonim işlem gerçekleştirmeleri konusunda sunduğu olanakları incelemesi, mevcut kripto para birimlerinin terör örgütleri tarafından kullanımına yönelik oluşturduğu sınırlamaları sistematik şekilde analiz etmesi bakımından oldukça geniş kapsamlıdır. Ancak çalışma, yalnızca sınırlı olduğu kripto para birimlerinin terör örgütleri tarafından kullanımını incelemiş ve kripto para birimi dışındaki kripto varlıklara ilişkin herhangi bir değerlendirme sunmamıştır.

Wang ve Zhu (2021, ss. 2329-2340) yazmış oldukları “*Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing (Terörizmin Finansmanında*

Potansiyel Kripto Para Geliştirme Yeteneğinin Değerlendirilmesi)” adlı makalede, kripto para birimlerinin terörizmin finansmanında oluşturduğu potansiyel riskleri ele almış ve kripto para birimlerinin özelliklerini, gelişim durumunu, uluslararası kuruluşların denetim sistemlerini incelemiştir. Yazarlar, terörizmin finansmanı bağlamında kripto para birimlerinin, henüz olgun bir yöntem olmasa da teknolojinin gelişmesi ve anonimlik özelliklerinin iyileştirilmesiyle kullanımının artacağını değerlendirmiştir. Konuyu çok çeşitli açılardan ele alarak oldukça zengin bir değerlendirme sunan yazarlar, terörizmin finansmanında kripto para birimlerinin kullanımını etkileyen faktörleri yalnızca kripto para birimlerinin özelliklerine, kripto para piyasasının gelişimine, geleneksel finansman araçlarına, ulusal ve uluslararası denetim düzeyine dayandırmıştır. Ancak yazarların, sadece kripto para dünyasındaki genel eğilimlere odaklandıkları, terör örgütlerinin finansman kararları üzerinde de etkili olan iç dinamiklerine, imkân ve kapasitelerine dayalı faktörleri dikkate almadıkları görülmektedir.

Dyntu ve Dykyj (2021, ss. 67-72) tarafından yayınlanan “*Cryptocurrency As an Instrument of Terrorist Financing (Terörizmin Finansmanında Bir Araç Olarak Kripto Para Birimi)*” adlı makalede, Bitcoin özelinde kripto para birimlerinin terörizmin finansmanı aracı olarak kullanılması incelenmiştir. Merkezi olmayan yapısı ve sözde anonim niteliği sayesinde terörizmin finansmanında kullanılmaya oldukça elverişli olduğu vurgulanan Bitcoin kripto para birimini kullanan terör örgütlerinin, karıştırıcı (mixer) hizmetleri gibi anonimliği artırıcı teknikleri de kullanmaya başladıklarına dikkat çekilmiştir. Makale, kripto para birimlerinin anonimliğini artırmak için kullanılan yöntem ve tekniklere değinmesi ve bir terör örgütünün kripto para birimleriyle bağış toplamada anonimleştirme yöntemlerini de kullandığı iki örnek olayı incelemesi bakımından literatüre büyük katkı yapmıştır. Ancak makalede, terör örgütlerinin bunlardan tam olarak nasıl istifade ettiklerinin veya edebileceklerinin yeterli şekilde incelenmediği görülmüştür.

Ayrıca, kripto varlıkların yasa dışı faaliyetlerde kullanılmasını önlemeye, mali suçları tespit etmeye ve uyumluluk standartlarını karşılamaya yönelik güvenlik, izleme ve uyumluluk hizmetleri sunan *Elliptic*, *Chainalysis*, *CipherTrace* ve *Sanction Scanner* gibi şirketlerin düzenli olarak kripto varlıkların kullanımıyla ilgili raporlar yayınladığı görülmektedir. İlgili raporlar, kripto varlıklar alanında farkındalığın artırılmasına ve ilgili paydaşların daha etkili önlemler almasına yardımcı olmayı amaçlamakla birlikte, kripto

varlıkların terörizmin finansmanı gibi yasa dışı faaliyetlerde kullanılma örneklerini ve eğilimlerini inceleyerek bu alandaki literatüre de büyük katkı sağlamaktadır.

Kripto varlıkların terörizmin finansmanı amacıyla kullanılması konusunda literatürde yer alan çalışmalarda, çoğunlukla yalnızca kripto para birimlerine ve hatta sadece Bitcoin'e odaklanıldığı, para birimi olarak nitelendirilemeyen NFT gibi Token'lara veya kripto varlık teknolojisinden ileri gelen madencilik (mining) ve kripto varlıkların ilk arzı (*Initial Coin Offering*-ICO) gibi konulara değinilmemesi sebebiyle kapsamın sınırlı tutulduğu, kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesine yönelik olarak FATF tavsiyeleri gibi uluslararası standartların yeterince incelenmediği, FATF standartlarının incelendiği takdirde ise sınırlı bir perspektiften FATF'in yalnızca birkaç tavsiye kararının bu kapsamda değerlendirildiği görülmüştür. Ayrıca ilgili literatür incelendiğinde, kripto varlık, kripto para birimi, sanal varlık, sanal para birimi, dijital varlık, dijital para birimi kavramları arasında sürekli bir anlam kargaşası olduğu, kavramların sıklıkla benzer bağlamlarda birbirleri yerine kullanıldığı, genel kabul görmüş tanımları ve tasnifleri bulunmadığı da görülmektedir.

Kripto varlıkların doğasından kaynaklanan özellikleriyle birlikte düzenleme boşluklarından faydalanmayı hedefleyen terör örgütleri, finansman faaliyetlerinde tespit, müdahale ve cezadan kaçınmak adına kripto varlık kullanımına yönelmiştir. Gelişen teknolojinin etkisiyle ortaya çıkan kripto varlıkların terörizmin finansmanı ile mücadele kapsamında oluşturduğu riskleri anlamak önemlidir. Terörizmin finansmanı ile mücadele düzenlemelerinin kripto varlıklar bağlamında incelenmesi ve değerlendirilmesi de teknolojinin hızla değişen doğasıyla başa çıkmak adına ayrıca öneme sahiptir. Bu kapsamda, yukarıda bahsedilen literatürdeki eksikliklere de odaklanan tezin, kripto varlıkların terörizmin finansmanındaki rolü ile bu bağlamda düzenleyici bir çerçeve olarak FATF tarafından geliştirilen tavsiyelerin anlaşılmasına katkı sağlayacağı değerlendirilmektedir.

Tezin amacı, kripto varlıkların terörizmin finansmanında hangi faktörlerden etkilenerken ve hangi yöntemlerle kullanılabileceğinin ve ne derecede kullanıldığının ortaya konulması ile konu bağlamında ilgili FATF tavsiyelerinin incelenmesidir. Bu amaç doğrultusunda, esas olarak “*Kripto varlıklar terörizmin finansmanında neden, nasıl, ne derecede kullanılmaktadır ve bu bağlamda FATF tavsiyeleri nasıl değerlendirilmektedir?*”

sorusuna cevap aranırken, cevaba ulaşabilmek için aşağıdaki sorulara da yanıtlar bulmaya çalışılmaktadır:

- Kripto varlıklar nedir? Kripto varlıklar nasıl ortaya çıkmış ve gelişmiştir?
- Kripto varlıkların ve dayandığı teknolojinin özellikleri ve teknik unsurları nelerdir?
- Kripto varlıklar ve dayandığı teknoloji hangi amaçlarla kullanılabilir?
- Kripto varlıkların terörizmin finansmanında kullanılmasını etkileyen faktörler nelerdir?
- Kripto varlıkların terörizmin finansmanında potansiyel kullanım yöntemleri nelerdir?
- Kripto varlıkların terörizmin finansmanında kullanım örnekleri nelerdir?
- Kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi kapsamında FATF ne gibi çalışmalar yürütmektedir?
- Kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi kapsamında ilgili FATF tavsiyeleri nelerdir ve nasıl değerlendirilmektedir?

Söz konusu sorulara yanıtlar aranırken nitel araştırmanın yürütüldüğü bu tezde, veri toplama yöntemi olarak doküman incelemesi yapılmıştır. Doküman incelemesi, araştırılan konu hakkında gerekli bilgileri ihtiva eden çeşitli formlardaki belgelerin çözümlenmesi olup diğer veri toplama araçlarının mümkün olmadığı durumlarda nitel araştırmalar için tek başına veri toplama yöntemi olarak kullanılabilir (Balaban Salı, 2018, s. 151). Tezde doküman incelemesi yoluyla; yönetmelik ve kanunlar, direktifler, bildirimler, FATF tavsiyeleri ve raporları, kripto varlıkların Whitepaper'ları, uluslararası kurum ve kuruluşlar ile özel şirketlerin raporları ve internet siteleri, terör örgütü destekçileri tarafından kripto varlıklara ilişkin rehberlik sağlamak amacıyla oluşturulan dijital dokümanlar gibi birincil kaynaklar ile birlikte konu hakkında çeşitli yazarlar tarafından kaleme alınan makaleler, kitaplar, kitap bölümleri, haberler gibi ikincil kaynaklardan veri toplanmış ve toplanan verilerin analiz edilmesi ve yorumlanması için içerik analizi yöntemi kullanılmıştır. Derinlemesine bir çözümleme gerektiren içerik analizinde benzer veriler, belirli kavramlar ve temalar çevresinde bir araya getirilerek anlaşılır şekilde düzenlenmekte ve yorumlanmaktadır (Akbulut, 2018, ss. 186-187). Genellikle belirli konular etrafındaki ilişkileri, desenleri ve eğilimleri anlamak için kullanılan içerik analizi, derinlemesine bir bakış sunması ve kapsamlı bilgi elde etmeye yardımcı olması bakımından önemli bir

yöntemdir. Tezde, kripto varlıkların mevcut ortamının, terörizmin finansmanı ile ilişkisinin, terörizmin finansmanında kullanım biçimlerinin ve eğilimlerin, FATF tarafından geliştirilen düzenleyici çerçevenin anlaşılmasına yardımcı olmak amacıyla sistematik içerik analizi yöntemi kullanılmıştır. Bu kapsamda, toplanan veriler kripto varlıklar, terörizmin finansmanı ve FATF tavsiyeleri etrafında kodlanarak kripto varlıkların terörizmin finansmanındaki rolüne ve bu bağlamdaki FATF tavsiyelerine ilişkin, tezin alt konu başlıkları olarak da belirlenen temalar tanımlanmıştır. Sonrasında kodlanan veriler, söz konusu temalar altında düzenlenerek çeşitli bulgular ortaya konmuş ve bulguların analizi sonucu kripto varlıkların terörizmin finansmanına ilişkin mevcut ve potansiyel riskleri ile FATF tarafından geliştirilen düzenleyici çerçeveye ilişkin değerlendirmeler gerçekleştirilmiştir.

Tezin kapsamı, günümüzde kullanımı yaygınlaşan kripto varlıkların terörizmin finansmanında kullanılma potansiyeli, açık kaynaklara yansıyan birtakım kullanım örnekleri ve konuyla daha ilgili olduğu değerlendirilen FATF tavsiyelerinin bu bağlamda incelenmesi olup tezin bazı sınırlılıkları mevcuttur. Öncelikle kripto varlıklar, sosyal bilimler alanında incelenirken araştırmacılar için anlaşılması zor olabilen oldukça karmaşık ve detaylı bir teknik altyapıya sahiptir. Bu tezde, tüm teknik detayların geniş kapsamda ele alınması değil, kripto varlıkların terörizmin finansmanı amacıyla kullanımına odaklanılarak, kripto varlıkların teknik boyutuna ilişkin genel bir anlayış sunulması amaçlanmıştır. Ayrıca incelenen teknolojik dinamikler araştırma dönemine özgü olup kripto varlık teknolojisinin sürekli olarak evrilen doğası sebebiyle gelecekte ortaya çıkacak kullanım modellerinin tahmin edilmesinde de sınırlılıklar mevcuttur.

Diğer taraftan, terörizmin finansman faaliyetlerinin genellikle gizlilik içerisinde gerçekleştirilmeye çalışılmasından dolayı tespit ve izlenmesi oldukça zordur. Ayrıca kripto varlıkların çeşitli düzeylerde sağladığı anonimlik özelliklerinin, terörizmin finansmanı bağlamında kullanılması faaliyetlerinin belirlenmesini bir dereceye kadar zorlaştırdığını da söylemek mümkündür. Dolayısıyla, terörizmin finansmanında kripto varlıkların kullanıldığına ilişkin somut kanıt ve verilere ulaşmanın zorluğu, tezin diğer bir sınırlılığını oluşturmaktadır. Bununla birlikte, açık kaynaklarda yer alan mevcut kullanım örneklerinin incelenmesinin, kripto varlıkların terörizmin finansmanında ne dereceye kadar kullanıldığı konusunda fikir vermesi açısından yardımcı olacağı değerlendirilmektedir.

Son olarak, yaklaşık son on yıldır dikkatleri çeken kripto varlıkların hukuki statüsü ve düzenlemeleri ülkeden ülkeye büyük farklılıklar göstermekte olup henüz küresel düzeyde uyumlu bir düzenleyici çerçeve bulunmamaktadır. FATF tavsiyeleri, kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi konusunda önemli standartlar ortaya koysa da ülkelerin gerek terörizm anlayışındaki gerekse hukuki çerçevelerindeki farklılıklardan dolayı tavsiye gerekliliklerinin uygulanması değişkenlik göstermektedir. Dolayısıyla FATF tavsiyelerinin bu konudaki etkinliğinin değerlendirilmesindeki zorluk tezin diğer bir sınırlılığını oluşturmaktadır.

Toplam üç bölümden oluşan tezin birinci bölümünde, kripto varlıkların ortaya çıkışı ve gelişimi incelenmiştir. Öncelikle, kripto varlıkların ortaya çıkış sürecini anlayabilmek adına para kavramına ve tarihine ilişkin kısa bir anlatı sunulmaya çalışılmıştır. Bu bölümde, paranın tanımı, özellikleri ve işlevlerinin açıklanmasının ardından tarihteki para sistemlerine değinilmiştir. Hakiki değeri olan malların para olarak kullanıldığı mal para sisteminden, merkezi olmayan sanal para birimleri olan kripto paralara uzanan paranın evrim süreci incelenmiş ve dijital para birimleri içerisinde elektronik, sanal ve kripto para birimlerinin farkları açıklanarak tasnifi yapılmıştır. Ardından diğer bölümde, kripto varlıkların temelinde yatan dağıtık defter teknolojisinin en yaygın kullanım şekli blokzincirinin teknik altyapısına, özelliklerine ve kullanım alanlarına değinilmiştir. Birinci bölümün son bölümünde ise genel olarak kripto varlıklar incelenmiştir. Bu bölümde, kripto varlıklara çeşitli kuruluşlar tarafından getirilen tanımlar açıklanmış, kripto varlıklara ilham verdiği düşünülen çalışmalara da değinilerek kripto varlıkların ortaya çıkışına zemin hazırlayan süreç incelenmiş, güven algısı ve kripto varlıkların benimsenmesinden bahsedilmiş, kripto varlıkların teknik unsurları ifade edilmiş, kripto varlık ekosisteminde yer alan aktörler açıklanmıştır. Son olarak, kripto varlık türleri sınıflandırılarak, özellikleri, farkları, kullanım amaçları anlatılmıştır.

Tezin ikinci bölümünde, kripto varlıkların terörizmin finansmanında kullanılması incelenmiştir. Terörizmin finansmanı konusuna geçilmeden önce, ilk olarak terör ve terörizm kavramlarına değinilmiştir. Ardından terörizmin finansmanı kavramı açıklanmış, terörizmin finansmanında toplama, aktarma, depolama aşamaları ifade edilmiş, terörizmin finansmanı ve internetin ilişkisi incelenmiştir. Sonraki bölümde, terörizmin finansmanı amacıyla kripto varlıkların kullanılması konusuna geçilerek kripto varlıkların terörizmin finansmanında kullanılmasını etkileyen faktörler belirtilmiştir. Bu kapsamda, kripto

varlıkların terörizmin finansmanında kullanılmasını kolaylaştıran faktörler; anonimlik, merkeziyetsiz yapı, küresel erişim ile sınır ötesi ve hızlı transfer mekanizması, düzenleme eksiklikleri olarak dört ana başlık halinde ve kripto varlıkların terörizmin finansmanında kullanılmasını zorlaştıran faktörler; örgütsel öğrenim ve kontrol sorunları, teknik altyapı eksikliği, likide dönüştürülemezlik, değer oynaklığı olarak dört ana başlık şeklinde incelenmiştir. Sonrasında, kripto varlıkların terörizmin finansmanında potansiyel kullanım yöntemleri; bağışlar, Dark Web içerisinde suç geliri ve malzeme temini, suç gelirlerinin aklanması, NFT, merkezi olmayan finans (*Decentralized Finance-DeFi*), madencilik, ICO, karıştırıcı (*mixer*) hizmetleri, gizlilik tabanlı kripto varlıklar (*Privacy Coins*) şeklinde başlıklar halinde incelenmiştir. Son olarak, kripto varlıkların terörizmin finansmanında kullanımına ilişkin açık kaynaklara yansıyan örnek olaylar açıklanmıştır.

Konu kapsamında kripto varlıklara düzenleyici çerçeveden bakmanın da gerekli olduğu değerlendirildiğinden, tezin üçüncü ve son bölümünde kripto varlıklar ve Mali Eylem Görev Gücü (*Financial Action Task Force-FATF*) tavsiyeleri incelenmiştir. Öncelikle FATF'in ne olduğu ve tarihçesine değinilmiş, sonrasında ise yöntem ve trendlerin belirlenmesi, FATF tavsiyeleri, karşılıklı değerlendirme raporları ve yüksek riskli ülkeler ile artırılmış izlemeye tabi ülkelerin belirlenmesi başlıkları altında FATF'in temel çalışma alanları ifade edilmiştir. Devam eden bölümde, kripto varlıklara sanal varlık kavramı üzerinden atıfta bulunan FATF'in bu alanda 2014 yılından günümüze değin yayınlamış olduğu raporlar ve rehberler açıklanmıştır. Son olarak, "*FATF'in 40 Tavsiyesi*" içerisinde kripto varlıkları daha fazla ilgilendirdiği değerlendirilen toplam 28 tavsiye ve gerekliliklerinin kripto varlıklar bağlamında nasıl değerlendirildiği incelenmiştir.

Tezin sonuç bölümünde ise kripto varlıkların terörizmin finansmanında kullanılması potansiyeli ile mevcut eğilimlere ve FATF'in düzenleyici çabalarının yeterliliğine ilişkin bazı değerlendirmeler gerçekleştirilmiştir. Kripto varlıkların doğasından kaynaklanan çeşitli benzersiz özellikleri ile mevcut düzenleme eksikliklerinin, terörizmin finansmanında kullanımı konusunda önemli bir potansiyel yarattığı sonucuna ulaşılmıştır. Ayrıca, terör örgütlerinin içsel ve faaliyet gösterdiği bölgelerin dinamiklerinden veya kripto varlıkların henüz geniş çapta benimsenmemesinden kaynaklanan birtakım faktörlerin kripto varlıkların terörizmin finansmanında kullanılmasını zorlaştırdığı; ancak ilerleyen süreçte, dünya çapında daha yaygın kabul görmesi beklenen kripto varlıkların terörizmin finansmanı bağlamında kullanımının artabileceği değerlendirilmiştir. Terörizmin finansmanı

kapsamında çok çeşitli kullanım yöntemleri olabileceği de ortaya konulan kripto varlıkların, terör örgütleri tarafından finansman faaliyetlerinde geleneksel yöntemlerin yanı sıra kullanıldığı ve genel olarak kullanım eğilimi ile yöntemlerinin karmaşıklığının giderek arttığı sonucuna varılmıştır. Son olarak, FATF tarafından geliştirilen tavsiyelerin kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi konusunda önemli bir düzenleyici çerçeve sağladığı; ancak ülkelerin FATF tavsiyelerini kendi sistemlerine ve ulusal düzeydeki risklerine uyarlayarak kripto varlıkların özgün özellikleri ile dinamikleri doğrultusunda etkin düzenleme ve denetim mekanizmaları oluşturmadığı ve uluslararası iş birliği ile bilgi paylaşımına aktif şekilde katılım sağlamadığı sürece yeterli olmayacağı değerlendirilmiştir.



BİRİNCİ BÖLÜM

KRİPTO VARLIKLARIN ORTAYA ÇIKIŞI VE GELİŞİMİ

1.1. Para Kavramı

Yazının tarihinden muhtemelen daha eski olan paranın tarihi geleneksel yaklaşıma göre isteklerin karşılıklı çakışması esasına göre işleyen *trampa*¹ sisteminde ortaya çıkan işlem maliyetlerini azaltmak için paranın yaratılmasıyla başlamıştır. Tarih sahnesinde, iş bölümünün gelişmesiyle birlikte trampa ekonomisinin yetersiz ve karmaşık hale gelmesinin bir sonucu olarak paranın kullanılmaya başlandığı görülmektedir. İnsanların gereksinim duyduğu şeylerin mübadelesi belirli sınırları aştığında ve gereksinim duyulan şeyler kolay taşınmadığında, değiş-tokuş sırasında bir başka nesne kullanılmaya başlanarak para icat edilmiş ve trampa ekonomisinden para ekonomisine geçilmiştir (Aristoteles, 1993, ss. 20-21).

1.1.1. Para Nedir?

En temel anlamıyla paranın, mal ve hizmetlerin mübadelesinde kullanılan genel olarak kabul görmüş şey olduğu söylenebilir. Aristoteles parayı, *uylaşım*² bir *değişim aracı* olarak ifade etmiştir. Aristoteles'e göre paranın uyluşıma dayanan kullanımı ve para sistemini kullananlar dışında doğada yeri veya kendi içsel değeri yoktur (Aristoteles, 1993, ss. 20-21). Daha sonraları Keynes (2012, s. 19) parayı, teslimiyle borç ve fiyat sözleşmelerinin ifa edildiği ve genel satın alma gücünün temsil edildiği biçim olarak ifade etmiştir. Ayrıca Keynes, mübadelede araç olarak kullanılan şeyin para olarak değerlendirilmesini, o şeyin genel satın alma gücünü temsil edebilmesine dayandırmaktadır. Zaman içerisinde genel satın alma gücü, değişen ekonomik koşulların etkisiyle dünyanın farklı yerlerinde, farklı zamanlarda ve farklı şekillerde temsil edilmiştir. Tarihçi yazar Yuval Noah Harari (2017, ss. 184-190)'ye göre ise neredeyse tüm kültürel farkları aşabilen ve insanların etkin şekilde iş birliği yapabilmesini sağlayan para, insanlar tarafından şu ana kadar yapılan en etkili ve evrensel karşılıklı güven sistemini oluşturmaktadır. Paranın genel

¹ Trampa bir kısım malın faydalı görülen bir başkasıyla değiş tokuş edilmesidir (Aristoteles, 1993, s. 20).

² TDK (2022)'ya göre uyluşım, saymaca bir şey benimsemek için yapılan anlaşma olarak tanımlanmıştır.

olarak kabul görmesi güven duygusuna, güven duygusu ise paranın özelliklerini ve işlevlerini yerine getirmedeki etkin başarısına bağlıdır (Gürsoy, 2021, ss. 12-13).

1.1.2. Paranın Özellikleri ve Fonksiyonları

Geleneksel yaklaşımda bir mübadele aracı olarak paranın; toplum tarafından geniş ölçüde kabul görmesi, kolayca deforme olmayacak dayanıklı bir maddeden yapılması, kolay taklit edilememesi, kolay taşınabilirlik, bölünebilirlik, standartlık ve homojenlik gibi özelliklere haiz olması gerekmektedir (Şıklar, 2004, s. 6). Bu özelliklerin yanında paranın değerinin istikrarlı olması için arzı sınırlı olmalı ancak ihtiyaç halinde de artırılabilmelidir.

Bir varlığın para olarak sayılabilmesi için geleneksel anlayışla kabul edilen üç temel fonksiyonu ise; mal ve hizmetlerin mübadelesinde değişim ve ödeme aracı olarak kullanılması, mal ve hizmetlerin değerini sistemli olarak belirleyen bir değer ölçüsü ve hesap birimi olması, değer saklama ve servet biriktirmeye yaramasıdır (Ünsal, 2016, ss. 587-588).

Likit bir varlık olan paranın sayılan fonksiyonlarının etkinliği ekonomide fiyatlar genel düzeyinin artış oranına bağlı olup, özellikle yüksek enflasyonun yaşandığı bir ekonomide tahvil ve hisse senedi gibi çeşitli varlıklar değer saklama aracı olarak tercih edilmektedir (Pınar ve Erdal, 2016, ss. 4-6). Bu durumda değer saklama işlevi yalnızca paraya özgü değildir, değer biriktirme araçlarına paradan daha geniş bir kavram olan *varlık* denilmektedir ve para serveti oluşturan varlıklardan yalnızca bir tanesidir (Ünsal, 2016, s. 588).

Genel kabul görme özelliği sayesinde para, taraflar arasındaki güveni artırarak herhangi bir mübadelede kolaylık ve standartlık sağlar. Öte yandan para, yalnızca bir mübadele aracı değil aynı zamanda ödeme aracıdır. Para, taraflar arasındaki mübadeleden doğan hukuki ilişkiyi sona erdirdiğinden dolayı çek ve senet gibi mübadele sırasında araç olarak kullanılabilen diğer varlıklardan ödeme aracı olma özelliğiyle ayrılmaktadır (Somel, 2014, s. 105).

Para ödeme aracı olması açısından ele alındığında, aynı zamanda iletişim aracı olma özelliği taşımaktadır. Para, ortak anlam üreten bilgiyi aktarmanın bir yolu olarak iletişim biçimi şeklinde görülebilmekte ve ödeme üzerinden kurulan iletişim ile insanları ortak bir

ekonomik dünyada, işlemsel topluluk bünyesinde bir araya getirebilmektedir. Bu durum, parasal araçların politika amacıyla kullanılmasının yanında topluluklar ve kurumlar arasındaki ilişkileri belirlemek amacıyla da kullanılması durumunu beraberinde getirmektedir. Dolayısıyla para değişim aracı olma işlevinin yanında temsil aracı olma özelliği de taşımakta ve değer iletme amacının yanında toplumsal gerçeklik üretmek için de kullanılmaktadır (Swartz, 2021, ss. 18-34). Zamanla işlemsel topluluklar bünyesinde yeni para birimleri oluşturulmuş ve toplumsal gerçeklik dönüşümlere uğramıştır.

1.1.3. Paranın Tarihi ve Para Sistemleri

Antik çağlardan günümüze kadar farklı medeniyetlerde çeşitli para sistemleri kullanılmıştır. İlk başlarda kullanım değeri olan mallar para olarak kullanılırken, zamanla madeni paraların ve ardından kâğıt para biçimindeki temsili para ile itibari paranın kullanımına geçildiği görülmektedir. Modern çağda ise, dijital teknolojinin yükselmesiyle birlikte elektronik para, sanal para ve kripto para gibi dijital para birimleri ortaya çıkmıştır. Gelecekte ortaya çıkacağı form belirsiz olarak paranın tarihi, insanlık tarihine paralel olarak evrim geçirmeye devam etmektedir.

1.1.3.1. Mal (Meta) para

Geçmişte kullanılan ilk para türlerinin, değeri kendisine içkin olan mal veya meta paralar olduğu bilinmektedir. Paranın mutat fonksiyonlarına uygun şekilde seçilen mal para, özgürce edinilebilse de arzı diğer mallarda olduğu gibi üretim maliyetine ve kıtlığına bağlı bir malın fiili birimlerinden oluşmaktadır (Keynes, 2012, s. 22). Eski çağlarda mallara çoğu kez, elde edilmeleri için karşılığında verilen hayvan sayısı ile değer biçildiği görülmektedir. Önceleri dünyanın farklı bölgelerinde, deniz kabukları, tuz, şeker, tütün, post gibi çeşitli nesnelerin para olarak kullanıldığı düşünülmektedir (Smith, 2006, s. 64). Mal paranın bölünme, taşınma, saklanma, dayanıklılık ve değerini koruma konusunda karşılaşılan zorluklar nedeniyle daha sonraki süreçte çeşitli metaller para olarak kullanılmıştır.

1.1.3.2. Madeni para

Başlarda metaller işlenmemiş, işaretsiz ve damgasız şekilde kullanılırken, değiş-tokuş sırasında metalleri tartmanın ve ayarlarına bakmanın zahmeti nedeniyle insanların alışverişte

kullandığı metaller ülkeler tarafından damgalanmaya başlanmıştır (Smith, 2006, ss. 65-66). Böylelikle değerli bir veya birkaç madenden darp edilen sikkelerin para olarak kullanıldığı madeni para sistemine geçilmiştir. Lidyalıların buluşundan sonra madeni paranın kullanımı, Yunan Şehir Devletleri'nde ve kolonilerinde büyük ölçüde gelişmiştir. Ancak zaman içerisinde dolaşımdaki madeni paraların çeşitli şekillerde karıştırılması ve kırılmasıyla değerinin düşürülmesi (tağşiş), büyük miktarlardaki madeni paranın taşınmasının ve saklanmasıyla ilgili sebepler birer sorun haline gelmiştir. Bu sorunlara ilişkin çözüm ise para tarihini bankacılık tarihiyle birleştiren bir adım olarak 17. yüzyılda modern anlamda bankaların kurulmasıyla temsili para sisteminin ortaya çıkışı ile gelmiştir (Galbraith, 2017, ss. 17-19).

1.1.3.3. Temsili para

Keynes (2012, s. 22) temsili parayı, malzeme değeri olarak hakiki değeri ile üzerinde yazılı olan parasal değeri farklı olan simgesel para şeklinde ifade etmiştir. Temsili para sisteminin doğuşu, madeni paranın güvenlik amacıyla bankalara ve kuyumculara emanet edilmesi ve karşılığında alınan senedin ödemelerde kullanılması suretiyle kâğıt paranın ortaya çıkışı ile gerçekleşmiştir. Kâğıt para ilk olarak, 17. yüzyılın sonlarında Amerika Birleşik Devletleri (ABD)'nde Massachusetts Hükûmeti tarafından ve İngiltere'de kuyumcular tarafından basılarak dolaşıma çıkarılmış ve ülkelerin merkez bankalarının kurulması ile kullanımı yaygınlaşmıştır (TCMB, 2018, s. 2).

Başlangıçta kâğıt paralar tamamen kıymetli maden karşılığı çıkarılsa da bir süre sonra, bankaların karşılıksız banknotlar çıkarmaktan kazanç elde edebileceğini fark etmesiyle birlikte kıymetli maden karşılığı olmayan kâğıt paralar da ihraç edilmeye başlanmıştır. Bankaların, ihraç ettiği bu tür kâğıt paraların miktarını çok artırarak insanların temsili parayı kıymetli madene çevirme talebini karşılayamayacak duruma gelmediği müddetçe temsili para sisteminin sorunsuz işlediği görülmüştür (TCMB, 2018, s. 2). Kıymetli maden üretiminin para arzını kısıtlayarak paranın dolaşımında yetersiz kalması nedeniyle temsili para sistemi zamanla Avrupa genelindeki parasal sistemlerin hayati bir parçası haline gelmiş ve insanların parayı kullanma şekli ile düşünme biçimlerini dönüştürmüştür (Eagleton ve Williams, 2011, s. 251).

Ülkelerin, merkez bankalarındaki altın rezervlerinin yalnızca belirli bir oranını aşacak şekilde temsili para ihracını sınırlandırmaları 19. yüzyılda genel bir kural haline gelmiştir (Somel, 2014, s. 106). Bu dönemde birçok gelişmiş ekonomi, parasal sistemin merkez bankaları aracılığıyla düzenlenmesi konusunda altın standardına bağlı kalmıştır (Ferguson, 2012, s. 51). Altın standardı, temsili para sisteminde paranın değerinin, altına göre sabit bir oran üzerinden belirlendiği sabit kur sistemidir. Ünlü iktisatçı David Ricardo (2008, s. 589) altın standardına ilişkin olarak, dolaşımdaki kağıt paranın değerini koruyabilmesi için, madeni parayla değiştirilebilir olmasının şart olmadığını ancak basılan kağıt para miktarının standart ilan edilen maden değerine göre belirlenmesinin şart olduğunu söylemiştir. Arzı sınırlanan kağıt para değerini koruma güvencesine sahipken; miktarını kısıtlayacak herhangi bir mekanizmaya sahip olmayan kağıt para, değerini azaltacak veya yok edecek arz artışına karşı savunmasızdır (Galbraith, 2017, s. 54). Bu açıdan altın standardı uygulaması, ekonomide enflasyonist beklentiler yerine fiyatların öngörülebilir olmasını sağlayarak istikrarın gelişmesine katkıda bulunurken, diğer yandan altın rezervlerinin para arzını kısıtlaması nedeniyle parasal genişleme gereken dönemlerde ekonomik istikrarsızlığa yol açmıştır. 20. yüzyılda finansal istikrar için tehdit olmaya devam eden para politikasında altın standardı uygulaması 1929 Büyük Buhranı'nın en önemli sebepleri arasında sayılmaktadır (Eichengreen, 2003, ss. 28-31).

Dünyada kitlesel işsizlik ve yoksulluğa yol açan Büyük Buhran'ın patlak vermesiyle 1930'lu yıllarda ülkeler altın standardını terk etmeye başlamış ve 1936 itibarıyla tüm Batı ülkelerinin paraları altın standardının dışına çıkmıştır (Eagleton ve Williams, 2011, ss. 337-338). Yeni bir uluslararası para sistemi tasarlamak üzere 1944 yılında ABD'de düzenlenen Birleşmiş Milletler Para ve Finans Konferansı'nın ardından, adını anlaşmanın yapıldığı bölgeden alan Bretton Woods Anlaşması imzalanarak *Bretton Woods Sistemi* oluşturulmuştur. Sistem, sabit bir orandan altına dönüştürülebilen ABD Dolarına, neticede ABD para otoritelerine bağlı bir altın-dolar standardına dayanmıştır. Bretton Woods Sistemi 1959'dan 1971'e kadar yalnızca 12 yıl sürmüştür ve sistem geliştikçe, altın standardında olduğu gibi uyum, güven ve likidite sorunlarıyla karşı karşıya kalmıştır (Bordo, 2017, s. 2). 1971 yılında ABD'nin doları altın karşılığı basmayı bırakmasıyla, söz konusu sistem ve dünya üzerindeki dolar üzerinden altın ile ilişkilendirilen kâğıt paraların, altın karşılığı tekrar son bulmuştur. Nesnel standardın terk edilmesiyle birlikte doğrudan veya dolaylı olarak altına dayanan temsili para sistemi, devletlerin para basma tekeline dayanan itibari para sistemi ile değiştirilmiştir.

1.1.3.4. İtibari para

Gücünü kıymetli maden yerine devletin hukuki ödeme aracı olarak ilan etmesinden alan itibari para sistemi, kâğıt para sisteminin modern uygulaması olarak karşımıza çıkmakta ve günümüzde tüm ülkelerde geçerliliğini korumaktadır (Ünsal, 2016, s. 590). İtibari para veya fiat para olarak ifade edilen kavram, devletçe yaratılıp tedavüle çıkarılan, ufak değerler dışında genellikle kâğıt olan, kendinden başka bir şeye tahvil edilemeyen ve değeri nesnel bir standarda bağlı olmayan temsili para olarak tanımlanmıştır. İtibari paranın devlet pratiği veya dayandığı yasalar dışında kendine özgü bir değeri yoktur ya da çok azdır (Keynes, 2012, ss. 22-25). İtibari paranın değeri, yapıldığı materyalden çok güven esasına dayanmaktadır (Eagleton ve Williams, 2011, s. 309). Burada güven, itibari parayı oluşturan merkezi otoriteye ve itibari paranın kolay taklit edilemeyeceğine karşı duyulmaktadır. İtibari paranın ödemelerde kullanılması kanuni olarak mecburiyet teşkil etmektedir.

1.1.3.5. Kaydi para

Günümüzde, asli paralar olarak adlandırılan devletçe tedavül edilen kâğıt para (itibari para) ve metal para (madeni ufaklık para) ile birlikte, kaydi para olarak adlandırılan banka mevduatları da kullanılmaktadır. Bankacılık sektörünün gelişmesi ile birlikte, bankaların kredi vermesi gibi durumlarla bankalarca oluşturulan kaydi paranın kullanımı yaygınlaşmıştır. Fiziki bir varlığa sahip olmayan kaydi para, çek veya kredi ve banka kartları gibi nakit dışı ödeme araçları vasıtasıyla paranın ödeme aracı olma fonksiyonunu yerine getirebilmektedir. Mevduatlarının belirli bir kısmını rezerv olarak bulundurmak zorunda olan bankaların kaydi para yaratma imkânları devletlerce belirli oranlarda kısıtlamalara tabi tutulmaktadır.

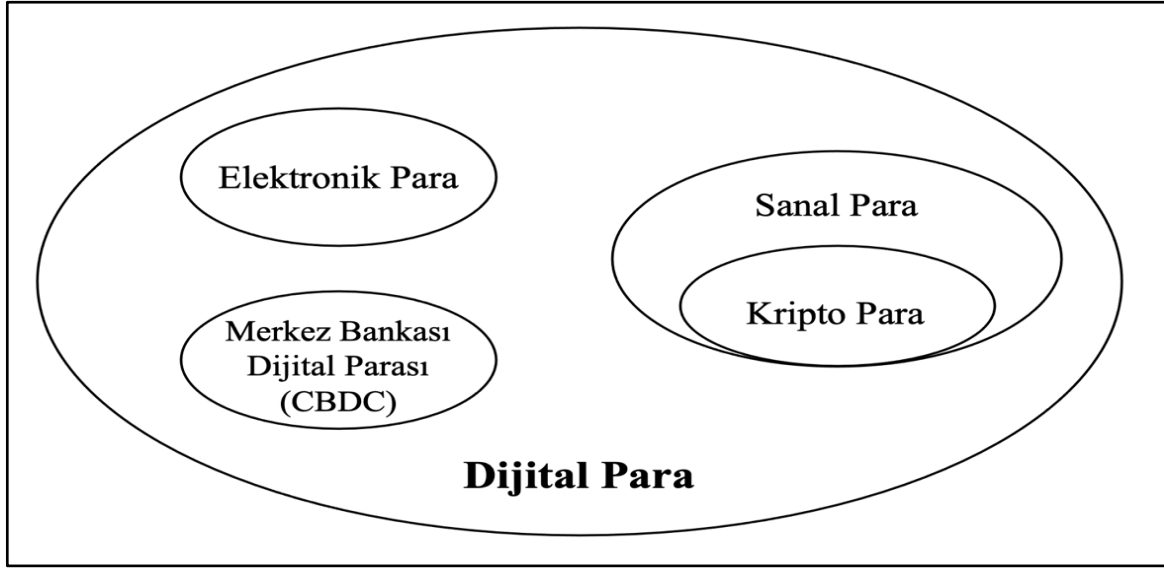
Özellikleri ve işlevlerinden yola çıkarak tanımının yapıldığı ana akım yaklaşımın aksine para, kimi çevrelerce, bir bütün olarak ekonominin işleyişine göre tanımlanmaktadır. Bu yaklaşımda para ile hesap parası olarak ifade edilen varlıklar arasında ayırım yapmak gerekmektedir (Wray, 2012, ss. 8-9). Keynes (2012, ss. 19-21), para ile hesap parası, düz para ile banka parası (kaydi para) kavramlarını birbirinden ayırarak banka parasının hesap parası ile ifade edildiğini söylemiştir. Bu açıdan kaydi para, somut varlık olarak paranın kendisi şeklinde değil, hesap birimi olan hesap parası şeklinde değerlendirilmelidir. Banka

mevduatları (somut) para değildir, ancak sosyal hesap birimi cinsinden ifade edilmektedir (Wray, 2012, s. 9).

1.1.3.6. Dijital para

Ekonomik, toplumsal ve kültürel dönüşümlere yol açan teknolojik gelişmeler, para ve finans sektörüne de sirayet etmiştir. Para ve finans sektörünün dijitalleşmesi yeni ürünler, hizmetler, süreçler ve iş modelleri geliştirilmesini de beraberinde getirmiştir (Puschmann, 2017, s. 69). Dijital para birimleri bu gelişmelere örnek olarak verilebilir. Her ne kadar literatürde “*dijital para*” ifadesi sıkça yer alsa da genellikle parayla ilişkilendirilen kabul düzeyine ulaşmaması bakımından dijital para birimlerinin *para* niteliğine sahip olup olmadığı tartışma konusudur. Bununla birlikte dijital para birimleri, paranın bazı özelliklerine sahip olmasının yanında bir varlığın özelliklerini de taşıyabilmektedir (Bank for International Settlements/BIS, 2015, s. 1).

Paranın tarihine bakıldığında, kendi içsel değeri veya karşılığı olan paradan karşılığı olmayana doğru ve somuttan soyuta doğru bir ilerlemenin olduğu görülmektedir. Gelenen son noktada para fiziki varlığının yanında dijital bir form da kazanmıştır. Dijital varlığın, bir bireyin hak veya çıkarına sahip olduğu dijital bir kayıt (World Bank, 2022, s. 18) olduğu düşünüldüğünde dijital paranın, dijital biçimdeki değer ihtiva eden varlıklar ile ilişkilendirilen geniş bir kavramı ifade ettiği anlaşılmaktadır. Değerin dijital temsili olarak dijital para, dijital ortamda üretilmekte, saklanmakta ve transfer edilmektedir. İçsel bir değere sahip olmayan dijital para birimleri değerini, sonraki bir zaman diliminde diğer mal veya hizmetlerle ya da belirli bir ulusal para birimiyle değiş tokuş edilebileceklerine olan inançtan almaktadır (Bank for International Settlements/BIS, 2015, s. 1). Aşağıda yer alan Şekil 1.1.’de gösterildiği gibi dijital para; elektronik paraları, merkez bankası dijital para birimlerini, sanal para birimlerini ve sanal paranın bir alt kümesi olan kripto para birimlerini kapsamaktadır.



Şekil 1.1. Dijital para kategorileri

Dijital para birimi, elektronik para veya sanal paranın dijital temsili anlamına gelmektedir (World Bank, 2022, s. 17). Yasal ihale statüsüne sahip itibari paranın dijital bir temsili olan ve itibari para biriminde ifade edilen değeri elektronik şekilde aktarmak için kullanılan *elektronik para* ile *sanal para birimleri* farklı kavramlardır (FATF, 2014, s. 4). Dijital para ise hem itibari para cinsinden bir elektronik ödeme mekanizması olan elektronik para kavramını hem de itibari para cinsinden olmayıp kendi hesap birimine sahip olan değerlerin dijital temsili olarak sanal para kavramını içeren geniş bir kategoridir (He vd., 2016, s. 7). Bunun yanında, Merkez Bankalarınca üretilen, yönetilen ve denetlenen, itibari para cinsinden ifade edilen Merkez Bankası Dijital Parası (*Central Bank Digital Currency-CBDC*) diğer bir dijital para biçimidir. Merkez Bankalarının doğrudan yükümlülüğü olan CBDC, özel finans kurumlarının yükümlülüğü olan kaydi para ve elektronik paradan farklılaşmaktadır (Mohammed vd., 2022).

Uluslararası Ödemeler Bankası (*Bank for International Settlements-BIS*); ihraç eden (merkez bankası veya diğer), form (dijital veya fiziksel), erişilebilirlik (evrensel veya sınırlı) ve transfer mekanizması (merkezileştirilmiş veya dağıtılmış) şeklinde dört temel özelliği temel alan bir para sınıflandırması yapmıştır (Bech ve Garratt, 2017, s. 55). Sınıflandırmaya göre dijital para form yönünden dijital olup, diğer özellikler yönünden farklılaşabilmektedir. Örneğin itibari para cinsinden ifade edilen, merkezi bir yapıya ve merkezileştirilmiş transfer mekanizmasına sahip olan, dijital para tanımı içerisinde yer alan elektronik paralar ile CBDC; CBDC'nin merkez bankası tarafından ve elektronik paranın merkez bankası dışındaki kuruluşlar tarafından ihraç edilmesiyle birbirinden ayrılmaktadır.

Dijital para dijital yollarla değiştirilmekte, hiçbir zaman bulunduğu dijital ortamı terk edememekte ve fiziksel biçim alamamaktadır (*Digital Currency: The Future Of Your Money*, 2023). Elektronik paralar, istendiği takdirde temsil ettiği itibari paraya dönüştürülebilmesiyle yani fiziksel şekil alabilmesiyle dijital paranın istisnai bir durumunu oluşturmaktadır. Dijital paralar, gerçek dünyada bir değere sahip olan ve mal ve hizmet satın alımında yaygın olarak kullanılan hediye kartları, indirim kuponları, uçuş milleri, kredi kartı puanları gibi çeşitli ürünleri içerebilmektedir (Helme ve Wilkinson, 2016, s. 1).

1.1.3.7. Elektronik para

Günümüzde kâğıt para ve madeni ufaklık paralara alternatif olarak elektronik paranın kullanımı ciddi ölçüde yaygınlaşmıştır. İtibari paranın elektronik temsili olan elektronik para, elektronik şekilde saklanmakta ve aktarılmaktadır. Elektronik para düzenlenmiş ve merkezi otoriteye bağlı bir alan olarak kabul edilmektedir.

Avrupa Merkez Bankası (*European Central Bank-ECB*) (1998, s. 7)'na göre elektronik para, “*genel olarak, işlemde banka hesaplarını içermesi gerekmeyen, ancak ön ödemeli hamiline bir araç olarak hareket ederek, elektronik para ihraç eden kuruluş dışındaki kuruluşlara ödeme yapmak için yaygın olarak kullanılabilen, teknik bir cihaz üzerinde parasal değer elektronik olarak saklanması*” olarak tanımlanmıştır. Tanımdan da görüldüğü gibi elektronik para, elektronik para ihraç eden kuruluşlar tarafından merkezi bir yapıda oluşturulmaktadır ve yalnız bu kuruluşlar tarafından değil dışındakilerce de kabul görmektedir.

Elektronik para kuruluşu hizmetlerinin alınması, takibi ve ihtiyatlı denetimi ile ilgili üye ülkelerin hukuki çerçevelerini ve idari hükümlerini koordine etmek ve uyumlu hale getirmek için gerekli uygun önlemlerin sağlanması amacıyla Avrupa Birliği, elektronik para kavramı ile elektronik para kuruluşlarına ilişkin olarak *2000/46/EC sayılı Direktifi* ve sonrasında *2009/110/EC sayılı Direktifi* yayımlamıştır.

18 Eylül 2000 tarihinde yayımlanan *2000/46/EC sayılı Avrupa Parlamentosu ve Konsey Direktifine* göre elektronik para, genellikle sınırlı miktarlarda elektronik ödemeleri gerçekleştirmek amacıyla madeni ve kâğıt paraların elektronik temsili olarak değerlendirilmektedir. Elektronik para ihraç eden kuruluş üzerindeki hak talebiyle temsil

edilen parasal değer anlamına gelen elektronik para; elektronik bir cihazda saklanmakta, değeri ihraç edilen parasal değerden daha az olmayan bir miktarda fon alındığında ihraç edilmekte ve elektronik para ihraç eden kuruluş dışındaki teşebbüsler tarafından ödeme aracı olarak kabul edilmektedir (Directive 2000/46/EC of The European Parliament and of The Council, 2000, ss. 1-2). Direktifin bazı hükümlerinin, elektronik para hizmetlerinin gelişimini engellediği ve elektronik para tanımının teknolojik yenilikler ile gelecekte geliştirilebilecek ürünleri de kapsayacak şekilde geniş olması gerektiği düşüncesi ile revize edilmesi ihtiyacı hasıl olmuş ve 2009/110/EC sayılı Avrupa Parlamentosu ve Konsey Direktifinin 16 Eylül 2009 tarihinde yayımlanması ile söz konusu Direktif yürürlükten kaldırılmıştır.

16 Eylül 2009 tarihli 2009/110/EC sayılı Avrupa Parlamentosu ve Konsey Direktifine göre ise elektronik para aşağıdaki gibi tanımlanırken elektronik para kuruluşu, “*elektronik para ihraç etme yetkisi verilen tüzel kişi*” olarak tanımlanmaktadır (Directive 2009/110/EC of The European Parliament and of The Council, 2009, s. 5).

“Ödeme işlemleri yapmak amacıyla fonların alınması üzerine ihraç edilen ve elektronik para ihraç eden kuruluş dışındaki gerçek veya tüzel kişiler tarafından kabul edilen, elektronik para ihraç eden kuruluş üzerindeki hak talebi ile temsil edilen, manyetik dahil olmak üzere elektronik olarak depolanmış parasal değer.”

Yeni Direktif ile yapılan elektronik para tanımında, teknolojik gelişmelere bağlı olarak elektronik paranın saklanması/depolanmasının kapsamı ile elektronik paranın kabul görmesinin kapsamı genişletilmiş ve “*değeri ihraç edilen parasal değerden daha az olmayan bir miktarda fon alındığında ihraç edilen*” ifadesi “*ödeme işlemleri yapmak amacıyla fonların alınması üzerine ihraç edilen*” ifadesi ile değiştirilmiştir.

Elektronik para, parasal değeri depolamak için kullanılan teknolojiye bağlı olarak donanım tabanlı, yazılım tabanlı veya her ikisinin özelliklerinin bir arada bulunacağı şekilde olabilmektedir. Donanım tabanlı elektronik para satın alma gücü, çipli kart gibi kişisel bir fiziksel cihazda bulunmakta ve uzak bir sunucuya eş zamanlı erişim gerektirmeyen cihaz okuyucuları aracılığıyla parasal değerlerin transferi gerçekleşmektedir. Yazılım tabanlı elektronik para ise kişisel bilgisayarlar veya tabletler gibi kişisel cihazlarda çalışan özel

yazılımlar kullanılmakta ve cihazın satın alma gücünün kullanımını kontrol eden uzak bir sunucu ile online bağlantı kurulması suretiyle parasal değerlerin transferi gerçekleşmektedir (European Central Bank, 2023).

Birçok ülkede hukuki düzenlemelere tabi kılınan elektronik para ve elektronik para kuruluşları ülkemizde 6493 sayılı *Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun* ile düzenlenmiştir. 2009/110/EC sayılı Direktife benzer şekilde ilgili Kanun'un 3'üncü maddesinde elektronik para ve elektronik para kuruluşunun tanımları yapılmış ve 5'inci bölümünde elektronik para kuruluşları ile elektronik paranın ihracına ilişkin hükümler düzenlenmiştir. Söz konusu Kanun'a göre bankalar, Posta ve Telgraf Teşkilatı Anonim Şirketi ve Merkez Bankası tarafından faaliyet izni verilen elektronik para kuruluşları, aldığı fon kadar elektronik para ihracında bulunabilmektedir (6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, 2013).

Banka kartları, ön ödemeli kartlar ve banka hesaplarında elektronik olarak var olan ve elektronik ticarete kullanılabilen para, elektronik paranın ilk örneklerini oluşturmaktadır (Mishkin, 2004, s. 51). Günümüzde elektronik para kuruluşları tarafından da oluşturulabilen elektronik paralar, hızla gelişen çeşitli elektronik ödeme sistemleri sayesinde ödemelerde artan bir sıklıkla kullanılmaya devam etmektedir. Elektronik paralar gibi sanal paralar da finansal teknolojinin ilerlemesi ve dijital dönüşüm süreciyle birlikte hayatımıza girmiş bir kavram olup elektronik paraların aksine, geleneksel finansal sistemlerin dışında bir finansal yenilik olarak karşımıza çıkmaktadır.

1.1.3.8. Sanal para

Teknolojik gelişmeler ile birlikte artan internet kullanımı, sanallaşmaya ve sanal para birimlerinin yaygınlaşmasına yol açmıştır. Sanal paralar, yalnızca para birimi, emtia, finansal varlık veya ödeme ağı şeklinde net bir şekilde sınıflandırılmadığından sanal para birimlerine ilişkin tanım da kullanıldığı bağlama göre değişmektedir. Dünyada pek çok kuruluşun, taşıdığı potansiyel riskler sebebiyle sanal paraları yakından takip ettiği, uyarılar ve açıklamalarda bulunduğu, belirli düzenlemeler yaptığı ve çeşitli tanımlar geliştirdiği görülmektedir.

Avrupa Bankacılık Otoritesi (*European Banking Authority-EBA*), sanal para birimleri hakkında 2014 yılında yayımladığı raporda, “*para birimi*” teriminin kullanımının diğer para birimlerine karşı değiş tokuş edilebilir olduğunun ima edilmesi de dahil olmak üzere çeşitli nedenlerle yanıltıcı olduğunu; ancak genel kullanımı yansıtmak için terimin bu şekilde kullanıldığını belirtmiştir. Raporda sanal para birimi “*bir merkez bankası veya kamu otoritesi tarafından çıkarılmayan veya mutlaka bir itibari para birimine bağlı olmayan, ancak gerçek veya tüzel kişiler tarafından bir değişim aracı olarak kullanılan ve elektronik olarak aktarılabilen, saklanabilen veya alınıp satılabilen dijital bir değer temsili*” olarak tanımlanmıştır (*EBA Opinion on ‘Virtual Currencies’*, 2014, s. 11).

Avrupa Merkez Bankası 2012 yılında yayımladığı raporda, gelecekte değişebileceğini belirterek, özelliklerine dayalı olarak sanal paraları tanımlayarak sınıflandırmaya çalışmıştır. Söz konusu raporda sanal para, “*geliştiricileri tarafından çıkarılan ve genellikle kontrol edilen, belirli bir sanal topluluğun üyeleri arasında kullanılan ve kabul edilen, düzenlenmemiş dijital para türü*” olarak tanımlanırken diğer para türleri ve gerçek ekonomi ile olan ilişkisi bakımından sanal para birimleri; temelde bir çevrim içi oyunda kullanılan “*kapalı sanal para*”, genellikle sanal mal ve hizmetleri satın almada kullanılan “*tek yönlü bir akışa sahip sanal para*”, dönüştürülebilir para birimi gibi davranan ve sanal veya gerçek mal ve hizmetleri satın almada kullanılabilen “*çift yönlü akışa sahip sanal para*” olmak üzere üç türe ayrılmıştır (European Central Bank, 2012, s. 5). Sanal varlık borsalarında arz ve talebe göre fiyatı belirlenen ve bu platformlarda diğer para birimleri ile karşılıklı dönüşümü mümkün olan sanal para birimleri çift yönlü akışa sahip olduklarından üçüncü türe dahil edilmektedir.

Avrupa Merkez Bankası tarafından 2015 yılında yayımlanan sanal para birimlerine ilişkin daha ileri bir analize dayanan raporda ise önceki raporda sanal para birimlerine ilişkin oluşturulan tanımdan çeşitli sebeplerle bazı ifadelerin çıkarılarak yeni bir tanım getirildiği görülmektedir. Tanımdan, merkezi bir geliştirici tarafından çıkarılmayan ve kontrol edilmeyen matematik tabanlı merkezi olmayan sanal para birimlerinin varlığı nedeniyle “*geliştiricileri tarafından çıkarılan ve genellikle kontrol edilen*” ifadesi, her ne kadar eşler arası ağlar ve internet platformları sanal bir topluluk olarak tanımlanabilse de sanal paranın kabulüne ilişkin herhangi bir sınır getirilmemesi adına “*belirli bir sanal topluluğun üyeleri arasında kullanılır ve kabul edilir*” ifadesi, bazı ülkelerde geliştirilen mevzuat ve düzenlemeler sebebiyle “*düzenlenmemiş*” ifadesi, Avrupa Merkez Bankası sanal para

birimlerini ekonomi literatüründe tanımlandığı şekliyle tam bir para biçimi olarak kabul etmediğinden “*para türü*” ifadesi çıkarılarak tanım revize edilmiştir. Raporda sanal para birimleri “*bir merkez bankası, kredi kurumu veya e-para kurumu tarafından verilmeyen ve bazı durumlarda paraya alternatif olarak kullanılabilen, değer dijital bir temsili*” olarak tanımlanmıştır (European Central Bank, 2015, s. 25).

Fiziksel karşılığı bulunmayan sanal para birimlerinin doğası gereği kontrolü geleneksel finansal aktörlerde değildir. Anonim özellikleri ve sınır ötesi karakterleri nedeniyle sanal varlıklar için gerekli yasal düzenlemeleri geliştirmek, takibi ve denetimi zorluk oluşturmaktadır. Sanal varlıklar bu açılardan suç gelirlerinin aklanması ile terörizmin finansmanında kullanılması bakımından risk teşkil etmekte ve söz konusu risklerin değerlendirilmesi için gelişmelerin düzenli olarak yakından takip edilmesi gerekmektedir. Küresel mali sistemi suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanına karşı korumak için politikalar geliştiren Mali Eylem Görev Gücü (*Financial Action Task Force-FATF*), sanal para birimlerine ilişkin çalışma mekanizmalarını ve sundukları risk ve faydaları anlatmak adına -gelecekte değişebileceğini belirterek- ortak bir kavramsal anlayış ve potansiyel suç gelirlerinin aklanması ile terörizmin finansmanı risk değerlendirmesi geliştirmeye çalışmıştır.

FATF tarafından 2014 yılında yayımlanan sanal para birimlerine ilişkin raporda sanal para,

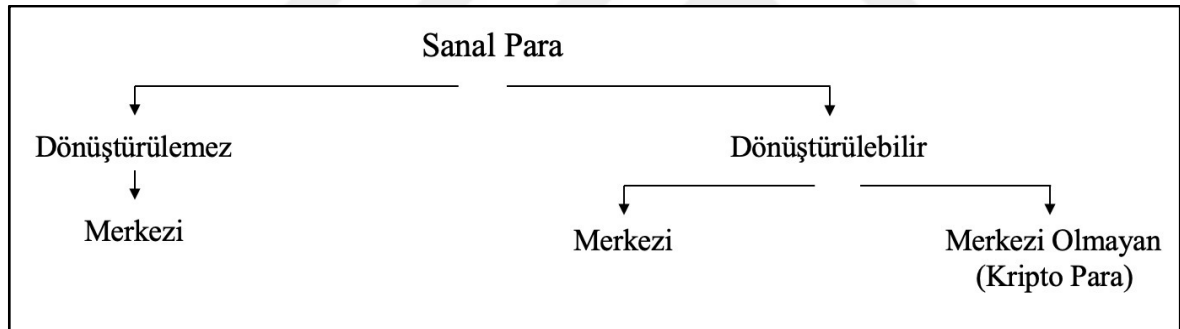
“...*dijital olarak alınıp satılabilen ve (1) bir değişim aracı; ve/veya (2) bir hesap birimi; ve/veya (3) bir değer deposu şeklinde işlev gören ancak herhangi bir yargı alanında yasal ihale statüsüne (bir alacaklıya sunulduğunda, geçerli ve yasal bir ödeme teklifine) sahip olmayan, dijital bir değer temsili*”

olarak tanımlanmıştır (FATF, 2014, s. 4).

Sanal paralar, paranın değişim aracı, hesap birimi ve değer saklama aracı olma fonksiyonlarından bir veya birkaçı şeklinde işlev görebilmektedir. Ancak günümüzde küresel olarak kullanılan sanal paraların, yasal olarak bir ödeme aracı olarak tanınmadığı veya istikrarları konusunda kamu güveni oluşturamadığı sürece işlemsel rollerinin sınırlı kalması ve değişim aracı veya hesap birimi fonksiyonlarından çok değer saklama amacıyla

kullanılması beklenmektedir. Nispeten güvenli, hızlı ve ucuz bir işlem mekanizması sağlayabilmesi sanal para birimleri için büyük bir avantaj olsa da hâkim para birimi haline gelmesi şu an için uzak bir seçenektir. Ancak hiperenflasyon, mali kriz, siyasal çalkantı veya savaş dönemleri gibi durumlarda, para ikamesi haline gelebilmesi mümkün görünmektedir (Dabrowski ve Janikowski, 2018, s. 5). 2017 yılında Zimbabwe’de yaşanan darbe gibi olaylar ile hiperenflasyonun etkilerine bağlı olarak ortaya çıkan ekonomik belirsizlikler, halkın yerel para birimine olan güveninin azalması ve bir merkezi olmayan dönüştürülebilir sanal para birimi ve bir kripto para birimi olan Bitcoin kullanımının yaygınlaşması sonucunu doğurmuştur (Güven ve Şahinöz, 2021, s. 34).

Aşağıda yer alan Şekil 1.2.’de gösterildiği gibi sanal paralar, dönüştürülemez (kapalı) sanal para birimleri ve dönüştürülebilir (açık) sanal para birimleri olmak üzere, dönüştürülebilir sanal paralar ise merkezi sanal para birimleri ve merkezi olmayan sanal para birimleri şeklinde iki kategoriye ayrılmaktadır (FATF, 2014, ss. 4-5).



Şekil 1.2. Sanal paranın sınıflandırılması (FATF, 2014, ss. 4-5)

İtibari para ile değiştirilemeyen *dönüştürülemez sanal para birimleri*, yalnızca belirli bir sanal ortamda transfer edilebilmekte ve belirli bir sanal alana özgü şekilde belirli kurallar çerçevesinde kullanılmaktadır. Söz konusu kuralları belirleyen, sistemi kurgulayarak kontrol eden bir merkezin bulunduğu dönüştürülemez sanal para birimleri doğası gereği merkezi bir yapıdadır. Çevrimiçi oyunlar veya alışveriş siteleri gibi platformlarda kullanılan ve itibari paraya dönüştürülerek resmi finans sektörüne taşınamayan sanal paralar dönüştürülemez sanal paralara örnek olarak verilebilmektedir. Doğrudan veya sanal para borsası aracılığıyla gerçek bir para birimi ile karşılıklı olarak değiştirilebilen *dönüştürülebilir sanal para birimleri*, merkezi ve merkezi olmayan sanal paralar olarak ikiye ayrılmaktadır. Merkezi sanal para birimlerinde bir üçüncü taraftan bahsedilebilirken merkezi olmayan sanal para birimlerinde herhangi bir aracı veya merkezi yapı bulunmamaktadır. Dönüştürülebilir sanal

paralar resmi finans sektörüne değer taşıyabildiğinden suç gelirlerinin aklanması ile terörizmin finansmanında kullanılması riskine sahip olduğu kabul edilmektedir (FATF, 2014, ss. 4-5). Merkezi bir yapının olmayışı sebebiyle kripto para olarak adlandırılan merkezi olmayan sanal para birimlerinde ise bu riskin daha fazla olduğu değerlendirilmektedir.

Günümüz ile geleceği anlayabilmek adına geçmişi incelemenin önemli olduğu düşünüldüğünden, bu bölümde paranın tarihine ilişkin kısa bir anlatı sunulmaya çalışılmıştır. Trampa sisteminin yetersiz kalması sonucu kullanılmaya başlanan para tarih boyunca çeşitli dönüşümlere uğramıştır. Değeri kendisine içkin olan mal paralardan günümüzün tartışma konusu kripto paralara uzanan süreçte ekonomik, toplumsal, kültürel ve teknolojik gelişmelere paralel şekilde paranın evrim geçirdiği görülmektedir. Mal para, madeni para, kâğıt para olarak da adlandırılan temsili ve itibari paranın somut formuna karşılık olarak; kaydi para, dijital para, elektronik para, sanal para ve son olarak kripto para şeklinde paranın giderek daha soyut ve merkeziyetsiz bir hal aldığı anlaşılmaktadır. Kripto paraları içine alan kripto varlıklar ile dayandığı teknoloji olan Dağıtık Defter Teknolojisi (*Distributed Ledger Technology*-DLT)'nin en yaygın kullanım şekli blokzincirin ortaya çıkış süreci, tanımları, teknik altyapısı ve özellikleri sonraki bölümde detaylandırılacaktır.

1.2. Blokzinciri Teknolojisi

Dünya üzerindeki etkileşimin artması sonucunda özellikle ekonomik düzlemde oluşan karşılıklı bağımlılık şeklinde karakterize edilen küreselleşme, dünya ekonomisini kontrolü güç ve karmaşık bir yapıya dönüştürmesi sebebiyle 2008 Küresel Krizi'ne yol açan gelişmelerden biri olarak kabul edilmektedir. Son olarak Bretton Woods Sistemi'nin yıkılmasıyla dünyadaki para arzını kontrol edecek ve sınırlayacak bir mekanizmanın kalmaması, parasal dengesizliklere ve ekonomik istikrarsızlığa sebep olmuştur (Çağlar ve Dışkaya, 2018, ss. 1-24). Küresel ekonomik krizlerin, hükümetlerin ve finans kuruluşlarının meşruiyetine zarar verdiği ve güvensizlik ortamı oluşturduğu bilinmektedir. Kripto varlıkların dayandığı dağıtık defter teknolojisinin en yaygın kullanım şekli olan blokzinciri, 2008 Küresel Krizi sırasında söz konusu güvensizlik ortamında yeşermiş ve karşılıklı güvensizlik temelinde ortak bir güven oluşturarak yeni bir güven mimarisi inşa etmiştir (Werbach, 2021, s. 18).

Blokzinciri, insani etkileşimlerde her zaman var olduğu kabul edilen *karşı taraf riski* için çözüm olmuştur. Karşı taraf riskinden kaynaklanan güven bunalımına çözüm olarak merkezi otorite ve aracı kurum gibi güvenilir bir üçüncü tarafın sağladığı kısmi güveni, kalabalıkların mutabakatına dayalı ve merkeziyetsiz yapısıyla mutlak güvene dönüştürmüştür (Güven ve Şahinöz, 2021, ss. 167-184). Güven zaten yapının bir parçası olduğundan blokzinciri, başka bir şeye itimat gereği kalmaksızın insanlar arasında koşulsuz güven sağlamaktadır (Williams, 2020, ss. 86-90). En basit haliyle dağınık yapıda oluşturulan dijital bir kayıt defteri olduğu söylenebilen blokzincirinde oluşturulan kayıtları silmek veya değiştirmek neredeyse imkânsız olduğundan dijital veriler ağda güvenli şekilde saklanabilmektedir (Başaranel, 2021, s. 261). Taraflar, birbirleri veya bir merkez yerine ağın kendisine ve paylaşılan dağınık bir deftere kaydedilen bilgilere güvendiğinden, işlemlerde üçüncü bir tarafa olan ihtiyaç ortadan kalkmaktadır.

Hesaplama ve iletişim teknolojileri üzerine kurulu *bilgi internetinden değer internetine* geçiş, güvenilir bir üçüncü taraf olmaksızın değer transferinin mümkün hale gelmesi ile yaşanmıştır. Mutlak güven teknolojisi üzerinde gerçekleşebilen değer transferi sayesinde günümüzde, bankacılık, sağlık, eğitim, turizm, emlak gibi çok çeşitli sektörlerdeki iş modellerini kökten değiştirebilecek tam teşekküllü bir dijital ekonomi söz konusudur (Güven ve Şahinöz, 2021, ss. 160-185). Kripto para birimleri ve kripto varlıklar ile iç içe geçmiş bir kavram haline gelen blokzinciri teknolojisi, hayatın çok farklı alanlarında büyük dönüşümlere yol açması beklenen değerli bir teknoloji olarak değerlendirilmektedir.

2008 yılında gerçek kimliği veya kimlikleri bilinmeyen Satoshi Nakamoto lakaplı bir şahsın veya şahısların “*Bitcoin: A Peer-to-Peer Electronic Cash System (Bitcoin: Eşten-eşe Elektronik Nakit Ödeme Sistemi)*” başlığıyla yayınladığı yazı, dünyayı merkezi olmayan bir sanal para birimi sistemi ile tanıştırmıştır. Yazıda, blokzinciri (blockchain) ifadesinin doğrudan kullanılmamasına karşılık, kripto para birimi olan Bitcoin’in üzerine inşa edildiği blokzinciri teknolojisi teknik açıdan incelenmiştir (Nakamoto, 2008). Hayatın çeşitli alanlarında geleneksel düzeni bozarak devrim yaratma potansiyeline sahip olan blokzinciri, heyecan verici bir teknolojik gelişme olarak son yıllarda dünyada yakından takip edilen konulardan biri haline gelmiştir. Esasında tamamen yeni bir teknolojik gelişme olmayıp neredeyse tüm teknik bileşenleri 1980’ler ve 1990’lardaki akademik araştırmalardan kaynaklanmıştır (Narayanan ve Clark, 2017, s. 1).

İşlemlerin farklı ağ katılımcılarından oluşan dağıtılmış bir ağda kaydedilmesine ve paylaşılmasına imkân tanıyan dağıtık defter teknolojisinin belirli bir alt türü olan blokzinciri teknolojisi, dijital bir “*zincir*” içinde birbirine bağlı “*blok*”larda veri depolayan ve verileri bir ağ genelinde değişmez bir şekilde kaydetmek ve senkronize etmek için kriptografik ve algoritmik yöntemler kullanan bir teknoloji olarak karşımıza çıkmaktadır. Zaman zaman birbirleri yerine kullanılan ve birbirleri ile ilişkili olan blokzinciri teknolojisi ve dağıtık defter teknolojisinin farklı kavramlar olduğu, tüm dağıtık defterlerin blokzinciri kullanmadığı, blokzincirinin belirli bir dağıtık defter teknolojisi türü olduğu ve yalnızca bir blokzinciri veri yapısı kullanan dağıtık defterlere atıfta bulunduğu unutulmamalıdır (The World Bank, 2017, ss. 1-2). Blokzinciri teknolojisi gibi birçok dağıtık defter teknolojisi örneği mevcuttur. Bunlardan bazıları, blokzinciri teknolojisinin hız ve ölçeklenebilirlik açısından yeterli olmadığını görülmesi sebebiyle geliştirilen Hashgraph, Tangle, Holochain ve Tempo dağıtık defter teknolojileridir (Şafak vd., 2021, ss. 36-40).

Basitçe blokzincirin, her tür verinin izlenebileceği çevrimiçi bir kayıt defteri olduğu söylenebilir. Tasarımının bir parçası olarak bilgileri değişmez bir şekilde depolayabilme yeteneğine sahip olan blokzinciri, ilk yaygın uygulaması olan Bitcoin gibi kripto para birimlerine ilişkin işlemleri kayıt altına alarak kripto paraları olanaklı kılmaktadır (Williams, 2020, ss. 20-28). Kripto para birimleri blokzincirine bağlı olsa da blokzincirinin tek uygulaması değildir. Kripto para birimlerinin ötesinde çeşitli uygulamalara sahip olan blokzinciri, kaynak takibi ve dijital varlık yönetimi gibi amaçlar için çok çeşitli sektörlerde kullanılabilmektedir (Fleming, 2021). Blokzinciri; ev, araba, para gibi somut varlıkların veya fikri mülkiyet, patentler, telif hakları gibi soyut varlıkların dağıtılmış ve değiştirilemez bir defterde izlenmesi ile alınıp-satılması sürecini kolaylaştırarak risk ve maliyetleri azaltmaktadır (*What is blockchain technology?*, IBM). Dolayısıyla blokzinciri varlıkların izlenmesi ve işlemlerin kaydedilmesi açısından finans, tedarik zinciri yönetimi, sağlık, emlak, fikri mülkiyet gibi çeşitli sektörlerde potansiyel uygulama alanlarına sahiptir.

Blokzinciri, “*düğüm (node)*” adı verilen bilgisayarlar arasında paylaşılan ve senkronize edilen dijital bir veri tabanıdır. Düğümlerin farklı eşler olarak hizmet verdiği ve her düğümün veri tabanının bir kopyasına sahip olduğu eşler arası bir ağ olarak düşünülebilen blokzincirinde veri tabanının içeriği üzerinde anlaşmak için bir mutabakat algoritması kullanılmaktadır (Finck, 2019, s. 3). Blokzinciri merkezi bir yapıda olmayıp dağıtık yapıdadır (Başaranel, 2021, s. 260), işlemleri doğrulamak ve defterin bütünlüğünü

korumak için merkezi bir otorite veya yönetim organı yerine birlikte çalışan bir düğüm ağına dayanmaktadır. Bu merkezi olmayan mimari blokzincirini saldırılara veya manipülasyona karşı dayanıklı hale getirmektedir. Ayrıca blokzinciri ağında eş zamanlı olarak kayıt tutabilen düğümler, aynı yetki seviyesinde ve eşit kabul edildiğinden, blokzinciri hiyerarşik bir sistem yerine internet bağlantısı olan herkesin erişebileceği şeffaf ve demokratik bir sistem oluşturmaktadır.

Blokzincirinin çalışma süreci sayesinde kayıtların dağıtık ve şeffaf bir şekilde tutulması ve paylaşılması sağlanmaktadır. Blokzincirinin ana çalışma süreci şu şekilde özetlenebilir (Iuon-Chang ve Tzu-Chun, 2017, s. 654):

- 1) Gönderici bir düğüm yeni verileri toplayarak bu verileri içeren bir blok oluşturduktan sonra söz konusu bloğu ağına yayımlar.
- 2) Alıcı düğümler, alınan bloğu ve verilerini kontrol eder. Blok geçerli ise alıcı düğümler bloğu kabul eder.
- 3) Zincirdeki her düğüm bloğun doğruluğunu teyit etmek için “iş ispatı (*Proof of Work-PoW*)” ve “pay ispatı (*Proof of Stake-PoS*)” gibi veya başka bir mutabakat algoritması uygular.
- 4) Mutabakat algoritması yürütüldükten sonra blok zincirde depolanır. Ağdaki tüm düğümlerin yeni bloğu kabul etmesiyle blokzincirinin tabanı bu blok üzerinde genişlemeye devam eder.

Blokzincirinde, her kaydın zaman damgası olacak şekilde veriler sıralı bir biçimde bloklara kaydedilmekte ve bu bloklar birbirine “Hash” fonksiyonu ile zincir şeklinde bağlanmaktadır. Her blok bir dizi işlem, bir zaman damgası ve benzersiz bir kriptografik Hash içermektedir. Hash fonksiyonu, verilerin özgünlüğünü kanıtlamak ve dijital parmak izini oluşturmak için kullanılan benzersiz bir özet değer olarak ifade edilebilir. Bir blok tamamlandığında oluşturulan Hash değerinin bir sonraki bloğun girdilerinden biri olması, zincirin değiştirilemez olmasını sağlamaktadır. Bir bloğun oluşturulması için gerekli olan uygun Hash değerinin hesaplanması ve bloğu oluşturma karşılığında ödül kazanmak amacıyla blokzinciri aktörlerinden biri olan madenciler yarışmaktadır. Blok için doğru Hash değerini üretmeyi başaran madenci, yeni oluşturulan kripto para birimi ile ödüllendirilmektedir. Madenciler yeni kripto para birimi üretmenin yanı sıra blokların

oluşturulması ve doğrulanmasını sağlayarak sistemin sürekliliği ve işlevselliğinde çok önemli bir rol oynamaktadır (Güven ve Şahinöz, 2021, ss. 44-65).

Blokszinciri, işlemlerin güvenliğini ve şeffaflığını sağlayan bir *mutabakat algoritması* oluşturarak üçüncü bir tarafın güvenlik ve doğrulamayı sağlamasına ihtiyaç olmadan iki taraf arasında doğrudan ürün veya hizmet transferi işlemlerini mümkün kılmaktadır (Tanrıverdi vd., 2019, s. 204). Güven protokolü olarak da bilinen mutabakat algoritmasının, blokszincirin bütünlüğünü ve güvenliğini koruyan bir mekanizma olduğu söylenebilir. Çeşitli blokszinciri sistemleri tarafından kullanılan farklı mutabakat algoritmaları olmakla birlikte iş ispatı ve pay ispatı en yaygın iki yöntemdir (Güven ve Şahinöz, 2021, s. 75). Mutabakat algoritmaları temelde işlemlerin şeffaf ve kurcalamaya karşı dayanıklı bir şekilde doğrulanması ve kaydedilmesi amacıyla hizmet etmektedir. Blokszinciri üzerine yeni verilerin eklenerek güncellenmesi ve herhangi bir uyuşmazlık veya güvenlik sorununun çözümü için, salt çoğunluğun onayı olmaksızın zincire yeni veri eklenmesini engelleyen ortak bir veri güncelleme protokolü üzerinde tüm düğümlerin anlaşmaları gerekmektedir (Tanrıverdi vd., 2019, s. 208).

Verilerin doğruluğunu kanıtlamak için kullanılan iş ispatı yönteminde madenciler hesaplama gücü ile birbirleriyle yarışmaktadır (Güven ve Şahinöz, 2021, s. 78). Her blokta “*Nonce*” adı verilen rastgele bir değer bulunmaktadır ve iş ispatında Nonce değeri deneme yanılma yöntemi ile değiştirilerek, blok başlığı Hash değerini önceden ayarlanmış bir *zorluk hedefinden* daha düşük yapan bir değer oluşturulmaya çalışılmaktadır (Luon-Chang ve Tzu-Chun, 2017, s. 654). Hash değerine ilk ulaşan madenci zincire yeni bloğu eklemeye hak kazanmakta ve ağdaki tüm düğümlerden doğruluk onayı alınmasının ardından blok zincire eklenmektedir. Bloğu yayınlayan madenci işlem sonunda ödüllendirilmektedir (Tanrıverdi vd., 2019, s. 209). Bitcoin blokszincirinin kullandığı iş ispatı mutabakat algoritmasında, ağ tarafından ayarlanan zorluk hedefi nedeniyle yüksek miktarda bilgi işlem gücü ve elektrik enerjisi kullanılması eleştirilere neden olmaktadır. Ancak zorluk hedefinin aynı zamanda manipülasyon ve saldırılara karşı blokszincirinin dayanıklılığını arttırdığı düşünülmektedir.

Pay ispatı yönteminde madenciler bir değerın sahipliğini kanıtlamak durumundadır (Tanrıverdi vd., 2019, s. 209). Bu protokolde, bir madencinin blok oluşturmakla görevlendirilme olasılığı sistemde elinde bulunan pay miktarı ile doğru orantılıdır. Pay ispatı yönteminde oluşturulan blok için madenci ödül kazanmamakta, yalnızca blok içindeki

işlemlerin komisyonunu kazanmaktadır (Güven ve Şahinöz, 2021, s. 78). İş ispatı yöntemine kıyasla bu yöntemde daha az elektrik ve bilgi işlem gücüne ihtiyaç duyulmaktadır. Pay ispatı yönteminin ağa yapılacak kötü niyetli saldırılara karşı çalışma mantığından ötürü daha fazla koruma sağlayabileceği (Iuon-Chang ve Tzu-Chun, 2017, ss. 654-655) veya madencilik (mining) maliyetinin sıfıra yakın olmasından dolayı ağa yapılacak saldırılara karşı daha savunmasız durumda kalabileceği (Tanrıverdi vd., 2019, s. 209) şeklinde zıt görüşler mevcuttur. Bitcoin gibi bir kripto para birimi olan Ethereum, pay ispatı mutabakat algoritmasını benimsemek üzere tasarlanmışsa da geçiş henüz sağlanamadığından mevcut sürümü iş ispatı mutabakat algoritmasını kullanmaktadır.

Blokszinciri teknolojisi altında beş temel ilke yatmaktadır (Harvard Business Review Press, 2021, s. 20):

- 1) Dağıtık (merkeziyetsiz) yapısı sayesinde blokszinciri, merkezi olmayan şeffaf veri yönetimi sağlayarak üçüncü taraf araçlara olan güven ihtiyacını ortadan kaldırmaktadır. Blokszincirindeki taraflardan her biri veri tabanının tamamına ve geçmişine erişerek mutabakat mekanizması aracılığıyla doğrudan kendi işlem ortaklarının kayıtlarını doğrulayabilmektedir.
- 2) Eşler arası (*peer to peer*-P2P) aktarım mekanizması sayesinde blokszinciri ağında iletişim, doğrudan doğruya taraflar arasında gerçekleşmektedir ve bilgi akışını kontrol eden merkezi bir düğüm veya hiyerarşik bir yapı bulunmamaktadır. Ağdaki her bir düğüm veri tabanının bir kopyasını saklamakta ve bilgileri diğer düğümlere iletmektedir.
- 3) Şeffaflık, blokszincir ağında her işlem ve değerinin sisteme erişimi olan herkes tarafından izlenebilmesi anlamına gelmektedir. Ağdaki işlemler her düğümün sahip olduğu alfanümerik blokszinciri adresleri arasında gerçekleşmektedir. Kullanıcılar anonim kalma veya kimliklerini başkalarına kanıtlama seçeneğine sahiptir.
- 4) Kayıtların geri çevrilemezliği, işlemlerin blokszincirine kaydedildikten sonra değiştirilemeyeceği veya silinemeyeceği anlamına gelmektedir. İşlem veri tabanına girip hesaplar güncellendiğinde kendisinden önceki işlem kayıtlarının her biriyle bağlantılandırılmış olduğundan kayıtlar değiştirilememektedir. Çeşitli hesaplama algoritma ve yaklaşımları kullanılarak veri tabanındaki

kayıtların kalıcı, kronolojik sıralı ve ağdaki tüm katılımcılar tarafından erişilebilir olması sağlanmaktadır.

- 5) Blokzinciri işlemleri bilgisayarımsal mantığa bağlanabilmekte ve özü itibarıyla programlanabilmektedir. Kullanıcılar düğümler arasında işlemleri otomatik olarak tetikleyen algoritma ve kurallar oluşturabilmektedir. Önceden tanımlanmış koşullar karşılandığında kendi kendini yürüten akıllı sözleşmeler, araçlara veya manuel müdahaleye ihtiyaç duymadan işlemlerin güvenli, şeffaf ve otomatik olarak yürütülmesini sağlamaktadır.

Blokzinciri teknolojisinin avantajları; ağdaki tüm paydaşların verilerin bir kopyasına sahip olmasıyla veri kaybının önlenmesi, dijital imzalar ve doğrulamaların araçlara olan ihtiyacı ortadan kaldırmasıyla paydaşlar arasında güven oluşturması, paydaşların tüm işlemlerin durumunu ve ayrıntılarını görmesiyle şeffaflık sağlanması, verilerin silinememesi veya değiştirilememesi, merkeziyetsiz doğası sayesinde kontrol veya iptal edilememesi, akıllı sözleşmelerin kodlanmasıyla belirli etkinlik ve süreçlerin otomatikleştirilebilmesi olarak sayılabilmektedir. Dezavantajları ise; iş ispatı mutabakat protokolü kullanılan blokzincirlerinde yoğun enerji tüketimi, her düğümün verileri ayrı ayrı depolaması ve her işlem sonrası düğümlerdeki verilerin tutarlılığının sağlanması dolayısıyla geleneksel veri tabanlarına kıyasla performansının yetersiz kalabilmesi, blokzincirinin şeffaf mimarisinin kullanıcı gizliliğine zarar verebilmesi, akıllı sözleşmelerin oluşturulduktan sonra değiştirilememesi dolayısıyla saldırılara karşı savunmasız bırakılabilmesi olarak ifade edilebilmektedir (Tanrıverdi vd., 2019, ss. 204-205).

Blokzincir sistemleri temelde; genel, özel ve konsorsiyum blokzincirleri olarak üç kategoride sınıflandırılmaktadır (Puthal vd., 2018, ss. 11-12):

- 1) İzinsiz blokzincirleri olarak da adlandırılan genel blokzincirleri, ağdaki her katılımcının tüm işlemleri görüntülemesine ve doğrulamasına olanak tanımakta olup herkesin katılımına açıktır. Bitcoin ve Ethereum gibi kripto para birimlerinin temelini oluşturan (Iuon-Chang ve Tzu-Chun, 2017, s. 655) genel blokzincirlerindeki işlemler tüm düğümler tarafından onaylanmakta ve bu düğümler blokzincirinin bir kopyasını bulundurmaktadır. Bu sayede kayıtların değişmediği, merkezi veya hiyerarşik bir yapının bulunmadığı bir sistem sağlanmaktadır.

- 2) İzinli blokzincirleri olarak da adlandırılan özel blokzincirleri, ağdaki katılımcıların işlemleri doğrulama ve blokzincirine yeni bloklar eklemek için özel bir izne sahip olduğu sınırlı sayıda katılımcıya açık olan sistemlerdir. Erişimi kontrol eden ağ veya kurallar tarafından düğümlerin sisteme katılmasına karar verilmekte ve ağın bir parçası olduğunda düğümler blokzincirinin bir kopyasını bulundurarak ve güncelleme için iş birliği yaparak merkezi bir ağın yürütülmesine katkıda bulunmaktadır.
- 3) Kısmen izin verilen blokzincirleri olarak düşünülebilen konsorsiyum blokzincirleri, merkezi olmayan genel blokzincirleri ve merkezi olan özel blokzincirlerinin aksine seçilen bazı doğrulayıcı düğümlerin kontrolü sayesinde kısmen merkezi yapıdadır. Konsorsiyum blokzincirlerinde tek bir organizasyon blok doğrulamasından sorumlu olmayıp fikir birliği önceden belirlenmiş düğümler tarafından sağlanmakta ve bu düğümler ağa kimin katılacağına ve madencilik yapacağına karar vermektedir. Hyperledger ve R3CEV konsorsiyum blokzincirlerine örnektir (Iuon-Chang ve Tzu-Chun, 2017, s. 655).

Blokzinciri teknolojileri sadece finansal uygulamalarda değil, aynı zamanda Nesnelerin İnterneti (*Internet of Things-IoT*), tedarik zinciri yönetimi, oylama sistemleri, sağlık sektörü ve depolama gibi birçok alanda kullanılabilmektedir (Iuon-Chang ve Tzu-Chun, 2017, s. 653). Blokzinciri; kripto paraların oluşturulması ve kullanılmasında, eşler arası doğrudan değer transferinde, Ethereum blokzinciri ile blokzinciri üzerinde kod şeklinde oluşturulan ve kendi kendini yürüten akıllı sözleşmelerde, olağan şekilde akdedilen sözleşmeler ile birlikte diploma ve sertifika gibi belgelerin blokzincir üzerinde üretilmesi ve saklanmasında, nesneler arası internet üzerindeki iletişimi ve işlemleri ifade eden nesnelerin internetine entegrasyonda, bir kripto para projesi veya blokzinciri tabanlı uygulamanın finansmanını sağlamak için gerçekleştirilen kitle fonlaması yöntemi olan ICO (*Initial Coin Offering*) şeklinde ilk kripto varlık arzının sağlanmasında, blokzinciri üzerinde üretilen eşsiz ve tekil kripto varlıklar olan Nitelikli Fikrî Tapu (*Non-Fungible Token-NFT*)'ların saklanması ve satılması gibi türlü işlemlere konu edilmesinde, bir güven kurumu olarak hizmet veren noterlik işlemlerinde olası sektörel kullanım alanlarına sahiptir (Tevetoğlu, 2021, ss. 30-40). Tüm potansiyel kullanım alanları henüz keşfedilmeyen blokzinciri teknolojisi gelişme aşamasında olup devam eden araştırmalar sonucu yeni kullanım alanlarının keşfedilmesi kaçınılmaz olacaktır.

Özetle blokzinciri teknolojisi, merkezi olmayan dağıtık yapısı sayesinde güvenli ve şeffaf bir veri yönetimi ile veri transferi sağlamaktadır. Blokzinciri, iş ispatı ve pay ispatı gibi bir mutabakat algoritması kullanarak çalışmaktadır. Blokzinciri, işlemlerin güvenli, şeffaf ve doğrulanabilir şekilde merkezi araçlar kullanılmadan doğrudan iki taraf arasında gerçekleştirilmesini mümkün kılmaktadır. Blokzinciri teknolojisi; dağıtık yapı, eşler arası aktarım, şeffaflık, kayıtların geri çevrilmezliği ve bilgisayarımsal mantık (programlanabilirlik) gibi ilkelere dayanmaktadır. Blokzinciri teknolojileri finansal uygulamaların yanı sıra birçok sektörde kullanılabilmektedir; sağlık, gayrimenkul ve diğer endüstrilerdeki veri işleme ve kayıt tutma süreçlerinin güvenli, şeffaf ve verimli bir şekilde yönetilmesi için potansiyel kullanım alanları sunmaktadır.

1.3. Kripto Varlık Kavramı

1.3.1. Getirilen Tanımlar

Düzenleyici alanda genel olarak, kripto varlık ve kripto para terimlerinin tanımlarının oluşturulmasından kaçınıldığı ve kripto para birimlerine, dijital paranın veya sanal paranın bir biçimi veya alt kümesi olarak yaklaşıldığı görülmektedir (Houben ve Snyers, 2018, ss. 20-22) . Üzerinde anlaşarak genel kabul görmüş bir tanımla bulunmamakla birlikte kripto varlık ve kripto para birimlerine ilişkin getirilen bazı tanımlara aşağıda yer verilmiştir.

16 Nisan 2021 tarihli ve 31456 sayılı Resmî Gazete’de yayımlanan Türkiye Cumhuriyet Merkez Bankası tarafından *Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik* (2021)’te kripto varlık, “*dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıklar*” olarak tanımlanmıştır. Söz konusu Yönetmelik ile birlikte Türkiye’de kripto varlıkların, doğrudan veya dolaylı şekilde ödemelerde kullanılması veya kullanılmasına yönelik hizmet sunulması yasaklanmıştır.

FATF, sanal varlık kavramı üzerinden atıfta bulunduğu kripto varlıkları; “*dijital olarak alınıp satılabilen veya transfer edilebilen ve ödeme veya yatırım amacıyla kullanılabilen, değerini dijital bir temsil*” olarak tanımlamış ve kripto varlıkların, itibari para birimlerinin, menkul kıymetlerin ve diğer finansal varlıkların dijital temsillerini içermediğini

vurgulamıştır (FATF, 2021a, s. 109). Avrupa Merkez Bankası (2019, s. 3) ise kripto varlıkları, *“dijital biçimde kaydedilen ve herhangi bir tanımlanabilir varlık üzerinde finansal bir hak talebi veya yükümlülüğünü temsil etmeyen ve kriptografi kullanımıyla etkinleştirilen yeni bir varlık türü”* olarak tanımlamıştır. Kripto varlıklar kripto para birimlerinin yanı sıra Menkul Kıymet Token’ı (*Security Tokens*) ve Fayda Token’ı (*Utility Tokens*) gibi para birimi olmayan yani para birimi işlevinden ziyade farklı amaçlarla kullanılan varlıkları da içermektedir (World Bank, 2022, s. 17). Kripto varlık şemsiye bir kavram olup (Blandin vd., 2019, s. 15), kripto para bu kavramın altında yer alan bir alt kategoriyi ifade etmektedir. Tüm kripto para birimleri aynı zamanda bir kripto varlık iken, tüm kripto varlıklar bir kripto para birimi olmayabilir (Global Blockchain Business Council, 2020, s. 4).

Dünya Bankası (*The World Bank*) (2022, s. 17) kripto para birimlerini, *“yasal olarak para veya para statüsüne sahip olmayan ancak gerçek ve tüzel kişiler tarafından değişim aracı olarak kabul edilebilen, elektronik ortamda transfer edilebilen, saklanabilen ve alım satımı yapılabilen bir dijital para birimi sınıfı”* olarak tanımlamış ve kripto para birimlerinin merkeziyetsizliğini vurgulamıştır. Kripto para hem sanal para hem de dijital para sınıfına girmektedir. Kripto para, merkeziyetsiz doğası ve kriptografi teknikleri kullanması yönüyle sanal para ve dolayısıyla dijital para içerisinde ayrı bir alt kategoride gruplanmaktadır.

FATF (2014, ss. 4-5) ise kripto para birimlerine sanal para birimlerinin bir alt kümesi olarak yaklaşmıştır. FATF, sanal paraları, gerçek para biriminde eşdeğer bir değere sahip olan ve gerçek para birimiyle karşılıklı olarak değiştirilebilen dönüştürülebilir sanal para ile dönüştürülemez sanal para olmak üzere ikiye ayırırken dönüştürülebilir sanal paraları, sistemi kontrol eden merkezi bir idari otoriteye sahip merkezi sanal para ile hiçbir merkezi gözetime sahip olmayan merkezi olmayan sanal para şeklinde ikiye ayırmış ve merkezi olmayan sanal para birimlerini kripto para olarak adlandırmıştır. FATF’e göre Bitcoin, Litecoin ve Ripple’ın örnek olarak verilebileceği kripto para birimleri; *“dağıtık, açık kaynaklı, matematik tabanlı, merkezi yönetim yetkisi ve merkezi izleme veya gözetimi olmayan eşler arası sanal para birimleri”* olarak tanımlanmıştır. Dağıtık terimi, her işlemin, işlemi doğrulamak için algoritmayı çalıştıran bir katılımcı ağı arasında dağıtıldığı anlamına gelmektedir. Diğer bir ifadeyle işlemler dağıtılmış bir mutabakat algoritması tarafından doğrulanmaktadır.

İşlemleri güvence altına almak ve doğrulamak için kriptografi ile korunan matematik tabanlı, merkezi olmayan, dönüştürülebilir sanal paraları ifade eden kripto paralar; eşten eşe değer transferi için her transferde kriptografik olarak imzalanmak suretiyle genel ve özel anahtarlara dayanmaktadır. Kripto para işlemlerinin bütünlüğü ve güvenliği, katkılarından dolayı yeni oluşturulan para birimleriyle veya işlem komisyonlarıyla ödüllendirilen, genellikle madenciler olarak adlandırılan karşılıklı olarak güvensiz taraflardan oluşan bir katılımcı ağı tarafından sağlanmaktadır. Bitcoin, tam anlamıyla uygulanan ilk kripto para protokolünü ortaya koymuştur (FATF, 2014, s. 5).

1.3.2. Ortaya Çıkış Süreci ve Benimsenmesi

Bitcoin'in ortaya çıkışından önce gizlilik ve güvenlik konularında kripto para birimlerinin gelişmesine ilham verdiği düşünülen çeşitli çalışmalar olduğu bilinmektedir. Kripto para birimlerinin öncüsü olarak kabul edilen Digicash'in geliştiricisi, kriptografi ve bilgisayar güvenliği alanında ünlü matematikçi ve bilgisayar bilimcisi David Chaum, gizlilik ve güvenlik konularında yaptığı çalışmaları ve katkıları ile tanınmaktadır. David Chaum (1982, s.II) yazdığı tezde, karşılıklı şüpheli gruplar tarafından kurulan ve sürdürülen, bu grupların güvenebileceği yüksek güvenlikli dağıtılmış bir bilgisayar sisteminin tasarımını tanımlamasıyla blokzincirinin temel prensiplerinin adımı atılmıştır.

David Chaum fiziksel güvenlikle bireysel mahremiyeti koruyan, grup üyeliği tutarlılığı ve özel işlem hesaplamalarıyla halka açık bir kayıt tutma sistemi önermiştir. Önerdiği sistem; simetrik ve asimetrik şifreleme, dijital imzalar gibi kriptografik öğeler ile fiziksel olarak güvenli kasalar ve Chaum tarafından tanıtılan gizli paylaşım esasına dayanmaktadır. Bireysel mahremiyete ulaşmak için farklı yaklaşımlar geliştirmeye çalışan David Chaum'un 1982 yılındaki çalışması, konferans veya dergide yayınlanmaması sebebiyle büyük ölçüde fark edilmemiştir (Sherman vd., 2019, s. 73).

David Chaum (1983, ss. 199-203) makalesinde, mevcut sistemlere kıyasla daha fazla denetlenebilirlik ve kontrol imkânı sunduğu ve aynı zamanda kişisel mahremiyeti artırarak izlenemez ödeme sistemlerinin gerçekleştirilmesine olanak tanıdığı iddiasındaki yeni bir kriptografi türü olarak "*kör imza*" sistemini tasarlamıştır. Bu teknikle ödemenin gerçekleştirildiği kişi, miktar veya zaman gibi bilgilerin üçüncü kişiler tarafından görülmesi

engellenerek kullanıcılar arasında gizlilik sağlanırken güvenli ödeme işlemleri gerçekleştirilebilecektir.

Temelleri söz konusu çalışmalara dayanan, merkezi bir otoriteye ihtiyaç duymadan dijital para birimlerinin anonim ve güvenli bir şekilde kullanılmasını sağlayan kriptografiye dayalı bir ödeme sistemi olan Digicash, 1989 yılında David Chaum tarafından kurulmuştur. Anonimlik ve güvenlik açıkları konusunda maruz kaldığı eleştiriler ile birlikte benimsenme sorunu nedeniyle Digicash başarısız olmuş ve piyasada sürdürülebilir bir varlık haline gelemeyerek zamanla etkisini kaybetmiştir (Clark, 2016, ss. 21-26). Ancak, Digicash'in geliştirilen diğer kripto para birimlerine ve dijital ödeme sistemlerine ilham verdiği ve kripto para dünyasının ilerlemesine katkı sağladığı unutulmamalıdır.

2008 yılında Satoshi Nakamoto tarafından Bitcoin'in temel prensiplerini ve çalışma mantığını detaylı bir şekilde açıklayan "*Bitcoin: A Peer-to-Peer Electronic Cash System (Bitcoin: Eşten-eşe Elektronik Nakit Ödeme Sistemi)*" başlıklı Bitcoin Whitepaper'ının yayınlanmasının ardından, 2009 yılında yine Satoshi Nakamoto tarafından Bitcoin için başlangıç noktası olarak kabul edilen Bitcoin'in ilk bloğu olan *Genesis Blok* oluşturulmuştur. Dünyanın en önemli finansal hizmet şirketlerinden biri olarak değerlendirilen Amerikan yatırım bankası Lehman Brothers'ın 2008 tarihindeki iflasıyla birlikte finansal kuruluşlara karşı oluşan güvensizlik ortamında ilk kripto para birimi olan Bitcoin'in ortaya çıkışı tesadüf olarak görülmemektedir. Bitcoin'in *güvenilen üçüncü taraflara* olan ihtiyacı ortadan kaldırma iddiası ile ortaya çıkışı, para sisteminin merkezileşmesinin yıkıcı etkilerine karşı bir tepki olarak değerlendirilmesine yol açmıştır. Bitcoin ile karşılaşan çok sayıda kişi giderek sayıları artacak şekilde, eski sistemden bu yeni bozulamaz algoritma tabanlı sisteme güvenmenin daha iyi olduğuna kanaat getirmiş ve Bitcoin'in sahip olduğu değer algısı zamanla gelişmiştir (Vigna ve Casey, 2020, ss. 66-103).

İlk merkezi olmayan dönüştürülebilir sanal para birimi ve ilk kripto para birimi olan Bitcoin'in değeri, kullanıcıların kendisi ile ödeme yapmaya istekli olmasından kaynaklanmaktadır (FATF, 2014, ss. 5-6). Bitcoin'in değeri genel olarak piyasa katılımcılarının ortak değer algısına dayanmaktadır (Dostov ve Shust, 2014, s. 253). Diğer kripto para birimleri gibi Bitcoin'in değeri kendisine atfedilen değere bağlı olup, atfedilen değer de Bitcoin'in ne derece paranın yerine geçtiği ile ilgilidir (Güven ve Şahinöz, 2021, s.

38). Kripto para birimlerinin para niteliğinin değerlendirilmesi, paranın fonksiyon ve özelliklerine sahip olup olmadığının incelenmesi ile yapılabilir.

Kripto para birimlerinin, daha öncesinde bahsedilen paranın değişim aracı, hesap birimi ve değer saklama fonksiyonlarını yerine getirmesi mümkündür. Ayrıca paranın özelliklerinden kolay taklit edilememesi, uzun ömürlü, taşınabilir, bölünebilir, standart ve homojen olması özelliklerini oldukça iyi bir şekilde karşılayan kripto paralar, paranın toplum tarafından kabul görmesi ve değer istikrarlı olması özelliklerini karşılamakta güçlük yaşayabilmektedir. Kripto para birimlerindeki büyük fiyat dalgalanmaları değer istikrarlı olması konusunda engel teşkil etmekte ve kripto paraların para yerine geçmesinin önündeki en önemli problemi oluşturmaktadır. Duyulan güven çerçevesinde her geçen gün artmaya devam etse de kripto paraların geniş ölçüde kabul edilebilirliği ise henüz tam anlamıyla sağlanamamıştır (Güven ve Şahinöz, 2021, ss. 38-39). Bu sebeplerle kripto paraların, para birimi olarak tanımlanması konusu kimi çevrelerce tartışılmakta ve paradan daha geniş bir kavram olan varlık olarak sınıflandırılması gerektiği savunulmaktadır. Bununla birlikte, genel olarak paranın üzerinde anlaşmaya varılan bir değeri temsil ettiği kabul edildiğinde, kripto paralar birtakım benzerlikleri nedeniyle para birimi olarak değerlendirilebilmektedir (Furneaux, 2018, s. 6). Kripto paraların, para birimi veya varlık şeklinde tasniflenmesi ayrı bir tartışma konusunu oluşturmakta olup devam eden çalışmalarla birlikte gelecekte daha fazla netlik kazanacağını söylemek mümkündür.

Kripto varlıkların arz ettiği bazı zorluklar kabul görmesi ile yaygınlık kazanmasının önünde engel teşkil etmektedir. Hata halinde blokzinciri üzerindeki işlemlerin değiştirilemezliği nedeniyle ortaya çıkan sorunlar gibi teknik problemler, nihayete ermeyen hukuki tartışmalar ve yasal düzenlemeler, kripto varlıklardaki değer istikrarsızlığı, kripto varlık alım-satım platformlarında yaşanan güvenlik zafiyetleri ile bunların medyaya yansımaları sonucu oluşan itibar kaybı, kripto varlıkların yasa dışı işlemlerde araç olarak kullanılmaya elverişli bazı özelliklere sahip olması gibi pek çok husus, kripto varlıkların tam anlamıyla kabul görmesi için zorluk oluşturmaktadır (Tevetoğlu, 2021, ss. 41-44). Kripto varlıkların kabul edilebilirliği, düzenleyici çerçevenin oluşturulması ve güvenlik önlemlerinin iyileştirilmesi gibi alanlarda yapılmakta olan çalışmalarla birlikte güven algısı çerçevesinde ve tanınırlığı ölçüsünde artmaya devam edecektir.

Sayılan zorlukların yanında doğasından kaynaklanan birtakım özellikleri kripto varlıkların geleneksel finansal sistemlere tercih edilerek kullanımının yaygınlaşması sonucunu doğurmaktadır. Her kripto varlığın kendine özgü özellikleri ve kullanım alanları olabileceği unutulmadan kripto paraların genel olarak; geleneksel sisteme alternatif olarak ortaya çıkan, bir merkezi otorite yerine kullanıcılar arasında doğrudan işlem gerçekleştirmeye olanak tanıyan, kriptografi mekanizması ile güvence altına alınan, takas aracı olarak kullanılabilen ve itibari para birimlerine karşılıklı olarak dönüştürülebilen değer dijital bir temsili olduğunu söylemek mümkündür (Houben ve Snyers, 2018, s. 23). Merkezi otoriteye bağımlı olmaksızın işlemlerin kullanıcıları arasında şeffaf ve güvenli bir şekilde gerçekleşmesini sağlayan ve kullanıcı kimliklerinin ifşa edilmeden işlem yapabilme imkânı sunan teknik mimarisi, kripto varlıkların benimsenmesini ve kullanılmasını teşvik eden önemli bir güven unsurunu oluşturmaktadır.

1.3.3. Teknik Unsurları

İnternet gibi elektronik iletişim biçimlerinin yaygınlaşmasıyla siber güvenlik artan bir önem kazanmıştır. Kurumsal veriler, e-posta mesajları, kredi kartı bilgileri gibi verileri korumak için kullanılan *kriptografi*, temel olarak, bilginin şifrelenerek okunamaz bir hale getirilip sadece gizli anahtara sahip olanların şifreyi çözebileceği şekilde bilginin korunmasını sağlamaktadır. Kriptografi, veri şifrelemenin yanı sıra gizlilik, bütünlük, inkâr edilemezlik şeklinde üç ana güvenlik temasını sağlamaktadır. Şifreleme işlemine tabi tutulmak suretiyle tamamen okunamaz hale getirilerek veri gizlenmekte, yetkisiz şekilde veya tespit edilmeden değiştirilmesinin önüne geçilmek suretiyle doğruluğu ve tutarlılığı korunarak veri bütünlüğü güvence altına alınmakta, sözleşmenin veya iletişimin taraflarının belge üzerindeki imzalarının gerçekliğini veya kendilerinden kaynaklanan bir mesajın gönderildiğini reddedememek suretiyle veri inkâr edilememektedir (Faulkner, 2016, ss. 5-8). Bu sayede gerçek ve tüzel kişiler hassas bilgilerini güvende tutabilmekte ve siber saldırılardan korunabilmektedir. Blokzincirinde kriptografi, kullanıcıların kimliklerinin korunması ile veri ve değerlerin güvence altına alınması için kullanılmaktadır (Atabaş, 2018, ss. 24-26). Kriptografi, kripto varlıklar ve blokzinciri gibi dağıtık defter teknolojilerinin güvenliği ve bütünlüğü için temel bir unsurdur.

Kullanıcıların kimliklerinin tespit edilmesine gerek olmadan kimlik doğrulanmasına imkân tanıyan asimetrik şifreleme veya açık anahtar şifreleme olarak bilinen kriptografi

yöntemi, blokzinciri üzerinde oluşturulan kripto paraların teknik altyapısının ayrılmaz bir parçasıdır. Açık anahtar şifreleme yöntemiyle her kullanıcının bir açık ve bir özel anahtarı bulunmaktadır. Özel anahtarı keşfetmek için kullanılamayan ve bu nedenle de açıkça paylaşılabilen açık anahtar, kullanıcının özel anahtarıyla çözebileceği bir mesajın şifrelenmesi için kullanılmaktadır. Bu işlemin tersi şekilde çalışan dijital imzalama tekniğinde ise; bir kişinin özel anahtarını kullanarak şifrelediği bir mesajı, bir başkasının o kişinin açık anahtarını kullanarak çözebilmesi, kullanıcıların taklit veya inkâr edilemeyecek şekilde bir mesajı veya dokümanı dijital olarak imzalamalarına imkân sağlamaktadır (Demartino, 2021, ss. 36-37). Veri güvenliğinin gizlilik ve doğruluk boyutları düşünüldüğünde, gizlilik için bilginin şifrelenmesi ve doğruluk için dijital imza hususları ile birlikte açık anahtar şifreleme yöntemi kripto paralarda önemli bir güvenlik katmanı sağlamaktadır (Güven ve Şahinöz, 2021, s. 45).

Kripto para cüzdanı, kripto para birimlerini tutmak, saklamak veya transfer etmek için kullanılan bir araçtır (FATF, 2014, s. 7). Blokzinciri ağında işlem gerçekleştirmek isteyen her kullanıcı kripto para cüzdanı kullanmak zorundadır. Her cüzdanın bir açık anahtarı ve bir özel anahtarı bulunmaktadır. Herkese gösterilebilen ve kripto para transferi almaya yarayan açık anahtar alfanümerik karakterlerden oluşmaktadır. Özel anahtar ise yine alfanümerik karakterlerden oluşan kullanıcıların kripto paraya erişimlerini ve kripto para üzerinde tasarruflarını sağlayan bir kod olarak temsil edilmektedir. Kripto para transferleri geri alınamadığından özel anahtarı güvenli bir şekilde saklamak önemli bir prensiptir (Demartino, 2021, s. 28). Özel anahtarın bilgisi depolanan kripto paranın kontrolünü ele geçirmek için yeterli olduğundan kripto para teknolojisi, sahibin hatası sonucunda özel anahtarı ele geçiren bir saldırgan ile meşru sahibi arasında bir ayrım yapmamaktadır (Lansky, 2018, s. 21).

Açık ve özel anahtarın saklanması kolaylaştıran cüzdanlar, kripto para birimi bakiyelerini görüntülemeye ve blokzinciri üzerinde işlem yapmaya izin vermektedir. Cüzdanlar genellikle, verileri cihazda bulunan özel olarak tasarlanmış bir sabit sürücüde depolayan fiziksel kasalar olan donanım cüzdanları ve bilgisayar veya telefonlara indirilebilen yazılım programları olan yazılım cüzdanları olmak üzere; yazılım cüzdanları ise, internete bağlı olduğunda sıcak cüzdan ve güvenli bir şekilde çevrimdışı olduğunda soğuk cüzdan olmak üzere iki temel kategoriye ayrılmaktadır. Donanım cüzdanları koruma ve güvenlik konusunda, yazılım cüzdanları hız ve erişim kolaylığı konusunda avantaj

sağlamaktadır (Suratkar vd., 2020). Özel anahtarın çevrimdışı ortamda tutulması çevrimiçi saldırılara karşı koruma sağlayabildiğinden dolayı soğuk cüzdanlar ve donanım cüzdanları daha güvenli bir seçenek olarak kabul edilmektedir. Öte yandan çevrimiçi platformlar ve kripto para borsalarıyla entegre olabilen sıcak cüzdanlar kullanıcılarına hızlı erişim ve kullanım kolaylığı sağlamaktadır. Kripto para cüzdan kullanıcıları ihtiyaçlarına ve risk toleranslarına bağlı olarak hangi cüzdan türünü tercih edecekleri belirlemektedir.

1.3.4. Kripto Varlık Ekosistemindeki Aktörler

Kripto varlıkların elde edilmesi, saklanması, erişilmesi ve transfer edilmesi etrafında inşa edilen iş modelleri, daha önce ödemeler ortamında bulunmayan belirli yeni aktör kategorilerini meydana getirmiş olup söz konusu aktörler aşağıda açıklanmıştır.

1.3.4.1. Kripto varlık kullanıcıları

Kullanıcı; çeşitli şekillerde kripto para birimi elde eden ve bunu mal ve hizmet satın almak ya da başka bir kişiye transfer göndermek için kullanan veya kripto para birimini yatırım amacıyla elinde bulunduran gerçek veya tüzel kişiyi ifade etmektedir (FATF, 2014, s. 7). Kripto varlık ekosistemindeki en önemli aktör olan kullanıcılar, kendi ihtiyaçları ve hedefleri doğrultusunda kripto para kullanma veya elinde tutma kararı vermektedir.

1.3.4.2. Madenciler

Madenciler, kripto para ile yapılan işlemleri doğrulayarak blokzincirine ekleyen ve bu işlemi genellikle gönüllü olarak gerçekleştiren, bazen bireysel bazense bir grubun güçlerini birleştirerek faaliyetlerini yürüttüğü madencilik havuzları şeklinde çalışanları ifade etmektedir. Madenciler işlemleri doğrulamak için bilgi işlem gücünden yararlanarak blokzinciri ağını desteklemekte ve çifte harcama veya hatalı işlemlerin önlenmesine yardımcı olmaktadır. İş ispatı mutabakat mekanizmasına dayanan kripto para birimleri ile ilgili olan madencilik sürecinde madenciler, çalışmalarının karşılığında otomatik şekilde yeni çıkarılan kripto paralar ile ödüllendirilmektedir. Ayrıca madenciler işlem başlatanlardan, kullanıcıların işlemlerini hızlandırmak veya önceliklendirmek istediklerinde madencilere ödedikleri bir miktar olan işlem ücreti talep edebilmektedir (European Central

Bank, 2015, s. 7). Madenciler, blokzinciri ve kripto para sisteminin bütünlüğünü koruyarak önemli bir rol oynamakta ve sistemin doğru ve güvenli bir şekilde çalışmasını sağlamaktadır.

1.3.4.3. Kripto varlık hizmet sağlayıcıları

Kripto varlık hizmet sağlayıcıları, kullanıcılarına kripto varlıkları kullanma, saklama ve yönetme konusunda kolaylık ve güvenlik sağlayan önemli bir aktör kategorisidir. FATF (2021a, s. 22)'e göre kripto varlık hizmet sağlayıcısı şu şekilde tanımlanmıştır:

“Bir işletme olarak başka bir gerçek veya tüzel kişi adına; sanal varlıklar ve itibari para birimleri arasındaki değişim, bir veya daha fazla sanal varlık biçimi arasında değişim, sanal varlıkların transferi, sanal varlıkların veya sanal varlıklar üzerinde kontrol sağlayan araçların saklanması ve/veya yönetimi, bir ihraççının sanal bir varlığın teklifi ve/veya satışı ile ilgili finansal hizmetlere katılım ve bu hizmetlerin sağlanması faaliyet ve işlemlerinden bir veya birkaçını yürüten herhangi bir gerçek veya tüzel kişi.”

2024 yılında yürürlüğe girmesi beklenen ve 16 Mayıs 2023 tarihinde Avrupa Birliği (AB) Konseyi tarafından kabul edilen Kripto Varlık Piyasaları (*Markets in Crypto Assets-MiCA*) düzenlemesi olarak bilinen *Kripto Varlık Piyasaları Tüzüğü*, kripto varlıklar ve kripto varlık hizmet sağlayıcıları için Avrupa Birliği genelinde yasal bir çerçeve oluşturmaktadır. Söz konusu düzenlemede kripto varlık,

“dağıtılmış defter teknolojisi veya benzer teknoloji kullanılarak elektronik olarak aktarılabilen ve saklanabilen bir değer ve hakkın dijital temsili” olarak ve kripto varlık hizmet sağlayıcısı, *“mesleği veya işi müşterilere profesyonel bir temelde bir veya daha fazla kripto varlık hizmeti sağlamak olan ve ... kripto varlık hizmetleri sağlamasına izin verilen tüzel kişi veya diğer teşebbüs”*

olarak tanımlanmıştır (Regulation of The European Parliament and of The Council On Markets In Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023, ss. 63-64). Tanımda yer alan kripto varlık hizmeti ise herhangi bir kripto varlıkla ilgili aşağıda yer verilen hizmet ve

faaliyetlerden herhangi biri anlamında kullanılmıştır (Regulation of The European Parliament and of The Council On Markets In Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023, s. 64):

“müşteriler adına kripto varlıkların gözetimini ve yönetimini sağlamak, kripto varlıklar için bir ticaret platformunun işletilmesi, fonlar için kripto varlıkların takası, kripto varlıkların diğer kripto varlıklarla takası, müşteriler adına kripto varlık emirlerinin gerçekleştirilmesi, kripto varlıkların yerleştirilmesi, müşteriler adına kripto varlık siparişlerinin alınması ve iletilmesi, kripto varlıklar hakkında tavsiye vermek, kripto varlıklar üzerinde portföy yönetimi sağlamak, müşteriler adına kripto varlıklar için transfer hizmetleri sağlamak.”

Kripto varlık hizmet sağlayıcıları, kripto para borsaları ve cüzdan sağlayıcıları gibi kripto varlık alanında hizmet verenleri içermektedir. Kripto para borsaları, kripto para kullanıcılarına genellikle belirli bir komisyon karşılığında alım-satım ve takas hizmetleri sunan platformlardır. Cüzdan sağlayıcıları ise kripto para kullanıcılarına kripto para birimlerini yönetmek için kriptografik anahtarlarını tutan cüzdanlar sağlayanları ifade etmektedir (Houben ve Snyers, 2018, ss. 26-27). Kripto para borsalarına Binance, Kraken ve Coinbase, cüzdan sağlayıcılara MetaMask ve Ledger gibi platformlar örnek olarak verilebilmektedir. Bunlarla birlikte doğrudan kripto para alım-satım işlemleri gerçekleştirmeye yarayan fiziksel cihazlar olan kripto para ATM (*Automated Teller Machine*-Otomatik Vezne Makinesi)’lerinin kripto varlık hizmet sağlayıcı kapsamında değerlendirilmesi mümkündür.

Kripto varlık alanında merkezi borsalar (*Centralized Exchange*-CEX) olduğu gibi, Uniswap ve Balancer platformlarının örnek olarak verilebileceği merkezi olmayan borsalar (*Decentralized Exchange*-DEX) da mevcuttur. Merkezi olmayan borsalar, kripto para satmak veya almak isteyen farklı kripto para kullanıcılarını bir araya getiren ve onlara birbirleriyle doğrudan işlem yapabilecekleri bir platform sağlayan pazaryerleridir (Houben ve Snyers, 2018, s. 27). Merkezi borsalardan farklı, işlemlerin aracısız şekilde doğrudan eşler arasında gerçekleşmesi olarak ifade edilebilmektedir.

1.3.4.4. Kripto varlık yaratıcıları

Kripto varlık yaratıcıları, kripto varlıkları oluşturan ve teknik bölümünü geliştiren, bazı durumlarda kripto varlıklar piyasaya sürüldükten sonra da teknik özelliklerinin korunması ve geliştirilmesiyle ilgilenmeye devam eden aktör grubudur (European Central Bank, 2015, s. 7). Kripto varlık yaratıcıları, genellikle bir kripto varlık projesinin temel çalışma prensiplerini, teknik özelliklerini, hedeflerini ve potansiyel kullanım senaryolarını açıklayan bir doküman olan *Whitepaper* aracılığıyla kripto varlıkları tanıtmakta ve topluluğa sunmaktadır.

1.3.4.5. Kripto varlık arz edenler (ihraççıları)

Kripto varlık arz edenler, halka kripto varlıkları sunan gerçek kişi, tüzel kişi, başka bir teşebbüs veya ihraççı anlamına gelmektedir (Regulation of The European Parliament and of The Council On Markets In Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023, s. 81). Bu aktör kategorisi kripto paranın ilk piyasaya sürülmesinden sonra, toplu satış yoluyla ödeme karşılığında veya belirli bir kayıt programı çerçevesinde ücretsiz olarak kullanıcılara kripto para sunmaktadır. Kripto varlık arz edenlerin kullanıcılara sunduğu kripto para birimleri, kripto paranın resmi olarak piyasaya sürülmesinden önce oluşturulmakta veya çıkarılmaktadır. Kripto varlık arz edenler, kripto varlık yaratıcıları ile aynı kişi veya kuruluş olduğu gibi farklı kişi veya kuruluş olabilmektedir. Ancak unutulmaması gereken nokta, tüm kripto varlıkların önceden çıkarılmadığı veya arzının önceden oluşturulmadığı ve dolayısıyla söz konusu aktör kategorisine sahip olmadığıdır (Houben ve Snyers, 2018, s. 28).

1.3.5. *Kripto Varlık Türleri*

Kripto varlıklar çeşitli açılardan bazı sınıflandırmalara tabi tutulmaktadır. Avrupa Bankacılık Otoritesi'nin 2019 tarihli "*Kripto Varlıklar Hakkında Avrupa Komisyonu'na Tavsiye İçeren Rapor*"unda kripto varlıklar, kullanım amaçlarına göre üç temel kategoride gruplandırılmıştır (European Banking Authority (EBA), 2019, s. 7):

- Kripto Para Birimi: Ödeme, takas, para birimi esasına göre tasniflenen söz konusu kripto varlık türü, diğer kripto varlık türlerinde olduğu gibi hak

sağlamamaktadır. Bitcoin, Litecoin ve istikrarlı kripto para olarak da adlandırılan Stablecoin'in örnek olarak verilebileceği kripto para birimleri, takas aracı olarak ya da yatırım veya değerin saklanması amacıyla kullanılmaktadır. İstikrarlı kripto paralar, fiziksel teminat ile veya kripto varlıklar tarafından varlığı desteklenen veyahut algoritmaların volatilitiyi dengelemek için bir yol olarak kullanıldığı kripto varlıkları ifade etmektedir.

- Yatırım Token (Investment Token): Mülkiyet hakları ve/veya temettüye benzer şekilde haklar sağlayan kripto varlıklardır. İşletmeler, ICO'lar aracılığıyla itibari para veya diğer kripto varlıklar karşılığında yatırım Token'lar çıkararak sermaye artırımını yapabilmekte ve yatırımcılara bu Token'lar aracılığıyla belirli haklar sunabilmektedir.
- Fayda Token (Utility Token): Genellikle dağıtık defter teknolojisi platformları üzerinde sağlanan ve diğer ürün veya hizmetler için ödeme aracı olarak kabul edilmeyen belirli bir ürün veya hizmete erişimi etkinleştiren kripto varlıklardır.

Uluslararası Para Fonu (*International Monetary Fund-IMF*)'nin *Fintech Notları*'nda yapılan bir sınıflandırmada ise dünya genelinde pek çok finansal düzenleyici tarafından benimsendiği iddiasıyla kripto varlıklar dört temel kategoriye ayrılmıştır (Bains vd., 2022, ss. 11-12):

- Desteklenmeyen Kripto Varlıklar (Unbacked Crypto Asset): Bitcoin ve Ethereum'un örnek olarak verilebileceği söz konusu kripto varlık türü öncelikle bir değişim aracı olarak kullanılmak üzere tasarlanmıştır, dolayısıyla transfer edilebilir niteliktedir. Desteklenmeyen kripto varlıklar genellikle merkeziyetsiz yapıda olmalarına karşın merkezi olarak verilen ve kontrol edilen örnekleri de mevcuttur.
- Fayda Token'ları (Utility Tokens): Tokenize edilmiş bir mağaza kartı veya belirli oyun Token'larının örnek olarak verilebileceği söz konusu kripto varlık türü, sahibine, mevcut veya olası bir ürün veya hizmete erişim sağlaması amacıyla tasarlanmış olup genellikle kapalı bir ağ ile sınırlanmıştır.
- Menkul Kıymet Token'ları (Security Tokens): Söz konusu kripto varlık türü sahibine, ihraççının kârından pay alma gibi geleneksel bir menkul kıymetin haklarını sağlamaktadır.

- İstikrarlı Kripto Paralar (Stablecoin'ler): Binance USD, USD Coin, Tether'in örnek olarak verilebileceği söz konusu kripto varlık türü istikrarlı bir fiyat değerine sahip olmayı amaçlamaktadır. İstikrarlı kripto paralar, tek bir varlığa, itibari paraya, altın gibi emtialara veya diğer kripto varlıklara bağlanarak veyahut merkezi olmayan finasta (*Decentralized Finance-DeFi*) kullanıldığı şekliyle bir algoritma aracılığıyla bir varlığa bağlı olmaksızın başka bir mekanizma kullanarak istikrar sağlayabilmektedir.

2023 tarihinde AB Konseyi tarafından kabul edilen MiCA düzenlemesi ile kripto varlıklar, değerlerini diğer varlıklara göre dengelemeye çalışıp çalışmadığına bağlı olarak üç türde gruplanmıştır (Regulation of The European Parliament and of The Council On Markets In Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, 2023, s. 44):

- E-Para Token'ları (E-Money Tokens): Yalnızca itibari birimini referans alarak değerlerini dengelemeyi hedefleyen söz konusu kripto varlıklar genellikle ödeme yapmak amacıyla kullanılmaktadır. Bazı istikrarlı kripto paralar bu kapsamda değerlendirilmektedir.
- Varlık Temelli Token'lar (Asset-Referenced Token): Söz konusu kripto varlıklar, bir veya birkaç itibari para birimine, başka bir değere, hakka veya bunların kombinasyonuna atıfta bulunarak değerlerini dengelemeyi hedeflemektedir. Algoritmik kripto varlıklar ve algoritmik istikrarlı kripto paralar bu kapsamda değerlendirilmektedir.
- Diğer Kripto Varlıklar: Diğer iki kategoride değerlendirilmeyen Fayda Token (*Utility Token*) gibi çeşitli kripto varlıklar bu grupta değerlendirilmektedir.

Kripto varlıkların doğası ve özellikleri hakkında henüz evrensel bir mutabakat sağlanamadığından, kripto varlık türlerinin sınıflandırması çeşitli düzenleyiciler, kuruluşlar ve yapılan çalışmalar arasında farklılık gösterebilmektedir. Ayrıca yapılan sınıflandırmalar kripto varlıkların kullanım amacı, teknolojik özellikleri, hukuki niteliği, ekonomik yönü gibi hangi açıdan incelendiğine bağlı olarak değişebilmektedir.

Yasal düzenlemelerde araç ve teknolojiye bağımsızlığın sağlanarak konunun temel hukuki ilkeler ekseninde analiz edilmesi ve düzenlenmesi hedeflendiğinden, kripto

varlıkların hangi ağ üzerinde olduğu veya hangi standart kullanılarak oluşturulduğu ve kullanıldığı, kripto varlıklara yönelik yapılan sınıflandırma çalışmalarında ön plana çıkmamıştır. Kripto varlık türlerinin teknik açıdan tasnifi kapsamında *Coin* ve *Token* kavramlarının incelenmesi gerekmektedir. İki kavram arasında bazen anlam ve fonksiyon bakımından kesişmeler olsa da, *Coin* ve *Token*'ın sahip olduğu özellikleri teknik, hukuki ve operasyonel açılardan farklılıklar içermektedir (Tevetoğlu, 2021, ss. 47-55).

Teknik yönüyle kripto varlıkları kendine ait bir blokzinciri olup olmadığına göre *Coin* veya *Token* şeklinde incelemek mümkündür. Kavramsallaştırma henüz standardize edilmemişse de, *Coin*'lerin kendi ayrı blokzincirlerinin bulunduğunu, *Token*'ların ise genellikle başka mevcut bir blokzinciri veya platform üzerinde çalıştığını söylemek mümkündür (Van der Merwe, 2021, s. 448). Daha doğru bir ifade ile, *Coin*'ler genellikle bağımsız blokzinciri veya Hashgraph, Tangle, Holochain ve Tempo gibi farklı dağıtık defter teknolojilerini kullanmaları ile *Token*'lardan ayrılmaktadır. *Coin*'ler platformlardan bağımsız biçimde kullanılabilirken *Token*'lar belirli bir platformda belirli bir amaç için kullanılmaktadır (Güven ve Şahinöz, 2021, s. 87). *Token*'ların isimlendirmelerinde bazen *Coin* ifadesi bulunsa da esas dikkate alınması gereken husus, kripto varlığın hangi ağ üzerinde olduğu ve hangi standardı kullandığıdır (Tevetoğlu, 2021, ss. 53-54).

1.3.5.1. *Coin* kavramı ve türleri

Türkiye Bilişim Vakfı altında çalışmakta olan *Blockchain Türkiye Platformu* tarafından hazırlanan terminoloji raporunda (2019, s. 11) Türkçe'ye "*akçe/koin*" olarak geçen *Coin* kavramı; "*kendisine ait bir blokzinciri platformuna sahip olan ve bir projeden bağımsız olarak faaliyet gösterebilen, bir ödeme metodu olarak kullanılabilen para birimi benzeri dijital değer temsili*" olarak açıklanmıştır. Bitcoin, Ethereum, Litecoin gibi kendi bağımsız blokzinciri üzerinde işlem gören veya IOTA, Nano, Byteball gibi blokzinciri yerine farklı bir dağıtık defter teknolojisi kullanan kripto varlıklar *Coin*'e örnek olarak verilebilmektedir (Do All Cryptocurrencies Use The Blockchain?, 2022). İlk kripto varlık kabul edilen Bitcoin'i takiben çok sayıda farklı *Coin* örnekleri ortaya çıkmış olup bunlar Bitcoin alternatifleri olarak "*Altcoin*" şeklinde adlandırılmaktadır (Güven ve Şahinöz, 2021, s. 86).

Ripple ve Litecoin'in örnek olarak verilebileceği Altcoin'ler, Bitcoin dışındaki kripto para birimlerini ifade etmektedir (FATF, 2014, s. 6). Litecoin gibi Bitcoin'in açık kaynak protokolü kullanılarak temel kodlarında yapılan değişikliklerle farklı özelliklere sahip olacak şekilde oluşturulan Altcoin'ler ile Ethereum ve Ripple gibi Bitcoin'in açık kaynak protokolünü temel almak yerine kendi protokolüne sahip olan Altcoin'ler olmak üzere temelde iki tür Altcoin bulunmaktadır (Houben ve Snyers, 2018, s. 29). İlerleyen kısımlarda Bitcoin, Ethereum, Ripple, Litecoin'in yanı sıra terörizmin finansmanı başta olmak üzere yasa dışı aktivitelerde kullanılma riskinin yüksek olduğu değerlendirilen gizlilik tabanlı kripto varlıkların (*Privacy Coins*) yaygın örnekleri Monero, Dash ve Zcash incelenecektir.

1.3.5.1.1. Bitcoin

Önceki kısımlarda değinildiği üzere Bitcoin, 2008 yılında Satoshi Nakamoto adını kullanan kişi veya kişilerce yayınlanan makale üzerine 2009 yılında Bitcoin blokzinciri üzerinde ortaya çıkarılan ilk ve en popüler kripto varlıktır. Bitcoin (BTC) şu an kripto para birimleri içerisinde fiyat ve piyasa değeri bakımından ilk sırada yer almaktadır (*CoinMarketCap*, 2023). Bitcoin, gerekli teknik uzmanlığa sahip kişiler tarafından incelenmesi, değiştirilmesi ve geliştirilmesi için kaynak kodunun herkese açık olmasına izin veren açık kaynaklı bir yazılım temeli üzerinde çalışmaktadır (Van der Merwe, 2021, s. 448). Eşler arası bir ağ üzerinde merkezi otoriteye ihtiyaç duymaksızın transfer gerçekleştirilebilmesini sağlayan Bitcoin'in temel özellikleri arasında anonimlik, güvenilirlik, sınırlı arz ve merkezi olmayan yapı bulunmaktadır.

Bitcoin, tüm işlemlerin katılımcılar tarafından kaydedildiği, mevcut işlemlerin değiştirilemediği, kaldırılamadığı, yeniden sıralanamadığı dolayısıyla güvenilirliğin sağlandığı, kriptografiyle korunan, merkezi olmayan bir deftere dayanmaktadır. Defterin herhangi bir şekilde değiştirilmesi durumunda değişen ve bu sayede kurcalamanın tespit edilebildiği, tüm defterin depolanmasını gerektirmeyen, herhangi bir zamanda elde edilebilen defterin kriptografik özeti, veri güvenliğinin ve bütünlüğünün sağlanmasında kritik bir rol oynamaktadır (Narayanan ve Clark, 2017, ss. 3-4). Bu sayede Bitcoin işlemleri, birbirine güvenmeyen bir dizi katılımcı arasında Bitcoin'in teknik altyapısına duyulan güven temelinde küresel ölçekte gerçekleştirilmektedir.

Bitcoin, her Bitcoin adresinin bir açık anahtara ve bir özel anahtara sahip olduğu, asimetrik şifreleme adı verilen kriptografik bir sistem kullanmaktadır. Açık anahtar, mesajları şifrelemek ve imzaları doğrulamak için kullanılırken özel anahtar, mesajların şifresini çözmek ve dijital imzalar oluşturmak için kullanılmaktadır. Her özel anahtar tek yönlü bir işlev ile açık anahtar oluşturmakta ve daha sonra açık anahtar başka bir tek yönlü işlev aracılığıyla bir adres oluşturmaktadır. Söz konusu matematiksel fonksiyon, özel anahtarın her zaman aynı açık anahtarı üretmesini sağlamakta ve açık anahtarın eşleştirilmiş olduğu özel anahtarı bulmak için tersine çalıştırılmamaktadır. Özel anahtar gizli tutulmaktadır ancak özel anahtarın belirli bir işlem için dijital imzanın üretilmesine yardımcı olup olmadığını ağdaki herkes doğrulayabilmektedir (Warmke, 2021, ss. 25-30). Bitcoin’de asimetrik şifrelemenin kullanımı, güvenli ve şeffaf dijital imzaların oluşturulmasını mümkün kılmakta ve işlemlerin güvenli bir şekilde şifrlenmesini, şifresinin çözülmesini ve doğrulanmasını sağlamaktadır.

Öte yandan her cüzdanın açık anahtar vasıtasıyla kullanıcıların Bitcoin kimliği işlevi gören alfanümerik karakterler ile tanımlanması ve Bitcoin işlemlerinin blokzinciri üzerinde şeffaf şekilde herkesçe takibinin mümkün olması, Bitcoin’in genel olarak *sözde anonim* şeklinde kabul edilmesine neden olmaktadır. Bitcoin işlemlerinde cüzdan adresleri gerçek hayattaki kimliklerle doğrudan ilişkilendirilememektedir; ancak Bitcoin ağına girmek ve işlem yapmak için çoğu durumda kripto varlık hizmet sağlayıcı gibi bir aracıya ihtiyaç duyulmaktadır. Bu araçlar veya araçların kullandığı geleneksel finansal yöntemler vasıtasıyla bir kullanıcının Bitcoin cüzdan adresi ile gerçek kimliği arasında bağlantı kurulabildiğinde, bu kullanıcının Bitcoin işlemleri kimliğiyle ilişkilendirilebilir şekilde takip edilebilir hale gelmektedir (Demartino, 2021, ss. 101-102).

Bitcoin’in bir kripto varlık olarak devrim yaratan başarısı, teknik bileşenlerinin kombinasyona dayanmaktadır. Bitcoin’in tasarımı, değerli bir para birimi, madencilik gücü ve güvenli bir defter arasındaki döngüsel bağımlılığı başarıyla birleştirmektedir. Çifte harcamayı önlemek ve böylece para biriminin değerli olmasını sağlamak için güvenli bir defter gerekmekte, defterin güvence altına alınması için madencilik gücü gerekmekte ve madencilerin ödüllendirilmesi için değerli bir para birimi gerekmektedir (Narayanan ve Clark, 2017, s. 17). Merkezi otoritenin yokluğunda önemli bir problem olan ve aynı paranın birden fazla kez harcanması girişimi olarak açıklanabilen çifte harcama sorunu Bitcoin’de madencilik süreci ile çözülmektedir. İşlemler, blokzincirine eklenmeden önce,

bilgisayarların yüksek hesaplama gücü gerektiren matematiksel problemleri çözmesi ile işleyen iş ispatı mutabakat algoritması aracılığıyla madenciler tarafından doğrulanmaktadır.

Bitcoin madenciliği, blokzincirine doğrulanmış yeni bloklar ekleyerek blokzincirinin devamlılığını sağlamak için bilgi işlem gücünü ağa tahsis etme sürecidir. Madenciler, belirli bir hedef değerden küçük rastgele bir sayıyı bulmalarını gerektiren karmaşık problemleri çözerek blokların doğrulanmasını ve işlemlerin onaylanmasını sağlamaları karşılığında yeni oluşturulan Bitcoin'ler ve işlem ücretleriyle ödüllendirilmektedir. Sınırlı bir arza sahip olan Bitcoin toplamda 21 milyon sınırına ulaştığında, daha fazla yeni Bitcoin oluşturulmayacak ve dolayısıyla madenciler işlem komisyonları dışında ödül alamayacaktır. Yüksek bilgi işlem gücüne sahip madencilerin bir bloğu daha önce çözmesi muhtemel olup, daha fazla blok çözüldükçe madenciliğin zorluğu artmaktadır (Bhaskar ve Chuen, 2015, s. 53). Blok üretiminin yaklaşık 10 dakikada bir olması hedeflendiği için yüksek bilgi işlem gücü ile birlikte yeni blok üretiminin hedeflenenden daha erken olmaması adına çözülecek problemin zorluk derecesi artmaktadır. Bu durum, madencilik faaliyetlerinin kişisel bilgisayarlardan ziyade büyük madencilik merkezlerine kaymasına sebep olmuş ve merkezileşme endişeleri Bitcoin'in dağıtık ve merkezi olmayan yapısına ters düştüğü eleştirilerine yol açmıştır. Bu nedenle madencilik faaliyetlerinin daha merkezi olmayan bir şekilde gerçekleşmesini teşvik etmek için farklı protokol veya algoritma değişikliklerini barındıran, mevcut bir blokzincirin veya kripto para biriminin iki ayrı versiyona ayrılması anlamına gelen çatallanma ile 2017 yılının ağustos ayında meydana çıkan Bitcoin Gold gibi bazı Altcoin'ler ortaya çıkmıştır (Güven ve Şahinöz, 2021, ss. 64-67).

Bitcoin blokzincirinde, çifte harcama saldırıları gibi kötü niyetli manipülasyonlar veya yayılma gecikmelerinden kaynaklanan blokzincirinde çatallanma durumları, en uzun çatalın fikir birliği olarak kabul edilmesiyle çözülmektedir. Bu kural, en çok iş ispatına sahip olan çatalın geçerli blokzinciri olarak kabul edileceği anlamına gelmektedir. Toplam bilgi işlem gücünün yarısından fazlasını kontrol eden biri, blokzincirinde hangi blokların nihayetinde kabul edileceğine karar verebilmektedir. “%51 saldırısı” olarak da adlandırılan bu saldırı için geçmiş işlemler ne kadar uzunsa, hileli bir zincir kabul edilene kadar o kadar çok bloğun yakalanması gerekmektedir. Bu durum, saldırganların işlem geçmişini değiştirmek için sınırlı olanaklara sahip olmalarını sağlamaktadır (Tschorsch ve Scheuermann, 2016, ss. 1-5).

Bir blokzincirinde işlem hacmi, blok boyutu ve birbirini izleyen iki blok arasındaki ortalama blok aralığı tarafından etkilenmektedir; daha büyük bir blok daha fazla işlem depolayabilirken, blok yayılma süresini de uzatabilmektedir. Bitcoin’de blok aralığı yaklaşık 10 dakikadır ve blok boyutu yaklaşık 1 Megabyte (MB)’dır, bu da her blokta depolanabilecek işlem sayısını saniye başına en fazla 7 işlem olacak şekilde sınırlamaktadır. Bu durum nedeniyle Bitcoin verimliliğinin giderek artan işlem hacmi karşısında yetersiz kalması ve Bitcoin’in kullandığı iş ispatı mutabakat algoritmasında madencilerin hesaplama yoluyla birbirleri ile rekabet halinde olmalarının getirdiği yüksek enerji tüketimi Bitcoin’e getirilen eleştiriler arasında yer almaktadır (Q. Zhou vd., 2016, ss. 2-3). İş ispatı mutabakat algoritmasına ilişkin yüksek hesaplama maliyetleri, saniye başına nispeten sınırlı işlem kapasitesi ve blok başına işlem sayısındaki kısıt gibi Bitcoin’in belirli dezavantajlarının üstesinden gelmek için Altcoin’ler geliştirilmiştir (Van der Merwe, 2021, s. 448).

1.3.5.1.2. *Ethereum*

Ethereum, Bitcoin’den sonra piyasa değeri en yüksek kripto para birimi olarak listede yerini almaktadır (*CoinMarketCap*, 2023). Ethereum’un 2015 yılında ortaya çıkışından önce Vitalik Buterin tarafından 2014 yılında Whitepaper’ı yayınlanmıştır. Ethereum Whitepaper’ında; Ethereum protokolünün başlangıçta bir kripto para biriminin geliştirilmiş bir versiyonu olarak tasarlandığı, ancak temsil ettiği *Turing-complete* programlama diline sahip blokzinciri sayesinde önceden belirlenmiş kurallara göre otomatik olarak yürütülen akıllı sözleşmeler ile bunun bir uzantısı olarak Merkeziyetsiz Otonom Organizasyonları (*Decentralized Autonomous Organizations-DAO*) da mümkün kıldığı ifade edilmektedir. Ayrıca Ethereum ağı, akıllı sözleşmeler aracılığıyla Token ve istikrarlı kripto paralar gibi kripto varlıkların oluşturulmasını ve işlem görmesini de sağlamaktadır (Buterin, 2014).

Ethereum blokzinciri Bitcoin blokzincirine benzer şekilde, ortak kullanıma açık, izinsiz ve kayıtların dağıtık şekilde her node veya terminalde kopyalarının tutulduğu bir sistem olarak işlese de; blok yapıları Bitcoin blokzincirinden farklı olarak yalnızca işlem verilerini değil, aynı zamanda hesap bakiyeleri ve akıllı sözleşmelerin kodları gibi bilgileri de içermektedir (Güven ve Şahinöz, 2021, ss. 104-105). Bu nedenle Ethereum, daha geniş bir uygulama yelpazesini destekleyen bir blokzinciri platformu olarak karşımıza çıkmaktadır.

Bitcoin kısıtlamalarını aşma iddiasıyla ortaya çıkan Ethereum, *Solidity* adı verilen popüler programlama dili ile akıllı sözleşmelerin kodlanmasına olanak tanımaktadır. Bitcoin'e benzer şekilde Ethereum'un da ölçeklenebilirliği ile ilgili endişeler olsa da, Ethereum ağı saniyede ortalama 11 işlemle günde milyondan fazla işlemi başarıyla gerçekleştirebilmektedir. Ethereum platformu; Token sistemleri, finansal türevler, dosya depolama, bulut bilişim ve en önemlisi merkezi olmayan uygulamalar (Decentralized Applications-DApps) gibi çeşitli potansiyel kullanım alanları sağlamaktadır (Vujičić vd., 2018, ss. 4-5).

Ethereum'un kripto para birimi olan ve sözde anonim olarak kategorize edilen *Ether* (ETH), değişim aracı işlevinin yanında akıllı sözleşmelerin ve merkezi olmayan uygulamaların yürütülmesini de sağlamaktadır. Ethereum'un gelişimi, Ethereum'un yaratıcıları tarafından kurulan, kâr amacı gütmeyen bir kuruluş olan Ethereum Vakfı tarafından desteklenmektedir. Büyük miktarda Ether, resmi olarak halka arz edilmeden önce yaratıcıları tarafından oluşturularak geliştirme maliyetlerini ve Ethereum Vakfı'nı finanse etmek için kullanılmıştır (Houben ve Snyers, 2018, s. 34).

Blokszinciri teknolojisi üzerinde belirli koşulların yerine getirilmesi durumunda otomatik olarak çalışan ve belirli eylemleri gerçekleştiren programlanabilir sözleşmeler olan akıllı sözleşmeler, DAO'ların otomatik ve güvenilir bir şekilde işlem yapması ile katılımcılar arasında anlaşmazlıkları çözmesini sağlayarak temel işleyiş mekanizmasını oluşturmaktadır. Geleneksel şirketlerde olduğu gibi merkezi bir otorite veya yöneticiye ihtiyaç duymayan DAO'lar, akıllı sözleşmeler aracılığıyla karar alabilmekte, varlıklarını yönetebilmekte ve üyeleri arasında kaynak paylaşımını gerçekleştirebilmektedir. DAO'ların fiziksel bir adresi veya herhangi bir devlete bağlılığının bulunmaması, yasal düzenlemeler açısından tartışmalara yol açmaktadır (Güven ve Şahinöz, 2021, s. 111).

Programlanabilir blokszinciri ve akıllı sözleşmeler ile desteklenen ve dolayısıyla geniş bir işlevsellik ve uygulama alanı sağlayan Ethereum'un ilerleyen süreçte iş ispatı mutabakat algoritmasından, özellikle %51 saldırılarına karşı daha güvenli ve enerji tüketimi konusunda daha avantajlı olduğu değerlendirilen pay ispatı mutabakat algoritmasına geçmesi beklenmektedir. Pay ispatı mutabakat algoritması ile birlikte Ethereum blokszincirinin daha sürdürülebilir olacağı değerlendirilmektedir.

1.3.5.1.3. *Ripple*

David Schwartz, Jed McCaleb ve Arthur Britto tarafından 2012 yılında *Ripple* (XRP) kripto para birimi ve ödeme protokolü ile dayandığı *XRP Ledger* blokzinciri oluşturulmuştur. Aynı yıl Chris Larsen ile birlikte Ripple şirketi kurulmuş ve Ripple kripto varlık yaratıcıları tarafından söz konusu şirkete 80 milyar XRP hediye edilmiştir. XRP Ledger blokzinciri, iş ispatı veya pay ispatı mutabakat algoritması kullanan blokzincirlerinden farklı olarak, doğrulayıcılar olarak adlandırılan belirlenmiş sunucuların her 3-5 saniyede bir XRP işlemlerinin sırası ve sonucu üzerinde anlaşmaya vardığı bir mutabakat algoritması kullanmaktadır. Ripple; işlemlerin XRP Ledger blokzincirine 3-5 saniyede hızlı bir şekilde yerleştiği, XRP Ledger blokzincirinin saniyede 1.500 işlemi işleyebilmesiyle ölçeklenebilir olduğu, XRP işlem ücretlerinin işlem başına ortalama 0,0002 ABD Doları olmasıyla düşük maliyetli olduğu, XRP Ledger blokzincirinin iş ispatı mutabakat algoritması kullanan blokzincirlerinden çok daha fazla enerji verimliliği sağlamasıyla sürdürülebilir olduğu ve merkeziyetsiz yapıdaki XRP Ledger blokzincirinin 150'den fazla doğrulayıcıdan oluşan küresel bir ağ tarafından yürütüldüğü iddiasındadır (Ripple, 2023).

Sözde anonim olma özelliği taşıyan XRP'nin toplam arzı yaratıcıları tarafından tamamen önceden çıkarılmış olup dağıtımını Ripple şirketi kontrol etmektedir. XRP, finans kurumlarının sınır ötesi ödemelerini hızlı ve düşük maliyetle yapabilmeleri için bir köprü para birimi olacak şekilde inşa edilmiştir; ancak Ripple ödeme platformunun fiilen çalışması için bir köprü para birimine ihtiyacı yoktur (Houben ve Snyers, 2018, ss. 35-36). Başka bir deyişle, Ripple ödeme platformunda XRP kullanmadan da işlem gerçekleştirilebilmektedir.

Ripple kripto varlık yaratıcıları tarafından üretilen ve sonrasında büyük bir kısmı Ripple şirketine hediye edilen toplam 100 milyar XRP ile toplam XRP arzı sabit tutulmuştur. Ripple ağındaki transfer işlemlerinden alınan komisyonlar silinmek suretiyle sistemden çıkarılmaktadır. Bu durum, işlem yapıldıkça piyasadaki XRP miktarının azaldığı anlamına gelmektedir (Güven ve Şahinöz, 2021, s. 117). Bu mekanizma, dolaşımdaki XRP miktarını azaltarak değer artışı potansiyelini artırırken, aynı zamanda Ripple ağının verimli çalışmasına da katkıda bulunmaktadır.

1.3.5.1.4. Litecoin

Litecoin (*LTC*), merkezi olmayan ve herkese açık bir ağ üzerinde düşük maliyetli, sınırsız ve güvenli ödemeler yapılabilmesine yardımcı olmaktadır. Litecoin blokzinciri, Scrypt tabanlı bir kriptoloji algoritması kullanmaktadır. Litecoin, Lightning Network gibi önemli teknolojik gelişmelere öncülük ederek ölçeklenebilirlik ve işlem hızı konularında çözümler sunmaktadır (Litecoin, 2020).

Bitcoin'in açık kaynak kodlu yazılımı geliştirilerek üretilen ilk kripto para olan Litecoin, eski bir Google çalışanı olan Charles Lee tarafından ortaya çıkarılmıştır. Litecoin, tarafların işlemlerini ana zincir yerine kendi aralarında oluşturdukları ödeme kanallarında gerçekleştirerek belirli dönemlerde mahsuplaşmanın sonucunun ana zincire kaydedildiği Lightning Network ve dijital imzaların blok dışında takip edilmesinin sağlandığı SegWit destekleri ile Bitcoin'den ayrılmaktadır. Bu destekler sayesinde Bitcoin'de ortaya çıkan yüksek işlem komisyonları ve uzayan işlem sürelerine ilişkin iyileştirme sağlanmıştır (Güven ve Şahinöz, 2021, ss. 115-120).

Sözde anonim bir kripto para birimi olan Litecoin, Bitcoin'e benzer şekilde, açık kaynaklı, merkezi olmayan, eşler arası bir ağ üzerinde oluşturulmakta ve kullanılmaktadır. Litecoin, Güvenli Hash Algoritması 256-bit (*Secure Hash Algorithm 256-bit-SHA-256*) iş ispatı mutabakat algoritması kullanan Bitcoin'den farklı olarak *Scrypt* iş ispatı mutabakat algoritmasına dayanmaktadır. Söz konusu algoritma ile birlikte Litecoin blokzincirinde yaklaşık 2,5 dakika olan ortalama blok oluşturma süresi, Bitcoin'e kıyasla çok daha yüksek bir işlem hızı sağlamaktadır. Açık ve izinsiz bir blokzinciri üzerinde çalışan Litecoin'in toplam arz limiti 84 milyon adet olup, bu sayı Bitcoin'in toplam arz limitinden tam dört kat daha fazladır (Houben ve Snyers, 2018, ss. 37-39).

Küresel ödemeleri kolaylaştırmak amacıyla Bitcoin'e alternatif olarak ortaya çıkan Litecoin, daha hızlı işlem onay süreleri ve düşük işlem maliyetleri gibi özellikleri sayesinde küresel ölçekte hızlı, güvenli ve düşük maliyetli bir kripto varlık ve ödeme yöntemi olarak kullanılabilir.

1.3.5.1.5. Gizlilik tabanlı kripto varlıklar (Privacy Coins)

Ağıdaki herkesin işlemleri izleyebilmesine olanak tanıyan Bitcoin'in halka açık blokzinciri, hem bir zayıflık hem de bir güç olarak görülebilmektedir. Blokzincirinin şeffaf yapısı, Bitcoin ile yapılan tüm işlemlerin herkesçe takip edilebilir ve hesapların ilişkilendirilebilir olmasına neden olmaktadır. Bitcoin'in anonimlik ve mahremiyet konularındaki bazı zayıf yönleri, bu zayıflıkların üstesinden gelmeye çalışan Monero, Dash, Zcash gibi gizlilik tabanlı kripto varlıkların ortaya çıkmasına yol açmıştır (Hilmola, 2021, ss. 1-4).

Bir Bitcoin cüzdan adresi, herhangi bir kişisel kimlik bilgisine açıkça bağlı olmadığından sahibinin kimliği genellikle gizli kalmaktadır; ancak kullanıcıların kimlikleri hakkında cüzdan transferlerinin analizi ile çıkarımlarda bulunmak mümkündür. Blokzinciri analizi, kullanıcılar ve işlemleri arasındaki bağlantıları ortaya çıkarabilmekte ve bu bağlantılar nedeniyle mahremiyet tehlikeye girebilmektedir. Gizlilik ve anonimlik konularına daha fazla odaklanan özellikler sunarak kullanıcı meta verilerini gizlemeye veya karartmaya çalışan gizlilik tabanlı kripto varlıklar, teknolojik gelişmişlik açısından farklılıklar gösterebilmektedir. Gizlilik tabanlı kripto varlıklar, özellikle Dark Web başta olmak üzere yasa dışı alanlarda kullanıldığı ile ilgili yaygın bir inanca sahiptir (Harvey ve Branco-Illodo, 2019, ss. 3-4).

Gizlilik tabanlı kripto varlıklar düşük likidite, kullanılabilirlik sorunları, bazı düzenleyici zorluklarla karşı karşıya kalabilmekte ve gizlilik sağlama konusunda kullandığı teknikler bazen tartışmalara sebep olabilmektedir. Gizlilik tabanlı kripto varlıkların kullanımı ve benimsenmesi, sahip olduğu avantajlar ve dezavantajlar ile kullanıcılar tarafından tercih edilen gizlilik seviyesine bağlı olarak değişmektedir.

Monero

2014 yılı Nisan ayında piyasaya sürülen, Bitcoin'e benzer şekilde açık kaynak kodlu, merkeziyetsiz ve izinsiz bir blokzinciri üzerinde çalışan, madencilik yoluyla yeni üretimlerin yapıldığı ve ödeme aracı olarak kullanılabilen bir kripto para birimi olan Monero (XMR); Bitcoin'den farklı olarak *CryptoNote* iş ispatı mutabakat algoritması kullanmaktadır. Monero, kullanıcılarının işlemlerini tam bir anonimlik içinde yürütmesine imkân sağlamak

amacıyla özel olarak geliştirilmiştir. Diğer bazı kripto para birimlerinin aksine önceden çıkarılmamış olan Monero, tamamen değiştirilebilir olarak karakterize edilmiştir. Bunun anlamı, XMR kripto para biriminin her zaman karşılıklı olarak ikame edilebileceği ve Bitcoin veya Litecoin gibi bazı kripto para birimlerinin aksine, geçmişte yasa dışı bir amaç için kullanılması nedeniyle belirli XMR kripto para birimlerinin kara listeye alınamayacağıdır (Houben ve Snyers, 2018, ss. 45-46).

Bitcoin ve Ethereum gibi sözde anonim kripto para birimlerinin aksine Monero’da tam bir gizlilik söz konusudur. Bitcoin ve Ethereum dahil olmak üzere şeffaf blokzincirine sahip kripto para birimleri ile yapılan işlemlerin herkesçe izlenebilmesi, işlemlerdeki gönderici ve alıcı adreslerinin gerçek dünyadaki kimliklerle ilişkilendirilebileceği anlamına gelmektedir. Monero ise bunun önüne geçmek ve kullanıcılarının gizliliğini sağlamak için çeşitli teknolojiler kullanmaktadır; her işlemin alıcı ve gönderici adresi ile işlem tutarına ilişkin bilgiler “Gizli Adresler (*Stealth Addresses*)” ve “Halka Gizli İşlemler (*Ring Confidential Transactions-RingCT*)” teknolojilerinin kullanımıyla gizlenmektedir (Monero, t.y.).

İşlemlerin gizliliğini artırmak için tasarlanan Halka Gizli İşlemler teknolojisi, “Halka İmzalar (*Ring Signatures*)” tekniğini ve “Gizli İşlemler (*Confidential Transactions*)” kavramını birleştirmektedir. Halka İmzalar, bir kullanıcının hesap anahtarlarını Monero blokzincirinden elde edilen açık anahtarlarla birleştirerek veya *kariştirarak* olası imzalayanların halkasını oluşturmaktadır. Bu sayede bir imzanın belirli bir kullanıcıyla ilişkilendirilmesinin önüne geçerek gönderici ve alıcı kimliklerinin tamamen gizlenmesine olanak vermektedir. Gizli İşlemler ise girdi miktarlarının toplamının çıktılarının toplamıyla aynı olduğuna dair kullandığı kriptografik ispat sayesinde işlem tutarlarını gizleyerek söz konusu *karişime* başka bir gizlilik katmanı eklemektedir. Halka Gizli İşlemler teknolojisine ek olarak Monero, alıcı adına gönderici tarafından yapılan her işlem için rastgele oluşturulmuş tek seferlik adresler olan Gizli Adresleri de kullanmaktadır. Ödemeler bu adresler üzerinden yönlendirildiği için blokzincirinde alıcı ve gönderici adresleri arasında bağlantı olmaması sağlanmaktadır (Houben ve Snyers, 2018, ss. 46-47).

Blok üretim hedef süresi iki dakika olan Monero’nun başlıca özellikleri; gizlilik, kara listeye alınamadığından tam değiştirilebilirlik, üretilen blok boyutuna bağlı olarak madencilere verilen ödülün değişmesi suretiyle ayarlanan blok büyüklüğü sayesinde dinamik ölçeklendirme, büyük yatırım yapan madencilerde merkezileşmeyen yaygın

madencilik, gönderiyi gizlemek için kullanılan genel görünüm anahtarı ve gizlenmiş göndericiden gizlenmiş tutarın doğru kişiye gitmesi için kullanılan özel görünüm anahtarı olmak üzere çoklu anahtarlar olarak ifade edilebilir (Güven ve Şahinöz, 2021, ss. 126-131). Söz konusu özellikleri ile birlikte bilhassa gizlilik ve mahremiyet odaklı kullanıcılar için Monero, giderek artan bir kullanım ve benimsenme düzeyine ulaşmıştır. Monero'nun kullandığı teknolojiler ile birlikte sağladığı gizlilik özellikleri, potansiyel olarak terörizmin finansmanı dahil olmak üzere çeşitli yasa dışı faaliyetlerde kullanılma riskini de beraberinde getirmektedir.

Dash

Satoshi Nakamoto'nun çalışmasına dayanan ilk gizlilik merkezli kripto para birimi olan Dash, Bitcoin tasarımını geliştirerek gelişmiş gizlilik ve değiştirilebilirlik, daha az fiyat oynaklığı, ağ boyunca daha hızlı mesaj yayılımı sağlamaktadır. Bitcoin gibi bazı kripto para birimlerindeki gibi tek katmanlı model yerine "*Masternode*" ağı olarak bilinen iki katmanlı bir model kullanmaktadır. Dash, değiştirilebilirliği artırmak için *PrivateSend* ve merkezi bir otorite olmadan anında işlem onayına imkân tanıyan *InstantSend* gibi özellikler içermektedir (Duffield ve Diaz, 2015).

2014 yılının ocak ayında piyasaya sürülen, Bitcoin'e benzer şekilde açık kaynak kodlu, merkeziyetsiz ve izinsiz bir blokzinciri üzerinde çalışan ve ödeme aracı olarak kullanılabilen bir kripto para birimi olan Dash; *XII* iş ispatı mutabakat algoritması kullanmaktadır. Eskiden "*Darkcoin*" olarak bilinen, eşler arası gizlilik merkezli bir kripto para birimi olan Dash, diğer çoğu kripto paradan farklı olarak iki katmanlı bir ağa sahiptir; Dash blokzinciri, madenciler tarafından yapılan iş ispatına ek olarak Masternode'ler aracılığıyla güvence altına alınmaktadır. Masternode, anonimlik için kullanılan PrivateSend ve anında işlem için kullanılan InstantSend özellikleri ile ilgili belirli görevleri gerçekleştirmek için belirli bir minimum düzeyde performans ve işlevselliği garanti eden Dash ağına bağlı bir sunucudur (Houben ve Snyers, 2018, ss. 48-49).

Masternode'lar madencilik yapmamaktadır ancak madenciler yeni bloklar oluşturduklarında madenciler ile birlikte Masternode'lar da katkılarının karşılığı olarak ödüllendirilmektedir. Dash'in iki katmanlı yapısında, Masternode'lar işlemlerin hızlı bir şekilde onaylanmasını ve gizlilik özelliklerini destekleyerek ağa ekstra hizmetler

sağlamaktadır (Dash, 2023). Madenciler ve Masternode'lar Dash ağının güvenliğine ve işleyişine katkıda bulunmaktadır.

Masternode'ların desteklediği InstantSend özelliği kredi kartları gibi neredeyse anlık işlemler yapılmasını sağlamak ve PrivateSend özelliği gizlilik odaklı işlemlere katkıda bulunmaktadır. Bitcoin blokzinciri gibi Dash'in varsayılan olarak şeffaf blokzinciri, genel anlamda, işlemlerin blokzincirinde açıkça doğrulanabilir ve izlenebilir olmasını sağlamaktadır. Ancak kullanıcılar, Dash'in anonimlik ve gizlilik özelliği olan PrivateSend'i kullanarak, işlemlerinin izlenmesini ve finansal aktivitelerinin tamamen şeffaf hale gelmesini engelleyebilmektedir. PrivateSend, Dash kullanıcılarına daha fazla gizlilik sağlamak için tasarlanmış olup *kariştirme* olarak bilinen bir işlemle kullanıcıların fonlarının kaynağının gizlenmesini sağlamaktadır. Bu özelliğin kullanılması kullanıcıların tercihine bağlı olduğundan Dash, isteğe bağlı anonim bir kripto para olarak değerlendirilmektedir (Houben ve Snyers, 2018, ss. 48-49).

Kendi blokzinciri teknolojisini kullanan ve kullanıcı dostu bir deneyim sunmayı hedefleyen Dash, hızlı işlem süreleri, kullanıcı dostu arayüzü ve gizlilik özellikleriyle birlikte diğer kripto para birimlerine göre avantajlı bir seçenek olmayı amaçlamaktadır. Dash, gizlilik odaklı özelliklere sahip olmasından dolayı kullanıcıların fonlarının kaynağını gizleyebilmektedir. Söz konusu özellikleri, kullanıcıların mahremiyetini koruma amacı güderken aynı zamanda potansiyel yasa dışı faaliyetlerde kullanılma riskini de barındırmaktadır.

Zcash

Bitcoin'in açık kaynak kodu ile oluşturulan Zcash, işlem bilgilerini şifreleyen bir gizlilik teknolojisi kullanmaktadır (Zcash, t.y.). 2016 yılında piyasaya sürülen ve isteğe bağlı anonim bir kripto para birimi olan Zcash, "*Sıfır Bilgi Kanıtı (Zero-Knowledge Proof)*" olarak bilinen gelişmiş ve yenilikçi bir kriptografi yöntemi olan *zk-SNARK* teknolojisi kullanmaktadır. Söz konusu teknoloji, bir tarafın başka bir tarafa belirli bir bilgiyi bildirmesine gerek kalmaksızın o bilgiye sahip olduğunu ispatlamasına olanak tanımaktadır. Sıfır bilgi kanıtı, iki taraf arasında bir bilginin geçerliliği hakkında mutabakata varılmasını sağlarken, asıl bilginin gizli kalmasına ve tarafların kimliğinin korunmasına imkân vermektedir. Zcash işlemleri; alıcı ve gönderici adresleri ile işlem detaylarının

blokzincirinde görüneceği şekilde tamamen şeffaf, bir tarafın adresinin blokzincirinde görüneceği ve diğer tarafın adresinin korumalı kalacağı şekilde kısmen korumalı, taraflar hakkındaki bilgiler ile işlem detaylarının blokzincirinde görünmeyeceği şekilde tamamen korumalı olabilmektedir (Keatinge vd., 2018, ss. 32-33).

Bitcoin'in gizlilik eksikliğini gidermek amacıyla 2013 yılında geliştirilmiş olan Zerocoin, Zcash'in öncü projesi kabul edilmektedir. Bilgilerin korunması için madeni paraların yok edildiği ve yeniden yaratıldığı anonimlik için sıfır bilgi kanıtı kullanma fikrini ilk olarak *Zerocoin* ortaya atmıştır. Zerocoin'in sıfır bilgi kanıtını anonimlik için kullanma fikri, Monero ve Zcash gibi farklı kripto para birimlerinde benimsenmiş ve geliştirilmiştir. Zcash'in sıfır bilgi kanıtı için kullandığı zk-SNARK teknolojisi sayesinde Zcash işlemlerinde alıcı, gönderici ve işlem tutarı bilgileri gizli kalarak işlemler izlenemez hale getirilmektedir (Zhou vd., 2021, ss. 45-46). Zcash'in sağladığı gizlilik özellikleri, finansal özgürlüğünü ve mahremiyetini korumak isteyen kullanıcılar için önemli bir avantaj oluşturduğu gibi, Zcash'in terörizmin finansmanı veya suç gelirlerinin aklanması gibi yasa dışı amaçlarla kullanıma potansiyeli oluşturduğunun değerlendirilmesine neden olmaktadır.

1.3.5.2. Token kavramı ve türleri

Blockchain Türkiye Platformu tarafından hazırlanan terminoloji raporunda Türkçe'ye “*jeton*” olarak geçen Token kavramı bir kripto varlık türü olarak açıklanmış ve Ethereum'un akıllı sözleşmeleri üzerinde üretilen projeler örnek verilmiştir (Blockchain Türkiye, 2019, s. 19). Genel amaçlı bir değişim aracının dışında ve ötesinde işlevsellik sunabilen Token'lar, blokzinciri gibi bir dağıtık defter teknolojisinin kullanımından kaynaklanan bir varlığa karşı bir tür iddia içeren farklı bir kripto varlık sınıfını oluşturmaktadır (Houben ve Snyers, 2018, s. 23). Bahsedildiği üzere, mevcut bir blokzinciri veya dağıtık defter teknolojisi üzerinde kullanılan Token'ların, Ethereum başta olmak üzere *Polkadot* ve *Solana* gibi akıllı sözleşmelere imkân veren çeşitli ağlar üzerinde oluşturulması, yönetilmesi ve transferi mümkündür.

Esasında, elektronik kayıt tutma sistemlerinde güvenilir üçüncü şahıslar tarafından onlarca yıldır kullanılmakta olan ve doğası gereği parasal olması gerekmeyen Token'lar temel olarak, belirli bir bağlamda kullanılabilen birtakım hakların kriptografik olarak güvenli bir temsilini oluşturan karakter dizisidir. Varlıkların dijital olarak düzenlenme ve

aktarım mekanizmasını önemli ölçüde değiştiren blokzinciri ve dağıtık defter teknolojileri sayesinde Token'lara olan ilgi artmıştır. Güvenilir bir üçüncü tarafa gerek olmaksızın dağıtık şekilde kayıt tutmayı sağlayan blokzinciri ve dağıtık defter teknolojileri, dijital varlıkların oluşturulmasına ve mevcut varlıkların veya hakların dijital Token'lara dönüştürülmesine (tokenleştirilmesine) imkân vermektedir (Blandin vd., 2019, ss. 14-15).

Coin'lerden farklı bir kripto varlık türü olarak değerlendirilen Token'lar, genellikle belirli bir proje veya işletme için fon toplamak amacıyla ICO çerçevesinde verilmektedir (Houben ve Snyers, 2018, s. 23). ICO'lar, Token ihraç ederek dış finansman sağlamak için tasarlanmış dağıtık defter teknolojisine dayalı akıllı sözleşmelerdir (Momtaz, 2020, s. 1). ICO olarak adlandırılan Token satışında, bir projenin düzenleyicileri, yeni teknolojik platformların ve hizmetlerin geliştirilmesini finanse etmek için Token satışı gerçekleştirmektedir (Rohr ve Wright, 2017, s. 1). Token'ların işlevleri, kullanım alanları ve sahiplerine sunabileceği özellikler genellikle ihraççısı tarafından belirlenen ve projenin Whitepaper'ında tarif edilen özelliklere bağlı olarak değişebilmektedir. Bu nedenle, her ICO projesinde Token'lar farklı hak, yetki ve olanaklar taşıyabilmekte ve sağlayabilmektedir (Tevetoğlu, 2021, ss. 51-66).

Farklı işlev ve kullanım alanlarına sahip olabilen Token'lar; *Ödeme Token (Payment Token)*, *Fayda Token (Utility Token)*, *Menkul Kıymet Token (Security Token)* şeklinde sınıflandırılabilir. Bu üç kategori altında sınıflandırılmayan Token'lar da bulunmaktadır (European Banking Authority (EBA), 2019, s. 6; Blandin vd., 2019, s. 18). NFT, benzersiz ve değiştirilemez dijital varlıkları temsil eden bir Token türü olarak karşımıza çıkmaktadır. NFT'lerin, koleksiyon ürünleri, oyun, sanat, sanal varlıklar, varlıkların tokenleştirilmesi gibi çok çeşitli kullanım alanları bulunmaktadır (Lau, 2020, s. 4). İlerleyen kısımlarda Ödeme Token (Payment Token), Fayda Token (Utility Token), Menkul Kıymet Token (Security Token), NFT şeklinde sınıflandırılan Token türleri detaylandırılacaktır.

1.3.5.2.1. *Ödeme Token (Payment Token)*

Ödeme Token'ları, bir değer alışverişi aracıdır (Blandin vd., 2019, s. 18). Kendi bağımsız blokzinciri veya dağıtık defter teknolojisi bulunmayan ancak başka bir platformun altyapısını kullanan kripto para birimleri olarak değerlendirilebilen Ödeme Token'ları

genellikle, Fayda Token veya Menkul Kıymet Token'larında olduğu gibi hak sağlamamaktadır. Ödeme Token'ları; Token'ın ihraççısı dışındakilerce sağlanan bir mal veya hizmetin alım-satımında kullanımının örnek verilebileceği şekilde bir değişim aracı olarak veya değer saklama aracı olarak veyahut yatırım amacıyla kullanılabilir (European Banking Authority (EBA), 2019, s. 7). Coin'lere tür olarak en yakın Token türü olan Ödeme Token'larının ödeme işlemlerinde kullanılma özelliği bulunsu da, bir Coin veya Token'ın bir ülkede ya da Avrupa Birliği gibi bölgesel yapılarda ödeme aracı özelliğine sahip olup olmayacağı, ilgili ülke veya bölgenin yasal düzenlemelerine bağlı olarak değişebilmektedir (Tevetoğlu, 2021, s. 69). Kripto varlıkların ödemelerde kullanılmasının kabul edilmediği durumda, Ödeme Token'ları değişim aracı olarak kullanılmak yerine, yatırım amacıyla veya değer saklama aracı olarak kullanılmaktadır.

Ödeme Token'larının tipik örneği olarak istikrarlı kripto paralar, genellikle fiziksel teminat veya kripto varlıklar gibi varlığa dayalı şekilde ya da Token değerindeki volatilitiyi dengelemenin bir yolu olarak algoritmaların kullanıldığı algoritmik biçimindedir (European Banking Authority (EBA), 2019, s. 7). İstikrarlı kripto paraların temel amacının, genellikle, kripto varlıkların yüksek volatilitisini dengelemek ve daha istikrarlı bir değer sunmak olduğu söylenebilir. İstikrarlı kripto paralar bir varlığa dayalı olarak veya algoritmalar aracılığıyla Token değerini sabit tutmaya çalışmaktadır.

İstikrarlı Kripto Para (Stablecoin)

İstikrarlı kripto paralar, belirli bir varlığa ya da bir varlık havuzuna veya bir varlık sepetine göre sabit bir değeri korumayı amaçlayan bir kripto varlık türüdür (Financial Stability Board (FSB), 2020, s. 5). Bir merkez bankası, finansal piyasa altyapısı, banka, kredi kuruluşu veya yüksek düzeyde düzenlemeye tabi saklama kuruluşu tarafından ihraç edilmeyen diğer varlıklara göre veya bunlara ilişkin fiyat dalgalanmalarını en aza indirmek ya da ortadan kaldırmak için tasarlanmış Token'lardır. Varsa, ihraç eden kuruluş ve/veya dayanak varlıklar üzerinde bir talebi temsil edebilmektedir (Global Blockchain Business Council, 2020, s. 5).

İstikrarlı kripto paralar, sabitlenmiş bir varlık veya bir mal sepeti şeklinde satın alma gücü ile ilgili olarak fiyat istikrarını korumak için tasarlanmıştır. Varlığa dayalı ve algoritmik şeklinde iki kategoride incelemek mümkündür. Varlığa dayalı istikrarlı kripto paralarda,

itibari para ve altın gibi finansal veya finansal olmayan geleneksel varlıklar ile kripto varlıklar teminat olarak kullanılabilmekte ve bunlar genellikle istikrarlı kripto para ihraççısı tarafından gözetiminde tutulmaktadır. Algoritmik istikrarlı kripto paralarda ise arz ve talebi eşleştirmek ve dolayısıyla fiyat oynaklığını azaltmak için istikrarlı kripto para ihracını ve itfasını düzenlemek üzere programlanmış akıllı sözleşmeler kullanılmaktadır (Blandin vd., 2019, s. 53).

En bilinen istikrarlı kripto para örneklerinden olan *Tether* (USDT) varlığa dayalı bir istikrarlı kripto para türüdür. Başlangıçta Bitcoin blokzincirini kullanan ancak daha sonra farklı blokzincirleri ve ağlar üzerinde oluşturulan Tether, fiyatını dolara endeksleyerek 1 Amerikan Doları (*United States Dollar*-USD) civarında sabit tutmaya çalışmaktadır. Tether, kripto varlık hizmet sağlayıcılarda itibari paraya kıyasla kripto varlık alışverişinin daha kolay olması sebebiyle tercih edilmektedir. Tether bir yandan, kripto varlıklar arasındaki akışkanlığı sağladığı düşüncesi ile faydalı bulunurken diğer yandan, rezervlerinin tamamını şeffaf bir şekilde kanıtlanamaması ve tutarsız beyanları sebebiyle eleştirilmektedir (Güven ve Şahinöz, 2021, ss. 131-132). Tether dışında *USD Coin* (USDC) ve *Binance USD* (BUSD) gibi pek çok istikrarlı kripto para örneği mevcuttur (Bains vd., 2022, s. 12).

1.3.5.2.2. *Fayda Token (Utility Token)*

Fayda Token'ları, bir dijital platform veya hizmet için erişim izni aracıdır (Blandin vd., 2019, s. 18). Hizmet Token'ı olarak da adlandırılan Fayda Token'lar, belirli bir ağ veya platformda belirli hizmetlere veya faydalara erişimi temsil eden kripto varlık türü olarak karşımıza çıkmaktadır. Bir dağıtık defter teknolojisi platformuna erişmenin bir yolu ve/veya takas aracı olarak kullanılabilen, platformdaki katılımcıların o platform üzerinde sunulan mal ve hizmetlerin sağlanması için kullanabileceği veya temel ağla doğrudan ilişkili olmayan ancak başka bir dağıtık defter teknolojisi platformunun üzerinde inşa edilen uygulamalara erişmek için kullanılan Token'lardır (Global Blockchain Business Council, 2020, s. 5). Genellikle bir dağıtık defter teknolojisi platformu kullanılarak sağlanan ancak diğer ürün veya hizmetler için ödeme aracı olarak kabul edilmeyen belirli bir ürün veya hizmete erişim olanağı vermektedir. Bulut hizmetleri bağlamında erişimi kolaylaştırmak için verilen bir Token Fayda Token'a örnek olarak gösterilebilmektedir (European Banking Authority (EBA), 2019, s. 7).

Finansal olmayan amaçlarla üretilen, ihraç edilen ve kullanılan Fayda Token'ların menkul kıymet, sermaye piyasası veya ödeme aracı olma özellikleri bulunmamaktadır. Fayda Token'ları arasında, kitle fonlaması amacıyla çıkarılan ve fonlama sürecine katılan kişilere üretilecek ürünlerden avantajlı şekilde yararlanma ve satın alma hakkı tanıyan DAO Token'ları bulunmaktadır. Spor kulüplerinin çıkardığı, takımların marşlarına, formlarına, asil ve yedek oyuncularına, transferlerine ilişkin karar alma süreçlerine katılım hakkı ve kulüple ilişkili ayrıcalıklara erişim sağlayan Fan Token'ları, Fayda Token'lara örnek olarak verilebilmektedir (Tevetoğlu, 2021, s. 70). Bunların yanında, tokenleştirilmiş bir mağaza kartı veya belirli oyun Token'ları, Fayda Token türleri olarak kabul edilmektedir (Bains vd., 2022, s. 11).

1.3.5.2.3. Menkul Kıymet Token (Security Token)

Menkul Kıymet Token'ları bir yatırım aracıdır (Blandin vd., 2019, s. 18). Yalnızca geçerli düzenleyici menkul kıymet tanımını karşılayan dağıtık defter teknolojisinde çıkarılan veya farklı bir platformda çıkarılan ve dağıtık defter teknolojisine dayalı menkul kıymetleri veya finansal enstrümanları temsil eden Token'lardır (Global Blockchain Business Council, 2020, s. 5). Bu Token'lar, düzenleyici kurallara tabi olan finansal enstrümanları temsil etmek için kullanılmaktadır. Sahibine, ihraççının kârından pay alma hakkı gibi geleneksel bir menkul kıymetinki gibi haklar sağlayan Menkul Kıymet Token'ının tanımı, yetki alanlarına göre değişiklik gösterebilmektedir (Bains vd., 2022, s. 11).

ABD'de "Howey Testi" ile Token'ların sınıflandırılması konusu aydınlatılmaya çalışılmaktadır. ABD Menkul Kıymetler ve Borsa Komisyonu (*Securities and Exchange Commission-SEC*), kripto varlık arzının ve arza konu Token'ın hukuki niteliğinin analizinde Howey Testi'ne tabi tutulmasına karar vermiştir. Howey Testi, bir varlığın menkul kıymet olarak kabul edilip edilmeyeceğini belirlemek için; para veya değerli bir şey karşılığında elde edilmesi, yatırımcının kâr elde etme beklentisi olması, yatırımın bir ortaklığa veya girişime katılmayı içermesi, kârın üçüncü bir taraf veya müteşebbisin çabalarından kaynaklanması gerektiği şeklinde dört temel kriter kullanılmaktadır. Eğer bir Token söz konusu kriterleri karşılıyorsa, Menkul Kıymet Token'ı olarak kabul edilmekte ve ABD menkul kıymet düzenlemelerine tabi olmaktadır (Tevetoğlu, 2021, ss. 59-68). Menkul Kıymet Token'ları yatırımcılara güvenli bir ortamda menkul kıymetlere yatırım yapma imkânı sunarken, koruma ve şeffaflık sağlamak amacıyla da ilgili düzenleyici standartlara

tabi olmak zorundadır. Menkul Kıymet Token'larının sermaye piyasası düzenlemeleri çerçevesinde ihraç edilmesi ve işlem görmesi gerekmektedir.

1.3.5.2.4. Nitelikli Fikrî Tapu (Non-Fungible Token-NFT)

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Türk Dil Kurumu'nun koordineli çalışmaları sonucunda NFT'nin Türkçe karşılığına “*Nitelikli Fikrî Tapu*” olarak öneri getirilmiştir (Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2022). NFT'ler sanat eserleri, koleksiyonlar veya diğer dijital öğelerin sahipliğini kanıtlamak için ortaya çıkmış olup, sanat eserlerine dayalı olarak oluşturulan Token'ların orijinalliğini garanti etmekte ve sahiplik konusunda güvence sağlamaktadır (*Why Decentralised Finance (DeFi) Matters and the Policy Implications*, 2022, s. 55).

FATF, NFT'leri “*değiştirilebilir olmaktan ziyade benzersiz olan ve pratikte ödeme veya yatırım aracı yerine koleksiyon olarak kullanılan dijital varlıklar*” olarak tanımlamış ve NFT'lerin özelliklerine bağlı olarak genellikle kripto varlık olarak kabul edilmediğini ancak uygulamada ödeme veya yatırım amaçlı kullanılan NFT'lerin kripto varlık kapsamında değerlendirilebileceğini açıklamıştır (FATF, 2021a, s. 24). NFT'lerin kullanım amacına göre değerlendirilmesi gerektiğini ifade eden FATF, NFT'ler konusunda işlevsel yaklaşımın önemine dikkat çekmektedir.

Benzersiz ve benzeriyle değiştirilemez kripto varlıklar olan NFT'ler, Ethereum gibi akıllı sözleşme platformlarında kullanılarak, bir yaratıcının video, resim, sanat, etkinlik biletleri vb. biçimdeki dijital varlıklarının varlığını ve sahipliğini kanıtlayabilmektedir. NFT sahibi, NFT pazarında varlıklarını satışa çıkarabilmekte veya diğer kullanıcılarla değiş tokuş yapabilmektedir. Bu işlemlerin her seferinde, bir yandan yaratıcı da telif ücreti alabilmektedir (Wang vd., 2021, s. 2). NFT'ler, yaratıcıların dijital varlıklarını değerlendirmeleri ve ticaretini yapmaları için fırsat sunmaktadır. 2021 yılında popüleritesinde patlama yaşanan NFT'ler, çalışmalarından gelir elde etmenin yeni bir yolu olarak giderek artan sayıda sanatçı ve müzisyen tarafından kullanılmaktadır (Sanction Scanner, 2023, s. 34).

NFT'ler, birbirinin yerine ikame edilebilen diğer kripto varlıklardan eşsiz ve tekil olması yönüyle ayrılmaktadır. Eşsizlik ve tekillik en çok fikir ve sanat eserlerinin ihtiyaç

duyduğu özellikler olduğu için NFT'ler genellikle, yalnızca fikir ve sanat eserleri ile ilişkili olarak algılsa da herhangi bir varlık NFT formunda ifade edilebilmektedir. NFT'ler bir varlığın orijinalliğini dağıtık defter teknolojisi ile temin etmekte ve korumaktadır (Tevetoğlu, 2021, ss. 73-74). Avantajlarına rağmen NFT'ler henüz diğer kripto varlıklara kıyasla yeterli benimsenme düzeyine ulaşmamıştır. Erişilemezlik, teknolojinin yeniliği, işlem ücretlerinin oynaklığı, gerçek dünya varlıklarını NFT'lere bağlama zorluğu gibi nedenler NFT'lerin yaygın olarak benimsenmesinin önünde engel oluşturmaktadır (Lau, 2020, s. 4).

Özetle, kripto varlıklar; kriptografi ve dağıtık defter teknolojisine dayanan, dijital şekilde oluşturulan ve işlem gören, itibari para birimlerinin veya diğer finansal varlıkların temsillerini içermeyen dijital bir değer temsidir. David Chaum'un gizlilik ve güvenlik üzerine yaptığı öncü çalışmalar, kripto varlıkların gelişimine ilham kaynağı olmuştur. Kripto varlıkların benimsenme oranı ise çeşitli özellikleri ve teknik altyapısı sayesinde güven algısı çerçevesinde her geçen gün artmaya devam etmektedir. Ayrıca kripto varlıklar etrafında inşa edilen iş modelleri, kripto varlık kullanıcıları, madenciler, kripto varlık hizmet sağlayıcıları, kripto varlık yaratıcıları ve kripto varlık arz edenler gibi yeni aktör kategorilerini meydana getirmiştir. Kullanım amacı, hukuki niteliği, ekonomik yönü gibi çeşitli açılardan farklı sınıflandırmalara tabi tutulabilen kripto varlıkların, kendi bağımsız dağıtık defter teknolojisini kullanıp kullanmadığına göre teknik açıdan Coin ve Token şeklinde sınıflandırılması mümkündür. Coin'ler, Bitcoin ve alternatifleri Altcoin'ler ile Altcoin'ler içerisinde incelenmesi mümkün olan gizlilik tabanlı kripto varlıkları içermekteyken Token'lar; Ödeme Token, Fayda Token, Menkul Kıymet Token ve NFT'leri içermektedir. Kripto varlıklar, çeşitli avantajları sayesinde yasal amaçlara yönelik finansal işlemlerde önemli fırsatlar yaratırken, aynı zamanda terörizmin finansmanı gibi yasa dışı faaliyetlerde yeni olanaklar sağlamaktadır.

1.4. Birinci Bölüme İlişkin Değerlendirme

Bu bölümde, tezin esas amacı doğrultusunda belirlenen “*Kripto varlıklar nedir? Kripto varlıklar nasıl ortaya çıkmış ve gelişmiştir?*”, “*Kripto varlıkların ve dayandığı teknolojinin özellikleri ve teknik unsurları nelerdir?*”, “*Kripto varlıklar ve dayandığı teknoloji hangi amaçlarla kullanılabilir?*” şeklindeki tezin alt sorularına yanıtlar aranmıştır. Bu bağlamda, düzenleyici alanda net bir tanıma sahip olmamakla birlikte zaman

içerisinde farklı şekillerde ifade edildiği görülen, kripto para birimlerini de kapsayan daha geniş bir kavram olan kripto varlıklara getirilen çeşitli tanımlar incelenmiştir. Kripto varlıkların ortaya çıkışı ve gelişiminin, küresel krizler ile gizlilik ve güvenlik odaklı çalışmalardan etkilendiği, kripto varlıkların kullanılması ve benimsenmesinde ise merkezi otoriteye bağımlı olmadan güvenli ve şeffaf işlemlerin gerçekleşmesini sağlayan teknik unsurlarının önemli rol oynadığı ifade edilmiştir. Dolayısıyla, kripto varlıkların ne olduğu ile nasıl ortaya çıktığı ve geliştiği ortaya konmuştur.

Diğer taraftan, gizlilik, bütünlük ve inkâr edilemezlik gibi veri güvenliği temalarını sağlayan kriptografinin, kripto varlıklar ile kripto varlıkların dayandığı blokzinciri gibi dağıtık defter teknolojilerinin güvenliği ve bütünlüğü için temel bir unsur olduğu açıklanmıştır. Ayrıca kripto varlıklarda yaygın olarak kullanılan asimetrik şifreleme kriptografi yönteminin, gizlilik için bilginin şifrenmesi ve doğruluk için dijital imza hususları ile birlikte önemli bir güvenlik katmanı sağladığı ifade edilmiştir. Merkezi olmayan dağıtık yapısı sayesinde güvenli ve şeffaf bir veri yönetimi ile veri transferi sağlayan blokzinciri teknolojisinin, kripto varlık işlemlerinin güvenli, şeffaf, doğrulanabilir ve geri alınamaz şekilde merkezi araçlar kullanılmadan doğrudan iki taraf arasında gerçekleştirilmesini mümkün kıldığı detaylandırılmıştır. Dolayısıyla, kripto varlıkların ve dayandığı teknolojinin özellikleri ve teknik unsurlarının neler olduğu ortaya konmuştur.

Ek olarak, kripto varlıklar ve temelinde yatan dağıtık defter teknolojisinin kullanım amaçları da incelenmiştir. Özellikle blokzinciri teknolojisinin, varlıkların izlenmesi ve işlemlerin kaydedilmesi açısından finans, tedarik zinciri yönetimi, sağlık, emlak, fikri mülkiyet gibi çeşitli sektörlerde potansiyel uygulama alanlarına sahip olduğu dolayısıyla değerli bir teknoloji olarak kabul edildiği açıklanmıştır. Ayrıca, teknik açıdan Coin ve Token şeklinde sınıflandırılabilen kripto varlıkların, sağladığı pek çok fayda ile birlikte yasal ve meşru amaçlara yönelik olarak kullanılabildiği ifade edilmiştir. Öte yandan, Coin'lerin ve kullanım amaçlarına göre bazı Token'ların, doğrudan kullanıcı kimliği ile ilişkilendirilememe gibi sağladığı gizlilik özelliklerinin suistimal edilerek, merkezi olmayan dağıtık yapısı ve sınır ötesi transfer kabiliyetleri nedeniyle terörizmin finansmanı gibi suç faaliyetlerinde de kullanılabildiğine değinilmiştir. Dolayısıyla, kripto varlıkların ve dayandığı teknolojinin hangi amaçlarla kullanılabildiği ortaya konmuştur.



İKİNCİ BÖLÜM

KRİPTO VARLIKLARIN TERÖRİZMİN FİNANSMANINDA KULLANILMASI

2.1. Terör ve Terörizm

2.1.1. Terör Kavramı

“Terör” kavramı Türkçe’de (TDK, 2022) “*Karşı tarafa korku salma, cana kıyma, malı yakıp yıkma, yıldırı, tedhiş*” olarak tanımlanmaktadır. Tanımdan da anlaşılacağı üzere eylemin içeriğindeki “*şiddet kullanımı*” veya “*şiddet tehdidi*” açık bir şekilde ifade edilmişken, “*karşı taraf*”ın kim olduğu veya eylemin amacı gibi hususlar muallakta kalmaktadır.

Akademik literatüre kavramsal tanımlamayı ilk kazandıran yazarlardan biri olan Thornton (1964, s. 71) “*terör*” kavramını, iç savaş bağlamında ele almış ve eylemi, siyasi hedeflere ulaşmak için şiddet kullanımı veya şiddet tehdidini içeren rasyonel bir tercih, araç olarak sınıflandırmıştır. Bu sınıflandırmayla Thornton, terör olarak nitelendirilen ve geniş anlamda kullanılan kavramı, politik amaçlar ve şiddet içeriği ile sınırlandırmıştır. Ayrıca terörü, “*şiddet kullanımını veya tehdidini gerektiren, normal dışı yollarla siyasi davranışı etkilemek için tasarlanmış sembolik bir eylem*” olarak tanımlamıştır (Thornton, 1964, s. 73).

“*Mevcut rejim içinde rutin olarak işleyen siyasi mücadele biçimlerinin dışındaki düşmanlara yönelik tehditlerin ve şiddetin asimetric olarak uygulanması*” şeklindeki benzer bir tanımlama yapan Tilly (2004, s. 9), terörün bir stratejisi olduğunu savunmaktadır. Tilly bu stratejideki başarının; hedefin tasvip edilmeyen davranışını değiştirmesi veya engellemesi, uygulayanların potansiyel müttefikler nezdindeki konumunu yüceltmesi ve üçüncü tarafları, uygulayıcıların amaç ve hedeflerine daha fazla yöneltmesiyle ilişkili olduğunu belirtmektedir.

Türkiye Barolar Birliği’nin hazırlamış olduğu “*Türkiye ve Terörizm*” başlıklı Rapor’da (2006, s. 4) ise terörün; iradi olmadan da meydana gelebilen, örgütlenme gereksinimi olmayan, sistemsiz, genellikle anlık veya kısa süreli bir şiddet olgusunu ifade ettiği

belirlenmektedir. Fakat 3713 sayılı Terörle Mücadele Kanunu (1991, s. 1), bahse konu eylemlerin örgüt bünyesinde olması gerektiğini şart koştuğu terör tanımlamasını aşağıdaki gibi yapmaktadır:

“Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.”

Bu tanımlamalardan yola çıkarak bir eylem hakkında “*terör*” nitelendirmesi yapabilmek için ilk olarak bu eylemin politik bir amacının bulunması, ikinci olarak içeriğinde şiddet veya şiddet tehdidi bulunması gerektiği sonucuna varılabilmektedir.

2.1.2. Terörizm Kavramı

“*Terör*” kavramı ile “*terörizm*” kavramı arasında önemli bir farklılık bulunduğunu belirten Wilkinson (1974, ss. 17-18), bir veya bir dizi rastgele eylem terör olarak tanımlanabilirken, bunların terörizm olarak nitelendirilemeyeceğini ifade etmektedir. Terörizmi ise devlet, örgüt, hareket ya da kişi tarafından uygulanmasından bağımsız şekilde, terör eyleminin sürekli ve organize bir şekilde yürütülen politikaya verilen isim olarak tanımlamaktadır. Wilkinson ayrıca sistematik bir şekilde yürütülen terörizmin örgütsel yapıya ve terör teorisine veya ideolojisine sahip olması gerektiğini vurgulamaktadır. Dolayısıyla Hardman’ın (1936, ss. 575-576) da belirttiği üzere terörizm, örgütlü bir grup, parti ya da kuruluşun amaç ve hedeflerine ulaşmak için sistematik şiddet kullanma yöntemine veya yöntemin ardındaki teoriye verilen isimdir. Crenshaw (1981, s. 380) terörizmi, devletin otoritesine meydan okuyarak, sivil bir nüfusu kontrol etmek veya amaçlar doğrultusunda yönlendirmek için sistematik olarak korku ve endişe yaratma olarak nitelendirmektedir. Taktiksel açıdan iradi ve örgütlü terör eylemlerinin sistemli ve uzun

sürekli kullanılarak stratejiye dönüştürülmesi terörizm kavramı ile açıklanmaktadır (Türkiye Barolar Birliği, 2006, s. 4).

Terörizmin kendisine özgü birtakım karakteristik özelliklerini aşağıda belirtildiği üzere maddeler halinde toplamak mümkündür (Hoffman, 2006, ss. 40-41; Jenkins, 1975, ss. 4-7; Richardson, 2006, ss. 20-23; Wilkinson, 2011, s. 4):

- Terörizmin amacı ve motivasyonu politiktir.
- Eylem şiddet veya şiddet tehdidi içermelidir.
- Terörizm mesaj iletme amacı gütmektedir. Bir kişinin ölümü milyonlarca kişiyi tedirgin ettiğinden terörizm insanları seyrettirmektedir.
- Toplum tarafından kabul gören protesto, uyuşmazlık ve görüş ayrılığı gibi muhalefet normlarının haricinde normal dışı yollar kullanılmaktadır.
- İcra edilen eylemin ve etkilenen mağdurun sembolik bir anlamı vardır. Eylemin etkisi mağdurun sembolik gücüyle doğru orantılıdır. Geniş kitleyi etkilemek için psikolojik etki, fiziksel etkiden daha önemlidir.
- Önceden tasarlanmış ve ayrıntılı olarak planlanmıştır.
- Devletlerin kullanmadığı anlamına gelmese de terörizm çoğunlukla devlet dışı aktörlerin veya devlet altı grupların bir eylemidir.
- Kurban, daha geniş bir kitlenin veya sosyal grupların davranışlarını ya da devlet otoritesini etkilemenin bir aracı olarak rastgele ve sembolik olarak seçilmektedir.
- Hiyerarşik bir sistemle birbirine bağlı veya gizli hücre yapılanması ile teşkil edilmiş bir örgüt ya da ideolojik amaç veya örnek alınan hareket, lider tarafından etkilenen, motive olan veya ilham alan grup ya da birey tarafından gerçekleştirilmektedir.
- Terörizm güçsüzün silahı olduğundan, yarattığı etki ile güç kazanmaya ve bu gücü pekiştirmeye hizmet etmektedir.
- Terörizm toplum içinde yaygın bir kargaşa ortamı yaratarak toplumu demoralize etmeyi ve toplumsal düzeni bozmayı amaçlamaktadır.

Tanımlama ve açıklamalardan da anlaşılacağı üzere sürekli ve sistematik bir şekilde terör eylemleri icra edebilmek için terör örgütlerinin sağlam bir teorik veya ideolojik altyapıya, önceden hazırlanmış bir programa, ayrıntılı bir şekilde oluşturulmuş organizasyonel yapıya sahip olması gerektiği açıktır. Terör örgütlerinin bahse konu bu

organizasyonel yapının devamlılığını sağlayabilmesi ve faaliyetlerini yürütebilmesi için bazı kaynaklara sahip olması gerekmektedir. Bu sebeple diğer başlıkta terörizmin finansmanı konusuna değinilecektir.

2.2. Terörizmin Finansmanı

2.2.1. Terörizmin Finansmanı Kavramı

Siyasi şiddet eylemine başvuran terör örgütlerinin belirlemiş olduğu talepleri elde etmesi ve örgütsel amaca ulaşabilmesi için öncelikli olarak hayatta kalabilmesi yani varlığını idame ettirebilmesi gerekmektedir. Örgütsel devamlılığın sağlanmasındaki en önemli hususlardan biri de şüphesiz maddi ve maddi olmayan bütün kaynakların doğru bir şekilde planlanması, yürütülmesi ve yönetilmesi ile direkt ilişkilidir. Terör örgütlerinin varlığını sürdürebilmek için ihtiyaç duyduğu söz konusu kaynakları, “*terörist kaynak sağlama*” olarak nitelendiren Myres (2012, s. 694) ve “*asgari gereksinimler*” olarak sınıflandıran Vittori (2011, ss. 13-14) üç ayrı kategoriye ayırmaktadır:

- Para veya hazır likit varlıklar,
- Eylem için ihtiyaç duyulan teçhizat, malzemeler ve yaşamsal ihtiyaçlar gibi maddi varlıklar,
- Güvenli ortam, operasyonel alan, güvenlik, istihbarat, yeterli düzeyde eğitim ve uzmanlık gibi maddi olmayan gereksinimler.

Yukarıda belirtilen kaynaklar terör örgütlerinin idari ve askeri faaliyetlerini etkili ve istikrarlı bir şekilde yürütmesi için hayati öneme sahiptir. Bu bağlamda “*terörizmin finansmanı*” kavramı, terör örgütü veya üyelerinin ya da bunlar ile birlikte hareket eden müttefik kuruluş ve vekillerin yararına para veya mali kaynakların elde edilmesi, kullanılması, yönetilmesi ve dağıtılması gibi finansal faaliyetlerin bir parçası olarak açıklanmaktadır (Myres, 2012, ss. 694-695).

ABD’ye yönelik 11 Eylül 2001 saldırısı sonrası terörizmin finansmanı konusundaki çalışmaların hızlandığı görülse de bahse konu kavram hakkında ilk girişimin 1994 yılında Birleşmiş Milletler Genel Kurulu tarafından yapıldığı söylenebilmektedir. Terörizme son vermek için uluslararası iş birliğinin güçlendirilmesi ve etkinliğinin arttırılmasına yönelik

49/60 sayılı ve “*Uluslararası Terörizmin Ortadan Kaldırılmasına Yönelik Tedbirler (Measures to Eliminate International Terrorism)*” başlıklı karar metninde ilk defa terör faaliyetlerinin finanse edilmesinin engellenmesi gerekliliği vurgulanmıştır (United Nations, 2008a, s. 351). Terörizmin finansmanına yönelik Birleşmiş Milletler öncülüğündeki asıl gelişmenin 1999 yılında hazırlanan “*Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme (International Convention for the Suppression of the Financing of Terrorism)*” olduğu görülmektedir. Bu sözleşme ile ilk defa terörizmin finansmanı alanına giren eylemler tanımlanarak suç kapsamına alınmış ve bu suçların işlenmesi amacıyla kullanılan veya tahsis edilen fonların ve yine bu suçlardan elde edilen gelirlerin belirlenmesi, tespiti, dondurulması veya el konulması için taraf devletlere yükümlülük getirmiştir (United Nations, 2008b, ss. 90-94). Sözleşmenin diğer bir katkısı ise ikinci maddede yer alan terörizmin finansmanı kavramı hakkında tanımlamaya yer vermesidir. Sözleşmeye göre terörizmin finansmanı aşağıdaki gibi tanımlanmıştır (United Nations, 2008b, s. 91):

“Herhangi bir kişi, herhangi bir yolla, doğrudan veya dolaylı olarak, belirtilen suçları gerçekleştirmek amacıyla tamamen veya kısmen, hukuka aykırı ve kasıtlı olarak, kullanılması niyetiyle veya kullanılacağını bilerek fon sağlar veya toplarsa, bu Sözleşme anlamında bir suç işlemiş olur:

(a) Ekte sayılan anlaşmalardan birinin kapsamına giren ve tanımlanan bir suç teşkil eden eylem; veya

(b) Doğası veya bağlamı itibarıyla bir eylem, bir halkı korkutmak ya da bir hükûmeti veya uluslararası bir kuruluşu herhangi bir eylemi yapmaya veya yapmaktan kaçınmaya zorlamak amacı gütmesi durumunda, bir sivilin veya bir silahlı çatışma durumundaki düşmanlıklarda aktif olarak yer almayan herhangi bir kişinin ölümüne veya ciddi bedensel yaralanmasına neden olmayı amaçlayan diğer herhangi bir eylem.”

Türkiye için kavramsal tanımlama ilk olarak 2013 yılında yürürlüğe giren 6415 sayılı “*Terörizmin Finansmanının Önlenmesi Hakkında Kanun*” ile belirlenmiştir. Kanunun 1’inci maddesinde belirtildiği gibi terör ve terörizmin finansmanı ile etkin bir şekilde mücadele etmek için (Terörizmin Finansmanının Önlenmesi Hakkında Kanun, 2013, s. 1):

“1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşmenin ve Birleşmiş Milletler Güvenlik Konseyinin bu Kanun kapsamındaki terör ve terörizmin finansmanı ile mücadeleyle ilişkin kararlarının uygulanması ile terörizmin finansmanı suçunun düzenlenmesi ve terörizmin finansmanının önlenmesi amacıyla malvarlığının dondurulmasına ilişkin usul ve esasların belirlenmesi amacıyla hazırlanmıştır.”

Aynı Kanun, “Terörizmin Finansmanı Suçu”nu tanımlamak maksadıyla fon sağlanması veya toplanması yasaklanan fiilleri 3’üncü maddesinde ele almış ve bunları üç kategoriye ayırmıştır (Terörizmin Finansmanının Önlenmesi Hakkında Kanun, 2013, s. 2):

- Bir halkı korkutmak veya sindirmek ya da ulusal veya uluslararası bir otoriteyi bir şeyi yapmaya veya yapmamaya zorlamak amacıyla, kasten öldürme veya ağır yaralama fiilleri.
- 3713 sayılı Terörle Mücadele Kanunu çerçevesinde terör suçu olarak kabul edilen fiiller.
- Türkiye’nin taraf olduğu uluslararası sözleşmeler ve protokoller ile yasaklanan ve suç olarak düzenlenen fiiller.³

Dolayısıyla, 3’üncü maddede belirtilen fiillerin gerçekleştirilmesi için “tümüyle veya kısmen kullanılması amacıyla veya kullanılacağını bilerek ve isteyerek belli bir fiille ilişkilendirilmeden dahi bir teröriste veya terör örgütlerine fon sağlayan veya toplayan kişi, fiili daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde” cezalandırılacağını belirten 4’üncü madde ile terörizmin finansmanı suçu tanımlanmıştır (Terörizmin Finansmanının Önlenmesi Hakkında Kanun, 2013, s. 2).

³ Bu sözleşme ve protokoller arasında; 1) Uçakların Kanun Dışı Yollarla Ele Geçirilmesinin Önlenmesi Hakkında Sözleşme, 2) Sivil Havacılığın Güvenliğine Karşı Kanun Dışı Eylemlerin Önlenmesine İlişkin Sözleşme, 3) Diplomasi Ajanları da Dahil Olmak Üzere Uluslararası Korunmaya Sahip Kişilere Karşı İşlenen Suçların Önlenmesi ve Cezalandırılmasına Dair Sözleşme, 4) Rehine Alınmasına Karşı Uluslararası Sözleşme, 5) Nükleer Maddelerin Fiziksel Korunması Hakkında Sözleşme, 6) Sivil Havacılığın Güvenliğine Karşı Kanun Dışı Eylemlerin Önlenmesine İlişkin Sözleşmeye Munzam, Uluslararası Sivil Havacılığa Hizmet Veren Havaalanlarında Kanun Dışı Şiddet Olaylarının Önlenmesine İlişkin Protokol, 7) Denizde Seyir Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesine Dair Sözleşme, 8) Kıta Sahanelğinde Bulunan Sabit Platformların Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesine Dair Protokol, 9) Terörist Bombalamalarının Önlenmesine İlişkin Uluslararası Sözleşme bulunmaktadır (Terörizmin Finansmanının Önlenmesi Hakkında Kanun, 2013, s. 2).

Tüm bu tanımlama ve kanuni metinlerden de anlaşılacağı üzere terörizmin finansmanı, yalnızca finansman kaynağı sağlanması sürecini ifade etmemekte, aynı zamanda terör örgütlerinin toplanan fon veya değerleri saklaması, yönetmesi ve transfer etmesi süreçlerini de içermektedir (Başaranel ve Türkşen, 2019, s. 20). Terörizmin finansman aşamaları; fon veya değerlerin toplanması, kullanılmak veya saklanmak üzere ihtiyaç duyulan yere aktarılması, ihtiyaç duyulana kadar depolanması şeklinde üç düzeyden oluşan bir çerçeveye ayrılabilmekte olup (Vittori, 2011, s. 26) aşağıda başlıklar halinde incelenecektir.

2.2.2. Terörizmin Finansman Aşamaları

2.2.2.1. Toplama

Terörizmin finansmanında “*toplama*” aşamasının öncül bir rolü olduğu görülmektedir. Çünkü, diğer aşamalara geçebilmek için toplama aşamasının gerçekleşmiş olması yani terör örgütünün finansal bir kaynağa sahip olması gerekmektedir. Terörizmin finansman kaynaklarının geniş bir yelpazeye yayıldığını belirten Freeman (2011, s. 465) bu kaynakların dört genel kategoride ele alınabileceğini belirtmektedir:

- 1) Devlet Sponsorluğu: Son yıllarda azalsa da bir devletin ideolojik ya da politik çıkarları doğrultusunda terör örgütüne kaynak sağlamasıdır.
- 2) Yasa Dışı Faaliyetler: Gasp, fidye için adam kaçırma, hırsızlık, kaçakçılık, soygunculuk, korsan mal ve sahtecilik, yasa dışı vergi toplama, dolandırıcılık, şantaj gibi gelir sağlayan çeşitli suç faaliyetlerini kapsamaktadır.
- 3) Yasal Faaliyetler: Yasal olarak kurulmuş farklı sektörlerdeki iş yeri ve şirketlerin işletilmesinden elde edilen geliri ifade etmektedir.
- 4) Halk Desteği: Sempatizanlardan toplanan bağışlar, üyelerden alınan aidatlar, diaspora topluluklarından sağlanan fonları içermektedir.

Terör örgütlerinin kendi güvenliğini sağlama, etkili eylem yapabilme ve hayatta kalma becerisini geliştirebilme konularını etkileyen önemli faktörlerden biri de finansman kaynaklarının çeşitliliği, güvenilirliği ve verimliliğidir. Dolayısıyla, ihtiyaç duyulan fonların nereden ve ne şekilde toplanacağı terör örgütlerinin faaliyetlerini olumlu ya da olumsuz şekilde doğrudan etkilemektedir (Barrett, 2012, ss. 722-723). Bu sebeple terör örgütleri oldukça çeşitli kaynak ve yöntemleri birtakım kriterlere göre değerlendirerek seçmektedir.

Her kaynağın ve yöntemin kendi içerisinde birçok avantajı ve dezavantajı olduğuna dikkat çeken Freeman (2011, ss. 463-465) bu kriterleri aşağıda kısaca açıklanan altı başlık altında ele almaktadır.

- 1) Miktar: Örgütlerin daha güçlü ve kabiliyetli olmasını sağlayacak, mümkün olduğunca çok miktarda para getiren kaynakların seçilmesi.
- 2) Meşruiyet: Hem üyeleri hem de destekçileri tarafından meşru olarak görülen finansal kaynakların tercih edilmesi, örgüt içerisinde veya destekçiler arasında tasvip edilmeyecek kaynaklardan (uyuşturucu ticareti, fidye için çocuk kaçırma, kişisel yolsuzluk, vb.) kaçınılması.
- 3) Güvenlik: Örgütü ifşa edecek veya istihbari zafiyet yaratacak kaynakların tercih edilmemesi.
- 4) Güvenilirlik: Özellikle faaliyet yürütülen coğrafya ve demografik yapı ile doğrudan ilişkili, tutarlı gelir elde edilebilecek finansal kaynakların tercih edilmesi.
- 5) Kontrol: Örgütün amaç ve hedeflerini yönlendirecek (sponsor devlet veya özel kuruluş), alt/yerel birimlerin güçlenmesini sağlayacak ya da aynı kaynaktan yararlanan aktörler arasında rekabet yaratacak kaynaklardan ziyade istenilen zamanda ve istenilen miktarda gelir sağlayacak kaynakların tam olarak himaye altında bulundurulması.
- 6) Basitlik: Uzmanlık istemeyen, az çaba gerektiren, az maliyetli ve basit süreçlere sahip kaynakların tercih edilmesi.

Sonuç olarak terörizmin finansman kaynaklarının seçilmesine yönelik bu kriterler örgütsel davranışı büyük ölçüde etkilemektedir. Örneğin, sponsor devlete dayanan tek bir kaynak, terör örgütünün büyük miktarda finansman elde etmesini sağlarken, diğer taraftan örgütün sponsor olan devletin güdümüne girmesine de neden olabilmektedir. Aynı şekilde, büyük miktarda ya da basit yoldan finansman elde etmeye yönelen terör örgütü bir süre sonra kontrolü kaybetme veya meşru olarak görülen zeminden çıkma riski ile karşı karşıya kalabilmektedir (Freeman, 2011, ss. 464-465). Dolayısıyla terör örgütleri için finansman kaynağı ve yönteminin seçimi, sağlanan fayda ve alınacak risk faktörlerine göre değişkenlik gösterebilmektedir. Terör örgütleri bu faktörleri göz önünde bulundurarak, kripto varlıklar gibi yeni teknolojileri ve ürünlerini de kaynak sağlamada kullanabilmektedir.

2.2.2.2. Aktarma

Fon veya değerlerin toplanması terörizmin finansmanının yalnızca ilk aşamasıdır, toplanan fonlar dağıtım sürecinden de geçmektedir (Croissant ve Barlow, 2007, s. 138). Terör örgütlerinin çeşitli kaynaklardan elde ettiği fonları ve değerleri ihtiyaç duyulan yere kaydırması “*aktarma*” aşamasını oluşturmaktadır. Freeman ve Ruehsen (2013, ss. 6-7) birtakım kanıtlara, varsayımlara ve davranışsal çıkarımlara dayanarak terör örgütlerinin fon transfer yöntemini seçerken; hacim, risk, kullanışlılık, basitlik, maliyet ve hız gibi nitelikleri göz önünde bulundurduğunu belirtmektedir. Bahse konu niteliklere ilaveten fonların aktarıldığı yerin kültürel, coğrafi ve yapısal koşulları aşağıdaki maddeler halinde listelenen transfer yöntemlerinin seçilmesini etkilemektedir (Freeman ve Ruehsen, 2013, ss. 7-21):

- Nakit paranın kuryeler aracılığıyla fiziki olarak taşınmasını sağlayan “*nakit kuryeler*”,
- Hawala/Hundi (Orta Doğu ve Güney Asya), Fei Ch’ien (Çin), Phoe Khan (Tayland), Door-to-Door (Filipinler) gibi geleneksel köklere ve etnik bağlara dayanan “*gayri resmi transfer sistemleri*”,
- Yasal olarak faaliyet yürüten dövizciler, para aktarıcılar, tahsilatçılar gibi “*para hizmeti işletmeleri*”,
- Mevduat alma ve bu mevduatlara erişim sağlama izni verilen kuruluşları içeren “*resmî bankacılık*” sektörü,
- Birtakım malların fazla veya eksik faturalandırılarak paranın aktarılmasını sağlayan “*sahte ticari faturalama*”,
- Altın ve elmas gibi maddi değeri yüksek, kolay nakde çevrilebilir malların kullanıldığı “*yüksek değerli emtialar*”,
- Ön ödemeli kartlar, mobil ödemeler veya dijital para birimlerinin kullanımını içeren “*diğer yöntemler*”.

2.2.2.3. Depolama

Terörizmin finansmanında bir diğer aşama ise çeşitli kaynaklardan elde edilen fon veya değerleri “*depolama*” aşamasıdır. Terör örgütleri elde ettikleri fonları güvenli bir şekilde depolamayı ve gerektiği zaman (terör eylemlerinde, lojistik ve seyahat

ihtiyaçlarında, güvenli ortamların tesis edilmesinde, vb. durumlarda), gerektiği yere aktarmayı veya nakde dönüştürmeyi istemektedir (Keatinge vd., 2018, s. 27).

Diğer taraftan terör örgütleri tarafından depolanan fonların güvenlik kuvvetleri tarafından tespit edilmemesi gerekmektedir. Bu sebeple terör örgütleri, geleneksel bankacılık sistemlerine yönelik alınan tedbirlerden dolayı sahip olduğu fonların tespit edilerek dondurulmasını veya el konulmasını önlemek için faaliyet yürüttüğü coğrafyanın fiziksel ve kültürel koşullarına uyumlu değerli madenlere veya teknolojik gelişmelerle ortaya çıkan, takip edilmesi ve erişilmesi zor, kolay transfer imkânı sunan alternatif dijital sistemlere başvurmayı tercih edebilmektedir (Eisermann, 2020, s. 27).

Terör örgütleri bu aşamada, depolanan fonları hem güvence altına alacak hem de bunlardan daha fazla gelir elde edecek yatırım fırsatlarını da değerlendirmektedir. Özellikle toplama faaliyetinden elde ettikleri fonların azalması, kesilmesi veya kullanılamaması durumunda terör örgütleri, yaptıkları yatırımlar sayesinde kendi kendilerini finanse etme olanağı bulmaktadır. Bu kapsamda terör örgütleri, gelir elde etmek için suç piyasasına, kayıt dışı ekonomiye ya da fırsatların uygun olduğu durumlarda meşru faaliyetlere yönelebilmektedir (Myres, 2012, s. 703). Terör örgütleri açısından, mevcut fonların suç piyasası içerisinde değerlendirilmesinin diğer yollara kıyasla oldukça kazançlı getiriler sağlasa da potansiyel güvenlik riskleri barındırdığı bilinmektedir.

2.2.3. Terörizmin Finansmanı ve İnternet

Küreselleşme ve teknolojik ilerlemeler, internetin hayatımızın önemli bir parçası haline gelmesini sağlarken, aynı zamanda terör örgütlerinin de internetin avantajlarından yararlandığı anlamına gelmektedir. Keene'e göre (2011, ss. 359-368) internet; bir taraftan terör saldırılarının hedefi olabilecek ve korunması gereken önemli bir ulusal altyapı, diğer taraftan terör örgütlerinin stratejik ve operasyonel kısa, orta ve uzun vadeli hedeflerine ulaşmak için kullandıkları bir araç olarak terörle mücadele açısından iki tarafı keskin bir kılıçtır. Terör örgütleri interneti; radikalleşme, üye toplama, plan yapma gibi örgütlenme amaçlarına ek olarak, terörizmin finansmanı kapsamında mali destek sağlama, mali suç işleme, terör amaçlı yasa dışı fon toplama, terör ağı üzerinden fon transferi yapma, terör amaçlarında kullanılmak üzere fon saklama amacıyla kullanabilmektedir.

İnternet ve diğer dijital teknolojilerin kullanılmasıyla gerçekleştirilen siber suçlar, suçlulara sınır ötesinde faaliyet göstermeyi sağlayarak, suçların daha büyük çapta, daha hızlı ve daha yüksek getiri potansiyeliyle gerçekleştirilmesine imkân tanımıştır. Siber suçlar aynı zamanda; kredi kartı dolandırıcılığı, uyuşturucu ticareti, şantaj, silah ve mühimmat kaçakçılığı, kimlik hırsızlığı, suç gelirlerinin aklanması gibi suçların çevrimiçi ortamda gerçekleştirilmesiyle de oluşmakta ve terör örgütleri tarafından operasyonel veya finansal amaçlar için kullanılmaktadır. Ayrıca terör örgütleri, internet şirketleri kurarak ve çevrimiçi ürün satışı yaparak yasal ticari faaliyetler yoluyla veya çevrimiçi kâr amacı gütmeyen kuruluşlar kurarak bağış yoluyla gelir elde etmektedir (Carroll ve Windle, 2018, ss. 287-288). Siber araçlar ve internet, terör örgütlerinin finansman sağlama çabalarına çeşitli şekillerde büyük katkıda bulunmaktadır (United Nations Office on Drugs and Crime, 2012, s. 7).

Başlangıcında yapılması gereken yatırım, gerekli teknik beceri ve tespit edilme riski nedeniyle siber araçların, terör örgütleri tarafından diğer finansman yöntemlerine kıyasla daha az kullanılabileceği söz konusuysa da çeşitli geleneksel yöntemler siber araçlarla etkinleştirilerek aynı operasyonda finansman sağlanması ve ulusal ekonomik altyapıya zarar verilmesi mümkün olduğu için siber araçların ve internetin terör örgütlerinin ilgisini çektiği söylenebilmektedir (Carroll ve Windle, 2018, s. 288). İnternet terör örgütlerinin çeşitli ihtiyaçlarına cevap vererek, terör örgütleri tarafından farklı işlevlerde kullanılmaya devam etmektedir.

Özetle terör, siyasi davranışı normal dışı yollarla etkilemek için tasarlanmış, şiddet kullanımını veya tehdidini içeren sembolik bir eylemken, terörizm terörün, sistematik, sürekli ve çoğu kez örgütlü kullanımını içermektedir. Terör örgütleri, organizasyonel devamlılığını sağlamak adına maddi ve gayri maddi kaynaklar ile birlikte finansman kaynaklarına ihtiyaç duymaktadır. Terörizmin finansmanı, terör örgütleri tarafından fon veya değerlerin toplanması, aktarılması ve depolanması aşamalarını ihtiva etmektedir. Terör örgütleri finansman kaynaklarını, miktar, meşruiyet, güvenlik, güvenilirlik, kontrol ve basitlik gibi kriterleri dikkate alarak yasal veya yasa dışı faaliyetlerden ya da halk veya devlet desteği yoluyla sağlayabilmektedir. Diğer taraftan terör örgütleri, toplanan söz konusu fonları hacim, risk, kullanışlılık, basitlik, maliyet ve hız gibi kriterleri göz önünde bulundurarak çok çeşitli yöntemlerle ihtiyaç duyulan yere aktarmakta veya ihtiyaç duyulana dek depolamaktadır. Terörizmin finansmanında, her üç aşama için de teknolojinin

ilerlemesiyle birlikte hayatımızın vazgeçilmez bir parçası haline gelen internet ve internetin evrimiyle gelişen kripto varlıklar kullanılabilmektedir.

2.3. Terörizmin Finansmanı Amacıyla Kripto Varlıkların Kullanılması

Kripto varlıklarla yapılan işlemlerin tamamı suç teşkil etmemekle birlikte, çeşitli kötü niyetli aktörler kripto varlıkları farklı yasa dışı amaçları için kullanmaya başlamıştır. Kripto varlıkların genel olarak üç ana yasa dışı kullanım durumunun yasa dışı mal ve hizmetlerin ticareti, suç gelirlerinin aklanması ve terörizmin finansmanı olduğu söylenebilmektedir (Silfversten vd., 2020, s. 33). Kripto varlıkların terörizmin finansmanı amacıyla kullanılması dikkat çeken bir konu haline gelmiştir.

Soğuk Savaş'ın sona ermesiyle birlikte yeni bir dünya düzeninin ortaya çıkması ve terörizmi desteklemeye istekli devletlerin sayısının azalmasıyla birlikte, terör örgütleri finansman sağlamanın yeni yollarını aramak zorunda kalmıştır (Kfir, 2020, s. 118). Dünya ekonomisinin ve teknolojinin ilerlemesiyle birlikte, terörizmin finansman yöntemleri çeşitlenmiş ve karmaşık hale gelmiştir. Terör örgütleri, genellikle faaliyet gösterdikleri bölgenin ekonomik durumuna bağlı olarak çeşitli finansman yöntemlerini bir araya getirme eğilimindedir (Wang ve Zhu, 2021, s. 2336). Terörizmin finansmanında kaynak ve yöntem seçimi, terör örgütünün yapısına bağlı olarak değişiklik gösterebilmekte ve zamanla gelişebilmektedir (Dion-Schwarz vd., 2019, s. 8). Dünya üzerinde giderek artan bir kullanım oranına sahip olan kripto varlıklar, terör örgütlerinin de ilgisini çekmiştir.

Suç gelirlerinin aklanması ve terörizmin finansmanının önlenmesine yönelik ulusal ve uluslararası düzenlemeler karşısında, terör örgütleri kripto varlıkları finansman faaliyetlerinde kullanmaya başlamıştır. Kripto varlıklar, terör örgütleri için bağış toplama faaliyetleri gibi yeni fon kaynakları elde etmede ve bu fonları ihtiyaç halindeki kişilere hızlı, anonim ve küresel bir şekilde aktarmada kullanılmaktadır (Silfversten vd., 2020, s. 8). Ayrıca, terör örgütlerinin faaliyetlerini finanse etmek amacıyla söz konusu fonların saklanması da kripto varlıkların tercih edebildiği görülmektedir (Whyte, 2019, ss. 12-15). Terör örgütleri kripto varlıkları, sahip olduğu varlıklarını çeşitlendirmek, Dark Web'de varlık göstermek, mevcut kaynaklarını değer oynaklığına karşı korumak gibi çeşitli amaçlarla kullanabilmektedir (Patel ve Pereira, 2020, s. 4).

Terör örgütlerinin, finansal sistemlere sınırlı erişime sahip oldukları durumlarda veya kripto varlıkların diğer seçeneklere göre önemli avantajlar sunması halinde, finansman faaliyetlerinde kripto varlık kullanımını artırabilecekleri değerlendirilmektedir. Ayrıca, gelecekteki kripto varlık teknolojilerinde yaşanacak gelişmelerin, terörizmin finansmanı üzerinde uzun vadeli önemli etkiler yaratması muhtemel görülmektedir (Dion-Schwarz vd., 2019, ss. 1-4). Terör örgütlerinin fonların kaynağını, aktarımını, kullanımını ve saklanmasını gizlemek için operasyonel bir güvenlik avantajının olduğu durumlarda, fonları küresel ölçekte hızlı, kolay ve daha az maliyetli bir şekilde taşımalarına ve ihtiyaç duydukları mal ve hizmetleri satın almalarına olanak tanıdığı ölçüde, teknolojinin kolayca kullanılmasına ve aralarında saklanabilecekleri yeterli kullanıcının olmasına izin verecek yeterli pazar doygunluğu olduğunda yeni teknolojilere yönelebilecekleri değerlendirilmektedir (Argentino vd., 2023, s. 38).

Aşağıda, terör örgütlerinin kripto varlıkları finansman faaliyetlerinde; hangi nedenlerden dolayı kullanmayı tercih edebilecekleri veya etmeyebilecekleri, hangi yöntemlerle kullanabilecekleri ve hangi olaylarda kullandıkları incelenecektir.

2.3.1. Kripto Varlıkların Terörizmin Finansmanında Kullanılmasını Etkileyen Faktörler

Terör örgütlerinin finansman faaliyetlerinde kripto varlıkları kullanmasında pek çok olanak olduğu gibi engeller de vardır (Keatinge vd., 2018, s. 28). Kripto varlıkların terörizmin finansmanında kullanılmasını kolaylaştıran ve zorlaştıran birçok faktör bulunmaktadır.

2.3.1.1. Kolaylaştıran faktörler

Kripto varlıkların ortaya çıkışı, teknolojik ilerlemenin etkisiyle gelişen pazarın bir sonucudur (Song vd., 2023, s. 17). Kripto varlıkların geliştirilmesinin ardındaki temel motivasyonun, merkezi otoritelerin müdahalesinden kaçınılarak, işlemlerin sınırlamalar olmaksızın mahremiyet ve eşitlik ilkeleri içerisinde gerçekleşmesi olduğu söylenebilir. Bu ilkeler, kripto varlıklar çerçevesinde alternatif bir finansal sistemin gelişmesine yol açarken aynı zamanda, yüksek riskli kabul edilen ve geleneksel finansal araç ve hizmetlerden dışlanan kişiler için yeni fırsatlar yaratmıştır (Kethineni ve Cao, 2020, s. 330). İnternetin sınır ötesi doğası, kripto varlıkların finansal anlamda dünyanın dört bir yanından insan

tarafından kullanılmasına olanak tanırken, kripto varlıkların mevcut finansal piyasaları aşma potansiyeline sahip olduğu anlamına gelmektedir (Lee, 2022, s. 1).

Geleneksel finansal yöntemlere alternatif olarak ortaya çıkan kripto varlıklar, tıpkı geleneksel finansal araçlar gibi suç gelirlerinin aklanması ve terörizmin finansmanı gibi yasa dışı faaliyetlerde kullanılabilmektedir. Ancak diğer finansal araçların sunmadığı kripto varlıkların bazı benzersiz özellikleri, suç ve terör faaliyetleri açısından belirli avantajlar sağlamaktadır (Sanction Scanner, 2023, s. 33). Yüksek volatilitelerine rağmen kripto varlıkların, özellikle terör örgütleri için çekici olmalarını sağlayan özelliklere sahip olarak terörizmin finansmanında kullanılabileceği rahatlıkla söylenebilir (Wiwoho vd., 2023, ss. 103-104).

Merkezi olmayan bir finansal ekosistem üzerinde gelişen kripto varlıklar, finansal kapasitelerini artırmak için fonları küresel olarak taşıma ihtiyacındaki terör örgütleri için çekici hale gelmiştir. Kripto varlıklar, terör örgütlerine, geleneksel finansal kurumlar ve terörizmin finansmanı ile mücadele kapsamında tasarlanmış operasyonel araçları atlatmaları konusunda yeni fırsatlar yaratmıştır (Hasbi ve Mahzam, 2018, s. 1). Terörle mücadele çabaları güçlendikçe, terör örgütleri de bankalar gibi geleneksel finansal sistem içerisinde takip edilmekten kaçınmak için faaliyetlerinin finansmanında kripto varlıklar gibi alternatif yollara yönelmiştir. Terör örgütleri Bitcoin gibi kripto varlıkları, ilgili ülkelerin bankacılık sisteminin gözetim mekanizmasını aşarak terörist faaliyetleri ile diğer yasa dışı ve suç teşkil eden faaliyetleri için bir finansman aracı olarak kullanmaktadır (Majumder vd., 2019, s. 125).

Kripto varlıklar terör örgütlerine çeşitli avantajlar sunmaktadır. Hükûmetler, bankalar veya elektronik para ve ödeme kuruluşlarında olduğu gibi kripto varlık işlemlerini durduramamakta ve kripto varlıkların hükûmetin yetki alanı dahilindeki bir kripto varlık hizmet sağlayıcı hesabında tutulmadığı sürece kripto varlıkları donduramamaktadır. Ayrıca kripto varlıklara erişim sağlayan özel anahtarın ezberlenmesi suretiyle kripto varlıkların blokzinciri üzerinde saklanabilmesi, kripto varlıklara el konulması zorlaşmaktadır (Krishnan, 2020, s. 45).

Song vd. göre (2023, ss. 6-7), kripto varlıkların terörizmin finansmanında kullanılmasının tercih edilmesinde üç ana neden bulunmaktadır:

- 1) Fonların kaynağı ile lokasyon geçmişinin kolaylıkla gizlenebilmesinden kaynaklanan işlemlerin anonimliği ve transferlere ilişkin kotalar ile düzenlemeleri aşmayı kolaylaştıran fonların sınır ötesi transfer edilebilirliği,
- 2) İşlemlerin, kullanıcıların kimliği ile doğrudan ilişkilendirilememesinden kaynaklanan anonimlik ve düzenleyici alanda oluşturduğu zorluklar,
- 3) İtibari para birimine dönüştürülebilirlik ve merkezi olmayan doğası nedeniyle denetimden kaçınma imkânı.

Majumder vd. göre (2019, s. 134) ise kripto varlıkların; anonimlik, inkâr edilemezlik, merkezi gözetimin yoksunluğu veya eksikliği, düşük kullanım maliyeti ve göreceli kullanım kolaylığı, mekân ve para birimi değişikliğinde esneklik, işlem hızı, işlem karmaşıklığı ve küresel erişim gibi doğasından kaynaklanan özellikleri nedeniyle terörizmin finansmanında kullanılabileceği değerlendirilmektedir.

Toparlanacak olursa, terör örgütleri, kripto varlıkların belirli özelliklerini belirli amaçlar için yararlı bulabilmektedir (Keatinge vd., 2018, s. 30). Kripto varlıkların diğer finansal enstrümanlardan farklı şekilde terörizmin finansmanında kullanılmaya elverişli özellikleri temel olarak; anonimlik, merkeziyetsiz yapı, küresel erişim ile sınır ötesi ve hızlı transfer mekanizması, düzenleme eksiklikleri olarak dört başlık halinde sıralanabilir.

2.3.1.1.1. Anonimlik

Önceki bölümlerde değinildiği üzere kripto varlıklar ile gerçekleştirilen işlem kayıtları çoğunlukla blokzinciri gibi bir dağıtık defter teknolojisi üzerinde şeffaf bir şekilde yer alırken, işlemi gerçekleştiren tarafların gerçek kimlikleri doğrudan ağ üzerinde yer almamaktadır. Önde gelen çoğu kripto varlık borsası kimlik doğrulaması gerektirse de, dağıtılmış defter üzerinde kripto varlıklar ile gerçek dünya kimlikleri arasında bağlantı bulunmadığından kripto varlıklar bir dereceye kadar anonim özellik ihtiva etmektedir (Whyte, 2019, s. 4). Söz konusu özellik dolayısıyla kripto varlıklar; uyuşturucu ve silah kaçakçılığı, terörizmin finansmanı, suçtan kaynaklanan malvarlığı değerlerinin aklanması gibi suçlar kapsamında ödeme aracı olarak yaygın şekilde kullanılmaktadır (Bank of Russia, 2022, ss. 18-23). Ancak bahsedilen anonim özelliğin kullanıcılara tam bir gizlilik sağladığı yanılgısına düşmemek gerekmektedir. Bir kripto varlığın ne kadar anonim olduğu operasyonel ve teknik açıdan pek çok faktöre bağlıdır (Dion-Schwarz vd., 2019, s. 24).

Bitcoin gibi sözde anonim olarak nitelendirilen kripto varlıkların kullanıcıları, blokzincirinde kripto varlık cüzdanlarıyla ilişkili alfanümerik adreslerle temsil edilmekte ve işlemleriyle ilgili tarihler, değerler ve karşı tarafların kripto varlık adresleri gibi bilgiler kronolojik sırayla halka açık ve şeffaf şekilde kaydedilmektedir. Bu durum, blokzinciri üzerinde kripto varlıklar ile gerçekleştirilen işlemlerin ve işlem taraflarının takibi konusunda bir resim çıkarmayı mümkün kılmakta olup birçok özel şirketin kripto varlık işlemlerinin analizi için çeşitli araçlar geliştirdiği bilinmektedir (Keatinge vd., 2018, ss. 30-31). Blokzinciri analizi, gerçekleşen işlemlere dayalı olarak belirli kripto cüzdanları arasındaki ilişkileri belirlemenin yanı sıra mevcut bilgilere göre cüzdanların karıştığı çeşitli suçlar kapsamında etiketlenmesini içermekte ve gerçekleştirilen işlemlerin yasa dışı faaliyetlere karışma riskinin düzeyine göre değerlendirilmesine olanak tanımaktadır. Blokzinciri üzerindeki işlemler cüzdan adresleri arasında gerçekleştiğinden, bir cüzdanın gerçek sahibi, cüzdanın bir kimlik doğrulama sürecinden geçen müşterilere hizmet sağlayan platformlarda kullanılmış olması durumunda belirlenebilmektedir (*Cryptocurrencies: Trends, Risks, and Regulation*, 2022, ss. 18-23; Song vd., 2023, s. 14). Doğası gereği yanıltıcı ve son derece zor olabileceği unutulmadan, kripto varlık borsaları tarafından kullanıcı bilgilerinin tutulması ve bilgi paylaşımına yönelik düzenlemeler sayesinde, kripto varlıkların sahiplik ve konum açısından izlenmesi ve işlem desenlerinin analizi mümkün olmaktadır (Whyte, 2019, ss. 4-5). Sonuç olarak, izlenebilirlik potansiyeli nedeniyle kripto varlık kullanımı kullanıcılarına tam bir anonimlik sağlamak yerine daha fazla anonimlik sağlamaktadır (Carroll ve Windle, 2018, s. 288).

Bununla birlikte, gerçekleştirilen işlemlerin gizliliğini sağlamayı amaçlayan çeşitli araç ve yöntemler, anonimlik katmanı ekleyerek kripto varlık işlemlerinin kapsamlı bir şekilde izlenmesini zorlaştırmaktadır (*Cryptocurrencies: Trends, Risks, and Regulation*, 2022, s. 18). Bu duruma örnek olarak verilebilecek olan işlemlerin ve kullanıcıların gizliliğini artırmak için tasarlan gizlilik tabanlı kripto varlıklar ile işlemlerin karıştırılarak izlenmesini zorlaştıran karıştırıcı (mixer) hizmetleri tezin ilerleyen bölümlerde detaylandırılacaktır. Bunların yanı sıra, kripto varlık işlemlerinin gizliliğini artıran başka yöntemler de mevcuttur. Terörizmin finansmanının tespit ve müdahalesinden kaçınmak için anonimliğin önemli bir faktör olduğu göz önüne alındığında, kripto varlık işlemlerinin gizliliğini artıran yöntemlerin, terör örgütlerini kripto varlıkları kullanmaya teşvik edebileceği değerlendirilmektedir (Wang ve Zhu, 2021, s. 2333).

Her durumda güvenli giriş bilgileri gerektirmekle birlikte, kripto varlık hizmet sağlayıcılarda veya çevrimiçi ve çevrimdışı cüzdanlarda saklanabilen kripto varlıkların mülkiyeti, kâğıt cüzdan ve donanım cüzdan gibi fiziksel bir formun el değiştirmesi yoluyla başkasına geçebilmektedir (Whyte, 2019, ss. 13-14). Bu şekilde eski cüzdanların satın alınması yöntemi, ağda herhangi bir iz bırakmadan mülkiyet değişikliği gerçekleştirme olanağı sayesinde kripto varlık kullanıcılarının anonimliğini artırabilmektedir. Fiziksel bir formda saklanmayan kripto varlıklar ise, kripto varlık hizmet sağlayıcıların kullanıcılarına getirdiği -evrensel olarak tüm kripto varlık borsalarında uygulanmadığı ve uygulandığında da çalıntı kimlikler yoluyla borsaların yanıltılabildiği unutulmadan- kimlik doğrulama gereksinimlerinden kaçınılarak, aracı hizmetler kullanılmadan doğrudan eşler arasında transfer edilebilmektedir. Dolayısıyla terör örgütleri, sağladığı teknolojik güvenlik ve çeşitli anonimlik fırsatları sebebiyle kripto varlıkları gelir elde etme, değer aktarım ve saklama yöntemi olarak kullanabilmektedir (Whyte, 2019, s. 14).

Kripto varlıkların dayandığı anonimlik ilkesi, bir yandan kripto varlıkları suç ve terör örgütleri için cazip hale getirirken diğer yandan, kripto varlık borsalarının iflası veya hacklenme nedeniyle varlık sahipleri için mali kayıp riskini önemli ölçüde artırmaktadır (Kadyrov ve Prokhorov, 2018, s. 4). Bu durum, terör örgütlerinin de bu tür olaylara bağlı olarak fonlarını kaybetme endişesi yaşayabileceğini düşündürmektedir. Ancak genel anlamda kripto varlıkların, çoğu geleneksel finansal yöntemle kıyasla işlemlerin daha anonim şekilde gerçekleştirilmesine olanak tanıyarak anonimlik ihtiyacı içerisindeki terör örgütleri tarafından terörizmin finansmanında bir araç olarak kullanılabileceği değerlendirilmektedir.

2.3.1.1.2. Merkeziyetsiz yapı

Kripto varlıklar, merkezi bir yapının kontrolü ve güvenilirliği ile değil, blokzinciri gibi merkezi olmayan bir defter sistemi ve kriptoloji ile desteklenmektedir (Whyte, 2019, ss. 1-2). Birinci bölümde değinildiği üzere kripto varlıklarda güvenlik, geleneksel finansal yöntemlerin aksine üçüncü bir taraf aracılığıyla değil, dağıtık ve kriptografik yöntemlerle sağlanmakta ve işlemler merkezi bir otoriteye bağlı olmadan doğrulanarak kaydedilmektedir.

Geleneksel finansal sistemlerde aracı kurumlar işlemlerin doğruluğunu ve güvenliğini sağlarken aynı zamanda işlemleri ve verilerin güvenliğini kontrol etmektedir. Kripto

varlıklarda ise güvenlik merkezi bir otoritenin kontrolü olmadan, dağıtık yapı ve kriptografik algoritmalar ile sağlanmaktadır. Kripto varlıklarla işlem gerçekleştirilebilmesi için kripto varlığın sahibinin imzası (özel anahtarı kullanması) gerektiğinden, sahibinin izni olmaksızın işlem gerçekleştirilmesi ve işlem gerçekleştirildikten sonra algoritmik olarak dağıtık deftere kaydedildiğinden dolayı gerçekleştirilen işlemin geri alınması mümkün olmamaktadır (Whyte, 2019, s. 4). Bu durum kripto varlıkları, kullanıcılarının işlem güvenliği açısından daha dirençli ve güvenilir hale getirirken, merkezi otoritenin eksikliği ve işlemlerin doğrudan eşler arasında gerçekleşebilmesi, herhangi bir merkezi yapının engeline takılmayı ve işlemlerinin geri alınmasını istemeyen, güvenli ve güvenilir değer aktarım mekanizmaları arayışındaki terör örgütlerinin kripto varlıkları terörizmin finansmanı için kullanabilecekleri sonucunu doğurmaktadır (Whyte, 2019, s. 7).

Özellikle, merkezi olmayan kripto varlık borsalarında, güvenilir aracı kurum olmayışı ve işlemlerin akıllı sözleşmeler ile sistem kullanıcıları tarafından gerçekleştirilerek blokzincirine kaydedilmesi, suç gelirlerinin aklanması ile terörizmin finansmanının önlenmesi ilkelerinin işletilememesine neden olmaktadır (Gençcelep, 2022, s. 65). Bu tür doğrudan eşler arasında kripto varlıklarla işlem yapılabilmesini mümkün kılan platformlarda müşteri kimliğinin belirlenmesi için bir mekanizma bulunmaması, suçluların ve teröristlerin anonim olarak hareket etmelerine olanak tanımakta ve kripto varlıkların yasa dışı amaçlarla kullanılması için yeni fırsatlar sunmaktadır (Kadyrov ve Prokhorov, 2018, s. 4).

Merkezi olmayan yapısı sayesinde kripto varlıkların, terör örgütlerince ideolojik ve pratik nedenlerden dolayı kullanıma potansiyeli bulunmaktadır. Terör örgütleri, merkezi otoriteye karşı duydukları güvensizlik sebebiyle ideolojik sebeplerle veya resmi finansal sisteme erişimlerinin olmadığı durumlarda bir çözüm olarak pratik sebeplerle kripto varlıkları finansman faaliyetlerinde kullanabilmektedir (Keatinge vd., 2018, ss. 29-30).

2.3.1.1.3. Küresel erişim ile sınır ötesi ve hızlı transfer mekanizması

Kripto varlıklar geleneksel veya diğer alternatif finansal yöntemlere kıyasla daha hızlı, güvenli, geri alınamaz şekilde ve coğrafi sınırlamalardan bağımsız olarak küresel mesafelerde birkaç saniye içinde transfer edilebilme özelliği taşımaktadır (Whyte, 2019, s. 4). Kripto varlıklar, neredeyse anında ve büyük ölçüde geri dönülemez şekilde küresel olarak değer transferinden menkul kıymetlere, emtialara ve türev finansal ürünlere kadar çeşitli

finansal faaliyetleri kolaylaştırmak için kullanılabilmektedir (FATF, 2021a, s. 16). Kripto varlıkların bulunduğu ağa erişimi olan herkesçe, hızlı, küresel ölçekte ve kısıtlamasız bir şekilde işlem gerçekleştirme imkânı, terör örgütlerinin fonlarını hızlı, etkili ve çoğu zaman daha az maliyetli şekilde transfer etmelerine olanak tanımaktadır. Kripto varlıklar, küresel erişim ve işlem hızı bakımından terörizmin finansmanında kullanılma riskini artırabilmekte ve tespit ile mücadele için uygun risk azaltıcı önlemleri gerektirebilmektedir (FATF, 2021a, s. 16).

Kripto varlıklar, terör örgütlerine, düzenlenmeye tabi araçlar olmadan uluslararası düzeyde değer transferi yapma imkânı sunmaktadır. Günlük kullanım için hızlı ödemelerde büyük ölçüde başarılı olamayan kripto varlıklar, eşler arasında sınır ötesi değer transferinde etkili bir araçtır. Ayrıca, sadece bir kâğıt veya donanım cüzdanı taşıyarak veya telefon, tablet gibi taşınabilir cihazlarda bir yazılım cüzdanı kullanarak fonları sınırların ötesine taşımak mümkündür. Suç ve terör örgütleri arasındaki ilişki nedeniyle, kripto varlıkların suç amaçlı kullanımı arttıkça, terör örgütlerinin de bu araçları uluslararası transferlerde kullanma olasılığı artmaktadır (Keatinge vd., 2018, ss. 38-39).

2.3.1.1.4. Düzenleme eksiklikleri

Kripto varlıkların dayandığı anonimlik ilkesi, kripto varlıkların uluslararası kabul görmüş standartlara uymasını ve ulusal veya uluslararası otoritelerin düzenleyici çerçeve oluşturmasını zorlaştırmaktadır. Birçok hükûmet, yasa dışı faaliyetlerde kullanılma riskinden dolayı kripto varlıkların, geleneksel finansal sistemler gibi düzenlenmesi gerektiğine inanmaktadır. Almanya ve ABD gibi bazı ülkeler kripto varlıkları düzenlemekte iken Rusya ve Tayland gibi bazı ülkeler, etkili bir düzenleme sistemi oluşturmanın zorluğundan dolayı kripto varlıkların kullanımını tamamen veya kısmen yasaklamaktadır. Ancak hükûmetler ve bireyler açısından kripto varlıklar düzenleyici ve denetleyici yapılara ihtiyaç duymaktadır (Kadyrov ve Prokhorov, 2018, ss. 2-4).

Kripto varlıklara yönelik dünya çapında eşit olmayan düzenleme ve denetim mekanizmaları, kripto varlık hizmet sağlayıcılarının suç gelirlerinin aklanması ile terörizmin finansmanının önlenmesi programlarının yetersiz kaldığı ve uluslararası standartların etkin bir şekilde uygulanmadığı ülkeler, kripto varlıkların terörizmin finansmanında kullanılması bakımından potansiyel bir güvenlik açığı oluşturmaktadır (United States Department of the

Treasury, 2022, s. 23). Bu nedenle, uluslararası iş birliği kripto varlıkların yasa dışı amaçlarla kullanılmasının engellenmesi ve finansal sistemlerin güvende olmasını sağlamak için önem arz etmektedir.

Kripto varlık hizmet sağlayıcıların sıkı düzenlemelere tabi olduğu durumlarda, terör örgütleri kripto varlıkları itibari para birimlerine dönüştürmekte zorlanabilirken; yeterli düzenlemelerin olmadığı koşullarda, terör örgütlerinin faaliyetlerini finanse etmek için kripto varlıkları kullanma riski oluşmaktadır (Dion-Schwarz vd., 2019, s. 8). Suç gelirlerinin aklanmasının ve terörizmin finansmanının önlenmesine yönelik düzenlemelerin zayıf olduğu ülkelerde, kripto varlıkların yasa dışı kullanımlarına ilişkin denetimler yetersiz kalmaktadır. Sıkı denetimlerin olduğu ülkelerde ise küresel düzenleyici sistemdeki boşluklar sebebiyle kripto varlıkların terörizmin finansmanında kullanılmasında artış yaşanmaktadır. Genel olarak, kripto varlıkların terörizmin finansmanında kullanılması ve önlenmesine ilişkin hususlar tam anlamıyla dünya genelinde anlaşılamamış olup bu durum, düzenleme ve denetim boşluklarından yararlanmak isteyen terör örgütlerine kripto varlıkları finansal faaliyetlerinde kullanmaları için çeşitli fırsatlar sunmaktadır (Wang ve Zhu, 2021, ss. 2334-2335).

Kripto varlıkların kullanımına ilişkin farkındalık ile birlikte geliştirilen yaptırımlar ve tutarlı düzenlemeler, kripto varlıkların yasa dışı kullanımının önüne geçilmesi açısından önemlidir. Ulusal ve uluslararası düzeyde yeknesak düzenlemelerin olmaması, terörizmin finansmanı gibi birçok yasa dışı faaliyeti teşvik etmekte olup önemli bir risk faktörünü oluşturmaktadır (Kethineni ve Cao, 2020, ss. 338-339). Ülkeler kripto varlık alanında aktif şekilde iş birliği ile bilgi ve istihbarat paylaşımı yapmalı, küresel denetim mekanizmaları kurarak uygunluk standartları belirlemeli, bütüncül bir düzenleyici çerçeve oluşturmalıdır (Song vd., 2023, s. 17).

2.3.1.2. Zorlaştıran faktörler

Doğası gereği terör örgütleri gibi yasa dışı aktörler için çekici özelliklere sahip olan kripto varlıkları terör örgütlerinin kullanma yetenekleri pratikte bazı sınırlamalarla karşı karşıya kalmaktadır (Keatinge vd., 2018, s. 40). Kripto varlıkların terör örgütleri tarafından kullanılmasını zorlaştıran bazı faktörler bulunmaktadır. Bitcoin gibi daha yaygın kullanılan kripto varlıkların tamamen anonim olmadığı ve izlenebilir olduğu, öte yandan Zcash gibi

gizlilik odaklı kripto varlıkların daha yüksek düzeyde gizlilik sağlayabilmesine karşılık henüz Bitcoin kadar geniş çapta benimsenmediği dolayısıyla terör örgütlerinin finansman faaliyetlerinde kripto varlıkları yaygın biçimde kullanmadığı söylenebilir. Ancak gelecekte, mevcut kripto varlıklara göre terör örgütlerinin ihtiyaçlarını daha fazla karşılayan yeni kripto varlıkların ortaya çıkmasıyla terör örgütlerinin finansman faaliyetlerinde kripto varlıkları kullanmasının artabileceği değerlendirilmektedir (Dion-Schwarz vd., 2019, s. 14).

Song vd. göre (2023, ss. 13-14), kripto varlıkların terörizmin finansmanında kullanılmasının tercih edilmemesinde dört ana neden bulunmaktadır:

- 1) Terör örgütlerinin yaşamını sürdürdüğü bölgeler çoğunlukla kripto varlıkları yönetmek için gereken altyapı ve teknolojiye yoksundur.
- 2) Kripto varlıklarının geniş çapta benimsenmesinin önündeki en büyük engel olan likidite eksikliği, terör örgütlerinin kripto varlıkları nakde dönüştürmesini zorlaştırmaktadır.
- 3) Kripto varlıklar tamamen anonim değildir; Bitcoin gibi sözde anonim kripto varlıklar ile gerçekleştirilen işlemler blokzincirinde takip edilebilmektedir. Dolayısıyla terör örgütleri, sözde anonim kripto varlıklar ile düzenlenmiş bir kripto varlık hizmet sağlayıcı aracılığıyla işlem gerçekleştirdiğinde devlet kurumları tarafından kolaylıkla tespit edilebilmektedir.
- 4) Kripto varlıkların değer oynaklığı, terör örgütlerini spekülasyon riskleri almak zorunda bırakmaktadır.

Dion-Schwarz vd. göre (2019, ss. 51-53) kripto varlıkların terörizmin finansmanında kullanılmasını zorlaştıran faktörler şunlardır:

- 1) Kripto varlıklar içinde (çatallanmalar gibi) ve arasında devam eden çekişmeler belirsizliğe yol açarak kripto varlıkların geniş çapta benimsenmesini ve dolayısıyla terörist gruplar için kullanımını daha az uygulanabilir hale getirmekte ve güvensizliğe yol açarak terör örgütlerini finansman faaliyetlerinde kripto varlıkları kullanmaktan caydırmaktadır.
- 2) Kripto varlıklar konusunda güçlü uluslararası düzenlemeler ve yasal uygulamalar sağlandığı takdirde terörizmin finansmanı ile mücadelede etkin bir

kontrol sağlanarak kripto varlıkların terörizmin finansmanında kullanım olanakları kısıtlanabilecektir.

- 3) Kripto varlık sistemlerinde yaşanan güvenlik sorunları (kripto varlık borsalarındaki güvenlik ihlalleri ve kullanıcı hatalarından dolayı yaşanan güvenlik zafiyetleri) terör örgütlerinin kripto varlıklara olan güvenini azaltabilmektedir.

Toparlanacak olursa, terör örgütlerinin kripto varlıkları finansman faaliyetlerinde kullanmasını zorlaştıran faktörler; örgütsel öğrenim ve kontrol sorunları, teknik altyapı eksikliği, likide dönüştürülemez ve değer oynaklığı şeklinde dört başlık halinde sıralanabilir.

2.3.1.2.1. Örgütsel öğrenim ve kontrol sorunları

Terör örgütleri, genellikle yeni teknolojilere ve taktiklere kademeli şekilde adaptasyon sağlamaktadır. Diğer potansiyel adaptasyon alanlarına kıyasla finansman faaliyetleri daha fazla dış faktörlere bağlı olduğundan, terör örgütlerinin finansman faaliyetlerinde bütünüyle yeniliğe gitmesi zorlaşmaktadır. Diğer bir ifadeyle terörizmin finansmanı, terör örgütlerinin faaliyet gösterdiği finansal sistemlerle sınırlı olduğu için yüksek düzeyde yeniliğe direnç göstermektedir. Bu nedenle, terörizmin finansman yöntemlerindeki değişiklikler, ekonomik sistemlerdeki değişikliklere adaptasyon olarak değerlendirilmeli ve öğrenme süreci olarak görülmelidir (Argentino vd., 2023, ss. 37-38). Dolayısıyla, terör örgütlerinin kripto varlıkları bir finansman yöntemi olarak benimsemeleri, kripto varlıkları etkin bir şekilde yönetebilmeleri için bir adaptasyon ve öğrenme sürecinden geçmelerini gerektirmektedir. Bu durum, kripto varlıkların terörizmin finansmanında kullanılmasını zorlaştıran önemli faktörlerden birini oluşturmaktadır.

Terör örgütleri açısından, kripto varlıkların bir finansman yöntemi olarak kullanılmasının önündeki temel zorluklardan bir diğeri kontrol ve denetim sorunlarıdır. Kripto varlıkların kullanılması, finansal kaynakların daha etkin bir şekilde kontrol edilmesine olanak tanırken, diğer taraftan kripto varlıkların kontrolünü etkileyen örgüt içerisindeki kişiler bu varlıklar üzerindeki kontrol ve denetimi azaltabilmektedir. Kripto varlıkların, örgüt içerisindeki temsilcilere emanet edilmesi, terör örgütü liderlerinin fonlar üzerinde kontrol uygulama becerisini azaltmaktadır (Krishnan, 2020, s. 45). Operasyonel

güvenliği sürdürmek amacıyla kripto varlıkları hareket ettirme yeteneği verilen örgüt içerisindeki kişilerin, kripto varlıkları etkin bir şekilde kontrol edebilmeleri, kendi çıkarları doğrultusunda yeni riskler alma ve varlıkları sızdırma veya kaçırma ihtimallerini beraberinde getirirken, örgüt liderlerinin kripto varlıkların hareketlerini takip etmelerini zorlaştırarak varlıklar üzerindeki kontrolünü zayıflatabilmektedir (Whyte, 2019, ss. 2-15). Dolayısıyla kripto varlıkları kontrol eden örgüt içerisindeki kişilerin (vekil), kendi çıkarlarını ön planda tutarak örgüt ve örgüt liderinden (asil) farklı amaçlarla hareket etme olasılığı asil-vekil problemine yol açarak kripto varlıkların terör örgütlerinin finansman faaliyetleri çerçevesinde kullanılmasının tercih edilmemesine yol açabilmektedir. Asil-vekil probleminin yanı sıra basit şekilde, finansman kararlarını veren terör örgütü liderlerinin kripto varlıklara ilişkin geliştirmiş olduğu anlayışın da kripto varlıkların terörizmin finansmanında kullanılması tercihini etkileyebileceğini söylemek mümkündür.

2.3.1.2.2. *Teknik altyapı eksikliği*

Blokzinciri teknolojilerinin karmaşıklığı, birçok terör örgütünün kripto varlıkların potansiyelini tam olarak anlamasını zorlaştırmaktadır. Ayrıca, terör örgütlerinin bu teknolojiyi kullanmak için gerekli teknik becerilere sahip olma olasılıkları düşüktür (Kfir, 2020, ss. 118-119). Kripto varlıklara erişim ile söz konusu varlıkların anonim şekilde yönetilmesi için gereken teknik altyapının terör örgütleri ile terör örgütlerinin faaliyet gösterdiği bölgelerde kısıtlı olması, kripto varlıkların terörizmin finansmanında kullanılmasını zorlaştıran faktörler arasında yer almaktadır (Dion-Schwarz vd., 2019, ss. 24-30; Silfversten vd., 2020, s. 8).

Terör örgütlerinin kripto varlık kullanmasının önünde bazı teknolojik engeller bulunmaktadır. Terör örgütlerinin kripto varlıkları elde etmek ve anonim şekilde kullanmak için anlaşılması gereken teknik bir dil bulunmaktadır. Bunun yanı sıra bazı bölgelerde kripto varlık edinilmesi konusunda, birçok bankanın düzenlenmemiş kripto varlık borsalarına para gönderilmesini yasaklaması veya bazı ülkelerin kripto varlık ATM'lerini yasaklaması gibi birçok engelle karşılaşılmaktadır (Argentino vd., 2023, s. 33).

Terör örgütlerinin faaliyet gösterdiği bölgelerde kripto varlıkların kabul edilebilirliği düşük düzeydedir. Örneğin çok sayıda terör örgütünün faaliyet gösterdiği Orta Doğu'da çok az sayıda kripto varlık ATM'si yer almaktadır (Wang ve Zhu, 2021, s. 2334). Terör

örgütlerinin çoğu halihazırda, zayıf altyapı ve teknoloji düzeyine sahip kırsal bölgelerde faaliyet göstermekte ve kripto varlık ticareti veya madenciliği yapmak için gelişmiş bilgisayar teknolojisi kullanamamaktadır. Dolayısıyla kripto varlıklar terör örgütleri tarafından finansman faaliyetlerinde yaygın olarak kullanılmamaktadır, ancak terörist faaliyetler için önemli bir finansal seçeneği temsil etmektedir. Diğer bir ifadeyle Bitcoin gibi kripto varlıklar potansiyel bir terörizmin finansmanı aracı olsa da oynadığı rol henüz önemli sayılacak kadar yeterli değildir (Song vd., 2023, ss. 7-17). Bununla birlikte, kripto varlık piyasasındaki büyümenin, sistemin güvenilirliğinin artmasına ve kullanım kolaylığında iyileştirmelere yol açarak kripto varlıkların benimsenme ve kabul edilebilirliğinin artmasına yol açacağı söylenebilir. Kripto varlıkların dünya genelinde yaygınlaşmasıyla, terör örgütlerinin faaliyet gösterdiği bölgeler de dahil olmak üzere, bu sistemlerin mevcut kabul görmeme durumunun ortadan kalkabileceği değerlendirilmektedir (Dion-Schwarz vd., 2019, ss. 47-48).

2.3.1.2.3. *Likide dönüştürülemede*

Kripto varlıkların terörizmin finansmanında kullanılmasını zorlaştıran faktörlerden bir diğeri, kripto varlıkların diğer likit sermaye biçimlerine dönüştürülmesinin zorluğudur (Whyte, 2019, s. 5). Terör örgütlerinin faaliyet gösterdiği bölgelerde kripto varlıkların kabul edilebilirliği ve kullanılabilirliğinin sınırlı olması ve dolayısıyla kripto varlıklardaki likidite sorunları, terör örgütlerinin kripto varlıkları finansman faaliyetlerinde kullanmasını zorlaştırmaktadır (Dion-Schwarz vd., 2019, s. 13). Terör örgütleri kripto varlıkları her zaman takas edememekte ve itibari paraya dönüştürememektedir. Bir kripto varlığın likidite eksikliği, geniş çapta benimsenmesinin önündeki en büyük engeli oluşturmaktadır (Song vd., 2023, ss. 14-17).

Aynı tür kripto varlığın eşler arası ticaretini yapmak daha kolayken, kripto varlık türleri arasında geçiş yapmak veya kripto varlıkları itibari para birimlerine dönüştürmek daha zordur. Özellikle kripto varlığın ilk ediniminde, itibari para birimlerini kripto varlığa dönüştürmek için büyük ölçüde kripto varlık borsalarına ihtiyaç duyulmaktadır. Binance, Bitstamp, Bitfinex, Coinbase ve Kraken'in örnek olarak verilebileceği kripto varlık borsaları, kripto varlıkların ticaretini kolaylaştırarak ve saklama cüzdanları sağlayarak, ortalama bir kullanıcı için kripto varlıklara erişimde önemli bir rol oynamaktadır (Keatinge vd., 2018, s. 40). Kripto varlıkların terörizmin finansmanında kullanılmasındaki zorluk,

nakdin çok önemli olduğu çatışma bölgelerinde kripto varlıkları likide dönüştürme fırsatlarının sınırlı olmasından kaynaklanmaktadır (Keatinge vd., 2018, s. 38). Kripto varlıkları itibari para birimlerine çevirmek veya bunu saldırılar için silah veya cihaz bileşenleri satın almada kullanmak teknolojik açıdan zorlayıcı ve zaman alıcı olabilmekte ve kullanıcıyı potansiyel hırsızlığa açık hale getirebilmektedir (Argentino vd., 2023, ss. 33-34).

Diğer teknolojik yenilikler gibi kripto varlıklar, yasa dışı aktörlerin dikkatini çekerek kullanılmaya başlanmıştır. Bununla birlikte, genel olarak değerlendirildiğinde, yasa dışı faaliyetlerin çoğu hâlâ geleneksel bankacılık sistemi üzerinden gerçekleşmektedir. Kripto varlıkların toplam piyasa aktivitesi içindeki payı, geleneksel bankacılık sistemindeki yasa dışı kullanım oranından daha yüksek değildir. Yani, kripto varlıkların yasa dışı faaliyetler için tercih edilme oranı halihazırda geleneksel finansal sistemden daha düşüktür (Morell vd., 2021, ss. 3-4). Ayrıca pek çok terör örgütü, takip edilmesi elektronik transferden çok daha zor olan nakdi daha yararlı bulmakta ve yerel nakit bazlı finansman kaynaklarına güvenmektedir. Kripto varlıkların anlaşılabilirliği ve güvenilirliği arttıkça ve daha fazla satıcı tarafından bir ödeme aracı olarak kabul edildikçe, terör örgütlerinin kripto varlıkları kullanma olasılığı artacak ve mali faaliyetlerinin ve konumlarının izlenme riski azalacaktır (Carroll ve Windle, 2018, s. 289).

2.3.1.2.4. Değer oynaklığı

Çeşitli faktörlerden kaynaklanabilen kripto varlıkların değer oynaklığı, genel olarak kullanım düzeyini önemli ölçüde etkileyerek kripto varlıkların uzun vadeli gelişimine dezavantaj yaratmaktadır. Bu değer istikrarsızlığı, terör örgütlerinin kripto varlık kullanımını da etkilemektedir (Wang ve Zhu, 2021, s. 2335). Kripto varlıkların değerleri çoğunlukla oynaktır ve zaman zaman değerlerinde büyük dalgalanmalar yaşanabilmektedir. Bu nedenle terör örgütleri kripto varlıkları terörizmin finansmanında kullanırken, kripto varlıkların değerlerindeki ani düşüş veya yükselmelerden dolayı spekülatif risklere maruz kalmaktadır. Kripto varlıkların değerinin gelecekte belirsiz olması terör örgütleri açısından finansal planlamayı zorlaştırabilmektedir (Whyte, 2019, s. 14). Ayrıca birçok kripto varlığın değerinin son derece değişken olması, onları fon transferinde kullanışsız hale getirmektedir (Argentino vd., 2023, s. 34).

Terör örgütleri, sahip olduğu kaynakların sınırlı olması nedeniyle kaynaklarını riske atmak istememektedir. Kripto varlıklardaki değer oynaklığı, terör örgütlerinin kripto varlıklara çok fazla yatırım yapmalarını bu sebeple engelleyebilmektedir (Kfir, 2020, s. 119). Kripto varlıkların değerindeki artışlar, terör örgütlerine spekülasyonla gelir elde etme potansiyeli sunmakla birlikte kripto varlıkların değerinde yaşanan ani düşüşler, bu varlıkların istikrarlı bir gelir kaynağı olmadığını gösterdiği için kripto varlıkların terör örgütleri tarafından gelir elde etmede benzersiz bir araç olduğunu iddia etmek mantıklı değildir (Whyte, 2019, ss. 12-13). Kripto varlıkların değer oynaklığı, terör örgütleri için organizasyonel belirsizlikler yaratmaktadır (Krishnan, 2020, s. 45). Kripto alanının spekülasyon doğasından kaynaklanan değer dalgalanmaları ve düzenleme olasılığı gibi nedenlerle, kripto varlık kullanımı risk oluşturabilmektedir (Whyte, 2019, s. 2).

2.3.2. Kripto Varlıkların Terörizmin Finansmanında Potansiyel Kullanım Yöntemleri

Kripto varlık kullanımının yaygınlaşması, çeşitli suçlarda bir araç olarak kullanımının da artması sonucunu doğurmuştur. Silah ve uyuşturucu kaçakçılığı gibi yasa dışı malların ticareti, piramit satış sistemleri, dolandırıcılık, bilişim suçları, suçtan kaynaklanan malvarlığı değerlerini aklama vb. suçlarda kripto varlıklar bir ödeme aracı olarak suçlulara yeni fırsatlar yaratmıştır (Kethineni ve Cao, 2020, s. 329). Kripto varlıklar, terör örgütlerine de çeşitli yöntemlerle terörizmin finansmanında kullanılma konusunda fırsatlar sunmaktadır.

Terörizmin finansmanında kripto varlıkların hangi yöntemlerle kullanılacağı, terör örgütlerinin ihtiyaçlarına ve bu ihtiyaçları karşılamak için mevcut teknolojinin özellikleri ile terör örgütlerinin söz konusu teknolojiyi kullanma yeteneklerine bağlıdır (Dion-Schwarz vd., 2019, s. 14). Kripto varlıkların terörizmin finansmanında; bağışlar, madencilik, NFT ve ICO yoluyla fon temin etme sürecinde, terör örgütlerinin elde ettikleri suç gelirlerinin aklanmasında, DeFi ve akıllı sözleşmeler, karıştırıcı (mixer) hizmetleri, gizlilik tabanlı kripto varlıklar ile fonların yönetilmesi ve aktarılmasında, Dark Web içerisinde suç geliri ve malzeme temininde kullanılabileceği söylenebilir.

2.3.2.1. Bağışlar

Terörizmin finansmanı ile mücadele yöntemlerinin terör örgütlerinin para toplama yeteneklerini kısıtlamadaki başarısı, terör örgütlerini alternatif bağış toplama yöntemleri

aramaya yönelmiştir. Kripto varlıklar, terör örgütleri ve bağışçıları açısından sağladığı anonimlik, yönetim kolaylığı açısından kullanılabilirlik, güvenlik gibi özellikleri sayesinde terörizmin finansmanında bağış toplama yöntemi olarak kullanılabilmektedir (Dion-Schwarz vd., 2019, ss. 8-32). Terör örgütleri, üçüncü taraflara güvenmelerine gerek kalmadan, halka açık kripto varlık adreslerini yayınlayarak dünyanın herhangi bir yerindeki herhangi bir kişiden kripto varlık cinsinden kolaylıkla bağış alabilmektedir (Krishnan, 2020, s. 45).

Kripto varlıkların kullanımını kolaylaştıran son zamanlardaki gelişmelerle birlikte, ulus ötesi bağış toplama ihtiyacında olan terör örgütleri için kripto varlıklar çeşitli olanaklar sağlamıştır (Dion-Schwarz vd., 2019, s. 54). Uluslararası olarak bağış toplamak isteyen terör örgütleri, sosyal medya ve kripto varlıkları birleştiren yaklaşımı giderek daha fazla benimsemektedir. Terör örgütleri, sosyal ağlarda ve mesajlaşma kanallarında kripto varlık işlem süreçleri hakkında ayrıntılı talimatlar yayınlayarak dünya çapında birçok bağışçının ilgisini çekmektedir (Dyntu ve Dykyj, 2021, s. 72). Terör örgütleri, potansiyel bağışçıları sosyal medya platformları aracılığıyla şifreli mesajlaşma uygulamalarına yönlendirebilmektedir. Kripto varlıkların ve şifreli iletişim uygulamalarının terör örgütleri tarafından bağış kampanyalarında kullanılması potansiyel bir tehdit olarak karşımıza çıkmaktadır (Keatinge vd., 2018, s. 38).

Terör örgütünün elde ettiği bağışlar, bağışçıların algıladığı risk seviyesinden etkilenmektedir; risk düzeyinin arttığı durumlarda bağışçıların bağış yapma istekleri azalmaktadır. Yeterince güçlü, güvenli ve anonim bir kripto varlığın, terörizmin finansmanında bağışları önemli bir kaynak olarak yeniden etkinleştirebileceği değerlendirilmektedir. Terör örgütünün bağışçıları, sahip oldukları kripto varlıklarını bağışlayarak veya araçlar vasıtasıyla terör örgütüne fon transferi yapmak için kripto varlıkları kullanarak terör örgütüne destek olabilmektedir (Dion-Schwarz vd., 2019, s. 9).

Tezin ilerleyen bölümlerinde örneklerle de belirtileceği üzere, terörizmin finansmanında kripto varlıkların kullanılmasının en yaygın şekli, sosyal medya kanalları ve internet siteleri aracılığıyla paylaşılan kripto varlık cüzdan adreslerine terör örgütlerinin bağış toplamasıdır. Bu şekilde halka açık bağış toplama girişimleri ile terör örgütleri, yüksek tutarlarda kripto varlık cinsinden fon toplayabilmektedir. Ancak, kitle fonlaması kampanyaları aracılığıyla yapılan kripto varlık bağışları, genel olarak terörizmin

finansmanının ufak bir bölümünü oluşturmaktadır (Elliptic, 2023a). Bununla birlikte kripto varlıkların, değer oynaklığından kaynaklı yüksek kâr oranı ihtimali sayesinde, faaliyetlerini sürdürmek için yeni bir bağış toplama mekanizması arayan terör örgütleri tarafından daha geniş çapta kullanılabileceği değerlendirilmektedir (Hasbi ve Mahzam, 2018, s. 1).

2.3.2.2. Dark Web içerisinde suç geliri ve malzeme temini

İnternet katmanlardan oluşan bir yapıdır; “*Yüzey Web*” olarak ifade edilen üst katmana yaygın olarak kullanılan arama motorları vasıtasıyla kolayca ulaşılabilirken, “*Deep Web*” olarak ifade edilen derin katmanlara söz konusu arama motorları tarafından indekslenmediğinden kolayca ulaşılabilir. Dark Web ise Deep Web’in en derin katmanları olarak kasıtlı olarak gizlenmiş ve yalnızca özel tarayıcılar aracılığıyla erişilebilen kısmı olarak tanımlanmaktadır. Dark Web genellikle çocuk pornografisi, hassas bilgilerin izinsiz olarak sızdırılması, kara para aklama, telif hakkı ihlali, kredi kartı dolandırıcılığı, kimlik hırsızlığı, yasa dışı silah satışı gibi yasa dışı faaliyetlere ilişkin bilgiler ile mal ve hizmetler içeren bir alan olarak bilinmektedir (Weimann, 2015, ss. 2-3).

Yüzey Web ve Dark Web pazarları arasındaki en belirgin fark ödeme şeklidir; Dark Web pazarlarında ödemeler kripto varlıklar ile yapılmaktadır. Dark Web içerisinde en yaygın kullanılan kripto varlık Bitcoin olup Monero, Ethereum, Ripple ve Litecoin gibi Altcoin’ler de giderek popüler hale gelmektedir (Persi Paoli vd., 2017, s. 69). Yasa dışı malların kullanıcılarını ve tedarikçilerini eşleştiren söz konusu Dark Web pazaryerlerinde kripto varlıklar kullanılarak işlem gerçekleştirilmesi, kripto varlıkların yasa dışı aktivitelerle olan ilişkisini ön plana çıkarmaktadır. Kripto varlıklar, kullanıcıların kimliklerini gizlemelerine yardımcı olan bir web hizmeti olan Dark Web üzerinde, suç gelirlerinin aklanması ve terörizmin finansmanının yanı sıra söz konusu suçlar için bir araç olarak uyuşturucu ve silah kaçakçılığı, yasa dışı insan ticareti, şantaj, rüşvet, adam kaçırma gibi suçlarda da kullanılma riski taşımaktadır (Kadyrov ve Prokhorov, 2018, s. 8).

Dark Web’de silah ve ilgili ürünlerin satışını gerçekleştiren kripto pazarları ve satıcı dükkanları olmak üzere iki ana türde pazar bulunmaktadır. Kripto pazarları, müşterilere ödeme koruması sağlayan üçüncü taraf hizmetleri sunmakta ve çeşitli satıcıları bir araya getirerek satışlardan elde edilen komisyonlar karşılığında pazar yöneticileri tarafından işletilmektedir. Satıcı dükkanları ise üçüncü taraf hizmetleri kullanmadan doğrudan

müşterilere satış yapan bir satıcı tarafından kurulan ve yalnızca o satıcıya ait satışları barındıran pazarlardır (Persi Paoli vd., 2017, ss. 10-11). Ayrıca Dark Web’de, kullanıcılara anonimlik sağlayan *Tor Ağı* gibi şifreli web hizmetleri ve kripto varlık işlemlerini daha anonim hale getirmeyi amaçlayan *Dark Wallet* gibi yazılımlar kullanılmaktadır. Ödemelerin büyük ölçüde kripto varlıklara dayandığı Dark Web, terör örgütlerinin gelir elde etmesinde ve ihtiyaç duydukları malzemelerin temininde çeşitli fırsatlar sunmaktadır. Dark Web pazaryerleri, coğrafi engelleri ortadan kaldırarak, küresel ölçekte yasa dışı uyuşturucu ve silah ticaretine olanak tanımaktadır (Keatinge vd., 2018, s. 36). Bitcoin’in öncü başarısı ile birlikte kripto varlıklar, suçlular ile terör örgütlerine bu kapsamda anonimlik konusunda yeni fırsatlar yaratmıştır. 2011 yılında kurulan ve Dark Web’de faaliyet gösteren *Silk Road*’un, uyuşturucu ve silah gibi yasa dışı ürünlerin satıldığı çevrimiçi bir pazaryeri olarak, yalnızca Bitcoin gibi kripto varlıklar ile kullanıcılarına işlem yapma imkânı tanıyan ilk büyük ölçekli suç organizasyonu olduğu söylenebilmektedir. İki yıl içerisinde 1,2 milyar USD’nin üzerinde kazanç elde eden Silk Road 2013’te kapatılmış ve site kurucusu Ross Ulbricht ömür boyu hapis cezasına çarptırılmıştır (Weimann, 2015, s. 5). Yetkililer tarafından tıpkı Silk Road gibi kapatılan Dark Web’in en büyük pazarlarından olan *AlphaBay* ve *Hansa* da; çalıntı kimlik, insan, uyuşturucu, silah kaçakçılığı ve dolandırıcılık gibi suçlar için çeşitli ürün ve hizmetleri içeren işlemlere izin vermekte ve işlemler için Bitcoin, Monero ve Ethereum kripto varlıkları kabul etmektedir (Kethineni ve Cao, 2020, ss. 329-330). Bitcoin ve diğer birkaç kripto varlığın mal ve hizmet satın alımında ödemelerde kabulü dünyada yaygınlaşmaya başlamış olsa da gerçek alım olanakları hâlâ sınırlıdır. Bununla birlikte özellikle Zcash veya Dash gibi gizlilik odaklı kripto varlıklar; silah, uyuşturucu veya kötü amaçlı yazılım satışını sağlayan *TheRealDeal* gibi sitelerde Dark Web içerisinde işlem birimi olarak tercih edilmektedir (Whyte, 2019, s. 13).

Kripto varlıklar günlük kullanıma kıyasla Dark Web içerisinde daha yaygın şekilde kullanılmakta olup, Dark Web üzerinden terör saldırıları için gerekli malzemelerin temininde kullanılabilmektedir. Dark Web terör örgütlerince, sahte belge ve pasaport, silah ve patlayıcı gibi ihtiyaç duydukları malzemeler için bir pazar olarak işlev görmesinin yanı sıra söz konu malzemeler için fon toplamalarına olanak sağlamaktadır. Terör örgütleri Dark Web üzerinden, Bitcoin gibi kripto varlıklar cinsinden bağış toplayarak gelir elde edebilmektedir (Weimann, 2015, ss. 11-14). Terör örgütleri bu yolla topladıkları kripto varlıkları biriktirmek suretiyle elde ettikleri büyük miktarlardaki kripto varlıklar ile Dark Web içerisinde ihtiyaç duydukları materyallere ulaşabilmektedir (Teichmann, 2018, ss. 517-519). Sağladığı coğrafi

kapsam, hız ve anonimlik derecesi göz önüne alındığında kripto varlıklar, siber suçlar ve Dark Web kapsamında terör örgütlerinin dikkatini çekmektedir.

Yasa dışı kullanımlarına ilişkin olarak kripto varlıkların; Dark Web’de yasa dışı ürün ve hizmet satın alma, dolandırıcılık ve fidye yazılım saldırılarında daha fazla kullanıldığı, terörizmin finansmanı konusunda ise kullanım düzeyinin daha sınırlı kaldığı değerlendirilmektedir (Morell vd., 2021, s. 4). Ayrıca kimi yazarlara göre, terörizmin finansmanı bağlamında kripto varlıklar asla itibari para birimlerine dönüştürülmeyecek ve Dark Web üzerinde yasa dışı mal ve hizmet alım-satımında kullanılacaktır (Carroll ve Windle, 2018, ss. 288-289). Kripto varlıklar itibari para birimlerine dönüştürülmese dahi, terör örgütlerinin Dark Web üzerinde yasa dışı uyuşturucu ve silah kaçakçılığı gibi faaliyetlerde bulunarak kripto varlık cinsinden suç geliri elde etmeleri ve elde ettikleri kripto varlıklar ile ihtiyaç duydukları silah ve patlayıcı gibi malzemeleri yine Dark Web üzerinden temin etmeleri mümkün olduğundan, kripto varlıkları finansman faaliyetlerinde kullanmaya devam edeceği sonucuna varılabilmektedir.

2.3.2.3. Suç gelirlerinin aklanması

Mevzuatımızda, 5237 sayılı Türk Ceza Kanunu (2004, s. 95)’nin “*Suçtan kaynaklanan malvarlığı değerlerini aklama*” başlığı altındaki 282’nci maddesiyle düzenlenen aklama suçu; alt sınırı altı ay veya daha fazla hapis cezasını gerektiren bir suçtan kaynaklanan malvarlığı değerlerinin, yurt dışına çıkarılması veya bunların gayrimeşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla, çeşitli işlemlere tâbi tutulması olarak belirtilmiştir. 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun (2006, s. 2)’de “*suç geliri*” kavramı kullanılarak aklama suçu, 5237 sayılı Türk Ceza Kanununun 282’nci maddesinde düzenlenen suç olarak tanımlanmıştır. Aklama suçu, suç gelirinin elde edilmesini mümkün kılan öncül suç, söz konusu suç dolayısıyla elde edilen suç geliri ve kaynağını gizlemek maksadıyla suç gelirinin meşru bir görüntüye kavuşturulmasına yönelik çeşitli eylemleri içermektedir (MASAK, 2018a). Pek çok değişkene bağlı olarak her durumda farklılık gösterebileceği unutulmadan tipik bir aklama süreci; yerleştirme, ayırıştırma, bütünleştirme şeklinde üç aşamada gerçekleşmekte olup, şirinler, parçalama, vergi cennetleri, paravan veya hayali şirketler gibi çok çeşitli yöntemlerle gerçekleştirilmektedir (MASAK, 2018b; MASAK, 2018c). Son

yıllarda kripto varlıkların da bir aklama yöntemi olarak suçlular tarafından kullanılmaya başlandığı bilinmektedir.

Suç gelirlerinin aklanması ve terörizmin finansmanı arasındaki en belirgin fark, aklama sürecine dahil olan malvarlığı değerlerinin tamamen yasa dışı olması ancak terörizmin finansmanında yasal ve yasa dışı olmak üzere çeşitli kaynaklardan fon sağlanabilmesidir. Suç gelirlerinin aklanması süreci, yasa dışı yollarla elde edilen gelirin meşrulaştırılması ile sonuçlanırken, terörizmin finansmanı süreci, yasal veya yasa dışı yollarla elde edilen gelirin meşrulaştırılması her zaman gerekli olmaksızın terör amacıyla kullanılmak üzere dağıtılması veya saklanması ile sonuçlanmaktadır (Turan ve Gemici, 2020, s. 271). Terör örgütleri uyuşturucu kaçakçılığı gibi suç faaliyetlerinden elde ettikleri gelirleri terör operasyonlarını finanse etmek için kullanırken, suç gelirlerini terör faaliyetlerinde kullanmak üzere aklamakta veya aklamadan doğrudan terör amacıyla kullanmaktadır. Dolayısıyla fonların hareketini ve kullanımını kolaylaştırmak amacıyla suç gelirleri ile birlikte terör fonları da aklama sürecine tabi tutulabilmektedir (Tofangsaz, 2012, ss. 399-401).

Terörist kampanyaların uygulanabilirliği, dolandırıcılık, kaçakçılık, silah ve uyuşturucu ticareti, adam kaçırma gibi suç girişimlerine doğası gereği bağlı olup, yasa dışı girişimlerden elde edilen fonların aklanmasında suç örgütleri kadar terör örgütlerinin de önemli çıkarları bulunmaktadır. Fonların ihtiyaç duyulduğunda güvenli bir şekilde transfer edilmesini sağlamak önemli olduğu için terör örgütleri, sahip oldukları yasa dışı fonları genellikle aklayarak üyeleri arasında veya bağlantılı kuruluşlara transfer etmektedir (Whyte, 2019, ss. 6-7). Dolayısıyla suç gelirlerinin aklanması sürecinin terör örgütleri için faaliyetleri ve finansman kaynaklarının devamlılığı açısından önemli olduğu kabul edilmektedir.

Dünyanın her yerinde eşler arası bir ağ üzerinde alınıp satılabilen ve işlemlerini düzenleyen bir merkezi otoriteden yoksun olan kripto varlıklar ile uyuşturucu ticareti, insan kaçakçılığı, dolandırıcılık vb. yasa dışı faaliyetlerden elde edilen gelirin gerçek niteliği ve kaynağı kolaylıkla kamufle edilebilmektedir. Kripto varlıkların suç gelirlerinin aklanmasında kullanılmasının en önemli sebebi, finansal işleme dahil olan tarafların gerçek kimliğinin gizlenmesine yardımcı olan anonimlik düzeyidir (Majumder vd., 2019, s. 132). Dolayısıyla terör örgütleri, elde ettikleri suç gelirlerini kripto varlıklar ile aklamak suretiyle de terör eylemlerini finanse etmede kripto varlıkları kullanabilmektedir.

2.3.2.4. Nitelikli Fikrî Tapu (*Non-Fungible Token*-NFT)

Dijital sanatçılar için yeni bir alan olarak popülerlik kazanan NFT'ler, her yeni teknolojide olduğu gibi yasa dışı amaçlarla kullanılabilir. NFT'ler, terör örgütleri tarafından fonların kaynağının gizlenmesi ve suç gelirlerinin aklanması konusunda kullanılma potansiyeli barındırmaktadır. Reddedilemeyecek şekilde çok yüksek tutarlarda fiyatlandırılabilmesi ve fiyatları kontrol edecek bir otoritenin bulunmaması NFT'leri kötü niyetli aktörler için cazip kılmaktadır (Sanction Scanner, 2023, s. 35).

Yasa dışı fonların kaynağını gizlemek amacıyla değersiz veya değeri oldukça az olan sanat eserleri gibi ürünlerin fahiş fiyatlarla satın alınmasını içeren ve suçlular tarafından uzun süredir yaygın şekilde kullanılan suç gelirlerinin aklanması tekniği, dijital varlıkların benzersizliğini ve sahipliğini belgeleyen NFT'ler yoluyla da uygulanmaktadır. Kullandıkları cüzdanların takip ve tespit edilmesinden kaçınmak için yasa dışı aktörler, yeni bir cüzdan oluşturarak kendi NFT'lerini fahiş fiyatlarla satın almak veya bir NFT satıcısı ile anlaşarak satıcının NFT'sini daha yüksek fiyattan satın aldıktan sonra ödedikleri tutarın büyük bir kısmını satıcıdan geri almak şeklinde iki ana yöntem kullanmaktadır (Küçük vd., 2023, s. 288). Dijital bir sanat formu olmasından dolayı diğer sanat eserlerine kıyasla lojistik sürecinin kolaylığı, yüksek tutarlarda fiyatlandırılabilmesi, işlem anonimliği ve NFT pazaryerleri ve platformları konusunda suç gelirlerinin aklanması ve terörizmin finansmanının önlenmesine yönelik düzenlemelerin yetersiz kalması, NFT'lerin yasa dışı amaçlarla kullanılmasını kolaylaştırmaktadır (Sanction Scanner, 2023, s. 35).

NFT'lerin, kripto varlık borsalarında yaygın bir endişe olan ve bir varlığın değerini yapay olarak artırmak için kullanılan yıkama ticaretinde ve suç gelirleri ile satın alınması suretiyle bir aklama yöntemi olarak kullanılabilmesi, yasa dışı durumlarla sık sık ilişkilendirilmesine neden olmaktadır. NFT yıkama ticaretinde amaç, kişinin NFT'sini, orijinal sahibinin de kontrol ettiği yeni bir cüzdana satarak gerçekte olduğundan daha değerli görünmesini sağlamak olup birçok NFT ticaret platformunun, kullanıcılarının kimliklerini doğrulamaksızın cüzdanlarını platforma bağlayarak ticaret yapmalarına olanak tanınması, NFT'lerin yıkama ticaretinde kullanılmasını kolaylaştırmaktadır (Grauer vd., 2022, s. 31). Bu durumda terör örgütlerinin NFT'leri, yıkama ticareti yoluyla gelir elde etmede veya sahip oldukları suç gelirlerini aklamada kullanabilecekleri gibi, ticaretin daha hızlı ve daha az

kısıtlanmış olması nedeniyle bir fon transfer mekanizması gibi de kullanabilecekleri söylenebilir.

2.3.2.5. Merkezi olmayan finans (*Decentralized Finance-DeFi*)

DeFi, aracılar ihtiyacı duymadan doğrudan eşler arası işlemlere imkân tanıyan, blokzinciri teknolojisi üzerine kurulu finansal protokolleri, uygulama ve hizmetleri, kısacası yeni bir finansal sistemi ifade etmektedir. 2021’de toplam 40 milyar dolarlık değere ulaşan DeFi, ekonomideki aracıları devre dışı bırakması dolayısıyla işlem maliyetlerini azaltarak daha fazla insanın finansal hizmetlere erişmesine olanak tanımaktadır. DeFi’nin büyümesi, ölçeklenebilirlik ve düzenleme gibi zorluklarla karşı karşıya kalırken, suç gelirlerinin aklanması ve terörizmin finansmanının önlenmesine yönelik düzenlemelerin akıllı sözleşmeler kapsamında genişletilerek akıllı sözleşmelerin denetlenmesini gerektirmektedir (Sanction Scanner, 2023, ss. 34-38).

Tezin önceki bölümlerinde değinildiği üzere DAO’lar, liderlik yapısı olmayan ve hiyerarşi içermeyen bir merkezi olmayan örgütlenme biçimini temsil etmektedir. Terör örgütlerinin, internet üzerinde bireylerin radikalleşmesini etkileme çabalarının yanı sıra, DAO’ları kullanarak liderlik yapısı olmayan bir örgütlenme modelini benimseyerek yeni organizasyon biçimleri, sosyal direniş ve terörizm için bir platform oluşturma potansiyeli bulunmaktadır (Krishnan, 2020, s. 46). DAO’lar, üyelerin oy kullanması yoluyla alınan kararları otomatikleştirmek ve belirli koşullar altında fonları yönetmek için akıllı sözleşmeleri kullanmaktadır.

Yaygın şekilde Ethereum platformu üzerinde oluşturulan akıllı sözleşmeler, belirli koşulların karşılanması durumunda otomatik olarak gerçekleşen işlemlere olanak tanıyarak, terör örgütlerinin de dahil olduğu dünya çapındaki güvensiz taraflar arasında güvenli ve aracısız şekilde eşler arası değer transferini mümkün kılmaktadır. Terör örgütlerinin, programlanabilir doğasının bir parçası olarak akıllı sözleşmeleri, cüzdanda tutulan kripto varlıkların yapılan anlaşma ve şartların yerine getirilmesi durumunda kararlaştırılan tarafa otomatik olarak transfer edilmesi şeklinde ve bütçe tahsisi ile harcamalar için bütçe yönetimini otomatize ederek kullanma potansiyeli bulunmaktadır (Whyte, 2019, s. 14). DAO’lar ve akıllı sözleşmeler, kripto varlıkların yönetimi ve finansal işlemlerin otomatize edilmesinde önemli bir rol oynamaktadır. Bu teknolojilerin kullanımı terör örgütlerine

finansman faaliyetlerini yürütmeye kolaylık sağlayabilmektedir. Terör örgütlerinin, DAO'lar aracılığıyla üyelerden gelen fonları toplayarak bu fonları belirli koşullar altında akıllı sözleşmeler aracılığıyla kullanabilecekleri söylenebilir.

2.3.2.6. Madencilik (Mining)

Madencilik, kripto varlık işlemlerini doğrulamanın bir parçası olarak karmaşık matematiksel problemleri çözme işlemi olup söz konusu süreçte yeni işlem kayıtlarını içeren bloklar blokzincirine eklenmekte ve madenciler sunucularının bu kapsamda çalışması sonucunda üretilen yeni kripto varlıklarla ödüllendirilmektedir. Terör örgütlerinin, itibari para birimlerini kripto varlıklara dönüştürürken karşılaşılan riskleri azaltabilecek şekilde doğrudan madencilik yaparak veya madencilik faaliyetlerine yatırım yaparak kripto varlık elde etme potansiyeli bulunmaktadır. Tüm kripto varlıkların madencilik ile üretilmediği unutulmadan, madencilik faaliyetlerine katılmanın terör örgütleri için özellikle anonimlik konusunda önemli ölçüde fayda sağlayabileceği söylenebilir (Whyte, 2019, ss. 13-14).

Kripto varlık madenciliği, terör örgütleri tarafından yaptırımlardan kaçınma ve terörizmin finansmanı gibi çeşitli amaçlarla kullanılmaktadır. El Kaide gibi bazı terör örgütlerinin kripto varlık madenciliği faaliyetlerinde bulunduğu ve DEAŞ'ın kripto varlık madenciliği konusunda rehberler ve tercih edilen madencilik havuzlarına yönlendiren bağlantılar yayınlarak bilgi paylaşımında bulunduğu bilinmektedir (Elliptic, 2023a).

Altcoin madenciliği, terör örgütleri için özellikle düşük maliyetli ve daha erişilebilir yatırım gereksinimleri sunarak potansiyel olarak oldukça kârlı bir seçenek olsa da, Bitcoin madenciliği için gerekli olan tesis, bilgisayar ve güvenlik yatırımı, geçmiş yıllara kıyasla önemli ölçüde arttığı için terör örgütleri açısından mantıklı bir değer teklifi olmaktan çıkmıştır (Whyte, 2019, s. 13). Bu nedenle terör örgütlerinin, değişen dinamiklere uyum sağlamak amacıyla finansman faaliyetlerinde kullanılan yöntemleri adapte etmek için Altcoin madenciliği gibi daha düşük maliyetli ve erişilebilir seçeneklere yönelebileceği söylenebilir.

2.3.2.7. Kripto varlıkların ilk arzı (*Initial Coin Offering-ICO*)

Önceki bölümlerde belirtildiği üzere kripto varlıkların ihracı madencilik dışında da gerçekleşebilmektedir. İhraççının yatırımcıları kendi projesinin etkinliği konusunda ikna etmesinin ve yatırımcıya kripto varlık geri alımı için bir garanti sunmasının yeterli olduğu ICO süreci, kitle fonlamasının bir örneği olarak suç gelirlerinin aklanması ve terörizmin finansmanı gibi yasa dışı faaliyetlerde kullanılma potansiyeli taşımaktadır (Kadyrov ve Prokhorov, 2018, s. 7). ICO'lar söz konusu suçlar için anonimliği artırıcı bir unsur olarak kullanılabilmektedir.

Genellikle yeni girişimlerin fon toplama yöntemleri olarak bilinen ICO'lar, düzenleyici alandaki belirsizlikler nedeniyle dolandırıcılık olaylarına da zemin hazırlamaktadır. ICO'lar, terör örgütlerinin sahte ICO projeleri ile yatırımcıları kandırarak veya dolandırarak kripto varlıkları ellerine geçirmeye çalıştıkları bir yöntem şeklinde terörizmin finansmanında kullanılma riski taşımaktadır. Terör örgütlerinin, sahte ICO projeleri düzenleyerek dolandırıcılık faaliyetinde bulunmak suretiyle fon toplayabileceği gibi, bağış toplama mekanizmaları için açık bir şekilde geliştirdikleri ICO projelerini duyurarak destekçilerinden fon toplayabileceği de söylenebilmektedir. Ancak terör örgütlerinin sürdürülebilir bir kripto varlık veya ilgili ICO projesini geliştirme olasılığı, finansal sistemle etkileşimdeki zorluklar ile hükûmetler tarafından hızlı ve etkili bir tepkiyle karşılanması muhtemel olduğundan oldukça düşük görünmektedir (Keatinge vd., 2018, s. 45).

ICO'lar, terör örgütlerinin sahip olduğu suç gelirlerinin aklanmasında da kullanılabilmektedir. Terör örgütleri sahip oldukları suç gelirlerini kripto varlıklara yatırarak bir ICO projesine dahil olduktan sonra söz konusu kripto varlıkları Token'lara dönüştürebilmekte ve sonrasında Token'ları serbestçe transfer ederek dünya çapındaki kripto varlık borsalarında diğer kripto varlıklarla veya itibari para birimleri ile takas edebilmektedir. Kayıt tutma eksikliği, yüksek miktardaki işlemler ve işlemlerin gerçekleşme hızı, ICO'ları suç gelirlerinin aklanması için cazip bir araç haline getirmektedir (Robinson, 2018).

2.3.2.8. Karıştırıcı (Mixer) hizmetleri

Kripto varlıkların terörizmin finansmanında kullanılma yöntemlerinden biri de, kripto varlık transferini özel işlemlere tabi tutarak gönderici ve alıcının kimliğini gizleyen, bu sayede kripto varlıkları şeffaflığından ayırarak çeşitli kullanımlara açık hale getiren işlemler olarak tanımlanabilen karıştırıcı (mixer) hizmetleridir (Sanction Scanner, 2023, s. 33). Mikser gibi yüksek derecede anonimlik sağlamaya olanak tanıyan çeşitli hizmet ve araçların geliştirilmesi ve kullanımının yaygınlaşması, kripto varlıkların yasa dışı faaliyetlerde kullanımının artmasına zemin hazırlamaktadır (Kadyrov ve Prokhorov, 2018, s. 8). Kripto varlıklarla işlem gerçekleştiren katılımcıların gerçek kimlikleri ile işlem zincirinin gizlenmesi, suç gelirini kaynağından uzaklaştırma açısından aklama konusunda ve terör örgütlerinin anonim şekilde finansman faaliyetlerini yürütebilmeleri açısından terörizmin finansmanı konusunda çeşitli olanaklar sunmaktadır.

Terör örgütleri, kripto varlıkların anonimliğini artırmak için merkezi karıştırma hizmetleri veya kişiden kişiye karıştırıcılar gibi çeşitli yöntemlere başvurmaktadır. Merkezi karıştırma hizmetleri komisyon karşılığında, kullanıcıların gönderdiği kripto varlıkları karıştırarak belirtilen adreslere transfer etmektedir. Kişiden kişiye karıştırıcılar ise üçüncü bir taraf olmadan kripto varlıkları doğrudan değiştirmeye istekli gruplara dayanmaktadır (Dyntu ve Dykyj, 2021, s. 69). Bir gönderici, mixer hizmeti kullanarak bir alıcıya aktarım yapmak istediğinde, göndericinin yaptığı aktarım ilk olarak mixer hizmet sağlayıcı aracıya ulaşmakta ve mixer hizmet sağlayıcı işlemi karıştırdıktan sonra aktarım, karışık işlemleri geçerek göndericiye ulaşmaktadır. Bu sayede, mixer hizmeti kullanılmadan alıcısından göndericisine ağ üzerinde kolaylıkla izlenebilecek olan aktarımın göndericisi ile alıcısı arasındaki bağı belirsizleştirilerek, yasa dışı kullanım açısından risk oluşturacak şekilde kripto varlık işlemlerinin şeffaflığı ortadan kaldırılmaya çalışılmaktadır (Sanction Scanner, 2023, s. 33). Kripto varlıkların karıştırılmasında anonimleşme seviyesi, karıştırmaya katılan kullanıcıların sayısına ve kripto varlıkların miktarına bağlı olarak değişmektedir. Blokzinciri analizini daha karmaşık hale getirmek için karıştırma işlemleri birden fazla kez gerçekleştirilebilmektedir. Karıştırma araçlarının geliştirilmesi sürekli bir süreçtir ve her gün yeni karıştırma hizmetleri ortaya çıkmaktadır (Dyntu ve Dykyj, 2021, s. 69).

Bitcoin gibi kripto varlıkları birçok kullanıcıdan toplayıp dağıtan, işlemlerin izini karıştırarak akışı takip etmeyi zorlaştıran mixer veya *Tumbler* gibi karıştırıcı hizmetlerin

yanı sıra, kullanıcının kripto varlık cüzdanına karıştırma özelliklerini entegre eden Dark Wallet gibi hizmetler de gizliliği artırarak izleri belirsizleştirmektedir. Karıştırma faaliyetlerinin tamamı yasa dışı olarak değerlendirilemese de, yapılan çalışmalar karıştırıcıların büyük ölçüde yasa dışı amaçlarla kullanıldığını ve söz konusu faaliyetlerin çok az sayıda karıştırıcı aracılığıyla gerçekleştiğini göstermektedir (Keatinge vd., 2018, s. 32).

2.3.2.9. Gizlilik tabanlı kripto varlıklar (Privacy Coins)

Kripto varlıkların yasa dışı kullanımlarının yanında, dayandığı teknoloji olan blokzinciri, şeffaf doğası nedeniyle yasa dışı faaliyetlerin tespitinde geleneksel finansal sistemlere kıyasla önemli bir araç olarak görülmektedir. Diğer veri analizi yöntemleriyle birleştirildiğinde blokzinciri analizi, terörizmin finansmanı gibi yasa dışı faaliyetlerin ve ilişkili kullanıcıların kimliklerinin belirlenmesine olanak sağlayabilmektedir. Dolayısıyla, terör örgütlerinin Bitcoin gibi sözde anonim kripto varlıklardan ziyade faaliyetlerini gizlemelerini kolaylaştıran gizlilik tabanlı kripto varlıkları kullanmaya yönelecekleri değerlendirilmektedir (Morell vd., 2021, ss. 5-8). Bitcoin'in ortaya çıkışından bu yana, kripto varlık ekosistemi önemli ölçüde gelişmiş ve Monero gibi Bitcoin'den daha az izlenebilir ve korunan bir yapıya sahip olan kripto varlıklar ile Zcash gibi çevrimdışı işlemleri destekleyen ve daha fazla gizlilik özellikleri sunan kripto varlıklar piyasaya sürülmüştür. Gizlilik tabanlı Coin'ler olarak da adlandırılan bu tür kripto varlıklar, devlet otoritelerinin yasa dışı işlemleri izlemesini zorlaştırarak gizlilik avantajları sağlamaktadır (İbrahim, 2019, ss. 2-3).

İşlem detaylarını gizlemek için özel şifreleme teknikleri kullanan Monero, Dash, Zcash gibi gizlilik odaklı kripto varlıklar ile işlemlerin şeffaf şekilde ağdaki herkesçe izlenebildiği dolayısıyla çeşitli yöntemlerle kullanıcı kimlikleri ile ilişkilendirilebilmesi nedeniyle sözde anonim olarak nitelendirilen Bitcoin, Ethereum, Ripple, Litecoin, Tether (USDT) gibi kripto varlıkların farkına dikkat çekmek gerekmektedir. Herkese açık ağ kaynakları aracılığıyla herhangi bir cüzdan adresini sorgulamanın ve ilgili cüzdanın bakiyesi ile gelen ve giden transferleri görüntülemenin mümkün olduğu kripto varlıklar ile gerçekleştirilen işlemlerin ağ üzerinde geriye dönük olarak izlenebilirliği şüpheli fonların takibini görece kolaylaştırmaktadır (Turan ve Demircan, 2021, ss. 166-167). Sözde anonim olarak nitelendirilen söz konusu kripto varlıklar bu nedenle önemli düzeyde şeffaflık vaat

etse de ağıdaki hareketlerinin izlenmesini zorlaştıracak şekilde tasarlanmış ve ağ üzerinde takip olasılığını ortadan kaldırabilen gizlilik odaklı kripto varlıklar bu durumun istisnasını oluşturmaktadır. Savunucuları tarafından gizlilik tabanlı kripto varlıkların mevcudiyetinin, Bitcoin gibi sözde anonim kripto varlıkların izlenebilirliğinin bir kusur olduğuna dikkat çekilerek mahremiyet ihtiyacından kaynaklandığı iddia edilse de, bu durumun terörizmin finansmanı gibi yasa dışı amaçlar için avantaj sağladığı ve ilgi gördüğü bir gerçektir (Keatinge vd., 2018, s. 33; Sanction Scanner, 2023, s. 33).

Bazı terör örgütlerinin fon akışlarını gizlemek için karmaşık kripto varlık anonimleştirme teknikleri kullanmaya başladıkları bilinmektedir. Piyasadaki hakimiyetinden ve dolayısıyla erişilebilirliğinden kaynaklı olarak Bitcoin, yasa dışı transferlerde en fazla kullanılan kripto varlık olmasına karşılık diğer kripto varlıklar, toplam işlemlerinin içerisindeki pay olarak yasa dışı amaçlar için çok daha sık kullanılmaktadır. Monero gibi gizlilik tabanlı kripto varlıkların yasa dışı amaçlarla kullanım oranları günden güne artış göstermektedir (Morell vd., 2021, ss. 4-5). Terörizmin finansmanında kullanılan kripto varlıkların, özellikle gizlilik tabanlı kripto varlıklar ile çeşitlendirilme çabaları devam etmekle birlikte, çoğu terör örgütünün Tether'i daha fazla tercih ettiği gözlemlenmiştir (Elliptic, 2023a). Bunun sebebinin, Tether'in bir istikrarlı kripto para olması dolayısıyla değerinde büyük dalgalanmalar olmaması ve kripto varlık borsalarında geniş bir şekilde kullanılması dolayısıyla likide dönüştürülme kolaylığı olduğu söylenebilir. Küresel ölçekte kitlesel olarak benimsenme potansiyeli istikrarlı kripto paraları, terör örgütleri tarafından finansman faaliyetlerinde kullanılmasında tercih edilebilir kılmaktadır (FATF, 2020b, s. 2).

Kripto varlık hizmet sağlayıcıları, daha izlenebilir olan sözde anonim kripto varlıkları, izlenmesi daha zor olan Monero gibi gizlilik tabanlı kripto varlıklarla takas yapma olanağı sunabilmektedir (Kfir, 2020, s. 122). Ancak düzenlenmeye tabi kripto varlık borsalarının, kullanıcılarına sınırlı sayıda gizlilik tabanlı kripto varlık sunması, bu tür kripto varlıklara erişimi zorlaştırmakta ve likidite sorunlarına yol açmaktadır. Söz konusu kripto varlık borsalarının kullanıcılarına gizlilik tabanlı kripto varlıkları sunduğu ve likidite sağladığı takdirde ise müşteri tanıma önlemleri nedeniyle bu tür kripto varlıkların anonimlik özellikleri zayıflayabilmektedir. Bununla birlikte yüksek düzeyde anonimlik sunan kripto varlıkların sayısı ve kullanılabilirliği artmakta ve yasa dışı faaliyetlerin tespiti konusunda önemli zorluklar oluşturmaktadır (Keatinge vd., 2018, s. 35).

Gizlilik tabanlı kripto varlıkların yanı sıra terör örgütleri, farklı blokzincirleri arasında geçiş yaparak fon akışını gizleme amacını taşıyan bir yöntem olan “*zincir atlama*” yoluyla da terör faaliyetlerini destekleyen fonları anonimleştirme veya nakde çevirme çabası içerisinde. Zincir atlama, kullanıcılarını yeterli kimlik doğrulama süreçlerinden geçirmeyen ve daha anonim bir şekilde kripto varlık takası yapılmasını sağlayan hizmet ve platformların yaygınlaşmasıyla önemli bir hız kazanmıştır (Elliptic, 2023b, ss. 57-143). Ancak bu durum, finansal düzenleyiciler ve güvenlik birimleri için daha fazla zorluk yaratmaktadır.

2.3.3. Kripto Varlıkların Terörizmin Finansmanında Kullanım Örnekleri

Yukarıda bahsedilen yöntemler ve diğer pek çok yöntemle birlikte, karmaşık terörle mücadele çabaları karşısında terör örgütlerinin son yıllarda operasyonlarını finanse etmek için kripto varlıkları kullanmayı denedikleri görülmektedir (Wiwoho vd., 2023, s. 104). Terör örgütlerinin gelir elde etmek, fon aktarmak, mal satın almak konusunda kripto varlık kullandıklarına ilişkin kanıtlar bulunsa da vakalar ile vakalara konu tutarların nispeten az ve çoğu örneğin çevrimiçi forumlarda daha fazla teknik beceriye sahip yeni nesil aşırılık yanlıları tarafından kripto varlık kullanımına ilişkin eğitim verme kapsamında olduğu değerlendirilmektedir. Dolayısıyla herhangi bir fiziksel terör hücresiyle bağlantısı olmayan ve terörizme yardım amacıyla suç faaliyeti yoluyla para toplayan yalnız aktör siber finansörleri olarak adlandırılabilirler. Kişilerin ortaya çıkışı ve siber aşinalığı daha fazla olan yeni nesil teröristler sayesinde kripto varlıkların terörizmin finansmanında kullanılmasının artacağı düşünülmektedir (Carroll ve Windle, 2018, ss. 289-290). Ayrıca, kripto varlıkların günlük ve pratik kullanım imkânlarının genellikle sınırlı olması, terör örgütleri için kripto varlıkların sağladığı potansiyel faydaları kısıtlamaktadır. Bununla birlikte, aşağıda yer alan örneklerden de anlaşılacağı üzere, kripto varlıkların terörizmin finansmanı bağlamında çevrimiçi faaliyet gösteren bazı yalnız aktörler ve küçük hücreler tarafından nispeten daha fazla kullanıldığını söylemek mümkündür (Keatinge vd., 2018, s. 28).

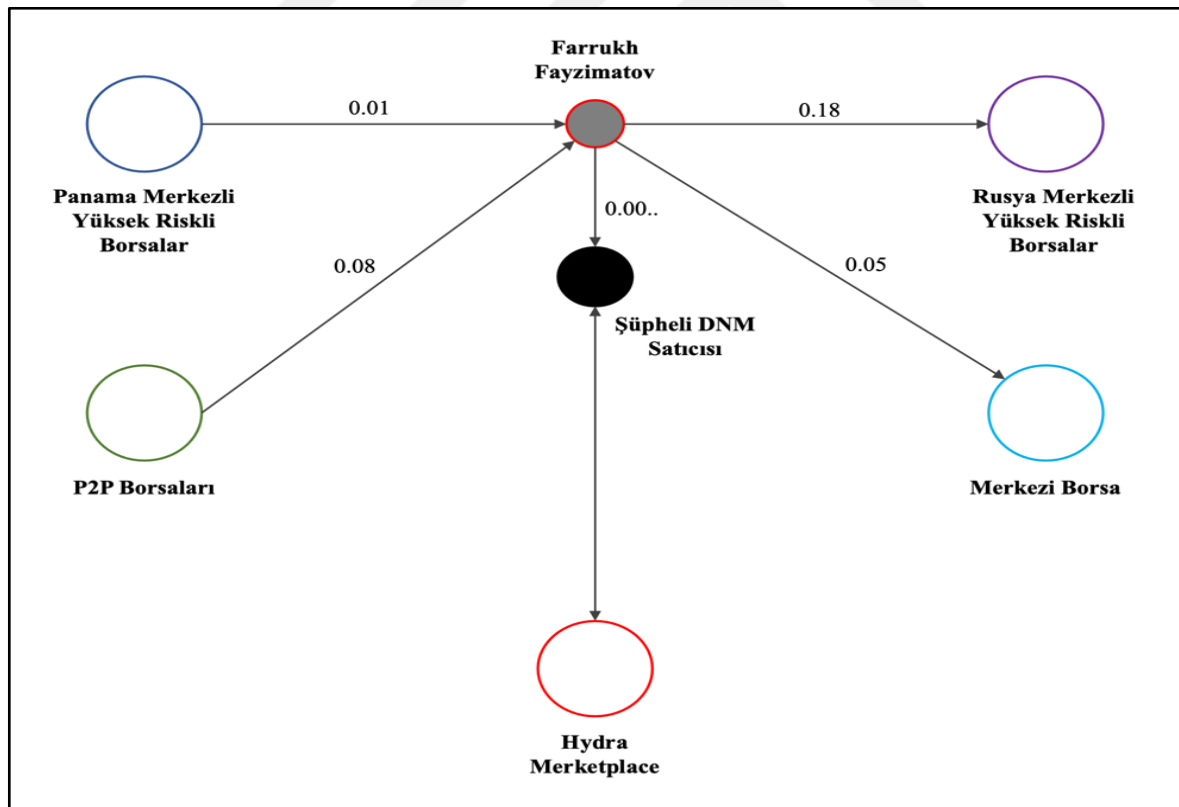
Terör örgütlerinin kripto varlıkları henüz erken bir dönemde fark ederek finansman faaliyetlerinde kullanma girişimleri olduğu görülmektedir. 2012 yılında Endonezya’nın Solo kentindeki kiliseye yönelik bombalama eylemini gerçekleştiren terör örgütünün, finansmanını Dark Web üzerinden ulusal ve uluslararası bağışçılardan toplanan Bitcoin cinsinden kripto varlıklar aracılığıyla sağladığı polis raporlarında kanıtlanmıştır. Örgütün bir

üyesinin ayrıca, Dark Web üzerinden edindiği çalıntı bir kimlik ile *www.speedlineinc.com* adresli Forex internet sitesini hacklediği ve parayı katlayarak 7 milyar Rupı (yaklaşık 600.000 USD) gelir elde ettiği ifade edilmektedir. Elde edilen gelir, terör örgütünün idamesini sağlamak ve bombalı eylemi finanse etmek için kullanılmıştır (Nastiti ve Wimmer, 2015, s. 5; Weimann, 2016, s. 43). Terörizmin finansmanı kapsamında kripto varlıkların, yalnızca terör eylemlerinin finansmanında değil, aynı zamanda örgüte veya üyelerine fayda sağlayacak her türlü finansal yardım kapsamında kullanılması mümkün olmaktadır. 2016-2020 yılları arasında, İngiltere'nin Leichester kentinde yaşayan Hisham Chaudhary isimli şahsın Suriye'de faaliyet gösteren DEAŞ terör örgütü üyelerine Bitcoin göndererek finansman sağladığı, gönderilen kripto varlıkların ise esir tutulan DEAŞ terör örgütü üyelerinin kaçması için kullanıldığı değerlendirilmektedir (Grauer ve Updegrave, 2021, s. 94).

Terör örgütleri ve destekçileri tarafından kripto varlıkların çeşitli özelliklerinden dolayı pratik nedenlerle bir bağış toplama mekanizması olarak kullanıldığı görülmektedir. Suriye iç savaşında faaliyet gösteren çeşitli terör örgütleri ile sıkı müttefik olan ve HTŞ (Heyet Tahrir el-Şam) gibi terör örgütlerine askeri eğitim ile danışmanlık sağlayan *Malhama Tactical* isimli özel bir şirket, sosyal medya üzerinden (Facebook, Twitter ve Youtube) videolar yayınlamaya bir taraftan popüleritesini arttırmaya diğer taraftan da bağış toplamaya çalışmıştır. Yayınladığı videoların sonuna “*Bizi Destekleyin*” ibaresi ile bir Bitcoin adresi paylaşan şirketin bu sayede kripto varlık cinsinden bağış topladığı bilinmektedir. Şirketin bu videolardan ne kadar bağış topladığı tam olarak belirlenemese de 2019 yılında dahi videolar yayınlamaya ve küçük de olsa kripto varlık bağışı almaya devam ettiği gözlemlenmiştir (Bernardi, 2019, ss. 12-13). 31 Ocak 2023 tarihinde Manhattan Bölge Savcılığı tarafından Victoria Jacobs (diğer adıyla Bakhrom Talipov) isimli şahsın, Malhama Tactical şirketine 5.000 USD tutarından fazla kripto varlık gönderdiği iddia edilmiştir. Şahıs hakkında ayrıca, söz konusu şirketin dünya genelindeki destekçilerinden kripto varlık ile birlikte *Western Union* ve *MoneyGram* üzerinden transferler aldığı, topladığı fonları şirket tarafından kontrol edilen Bitcoin cüzdanlarına yönlendirmek suretiyle şirket adına 10.661 USD değerindeki parayı akladığı iddia edilmiştir (Stalinsky vd., 2023).

Kripto varlıkların terörizmin finansmanında bir bağış toplama aracı olarak kullanıldığına ilişkin 2021 yılında farklı bir olay tespit edilmiştir. ABD Hazine Bakanlığı Yabancı Varlıkları Kontrol Ofisi (*Office of Foreign Assets Control-OFAC*) tarafından HTŞ

terör örgütüne maddi yardım ve destek sağladığı belirlenerek yaptırım uygulanan Farrukh Furkatovitch Fayzimatov isimli şahsın, sosyal medyayı örgüt propagandası amaçları için ve örgüte teçhizat temin etmek amacıyla kripto varlık cinsinden bağış toplamak için kullandığı belirlenmiştir. Söz konusu şahsın, müşterinin tanınması gereksinimlerine yönelik bilgilerin tutulmadığı Panama merkezli bir kripto varlık borsasındaki ve eşler arası işlemlerin gerçekleştirilmesini sağlayan platformlardaki anonim kullanıcılardan Bitcoin transferi aldığı görülmüştür. Akabinde şahsın müşterinin tanınmasına yönelik gerekli bilgilerin tutulduğu Rusya merkezli yüksek riskli kripto varlık borsalarındaki kullanıcılar ile Rusya'nın *Hydra Marketplace* adlı Dark Web pazaryerindeki şüpheli bir satıcıya söz konusu Bitcoin'leri gönderdiği anlaşılmıştır (Grauer vd., 2022, s. 97). Kripto varlık işlemlerinin takibi ve gerçek dünyadaki faaliyetlerle ilişkilendirilmesi konusunda “*Reactor*” adını verdiği bir blokzinciri analiz yazılımı bulunan (Chainalysis, 2023) araştırma şirketi Chainalysis'in 2022 yılı *Kripto Suç Raporu*'nda, söz konusu analiz programı vasıtasıyla bahsedilen olay aşağıda yer alan Şekil 2.1.'deki gibi görselleştirilmiştir (Grauer vd., 2022, s. 97).



Şekil 2.1. Örnek olay görsel analizi (Grauer vd., 2022, s. 97)

Merkeziyetsiz yapıdaki kripto varlıklar terörizmin finansmanında ideolojik nedenlerle de kullanılmaya başlanmış ve terör örgütü destekçileri tarafından bağış çağrılarına konu

olmuştur. Bu kapsamda 2015 yılının başında Abu-Mustafa olarak tanımlanan bir DEAŞ destekçisinin Bitcoin üzerinden bağış toplama çabasında olduğu tespit edilmiştir (Whyte, 2019, ss. 10-11). Şahıs, ifadelerinde batılı ülkeleri “*kâfir*” olarak nitelendirerek bu ülkelerin para birimlerini kullanmanın dahi bahse konu ülkelerin ekonomilerini güçlendirdiğini ve dolaylı yoldan bu ülkelere yardımcı olduğunu belirtmiştir. Sistemin kontrolünü elinde bulunduran bu kâfir ülkelere habersiz, şüpheli olsun veya olmasın herhangi bir mücahide banka havalesi gönderilemeyeceğini ifade ederek çözüm olarak, merkezi sisteme sahip olmayan, hızlı ve güvenilir Bitcoin sistemine işaret etmiştir (Al-Munthir, t.y., ss. 1-2). Şahsın kripto varlıkların merkeziyetsiz işleyiş sistematüğinden bir çözüm olarak bahsetmesi, kripto varlıkların ideolojik nedenlerle de terör örgütleri tarafından benimsenebileceğine işaret etmektedir. Şahıs aynı zamanda, Bitcoin ile alışveriş yapılan “*Silk Road*” isimli Dark Web pazaryeri vasıtasıyla kullanıcıların tespit edilmeden silah satın alabileceğini ve terör örgütü üyelerine bağış yapabileceğini belirtmiştir. İşlemleri çözülemez bir şekilde karıştıran Dark Wallet sayesinde dünyanın neresinden olursa olsun, kullanıcıların istediği miktarda kripto varlığı anonim bir şekilde bağışlayabileceğini ifade etmiştir. Son olarak ekonomik sistemin kontrolünü elinde bulunduran kâfir ülkeler nedeniyle kaybolmaya yüz tutmuş bağış yapma sünnetinin Bitcoin sayesinde yeniden canlandırılacağına olan inancını vurgulamıştır (Al-Munthir, t.y., ss. 2-3). Terör örgütü destekçilerinin yanı sıra terör örgütlerinin de kripto varlıklar hakkında örgüt içinde veya destekçileri arasında farkındalığı artırma ve finansman faaliyetlerinde kripto varlık kullanımını teşvik etme çabasında olduğu görülmektedir. 2018 yılının ocak ayında El-Kaide terör örgütünün internet sitesinde yayımlanan El-Haqiqa isimli dergide, kripto varlıkların terörizmin finansmanında nasıl kullanılması gerektiğini, kripto varlıkların avantaj ve dezavantajlarını, kripto varlıklar hakkında ayrıntılı bilgilerin bulunduğu bağlantıyı içeren bir makaleye yer verilmiştir (Al-Haqiqa, 2018; akt. Kfir, 2020, s. 119).

Bağış toplama faaliyetlerinin yanı sıra terör örgütleri, Dark Web üzerinde kripto varlıkları suç geliri elde etme faaliyetlerinde kullanabildikleri gibi, terör eylemlerinde ihtiyaç duydukları malzemelerin temininde de kullanabilmektedir. 13 Kasım 2015 tarihinde DEAŞ terör örgütü tarafından gerçekleştirilen Paris saldırılarında, terör örgütünün kullanmış olduğu dört adet uzun namlulu silahın (ikisi Çin yapımı AK 47, ikisi Yugoslavya yapımı Zastava M70) saldırıdan bir hafta önce Dark Web üzerinde yasa dışı silah kaçakçılığı yapan Almanya’daki Sascha W. isimli bir şahıstan kripto varlıklar ile temin edildiği belirlenmiştir. Sascha W. isimli şahsın silahları kendisine ait “*DW Guns*” adlı Dark Web ağı üzerinden

sattığının tespit edilmesi üzerine 27 Kasım 2015 günü şahsın evinde yapılan aramalarda 16 adet silah ele geçirilmiş ve şahıs tutuklanmıştır (Solms-Laubach, 2015). Kripto varlıkların uzun süredir yaygın şekilde benimsendiği Dark Web içerisinde bağışlar veya suç faaliyetleri yoluyla finansman sağlayabilen teröristler, elde ettikleri kripto varlıkları itibari para birimlerine dönüştürmelerine gerek kalmaksızın yine Dark Web üzerinde doğrudan malzeme temininde kullanabilmektedir. 8 Mart 2019 tarihinde Jahanzaib Sami ve Hina Bashir Beigh isimli çiftin Suriye merkezli DEAŞ terör örgütü üyesinden temin ettikleri Bitcoin adresine bağış toplamak, toplanan bağışlarla da silah ve patlayıcı madde tedarik etmeye çalışmaktan suçlanarak Hindistan'ın Delhi şehrinde tutuklanması bu duruma örnek teşkil etmektedir (Grauer ve Updegrave, 2021, s. 95). Yine DEAŞ terör örgütünün finansmanı kapsamında Dark Web üzerinde kripto varlıkların kullanımına ilişkin başka bir örnek olay 2022 yılının Kasım ayında kaydedilmiştir. Cardiff'li Khuram Ikbal isimli şahıs çalıntı cüzdan ile Dark Web üzerindeki “*Bypass Shop*” isimli pazaryerinden Bitcoin işlemleri yaptığı tespit edilerek tutuklanmış ve 16 ay hapis cezasına çarptırılmıştır. Şahsın daha önce de Kenya ve Türkiye üzerinden iki kez DEAŞ'a katılmak için girişimde bulunduğu ancak sınır dışı edildiği, 2014 yılında ise “*terörün babası*” anlamına gelen “*Abu Irhaab*” takma isim ile sosyal medya üzerinden terör örgütü propagandası yapma suçundan hapis cezası aldığı tespit edilmiştir (Grauer vd., 2022, s. 98).

Kripto varlıklar itibari para birimlerine dönüştürülerek de terörizmin finansmanında kullanılmaktadır. DEAŞ'ın Suriye kolu ile bağlantısı bulunan ve Endonezya'daki terör eylemlerinin planlayıcısı Bahrin Naim, edindiği yüksek tutarlardaki kripto varlığı Arif Hidayatullah isimli şahsın eşlerine ve diğer militan arkadaşları Nurohman isimli şahsa transfer etmiştir. Transfer edilen kripto varlıklar itibari para birimine dönüştürülerek 2016 yılının ocak ayında MH Tharim Caddesi'nde gerçekleştirilen intihar saldırısında ve aynı yılın temmuz ayında düzenlenen Solo Polis Karakolu saldırısının finansmanında kullanılmıştır (Wiwoho vd., 2023, s. 109). Kripto varlıkların itibari para birimine dönüştürülerek terör eyleminin finansmanında kullanıldığı söz konusu olaydan, kripto varlıkların likide dönüştürülebilirliğinin terörizmin finansmanında kullanılmasını kolaylaştıran bir faktör olduğu yönünde çıkarım yapılabilir. Paskalya Bayramı olan 21 Nisan 2019 günü Sri Lanka'da DEAŞ tarafından gerçekleştirilen ve 253 kişinin ölümü ile 485 kişinin yaralanmasıyla sonuçlanan bir dizi terör eyleminin finansmanında da benzer bir durum görülmektedir. Söz konusu terör eylemlerinin Bitcoin aracılığıyla finanse edildiğini tespit eden İsrail merkezli “*Whitestream*” isimli blokzinciri analiz şirketi, kripto varlıkların Kanada

merkezli bir kripto varlık borsası olan “*CoinPayments*” aracılığıyla transfer edildiğini ve likide dönüştürüldüğünü belirtmiştir. Şirket tarafından gerçekleştirilen analize göre, DEAŞ’ın bağış toplamak amacıyla kullandığı kripto varlık cüzdanındaki Bitcoin miktarının, saldırıdan bir gün önce 500.000 USD seviyesinden 4.5 milyon USD’ye yükseldiği; ancak saldırıdan sonraki gün, söz konusu miktarın tekrar 500.000 USD seviyesine düştüğü belirlenmiş (Katsiri, 2019) ve dolayısıyla cüzdanda toplanan Bitcoin’in söz konusu terör eylemini gerçekleştirmek amacıyla kullanıldığı değerlendirilmiştir.

Kripto varlıkların sınır ötesinde işlemlere olanak tanıyan doğasının, terörizmin finansmanında kullanılmasını kolaylaştıran faktörler arasında yer aldığı incelenen örnek olaylar neticesinde de anlaşılmaktadır. Hakkında Türkiye’de bulunan malvarlığının dondurulması kararı alınan bir kişiye banka kanalıyla para transfer etmek isteyen şahsa dair Türkiye’nin mali istihbarat birimi Mali Suçları Araştırma Kurulu (MASAK) Başkanlığı tarafından başlatılan ve kolluk birimleri tarafından yürütülen çalışmalar neticesinde; çatışma bölgeleriyle bağlantılı olan ve bu bölgede bulunan kamplarda tutulan yabancı şahıslara yurt dışından para gönderilmesi işlemlerine aracılık eden söz konusu şahsın, bu işlemlerde kripto varlıkları kullandığı tespit edilmiş olup savcılık makamınca terörizmin finansmanı suçu kapsamında iddianame düzenlenmiş ve sonrasında şahıs hakkında kovuşturma süreci başlamıştır. MASAK tarafından şahsın kripto varlık hizmet sağlayıcısı nezdindeki hesap hareketleri incelendiğinde, şahsın cüzdanına kimliği belirsiz kişiler tarafından düzenli olarak gönderilen kripto varlıkların genellikle aynı gün içinde itibari para birimine dönüştürülerek banka hesabına aktarıldığı veya tersi yönde işlemler gerçekleştirildiği tespit edilmiştir (MASAK, 2022, s. 28).

2019-2020 yılları arasında Fransız yetkililerin yürüttüğü soruşturmada ise pek çok şahsın, 11 USD ile 165 USD arasında değişen tutardaki kripto varlığı yurt dışı hesaplara aktararak Suriye’de faaliyet gösteren El-Kaide ve DEAŞ terör örgütü üyelerine finansman sağladıklarının tespit edilmesi neticesinde 29 kişi tutuklanmıştır (Grauer ve Updegrave, 2021, s. 94). Benzer şekilde, 2017 yılının başında, bir Amerikan vatandaşı olan ve ABD’de laboratuvar teknisyeni olarak çalışan Zoobia Shahnaz isimli şahsın, çok sayıda kredi kartından temin ettiği paranın bir kısmını Bitcoin ve diğer çeşitli kripto varlıklara çevirdiği, kendisinin ve alıcıların kimliğini gizleyerek 62.000 USD’lik kısmı kripto varlık cinsinden olmak üzere toplam 150.000 USD’den fazla tutarı Pakistan, Çin ve Türkiye’deki DEAŞ terör örgütüyle iltisaklı şahıs ve kuruluşlara gönderdiği tespit edilmiştir (Majumder vd., 2019, s.

134). Pakistan ve Türkiye üzerinden Suriye topraklarına gitmek üzere ABD’den çıkmaya çalıştığı sırada yakalanan şahıs, çeşitli suçlardan 90 yıl üzeri mahkûmiyet istemiyle yargılanmıştır (Ma, 2017; Bernardi, 2019, s. 14). Kripto varlıkların terörizmin finansmanı kapsamında sınır ötesi transfer işlemlerinde kullanıldığına ilişkin diğer bir olay 2023 yılının mayıs ayında tespit edilmiştir. Muhammed Azharuddin Chhippa isimli şahıs DEAŞ terör örgütünün kontrolündeki kripto varlık cüzdanlarına 61.000 USD değerinde kripto varlık gönderdiği suçlamasıyla Virginia’daki ikametinde tutuklanmıştır. Şahsın Kansalı olan Allison Fluke-Ekren isimli dini nikahlı eşinin ise geçmişte Suriye’de bulunarak uzun namlulu silah ve el bombası kullanma, intihar saldırısı düzenleme eğitimleri aldığı, aralarında 10 yaşındaki kız çocuklarının da bulunduğu tamamı kadınlardan oluşan 100 kişilik bir DEAŞ taburuna liderlik ettiği belirlenmiş ve 20 yıl hapis cezasına çarptırılmıştır (Stalinsky vd., 2023).

Terör örgütlerinin ve destekçilerinin, kâr amacı gütmeyen kuruluş görünümünde finansman faaliyetleri kapsamında kripto varlık toplama çabasında olduğu da görülmektedir. 2019-2020 yılları arasında, özellikle Suriye ve Özbekistan gibi Orta Asya ülkelerinde faaliyet yürüten terör örgütlerinin, kendilerini kâr amacı gütmeyen kuruluş olarak göstererek *Telegram* gibi sosyal medya platformları aracılığıyla dünya çapında kripto varlık bağışı topladığı ve toplanan bağışları Suriye merkezli “*BitcoinTransfer*” isimli kripto varlık borsasını kullanarak akladığı ve dağıttığı tespit edilmiştir (Grauer ve Updegrave, 2021, s. 94). Bu kapsamda diğer bir örnek olay, 2023 yılının temmuz ayında Kanada Kraliyet Atlı Polisi tarafından yürütülen soruşturma neticesinde kaydedilmiştir. Halilullah Yousuf isimli şahsın, DEAŞ terör örgütüne üye kazandırmak ve finansman sağlamak amacıyla sosyal medya platformları üzerinden propaganda yaptığı tespit edilmiş ve ayrıca Afganistan’da bulunan bir DEAŞ üyesi ile bağlantıya geçerek yabancı büyükelçiliklere ve yabancı uyruklu şahıslara yönelik araştırmaların ve düzenlenecek terör saldırılarının keşif ve propagandasının yapılması girişiminde bulunduğu öğrenilmiştir. Yousuf’un bu amaçla kâr amacı gütmeyen kuruluş görünümünde çok sayıda kampanya oluşturarak kripto varlık toplamaya çalıştığı belirlenmiştir (FATF, 2023a, s. 25). Bahse konu tarzda fon toplayan ve Suriye’deki terör örgütlerini destekleyen sözde hayır kurumu ve bağış toplama örgütü olan Al Sadaqah, 2017 yılından itibaren *Telegram* ve *Twitter* platformları üzerinden Bitcoin ile bağış yapılabilecek kripto varlık adresleri ile bağış yapmak için kullanılabilecek Bitcoin ATM’lerinin konumlarını paylaşmaya başlamıştır. 2018 yılının eylül ayı itibarıyla yalnızca 575 USD değerinde Bitcoin toplayabilen Al Sadaqah’ın, bu tarihten itibaren bağış toplama

kampanyası ABD kolluk kuvvetleri tarafından 2020 yılında sona erdirilene kadar Monero, Dash ve Verge gibi gizlilik tabanlı kripto varlıklara yöneldiği bilinmektedir (Elliptic, 2023b, s. 114). Gizlilik tabanlı kripto varlıkların, tespit edilme ve müdahale riskini azaltmak isteyen terör örgütleri tarafından kullanılmaya başlandığı görülmektedir. 22 Mart 2023 tarihinde, DEAŞ terör örgütü tarafından yönetilen “*Rocket.Chat*” sunucusu üzerinden bir kullanıcı “*Mübarek Ramazan ayının gelişi dolayısıyla Müslümanları tebrik ediyor, Yüce Allah'tan bu ayı Müslümanlar için fetih ve güçlenme, kâfirler için ise felaket ayı olmasını diliyoruz.*” mesajıyla DEAŞ yanlısı bir sitenin linkini paylaşmıştır. Söz konusu link ile ulaşılan DEAŞ yanlısı sitede, bir taraftan kripto varlık kullanımı konusunda tavsiyelere yer verilirken, diğer taraftan Monero cinsinden bağış toplamak amacıyla QR (*Quick Response*, Hızlı Cevap/Karekod) kodu ve cüzdan adresi bilgileri siteye yerleştirilmiştir (Stalinsky vd., 2023).

Terör örgütlerinin, kripto varlıkların finansman faaliyetleri kapsamında sağladığı avantajlardan yararlanmak amacıyla sürekli olarak yeni ve karmaşık finansman tipolojileri geliştirebildiği de anlaşılmaktadır. Fransa’da faaliyet yürüten bir elektronik para kuruluşunun şüpheli işlem bildirimine istinaden Fransa Maliye Bakanlığı’na istihbarat hizmeti veren *TracFin (Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins)*, Yasadışı Mali Hareketlere Karşı Eylem ve Bilgi İşlem Kuruluşu) tarafından başlatılan çalışmalar neticesinde, ön ödemeli kartlar aracılığıyla satın alınan kripto varlıkların terörizmin finansmanında kullanıldığı yeni bir tipoloji ortaya çıkmıştır. Soruşturma neticesinde; anonim olarak edinilebilen ön ödemeli kartlarla satın alınan kripto varlıkların, kitle fonlaması ile Kuzey Doğu Suriye’deki kamplarda esir tutulan DEAŞ’lı kadın terör örgütü üyelerinin kaçışını finanse etmek için kullanıldığı ve on aylık sürede 63 adet bağışçıdan 250.000 Euro değerinde bağış toplandığı tespit edilerek 2022 yılının haziran ayında 8 sanık terörizme finansman sağlamak ve terör örgütüne üye olmak suçlarından 3 ila 9 yıl arası cezaya mahkûm edilmiştir. Ayrıca ön ödemeli kartların anonim olarak satın alınabilmesi ve bu kartlar ile yapılan işlemlerin tespit edilmesinin çok zor olması dolayısıyla, kripto varlıkların satın alınmasında ön ödemeli kartların kullanılmasını yasaklayan ve kripto varlık hizmet sağlayıcılarının müşterinin tanınması önlemlerini uygulamalarını zorunlu kılan yasa çıkarılmıştır (FATF, 2023a, s. 30).

Kripto varlıkların takibi, güvenliği ve uyumluluk konularında hizmet veren bir şirket olan Elliptic’in 2023 *Tipolojiler Raporu*’nda; 2020 ve 2022 yılları arasında terör örgütlerinin önceki dönemlere kıyasla daha büyük miktarlarda çeşitli kripto varlıklar cinsinden fon

topladıkları, kripto varlıkların ediniminde yeni yöntemler belirledikleri, kripto varlık kullanımlarını gizlemek için gizlilik tabanlı kripto varlıklar ve şifreli iletişim yöntemleri gibi ek önlemler aldıkları ifade edilerek terörizmin finansmanında kripto varlık kullanımının daha karmaşık hale geldiği çıkarımı yapılmıştır (Elliptic, 2023b, s. 113). Yukarıda bahsedilen örnek olaylar da bu durumu destekler niteliktedir.

Son yıllarda aşırı sağ terör olaylarının artışıyla birlikte ana akım finans sisteminden dışlanmaya başlayan aşırılık yanlısı grupların da finansman faaliyetlerinde kripto varlıkları kullanmaya yöneldikleri görülmektedir. Elliptic 2021 yılının aralık ayında yayınlamış olduğu çalışmasında, aşırı sağcı neo-Nazi haber siteleri, beyazların üstünlüğünü savunan bloglar ve aşırı sağcı video paylaşım platformlarında tümüyle kripto varlıkların benimsendiğini ve aşırı sağ ile bağlantılı cüzdanlara 8,9 milyon USD’den fazla tutarda kripto varlık ödemesi yapıldığını ortaya koymuştur. Aşırılık yanlısı bir gruba ait Bitcoin cüzdanı örnek olarak incelendiğinde, gelen bağışların %47’sindeki Bitcoin miktarının “1488” küsuratlarını içerdiği tespit edilmiş ve bu durumun beyazların üstünlüğünü savunan ideolojik gruplar arasında bir anlam ifade ettiğine dikkat çekilmiştir (Elliptic, 2021). “14” sayısı beyazların üstünlüğünü savunan “14 Kelime⁴” sloganının sayısal ifadesi, alfabenin sekizinci harfi olan “H”nin iki kez kullanımı olan “88” sayısı ise Adolf Hitler’in selamı olan “Heil Hitler” anlamına gelmektedir (Elliptic, 2023a, s. 117). Diğer taraftan, John Bambanek isimli siber güvenlik uzmanı, geliştirmiş olduğu “Neo-Nazi BTC Tracker” isimli Twitter botu aracılığıyla aşırı sağcı bir neo-Nazi aktivistine ait “Daily Stormer” isimli web sitesine yapılan kripto varlık bağışlarının miktarını belirlemeye çalışmıştır (Matsakis, 2017). 11 Ağustos 2018 günü ABD’nin başkenti Washington’da ikincisi düzenlenen “Sağı Birleştirin” mitingi kapsamında bahse konu sitenin 60.000 USD tutarında kripto varlık cinsinden bağış topladığı belirtilmektedir. Bambanek’in Twitter botuna göre, söz konusu sitenin teknik kısmını yürüten “Weev” kullanıcı adlı aşırı sağcı aktivist (asıl ismi Andrew Alan Escher Auernheimer olan Amerikan asıllı hacker), 2014 yılında başladığı bağış kampanyasından 2018 yılı ağustos ayı itibarıyla sadece bilinen cüzdan adreslerine toplamda 1.8 milyon USD değerinde kripto varlık bağışı toplamıştır (Bambrough, 2018).

⁴ The Order isimli beyaz ayrılıkçı terör örgütünün kurucularından David Eden Lane tarafından ortaya çıkarılmış 14 kelimelik “We must secure the existence of our people and a future for white children (Halkımızın varlığını ve beyaz çocukların geleceğini güvence altına almalıyız)” sloganı, dünya çapındaki aşırı sağ yanlısı aktivistler için ilham kaynağı haline gelmiştir (Michael, 2009, s. 43).

Chainalysis (Grauer ve Updegrave, 2021, ss. 103-105) tarafından yayınlanan *Kripto Suç Raporu*'nda ise ABD'deki aşırı sağ yanlısı şahıs ve grupların 2016 yılından itibaren istikrarlı bir şekilde kripto varlıklar cinsinden bağış topladığı ifade edilmiştir. Kripto varlıkların ABD'deki aşırı sağ kullanımlarına örnek olarak, 6 Ocak 2021 günü eski ABD başkanı Donald Trump'ın mitingi sonrası 2020 seçim kaybını protesto etmek üzere Capitol (ABD Kongre Binası)'e düzenlenen baskında yer alan aşırı sağcı grupların ve şahısların olaydan bir ay önce Bitcoin üzerinden yüklü miktarda bağış aldığı tespitine yer verilmiştir. 8 Aralık 2020'de 28.15 BTC (yaklaşık değeri 522.000 USD) miktarındaki kripto paranın aralarında Nick Fuentes, Ethan Ralph gibi aşırı sağcı aktivist şahısların ve göçmenlik karşıtı *VDARE* gibi grupların bulunduğu 22 ayrı adrese gönderildiği belirlenmiştir. Raporda ismi açıklanmayan bağışçının, aşırı sağ yanlısı bir Fransız bilgisayar programcısı olduğu ve bağış yaptıktan kısa bir süre sonra yapmış olduğu bağışın gerisindeki motivasyonları belirten bir not bırakarak intihar ettiği ifade edilmektedir (Grauer ve Updegrave, 2021, ss. 99-102).

Doğu Avrupa'da ortaya çıkan ve kendilerini "*Order of Dawn (Şafak Tarikatı)*" olarak adlandıran Yahudi karşıtı ve aşırı sağcı bir grup ise www.orderofdawn.com uzantılı web sitesi üzerinden yapmış olduğu açıklamada, Afrika ve Orta Doğu'dan Avrupa'ya göçü "*istila*" ve "*soykırım*" olarak nitelendirerek Yahudilerin medya aracılığıyla bu durumun arkasındaki asıl sorunu gizlediğini iddia etmiştir. Örgüt, üyelerinin büyük bir kısmının silahlı kuvvetlerde veya kolluk kuvvetlerinde görev yaptığını öne sürerek "*işgalcilerin teknelerini ve işbirlikçilerin devasa gemilerini püskürtmek veya batırmak*" için gönüllü bir donanmanın, kısaca anti-DEAŞ milis yapılanmasının kurulması gerektiğini vurgulamıştır. Şiddet eylemlerini desteklemek, ateşli silah ile patlayıcı temin etmek ve gönüllü ordunun teşkil edilmesini sağlamak için özellikle gizlilik odaklı Monero kripto para biriminde bağış talep etmiştir. Ayrıca örgüt, sitesinde, gerekli altyapıya sahip olanların Monero madenciliği yaparak da destek olabileceğini belirterek farklı bir bağlantı paylaşmıştır (Counter Extremism Project, 2018). Birtakım aşırı sağcı grupların da tıpkı El Kaide ve DEAŞ terör örgütleri gibi finansman faaliyetleri kapsamında kripto varlık madenciliği yaptığı bilinmektedir.

Aşırı sağcı grupların "*aşırı sağın para birimi*" olarak gördükleri kripto paraları fon toplama, yönetme, kullanma ve depolama maksadıyla artan bir ilgiyle takip ve tercih ettikleri görülmektedir (Ebner, 2018). Aşırılık yanlısı grupların veya şahısların tespit edilmesinden sonra büyük sosyal medya platformlarından (*Twitter, Telegram, vb.*) ve kitle fonlaması

platformlarından (*Patreon, GoFundMe*, vb.) engellenmesi, çevrimiçi ödeme sağlayıcıları (*PayPal, Apple Pay, Google Pay, Visa, Mastercard*, vb.) tarafından bloke edilmesi, aşırı sağcıları “*Hatreon*” ve “*Stormfront*” gibi aşırılık yanlılarının yönettiği kitle fonlaması platformlarına veya Tor tabanlı bağış sitelerine yönlendirmiştir. Ayrıca Bitcoin ile yapılan bağışların blokzinciri analizi ile tespit edilmesi ve Bitcoin borsalarının aşırılık yanlılarına hesap cüzdanı tesis etmemesi, sağ aşırılıkçı grupların Monero gibi gizlilik tabanlı kripto varlıklara yönelmesine sebep olmuştur (Elliptic, 2023a, ss. 117-118). Örneklerden anlaşılacağı üzere kripto varlıkların, aşırı sağcı gruplar tarafından özellikle dini istismar eden terör örgütlerine kıyasla finansman faaliyetleri çerçevesinde daha fazla benimsendiği ve daha yoğun şekilde kullanıldığı, kripto varlıklar cinsinden çok daha yüksek tutarlarda fon toplandığı ve gizlilik tabanlı kripto varlıklar gibi kripto varlıkların anonimliğini artıran yöntemlere daha sık başvurulduğu görülmektedir. Bu durumun, söz konusu siyasi aşırılıkçı gruplar ve terör örgütlerinin kripto varlıklar konusunda geliştirdikleri anlayış, teknik bilgi düzeyleri ve örgütsel öğrenim kapasiteleri, faaliyet gösterdikleri ortamın özellikleri ve teknik altyapılarının farklılığı gibi çeşitli sebeplerden kaynaklandığını söylemek mümkündür.

Öte yandan kripto varlıklar, ülkelerin suç gelirlerinin aklanması ve terörizmin finansmanı risklerinin belirlenmesine, değerlendirilmesine ve anlaşılmasına olanak tanıyan ulusal risk değerlendirmelerine de konu olmaktadır. Tehdit ve Kırılganlık Çalışma Grupları tarafından geliştirilen metodoloji ekseninde 31 Aralık 2022 tarihinde hazırlanan ve Hazine ve Maliye Bakanlığı tarafından 22 Mart 2023 tarihinde onaylanan Türkiye’nin Ulusal Risk Değerlendirmesi (URD) özeti MASAK tarafından yayınlanmıştır. Söz konusu URD özetinde, Türkiye’de kripto varlık hizmet sağlayıcıları sektörünün risk düzeyinin yüksek olduğu değerlendirilerek sektörün varlık gizleme veya varlık transferi amacıyla kullanılması riskinin ön plana çıktığı ve hemen hemen tüm terör örgütlerinde kripto varlık kullanımına ilişkin bulgulara rastlandığı ifade edilmiştir (MASAK, 2023, ss. 2-11). Japonya’nın URD’sinde benzer şekilde, kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanı kapsamındaki risk düzeyinin diğer iş modellerine göre yüksek olduğu değerlendirilmiştir (National Public Safety Commission, 2019, s. 58).

ABD’nin terörizmin finansmanına ilişkin URD’sinde, finansman faaliyetleri kapsamında DEAŞ ve El Kaide gibi terör örgütleri ve ABD’deki şiddet yanlısı aşırılıkçı gruplar ile bunların destekçilerinin fon toplamada ve aktarmada kripto varlıkları kullandıklarına ilişkin birtakım bulgulara yer verilmiş olup terörizmin finansmanında

halihazırda geleneksel yöntemlerin kripto varlıklara kıyasla daha yaygın şekilde kullanıldığı ifade edilmiştir. Bununla birlikte, dünya çapında kripto varlıklara ilişkin yetersiz düzenleme ve denetim rejimleri ile kripto varlıkların kullanımının giderek yaygınlaşmasının terörizmin finansmanı riskini artırdığı değerlendirilmiştir (United States Department of the Treasury, 2022, ss. 5-23). Birleşik Krallık'ın suç gelirlerinin aklanması ve terörizmin finansmanına ilişkin URD'sinde ise kripto varlıkların terörizmin finansmanındaki riski orta seviye olarak derecelendirilmiş ve söz konusu riskin artışına dikkat çekilmiştir. Kripto varlıkların sağ aşırılıkçılar arasında kullanımının daha yaygın olduğu ve dini istismar eden terör örgütleri tarafından kullanımının yaygınlaştığı ifade edilmiştir (HM Treasury, 2020, ss. 70-75).

Almanya'nın suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadele kapsamındaki URD'sine göre, kripto varlıkların dini istismar eden terör örgütleri ile sağ aşırılıkçı gruplar tarafından kullanıldığına ilişkin kanıtlar olmasına karşılık bunların terörizmin finansmanında kullanıldığına ilişkin yeterli kanıt bulunmamaktadır. Dolayısıyla kripto varlıkların terörizmin finansmanında kullanılması riski düşük olarak derecelendirilmiş ancak risk potansiyelinin gelecekte artacağına da dikkat çekilmiştir (Federal Ministry of Finance, 2019, s. 110). Rusya'nın terörizmin finansmanına ilişkin URD'sinde vaka sıklığının az olması sebebiyle ve Singapur'un terörizmin finansmanına ilişkin URD'sinde terör örgütlerinin yoğun olarak faaliyet gösterdiği bölgelerdeki teknolojik altyapı eksikliği nedeniyle kripto varlıkların terörizmin finansmanındaki riski orta ve orta-düşük seviyede derecelendirilmiştir (Federal Financial Monitoring Service, 2018, s. 18; Monetary Authority of Singapore, 2020, s. 14). Özetle, kripto varlıklar ve kripto varlık hizmet sağlayıcıları sektörü bahse konu ülkeler ile birlikte diğer birçok ülkenin terörizmin finansmanına ilişkin URD'si tarafından kapsamaktadır. Söz konusu sektör terörizmin finansmanı bağlamında Türkiye ve Japonya tarafından yüksek seviyede, Birleşik Krallık ve Rusya tarafından orta seviyede, Almanya ve Singapur tarafından düşük seviyede riskli olarak derecelendirilmiştir. Ancak yüksek riskli olarak derecelendirilmeyen ülke URD'lerinde dahi sektörün gelişmekte olan risk olarak kabul edildiği ve risk potansiyelinin gelecekteki artışının vurgulandığı dikkat çekmektedir.

Sonuç olarak, kripto varlıkların terörizmin finansmanında kullanılmasını kolaylaştıran faktörler; anonimlik, merkeziyetsiz yapı, küresel erişim ile sınır ötesi ve hızlı transfer mekanizması, düzenleme eksiklikleri iken zorlaştıran faktörler; örgütsel öğrenim ve kontrol sorunları, teknik altyapı eksikliği, likide dönüştürülemezlik ve değer oynaklığıdır. Bağışlar,

Dark Web içerisinde suç geliri ve malzeme temini, suç gelirlerinin aklanması, NFT'ler, DeFi, madencilik, ICO, karıştırıcı (mixer) hizmetleri ve gizlilik tabanlı kripto varlıklar terörizmin finansmanında kripto varlıkların potansiyel kullanım yöntemleri arasında yer almaktadır. Kripto varlıklar, terör örgütlerinin ve siyasi aşırılık yanlısı grupların finansman faaliyetlerinde geleneksel yöntemlere ek olarak kullanılmaya başlanmıştır. Bu kapsamda incelenen örnek olayların analizi sonucu gerçekleştirilen değerlendirmelere aşağıdaki bölümde yer verilecektir.

2.4. İkinci Bölüme İlişkin Değerlendirme

İnternet ve teknolojik gelişmelerin, terör örgütlerinin çeşitli ihtiyaçlarına cevap verdiği ölçüde finansman gibi çeşitli faaliyetlerine katkıda bulunduğu bilinmektedir. Bu teknolojik gelişmelerden biri olan kripto varlıklar, giderek çeşitlenen ve karmaşık hale gelen terörizmin finansman yöntem ve araçlarından biri olarak terör örgütleri tarafından kullanılmaya başlanmıştır. Bu bölümde, tezin ana sorusu içeriğindeki “*Kripto varlıklar terörizmin finansmanında neden, nasıl, ne derecede kullanılmaktadır?*” sorusu ile birlikte bu bağlamda belirlenen “*Kripto varlıkların terörizmin finansmanında kullanılmasını etkileyen faktörler nelerdir?*”, “*Kripto varlıkların terörizmin finansmanında potansiyel kullanım yöntemleri nelerdir?*”, “*Kripto varlıkların terörizmin finansmanında kullanım örnekleri nelerdir?*” şeklindeki tezin alt sorularına yanıtlar aranmıştır.

Kripto varlıkların terörizmin finansmanında kullanılmasını kolaylaştıran ve zorlaştıran faktörler, terör örgütlerinin finansman faaliyetlerinde kripto varlıkları kullanma tercihlerini etkileyebilmektedir. Bu kapsamda kolaylaştıran faktörlerin; kripto varlıkların anonimlik derecesi, merkeziyetsiz yapısı, küresel erişim ile sınır ötesi ve hızlı transfer mekanizması, düzenleme eksiklikleri olduğu ve zorlaştıran faktörlerin; terör örgütlerinin örgütsel öğrenim süreci ve kontrol sorunları, terör örgütlerinin ve faaliyet gösterdiği bölgelerin teknik altyapı eksikliği, kripto varlıkların likide dönüştürülemezlik durumları ve değer oynaklığı olduğu ortaya konmuştur. Ancak, kripto varlıkların likide dönüştürülmesinde yaşanan sorunlar ve değerinde yaşanan büyük dalgalanmalar gibi kripto varlıkların henüz geniş çapta benimsenmemesinden kaynaklanan ve terörizmin finansmanı açısından zorluk oluşturan faktörlerin, kripto varlıkların dünya çapında kullanımının yaygınlaşmasıyla birlikte hafifleyebileceği ve kripto varlıkların terörizmin finansmanında kullanımının artabileceği

sonucuna varılmıştır. Dolayısıyla, kripto varlıkların terörizmin finansmanında neden kullanıldığı ile kullanılmasını etkileyen faktörlerin neler olduğu ortaya konmuştur.

İhtiyaç duydukları fonları toplamak, ihtiyaç duydukları yere fonları aktarmak veya ihtiyaç duyulana dek fonları saklamak amacıyla terör örgütlerinin finansman faaliyetlerinde kripto varlıkları çok çeşitli yöntemlerle kullanma potansiyeli bulunmaktadır. Bu bağlamda kripto varlıkların; bağışlar, Dark Web içerisinde suç geliri ve malzeme temini, suç gelirlerinin aklanması, NFT'ler, DeFi, madencilik, ICO, karıştırıcı (mixer) hizmetleri, gizlilik tabanlı kripto varlıklar yoluyla ve daha birçok yöntem ile terörizmin finansmanında kullanılabileceği ifade edilmiştir. Ayrıca, terör örgütlerinin kripto varlıkları finansman sağlama ve aktarma süreçlerinde söz konusu yöntemlerin de aralarında bulunduğu çeşitli şekillerde kullandıklarına ilişkin belirlenen ve 2012 ila 2023 yılları arasında gerçekleşen birçok olay bu kapsamda incelenmiştir. Dolayısıyla, kripto varlıkların terörizmin finansmanında nasıl kullanıldığı ile potansiyel kullanım yöntemlerinin neler olduğu ortaya konmuştur.

İncelenen söz konusu örnek olayların analizi neticesinde; terör örgütlerinin ve terör örgütlerine finansman sağlayan grupların veya bireylerin ideolojik ve pratik sebeplerle kripto varlık kullanımına yöneldikleri, son yıllarda terörizmin finansmanında kripto varlık kullanımının arttığı ve kripto varlıklar cinsinden daha yüksek miktarlarda finansman sağlanabildiği, terör örgütlerinin kripto varlıkları kullanarak yeni finansman tipolojileri oluşturma çabasında oldukları ve gizlilik tabanlı kripto varlıklar gibi kripto varlıkların anonimliğini artıran yöntemlere daha fazla başvurdukları değerlendirilmiştir. Ayrıca, siyasi aşırılıkçı grupların da genellikle geleneksel finansal sistemlerden dışlanmaları sonucunda finansman faaliyetleri çerçevesinde kripto varlık kullanımına yöneldikleri anlaşılmış ve bu kapsamda incelenen örnek olayların analizi sonucunda, aşırı sağcı grupların terör örgütlerine kıyasla finansman faaliyetlerinde kripto varlıkları daha fazla benimsedikleri, kripto varlıklar cinsinden çok daha yüksek tutarlarda fon topladıkları ve kripto varlıkların anonimliğini artıran yöntem ve teknolojileri daha fazla kullandıkları değerlendirilmiştir. Dolayısıyla, kripto varlıkların terörizmin finansmanında ne derecede kullanıldığı ile kullanım örneklerinin neler olduğu ortaya konmuştur.

ÜÇÜNCÜ BÖLÜM

KRİPTO VARLIKLAR VE MALİ EYLEM GÖREV GÜCÜ (FINANCIAL ACTION TASK FORCE-FATF) TAVSİYELERİ

3.1. Mali Eylem Görev Gücü’nün Tarihçesi

1989 yılında gerçekleşen G7 ülkelerinin Paris Zirvesi’nde, uluslararası düzeyde mali suçlarla mücadele ve finansal sistemin güvenliği konularında daha etkili bir iş birliği sağlama amacıyla Mali Eylem Görev Gücü (*Financial Action Task Force-FATF*) kurulmuş olup görevi, bankacılık sistemi ve finansal kuruluşların kara para aklama amacıyla kullanılmasını önlemek amacıyla yürütülen iş birliğinin sonuçları ile yasal ve düzenleyici sistemlerin uyarlanması da dahil olmak üzere bu alanda ek önleyici çabaları değerlendirmek olarak belirtilmiştir (United States Department of the Treasury, 2022, ss. 5-23). İktisadi İşbirliği ve Gelişme Teşkilatı (*Organisation for Economic Co-operation and Development-OECD*) rehberliğinde kurulan FATF, başlangıçta ABD, Kanada, Fransa, Almanya, İtalya, Japonya, Birleşik Krallık olmak üzere G7 ülkelerini, Avrupa Komisyonu’nu ve Avustralya, Avusturya, Belçika, Hollanda, İspanya, İsveç, İsviçre, Lüksemburg’u bünyesinde barındırmaktayken (Yurdakul, 2023, s. 51) zaman içerisinde üye sayısı artarak 40’a ulaşmış (Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation, 2023) ve 2019 yılından itibaren görev süresi süresiz olarak uzatılmıştır (FATF, 2023b).

FATF, küresel finansal sistemi suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanına karşı korumak için politikalar geliştiren bağımsız bir hükümetler arası kuruluş olarak bu alanda önemli bir rol üstlenmektedir (Salami, 2017, s. 9). Merkezi Paris olan FATF, suç ve terör örgütlerinin fon toplama, kullanma ve aktarmada uyguladıkları yöntem ve trendleri takip ederek, bu riskleri azaltmak için ülkelerin ve özel sektörün farkındalığını artırmak amacıyla düzenli olarak raporlar yayınlamakta; küresel ölçekte standartlar belirlemekte; ülkeleri söz konusu standartları tam ve etkili bir şekilde uyguladıklarından emin olmak için değerlendirmekte; standartlara tam olarak uymayan ülkeleri belirleyerek bu ülkeleri “*Artırılmış İzlemeye Tabi*” veya “*Yüksek Riskli*” olarak adlandırmaktadır (FATF, 2023c).

FATF, ülkelerin, suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı ile mücadelede uygulaması gereken tedbirlerin kapsamlı bir çerçevesini oluşturmak ve uluslararası iş birliğini kolaylaştırmak amacıyla tavsiye kararları almaktadır. FATF tavsiyeleri, ülkelerin kendi hukuki, idari, mali ve operasyonel sistemlerine uygun şekilde uyarlamaları gereken uluslararası standartlar belirlemektedir. Uyuşturucu kaçakçılığından elde edilen gelirlerin aklanması ve finansal sistemlerin kötüye kullanılmasıyla mücadele kapsamında ilk olarak 1990 yılında hazırlanan FATF 40 tavsiye kararı, gelişen kara para aklama eğilimlerini ve tekniklerini yansıtacak şekilde kapsamı genişletilerek 1996 yılında revize edilmiştir (FATF, 2012, s. 7).

Terörizmin finansmanı ile mücadele, 2001 yılından bu yana FATF'in odak noktası olmuştur (Wang ve Zhu, 2021, s. 2332). 2001 yılında ABD'de gerçekleştirilen 11 Eylül terör saldırısının ardından, terörizmle mücadeleye ek olarak terörizmin finansmanı ile mücadelenin gerekliliğinin gündeme gelmesiyle birlikte FATF, 30 Ekim 2001 tarihlerinde olağanüstü toplantısını gerçekleştirerek terörizmin finansmanı ile mücadeleyi de kapsayacak şekilde yetki alanını genişletmiş ve bu kapsamda 8 özel tavsiye kararını yayınlamıştır. Daha sonrasında FATF, 2004 tarihinde nakit taşıyıcılar konusundaki 9. özel tavsiye kararını kabul ederek terörizmin finansmanı ile mücadele kapsamındaki tavsiyelerini toplam 9 özel tavsiye kararı olacak şekilde revize etmiştir (Üstün, 2005, ss. 10-12). FATF'in suç gelirlerinin aklanmasının önlenmesine ilişkin 40 tavsiye kararı ile terörizmin finansmanının önlenmesine ilişkin 9 özel tavsiye kararı birleştirilerek, kitle imha silahlarının yayılmasının finansmanının önlenmesi konusunu da kapsayacak şekilde yeniden düzenlenmiş ve son olarak 16 Şubat 2012 tarihinde FATF tavsiyeleri adı altında kabul edilerek yayımlanmıştır. Toplamda 40 adet olan FATF tavsiyeleri söz konusu tarihten itibaren, yeni ortaya çıkan tehditleri ele almak, mevcut yükümlülükleri açığa kavuşturarak güçlendirmek, gerekli istikrarı ve titizliği korumak, yüksek risk durumlarına ilişkin gereklilikleri güçlendirerek ülkelerin daha odaklı bir yaklaşım benimsemesine olanak sağlamak gibi amaçlarla düzenli olarak güncellenmektedir (FATF, 2012). FATF, 2019 yılında kripto varlıklarla ilgili faaliyetlerin ve kripto varlık hizmet sağlayıcılarının düzenlenmesi ve denetlenmesine yönelik bağlayıcı tedbirleri içerecek şekilde standartlarını revize etmiş ve 2022 yılında yasa dışı faaliyetlerin ve suç gelirlerinin gizli kurumsal yapıların arkasına saklanması önlemek amacıyla standartlarındaki gerçek faydalanıcılık kurallarını güçlendirmiştir (FATF, 2023b).

FATF, dünya genelindeki üye ülkeleri, gözlemci üyeleri ve iş birliği yapılan diğer bölgesel gruplar ile birlikte geniş bir paydaş ağına sahiptir. FATF ile birlikte, FATF tavsiyelerinin üyeleri tarafından etkin bir şekilde uygulanmasının teşvik edilmesinde ve FATF politikalarının oluşturulmasına katkı sağlanmasında önemli bir role sahip olan dokuz adet FATF Benzeri Bölgesel Kuruluş (*FATF-Style Regional Bodies-FSRB*)’tan oluşan FATF küresel ağı, dünya üzerinde 200’den fazla hükûmeti ve 20 uluslararası gözlemci kuruluşu bir araya getirerek, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadelenin küresel ölçekte yürütülmesinde büyük önem taşımaktadır (FATF, 2023e). FATF’in 40 adet üyesi, 9 adet FSRB ve dünyada geniş çapta birçok ülke FATF tavsiyelerini uygulamayı taahhüt etmiştir (FATF, 2023e). FATF küresel ağı, mali suçlarla mücadelede uluslararası koordinasyonu sağlayarak iş birliğini geliştirmektedir. Söz konusu kapsamlı ve koordineli yaklaşım, mali suçlar karşısında uluslararası sistemin güvenliğini sağlamada merkezi bir öneme sahiptir (Keatinge vd., 2018, s. 20).

3.2. Mali Eylem Görev Gücü’nün Çalışma Alanları

FATF, suç gelirlerinin aklanması ve terörizmin finansmanında kullanılan yöntem ve eğilimleri belirlemek, önlemleri geliştirmek ve ülkeleri önlemleri uygulamaları konusunda değerlendirmek için çeşitli alanlarda çalışmalar yürütmektedir. FATF’in temel çalışma alanları; suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanında kullanılan yöntem ve trendler üzerine araştırmalar yürütmek, söz konusu mali suçlarla mücadelede uluslararası düzeyde kabul gören standartlar olan FATF tavsiyelerini oluşturmak, FATF tavsiyelerinin uygulanma düzeylerini belirlemek için farklı ülkelerden üyelerin başka bir ülkeyi değerlendirdiği emsal incelemeler olan ayrıntılı ülke raporları (FATF Karşılıklı Değerlendirme Raporları) yayımlamak, zayıf suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele rejimlerine sahip ülkeleri tespit ederek kamuya açık olarak listelemektir. Terörizmin finansmanı, kitle imha silahlarının yayılmasının finansmanı, gerçek faydalanıcılık, yolsuzluk, finansal tabana yayılma ve kâr amacı gütmeyen kuruluşlar, kripto varlıklar, dijitalleşme, çevre suçu, varlık kurtarma konuları ise FATF’in öncelik verdiği ek çalışma alanlarıdır (FATF, 2023f).

3.2.1. Yöntem ve Trendlerin Belirlenmesi

Yasa dışı faaliyetlerin finansmanı ile bu faaliyetlerden elde edilen malvarlığı değerlerinin aklanmasında kullanılan yöntem ve teknikler sürekli olarak gelişmekte olup FATF ülkelerin bu riskleri anlamalarına ve etkili önlemler almalarına yardımcı olmak amacıyla gelişen yöntem ve trendler üzerine araştırma faaliyetleri yürüterek sürekli olarak raporlar yayımlamaktadır (FATF, 2023h). Raporlar, ülkelerin söz konusu risklere karşı bilinçli ve hazırlıklı olmalarına katkıda bulunmayı ve küresel finansal sistemi daha güvenli hale getirmeyi hedeflemektedir.

3.2.2. FATF Tavsiyeleri

Tüm dünyada geniş ölçüde kabul gören standartlarının ulaşmış olduğu etki düzeyi göz önüne alındığında, faaliyet alanında uluslararası kuruluş gibi etkili olduğu söylenebilen FATF'in standartları içerisinde tavsiyeler önemli bir yere sahiptir (Yurdakul, 2023, ss. 51-52). Ülkelerin yasal, idari, operasyonel ve mali yapılarının farklılık göstermesi, suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı ile mücadelede aynı önlemleri almalarını imkânsız kılmaktadır. Bu nedenle FATF, ülkelerin kendi sistemlerine uyarlayacakları temel önlemleri belirlemek ve bu konuda uluslararası bir standart oluşturmak amacıyla 40 tavsiyeyi oluşturmuştur (FATF, 2012, s. 7). FATF tavsiyeleri bağlayıcı değildir ancak ülkeler tavsiyeleri uygulamaya teşvik edilmektedir (Salami, 2017, s. 9). Yasal olarak bağlayıcılığı bulunmamasına karşılık tavsiyelerin çoğu zaman birçok ülkenin mevzuatına dahil edildiği görülmektedir (Eisermann, 2020, s. 29). Çünkü FATF, doğrudan yaptırım uygulama yetkisine sahip olmasa da belirlediği standartlara uymaya teşvik etmek için yumuşak güç araçlarına sahiptir. Gri ve kara listelere alınma riskini önlemek isteyen ülkeler, finansal faaliyetlerinin olumsuz etkilenmesinden kaçınmak adına FATF tavsiyelerini benimsemeye ve uygulamaya özen göstermektedir (Başaranel ve Türkşen, 2019, s. 71). FATF tavsiyeleri, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadelede küresel düzeyde bir çerçeve sağlamaktadır (Kfir, 2020, s. 121).

FATF'in 40 tavsiyesi; “suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele politikaları ve koordinasyon”, “suç gelirlerinin aklanması ve müsadere”, “terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı”, “önleyici

tedbirler”, “*tüzel kişilerde ve yasal oluşumlarda şeffaflık ve gerçek faydalanıcılık*”, “*yetkili makamların yetki ve sorumlulukları ile diğer kurumsal tedbirler*” ve “*uluslararası iş birliği*” olmak üzere yedi başlık altında gruplandırılmıştır (FATF, 2012). FATF tavsiyelerinin etkili bir şekilde uygulanmasının merkezinde risk bazlı yaklaşım bulunmaktadır. Ülkelerin, risk bazlı yaklaşımı benimseyerek söz konusu mali suçlarla mücadelede kaynaklarını yüksek riskli alanlarda önceliklendirerek uygun tedbirler alması gerekmektedir (FATF, 2012, s. 8). Risk bazlı yaklaşımın benimsenmesi, ülkelerin daha etkili ve odaklı bir strateji oluşturmalarına olanak tanımaktadır.

Küresel finansal sistemin güvenlik ve bütünlüğünü sağlamak için özel sektör, sivil toplum ve ilgili diğer paydaşlarıyla yakın ilişki sürdürmeye çalışan FATF; tavsiyelerin kendisini, “*açıklayıcı notları*” ve “*sözlük*” tanımlarını içeren FATF tavsiyelerinin yanı sıra, tavsiyelerin uygulanmasına katkı sağlamak amacıyla rehberlik ve en iyi uygulama belgeleri ile diğer tavsiyeleri de hazırlamaktadır (FATF, 2012, ss. 8-9). Bunlarla birlikte, ülkelerin teknik uyum ve etkililik açısından değerlendirilmesine yönelik kriterlerin yer aldığı “*metodoloji*” de FATF standartlarından birini oluşturmaktadır (Yurdakul, 2023, s. 52).

3.2.3. Karşılıklı Değerlendirme Raporları

FATF’in en önemli araçlarından biri olan Karşılıklı Değerlendirme Raporları’nda, ülkelerin suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı ile mücadelede aldıkları tedbirler ve FATF tavsiyelerini uygulama düzeyleri değerlendirilmektedir. FATF metodolojisinin kullanıldığı karşılıklı değerlendirmelerde, farklı ülkelere üyeler başka bir ülkeyi yerinde ziyaret etmekte ve mali suçlar karşısında etkili bir çerçeveye sahip olup olmadığını etkililik (ülkenin aldığı tedbirlerin başarılı olduğunu gösteren kanıtlar) ve teknik uyum (yürürlükte olan kanunlar, düzenlemeler ve diğer yasal araçlar) açısından değerlendirerek sistemi güçlendirmek adına gerekli öneriler sunmaktadır (FATF, 2023i). Karşılıklı değerlendirmelerde, ülkeler arasında iş birliğinin teşvik edilerek mali suçların önlenmesinde daha güçlü ve koordineli bir mücadele sistemi ve etkili bir küresel çerçeve oluşturulması amaçlanmaktadır.

FATF standartlarından biri olan metodoloji, ülkelerin suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele sistemlerinin etkililik düzeyi ve FATF tavsiyelerine teknik uyum değerlendirmelerinin yapılması için temel oluşturmaktadır. Metodolojinin

teknik uyum bileşeni, yasaların ve uygulanabilir araçların yapısının yanı sıra yetkili makamların varlığını, yetkilerini ve prosedürlerini de kapsayacak şekilde FATF tavsiyelerinde belirtilen belirli gerekliliklerin uygulamaya konulmasıyla ilgilidir. Metodolojinin etkililik bileşeni ise FATF standartları doğrultusunda suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele sistemlerinin temel hedeflerine pratikte etkili bir şekilde ulaşıp ulaşılmadığının değerlendirilmesiyle ilgilidir (FATF, 2013, ss. 5-15). FATF'in mevcut değerlendirme metodolojisinde, etkililik kriteri olarak belirlenen 11 adet kısa vadeli hedef benimsenmiştir (Yurdakul, 2023, ss. 52-55). Son olarak 2023 yılı haziran ayında güncellenen metodolojide; finansal kuruluşlar, finansal olmayan belirli iş ve meslekler (FOBİM) ve kripto varlık hizmet sağlayıcılarının suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele yükümlülüklerine uyum açısından denetleyiciler tarafından risk bazlı yaklaşımla denetlenmesi ve düzenlenmesi konusundaki 3 nolu kısa vadeli hedef ile birlikte bunların söz konusu mali suçlarla mücadelede yeterli şekilde önleyici tedbirleri uygulaması ve şüpheli işlemleri bildirmesi konusundaki 4 nolu kısa vadeli hedef doğrudan kripto varlık hizmet sağlayıcılarını ve dolayısıyla kripto varlıkları ilgilendirmektedir (FATF, 2013, s. 16). Ayrıca, kripto varlıklar konusunun diğer etkililik kriteri olarak belirlenen kısa vadeli hedefler tarafından da dolaylı olarak kapsandığı görülmektedir.

3.2.4. Yüksek Riskli ve Artırılmış İzlemeye Tabi Ülkelerin Belirlenmesi

Yüksek riskli ve artırılmış izlemeye tabi ülkelerin belirlenmesi, FATF'in uluslararası finansal sistemin bütünlüğünün korunması amacıyla yürüttüğü kapsamlı bir süreçtir. FATF dünya genelindeki ülkeleri sürekli olarak izlemekte ve belirli kriterlere dayanarak hangilerinin yüksek riskli veya artırılmış izleme altında olması gerektiğini belirlemektedir. Suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele uygulamalarının zayıf olduğu belirlenen söz konusu ülkelere kaynaklanan riskler hakkında, hem uluslararası finansal sistemin bütünlüğünün korunması amacıyla hem de ülkelerin küresel ekonomideki konumlarını korumak için eksikliklerini gidermeleri yönünde baskı oluşturacağından dolayı kamuya açık uyarılar yayınlanmaktadır. Suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele rejimlerinde önemli stratejik eksiklikler bulunan yüksek riskli ülkeleri kara liste olarak bilinen kategoride, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele rejimlerindeki stratejik eksiklikleri gidermek amacıyla FATF ile aktif olarak çalışan artırılmış izlemeye tabi ülkeleri gri liste olarak bilinen kategoride

sınıflandırılarak duyurulmaktadır (FATF, 2023i). Bu listelerde yer alan ülkeler, FATF tarafından düzenli olarak gözden geçirilmekte ve güncellenmekte olup söz konusu süreç, ülkelerin suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele rejimlerindeki gelişmelerin veya eksikliklerin sürekli olarak takip edilmesini sağlamaktadır.

3.3. Mali Eylem Görev Gücü'nün Kripto Varlıklar Alanında Yaptığı Yayınlar

Kripto para birimlerini, merkezi olmayan sanal para birimleri şeklinde ifade eden ve sanal para birimleri içerisinde bir alt kategori olarak değerlendiren FATF'in, benzer şekilde kripto varlıkları da sanal varlıklar içerisinde değerlendirdiği söylenebilir. Nitekim FATF, birçok kurumun kripto varlıkları tanımlarken kullandığı matematik tabanlı ve dağıtık ifadelerini sanal varlık tanımında kullanmayarak sanal varlıkların kapsamını daha geniş tutmaktadır (Coelho vd., 2021, s. 3). FATF, kripto varlıklar alanında gelişen teknoloji ve iş modellerinin belirsizliğini göz önünde bulundurarak, bu alanda kapsamlı bir anlayış ve çerçeve geliştirmeye çalışmakta ve bu nedenle terminolojisinde sanal varlık kavramını kullanmaktadır. FATF'in kripto varlıklara sanal varlık kavramı üzerinden atıfta bulunduğu ve sanal varlıklara ilişkin değerlendirmelerinin kripto varlıkları da içerdiği açıkça görülmektedir (FATF, 2023k). Dolayısıyla bağlamın korunacağı değerlendirilerek, bu bölümde her ne kadar FATF'in yaklaşımı ele alınsa da terminolojisinde kullandığı sanal varlık kavramı yerine tezin bütünlüğü açısından kripto varlık teriminin kullanımı tercih edilmiştir.

FATF, kripto varlıklar ve kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanı açısından finansal sistemde oluşturduğu potansiyel riskler ile ilgili olarak birçok çalışma yürüterek raporlar ve rehberler yayınlamıştır. Standartların güçlendirilmesi, FATF'in kripto varlık faaliyetlerinin finansal sistemi suistimal etmesinin önlenmesi için geliştirdiği kapsamlı yaklaşımın bir parçasıdır. Kripto paralara olan ilginin artmasıyla birlikte 2014 yılının haziran ayında FATF, temel tanımlar ile potansiyel suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele risklerine ilişkin bir rapor yayınlamıştır. Raporda, bu alana ilişkin temel tanımlar yapılarak ortak bir sözlük oluşturulması hedeflenmiştir. Ayrıca, kripto para birimleri sınıflandırılmış ve tipik bir kripto para sistemindeki katılımcılar açıklanmıştır. Rapor aynı zamanda kripto para birimlerinin suç gelirlerinin aklanması ve terörizmin finansmanı risklerine ilişkin bir ön değerlendirme yapmıştır (FATF, 2014). FATF, bu çalışma ile kripto varlıkların geleneksel finansal sistemle

etkileşimini anlamak ve uygun düzenlemelerin oluşturulmasına katkıda bulunmak amacıyla önemli bir ilk adım atmıştır.

FATF, aşamalı yaklaşımın bir parçası olarak 2015 yılının haziran ayında kripto para birimlerine ilişkin risk bazlı yaklaşım rehberini yayınlamıştır. Rehber, risk bazlı yaklaşımın, düzenlenmiş finansal sistemle etkileşime girebilen kripto para ödeme ürünleri ve hizmetleri ile ilişkili suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele risklerine uygulanmasına odaklanmıştır. Rehber aynı zamanda, FATF tavsiyelerinin kripto para birimleri bağlamında nasıl uygulanması gerektiğine dair detaylı bilgiler sunmaktadır (FATF, 2015). Rehber, dünya genelinde kripto paraların kullanımının artmasıyla birlikte, bu alanda finansal kurumların ve düzenleyicilerin nasıl yaklaşımları gerektiğini belirlemek amacıyla yayımlanmıştır.

17-19 Ekim 2018 tarihleri arasında yapılan FATF Genel Kurulu toplantısında; kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanında artan kullanımı karşısında FATF tavsiyelerinin güçlendirilmesi için yapılması gereken değişiklikler tartışılmıştır (FATF, 2018). Bu kapsamda, tezin önceki bölümlerinde açıklandığı üzere sözlüğe yeni kripto varlık ve kripto varlık hizmet sağlayıcısı tanımları eklenmiş ve “Yeni Teknolojiler” adlı 15 nolu tavsiye, aşağıda belirtilen paragrafın eklenmesiyle genişletilerek revize edilmiştir (FATF, 2012, ss. 17-138).

“Sanal varlıklardan kaynaklanan riskleri yönetmek ve azaltmak için ülkeler; sanal varlık hizmet sağlayıcılarının, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele amaçları doğrultusunda düzenlenmesini, lisanslı veya kayıtlı olmasını ve FATF tavsiyelerinde belirtilen ilgili tedbirlere uygunluğun izlenmesi ve sağlanması için etkili sistemlere tabi olmasını sağlamalıdır.”

2019 yılının haziran ayında FATF, kripto varlıklarla ilgili uluslararası standartlarda yaptığı değişiklikleri netleştiren ve standartların risk bazlı yaklaşım çerçevesinde kripto varlık faaliyetlerine ve kripto varlık hizmet sağlayıcılara uygulanmasını ortaya koyan, 15 nolu tavsiyeye ilişkin açıklayıcı notu kabul ederek yayımlamıştır. 15 nolu tavsiyeye ilişkin açıklayıcı not, kripto varlıkların suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanında kullanılmasının önlenmesi için ülkelerin ve

yükümlü kuruluşların ilgili FATF tavsiyelerine nasıl uyum sağlamaları gerektiğini açıklamaktadır. Söz konusu açıklayıcı not; kripto varlık hizmet sağlayıcılarının denetlenmesi veya izlenmesi, lisanslama veya kayıt, müşteri durum tespiti, kayıt tutma ve şüpheli işlem bildirimi gibi önleyici tedbirler, yaptırımlar ve diğer tedbirler ile uluslararası iş birliği gibi konuları içermektedir (FATF, 2019a).

Teknolojinin ilerleme ivmesinin, küresel düzenleyicilerin eylemleri koordine etme yeteneğini aşmasıyla birlikte FATF, kripto varlıklara ilişkin 2015 yılında yayınlamış olduğu rehberi revize etmiştir (Keatinge vd., 2018, s. 46). 2019 yılının haziran ayında FATF, söz konusu önceki rehberi temel alan kripto varlıklar ve kripto varlık hizmet sağlayıcılarına ilişkin risk bazlı yaklaşım rehberini yayınlamıştır. Rehber, ülkelerin kripto varlık faaliyetlerine ve kripto varlık hizmet sağlayıcılarına yönelik düzenleyici ve denetleyici mekanizmalarını risk bazlı yaklaşım çerçevesinde geliştirmelerine ve kripto varlık faaliyetlerinde bulunan aktörlerin suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele yükümlülükleri ile FATF gereksinimlerini anlamalarına katkıda bulunmayı amaçlamaktadır (FATF, 2019b, s. 4). Rehber aynı zamanda, özel sektördeki kuruluşların FATF gerekliliklerini anlamalarına ve uygulamalarına yardımcı olmaktadır (LexisNexis Risk Solutions, 2019, s. 2). Söz konusu rehber, risk bazlı yaklaşımı detaylı bir şekilde ele alarak ve kripto varlık faaliyetlerindeki güncel gelişmeler ile özel risklere odaklanarak, uluslararası düzeyde daha etkili bir önleyici yaklaşımın benimsenmesine destek olmayı hedeflemektedir.

FATF 2020 yılının haziran ayında, istikrarlı kripto paralar hakkında da bir rapor yayınlamış, söz konusu kripto varlık türünün diğer kripto varlıklara kıyasla daha fazla kitlesel olarak benimsenme eğilimine ve dolayısıyla suç gelirlerinin aklanması ve terörizmin finansmanında artan kullanımına dikkat çekmiş ve FATF tavsiyelerinin gerekliliklerinin uygulanması gerektiğinin altını çizmiştir. Söz konusu rapor, istikrarlı kripto paraların özellikleri, suç gelirlerinin aklanması ve terörizmin finansmanında kullanılma riskleri, FATF tavsiyelerinin nasıl uygulanacağı gibi konulara değinmektedir (FATF, 2020b).

FATF 2020 yılının eylül ayında, kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanında kullanılıyor olabileceğine ilişkin kırmızı bayrak göstergelerini içeren raporu yayınlamıştır. Raporun amacı; finansal kuruluşlar, finansal olmayan belirli iş ve meslekler ile kripto varlık hizmet sağlayıcıları gibi yükümlü kuruluşların kripto

varlıkların kullanıldığı potansiyel suç gelirlerinin aklanması ve terörizmin finansmanı faaliyetlerini tanımlamasını, bildirmesini ve FATF tavsiyelerinde yer alan yükümlülüklerini risk bazlı yaklaşım çerçevesinde yerine getirmesini kolaylaştırmaktır. Rapor yükümlü kuruluşların yanı sıra, mali istihbarat birimleri gibi düzenleyici ve denetleyici makamlar, yargı teşkilatı ve kolluk birimleri tarafından da kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanında kullanım belirtilerinin anlaşılmasına yardımcı olmayı amaçlamaktadır (FATF, 2020a). Söz konusu raporun, kripto varlıkların terör örgütleri tarafından finansman faaliyetlerinde kullanılmasının önlenmesi konusunda finans sektörünün müşteri durum tespiti yapmasına büyük katkısı olduğu değerlendirilmektedir (Wang ve Zhu, 2021, s. 2336).

FATF, 2019 yılında yayınlamış olduğu kripto varlıklara ve kripto varlık hizmet sağlayıcılarına ilişkin risk bazlı yaklaşım rehberini 2021 yılının ekim ayında güncellemiştir. FATF'in kripto varlık teknolojisi ve sektöründeki gelişmeleri takip etmesinin bir parçasını oluşturan söz konusu rehber, uygulama engellerine yönelik örnekler ve çözüm önerileri sunmasının yanı sıra altı ana alanda güncellemeler yapmıştır. Rehberde, kripto varlıkların ve kripto varlık hizmet sağlayıcılarının tanımları netleştirilmiş, FATF tavsiyelerinin istikrarlı kripto paralara nasıl uygulanması gerektiği açıklanmış, üçüncü bir tarafın bulunmadığı eşler arası gerçekleşen işlemlere ilişkin riskler karşısında ülkelerin kullanabileceği araçlar hakkında ek rehberlik sağlanmış, kripto varlık hizmet sağlayıcılarının lisanslanması ve kayıt altına alınması konusunda güncellemeler yapılmış, “*Seyahat Kuralı (Travel Rule)*” hakkında kamu sektörü ve özel sektör için ek rehberlik sağlanmış, kripto varlık hizmet sağlayıcılarının denetimlerini gerçekleştirenler arasında benimsenmesi gereken iş birliği ve bilgi paylaşımı ilkeleri açıklanmıştır (FATF, 2021a).

Ayrıca FATF, standartlarının kripto varlıklara ve kripto varlık hizmet sağlayıcılarına uygulanmasının incelenmesine yönelik 2020, 2021, 2022, 2023 yıllarında dört adet rapor yayınlamıştır. FATF, güncellenmiş tavsiyelerinin kamu ve özel sektör dahilinde uygulanmasını gözden geçirmek ve kripto varlıklar sektöründe tipolojileri, riskleri ve piyasa yapısındaki değişiklikleri takip etmek amacıyla 12 aylık bir inceleme yapmış ve inceleme bulgularını 2020 yılının haziran ayında yayınladığı raporda ortaya koymuştur. Rapor, genel olarak, kamu ve özel sektörün güncellenmiş FATF tavsiyelerinin kripto varlıklar ve kripto varlık hizmet sağlayıcıları bağlamında uygulanmasında ve Seyahat Kuralı'nın

uygulanmasını sağlayacak teknolojik çözümlerin geliştirilmesinde ilerleme kaydedildiğini belirtmiştir (FATF, 2020c).

2021 yılının temmuz ayında FATF, 2020 yılında yayınladığı inceleme raporunun ardından ikinci 12 aylık inceleme bulgularını ortaya koyan raporunu yayınlamıştır. Raporda, birçok ülke ve kripto varlık hizmet sağlayıcıları sektörü tarafından, Seyahat Kuralı dahil olmak üzere FATF tavsiyelerinin kripto varlıklar bağlamında uygulanmasında ilerleme kaydedildiği; ancak küresel çapta suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele konusunda daha etkili bir çerçeve oluşturmak adına uygulamanın yeterli olmaktan uzak olduğu ifade edilmiştir (FATF, 2021b).

2022 yılının haziran ayında FATF, tavsiyelerinin kripto varlıklar ve kripto varlık hizmet sağlayıcıları bağlamında uygulanmasına ilişkin yukarıda bahsedilen önceki iki küresel incelemesine dayanan hedeflenen güncelleme raporunu yayınlamıştır. Raporda, FATF'in 15 nolu tavsiyesi ve açıklayıcı notunun ülkeler tarafından uygulamasına ilişkin kısa bir güncelleme yapılmış, Seyahat Kuralı'na odaklanılmış, DeFi, NFT pazaryerleri, kripto varlık borsalarında barındırılmayan cüzdanlar (*unhosted wallets*) gibi gelişmeler ve bunlara ilişkin ortaya çıkan yasa dışı finansman risklerinden bahsedilmiştir (FATF, 2022).

2023 yılının haziran ayında FATF, Seyahat Kuralı ile birlikte tavsiyelerinin kripto varlıklar ve kripto varlık hizmet sağlayıcıları bağlamında uygulanmasına yönelik dördüncü inceleme bulgularını ortaya koyan hedeflenen güncelleme raporunu yayınlamıştır. Raporda, Seyahat Kuralı dahil olmak üzere FATF'in 15 nolu tavsiyesi ve açıklayıcı notuna ülke uyumu hakkında ve DeFi, NFT'ler, barındırılmayan cüzdanlar, eşler arası işlemler, istikrarlı kripto paralar gibi kripto varlıklar alanında ortaya çıkan riskler ve piyasa gelişmeleri hakkında güncellemeler sunulmuştur. Ayrıca raporda, güncellenen standartlara göre değerlendirilen ülkelerin %75'inin gerekliliklere tamamen veya kısmen uymadığına dikkat çekilmiştir (FATF, 2023k).

2023 yılının ekim ayında FATF, kitle fonlamanın terörizmin finansmanında kullanılmasına dikkat çektiği raporunu yayınlamıştır. Raporda terör örgütlerinin kitle fonlaması yoluyla fon toplamada; kâr amacı gütmeyen kuruluşlar, özel kitle fonlaması platformları veya internet siteleri, sosyal medya platformları veya mesajlaşma uygulamaları, gizlilik tabanlı kripto varlıklar ve karıştırıcı (mixer) hizmetleri gibi anonimliği artırıcı

teknolojiler dahil olmak üzere kripto varlıklar şeklinde dört ana yöntem kullandıkları ortaya konmuştur. Rapora göre terör örgütleri sıklıkla söz konusu yöntemlerin bir kombinasyonunu kullanarak, kitle fonlaması kampanyalarıyla bağışçılarından kripto varlıklar ile fon toplayabilmekte, toplanan fonların anonimliğini artırmak için çeşitli yöntemlere başvurarak genellikle kripto varlık hizmet sağlayıcıları aracılığıyla kripto varlıkları itibari para birimlerine dönüştürmek suretiyle veya doğrudan operasyonel ihtiyaçları için kullanabilmektedir (FATF, 2023a).

Diğer taraftan FATF, 2019 yılının temmuz ayında terörizmin finansmanına ilişkin risk değerlendirme rehberini yayınlamıştır. Ülkelerin URD'lerinde terörizmin finansmanı riskini değerlendirirken benimsemesi gereken yaklaşımlar, ilgili bilgi kaynakları ve pratik örnekler sunan rehber, daha fazla bilgiye ihtiyaç duyulan alanların belirlenmesinin önemini vurgulamaktadır (FATF, 2019c). Ancak rehberde kripto varlıklar ile kripto varlık hizmet sağlayıcıları sektörüne değinilmemiş ve terörizmin finansmanı kapsamında oluşturduğu risklere ilişkin herhangi bir değerlendirme yapılmamıştır. Dünya üzerinde birçok ülkenin URD'sine de konu olan söz konusu risklerin, ülkelere bu konuda rehberlik etmeyi amaçlayan anılan rehberde ele alınmaması büyük bir eksiklik olarak değerlendirilmektedir.

Genel olarak bakıldığında, FATF, kripto varlıklar ve kripto varlık hizmet sağlayıcılarıyla ilgili olarak suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadelede ortaya çıkan riskleri belirlemek, sektörel gelişmeleri takip ederek güncellemeler yapmak, küresel düzenleyici çerçeve oluşturmak, standartlarının küresel ölçekte uygulanmasını takip etmek ve değerlendirmek amacıyla çeşitli raporlar yayınlamıştır. FATF yayınladığı raporlar aracılığıyla, uluslararası topluma rehberlik etmeyi ve ülkelerin kripto varlık alanındaki faaliyetleri düzenlemeleri konusunda etkili bir iş birliği sağlamayı hedeflemektedir.

3.4. FATF Tavsiyelerinin Kripto Varlıklar Bağlamında İncelenmesi

Yukarıda bahsedildiği üzere yapılan güncellemelerle birlikte, kripto varlıklar da FATF tavsiyelerinin bir parçası haline gelmiştir (Eisermann, 2020, s. 30). Ülkeler, FATF tavsiyeleri kapsamındaki ilgili önlemleri kripto varlıklar ile faaliyetlerine ve hizmet sağlayıcılarına da uygulamalıdır. FATF'e göre kripto varlık hizmet sağlayıcıları, finansal kuruluşlar ile finansal olmayan belirli iş ve meslekler ile aynı yükümlülüklerle sahiptir

(FATF, 2021a, ss. 4-5). Kripto varlık faaliyetleri bağlamında FATF tavsiyelerinin tamamı geçerli olsa da (Schwarz vd., 2021, s. 12), kripto varlıkları daha yakından ilgilendirdiği değerlendirilen tavsiyeler ile birlikte söz konusu tavsiyelerin kripto varlıklar ve kripto varlık hizmet sağlayıcıları bağlamında nasıl değerlendirildiği ve varsa bunlara ilişkin özel koşullar aşağıda detaylı bir şekilde ele alınmıştır.

3.4.1. FATF'in 1 Nolu Tavsiyesi

“Suç Gelirlerinin Aklanması ve Terörizmin Finansmanı ile Mücadele Politikaları ve Koordinasyon” başlığı altında yer alan “Riskleri değerlendirmek ve risk bazlı bir yaklaşım uygulamak” adlı 1 nolu tavsiye, ülkelerin risk bazlı yaklaşım uygulamaları gerektiğini anlatmaktadır (FATF, 2012, s. 10). Risk bazlı yaklaşım temel olarak, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadelede ülkelerin risk seviyelerini göz önünde bulundurarak çabalarını ve kaynaklarını uygun şekilde yönlendirmeleri anlamına gelmektedir. Gelişmekte olan finansal sistemlere sahip ülkelerde, tek tip düzenlemelerin başarıya ulaşmayabileceği ve ülkelerin düzenlemeleri uygulama konusunda isteksiz hale gelebileceği düşüncesi, risk bazlı yaklaşımın ortaya çıkmasına neden olmuştur (Başaranel ve Türkşen, 2019, s. 70).

Söz konusu tavsiyeye göre; ülkelerin, suç gelirlerinin aklanması ve terörizmin finansmanı risklerini tanımlaması, anlaması, değerlendirmesi ve bu riskleri etkili bir şekilde azaltmayı amaçlayan eylemlerde bulunması gerekmektedir. Ülkelerin, söz konusu riskleri önlemeye veya azaltmaya yönelik alınan önlemlerin kendi yetki alanlarında belirlenen risklerle orantılı olmasını sağlamak için risk bazlı yaklaşım uygulaması gerekmektedir. Ülkeler aynı zamanda, yalnızca 7 nolu tavsiyede atıfta bulunulan hedeflenen mali yaptırım yükümlülüklerinin potansiyel ihlali, uygulanmaması veya bunlardan kaçınılması anlamına gelen kitle imha silahlarının yayılmasına ilişkin riskleri de tanımlamalı, değerlendirmeli, anlamalı ve bu risklerin ortadan kaldırılmasını amaçlayan uygun önlemleri almalıdır. Ayrıca ülkeler, finansal kuruluşlar ile finansal olmayan belirli iş ve mesleklerden de bunları talep etmelidir (FATF, 2012, s. 10).

Bu kapsamda ülkelerin, kamu-özel sektör iş birliği çerçevesinde kripto varlıklar ve kripto varlık hizmet sağlayıcılara ilişkin olarak da suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı risklerini tanımlaması,

anlaması, değerlendirmesi ve bu riskleri etkili bir şekilde azaltmayı amaçlayan eylemlerde bulunması gerekmektedir. Ülkeler, kripto varlık faaliyetleri, ürünleri, hizmetleri ve hizmet sağlayıcılarının yanı sıra kripto varlık hizmet sağlayıcıları sektörüyle ilişkili bu teknolojiler hakkında bilgi sahibi kişilerin de dahil edilmesiyle koordineli bir risk değerlendirmesi yapmalıdır (FATF, 2021a, s. 38).

Risk bazlı yaklaşım kapsamında ülkeler, yüksek riskli durumlara veya kripto varlıkları içeren faaliyetlere yönelik gereklilikleri güçlendirmelidir. Ülkelerin kripto varlıklara ilişkin suç gelirlerinin aklanması ve terörizmin finansmanı risklerini değerlendirirken; eşler arası işlemler gibi belirli kripto varlık faaliyet türleri, kripto varlık hizmet sağlayıcılarının faaliyetleri ve işlemleri, kripto varlık türleri arasındaki ayrım ve bunların düzenlenmiş bir kripto varlık hizmet sağlayıcısı tarafından kontrole tabi olup olmadığı gibi konuları dikkate alması gerekmektedir. Kripto varlık hareketlerindeki artan gizlilik potansiyeli ve müşterinin tanınması sürecine ilişkin zorluklar nedeniyle, kripto varlıklar ve hizmet sağlayıcıları genel olarak daha yüksek suç gelirlerinin aklanması ve terörizmin finansmanı riskleri teşkil etmekte olup bu riskler izleme ve gelişmiş durum tespiti önlemlerinin uygulanmasını gerektirebilmektedir. Ülkeler, risk değerlendirmelerine dayanarak veya diğer politika hedefleri doğrultusunda kripto varlık faaliyetlerini veya kripto varlık hizmet sağlayıcılarını kısıtlama veya yasaklama yetkisine sahip olup bu kararın temelini oluşturan risk değerlendirme esasını periyodik olarak yeniden gözden geçirmelidir (FATF, 2021a, ss. 37-41).

Ülkeler ayrıca kripto varlık hizmet sağlayıcıları ve diğer yükümlü kuruluşlardan, kripto varlık faaliyetlerinin sağlanması veya kripto varlık ürün ve hizmetlerinin sunulmasıyla ilişkili suç gelirlerinin aklanması ve terörizmin finansmanı risklerini tanımlamasını, değerlendirmesini ve azaltmak için etkili eylemlerde bulunmasını talep etmelidir. Kripto varlık hizmet sağlayıcıları ve diğer yükümlü kuruluşlar, yeni geliştirilen ürünlerin piyasaya sürülmesinden sonra suç gelirlerinin aklanması ve terörizmin finansmanı risklerinin azaltılması daha zor olacağından, riskleri değerlendirerek ürünler piyasaya sürülmeden önce uygun risk azaltıcı önlemleri uygulamaya koymalıdır. Ülkeler de bu kuruluşları lisanslamadan önce, kullanıcıların anonim olarak işlem yapabilme yeteneğinin sınırlandırılması veya şüpheli işlemlerin tespit edilmesi için yazılım kullanılması gibi uygun risk azaltıcı önlemlerin mevcut olup olmadığını araştırmalıdır (FATF, 2021a, ss. 38-39).

Ülkeler eşler arası işlemlerle ilgili riskleri anlamalı ve azaltmalı; bu kapsamda özel sektörle iletişim kurmalı, denetleyici birimleri eğitmeli, eşler arası işlemler kapsamında sektör temsilcileriyle iş birliği yapmalıdır. Ülkeler, eşler arası işlemlerle ilgili riskleri azaltmaya yönelik olarak; suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele gereksinimlerini artırma, eşler arası aktiviteleri görünür kılan kontrol mekanizmaları oluşturma, kripto varlık hizmet sağlayıcılarını denetleme, özellikle barındırılmayan cüzdan işlemlerine odaklanan sürekli risk bazlı denetim, kripto varlık hizmet sağlayıcılarını belirli adreslere veya kaynaklara sınırlama, eşler arası işlemlere ilişkin risklere dair rehberlik ve farkındalık kampanyaları yürütme gibi çeşitli önlemler almalıdır. Zayıf suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele rejimlerinin olduğu bölgelerdeki kripto varlık hizmet sağlayıcıları ile kitlesel benimsenme potansiyeli olan ve eşler arası işlemlerde kullanılabilen istikrarlı kripto paralar gibi riskler, ülkelerin özel önlemler almalarını ve daha sıkı denetim uygulamalarını gerektirebilmektedir (FATF, 2021a, ss. 38-40).

Sonuç olarak kripto varlıklar, anonimlik özellikleri, sınırları aşan transfer yetenekleri ve hızlı işlem süreçleri gibi özellikleri nedeniyle daha yüksek terörizmin finansmanı riskleri oluşturabildiği için risk bazlı yaklaşımın bu alanda faaliyet gösterenler ile ülkeler için hayati bir araç haline gelmesi gerekmektedir. Risk bazlı yaklaşım, kripto varlıkların terörizmin finansmanında kullanımı konusunda dinamik ve değişen tehditler karşısında etkili önlemler geliştirilmesi ve kaynakların etkin kullanılması bağlamında risk seviyelerine göre öncelikli tehditlere odaklanılması açısından kritik bir stratejidir. Ayrıca, risk bazlı yaklaşımın kripto varlıklar bağlamında uygulanması, bu alanda ortaya çıkacak yenilik ve gelişmelerin önü kesilmeden ölçülü ve orantılı tedbirler alınması bakımından da önem arz etmektedir.

3.4.2. FATF'in 2 Nolu Tavsiyesi

“Suç Gelirlerinin Aklanması ve Terörizmin Finansmanı ile Mücadele Politikaları ve Koordinasyon” başlığı altında yer alan *“Ulusal iş birliği ve koordinasyon”* adlı 2 nolu tavsiyeye göre; ülkeler, suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı risklerine karşılık ulusal politikalar belirlemeli ve bunlardan sorumlu bir otorite veya koordinasyon mekanizması oluşturmalıdır. Ülkeler, politika yapıcılarının, mali istihbarat birimlerinin, kolluk kuvvetlerinin, denetleyicilerin ve diğer yetkili makamların söz konusu politikaların uygulanmasında, veri koruma, gizlilik kuralları ve diğer benzer hükümlerle uyumlu bir şekilde iş birliği yapmalarını ve

gerektiğinde koordinasyon ile bilgi alışverişinde bulunmalarını sağlamalıdır (FATF, 2012, ss. 10-11).

Bu kapsamda ülkeler, kripto varlık faaliyetleri ve kripto varlık hizmet sağlayıcıları ile ilişkili suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı risklerine karşı da ulusal politikalar belirlemeli ve ilgili kurumlar arasında çalışma grupları veya görev güçleri gibi mekanizmaları uygulayarak ulusal iş birliği ve koordinasyonu sağlamalıdır. Ulusal iş birliği ve koordinasyon, özellikle kripto varlık faaliyetlerinin hareketli ve sınır ötesi doğasından dolayı birden fazla düzenleyici kurumu etkileme şekli nedeniyle kripto varlıklar bağlamında oldukça önemlidir. Aynı zamanda, kripto varlıkların zorlukları karşısında farklı kurumların bir araya gelmesi, araştırmaların ilerlemesi ve kripto varlık ekosistemiyle ilgili çeşitli kurumlar arası araçların kullanılması açısından kritik bir rol oynamaktadır (FATF, 2021a, s. 41).

Kripto varlıkların hızla büyüyen ve evrim geçiren ekosistemi ile çeşitli benzersiz özellikleri, FATF tavsiyelerinin kripto varlıklar bağlamında uygulanmasını bir kez daha önemli kılmaktadır. Kripto varlıklar bağlamında ulusal iş birliği ve koordinasyon, etkili bir düzenleme ve denetim yaklaşımının temelini oluşturmaktadır. Ulusal iş birliği ve koordinasyon, terörizmin finansmanı riskleri karşısında bilgi paylaşımı ve hızlı tepki yeteneklerini içeren ortak stratejilerin oluşturulmasına da olanak tanımaktadır. Ulusal düzeyde bu alanda iş birliğinin sağlanması aynı zamanda kripto varlıklara ilişkin toplumsal güvenin oluşması ve kullanımın yaygınlaşmasına zemin hazırlamaktadır.

3.4.3. FATF'in 3-8 Nolu Tavsiyeleri

“Suç Gelirlerinin Aklanması ve Müsadere” başlığı altında yer alan “Kara para aklama suçu” adlı 3 nolu tavsiyeye göre; ülkeler, kara para aklamayı suç olarak saymalı ve öncül suçların kapsamını geniş tutarak tüm ciddi suçlara uygulamalıdır. Aynı başlık altında yer alan “Müsadere ve geçici tedbirler” adlı 4 nolu tavsiyeye göre; ülkeler, varlık kurtarmaya yönelik politika ve operasyonel çerçevelere sahip olmalı ve suç gelirlerini temsil eden malvarlığına ilişkin müsadere ve çeşitli geçici tedbirleri uygulamalıdır (FATF, 2012, s. 12).

Söz konusu tavsiyelerin uygulanması bağlamında, kripto varlıklar da suç gelirlerini temsil eden malvarlığı kapsamında sayılmalı ve ülkeler, suç gelirlerinin aklanmasıyla

mücadelede aldığı önlemleri kripto varlıkları da içeren suç gelirlerini kapsayacak şekilde genişletmelidir. Benzer şekilde müsadere ve geçici tedbirler kripto varlıklar için de geçerli olmalıdır. Ayrıca, terörizmin finansmanında elde edilen, kullanılan, kullanılması amaçlanan veya kullanılması için ayrılan malvarlığı kapsamına da kripto varlıklar dahil edilmelidir (FATF, 2021a, ss. 41-42).

“*Terörizmin Finansmanı ve Kitle İmha Silahlarının Yayılmasının Finansmanı*” başlığı altında yer alan “*Terörizmin finansmanı suçu*” adlı 5 nolu tavsiyeye göre; ülkeler, terörizmin finansmanını, belirli bir terör eylemi ile bağlantı kurmalarına gerek kalmaksızın suç saymalıdır. Açıklayıcı notuna göre ise terörizmin finansmanı suçu, kaynağı yasal ve yasal olmayan her türlü fon veya varlıkları kapsamalıdır. Aynı başlık altında yer alan “*Terörizm ve terörizmin finansmanı ile ilgili olarak hedeflenen mali yaptırımlar*” adlı 6 nolu tavsiyeye göre; ülkeler, terörizmin ve terörizmin finansmanının önlenmesine ilişkin Birleşmiş Milletler Güvenlik Konseyi kararlarına uymak amacıyla hedeflenen mali yaptırımları uygulamalıdır. Ülkeler, bu kapsamda belirlenen gerçek ve tüzel kişilerin fonlarını veya diğer varlıklarını dondurmaları ve bu kişiler yararına doğrudan veya dolaylı herhangi bir fon veya diğer varlığın sağlanmaması için gerekli tedbirleri almalıdır (FATF, 2012, ss. 13-43). FATF (2021a, s. 42)’e göre ülkeler, kripto varlıkları da “*fon veya diğer varlıklar*” kapsamında değerlendirerek söz konusu tavsiye gerekliliklerini uygulamalıdır. Bu kapsamda FATF, kripto varlıkların, fon veya diğer varlıklar çerçevesinde değerlendirilmesi ve önlemlerin kapsamlı şekilde kripto varlıklara da uygulanması gerektiğini açıkça ifade etmiştir.

Aynı başlık altında yer alan “*Kitle imha silahlarının yayılmasının finansmanına ilişkin hedeflenen mali yaptırımlar*” adlı 7 nolu tavsiyede ise bir önceki tavsiyeye benzer şekilde ülkelerin, kitle imha silahlarının yayılmasının finansmanına ilişkin Birleşmiş Milletler Güvenlik Konseyi kararları kapsamında hedeflenen mali yaptırımları, belirlenen gerçek ve tüzel kişilerin fonlarını veya diğer varlıklarını gecikmeksizin donduracak ve hiçbir fonun veya diğer varlığın doğrudan veya dolaylı olarak bu kişiler yararına kullanılmayacak şekilde uygulamaları gerektiği belirtilmiştir (FATF, 2012, s. 13). Aynı şekilde, fonlar veya diğer varlıklar kavramı, kripto varlıkları da içerek şekilde geniş bir kapsamda kullanılmaktadır (FATF, 2021a, s. 42).

Aynı başlık altında yer alan “*Kâr amacı gütmeyen kuruluşlar*” adlı 8 nolu tavsiyeye göre; ülkeler, FATF’in kâr amacı gütmeyen kuruluşlar tanımı dahilindeki kuruluşları

belirleyerek, fonların terör örgütlerine yönlendirilmesinin gizlenmesinde bu kuruluşların kullanılması gibi terörizmin finansmanı risklerini değerlendirmeli ve risk bazlı yaklaşım doğrultusunda uygun tedbirleri almalıdır (FATF, 2012, s. 13). Bu kapsama, kripto varlıklar aracılığıyla, kâr amacı gütmeyen kuruluşlar üzerinden yasal amaçlara yönelik fonların gizlice terör örgütlerine yönlendirildiği durumlar da dahil edilmiştir (FATF, 2021a, s. 42).

Nihayetinde FATF'in söz konusu tavsiyeleri, uluslararası alanda suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı ile mücadelede bir standart belirleme amacını taşımaktadır. Tavsiyelerin gerekliliklerinin kripto varlıkları da kapsayacak şekilde uygulanması, özellikle suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanı faaliyetlerinde kripto varlıkların potansiyel kötüye kullanımının önlenmesi açısından kritik bir öneme sahiptir. Bu yaklaşım, finansal suçlarla mücadelede uluslararası bir çerçeve oluşturarak kripto varlık sektörünü güvenilir ve şeffaf bir finansal sistemin parçası haline getirme amacını yansıtmaktadır.

3.4.4. FATF'in 10 ve 11 Nolu Tavsiyeleri

10 nolu tavsiye ve 16 nolu tavsiye içeriğindeki aşağıda belirtilecek olan özel koşullar göz önünde bulundurularak, önleyici tedbirlere ilişkin FATF'in 10 nolu tavsiye kararı ile 21 nolu tavsiye kararı arasında belirtilen gereklilikler benzer şekilde kripto varlık hizmet sağlayıcıları için de geçerli olmaktadır (FATF, 2012, s. 79). Bu kapsamda, kripto varlık hizmet sağlayıcılarının yürüttükleri kripto varlık faaliyetleri bağlamında ilgili tavsiyelere uyum sağlamaları ve gerekli önlemleri almaları sağlanmalıdır.

“Önleyici Tedbirler” başlığı ve “Müşterinin Tanınması ve Kayıtların Saklanması” alt başlığı altında yer alan “Müşterinin tanınması” adlı 10 nolu tavsiyede, finansal kuruluşların müşteri tanıma gereksinimleri anlatılmaktadır. Anonim hesaplar tutmasının açıkça yasaklanması gereken finansal kuruluşlar; iş ilişkisi tesis ederken, belirli bir eşik değeri (15.000 USD/Euro) üzerindeki veya 16 nolu tavsiyenin açıklayıcı notu kapsamındaki elektronik transferler niteliğinde arazi işlemler gerçekleştirirken, suç gelirlerinin aklanması ve terörizmin finansmanı şüphesinin bulunduğu durumda, önceden edinilen müşterilerin kimlik bilgilerinin doğruluğu ve yeterliliği konusunda şüphe duyduğunda müşterinin tanınması önlemlerini almalı ve bu gereklilik ülke mevzuatıyla da desteklenmelidir.

Müşterinin tanınması önlemleri; müşteri kimliğinin tespit edilmesi ile güvenilir ve bağımsız kaynaklardan teyit edilmesi, gerçek faydalanıcının belirlenmesi, iş ilişkisinin amacı ve niteliğinin belirlenmesi, müşteriyle kurulan iş ilişkisinin ve ilişki sürecinde gerçekleşen işlemlerin düzenli olarak gözden geçirilmesi ve durum tespiti yapılmasıdır. Finansal kuruluşlar söz konusu önlemlere uyamadıkları durumlarda, hesap açmamalı, iş ilişkisi başlatmamalı veya iş ilişkisini sonlandırmalı, şüpheli işlem bildiriminde bulunmalıdır (FATF, 2012, ss. 14-15).

Kripto varlık hizmet sağlayıcıları ile kripto varlık faaliyetlerinde bulunan diğer yükümlü kuruluşlar da kripto varlık faaliyetlerini yürütürken bu kapsamda ilgili müşterinin tanınması gereksinimlerine uymalıdır. Ancak, kripto varlık hizmet sağlayıcıları arızı bir işlem gerçekleştirirken, müşterinin tanınması önlemlerini almak zorunda olduğu belirlenen eşik değeri 1.000 USD/Euro olarak daha düşük olup ülkeler risk değerlendirmesine dayanarak mevzuatları kapsamında bu eşiği daha da düşük tutma yetkisine sahiptir (FATF, 2021a, ss. 48-49). Kripto varlıkların dijital ortamda teorik olarak sınırsız ve daha düşük maliyetle hızlı bir şekilde transfer edilebilmesi, ağ üzerinde çok fazla sayıda küçük miktarlı işlem gerçekleştirilmesine olanak tanımaktadır. Küçük miktarlı işlemlerin daha etkin bir şekilde denetim altında tutulmasını ve bu işlemlerdeki potansiyel terörizmin finansmanı gibi yasa dışı kullanım risklerinin minimize edilmesini sağlamak amacıyla kripto varlık hizmet sağlayıcıları nezdinde gerçekleşen arızı işlemler kapsamındaki müşterinin tanınması önlemleri için daha düşük bir eşik değeri belirlenmiştir.

Terör örgütlerine finansman veya destek sağlayan, terör örgütlerinin yoğun olarak faaliyet gösterdiği, yüksek düzeyde suç faaliyetlerinin gerçekleştiği tespit edilen, uluslararası yaptırımlara tabi, FATF tarafından özellikle kripto varlık hizmet sağlayıcıları için zayıf suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele rejimlerine sahip olduğu belirlenen ülkeler dahil olmak üzere yetersiz yönetim ve düzenleme sistemlerine sahip ülkeler, kripto varlıklarla ilgili faaliyetler ve kripto varlık hizmet sağlayıcıları bağlamında daha yüksek suç gelirlerinin aklanması ve terörizmin finansmanı riski ihtiva etmektedir. Ülkeye özgü risklerin yanı sıra, neredeyse tüm kripto varlıkların anonim, yüz yüze olmayan veya bilinmeyen üçüncü taraflarla işlemleri içerebilmesi nedeniyle kripto varlık ürünlerinin, hizmetlerinin ve işlemlerinin doğası gereği bu alandaki faaliyetler daha yüksek riskli olarak değerlendirilebilmektedir. Söz konusu faktörlerle ilişkili potansiyel riskleri azaltmak amacıyla kripto varlık hizmet sağlayıcılarının; müşteri, iş ilişkisinin

niteliği, fonların kaynağı ve işlemlerin nedenleri hakkında detaylı bilgilerin toplanmasını içeren ve 10 nolu tavsiyenin açıklayıcı notunda yer alan gelişmiş durum tespiti önlemlerinin yanı sıra, müşterinin İnternet Protokol (*Internet Protocol-IP*) adresinin izlenmesi ve blokzinciri analizi programlarının kullanılması gibi ek gelişmiş durum tespiti önlemleri alması gerekmektedir (FATF, 2021a, ss. 50-52). Müşterinin tanınması, temel bir önlem olmakla birlikte bazı durumlarda müşterinin veya gerçekleştirilen işlemlerin doğası, karmaşıklığı veya yüksek risk içermesi durumunda, standart müşterinin tanınması tedbirleri yetersiz kalabilmektedir. Kripto varlıkların benzersiz doğası, anonimlik ve sınır ötesi transfer yetenekleri, kripto varlık hizmet sağlayıcıları için gelişmiş durum tespiti tedbirlerini önemli kılmaktadır.

10 nolu tavsiye ile aynı ana ve alt başlık altında yer alan “*Kayıt tutma*” adlı 11 nolu tavsiyeye göre; finansal kuruluşlar, yetkili makamların bilgi taleplerine hızlı yanıtlar oluşturabilmek için müşterinin tanınması kapsamında elde edilen bilgileri ve tüm işlem kayıtlarını, iş ilişkisinin sona ermesinden veya arızı işlemlerin gerçekleşme tarihinden itibaren en az beş yıl süreyle saklamalı ve bu gereklilik ülke mevzuatıyla da desteklenmelidir (FATF, 2012, s. 15). Bu kapsamda ülkeler, kripto varlık hizmet sağlayıcıları ile kripto varlık faaliyetlerinde bulunan diğer yükümlü kuruluşlardan da işlem kayıtlarını ve tarafların kimliği, kripto varlık adresleri ve açık anahtarları, işlem tarihi, tutarı ve niteliği gibi müşterinin tanınması kapsamında elde edilen bilgileri az beş yıl boyunca saklamalarını talep etmelidir. Kayıt tutma kapsamında ilgili kripto varlığın dayandığı blokzinciri gibi dağıtılmış defter teknolojisi başlangıç olarak bir temel sağlayabilse de, kripto varlık adreslerinin kullanıcıların gerçek kimlikleri ile ilişkilendirilmesi için ek bilgiler gerekeceğinden, kayıt tutma için sadece dağıtılmış defter teknolojilerine dayanmak söz konusu tavsiye için yeterli olmamaktadır (FATF, 2021a, s. 52). Kayıt tutma, kripto varlık hizmet sağlayıcılarının müşterilerini tanıması, işlemleri izlemesi ve yetkili makamların taleplerine uygun yanıtlar oluşturması için önemli bir unsurdur. Bu süreç, güçlü bir veri yönetimi stratejisi ile desteklendiği takdirde terörizmin finansmanı gibi mali suçlarla mücadele etmede ve finansal sistemin bütünlüğünü korumada büyük katkı sağlamaktadır.

3.4.5. FATF’in 15 Nolu Tavsiyesi

“Önleyici Tedbirler” başlığı ve “*Belirli Müşteriler ve Faaliyetler İçin İlave Tedbirler*” alt başlığı altında yer alan “*Yeni teknolojiler*” adlı 15 nolu tavsiyede; ülkeler ile finansal

kuruluşların, yeni ürünlerin ve iş uygulamalarının geliştirilmesi ile yeni ve mevcut ürünler için gelişen teknolojilerin kullanımına ilişkin suç gelirlerinin aklanması ve terörizmin finansmanı risklerini belirlemeleri ve değerlendirmeleri gerektiği, ayrıca finansal kuruluşların söz konusu ürün, iş uygulaması ve teknolojilerin kullanılmaya başlanmasından önce risk değerlendirmesi yaparak uygun risk azaltıcı önlemleri almalarının önemli olduğu belirtilmektedir. Ülkeler, kripto varlıklardan kaynaklanan riskleri azaltmak amacıyla kripto varlık hizmet sağlayıcılarının; lisanslanmasını veya kayıt altına alınmasını, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele gereksinimleri doğrultusunda yeterli düzenlemeye, denetime veya izlemeye ve FATF tavsiyelerini uygulamasını sağlamak için etkili sistemlere tabi olmasını sağlamalıdır (FATF, 2012, s. 17).

15 nolu tavsiyeye ilişkin açıklayıcı not, suç gelirlerinin aklanması ve terörizmin finansmanı risklerinin değerlendirilmesi, lisanslama veya kayıt altına alma, denetim veya izleme, müşterinin tanınması, kayıt tutma, şüpheli işlem bildirimi gibi önleyici tedbirler, yaptırımlar ve diğer tedbirler, uluslararası iş birliği gibi FATF gerekliliklerinin kripto varlıklar, kripto varlık faaliyetleri ve kripto varlık hizmet sağlayıcıları bağlamında uygulanması konusunu netleştirmektedir. Açıklayıcı nota göre (FATF, 2012, ss. 78-79);

- Ülkeler kripto varlıkları, “*mülk*”, “*gelir*”, “*fon*”, “*fon veya diğer varlıklar*” ya da “*bunlara karşılık gelen değer*” olarak değerlendirmeli ve FATF tavsiyelerinin gerekliliklerini kripto varlıklar ve hizmet sağlayıcılarına uygulamalıdır.
- Ülkeler, gerçek veya tüzel kişi olabilen kripto varlık hizmet sağlayıcılarını lisanslamalı veya kayıt altına almalı ve lisanslı olmaksızın veya kayıt altına alınmaksızın kripto varlık hizmet sağlayıcısı faaliyeti yürütenleri belirleyerek yaptırımlar uygulamalıdır. Ayrıca ülkeler, suçluların kripto varlık hizmet sağlayıcısını kontrol edebilecek bir paya sahip olmasını veya yönetim pozisyonunda bulunmasını ya da kripto varlık hizmet sağlayıcısının gerçek faydalanıcısı olmasını önlemek için gerekli tedbirleri uygulamalıdır.
- Kripto varlık hizmet sağlayıcıları yetkili bir makam tarafından risk bazlı denetime veya izlenmeye tabi tutulmalı, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele gerekliliklerine uyumu denetlemesi veya izlemesi ve sağlaması gereken denetleyiciler; bilgi üretimini zorunlu kılma, mali yaptırım uygulama, gerektiği hallerde kripto varlık hizmet sağlayıcısının lisansını veya kaydını kaldırma veya kısıtlama gibi gerekli ve yeterli yetkilerle donatılmalıdır.

Denklik ilkesi üzerine kurulu söz konusu tavsiye içeriğindeki gereklilikler, kripto varlıklar bağlamında kripto varlık hizmet sağlayıcılarına, diğer yükümlü kuruluşlara olduğu gibi eşit ve aynı şekilde uygulanmalıdır. Ülkeler, kripto varlık hizmet sağlayıcılarının suç gelirlerinin aklanması ve terörizmin finansmanına karşı ilgili tüm önlemlere uymalarını sağlamalıdır (LexisNexis Risk Solutions, 2019, s. 5). Ayrıca ülkeler tarafından kripto varlık hizmet sağlayıcılarının, gizlilik tabanlı kripto varlıklar ve karıştırıcıların örnek olarak verilebileceği kripto varlığın alıcı, gönderici, sahibi veya gerçek faydalanıcısının kimliğini gizleyen teknolojiler gibi anonimliği artıran mekanizmaların kullanıldığı faaliyetlerde bulunduğu ortaya çıkan riskleri yönetmesi ve azaltması sağlanmalı, aksi takdirde bu tür faaliyetlerde bulunmasına izin verilmemelidir (FATF, 2021a, s. 55).

FATF'in 15 nolu tavsiyesi, kripto varlıkların düzenlenmesine yönelik önemli adımlar içermesiyle bu alanda en çok dikkat çeken konulardan biri haline gelmiştir. 15 nolu tavsiyenin tadil edilmesi ve açıklayıcı notunun kabul edilmesi, uzun süre boyunca ana akım finansal sistemlerden görece kopuk şekilde faaliyet gösteren kripto varlık hizmet sağlayıcılarının geleneksel finansal sistemlerle entegrasyonunda belirgin bir gelişme sağlamıştır. Söz konusu tavsiyede, kripto varlık ekosisteminin terörizmin finansmanı gibi yasa dışı amaçlarla suistimalinin önlenmesi ve daha güvenilir ve şeffaf hale getirilmesi hedefi doğrultusunda, kripto varlık hizmet sağlayıcılarının lisanslanmaları ile yeterli düzenleme ve denetim mekanizmalarına tabi olmaları gerekliliği ön plana çıkmaktadır.

Lisanslama süreci, kripto varlık hizmet sağlayıcılarının belirli suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele standartlarını karşılamalarını gerektirmekte olup lisans alan kripto varlık hizmet sağlayıcıları, bu standartlara uymak ve düzenleyici gerekliliklere uygun olarak faaliyet göstermek zorundadır. Kripto varlık hizmet sağlayıcılarının lisanslandıktan sonra düzenli aralıklarla otoriteler tarafından suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele standartlarına uyum açısından denetlenmesi de lisanslama süreci kadar önemlidir. Bu şekilde kripto varlık ekosistemindeki en önemli aktörlerden olan kripto varlık hizmet sağlayıcılarının, terörizmin finansmanı gibi yasa dışı faaliyetlerde kripto varlıkların ve gelişen teknolojilerinin ortaya çıkardığı riskler karşısında etkili önlemleri alarak finansal sistemin güvenliğine katkı yapmalarının sağlanması amaçlanmaktadır.

3.4.6. FATF'in 16 Nolu Tavsiyesi

“Önleyici Tedbirler” başlığı ve “Belirli Müşteriler ve Faaliyetler İçin İlave Tedbirler” alt başlığında yer alan “Elektronik transferler” adlı 16 nolu tavsiye ve açıklayıcı notu, terör örgütlerinin ve suçluların fon aktarımında elektronik olarak kolaylaştırılmış transfer mekanizmalarına kısıtlamasız şekilde erişmelerinin önlenmesi ve suistimallerin tespit edilmesi amacıyla geliştirilmiştir. Söz konusu tavsiyeye göre “elektronik transfer”, bir finansal kuruluştaki alıcı kişiye fon sağlamak amacıyla bir finansal kuruluş aracılığıyla gönderici adına elektronik yollarla gerçekleştirilen işlemdir (FATF, 2021a, s. 56).

16 nolu tavsiyede ülkelerin, finansal kuruluşların; elektronik transferlere ve ilgili mesajlara gerekli ve doğru gönderici ve gerekli alıcı bilgilerini dahil etmelerini ve bu bilgilerin ödeme zinciri boyunca elektronik transferlerde ve ilgili mesajlarda kalmasını, söz konusu bilgilerin eksikliğini tespit etmek amacıyla elektronik transferleri izlemelerini ve uygun önlemleri almalarını, Birleşmiş Milletler Güvenlik Konseyi kararlarında belirtilen yükümlülükler uyarınca elektronik transferlerin işleme konulması bağlamında dondurma tedbirinin alınmasını ve belirlenmiş kişi ve kuruluşlarla işlem yapılmasının yasaklanmasını sağlamaları gerektiği belirtilmektedir (FATF, 2012, ss. 17-80). İşlevsel yaklaşıma göre kripto varlık transferleri de elektronik transferlere benzediğinden, 16 nolu tavsiyeye ilişkin gereklilikler finansal kuruluşların yanı sıra kripto varlık hizmet sağlayıcıları için de geçerli olmaktadır. FATF'in elektronik transfer gerekliliklerinin kripto varlıklar bağlamında uygulanmasına Seyahat Kuralı adı verilmektedir (FATF, 2021a, s. 56). FATF'in söz konusu tavsiye ve açıklayıcı notu dahilinde oluşturduğu Seyahat Kuralı, kripto varlık endüstrisinin en önemli ve karmaşık yönlerinden biri olmuştur. Seyahat Kuralı'nın temel hedefi, bilgi paylaşımı yoluyla terörizmin finansmanı gibi yasa dışı aktivitelerin önlenmesidir (Ciphertrace, 2022, ss. 2-4).

16 nolu tavsiyenin açıklayıcı notuna göre; ülkeler, küçük miktarlı elektronik transferlerin terörizmin finansmanı açısından oluşturabileceği riskler nedeniyle eşikleri mümkün olduğunca düşük tutmalıdır. Yurt içinde de gerçekleştirilebilen elektronik transferler sınır ötesi olarak gerçekleştirildiğinde ülkeler, suç gelirlerinin aklanması ve terörizmin finansmanı şüphesi oluşmadığı sürece doğruluklarının onaylanması gerekmeksizin, alıcı ve göndericinin adı ile bunların bir hesap numarası veya benzersiz bir işlem referans numarası bilgilerinin dahil edilmesini zorunlu kılacak şekilde 1.000

USD/Euro'nun altında bir asgari eşik belirleyebileceği gibi, gerekli ve doğruluğu onaylanmış gönderici bilgilerinin dahil edilmesini de talep edebilir. Eşik değeri üzerinde gerçekleşen elektronik transferlerde ise her zaman gönderici bilgilerinin doğruluğu onaylanmalı ve bu bilgilere ek olarak göndericinin adresi, ulusal kimlik numarası, müşteri kimlik numarası, doğum tarihi ve doğum yeri bilgilerinden en az birini içermesi sağlanmalıdır (FATF, 2012, ss. 80-81). Ülkeler, sınır ötesi niteliğine dayanarak tüm kripto varlık faaliyetlerini sınır ötesi elektronik transferler olarak ele almalı ve bu kapsamda 16 nolu tavsiyenin gerekliliklerinin yerine getirilmesini sağlamalıdır (FATF, 2021a, s. 56).

Ülkeler, gönderici kripto varlık hizmet sağlayıcılarının, kripto varlık transferlerine ilişkin gerekli ve doğruluğu onaylanmış gönderici bilgilerini ve gerekli alıcı bilgilerini almalarını ve saklamalarını, söz konusu bilgileri alıcı kripto varlık hizmet sağlayıcıya veya varsa finansal kuruluşa eş zamanlı ve güvenli bir şekilde ve talep üzerine yetkili makamlara sunmalarını sağlamalıdır. Alınması ve saklanması gereken söz konusu bilgiler; gönderici ve alıcının isimleri ile işlemin gerçekleştirilmesinde hesap kullanıldıysa hesap numaraları veya kripto varlığın cüzdan adresleri, göndericinin adresi veya ulusal kimlik numarası veya doğum tarihi ve yeri ya da bunlardan en az birini içeren bir kayda atıfta bulunan müşteri kimlik numarası veyahut bunların kripto varlıklar bağlamındaki eş değer bilgileridir (FATF, 2012, s. 79; FATF, 2021a, ss. 56-58).

Geleneksel sistemlerde olmayan benzersiz teknolojik özellikleri nedeniyle kripto varlıklar bağlamında 16 nolu tavsiyede belirtilen diğer ilgili gerekliliklerin aynı temelde uygulanması gerekmele birlikte, bazı gereklilikler kripto varlık hizmet sağlayıcıları ve diğer yükümlü kuruluşların kripto varlık faaliyetleri kapsamında değişiklik göstermektedir (FATF, 2021a, ss. 55-65). İtibari para veya kripto varlık cinsinden olabilen bir elektronik transfer veya bir kripto varlık hizmet sağlayıcı ile diğer bir yükümlü kuruluş arasındaki kripto varlık transferi kapsamında kripto varlık hizmet sağlayıcıları için 16 nolu tavsiyenin tüm gereklilikleri geçerli olmakla birlikte, bir kripto varlık hizmet sağlayıcısı ile yükümlü olmayan bir kuruluş (barındırılmayan cüzdan sağlayıcı platform) arasında kripto varlık transferi oluşturulurken gerekli bilgilerin alınması gerekmekte ancak alıcı yükümlü olmayan kuruluşa gerekli bilgilerin sunulması beklenmemektedir (FATF, 2021a, ss. 61-65). Dolayısıyla kripto varlık hizmet sağlayıcıların topladığı ve sakladığı kişisel olarak tanımlanabilir bilgilerin alıcı tarafça her zaman görüntülenmesine gerek yoktur. Ayrıca söz konusu bilgiler, yetkisiz erişim ve kişisel olarak tanımlanabilir bilgi sızıntıları gibi kişisel

verilerin korunmasına yönelik riskler nedeniyle açık metin olarak da saklanmamalıdır (Ciphertrace, 2022, s. 4). Bu tür elektronik transferlere ülkeler tarafından ilave kısıtlamalar veya kontrol mekanizmaları getirilmesi mümkündür (FATF, 2021a, s. 65).

Kripto varlık hizmet sağlayıcıları tarafından Seyahat Kuralı uygulanırken karşı karşıya kalınan stratejik ve operasyonel risklerin azaltılması için; kripto varlıklar bağlamında suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele gereksinimlerinin aşamalı olarak uygulanması ve bu sırada riskleri azaltmak için alternatif önlemlere de sahip olunması, blokzinciri analiz araçlarının kullanılması, karşı taraf kripto varlık hizmet sağlayıcılarının tanımlanması, kayıtlı olup olmadıklarının belirlenmesi ve durum tespiti gerçekleştirilmesi, siber güvenlik, gizlilik ve veri koruma konularının ele alınması gerekmektedir (Ciphertrace, 2022, s. 4). Ancak bu noktada, kripto varlık sektöründe halihazırda tartışılan Seyahat Kuralı'nın uygulanmasındaki teknik zorluklara da dikkat çekmek faydalı olacaktır. Elektronik transferlerde gönderici ve alıcı bilgilerinin toplanması ve finansal kuruluşlar arasındaki paylaşımı uzun süredir devam eden bir süreç olmasına karşılık, kripto varlık hizmet sağlayıcıları için nispeten yeni bir gereklilik olup benzersiz bir iletişim ağı gerektirmektedir. Kripto varlık hizmet sağlayıcılarının 16 nolu tavsiye gereklilikleri karşısında verilerin toplanması ve paylaşılmasına yönelik bir çözüm geliştirmesi beklenmektedir. FATF, verilerin paylaşılmasına yönelik belirli bir yöntem veya teknoloji belirlemeyerek çözümü ülkelerin ve kripto varlık hizmet sağlayıcıların takdirine bırakmaktadır. Dolayısıyla şifreli veri aktarımına yönelik sektörde kullanılan mevcut protokol ve ağlar çeşitlilik göstermekte ve uyum sorunları ortaya çıkabilmektedir. Bu durumun, kripto varlık hizmet sağlayıcıları tarafından Seyahat Kuralı'nın etkin bir şekilde uygulanmasını zorlaştırarak kripto varlıkların terörizmin finansmanı bağlamında oluşturduğu riskleri artırabileceği değerlendirilmektedir.

3.4.7. FATF'in 19-21 Nolu Tavsiyeleri

“Önleyici Tedbirler” başlığı ve “Güven, Kontroller ve Finansal Gruplar” alt başlığı altında yer alan “Yüksek riskli ülkeler” adlı 19 nolu tavsiyeye göre; ülkeler, finansal kuruluşların, FATF tarafından talep edilen ülkeler de dahil olmak üzere yüksek riskli ülkelerdeki gerçek ve tüzel kişilerle kuracakları iş ilişkilerinde ve gerçekleştirecekleri işlemlerde etkili ve risklerle orantılı olacak şekilde gelişmiş durum tespiti önlemlerini uygulamalarını sağlamalıdır (FATF, 2012, s. 19). Sınır ötesi doğası göz önüne alındığında,

bu durum özellikle kripto varlık faaliyetleri için önemlidir. Dolayısıyla ülkeler, kripto varlık hizmet sağlayıcılarının da yüksek riskli ülkelerdeki kişilerle gerçekleştirecekleri kripto varlık işlemlerinde gelişmiş durum tespiti önlemlerini aldıklarından emin olmalıdır (FATF, 2021a, s. 66). FATF, kripto varlık hizmet sağlayıcılarının yüksek riskli ülkelerle gerçekleştirdikleri kripto varlık işlemlerinde ve tesis ettikleri iş ilişkilerinde, risk bazlı yaklaşım çerçevesinde artırılmış dikkat ve önlemleri hayata geçirmeleri için çağrıda bulunarak, uluslararası düzeyde terörizmin finansmanı dahil olmak üzere mali suçlarla mücadeleyle yönelik daha kapsamlı bir çabayı teşvik etmektedir.

“Önleyici Tedbirler” başlığı altında yer alan “Şüpheli işlem bildirimi” adlı 20 nolu tavsiyeye göre; fonların suç geliri olduğundan veya terörizmin finansmanı ile bağlantısı olduğundan şüphelenen ya da şüphelenmek için makul gerekçeleri olan finansal bir kuruluş, söz konusu şüphelerini kanun gereği hemen mali istihbarat birimine bildirmelidir (FATF, 2012, s. 19). Şüpheli işlem bildirimleri, yasayla doğrudan zorunlu bir yükümlülük haline getirilmeli ve işlemin gerçekleşip gerçekleşmediği (işlem girişimleri dahil) veya işlemin tutarına bakılmaksızın bildirim yapılması sağlanmalıdır (FATF, 2012, s. 89). Ayrıca, aynı başlık altında yer alan “Bilgi sızdırma ve gizlilik” adlı 21 nolu tavsiyeye göre; şüpheli işlem bildiriminde bulunan finansal kuruluşların yöneticileri, memurları ve çalışanları, kanun yoluyla, bilgi ifşasına ilişkin herhangi bir kısıtlamanın ihlali nedeniyle cezai ve hukuki sorumluluktan korunmalı ve şüpheli işlem bildirimlerini ifşa etmeleri yasaklanmalıdır (FATF, 2012, s. 19).

Bu kapsamda ülkeler, kripto varlık hizmet sağlayıcılarının ve kripto varlık faaliyetleri yürüten diğer yükümlü kuruluşların da mali istihbarat birimine şüpheli işlem bildiriminde bulunmalarını zorunlu hale getirmeli ve uygun şekilde şüpheli işlem bildiriminde bulunulmasının bilgi ifşası kapsamında değerlendirilmemesini ve şüpheli işlem bildirimlerinin ifşa edilmemesini sağlamalıdır. Ülkeler, söz konusu kuruluşların kripto varlık faaliyetiyle ilişkilendirilebilecek belirli göstergeleri bildirmelerini sağlamak amacıyla halihazırda var olan bildirim mekanizmalarında veya formlarında güncellemeler yapmayı da değerlendirmelidir. Kripto varlık faaliyetiyle ilişkilendirilebilecek belirli göstergeler arasında; cihaz tanımlayıcıları, ilişkili cüzdan adresleri, işlem Hash değerleri, zaman damgaları ve IP adresleri bulunmaktadır. Ülkeler aynı zamanda kripto varlık hizmet sağlayıcılarından, şüpheli işlemlerin etkin bir şekilde incelenmesini sağlamak ve yaptırımların uygulanması gerekliliklerini karşılamak amacıyla blokzinciri analiz araçları

gibi mekanizmaları kullanmalarını talep edebilmelidir (FATF, 2021a, ss. 66-67). Kripto varlıklara ilişkin şüpheli işlem bildirimlerinin, yetkili makamların kripto varlık ekosistemini daha iyi anlamalarını sağlayarak analiz ve değerlendirme ile soruşturma ve kovuşturma çabalarına büyük katkısı olduğu bilinmektedir. Şüpheli işlem bildirimleri, terörizmin finansmanı ile mücadelede önemli bir istihbarat kaynağı olarak hizmet etmektedir.

Ayrıca FATF, ulusal otoritelerin kripto varlıkların yasa dışı kullanım durumlarını belirlemelerine yardımcı olmak amacıyla ilgili öncül suçlar, suç gelirlerinin aklanması ve terörizmin finansmanı faaliyetlerine işaret edebilecek kripto varlıklar bağlamında kırmızı bayrak göstergelerini yayınlamıştır. Söz konusu kırmızı bayrak göstergeleri, şüpheli işlem bildiriminde bulunma yükümlülüğü olan kuruluşların kripto varlıklar bağlamında şüpheli işlemleri tespit ederek bildirmelerine ve mali istihbarat birimlerinin söz konusu şüpheli işlem bildirimlerini analiz etmelerine yardımcı olacak belirli işlem veya durum kalıplarını ifade etmektedir (FATF, 2020a). Kripto varlıkların doğal özelliklerine ve zayıf noktalarına odaklanan kırmızı bayrak göstergeleri altı kategoriye ayrılmıştır: Gerçekleştirilen işlemlerin tutarı ve sıklığı hakkında makul bir açıklama olmaması, düzensiz ve olağandışı işlem kalıpları, eşler arası değişim platformları, karıştırıcı (mixer) hizmetleri, gizlilik tabanlı kripto varlıklar gibi anonimliği artıran teknolojik özelliklerin kullanılması, olağandışı davranışlar sergileyen alıcı veya gönderici profilleri, fon veya servetin kaynağının şüpheli olması, kripto varlıklara yönelik alınan önlemlerin yetersiz olduğu coğrafi risk taşıyan ülkelerle ilişkilendirilen durumlar kripto varlıkların yasa dışı faaliyetlerde kullanılıyor olabileceğine ilişkin şüphe uyandırması bakımından bir çerçeve oluşturmaktadır (Schwarz vd., 2021, s. 14). Bu göstergeler, kripto varlıkların kullanıldığı terörizmin finansmanı gibi yasa dışı faaliyetlerin tespiti ve önlenmesi kapsamında kamu sektörü ile özel sektöre pratik bir araç sağlanması amacıyla oluşturulmuştur. Bu nedenle, göstergelerin başlı başına ele alınmaması ve daha geniş bir bağlam ile bütünlük içinde değerlendirilmesi önemlidir.

3.4.8. FATF'in 24 ve 25 Nolu Tavsiyeleri

“Tüzel Kişilerde ve Yasal Oluşumlarda Şeffaflık ve Gerçek Faydalanıcılık” başlığı altında yer alan “Tüzel kişilerde şeffaflık ve gerçek faydalanıcılık” adlı 24 nolu tavsiyeye göre; ülkeler, tüzel kişilerin suç gelirlerinin aklanması ve terörizmin finansmanı amacıyla kötüye kullanılmasını engellemek amacıyla önlemler almalı ve tüzel kişilerin gerçek faydalanıcı ve kontrolüne ilişkin olarak yetkili makamların gerçek faydalanıcı kayıtları veya

alternatif bir mekanizma yoluyla hızlı şekilde erişebileceği yeterli, doğru ve güncel bilgilerin bulundurulmasını sağlamalıdır (FATF, 2012, s. 22). Aynı başlıkta yer alan “*Yasal oluşumlarda şeffaflık ve gerçek faydalanıcılık*” adlı 25 nolu tavsiyeye göre ise ülkeler, benzer şekilde yasal oluşumların suç gelirlerinin aklanması ve terörizmin finansmanı amacıyla kötüye kullanılmasını engellemek amacıyla önlemler almalıdır. Trust kurucusunun, kendi malvarlığında bulunan bir hak üzerindeki yetkilerini kayyım ve faydalanıcılar arasında paylaşması ile kurulan trust şeklindeki yasal oluşumlarda söz konusu taraflar hakkındaki bilgiler dahil olmak üzere yetkili makamların gerektiğinde ulaşabileceği nitelikte yeterli, doğru ve güncel bilgilerin bulundurulması da sağlanmalıdır (MASAK, 2021, s. 6; FATF, 2012, s. 22). Ayrıca her iki tavsiyeye göre ülkeler, FATF tavsiyeleri ile getirilen müşterinin tanınması yükümlülüklerine tabi olan finansal kuruluşlar ile finansal olmayan belirli iş ve mesleklerin gerçek faydalanıcı ve kontrol bilgilerine erişimini kolaylaştıracak önlemler de almalıdır (FATF, 2012, s. 22).

Bu kapsamda ülkeler, finansal kuruluşlar ile finansal olmayan belirli iş ve mesleklerde olduğu gibi kripto varlık hizmet sağlayıcılarının da kötüye kullanımını önlemek için gerekli tedbirleri almalı ve müşterinin tanınması yükümlülüklerine tabi kripto varlık hizmet sağlayıcılarının gerçek faydalanıcı ve kontrol bilgilerine erişimini kolaylaştırmalıdır (FATF, 2021b, ss. 67-68). Gizlilik tabanlı kripto varlıklar ve karıştırıcı (mixer) hizmetleri gibi kripto varlıklarda gizliliği artırıcı teknolojiler, kripto varlık işlemlerinde gerçek faydalanıcının belirlenmesini zorlaştırmaktadır. Gerçek faydalanıcının belirlenmesindeki zorluklar, kripto varlıkların terörizmin finansmanı dahil olmak üzere yasa dışı faaliyetlerde kullanılma riskini artırmaktadır. Bu nedenle, özellikle anonimliği artırıcı teknolojilerin kullanıldığı kripto varlık işlemlerinde gerçek faydalanıcının belirlenmesi konusu büyük önem taşımaktadır. Kripto varlık hizmet sağlayıcılarının bu teknolojilerin kullanımının getirdiği riskleri yöneterek gerçek faydalanıcı ve kontrol bilgilerine ulaşmasının sağlanması, kripto varlıkların terörizmin finansmanı amacıyla kullanımının önlenmesinde kritik bir konu olarak karşımıza çıkmaktadır.

3.4.9. FATF’in 26 ve 27 Nolu Tavsiyeleri

“*Yetkili Makamların Yetki ve Sorumlulukları ve Diğer Kurumsal Tedbirler*” başlığındaki “*Düzenleme ve Denetim*” alt başlığında yer alan “*Finansal kuruluşların düzenlenmesi ve denetlenmesi*” adlı 26 nolu tavsiyeye göre; ülkeler, suç gelirlerinin

aklanması ve terörizmin finansmanı ile mücadelede, konsolide grup denetimi de dahil olmak üzere finansal kuruluşları yeterli düzenleme, denetim veya izlemeye tabi tutmalı ve suç gelirlerinin aklanması ve terörizmin finansmanı riskleri doğrultusunda FATF tavsiyelerini etkili bir şekilde uygulamalarını sağlamalıdır. Ayrıca temel prensiplere tabi olmayan diğer finansal kuruluşların da suç gelirlerinin aklanması ve terörizmin finansmanı riski göz önüne alınarak ya da asgari şekilde para/değer transferi veya para/döviz değişim hizmeti sağladıklarında lisanslanması veya kayıt altına alınması sağlanmalıdır (FATF, 2012, s. 23). Aynı başlık ve alt başlık altında yer alan “*Denetleyicilerin yetkileri*” adlı 27 nolu tavsiyede ise söz konusu denetimleri gerçekleştirecek denetleyicilerin teftiş yapma yetkisi ile birlikte yeterli yetkiye sahip olmaları gerektiği anlatılmaktadır. Denetleyiciler her türlü bilgiyi finansal kuruluşlardan alma ve gerekliliklere uyulmadığı takdirde lisans iptali gibi birçok disiplin ve mali yaptırım uygulama yetkisine sahip olmalıdır (FATF, 2012, s. 23).

Söz konusu tavsiyeler çerçevesinde ülkeler, kripto varlık hizmet sağlayıcılarını ve kripto varlık faaliyetlerinde bulunan diğer yükümlü kuruluşları da suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadelede kapsamında yeterli düzenleme, denetim veya izlemeye tabi tutmalı ve bunların FATF gerekliliklerine uymalarını sağlamalıdır. Benzer şekilde, kripto varlık hizmet sağlayıcıları bir öz denetim kuruluşu yerine yetkili makamlar tarafından risk bazlı yaklaşımla denetlenmeli veya izlenmeli ve denetleyicilerin yeterli yetkilere sahip olması sağlanmalıdır (FATF, 2021a, s. 47). Kripto varlık hizmet sağlayıcılarının finansal kuruluşlar olarak değerlendirilmesi, ülkelerin kendi düzenleyici yaklaşımlarına ve hukuki çerçevelerine bağlı olarak değişmektedir. Ancak ulusal düzeyde finansal kuruluş olarak değerlendirilmese dahi kripto varlık hizmet sağlayıcılarının finansal faaliyetleri çerçevesinde finansal kuruluş seviyesinde düzenleme ve denetime tabi tutulması, kripto varlıkların terörizmin finansmanı gibi yasa dışı faaliyetlerde kullanımının önüne geçilmesinde hayati öneme sahiptir.

3.4.10. FATF’in 29-31 Nolu Tavsiyeleri

“*Yetkili Makamların Yetki ve Sorumlulukları ve Diğer Kurumsal Tedbirler*” başlığındaki “*Operasyonel Hususlar ve Yasa Uygulama*” alt başlığında yer alan “*Mali istihbarat birimleri*” adlı 29 nolu tavsiyeye göre ülkeler; öncül suçlar, suç gelirlerinin aklanması, terörizmin finansmanı ile alakalı şüpheli işlem bildirimlerinin ve diğer bilgilerin alınmasında, analizinde, analiz sonuçlarının ilgili yerlere paylaşılmasında ulusal düzeyde bir

merkez olarak mali istihbarat birimi tesis etmeli ve mali istihbarat biriminin bildirim yapanlardan ek bilgi almasını ve işlevlerini düzgün bir şekilde yerine getirmesi amacıyla ihtiyaç duyduğu bilgilere zamanında erişmesini sağlamalıdır (FATF, 2012, s. 24). Bu kapsamda kripto varlık hizmet sağlayıcıları ve kripto varlık faaliyetlerinde bulunan diğer yükümlü kuruluşlar da mali istihbarat birimine şüpheli işlem bildirimlerini sunmalı ve ek bilgi sağlamalıdır (FATF, 2021a, s. 68). Mali istihbarat birimleri, şüpheli kripto varlık işlemlerinin izlenmesi ve analiz edilmesi yoluyla terörizmin finansmanı dahil olmak üzere yasa dışı finansal faaliyetlerin tespit edilmesi ve raporlanması konusunda finansal sistemin güvenliğinin sağlanmasında kilit bir role sahiptir.

Bir önceki tavsiye ile aynı ana ve alt başlıkta yer alan “*Yasa uygulama ve soruşturma makamlarının sorumlulukları*” adlı 30 nolu tavsiyede; suç gelirlerinin aklanması ve terörizmin finansmanı soruşturmalarından da sorumlu olmaları gereken belirlenmiş yasa uygulama makamlarının, ülke dışında gerçekleşen ilgili öncül suçlar da dahil olmak üzere, en azından gelir getirici önemli suçlarla ilgili tüm vakalarda öncül suçlar, suç gelirlerinin aklanması ve terörizmin finansmanı kapsamında proaktif bir şekilde paralel mali soruşturma yürütmeleri gerektiği anlatılmaktadır. Söz konusu tavsiyeye göre ülkeler, suça konu malvarlığının tespit ve takip edilmesi ile dondurulması ve el konulması işlemlerinden yetkili makamların sorumlu olmasını ve gerektiği hallerde diğer ülkelerdeki yetkili makamlarla iş birliğine dayalı soruşturmaların yapılmasını sağlamalıdır (FATF, 2012, ss. 24-25). Tavsiye içerisinde geçen gelir ve malvarlığı terimleri gibi fon veya değere atıfta bulunan tüm terimler kripto varlıkları da içerecek şekilde değerlendirmelidir. Bu kapsamda ülkelerin, mevzuatları çerçevesinde kripto varlıkların nasıl tasniflendiğine bakmaksızın yetkili makamların müsadereye konu veya suç geliri olduğu şüphesi bulunan kripto varlıklarla ilgili malvarlığının tespit ve takip edilmesi ile dondurulması ve el konulması işlemlerini yürütmelerini sağlaması gerekmektedir (FATF, 2021a, ss. 41-42). Bu bağlamda, kripto varlıkların mevcut düzenlemelerle uyumlu bir şekilde ele alınması ve bu varlıkların potansiyel yasa dışı faaliyetlere karışmasının önlenmesi, finansal istikrarın korunması ve ulusal güvenliğin güçlendirilmesi açısından büyük bir rol oynamaktadır.

Önceki tavsiyeler ile aynı başlıklar altında yer alan “*Yasa uygulama ve soruşturma makamlarının yetkileri*” adlı 31 nolu tavsiyeye göre; yetkili makamlar, ilgili öncül suçlar, suç gelirlerinin aklanması ve terörizmin finansmanı soruşturmalarını yürütürken finansal kuruluşlar, finansal olmayan belirli iş ve meslekler ile diğer gerçek ve tüzel kişiler tarafından

tutulan kayıtların temini için zorunlu tedbirleri kullanma yetkileri ile birlikte gerekli tüm bilgi ve belgelere erişim sağlamalıdır. Ülkeler, gerçek veya tüzel kişilerin hesapları olup olmadığını ve bu hesapları kontrol edip etmediklerini tespit edecek mekanizmalar kullanmalı, yetkili makamların da uygun soruşturma teknikleri ve sahibine önceden bildirimde bulunmaksızın malvarlıklarını tespit edecek mekanizmaları kullanmasını sağlamalıdır (FATF, 2012, s. 25). Bu kapsamda ülkeler ve yetkili makamlar, zorunlu tedbirleri kullanma yetkileri ile birlikte kripto varlık hizmet sağlayıcıları tarafından tutulan kayıtlar dahil olmak üzere tüm bilgi ve belgelere erişim elde edebilmeli, gerçek veya tüzel kişilerin kripto varlık cüzdanları bulunup bulunmadığı ile kontrol edip etmediklerini belirlemek için ve sahibine bildirimde bulunmaksızın kripto varlıkları tespit etmek için etkili mekanizmalara sahip olmalıdır (FATF, 2021a, s. 68). Söz konusu tavsiyenin uygulanması, kripto varlıklarla ilişkili suç gelirlerinin aklanması ve terörizmin finansmanı riskleri ile mücadele eden ülkeler ve yetkili makamlar için soruşturmaların etkinliği açısından büyük önem teşkil etmektedir.

3.4.11. FATF'in 34 ve 35 Nolu Tavsiyeleri

“Yetkili Makamların Yetki ve Sorumlulukları ve Diğer Kurumsal Tedbirler” başlığı altında yer alan “Rehberlik ve geri bildirim” adlı 34 nolu tavsiyeye göre; yetkili makamlar, suç gelirlerinin aklanması ve terörizmin finansmanı tedbirlerinin uygulanmasında ve şüpheli işlemlerin tespit edilmesinde ve bildirilmesinde finansal kuruluşlara ve finansal olmayan belirli iş ve mesleklere yardımcı olacak rehberler oluşturmalı ve geri bildirim sağlamalıdır (FATF, 2012, s. 26). Bu bağlamda, suç gelirlerinin aklanması ve terörizmin finansmanı tedbirlerinin uygulanmasında ve kripto varlıklarla ilişkili şüpheli işlemlerin belirlenmesi ile bildirilmesi kapsamında kripto varlık hizmet sağlayıcılarına da yardımcı olacak rehberler hazırlanmalıdır (FATF, 2021a, s. 68). Söz konusu tavsiye, ülkelerin kripto varlıklarla ilişkilendirilen riskleri tanımlamaları açısından önemlidir. Kripto varlık hizmet sağlayıcılarına yönelik hazırlanan rehberler, etkili bir yol haritası sunarak kripto varlık sektörünün düzenlenmesine ve kripto varlıkların yasa dışı faaliyetlerde kullanılmasının önlenmesine katkı sağlamaktadır.

Önceki tavsiye ile aynı başlık altında yer alan “Yaptırımlar” adlı 35 nolu tavsiyeye göre ise; ülkeler, 6 nolu tavsiye ve 8 nolu tavsiye ile 23 nolu tavsiye arasındaki suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele yükümlülüklerine uymayan

finansal kuruluşlar ve finansal olmayan belirli iş ve meslekler ile bunların müdür ve üst düzey yöneticileri dahil olmak üzere gerçek ve tüzel kişilerle ilgili olarak orantılı, caydırıcı ve etkili olan cezai, hukuki veya idari yaptırımların olmasını sağlamalıdır (FATF, 2012, s. 26). Bu kapsamda ülkeler, benzer şekilde suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele yükümlülüklerine uymayan kripto varlık hizmet sağlayıcıları ve kripto varlık faaliyeti yürüten diğer yükümlü kuruluşlar ile bunların müdür ve üst düzey yöneticilerine yönelik de yaptırım mekanizmalarına sahip olmalıdır (FATF, 2021a, s. 43). Yaptırım mekanizmaları, kripto varlık hizmet sağlayıcılarını ve diğer ilgili kuruluşları gerekli suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele tedbirlerini almaya zorlamak ve sektörde düzenlemenin sağlanması, güvenilirlik ve sorumlulukların artırılması amacıyla uygulanmaktadır.

3.4.12. FATF'in 37-40 Nolu Tavsiyeleri

“Uluslararası İş Birliği” başlığı altında yer alan “Karşılıklı adli yardımlaşma” adlı 37 nolu tavsiyede, ilgili öncül suçlar, suç gelirlerinin aklanması ve terörizmin finansmanı soruşturmaları, kovuşturmaları ve ilgili diğer süreçlerde uluslararası iş birliğinin ve karşılıklı adli yardımlaşmanın önemine vurgu yapılmaktadır. Aynı başlık altında yer alan “Karşılıklı adli yardımlaşma: Dondurma ve müsadere” adlı 38 nolu tavsiye, ülkelerin; ilgili öncül suçlar, suç gelirlerinin aklanması, terörizmin finansmanı suçlarına konu gelir, malvarlığı değeri veya karşılık gelen değerler ile araçların araştırılması, tespit edilmesi, dondurulması, el konulması ve müsadere edilmesi konusunda yabancı ülkelerin taleplerine yardımcı olmak için gerekli araçlara sahip olması gerektiğini anlatmaktadır. “Suçluların iadesi” adlı 39 nolu tavsiyede ise suç gelirlerinin aklanması ve terörizmin finansmanı faaliyetlerinde bulunan yasa dışı aktörler bağlamında iade taleplerinin yerine getirilmesi hususu ifade edilmektedir. Son FATF tavsiyesi olan “Diğer uluslararası iş birliği şekilleri” adlı 40 nolu tavsiyede ülkelerin; ilgili öncül suçlar, suç gelirlerinin aklanması ve terörizmin finansmanı kapsamında, kendiliğinden ve talep üzerine, yasal bir zemine oturarak, mümkün olan en geniş ölçüde uluslararası iş birliğinin sağlanmasında gerekli ve etkili araçlara sahip olması gerektiğinin altı çizilmektedir (FATF, 2012, ss. 27-30).

Kripto varlıkların sınır ötesi doğası dolayısıyla, ülkeler tarafından 37 nolu tavsiye ile 40 nolu tavsiye arasında belirtilen önlemlerin alınması büyük önem teşkil etmektedir. 15 nolu tavsiyenin açıklayıcı notunda, kripto varlıklarla ilişkili suç gelirlerinin aklanması ve

bağlı öncül suç ile terörizmin finansmanı risklerinin azaltılmasında söz konusu tavsiyelerin uygulanmasının ve uluslararası iş birliğinin önemine özellikle vurgu yapılmaktadır (FATF, 2012, s. 79). Bu kapsamda ülkeler, ilgili öncül suçlar, suç gelirlerinin aklanması ve terörizmin finansmanı suçlarına konu gelir, malvarlığı değeri veya karşılık gelen değerler ile araçlar kapsamına kripto varlıkları ve kripto varlık hizmet sağlayıcılarının faaliyetleri ile ilişkili diğer varlıkları dahil ederek, yabancı ülkelerin bunların tespit edilmesi, müsadere edilmesi, el konulması ve dondurulması taleplerine yardımcı olmalı ve kripto varlıklar ile ilişkilendirilen yasa dışı faaliyetlerde bulunan yasa dışı aktörler için etkili iade yardımı sağlamalıdır (FATF, 2021a, s. 69).

Ülkeler, kripto varlıklar bağlamında suç gelirlerinin aklanması ve terörizmin finansmanı ile ilgili olarak, 37 nolu tavsiye ile 40 nolu tavsiye arasındaki gereklilikler kapsamında uluslararası iş birliğini hızlı, yapıcı ve etkili bir şekilde sağlamalı, kripto varlık hizmet sağlayıcılarının denetleyicileri ve yabancı meslektaşlarıyla hızlı ve yapıcı bir şekilde bilgi alışverişinde bulunmalıdır (FATF, 2012, s. 79). Mali istihbarat birimlerinin, özellikle sınır ötesi kripto varlık ve kripto varlık hizmet sağlayıcı faaliyetleri bağlamında ilgili şüpheli işlem bildirimleri hakkında yabancı muhataplarıyla iş birliği yapması ve ilgili bilgileri paylaşması önem taşımaktadır. Ayrıca bir ülkede lisanslanan veya kayıt altına alınan kripto varlık hizmet sağlayıcılarının ürün veya hizmetlerini başka bir ülkedeki müşterilere sunduğu durumlarda da uluslararası iş birliği konusu ön plana çıkmaktadır (FATF, 2021a, s. 69). Kripto varlık faaliyetlerinin birden fazla ülkeyi ilgilendirmesi düzenleyicilerin ve yetkililerin iş birliği yapma ihtiyacını doğurmaktadır.

Ülkelerin, kendi yetki alanlarında faaliyet gösteren kripto varlık hizmet sağlayıcılarının üzerindeki gözetimi ve kontrolü, kripto varlıklar bağlamında diğer ülkelerle adli yardımlaşma ve uluslararası iş birliğini daha etkili şekilde yerine getirmelerini sağlamaktadır. Ancak birçok ülkenin, kripto varlıklarla ilgili suç gelirlerinin aklanması ve terörizmin finansmanı faaliyetlerinin suç olarak tanınmasına imkân veren yasal çerçevesi ile düzenleme ve soruşturma kapasitesinin bulunmaması veya yeterli olmaması, uluslararası iş birliğinin etkin şekilde sağlanmasının önünde engeller oluşturmaktadır (FATF, 2021a, s. 69). Bazı ülkeler, kripto varlıklar kapsamında FATF tavsiyelerine uygun bir yaklaşım benimserken diğer birçok ülkenin bunu henüz gerçekleştirmediği olması, kripto varlıklarla ilgili küresel düzenleyici yaklaşımın koordinasyon eksikliğine işaret etmektedir. Küresel ölçekte kripto varlıklara ilişkin düzenlemeler halihazırda bütünlükten uzak şekilde çeşitlilik

göstermektedir (Keatinge vd., 2018, s. 46). Bu durum, uluslararası toplumun terörizmin finansmanı risklerinden korunması bağlamında mücadele çabalarını zorlaştırmaktadır. Bu nedenle ülkeler, terörizmin finansmanı faaliyetlerinde kripto varlıkların kullanım risklerini anlamalı, bu konuda ilgili FATF tavsiyelerini sıkı bir şekilde uygulamalı, FATF standartlarını dikkate alarak kapsamlı bir yasal çerçeve ile düzenleme ve soruşturma mekanizmaları oluşturmaları ve küresel düzeyde iş birliğine aktif olarak katılmalıdır (Wang ve Zhu, 2021, s. 2338).

3.5. Üçüncü Bölüme İlişkin Değerlendirme

Başlangıçta suç gelirlerinin aklanmasıyla mücadeleye yönelik politikalar geliştirmek üzere hükümetler arası bir organ olarak OECD rehberliğinde kurulan FATF, 11 Eylül saldırılarının akabinde terörizmin finansmanı ile mücadeleyi de misyonuna eklemiştir. FATF'in yetki alanı, suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanının önlenmesine yönelik politikalar geliştirmek ve uluslararası iş birliğini teşvik etmektir. FATF söz konusu mali suçlarla mücadele kapsamında; yöntem ve trendleri takip etmekte, farkındalığı artırmak için raporlar yayınlamakta, tavsiyeler dahil olmak üzere küresel ölçekte standartlar belirlemekte, ülkeleri standartların uygulanması yönünden değerlendirmekte, standartlara tam olarak uymadığını belirlediği ülkeleri gri ve kara listelerde duyurmaktadır. Bu bölümde, tezin ana sorusunun bir parçası olarak, konu bağlamında “*FATF tavsiyeleri nasıl değerlendirilmektedir?*” sorusu ile bu doğrultuda belirlenen “*Kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi kapsamında FATF ne gibi çalışmalar yürütmektedir?*” ve “*Kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi kapsamında ilgili FATF tavsiyeleri nelerdir ve nasıl değerlendirilmektedir?*” şeklindeki tezin alt sorularına yanıtlar aranmıştır.

Bu bağlamda FATF'in, kullanımının yaygınlaşmaya başlamasından bu yana kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanı kapsamında oluşturduğu potansiyel riskler nedeniyle yürüttüğü çalışmalar sonucunda yayımladığı raporlar ve rehberler incelenmiştir. Ayrıca FATF'in, kripto varlıkların yasa dışı amaçlarla kullanımını önlemek ve uluslararası finansal sistemi güvenli kılmak amacıyla bu alandaki gelişmeleri sürekli olarak takip ettiğine ve standartlarını kripto varlıkların potansiyel riskleriyle başa çıkacak etkili bir düzenleyici çerçeve oluşturmak adına güncellediğine dikkat çekilmiştir. FATF'in 15 nolu tavsiyeyi revize ederek kripto varlık hizmet sağlayıcılarının lisanslanması

veya kayıt altına alınması hususunda getirdiği yeni gereksinimler, 15 nolu tavsiyeye ilişkin açıklayıcı notu kabul etmesi, sözlüğe bu alanda yeni tanımlar eklemesi ve Seyahat Kuralı'nın, FATF'in kripto varlıklar konusunda en dikkat çeken düzenleyici adımları olduğu değerlendirilmiştir. Dolayısıyla, kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi kapsamında FATF'in ne gibi çalışmalar yürüttüğü ortaya konmuştur.

Diğer taraftan, 15 nolu tavsiyenin yanı sıra FATF'in birçok tavsiyesinin kripto varlıkları ve bu alanda faaliyet gösteren ürün ve hizmet sağlayıcılarını yakından ilgilendirdiği anlaşılmış ve bu kapsamda toplam 28 tavsiye ve gereklilikleri incelenmiştir. Ülkelerin, 10 nolu tavsiye ve 16 nolu tavsiyede olduğu gibi kripto varlıklarla ilgili özel koşulları dikkate alarak, FATF tavsiyelerindeki tüm fon veya değer temelli terimlerin kripto varlıkları da içerdiğini anlaması ve ilgili tavsiyelerde belirtilen önlemlerin kripto varlıklar ve kripto varlık hizmet sağlayıcıları bağlamında da uygulaması gerektiği açıklanmıştır. Dolayısıyla, kripto varlıkların terörizmin finansmanında kullanılmasının önlenmesi kapsamında ilgili FATF tavsiyelerinin neler olduğu ve nasıl değerlendirildiği ortaya konmuştur.

Kripto varlık sektöründe faaliyet gösterenler tarafından, kripto varlıkların temel olarak kullanıcıların kimliği açık edilmeden ödeme yapılabilecek şekilde tasarlandığı belirtilerek, FATF tavsiyelerinin kripto varlık hizmet sağlayıcılarına getirdiği müşterinin tanınması gibi önlemler dolayısıyla kripto varlık işlemlerinin eşler arası transferlere imkân tanıyan platformlara kayabileceği endişesi gündeme getirilmiştir. Ayrıca yine sektördeki kişiler tarafından kripto varlıklar bağlamında FATF tavsiyelerinin uygulanması, ek uyumluluk ve teknolojik gereksinimler nedeniyle işletme maliyetlerinin yükseldiği ve dolayısıyla rekabet gücünün etkilenecek yeni girişimcilerin sektöre katılmasının zorlaştığı iddiasıyla eleştirilmektedir (Eisermann, 2020, ss. 34-35). Ancak FATF tavsiyelerinin, kripto varlık ekosistemindeki aktörlerin düzenlenmiş bir çerçevede faaliyet göstermelerini sağlayarak finansal sistemin güvenliğine yaptığı katkı karşısında, söz konusu eleştirilere odaklanarak kripto varlık sektörünün düzenlenmemesi gerektiğini savunmak mantıksız olacaktır. Kripto varlıkların uygun düzenlemeler olmadan, terör örgütlerinin finansal faaliyetleri için güvenli bir alan haline gelme riski bulunmaktadır (FATF, 2023k). FATF tavsiyelerinin uygulanması, bu riski azaltarak kripto varlık sektörünü daha güvenilir ve şeffaf hale getirmekte ve yatırımcılar ile kullanıcıların korunmasına katkı sağlayarak sektörün uzun vadeli sürdürülebilirliği ile güvenliği açısından önem taşımaktadır.

Diğer taraftan, eşler arası kripto varlık işlemlerinin, yalnızca FATF tavsiyelerinin gerektirdiği düzenlemelerin hayata geçirilmesiyle değil, kripto varlıkların daha geniş bir kabul düzeyine ulaşmasıyla da hızla artacağı endişesi hâkimdir. Eşler arası kripto varlık işlemlerindeki artışın, kripto varlıkların potansiyel olarak yasa dışı amaçlarla kullanılma riskini artırabileceği ve düzenleyiciler için yeni zorluklar doğurabileceği değerlendirilmektedir (Coelho vd., 2021, s. 2). Bu durumun, kripto varlık hizmet sağlayıcılarına olan talebi azaltarak otoritelerin terörizmin finansmanı gibi risklere karşı düzenleme ve kontrol yeteneklerini zayıflatabileceğini söylemek mümkündür. Eşler arası kripto varlık işlemlerinin düzenlenmesi, geleneksel finansal sistemlerden farklı dinamikleri içerdiği ve hızla evrildiği sebebiyle zorluklarla karşı karşıya kalmaktadır.

Kripto varlık ekosisteminin dinamik yapısı ve sürekli gelişen teknolojik yenilikler, düzenleyicilerin zamanında ve sürekli müdahalelerde bulunmasını gerektirmektedir. FATF'in 15 nolu tavsiyesinin 2018 yılında revize edilmesi ve açıklayıcı notunun 2019 yılında kabul edilmesi, 2009 yılında ortaya çıkmasının ardından dünya çapında kullanımı hızla artan kripto varlıkların terörizmin finansmanı gibi yasa dışı faaliyetler kapsamında oluşturduğu riskler karşısında gecikmiş bir yanıt olarak değerlendirilmektedir. Bu durum, kripto varlık hizmet sağlayıcılarının da düzenlenmiş bir çerçevede finansal sistemlerle güvenli ve şeffaf bir şekilde entegre edilmesini geciktirmiştir. Bu gecikme, aynı zamanda FATF'in de kabul ettiği üzere, kripto varlıkların terörizmin finansmanı ve diğer yasa dışı faaliyetlerde kullanılmasının önlenmesine yönelik küresel çapta tutarlı ve uyumlu düzenlemelerin eksikliğine yol açmıştır.

Ayrıca söz konusu gecikme karşılıklı değerlendirme süreçlerini de etkilemiştir. Bu bölümde değinildiği üzere FATF, yürüttüğü karşılıklı değerlendirme sürecinde kullandığı metodolojiyi 2023 yılının haziran ayında güncellemiş olup 3 ve 4 nolu etkililik kriterlerini kripto varlık hizmet sağlayıcılarını kapsayacak şekilde revize etmiştir. Ancak güncellemeye kadar FATF metodolojisindeki etkililik kriterlerinin kripto varlık hizmet sağlayıcılarını içermemesi, kripto varlıklar konusunda takip sürecinde olan ülkeler için etkililik değerlendirmeleri yapılamamasına ve teknik uyum ile sınırlı olacak şekilde değerlendirmeler yapılmasına sebep olmuştur. Nitekim, son olarak 2023 yılının şubat ayında güncellenen dördüncü tur karşılıklı değerlendirme prosedürlerinin kripto varlıklar konusunu içermediği görülmektedir (FATF, 2023). Ancak güncellenen metodoloji kullanılarak gerçekleştirilecek ve 2025 yılında başlayacak olan beşinci tur karşılıklı

değerlendirmelerinde, kripto varlıklar konusunun daha detaylı inceleneceği ve ülkelerin kripto varlık hizmet sağlayıcıları kapsamında daha detaylı bir değerlendirme sürecinden geçeceği anlaşılmaktadır.

FATF tavsiyeleri, genellikle küresel standartları belirleyen ve ülkelerin kendi yasalarını oluştururken bu standartlara uymalarını teşvik eden önemli bir referans noktasıdır. Ancak, bu standartların uygulanması ve etkinliği ülkeler arasında farklılık göstermektedir. Her ülkenin finansal sistemleri, hukuki çerçeveleri ve denetim kapasiteleri birbirinden farklı olduğu için FATF tavsiyeleri her ülkede eşit şekilde uygulanamamaktadır. Bu durum, ülkeler arasındaki farklılıkların ve çeşitli zorlukların dikkate alınması ile daha genel ve uygulanabilir standartlar oluşturulmasını gerektirmektedir. Bu bağlamda FATF, kripto varlıklara ilişkin düzenleyici bir çerçeve çizdiği 15 nolu tavsiyesinde ve genel olarak tavsiyelerini kripto varlıklar bağlamında değerlendirirken belirli konulara özellikle dikkat çekmektedir. FATF, kripto varlıkların terörizmin finansmanı gibi mali suçlarla ilişkili faaliyetlerde kullanılmasının önlenmesi kapsamında kripto varlık hizmet sağlayıcılarının lisanslanması veya kayıt altına alınması ihtiyacına sıklıkla vurgu yapmaktadır. Kripto varlık hizmet sağlayıcılarının faaliyetleri çerçevesinde müşterinin tanınması, kayıt tutma, şüpheli işlem bildirimi gibi önleyici tedbirler ile Seyahat Kuralı'nı uygulamasının sağlanması ve bu kapsamda düzenli olarak denetlenmesi gerektiğinin de altı çizilmektedir. Kripto varlıklar alanındaki risklerin değerlendirilmesinde ve tavsiyelerde belirtilen önlemlerin alınmasında risk bazlı yaklaşımın benimsenmesi gerekliliğine de sürekli şekilde dikkat çekilmektedir. Ayrıca, kripto varlıkların benzersiz özelliklerinden kaynaklanan ve düzenlenmesi ile yasa dışı faaliyetlerde kullanılmasının önlenmesi konusunda ortaya çıkan zorluklar karşısında ulusal ve uluslararası düzeyde iş birliğinin sağlanmasının kritik rolü özellikle vurgulanmaktadır.

FATF tarafından geliştirilen tavsiyeler, kripto varlık alanının düzenlenmesi için önemli bir çerçeve sunmakla birlikte, tek başına yeterli değildir. Bu bağlamda, FATF tavsiyelerinin etkin bir şekilde uygulamaya konulması, uluslararası düzeyde kripto varlıkların terörizmin finansmanı başta olmak üzere yasa dışı faaliyetlerde kullanılmasının önlenmesinde büyük önem arz etmektedir. Ülkeler, FATF tavsiyelerini kendi yasal ve düzenleyici çerçevelerine entegre ederek, kripto varlıkların özgün özellikleri ile dinamikleri doğrultusunda etkin düzenleme ve denetim mekanizmaları oluşturmaları olmalıdır. Kripto varlıkların sınır ötesi doğası ve hızla gelişen teknolojik yapısı, ulusal ve uluslararası düzeyde

koordinasyon ve iş birliđi ile birlikte tutarlı, uyumlu, esnek ve dinamik düzenleyici yaklaşımları zorunlu kılmaktadır. FATF tavsiyelerinin ulusal düzenleyici çerçevelere entegrasyonu ve uygulamadaki etkinliđi, kripto varlıkların yasa dışı faaliyetlerde kullanılmasının önlenmesi ve sektörün yenilikçi potansiyelinin sürdürülebilir büyümesi açısından hayati önem taşımaktadır.



SONUÇ VE ÖNERİLER

Esas olarak kripto varlıkların terörizmin finansmanı bağlamında kullanımının araştırıldığı tezde, öncelikle kripto varlıkların ortaya çıkışı ve gelişimi incelenmiştir. Kripto varlıkların ortaya çıkışının ve para birimi olarak işlevselliğinin daha iyi kavranabilmesi için ilk olarak para kavramı ve tarihine ilişkin kısa bir anlatı sunulmaya çalışılmıştır. Trampa sisteminin yetersiz ve karmaşık hale gelmesiyle kullanılmaya başlanan paranın, tarihteki gelişmelere paralel şekilde sürekli olarak dönüşümlere uğradığı, ancak ortaya çıktığı her formda belirli işlev ve özelliklere haiz olduğu görülmektedir. Paraya atfedilen değere ilişkin güven unsuruna bağlı şekilde genel kabul görmesi, paranın en temel özelliği olarak kabul edilmektedir. Paranın tarihi, ekonomik, toplumsal, kültürel ve teknolojik gelişmelerle birlikte, içsel değeri veya karşılığı olan paradan olmayana doğru ve fiziki formdan dijital forma doğru bir ilerlemenin olduğunu göstermektedir. Günümüzde, itibari para birimlerinin yanı sıra dijital para birimleri de yaygın olarak kullanılmakta olup kripto para birimlerinin kullanımı ise her geçen gün yaygınlaşmaktadır.

Tezde, konu kapsamındaki ilgili kavramlar arasındaki farkları açıklamaya yönelik bir çerçeve oluşturulmaya da çalışılmıştır. Mübadele aracı, fiyat birimi ve değer saklama aracı olarak üç temel fonksiyonu ile tanımlanan para kavramı ile bu üç fonksiyondan ziyade, değer saklama aracı olarak tanımlanan varlık kavramı arasındaki farka bakmak önemlidir. Varlık, genel olarak ekonomik değere sahip olan herhangi bir şeyi ifade ederek paradan daha geniş bir anlam taşımakta ve para birimi olarak işlev görmeyen değer temsillerini de kapsamaktadır. Bununla birlikte, değerın dijital bir temsili olarak dijital olarak oluşturulan ve işlem gören dijital para türleri arasında da farklar bulunmaktadır. İtibari para cinsinden ifade edilen elektronik para ve kendi hesap birimine sahip olan sanal para farklı dijital para türleri olup kripto para, dönüştürülebilir ve merkezi olmayan sanal para türü olarak sanal para içerisindeki ayrı bir alt kategoriyi ifade etmektedir. Dolayısıyla dijital para birimleri, sanal para birimlerini ve sanal para birimleri de kripto para birimlerini kapsamaktadır. Benzer şekilde, varlık kavramının para kavramını da içerdiği göz önüne alındığında, dijital varlıkların sanal varlıkları ve sanal varlıkların kripto varlıkları kapsayan daha geniş terimler olduğu sonucuna varılmaktadır.

Kripto para birimlerini de içerisine alan kripto varlıklar, kriptografiye ve dağıtık defter teknolojisine dayanmaktadır. Dağıtık defter teknolojisinin en yaygın kullanım örneği olan

blokzincirinin teknik altyapısının incelenmesi, kripto varlıkların işleyiş mantığının anlaşılması için önem arz etmektedir. Satoshi Nakamoto'nun 2008 yılında yayınladığı Bitcoin kripto para birimini tanıtan yazısı, blokzinciri teknolojisinin de başlangıcı olarak kabul edilmektedir. Kripto varlıkların ve blokzincirinin ortaya çıkışı ve gelişim süreci gizlilik ve güvenlik odaklı çalışmalardan etkilenmiş olup merkezi otoritelere duyulan güveni azaltan küresel ekonomik krizlerin de bu süreçleri hızlandırdığı değerlendirilmektedir. Blokzinciri, ağdaki katılımcılar arasında anlaşmaya varmak için bir mutabakat algoritması kullanarak verilerin doğrulanmasına ve bloklara kaydedilmesine olanak tanıyan, her bloğun birbirine kriptografik olarak bağlı olduğu sıralı ve değiştirilemez dijital bir kayıt defteridir. Blokzinciri, güvensiz taraflar arasında teknolojiye duyulan güven sayesinde şeffaflık içerisinde doğrudan işlem gerçekleştirilmesini sağlayarak merkezi otoritelere ve üçüncü taraflara olan ihtiyacı ortadan kaldırmıştır. Merkezi olmayan dağıtık yapı, eşler arası aktarım, şeffaflık, kayıtların geri çevrilemezliği ve programlanabilirlik ilkeleri sayesinde güvenli bir veri yönetimi ile veri transferi sağlayan blokzinciri, kripto varlıkların yanı sıra finans, sağlık ve tedarik zinciri gibi çeşitli sektörlerde potansiyel kullanım alanları sunan değerli bir teknoloji olarak kabul edilmektedir.

Blokzinciri teknolojisinin sağladığı teknik altyapıya duyulan güven, kripto varlıkların kullanımının yaygınlaşmasını ve bu bağlamda yeni iş modelleri ile aktör kategorilerinin oluşmasını sağlamıştır. Blokzinciri; kripto varlıkların oluşturulmasını ve işlemlerinin doğrulanarak gerçekleştirilmesini sağlayan madencilik sürecini, doğrudan eşler arası değer aktarımına imkân tanıyan DeFi sistemini, önceden belirlenmiş kurallara göre otomatik olarak yürütülen akıllı sözleşmeler ile bunun bir uzantısı olarak katılımcılar arasında demokratik yönetim sağlayan DAO'ları, projelerin finansmanını sağlamak amacıyla Token satışları olarak gerçekleştirilen ICO'ları içeren bir dizi yenilik ve uygulamayı mümkün kılarak finansal ve teknolojik alanda çeşitli gelişmelere kapı aralamıştır.

Çeşitli açılardan farklı şekillerde sınıflandırılabilen kripto varlıklar; Bitcoin'i ve gizlilik tabanlı kripto varlıkların da aralarında bulunduğu Altcoin'leri içeren Coin'ler ile Ödeme, Fayda, Menkul Kıymet Token'ları ve NFT'leri içeren Token'lar şeklinde, kendi bağımsız blokzinciri gibi bir dağıtık defter teknolojisini kullanıp kullanmadıklarına dayalı olarak sınıflandırılabilir. Kripto varlıklar ve temelinde yatan teknoloji, bahsedildiği üzere birçok potansiyel fayda sunarken, aynı zamanda çeşitli risk ve zorlukları da beraberinde getirmektedir. Coin'ler ve özellikle Ödeme Token'ları ile NFT'ler, benzersiz

özellikleri dolayısıyla yasa dışı faaliyetler kapsamında yasa dışı aktörlere birtakım olanaklar sunmaktadır. Ayrıca, kripto varlık teknolojilerinden ileri gelen yukarıda bahsedilen söz konusu gelişmeler de kripto varlıkların yasa dışı amaçlarla kullanımı konusunda kötü niyetli aktörlere yeni fırsatlar yaratmıştır.

Tezin odak konusu olan kripto varlıkların terörizmin finansmanında kullanılması konusuna geçilmeden önce son olarak, terör, terörizm, terörizmin finansmanı kavramları açıklanmış olup terörizmin finansman faaliyetlerinin kapsamı ve internet ile ilişkisi incelenmiştir. Terörizmin finansmanı; ihtiyaç duyulan fon veya değerlerin yasal veya yasa dışı yollarla elde edilmesi ve toplanması faaliyetleri, toplanan fon veya değerlerin ihtiyaç duyulan yer ile kişilere aktarılması faaliyetleri, fon veya değerlerin ihtiyaç duyulana dek güvenli şekilde saklanması faaliyetleri olmak üzere üç temel aşamayı içermektedir. Terörizmin finansmanı kapsamında uzun süredir önemli rol oynayan internet ve siber araçların yanı sıra kripto varlıklar, söz konusu üç aşamada da kullanım potansiyeli dolayısıyla terörizmin finansmanı ile mücadelede önemli bir risk unsuru haline gelmiş ve ulusal ile uluslararası otoriteler için pek çok zorluğu beraberinde getirmiştir.

Kripto varlıklar, giderek çeşitlenen ve karmaşık hale gelen terörizmin finansman araç ve yöntemlerinden biri olarak terör örgütlerinin ihtiyaç ve imkânları doğrultusunda kullanılmaya başlanmıştır. Tezin ana sorularından biri olan, kripto varlıkların terörizmin finansmanında neden kullanıldığı araştırılırken, kullanım tercihini etkileyebilecek kolaylaştırıcı ve zorlaştırıcı faktörler incelenmiştir. Kripto varlıkların doğasından kaynaklanan anonimlik veya sözde anonimlik, merkezi olmayan dağıtık yapı, küresel erişim ile sınır ötesi ve hızlı transfer özellikleri ile birlikte, kripto varlıklar konusunda henüz çoğu ülkede veya küresel düzeyde tutarlı bir düzenleyici çerçeve bulunmaması dolayısıyla mevcut düzenleme eksikliklerinin, kripto varlıkların terörizmin finansmanında kullanılmasını kolaylaştıran faktörler olduğu ortaya konmuştur.

Terör örgütleri, olası tespit ve müdahalelerden kaçınmak için finansman faaliyetlerini genellikle gizlilik içerisinde yürütmeye çalışmaktadır. Kripto varlıklar sözde anonim niteliğinde olsa dahi, işlem kayıtları şeffaf bir şekilde blokzinciri üzerinde yer alırken kullanıcıların gerçek kimlikleri doğrudan ağda yer almadığı dolayısıyla bir dereceye kadar anonim özellik ihtiva etmektedir. Ayrıca kripto varlık kullanıcılarının ve işlemlerinin gizliliğini artırmayı amaçlayan gizlilik tabanlı kripto varlıklar ve karıştırıcı (mixer)

hizmetleri başta olmak üzere çeşitli yöntem ve teknolojiler de bulunmaktadır. Dolayısıyla kripto varlıkların, diğer birçok finansal enstrümanda bulunmayan anonimlik özelliklerinin, terör örgütlerini kripto varlıkları kullanmaya teşvik edebilecek en önemli faktörlerden biri olduğu değerlendirilmektedir. Kripto varlıkların bir diğer eşsiz özelliği olan merkezi olmayan dağıtık yapısı, işlemlerin merkezi bir yapı olmaksızın doğrudan eşler arasında gerçekleşmesini sağlayarak, herhangi bir merkezi otorite tarafından tespit edilerek engellenmeyi ve işlemlerinin geri alınmasını istemeyen terör örgütleri için güvenli ve güvenilir bir değer aktarım mekanizması sunmaktadır. Ayrıca, kripto varlıkların bulunduğu ağa erişimi olan herkes tarafından hızlı, küresel çapta ve sınırlamalara tabi olmaksızın işlem gerçekleştirme imkânı, terör örgütlerinin fonlarını hızlı, etkili ve genellikle daha düşük maliyetlerle transfer etmelerine olanak sağlamaktadır. Kripto varlıkların doğasından kaynaklanan benzersiz özelliklerinin yanı sıra kripto varlıklara ilişkin dünya genelindeki yetersiz düzenleme ve denetim mekanizmaları, bu boşluklardan faydalanmak isteyen terör örgütlerine kripto varlıkları finansman faaliyetlerinde kullanma fırsatı yaratmaktadır.

Diğer taraftan, terör örgütlerinin kripto varlıkları etkin şekilde yönetmelerinin bir örgütsel öğrenim süreci gerektirmesi, kripto varlıkların gerekli teknik beceriye sahip örgüt içerisindeki kişilerin yönetimine emanet edilmesi durumunda örgüt liderlerinin bu varlıklar üzerindeki kontrolünün zayıflama olasılığı, kripto varlıklara erişim ve etkin şekilde yönetim için gereken teknik altyapının terör örgütleri ile faaliyet gösterdikleri bölgelerde yetersiz olması gibi terör örgütlerinin içsel ve faaliyet gösterdiği bölgelerin dinamiklerinden kaynaklan faktörlerin, kripto varlıkların terörizmin finansmanı kapsamında kullanılmasını zorlaştırdığı değerlendirilmiştir. Ayrıca, terör örgütlerinin faaliyet gösterdiği bölgelerde kripto varlık kullanımının sınırlı olması dolayısıyla kripto varlıkların likide dönüştürülmesinde yaşanan sorunlar, kripto varlıkların değerinde yaşanan büyük dalgalanmalar dolayısıyla terör örgütlerinin spekülatif risklere maruz kalması gibi kripto varlıkların henüz geniş çapta benimsenmemesinden kaynaklanan faktörler de terör örgütleri için bu konuda zorluk oluşturmaktadır. Ancak gelecekte, kripto varlıkların dünya çapında daha fazla kabul görmesi ve kullanımının yaygınlaşmasıyla birlikte, terör örgütleri açısından öne sürülen zorluk faktörlerinin hafifleyebileceği ve kripto varlıkların finansman faaliyetlerinde kullanımının artabileceği değerlendirilmektedir.

Tezin ana sorularından diğeri olan, kripto varlıkların terörizmin finansmanında nasıl kullanıldığı araştırılırken, terör örgütlerinin ihtiyaçlarına ve bu ihtiyaçları karşılamak için

mevcut teknolojinin özellikleri ile söz konusu teknolojiyi kullanma yeteneklerine bağlı olarak kripto varlıkların, terörizmin finansmanının üç aşamasında da çeşitli yöntemlerle kullanılabildiği görülmüştür. Bu bağlamda, terörizmin finansmanında kripto varlıkların; bağışlar, Dark Web içerisinde suç geliri ve malzeme temini, suç gelirlerinin aklanması, NFT'ler, DeFi ve akıllı sözleşmeler, madencilik, ICO, karıştırıcı (mixer) hizmetleri, gizlilik tabanlı kripto varlıklar yoluyla ve daha birçok yöntemle kullanılma potansiyeli bulunduğu ortaya konmuştur. Tezin ana sorularından bir diğeri olan, kripto varlıkların terörizmin finansmanında ne derecede kullanıldığı araştırılırken, kripto varlıkların söz konusu yöntemlerin de aralarında bulunduğu çeşitli şekillerde terörizmin finansmanı kapsamında kullanıldığına ilişkin belirlenen ve 2012 ila 2023 yılları arasında gerçekleşen birçok örnek olay incelenmiştir. Örnek olaylar üzerinden yapılan analiz neticesinde; terör örgütlerinin kripto varlıkları henüz erken bir dönemde fark ederek finansman faaliyetlerinde kullanma girişimlerinde bulundukları, kripto varlıkların terörizmin finansmanı bağlamında en fazla internet üzerinden bağış toplama faaliyetleri ile Dark Web içerisinde silah ve mühimmat gibi malzemelerin temininde kullanıldığı, terör örgütlerinin kripto varlıklar ile doğrudan eşler arasında işlemler gerçekleştirebildikleri gibi kripto varlık hizmet sağlayıcıları aracılığıyla da kripto varlıkları yönetebildikleri, terör örgütlerinin ve terör örgütlerine finansman sağlayan grupların veya bireylerin ideolojik ve pratik sebeplerle kripto varlık kullanımına yöneldikleri, son yıllarda terörizmin finansmanında kripto varlık kullanımının arttığı ve kripto varlıklar cinsinden daha yüksek miktarlarda finansman sağlanabildiği, terör örgütlerinin kripto varlıkları kullanarak yeni finansman tipolojileri oluşturma çabasında oldukları ve karıştırıcı (mixer) teknolojileri ile gizlilik tabanlı kripto varlıklar gibi kripto varlıklarda anonimliği artıran yöntemlere daha fazla başvurdukları anlaşılmıştır. Ayrıca, aşırı sağcı grupların da kripto varlıkları kullandıklarına ilişkin çeşitli örnek olaylar incelenmiş olup bu kapsamda terör örgütlerine kıyasla finansman faaliyetlerinde kripto varlıkları daha yoğun ve sofistike şekilde kullandıkları görülmüştür. Aşırı sağcı grupların finansman faaliyetlerinde kripto varlıkları daha etkin bir şekilde kullanmaları, daha gelişmiş teknik becerilere sahip ve teknolojik yenilikleri benimseme konusunda daha açık olmaları veya faaliyet gösterdikleri ortamın teknolojik altyapısının gelişmişliği ile açıklanabilmektedir.

Terörizmin finansmanı kapsamında kripto varlıkların, henüz geleneksel finansal araçların yerini almadığı, ancak geleneksel yöntemlerin yanı sıra kullanıldığı görülmektedir. Kripto varlıkların terörizmin finansmanında kullanılması şu an için erken bir aşamada

olmakla birlikte, mevcut kanıtlar ile yapılan analiz sonucunda, kripto varlıkların terörizmin finansmanında kullanım eğiliminin arttığı ve kullanım yöntemlerinin giderek karmaşık hale geldiği anlaşılmıştır. Bu durum, söz konusu alanın gelecekte daha fazla önem kazanabileceğine işaret etmekte olup uluslararası iş birliği ve etkili düzenleme önlemlerinin gerekliliğini ön plana çıkarmaktadır. Dolayısıyla tezde, terörizmin finansmanı ile mücadelede uluslararası alanda iş birliğini sağlayan ve geniş ölçüde kabul gören standartlar oluşturan FATF'in konu ile yakından ilgili tavsiye kararları incelenmiştir. Tezin ana sorularından sonuncusu, kripto varlıkların terörizmin finansmanında kullanılması bağlamında FATF tavsiyelerinin nasıl değerlendirildiği incelenmeden önce, FATF'in tarihçesi, uluslararası alandaki konumu, görev ve yetki alanları açıklanmıştır.

Mali suçlarla mücadelede küresel iş birliğinin sağlanması amacıyla 1989 yılında kurulan FATF, suç gelirlerinin aklanması, terörizmin finansmanı ve kitle imha silahlarının yayılmasının finansmanının önlenmesi amacıyla politikalar geliştiren hükûmetler arası bir kuruluştur. FATF bu alanlarda farkındalığı artırmak amacıyla düzenli olarak raporlar ve rehberler yayınlamakta, küresel ölçekte standartlar belirlemekte, ülkeleri standartlara uyum açısından değerlendirmekte, takip etmekte ve listelemektedir. Etki alanı oldukça geniş bir düzeye ulaşan FATF'in oluşturduğu standartlar, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadelede küresel ölçekte etkili ve önemli bir çerçeve sağlamaktadır. FATF, ülkelerin kendi sistemlerine uyarlayacakları temel önlemleri belirleyerek bu konuda uluslararası bir standart oluşturmak adına 40 tavsiyeyi geliştirilmiştir. FATF tavsiyeleri, tavsiyelerin kendisini, açıklayıcı notlarını ve sözlükteki tanımları içermekte olup FATF standartlarının temel bileşeni olarak kabul edilmektedir.

FATF, etkinliğini sürdürmek adına yeni gelişmeler ve tehditler karşısında standartlarını düzenli olarak gözden geçirmekte ve gerektiğinde güncellemektedir. Dünya üzerinde büyük ölçüde etkili düzenlemelere tabi olmayan kripto varlıklarla da yakından ilgilenen FATF, kripto varlıkların finansal sistemle olan etkileşiminin anlaşılmasına ve uygun düzenlemelerin oluşturulmasına katkıda bulunmak amacıyla önemli fakat gecikmiş adımlar atmıştır. FATF, kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanı açısından oluşturduğu potansiyel risklere odaklanarak çeşitli raporlar ile rehberler yayınlamış ve yeni teknolojilere ilişkin 15 nolu tavsiyeyi 2018 yılında revize etmiştir. Bu kapsamda ülkeler temel olarak, kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanı risklerinin farkında olmalı, kripto varlık hizmet sağlayıcılarını

lisanslamalı veya kayıt altına almalı, kripto varlık sektörünü denetlemeli, kripto varlık hizmet sağlayıcılarının müşterinin tanınması, kayıt tutma, şüpheli işlem bildirimi gibi önleyici tedbirler ile Seyahat Kuralı'nı uygulamasını sağlamalıdır. 15 nolu tavsiyenin yanı sıra, tezde de incelendiği üzere FATF'in ilgili birçok tavsiyesinin ve metodolojisindeki iki etkililik kriterinin kripto varlıkları ve hizmet sağlayıcılarını yakından ilgilendirdiği görülmüş olup FATF tavsiyelerindeki gerekliliklerin, kripto varlıkların terörizmin finansmanı gibi yasa dışı amaçlarla kullanılmasıyla mücadelede kritik bir rol oynadığı anlaşılmıştır. Ancak, FATF tavsiyelerinin uygulanmasındaki tutarsızlıklar, teknolojik yeniliklere adaptasyon zorlukları ve küresel uygulanabilirlik sorunları göz önünde bulundurulduğunda, mevcut çerçevenin sürekli geliştirilmesi ve güncellenmesi gerektiği de ortaya çıkmaktadır.

FATF tavsiyelerinin uygulanmasında dünya genelinde tutarsızlıklar ve zorluklar yaşanmaktadır. Her ülkenin hukuki ve düzenleyici çerçevesinin farklı olması, FATF tavsiyelerinin tam olarak uygulanmasını güçleştirmekte ve uluslararası düzeyde standartların tutarlı ve eşit bir şekilde uygulanmasını engellemektedir. Teknolojik yeniliklere adaptasyon konusunda da FATF zorluklarla karşı karşıya kalmaktadır. Kripto varlıkların ve blokzinciri teknolojilerinin sürekli evrimi, mevcut düzenlemelerin hızla eskimesine yol açmakta ve yeni teknolojik gelişmelerin takibini zorunlu kılmaktadır. FATF tavsiyelerinin küresel düzeyde uygulanabilirliği de ciddi bir zorluk oluşturmaktadır. Kripto varlıkların sınır ötesi karakteri, ülkeler arasında kapsamlı bir koordinasyon ve iş birliği süreci gerektirmektedir; ancak uluslararası iş birliği her zaman yeterli düzeyde sağlanamamakta ve bazı ülkelerin düzenleyici çerçeveleri diğerlerine göre geride kalmaktadır. Bu durum terör örgütlerine, farklı ülkelerdeki düzenleme boşluklarından faydalanarak finansman faaliyetlerini yeterli düzenleme ve denetim mekanizmalarına sahip olmayan ülkelerde yürütme imkânı tanımaktadır.

Kripto varlıklara ilişkin düzenlemeler halihazırda dünya genelinde büyük ölçüde farklılık göstermekte olup kripto varlıkların sınır ötesi doğası göz önüne alındığında, zayıf düzenleme ve denetim rejimlerine sahip ülkeler sebebiyle kripto varlıklar terörizmin finansmanı kapsamında risk oluşturmaya devam etmektedir. FATF tarafından geliştirilen tavsiyeler bu konuda önemli bir düzenleyici çerçeve sağlamakta olup tek başına yeterli değildir. Terörizmin finansmanı kapsamında kullanımı artarak devam eden kripto varlıklar konusunda ülkelerin, FATF tavsiyelerini kendi sistemlerine ve ulusal düzeydeki risklerine uyarlayarak ve kripto varlıkların özgün özellikleri ile dinamikleri doğrultusunda etkin

düzenleme ve denetim mekanizmaları oluşturmaları ve uluslararası iş birliği ile bilgi paylaşımına aktif şekilde katılım sağlamaları gerekmektedir. Kripto varlık kullanımının tamamen yasaklanmasının, faaliyetlerin yer altına kaymasına ve takibi ile denetiminin zorlaşmasına sebep olacağı; tutarlı ve yeterli düzenlemelerin oluşturulmamasının, kripto varlıkların terörizmin finansmanında kullanım riskini artıracığı değerlendirilmektedir. Dolayısıyla, birçok potansiyel faydası bulunan kripto varlıklar ile teknolojik uygulamalarının gelişiminin önü kesilmeden, riskler ile orantılı olarak ve sektör ile iş birliği içerisinde yapılacak uygun düzenlemeler, bu alanın terörizmin finansmanı gibi yasa dışı faaliyetler kapsamında suistimalinin önüne geçilerek güvenliğinin sağlanması ve uzun vadeli sürdürülebilirliği açısından büyük önem taşımaktadır.



KAYNAKÇA

- 5237 Sayılı Türk Ceza Kanunu § Dördüncü Kısım: Millete ve Devlete Karşı Suçlar ve Son Hükümler, İkinci Bölüm: Adliye Karşı Suçlar (2004).
- 5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun § Birinci Bölüm: Amaç ve Tanımlar (2006).
- 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, (2013).
- Akbulut, Y. (2018). Veri Çözümleme Teknikleri. İçinde A. Şimşek (Ed.), Sosyal Bilimlerde Araştırma Yöntemleri (ss. 162-195). Anadolu Üniversitesi.
- Al-Munthir, T. (t.y.). Bitcoin wa Sadaqat Al--Jihad. Erişim Tarihi: 17 Aralık 2023, <https://krypt3ia.files.wordpress.com/2014/07/btccedit-21.pdf>.
- Argentino, M.-A., Davis, J., & Hamming, T. R. (2023). Financing Violent Extremism: An Examination of Malignated Creativity in the Use of Financial Technologies (ss. 1-38). ICSR.
- Aristoteles. (1993). Politika (M. Tunçay, Çev.). Remzi Kitabevi.
- Atabaş, H. (2018). Blokzinciri Teknolojisi ve Kripto Paraların Hayatımızdaki Yeni Yeri (1. bs). Ceres Yayınları.
- Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets. NOTE/2022/007, (ss. 1-43).
- Balaban Salı, J. (2018). Verilerin Toplanması. İçinde A. Şimşek (Ed.), Sosyal Bilimlerde Araştırma Yöntemleri (ss. 134-161). Anadolu Üniversitesi.
- Bambrough, B. (2018, Ağustos 6). Bitcoin Donations To Neo-Nazis Are Climbing Ahead Of This Weekend's Unite The Right Rally. Forbes. Erişim Tarihi: 15 Ocak 2024, <https://www.forbes.com/sites/billybambrough/2018/08/06/bitcoin-donations-to-neo-nazis-are-climbing-ahead-of-this-weekends-unite-the-right-rally/?sh=4977662969ac>.
- Bank for International Settlements/BIS. (2015). Digital Currencies (ss. 1-21). <https://www.bis.org/cpmi/publ/d137.pdf>.
- Bank of Russia. (2022). Cryptocurrencies: Trends, Risks, and Regulation (ss. 1-31). Bank of Russia.
- Barrett, R. (2012). Preventing the Financing of Terrorism. Case Western Reserve Journal of International Law, 3(44), Article 44, (ss. 719-736).
- Başaranel, B. U. (2021). Kayıt Zinciri (Blockchain). İçinde N. Akdemir & C. O. Tuncer (Ed.), Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım (1., ss. 260-263). Pegem Akademi.

- Başaranel, B. U., & Türkşen, U. (2019). Counter-Terrorist Financing Law and Policy An Analysis of Turkey (1. bs). Routledge.
- Bech, M., & Garratt, R. (2017). Central Bank Cryptocurrencies. BIS Quarterly Review, (ss. 55-70).
- Bernardi, S. D. C. (2019). Terrorist Use of Cryptocurrencies (ss. 1-22). Blockchain Cunsultus Ltd. www.blockchainconsultus.io.
- Bhaskar, N. D., & Chuen, D. L. K. (2015). Bitcoin Mining Technology. İçinde Handbook of Digital Currency (ss. 45-65). Elsevier. <https://doi.org/10.1016/B978-0-12-802117-0.00003-5>.
- Bitcoin Donations to ISIS Soared Day Before Sri Lanka Bombings. (2019, Mayıs 2). [Haber]. Globes. Erişim Tarihi: 23 Aralık 2023, <https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276>.
- Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., Zhang, B. Z., & Cloud, K. (2019). Global Cryptoasset Regulatory Landscape Study. SSRN Electronic Journal, (ss. 1-122). <https://doi.org/10.2139/ssrn.3379219>.
- Blockchain Türkiye. (2019). Blokzinciri Teknolojisi Terminoloji Çalışması (ss. 1-30). Blockchain Türkiye-Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu.
- Bordo, M. (2017). The Operation and Demise of the Bretton Woods System; 1958 to 1971 (ss. 1-37). National Bureau of Economic Research. <https://doi.org/10.3386/w23189>.
- Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 36.
- Carroll, P., & Windle, J. (2018). Cyber As An Enabler of Terrorism Financing, Now and In The Future. Journal of Policing, Intelligence and Counter Terrorism, 13(3), (ss. 285-300). <https://doi.org/10.1080/18335330.2018.1506149>.
- Chainalysis. (2023). Chainalysis Reactor. Chainalysis. Erişim Tarihi: 27 Aralık 2023, <https://www.chainalysis.com/chainalysis-reactor/>.
- Chaum, D. (1983). Blind Signatures for Untraceable Payments. Advances in Cryptology, (ss. 199-203). https://doi.org/10.1007/978-1-4757-0602-4_18.
- Chaum, D. L. (1982). Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups [University of California, Berkeley]. <https://evervault.com/papers/chaum.pdf>.
- Ciphertrace. (2022). Your Go-To Guide to the FATF's Crypto Travel Rule (ss. 1-9). Ciphertrace.
- Clark, J. (2016). Bitcoin, Blockchain, Cryptocurrency, Cryptology. Kindle Edition.
- Coelho, R., Fishman, J., & Ocampo, D. G. (2021). Supervising Cryptoassets For Anti-Money Laundering (ss. 1-24). Bank for International Settlements, Financial Stability Institute.

- CoinMarketCap. (2023). Erişim Tarihi: 1 Temmuz 2023, <https://coinmarketcap.com/>.
- Counter Extremism Project. (2018, Ağustos 28). Far-Right European Terrorist Group Crowdfunding Cryptocurrency. Counter Extremism Project. Erişim Tarihi: 15 Ocak 2024, <https://www.counterextremism.com/blog/far-right-european-terrorist-group-crowdfunding-cryptocurrency>.
- Crenshaw, M. (1981). The Causes of Terrorism. *Comparative Politics*, 13(4), Article 4, (ss. 379–399).
- Croissant, A., & Barlow, D. (2007). Following the Money Trail: Terrorist Financing and Government Responses in Southeast Asia. *Studies in Conflict & Terrorism*, 30(2), (ss. 131-156). <https://doi.org/10.1080/10576100600959721>.
- Çağlar, Ü., & Dışkaya, S. (2018). Küreselleşme, Uluslararası Para Sistemi ve Kriz. *İktisat Politikası Araştırmaları Dergisi*, 5(2), (ss. 1-24).
- Dabrowski, M., & Janikowski, L. (2018). Virtual Currencies And Central Banks Monetary Policy: Challenges Ahead. *European Parliament*, (ss. 1-30).
- Dash. (2023). Understanding Masternodes. Dash. Erişim Tarihi: 5 Temmuz 2023 <https://docs.dash.org/en/stable/docs/user/masternodes/understanding.html>.
- Demartino, I. (2021). Bitcoin Rehberi: Kripto Paralar Hakkında Bilmek İstedığınız Her Şey (K. Tekneci, Çev.; 3.). Epsilon Yayınevi.
- Digital Currency: The Future Of Your Money. (2023, Şubat 16). Forbes Advisor. Erişim Tarihi: 27 Şubat 2023, <https://www.forbes.com/advisor/investing/cryptocurrency/digital-currency/>.
- Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats, (ss. 1-80). RAND Corporation. <https://doi.org/10.7249/RR3026>.
- Directive 2000/46/EC of The European Parliament and of The Council of 18 September 2000 On The Taking Up, Pursuit of and Prudential Supervision of The Business of Electronic Money Institutions, DIRECTIVE 2000/46/EC Directive 2000/46/EC of The European Parliament and of The Council, (ss. 1-5), (2000). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0046&from=en>.
- Directive 2009/110/EC of The European Parliament and of The Council of 16 September 2009 on The Taking Up, Pursuit and Prudential Supervision of The Business of Electronic Money Institutions Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC, Directive 2009/110/EC Directive 2009/110/EC of The European Parliament and of The Council, (ss. 1-11), (2009). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=en>.
- Do All Cryptocurrencies Use The Blockchain? (2022, Ağustos 9). Bitstamp Learn. Erişim Tarihi: 4 Temmuz 2023, <https://www.bitstamp.net/learn/blockchain/do-all-cryptocurrencies-use-the-blockchain/>.

- Dostov, V., & Shust, P. (2014). Cryptocurrencies: An Unconventional Challenge To The AML/CFT Regulators? *Journal of Financial Crime*, 21(3), (ss. 249-263). <https://doi.org/0.1108/JFC-06-2013-0043>.
- Duffield, E., & Diaz, D. (2015). Dash: A Privacy-Centric Crypto-Currency. (ss. 1-16).
- Dyntu, V., & Dykyj, O. (2021). Cryptocurrency As An Instrument Of Terrorist Financing. *Baltic Journal of Economic Studies*, 7(5), (ss. 67-72).
- Eagleton, C., & Williams, J. (2011). *Paranın Tarihi* (F. Kâhya, Çev.; 1. bs). Türkiye İş Bankası Kültür Yayınları.
- EBA Opinion on 'Virtual Currencies' (ss. 1-46). (2014). European Banking Authority. <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>.
- Ebner, J. (2018, Ocak 24). The Currency of the Far-Right: Why Neo-Nazis Love Bitcoin. *The Guardian*. Erişim Tarihi: 15 Ocak 2024, <https://www.theguardian.com/commentisfree/2018/jan/24/bitcoin-currency-far-right-neo-nazis-cryptocurrencies>.
- ECB (European Central Bank). (2019). *Crypto-assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructure*. Occasional Paper Series, 223, (ss. 1-38).
- Eichengreen, B. (2003). *Golden Fetters: The Gold Standard and the Great Depression, 1919-1939*. Oxford Scholarship Online.
- Eisermann, D. (2020). *Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges* (H.-J. Schindler, Çev.; ss. 1-52). Berlin Risk Ltd.
- Elliptic. (2021, Aralık 8). Hate Symbols in the Blockchain Used to Flag Crypto Fundraising by Neo-Nazis. Elliptic. Erişim Tarihi: 15 Ocak 2024, <https://www.elliptic.co/blog/blockchain-hate-symbols-flag-crypto-fundraising-by-neo-nazis>.
- Elliptic. (2023a). How Terrorist Groups Are Exploiting Crypto To Raise Funds and Evade Detection. Elliptic. Erişim Tarihi: 17 Ağustos 2023, <https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection>.
- Elliptic. (2023b). *Preventing Financial Crime in Cryptoassets: Typologies Report 2023* (ss. 1-152). Elliptic.
- European Banking Authority (EBA). (2019). *Report With Advice For The European Commission On Crypto-Assets* (ss. 1-30).
- European Central Bank (Ed.). (1998). *Report On Electronic Money*. (ss. 1-47). European Central Bank.

- European Central Bank. (2012). Virtual Currency Schemes (ss. 1-53). European Central Bank.
<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.
- European Central Bank. (2015). Virtual Currency Schemes: A Further Analysis (ss. 1-37). European Central Bank Publications Office.
<https://data.europa.eu/doi/10.2866/662172>.
- European Central Bank. (2023). Electronic Money. European Central Bank. Erişim Tarihi: 14 Şubat 2023,
https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html.
- FATF. (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (ss. 1-145). FATF. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>.
- FATF. (2013). Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (ss. 1-192). FATF. <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html>.
- FATF. (2014). Virtual Currencies – Key Definitions and Potential AML/CFT Risks (ss. 1-15). FATF.
- FATF. (2015). Guidance For A Risk-Based Approach: Virtual Currencies (ss. 1-46). FATF.
- FATF. (2018). Outcomes FATF Plenary, 17-19 October 2018. FATF. Erişim Tarihi: 13 Aralık 2023, <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Outcomes-plenary-october-2018.html>.
- FATF. (2019a). Public Statement on Virtual Assets and Related Providers. FATF. Erişim Tarihi: 13 Aralık 2023, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Public-statement-virtual-assets.html>.
- FATF. (2019b). Guidance For A Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers (ss. 1-57). FATF.
- FATF. (2019c). Terrorist Financing Risk Assessment Guidance (ss. 1-62). FATF.
- FATF. (2020a). Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets (ss. 1-20). FATF.
- FATF. (2020b). FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins (ss. 1-28). FATF.
- FATF. (2020c). 12-Month Review Virtual Assets and VASPs (ss. 1-24). FATF.
- FATF. (2021a). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (ss. 1-109). FATF.

- FATF. (2021b). Second 12-Month Review Virtual Assets and VASPs, (ss. 1-43). FATF.
- FATF. (2022). Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs (ss. 1-26). FATF.
- FATF. (2023a). Crowdfunding for Terrorism Financing (ss. 1-60). FATF.
- FATF. (2023b). History of the FATF. Erişim Tarihi: 12 Aralık 2023, <https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html>.
- FATF. (2023c). What We Do. FATF. Erişim Tarihi: 11 Aralık 2023, <https://www.fatf-gafi.org/en/the-fatf/what-we-do.html>.
- FATF. (2023d). FATF Global Network. FATF. Erişim Tarihi: 12 Aralık 2023, <https://www.fatf-gafi.org/en/countries/global-network.html>.
- FATF. (2023e). Countries. FATF. Erişim Tarihi: 12 Aralık 2023, <https://www.fatf-gafi.org/en/countries.html>.
- FATF. (2023f). Topics. FATF. Erişim Tarihi: 12 Aralık 2023, <https://www.fatf-gafi.org/en/topics.html>.
- FATF. (2023g). Methods and Trends. FATF. Erişim Tarihi: 12 Aralık 2023, <https://www.fatf-gafi.org/en/topics/methods-and-trends.html>.
- FATF. (2023h). Mutual Evaluations. FATF. Erişim Tarihi: 12 Aralık 2023, <https://www.fatf-gafi.org/en/topics/mutual-evaluations.html>.
- FATF. (2023i). High-Risk and Other Monitored Jurisdictions. FATF. Erişim Tarihi: 12 Aralık 2023, <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>.
- FATF. (2023j). Virtual Assets. FATF. Erişim Tarihi: 24 Aralık 2023, [https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20\(crypto%20assets\)%20refer,digital%20representation%20of%20fiat%20currencies](https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,digital%20representation%20of%20fiat%20currencies).
- FATF. (2023k). Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs (ss. 1-20). FATF.
- FATF. (2023l). Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations (ss. 1-39). FATF.
- Faulkner, J. (2016). Getting Started with Cryptography in .NET. BookRix. https://www.bookrix.com/book.html?bookID=ir0c7a3135af765_1454331854.1749091148#0,558,8496.
- Federal Financial Monitoring Service. (2018). The Russian Federation National Terrorism Financing Risk Assessment 2017-2018 Public Report (ss. 1-23). Federal Financial Monitoring Service.

- Federal Ministry of Finance (Germany). (2019). First National Risk Assessment 2018/2019: Anti-Money Laundering/ Countering the Financing of Terrorism (ss. 1-114). Federal Ministry of Finance.
- Ferguson, N. (2012). Paranın Yükselişi Dünyanın Finansal Tarihi (B. Pala, Çev.; 2. bs). Yapı Kredi Yayınları.
- Financial Stability Board (FSB). (2020). Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Final Report and High-Level Recommendations. Financial Stability Board, (ss. 1-69).
- Finck, M. (2019). Blockchain and the General Data Protection Regulation. Scientific Foresight Unit (STOA), European Parliamentary Research Service (EPRS), (ss. 1-105). <https://doi.org/10.2861/535>.
- Fleming, S. (2021, Nisan 5). What is blockchain and what can it do? World Economic Forum. Erişim Tarihi: 16 Nisan 2023, <https://www.weforum.org/agenda/2021/04/what-is-blockchain/>.
- Freeman, M. (2011). The Sources of Terrorist Financing: Theory and Typology. Studies in Conflict and Terrorism, 34(6), Article 6, (ss. 461–475).
- Freeman, M., & Ruehsen, M. (2013). Terrorism Financing Methods: An Overview. Perspectives on Terrorism, 7(4), Article 4, (ss. 5-26).
- Furneaux, N. (2018). Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence. John Wiley&Sons, Inc.
- G7/8 Paris Summit Economic Declaration. (1989, Temmuz 16). G7 Information Centre. Erişim Tarihi: 11 Aralık 2023, <http://www.g8.utoronto.ca/summit/1989paris/communique/index.html>
- Galbraith, J. K. (2017). Money Whence It Came, Where It Went. Princeton University Press.
- Gençcelep, R. (2022). Kripto Paraların Terörün Finansmanı Suçunda Kullanılması. Bilişim Hukuku Dergisi, 4(1), (ss. 33-80).
- Global Blockchain Business Council. (2020). Global Standard Mapping Initiative (GSMI): Insight Repor (ss. 1-34). Global Blockchain Business Council.
- Grauer, K., Kueshner, W., & Updegrave, H. (2022). The 2022 Crypto Crime Report (ss. 1-140) [Araştırma]. Chainalysis.
- Grauer, K., & Updegrave, H. (2021). The 2021 Crypto Crime Report (ss. 1-113) [Araştırma]. Chainalysis.
- Gürsoy, S. (2021). Para Gelmişi, Geçmişi, Geleceği (1. bs). Sonçağ Akademi.
- Güven, V., & Şahinöz, E. (2021). Blokzincir, Kripto Paralar, Bitcoin (8. bs). Kronik Kitap.
- Harari, Y. N. (2017). Hayvanlardan Tanrılara Sapiens (E. Genç, Çev.; 39. bs). Kolektif Kitap.

- Hardman, J. B. S. (1936). Terrorism. *İçinde Encyclopedia of Social Sciences* (1. bs, C. 14, ss. 575-579). Macmillan Publishing.
- Harvard Business Review Press. (2021). *Dijital Dönüşüm Blok Zinciri* (T. Gezer, Çev.). Optimist Yayın Grubu.
- Harvey, J., & Branco-Illodo, I. (2019). Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in “Privacy Coin” Whitepapers. *Journal of Political Marketing*, 19, (ss. 1-30). <https://doi.org/10.1080/15377857.2019.1652223>.
- Hasbi, A. H., & Mahzam, R. (2018). Cryptocurrencies: Potential For Terror Financing. *RSIS Commentaries*, (ss. 1-3).
- He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T. S., Stetsenko, N., & Verdugo-Yepes, C. (2016). Virtual Currencies and Beyond: Initial Considerations. *International Monetary Fund*, (ss. 1-42).
- Helme, J., & Wilkinson, E. (2016). Digital, Virtual and Crypto Currencies: Issues and Accounting Risks. *Grant Thornton*, (ss. 1-4).
- Hilmola, O.-P. (2021). On Prices of Privacy Coins and Bitcoin. *Journal of Risk and Financial Management*, 14(8), (ss. 1-15). <https://doi.org/10.3390/jrfm14080361>.
- HM Treasury (UK). (2020). National Risk Assessment of Money Laundering and Terrorist Financing 2020 (ss. 1-148). HM Treasury.
- Hoffman, B. (2006). *Inside Terrorism* (Revised and Expanded Edition). Columbia University Press.
- Houben, D. R., & Snyers, A. (2018). Cryptocurrencies and Blockchain. *European Parliament*, (ss. 1-100).
- Ibrahim, S. A. (2019). Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering. *Stratagem*, 2(1), (ss. 1-17).
- Iuon-Chang, L., & Tzu-Chun, L. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5), (ss. 653-659). [https://doi.org/10.6633/IJNS.201709.19\(5\).01](https://doi.org/10.6633/IJNS.201709.19(5).01).
- Jenkins, B. (1975). *International Terrorism: A New Mode of Conflict* (1. bs). California Seminar on Arms Control and Foreign Policy.
- Kadyrov R.E. & Prokhorov I.V. (2018). Regulating Cryptocurrencies: New Challenges to Economic Security and Problems Created by Individuals Involved in the Schemes of Laundering Cryptocurrencies-Generated Profits. *KnE Social Sciences*, 3(2), (ss. 1-12). <https://doi.org/10.18502/kss.v3i2.1568>.

- Katsiri, R. (2019, Mayıs 2). Bitcoin Donations to ISIS Soared Day Before Sri Lanka Bombings [Haber]. Globes. Erişim Tarihi: 23 Aralık 2023, <https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276>.
- Keatinge, T., Carlisle, D., & Keen, F. (2018). Virtual Currencies and Terrorist Financing: Assessing The Risks and Evaluating Responses. European Parliament Study, (ss. 1-87).
- Keene, S. D. (2011). Terrorism and The Internet: A Double-Edged Sword. *Journal of Money Laundering Control*, 14(4), (ss. 359-370). <https://doi.org/10.1108/13685201111173839>.
- Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), (ss. 325-344). <https://doi.org/10.1177/1057567719827051>.
- Keynes, J. M. (2012). Para Üzerine Bir İnceleme (C. Gerçek, Çev.; 1. bs). Türkiye İş Bankası Kültür Yayınları.
- Kfir, I. (2020). Cryptocurrencies, National Security, Crime and Terrorism. *Comparative Strategy*, 39(2), (ss. 113-127). <https://doi.org/10.1080/01495933.2020.1718983>.
- Krishnan, A. (2020). Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations. *Journal of Strategic Security*, 13(1), (ss. 41-58). JSTOR.
- Küçük, D., Yakut, Ö. F., Çakar, E., & Ertam, F. (2023). Investigation of Cryptocurrency-Centered Money Laundering Scenarios in Terms of Digital Forensics. *International Journal of Advances in Engineering and Pure Sciences*, 35(3), (ss. 285-296). <https://doi.org/10.7240/jeps.1224416>.
- Lansky, J. (2018). Possible State Approaches to Cryptocurrencies. *Journal of Systems Integration*, 9(1), (ss. 19-31). <https://doi.org/10.20470/jsi.v9i1.335>.
- Lau, K. (2020). Non-Fungible Tokens: A Brief Introduction and History (ss. 1-19). Crypto.com.
- Lee, J. (2022). *Crypto-Finance, Law and Regulation: Governing an Emerging Ecosystem* (1. bs). Routledge.
- LexisNexis Risk Solutions. (2019). A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers White Paper (ss. 1-7). LexisNexis Risk Solutions.
- Litecoin. (2020). Litecoin. Erişim Tarihi: 22 Aralık 2023, <https://litecoin.com/en/>.
- Ma, A. (2017, Aralık 15). A New York Woman Accused of Sending Bitcoin to ISIS Could Spend 90 Years in Prison [Haber]. Business Insider. Erişim Tarihi: 27 Aralık 2023, <https://www.businessinsider.com/zoobiah-shahnaz-charged-after-sending-bitcoin-to-isis-from-long-island-2017-12#:~:text=Zoobia%20Shahnaz%20is%20accused%20of,years%20in%20prison%20if%20convicted>.

- Majumder, A., Routh, M., & Singha, D. (2019). A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing. İçinde R. C. Das (Ed.), *The Impact of Global Terrorism on Economic and Political Development* (ss. 125-138). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-78769-919-920191012>.
- MASAK. (2018a). Aklama Suçu. T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu. Erişim Tarihi: 22 Ekim 2023, <https://masak.hmb.gov.tr/aklama-sucu-genel-bilgi>.
- MASAK. (2018b). Aklamanın Aşamaları. T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu. Erişim Tarihi: 22 Ekim 2023, <https://masak.hmb.gov.tr/aklamanin-asamaları>.
- MASAK. (2018c). Aklama Yöntemleri. T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu. Erişim Tarihi: 22 Ekim 2023, <https://masak.hmb.gov.tr/aklama-yontemleri>.
- MASAK. (2021). Yabancı Ülkelerde Kurulan Güven Sözleşmesi Taraflarına İlişkin Kimlik Tespiti Yükümlülüğü (ss. 1-19). MASAK. <https://ms.hmb.gov.tr/uploads/sites/12/2021/07/Yabanci-Ulkelerde-Kurulan-Guven-Sozlesmesi-Taraflarina-Iliskin-Kimlik-Tespiti-Yukumlulugu-Rehberi.pdf>
- MASAK. (2022). Finansal Kuruluşlara Yönelik Terörizmin Finansmanı ile Mücadele Rehberi (ss. 1-34). MASAK.
- MASAK. (2023). Ulusal Risk Değerlendirmesi (Özet): Kara Paranın Aklanması ve Terörizmin Finansmanı ile Mücadele (ss. 1-16). <https://ms.hmb.gov.tr/uploads/sites/12/2023/08/URD.pdf>.
- Matsakis, L. (2017, Ağustos 29). This Twitter Bot Tracks Neo-Nazi Bitcoin Transactions. Erişim Tarihi: 15 Ocak 2024, <https://www.vice.com/en/article/paax7z/this-twitter-bot-tracks-neo-nazi-bitcoin-transactions>.
- Michael, G. (2009). David Lane and Fourteen Words. *Totalitarian Movements and Political Religions*, 10(1), 43-61.
- Mishkin, F. S. (2004). *The Economics of Money, Banking, and Financial Markets* (7. bs). Pearson.
- Mohammed, N., Pesme, J., & Popovic, A. (2022, Aralık). Is Central Bank Digital Currency the right tool to expand financial inclusion? World Bank Blogs. Erişim Tarihi 26 Şubat 2023, <https://blogs.worldbank.org/allaboutfinance/central-bank-digital-currency-right-tool-expand-financial-inclusion#:~:text=CBDC%20is%20a%20form%20of,liabilities%20of%20private%20financial%20institutions>.
- Momtaaz, P. P. (2020). Initial Coin Offerings. *PLOS ONE*, 15(5), (ss. 1-30). <https://doi.org/10.1371/journal.pone.0233018>.
- Monero. (t.y.). What is Monero (XMR)? Erişim Tarihi: 27 Aralık 2023, <https://www.getmonero.org/get-started/what-is-monero/>.

- Monetary Authority of Singapore. (2020). Terrorism Financing National Risk Assessment: Singapore's Key Terrorism Financing (TF) Risk Areas (ss. 1-18). Monetary Authority of Singapore.
- Morell, M., Kirshner, J., & Schoenberger, T. (2021). An Analysis of Bitcoin's Use in Illicit Finance (ss. 1-11). Crypto Council for Innovation. <https://cryptoforinnovation.org/wp-content/uploads/2022/07/An-Analysis-of-Bitcoins-Use-in-Illicit-Finance-By-Michael-Morell.pdf>.
- Myres, G. (2012). Investing in the Market of Violence: Toward a Micro-Theory of Terrorist Financing. *Studies in Conflict & Terrorism*, 35(10), Article 10. (ss. 693-711). <https://doi.org/10.1080/1057610X.2012.712031>.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>.
- Narayanan, A., & Clark, J. (2017). Bitcoin's Academic Pedigree. *ACM*, (ss. 1-30).
- Nastiti, A., & Wimmer, A. (2015). Darknet, Social Media, And Extremism: Addressing Indonesian Counterterrorism on The Internet. *Deutsches Asienforschungszentrum Asian Series Commentaries*, 30, Article 30. (ss. 1-13).
- National Public Safety Commission (Japan). (2019). National Risk Assessment-Follow-up Report (ss. 1-127). National Public Safety Commission.
- Office of Assistant to Deputy Cabinet Secretary for State Documents & Translation. (2023, Kasım 6). Indonesia Becomes Full Member of FATF. Cabinet Secretariat of the Republic of Indonesia. Erişim Tarihi: 20 Ocak 2024, <https://setkab.go.id/en/indonesia-becomes-full-member-of-fatf/>.
- Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, (2021).
- Patel, P. C., & Pereira, I. (2020). The Relationship Between Terrorist Attacks and Cryptocurrency Returns. *Applied Economics*, (ss. 1-22). <https://doi.org/10.1080/00036846.2020.1819952>.
- Persi Paoli, G., Aldridge, J., Ryan, N., & Warnes, R. (2017). Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web (ss. 1-125). RAND Corporation. <https://doi.org/10.7249/RR2091>.
- Pınar, A., & Erdal, B. (2016). Para-Banka Mali Kuruluşlar ve Uluslararası Mali Sistem (3. bs). Turhan Kitabevi.
- Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering*, 59(1), (ss. 69-76). <https://doi.org/10.1007/s12599-017-0464-6>.
- Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything You Wanted to Know About the Blockchain. *IEEE Consumer Electronics Magazine*, (ss. 6-14).

- Regulation of The European Parliament and of The Council On Markets In Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, (ss. 1-469), (2023).
- Ricardo, D. (2008). Siyasal İktisadın ve Vergilendirmenin İlkeleri (B. Zeren, Çev.; 1. bs). Türkiye İş Bankası Kültür Yayınları.
- Richardson, L. (2006). What Is Terrorism. İçinde The Roots of Terrorism (2006. bs, ss. 19-39). Routledge.
- Ripple. (2023). Ripple. Erişim Tarihi: 27 Aralık 2023, <https://ripple.com/xrp/>.
- Robinson, T. (2018, Nisan 23). ICO Risk: Why AML Compliance Matters. Elliptic. Erişim Tarihi: 11 Aralık 2023, <https://www.elliptic.co/blog/ico-risk-why-aml-compliance-matters>.
- Rohr, J., & Wright, A. (2017). Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets. SSRN Electronic Journal, (ss. 1-115). <https://doi.org/10.2139/ssrn.3048104>.
- Salami, I. (2017). Terrorism Financing with Virtual Currencies – Can Regulatory Technology Solutions Combat this? Studies in Conflict & Terrorism, 41(12), (ss. 1-39). <https://doi.org/10.1080/1057610X.2017.1365464>.
- Sanction Scanner. (2023). Staying Ahead of the Game: A Report on Financial Crimes and Risks for 2023 (ss. 1-38). Sanction Scanner.
- Schwarz, N., Poh, K., Chen, K., Jackson, G., Kao, K., Fernando, F., & Markevych, M. (2021). Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2): Effective Anti-Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework—Some Legal and Practical Considerations (ss. 1-14). International Monetary Fund.
- Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the Origins and Variations of Blockchain Technologies. IEEE Computer and Reliability Societies, 17(1), (ss. 72-77). <https://doi.org/10.1109/MSEC.2019.2893730>.
- Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). Exploring the Use of Zcash Cryptocurrency For Illicit Or Criminal Purposes (ss. 1-49). RAND Corporation. <https://doi.org/10.7249/RR4418>.
- Smith, A. (2006). Milletlerin Zenginliği (H. Derin, Çev.; 1. bs). Türkiye İş Bankası Kültür Yayınları.
- Solms-Laubach, F. (2015, Kasım 27). Mord-Waffen Kamen Aus Deutschland! [Haber]. Bild. Erişim Tarihi: 26 Aralık 2023, <https://www.bild.de/politik/ausland/waffen/aus-pariser-terror-nacht-stammen-aus-deutschland-43565470,var=a,view=conversionToLogin.bild.html>.
- Somel, C. (2014). Makroiktisada Giriş (1.). Yordam Kitap.

- Song, Y., Chen, B., & Wang, X.-Y. (2023). Cryptocurrency Technology Revolution: Are Bitcoin Prices and Terrorist Attacks Related? *Financial Innovation*, 9(1), (ss. 1-29). <https://doi.org/10.1186/s40854-022-00445-3>.
- Stalinsky, S., Sosnow, R., Smith, A., Ali, S., Choukry, K., Schierer, M., Mozes, N., Kerman, Y., Pacchiani, G., & Kulka, Y. (2023, Mayıs 19). Jihadi Groups Around The World Continue To Fundraise In Cryptocurrency For Their Activity – Part II: January 2020-May 2023 [Araştırma]. MEMRI. Erişim Tarihi: 27 Aralık 2023, <https://www.memri.org/jttm/jihadi-groups-around-world-continue-fundraise-cryptocurrency-their-activity-%E2%80%93-part-ii-january>.
- Suratkar, S., Shirole, M., & Bhirud, S. (2020). Cryptocurrency Wallet: A Review. 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), (ss. 1-7). <https://doi.org/10.1109/ICCCSP49186.2020.9315193>.
- Swartz, L. (2021). Para Devrimi (1.). The Kitap.
- Şafak, E., Arslan, Ç., Gözütok, M., & Köprülü, T. (2021). Dağıtık Defter Teknolojileri ve Uygulama Alanları Üzerine Bir İnceleme. *European Journal of Science and Technology*, 29, (ss. 36-45). <https://doi.org/10.31590/ejosat.1011289>.
- Şıklar, İ. (2004). Para Teorisi ve Politikası (S. Gerek, Ed.; 1. bs). Anadolu Üniversitesi. <https://books.google.com.tr/books?id=0-p6VcWNUs4C&printsec=frontcover&hl=tr#v=onepage&q&f=false>.
- Tanrıverdi, M., Uysal, M., & Üstündağ, M. T. (2019). Blokzinciri Teknolojisi Nedir? Ne Değildir? : Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), (ss. 203-217). <https://doi.org/10.17671/gazibtd.547122>.
- TCMB. (2018). Kâğıt Paranın Tarihçesi. Türkiye Cumhuriyet Merkez Bankası. <https://www.tcmb.gov.tr/wps/wcm/connect/d189b219-fe71-40bf-9754-6a5f7d0a65eb/KagitParaTarihce.pdf?MOD=AJPERES#:~:text=%C4%B0lk%20k%C3%A2%20%C4%9F%C4%B1t%20paran%C4%B1n%201690'l%C4%B1,kurulmas%C4%B1%20ile%20de%20yayg%C4%B1nla%C5%9Ft%C4%B1%C4%9F%C4%B1%20g%C3%B6r%C3%BClmektedir>.
- TDK. (2022). Terör [Sözlük]. Türk Dil Kurumu Sözlükleri. Erişim Tarihi: 26 Aralık 2023, <https://sozluk.gov.tr/>.
- TDK. (2022). Uyuşum [Sözlük]. Türk Dil Kurumu Sözlükleri. Erişim Tarihi: 10 Aralık 2023, <https://sozluk.gov.tr/>.
- Teichmann, F. M. J. (2018a). Financing Terrorism through Cryptocurrencies – A Danger for Europe? *Journal of Money Laundering Control*, 21(4), (ss. 513-519). <https://doi.org/10.1108/JMLC-06-2017-0024>.
- Teichmann, F. M. J. (2018b). Financing terrorism through cryptocurrencies – a danger for Europe? *Journal of Money Laundering Control*, 21(4), (ss. 513-519). <https://doi.org/10.1108/JMLC-06-2017-0024>.
- Terörle Mücadele Kanunu, 3713 § 1 (1991). <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf>.

- Terörizmin Finansmanının Önlenmesi Hakkında Kanun, 6415 1 (2013).
<https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6415.pdf>.
- Tevetoğlu, M. (2021). Hukuki Yönleriyle Kripto Varlıklar ve Kripto Varlıkların İlk Arzı (2.bs). Aristo Yayınevi.
- The World Bank. (2017). Distributed Ledger Technology (DLT) and Blockchain (ss. 1-46).
 The World Bank.
<https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>.
- The World Bank. (2022). Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool: Guidance Manual (ss. 1-106). World Bank Group.
<https://doi.org/10.1596/37761>.
- Thornton, T. P. (1964). Terror as a Weapon of Political Agitation. İçinde H. Eckstein (Ed.), Internal War Problems and Approaches. The Free Press.
- Tilly, C. (2004). Terror, Terrorism, Terrorists. Sociological Theory, 22(1), Article 1. (ss. 5-13).
- Tofangsaz, H. (2012). A New Approach To The Criminalization Of Terrorist Financing And Its Compatibility With Law. Journal of Money Laundering Control, 15(4), (ss. 396-406). <https://doi.org/10.1108/13685201211265980>.
- Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys & Tutorials, 18(3), (ss. 1-41). <https://doi.org/10.1109/COMST.2016.2535718>.
- Turan, D., & Demircan, C. (2021). Kripto Paralar ile Terör ve Diğer İlgil Aktivitelerin Finansmanı. Anadolu Akademi Sosyal Bilimler Dergisi, 3(1), (ss. 161-176).
- Turan, D., & Gemici, E. (2020). Terörizmin Finansman Kaynakları ve Karapara Aklamanın Terörizmin Finansmanındaki Rolü. Anadolu Üniversitesi Sosyal Bilimler Dergisi, 20(2), (ss. 257-278). <https://doi.org/10.18037/ausbd.758070>.
- Türkiye Barolar Birliği. (2006). Türkiye ve Terörizm (Proje Raporu 107; Sayı 107, ss. 1-634). Türkiye Barolar Birliği.
- Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2022, Nisan 22). NFT'nin Türkçe Karşılığı Belli Oldu. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. Erişim Tarihi: 9 Temmuz 2023, <https://cbddo.gov.tr/haberler/6354/nft-nin-turkce-karsiligi-belli-oldu#:~:text=Payla%C5%9F%3A,Tabu%E2%80%9D%20olarak%20kullanmay%C4%B1%20d%C3%BC%C5%9F%C3%BCnd%C3%BCKlerini%20a%C3%A7%C4%B1klad%C4%B1>.
- United Nations. (2008a). Declaration on Measures to Eliminate International Terrorism General Assembly Resolution 49/60 of 9 December 1994. İçinde International Instruments Related to the Prevention and Suppression of International Terrorism (1. bs, ss. 349-352). United Nations Publication.

- United Nations. (2008b). International Convention for the Suppression of the Financing of Terrorism. İçinde International Instruments Related to the Prevention and Suppression of International Terrorism (1. bs, ss. 89-103). United Nations Publication.
- United Nations Office on Drugs and Crime. (2012). The Use Of The Internet For Terrorist Purposes (ss. 1-142). United Nations.
- United States Department of the Treasury. (2022). 2022 National Terrorist Financing Risk Assessment (ss. 1-28).
- Ünsal, E. M. (2016). İktisada Giriş (5.). BB101.
- Üstün, O. (2005). Mali Eylem Görev Gücü'nün (FATF) Dokuz Özel Tavsiyesi. Bankacılar Dergisi, 52, (ss. 10-27).
- Van der Merwe, A. (2021). Cryptocurrencies and Other Digital Asset Investments. İçinde M. Pompella & R. Matousek (Ed.), The Palgrave Handbook of FinTech and Blockchain (ss. 445-471). Springer International Publishing. https://doi.org/10.1007/978-3-030-66433-6_20.
- Vigna, P., & Casey, M. J. (2020). KriptoPara Çağı: Bitcoin ve Dijital Paranın Küresel Ekonomik Sistemde Meydan Okuması (A. Atav, Çev.; 3.). Buzdağı Yayınevi.
- Vittori, J. (2011). Terrorist Financing and Resourcing (1. bs). Palgrave Macmillan.
- Vujičić, D., Jagodić, D., & Randić, S. (2018). Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview. 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), (ss. 1-6). <https://doi.org/10.1109/INFOTEH.2018.8345547>.
- Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges, (ss. 1-20).
- Wang, S., & Zhu, X. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. Oxford University Press, 15(4), (ss. 2329-2340). <https://doi.org/10.1093/police/paab059>.
- Warmke, C. (2021). What Is Bitcoin? Inquiry, (ss. 1-43). <https://doi.org/10.1080/0020174X.2020.1860123>.
- Weimann, G. (2015). Going Dark: Terrorism on the Dark Web. Studies in Conflict & Terrorism, (ss. 1-24). <https://doi.org/10.1080/1057610X.2015.1119546>.
- Weimann, G. (2016). Terrorist Migration to the Dark Web. Perspectives on Terrorism, 3(10), Article 10, (ss. 40-44).
- Werbach, K. (2021). Blokzinciri ve Yeni Güven Mimarisi (A. Usta, Çev.; 1.). Koç Üniversitesi Yayınları.
- What is blockchain technology? (t.y.). IBM. Erişim Tarihi: 17 Nisan 2023, <https://www.ibm.com/topics/blockchain#:~:text=Blockchain%20defined%3A%20Blockchain%20is%20a,patents%2C%20copyrights%2C%20branding>).

- Why Decentralised Finance (DeFi) Matters and the Policy Implications (ss. 1-67). (2022). OECD. <https://doi.org/10.1787/eb61fd29-en>.
- Whyte, C. (2019). Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise. *Studies in Conflict & Terrorism*, (ss. 1-24). <https://doi.org/10.1080/1057610X.2018.1531565>.
- Wilkinson, P. (1974). *Political Terrorism* (1. bs). The Macmillan Press LTD.
- Wilkinson, P. (2011). *Terrorism versus Democracy* (3. bs). Routledge.
- Williams, S. P. (2020). *Blok Zinciri: Gelecekteki Her Şey* (O. Gündüz, Çev.; 1.). Kaknüs Yayınları.
- Wiwoho, J., Pratama, A., Khaerah Pati, U., & Tejomurti, K. (2023). Examining Cryptocurrency Use among Muslim Affiliated Terrorists: Case Typology and Regulatory Challenges in Southeast Asian Countries. *AL-IHKAM: Jurnal Hukum & Pranata Sosial*, 18, (ss. 102-124). <https://doi.org/10.19105/al-lhkam.v18i1.7147>.
- Wray, L. R. (2012). Introduction to an Alternative History of Money. *SSRN Electronic Journal*, (ss. 1-50). <https://doi.org/10.2139/ssrn.2050427>.
- Yurdakul, M. O. (2023). Mali Eylem Görev Gücü Nezdindeki Dördüncü Tur Karşılıklı Değerlendirme Süreci ve Türkiye'nin Uyum Düzeyindeki Gelişmeler. *Bankacılar Dergisi*, 34(127), (ss. 49-77).
- Zcash. (t.y.). What Is Zcash? Z.cash. Erişim Tarihi: 6 Temmuz 2023, <https://z.cash/learn/what-is-zcash/>.
- Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2016). Solutions to Scalability of Blockchain: A Survey. *IEEE Access*, 8, (ss. 1-16). <https://doi.org/10.1109/ACCESS.2020.2967218>.
- Zhou, Y., Wu, J., & Zhang, S. (2021). Anonymity Analysis of Bitcoin, Zcash and Ethereum. 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), (ss. 45-48). <https://doi.org/10.1109/ICBAIE52039.2021.9389894>.



“JSGA’lı, Her Zaman Yurt, Ulus ve Cumhuriyete Aşk
ve Sadakatle Bağlı Tevazu, Fedakârlık ve Feragat
Örneğidir.”