# KRİPTO PARALARIN TERÖRÜN FİNANSMANINDA KULLANILMASI

**Cemre Ç. Kadıoğlu Kumtepe***

## *ÖZ*

*Terörizmin finansmanın önlenmesi konusunda atılan adımlar, sanal paraların ortaya çıkmasıyla yetersiz kalmışlardır. Kripto paralar, sanal paraların bir türü olup blokzincir teknolojisine dayanmaktadır. Kripto paralar, merkezileşmemiş sistem üzerinden işlem görmektedir. Başka bir deyişle banka gibi aracı kuruluşların kullanılmasına gerek duyulmamaktadır. Aracı kuruluşlarla yapılan nakit akışı takip edilebilirken kripto paralarla yapılan işlemler tespit edilememektedir. Bu nedenle kripto paraların terörizmin finansmanında kullanılması endişe yaratmıştır. Kripto paraların sınır ötesi aktarılması ve bu alandaki ulusal ve uluslararası regülasyon eksikliği nedeniyle terörizmin finansmanında kripto paraların yaygınlaşacağı düşünülmektedir. Bu çalışmada genel olarak terör örgütlerinin finansman ihtiyaçlarından bahsedilmekte; kripto paraların bu ihtiyaçlara nasıl cevap verdiği açıklanmaktadır. Kripto paraların terörizmin finansmanında kullanılmasının engellenmesinde halihazırda yürürlükte olan düzenlemelerin ne derece etkili olduklarına değinildikten sonra kripto paralar özelinde yapılan birtakım çalışmalar ve bunların etkileri ele alınmaktadır. Çalışmanın sonucunda, kripto paraların terörizmin finansmanında kullanılmasının engellenmesinde uluslararası iş birliğinin sağlanması için gerekli adımların atılması gerektiği sonucuna varılmıştır.*

***Anahtar kelimeler:*** *Terörizmin finansmanı, kara paranın aklanması, kripto para, sanal para, blokzincir teknolojisi*

## GİRİŞ

Terör örgütleri veya etkinliklerini bireysel olarak sürdüren teröristlerin eylemlerine devam edebilmeleri ve ihtiyaçlarını karşılayabilmeleri için finansmana ihtiyaçları vardır. Finansman yasadışı veya yasal yollarla elde edilebilir. Günümüzde çatışma ve örgütlenme gibi konularda geleneksel yöntemlerden uzaklaşan terör örgütleri, finansman sağlama konusunda da yeni yöntemlere yönelmeye başlamışlardır.[1] Geleneksel olarak, devlet sponsorluğu, bağış toplama, yasal veya yasadışı işlerden elde edilen gelirlerle finansman sağlanırken, kripto para teknolojisinin gelişmesiyle bu yöntemlere bir yenisi daha eklenmiştir. Kripto para gibi gelişen yeni teknolojilerin, teknolojiden

[1] Anais Carmona, 'The Bitcoin The Currency of the Future, Fuel of Terror' (2015) 63 Advances in Information Security 127.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

faydalanan IŞİD gibi uluslararası suç örgütleri tarafından benimsendiği görülmektedir.[2] Terör örgütlerinin adeta ticari işletmeler gibi yeni finansman yöntemlerini benimsemeye başlaması, bu örgütlerin yasadışı eylemlerini farklı bir boyuta taşıyacağı endişesini doğurmaktadır.[3] Sanal paraların blokzincir teknolojisine dayanan bir türü olan kripto paraların banka gibi merkezi kuruluşların aracılığına ihtiyaç duymaması, sınır ötesi transferinin kolaylığı, kullanıcılara anonimlik sağlaması ve takibinin çok zor olması gibi özellikleri nedeniyle terörün finansmanında tercih edildiği görülmekte ve yasadışı eylemlerde kullanımının yaygınlaşacağı düşünülmektedir. Kripto paralar hem geleneksel yöntemlerle sağlanan para transferinin gizlenmesinde hem de finansmanın tedavüldeki resmi para birimleri yerine Bitcoin gibi kripto paralar üzerinden sağlanmasında kullanılabilecektir. Kripto paraların kullanımına yönelik birtakım ulusal ve uluslararası çalışmalar olsa da güncel düzenlemelerin kripto paraların ulusal ve uluslararası düzeyde terörizmin finansmanını engellemede yetersiz kaldığı görülmektedir.

Bu bölümde, kripto paraların terörizmin finansmanında kullanılması ve bununla ilintili olarak kara paranın aklanması uluslararası hukuk açısından ele alınmakta; bunların önüne geçilmesinde atılan teknolojik, politik ve hukuki düzenlemelere değinilmektedir. Konunun cezai boyutları çalışmanın kapsamının dışında bırakılmıştır. İlk bölümde kripto paraların tanımlanma ve nitelendirilme sorunu üzerinde durulmuştur. İkinci bölümde terör örgütlerinin finansman ihtiyaçlarının neler olduğu ve bu finansmanı hangi yöntemlerle sağladıkları özetlenmiştir. Kripto paraların terörizmin finansmanında tercih edilmesini sağlayan özellikleri ve bu özelliklerin terör örgütlerinin finansman ihtiyaçlarına nasıl cevap verdiği üzerinde durulmuştur. Üçüncü bölümde kara para aklama ve terörün finansmanın önlenmesi hakkındaki düzenlemelerin neler olduğuna değinilmiş ve bunların kripto paraların aynı amaçlarla kullanılmasında ne derece etkili oldukları tartışılmıştır. Son olarak, dördüncü bölümde kripto paraların terörizmin finansmanında kullanılmasının önüne geçilmesinde birtakım ulusal ve uluslararası düzenlemeler ele alınmıştır. Kripto paraların terörizmin finansmanında kullanılmasının önüne geçilmesinde ulusal düzenlemelerin hem aynı ülke içinde hem de uluslararası düzeyde yeknesak olmadığı, kripto paralara yaklaşımdaki farklılıkların terörizmin finansmanında kullanılmalarını engellemede yetersiz olacağı anlaşılmaktadır. Bu nedenle, ulusal düzenlemelerin eksiklerinin tespit edilmesi, devlet kurumlarının tutarlı politikalar geliştirmesi ve nihai olarak uluslararası düzeyde iş birliği yapılması gerektiği sonucuna varılmıştır.

## 1. Kripto Paranın Tanımlanması ve Nitelendirilmesi Sorunu

[2] Salman Ali Ibrahim, 'Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering' (2019) 2 *Stratagem*.
[3] Carmona (n 1) 130.

DRAFT - TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Bağımsız bir uluslararası örgüt olan Mali Eylem Görev Gücü (*Financial Action Task Force (FATF)*) sanal parayı 1) kambiyo ortamı ve/veya 2) hesap birimi ve/veya değerin depolanması görevlerini gören ancak hiçbir hukuk sisteminde yasal ödeme aracı değeri olmayan, sanal olarak takas edilebilen değerlerin sanal temsili olarak tanımlamaktadır.[4] Türkiye Blokzincir Çalışmaları ise sanal parayı ABD Vergi Dairesi'nin (*Internal Revenue Service (IRS)*) tanımından yola çıkarak "*Bir değişim aracı, bir hesap birimi ve/veya bir değer saklama aracı olarak çalışan ve herhangi bir yargı alanında yasal ihale statüsüne sahip olmayan bir değerin dijital temsili*" olarak tanımlamaktadır.[5]

Sanal paraların bir türü olan kripto paralar ise genel itibariyle merkezi otoritelerin kabul ettiği ödeme araçlarına alternatif olarak geliştirilmiş, bir değerin sanal ortamda şifreleme ile güvence altına alınmış temsilidir.[6] Ancak çeşitli özel ve resmi kurumlar farklı şekillerde kripto parayı tanımlamaya çalışmaktadır. Kripto paranın tanımlanması, yapılacak regülasyonların kapsamının belirlenebilmesi için önem arz ettiğinden başlı başına ele alınması gereken bir konu haline gelmiştir. Kripto paranın tanımlanması ve var olan tanımların yeknesak hale getirilmesi için çeşitli uluslararası çalışmalar yapılmaktadır.[7]

Kripto paralar, sanal paraların blokzincir denilen dağıtık defter (*distributed ledger*) üzerinde güvenli şekilde depolanması ve aktarılması teknolojisine dayanmakta; aracı kişi ve kurumlara ihtiyaç olmadan, sınırlar arasında hızlı para transferi yapılmasını hedeflemektedir. Kripto paralar sadece blokzincir teknolojisi üzerinde işlenebilen sanal paralardır.[8] Blokzincir ise eşler arası (*peer-to-peer*) ağ aracılığıyla sürdürülmektedir. Bu eşler arası ağ tüm işlemlerin geçmişini saklar ve işlemleri takip eder. Ancak bu işlemler doğrudan kullanıcıların kimliği ile ilintili olmadığından işlemlerin kim tarafından yapıldığının takibi neredeyse imkânsız denecek kadar zordur. Blokzincir, merkezileşmemiş bir veri tabanı veya sanal kayıt defteri olarak çalışır ve işlemi dağıtılmış bilgisayar kullanıcılarıyla (*distributed computer users*) paylaşır. Bu kullanıcılar dünyanın herhangi bir yerinde bulunabilir. Blokzincir teknolojisi sayesinde banka gibi bir kuruluşa ihtiyaç duymadan eşler arası

[4] Financial Action Task Force (FATF), 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> Erişim 14 Ekim 2020.

[5] Pelin Şirin ve ark, 'Blokzinciri Teknolojisi Terminoloji Çalışması' (Türkiye Bilişim Vakfı 2019) <https://bctr.org/dokumanlar/Blokzinciri_Teknoloji_Terminoloji.pdf> Erişim 10 Haziran 2021.

[6] ibid.

[7] Örneğin, Özel Hukukun Birleştirilmesi Uluslararası Enstitüsü'nün dijital varlıklar hakkındaki çalışmasının bir ayağını terimlerin yeknesaklaştırılması oluşturmaktadır bkz. Institute for the Unification of the Private Law (UNIDROIT), 'Study LXXXII – Digital Assets and Private Law Project' (31 Haziran 2021) <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law> Erişim 6 Temmuz 2021.

[8] D. Towne Morton, 'The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy' (2020) 16 Loyola University Chicago International Law Review 129, 130.

DRAFT - TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

onay mekanizması ile işlemin doğruluğu teyit edilir. İşlemler temel olarak tek yönlüdür ve geri alınamaz.

Kripto paralar, banknot veya madeni para şeklinde değildir. Dijital karakterler şeklinde ifade edilen birimlerdir. Kripto paraların alınması, satılması veya kullanılabilmesi için bir şekilde depolanması gerekmektedir. Bu depolama araçlarına sanal cüzdan (*digital wallet*) denmektedir. Sanal cüzdan hizmeti sağlayan birçok site, bulut teknolojisi veya bilgisayar programı bulunmaktadır. Kripto paralar bu şekilde çevrimiçi sağlanan cüzdanlarda (*hot wallet*) tutulabileceği gibi, internete bağlı olmadan bilgisayar, tablet veya telefonda (*cold wallet*) da tutulabilmektedir.[9] Her iki yöntemin de güvenlik açıkları bulunmaktadır. Çevrimiçi cüzdanlar siber saldırılara maruz kalabilir, çevrimdışı cüzdanlar ise fiziksel olarak kaybedildiğinde veya çalındıklarında kripto paralar da kaybolur.[10] İki sistemdeki güvenlik açıkları kripto paraların yasadışı elde edilmelerine ve kullanılmalarına neden olabilmektedir.[11] Örneğin, Mt. Gox adlı kripto para borsası Şubat 2015'te milyonlarca Bitcoin'in çalındığını açıklamış ve iflasını istemiştir.[12] Sistemin güvenlik açıkları, terörist grupların da bu şekilde kripto paraları elde edebileceği endişesi uyandırmaktadır.

Kripto paralar kullanılarak bir işlem gerçekleştirildiğinde şifreleme yardımıyla işlem onaylandıktan sonra blokzincir üzerine eklenir. Madencilik (*mining*) ile cihazların işlemci gücünü kullanarak hesaplamalar yapılmasıyla işlemin onaylanması ve zincire eklenmesi sağlanır.[13] Blokzincir, aynı bankaların yaptığı gibi işlem geçmişini kaydeder. Birbirine internet ile bağlı binlerce bilgisayar tarafından saklanan bilgilerin doğruluğu bu şekilde denetlenmektedir. Blokzincirin geleneksel bankalardan farkı, merkezi olmaması ve bu nedenle devlet denetimine tabi olmamasıdır.[14] Kripto paralar merkezileşmemiş, dağıtılmış ve ileri düzeyde şifrelenmiş oldukları için paranın akışının tespit edilmesi oldukça zordur.[15]

Kripto paraların yaygınlaşması merkezi düzenleme ve denetleme kuruluşlarının dikkatini çekmektedir ancak kripto paraların gerçek para birimi mi, emtia mı yoksa kıymetli evrak mı olduğu konusunda görüş birliği sağlanamamaktır.[16] Statü karmaşasına örnek olarak ABD'deki farklı kurumların kripto para tanımları verilebilir. ABD Milli Gelir İdaresi (*U.S. Internal Revenue Service*

[9] Alan Brill, Lonnie Keene, 'Cryptocurrencies: The Next Generation of Terrorist Financing?' (2014) 6 Defence Against Terrorism Review 7, 11.
[10] Carmona (n 1) 130.
[11] Kim-Kwang Raymond Choo, 'Chapter 15 - Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?' in David Lee Kuo Chuen (ed.), *Handbook of Digital Currency*: *Bitcoin Innovation, Financial Instruments, and Big Data* (Academic Press 2015) 300.
[12] ibid.
[13] Carmona (n 1) 128.
[14] Morton (n 8) 130.
[15] ibid.
[16] ibid 131.

DRAFT - TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

- *IRS*), kripto paraları para değil de eşya olarak tanımlayıp vergiye tabi tutmuştur.[17] Menkul Kıymetler ve Borsalar Komisyonu (*U.S. Securities and Exchange Commission - SEC*) kripto paraları özelliklerine bağlı olarak menkul kıymet olarak değerlendirebileceklerini;[18] Vadeli Emtia İşlem Komisyonu *(Commodities Futures Trading Commission*) ise kripto paraları eşya olarak nitelendirdiklerini açıklamışlardır.[19] 2020 yılında kabul edilen Kripto Para Kanunu (*Crypto-Currency Act of 2020*), kripto paraları ABD'nin para birimini temsil eden veya blokzincir ya da dağıtık şifrelenmiş defter üzerindeki yapay türevler olarak tanımlamakta; kapsamına sabit paraları (*stable coins),* kripto emtiaları, diğer kripto paraları veya kripto menkul kıymetlerle teminat altına alınmış yapay türevleri de dahil etmektedir.[20]

25 Kasım 2013 tarihli 2013/32 sayılı belgeyle Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Bitcoin'in elektronik para olarak değerlendirilmediğini, 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun[21] kapsamında gözetimi ve denetiminin mümkün olmadığını belirtmiş; Bitcoin ve benzeri sanal paralar ile gerçekleştirilen işlemlerde tarafların kimliklerinin bilinmemesi, söz konusu sanal paraların yasadışı faaliyetlerde kullanılması için uygun bir ortam yarattığını, Bitcoin'in piyasa değerinin aşırı oynak olabilmesi, dijital cüzdanların çalınabilmesi, kaybolabilmesi veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi gibi risklerin yanı sıra yapılan işlemlerin geri döndürülemez olmasından dolayı operasyonel hatalardan ya da kötü niyetli satıcıların suistimalinden kaynaklı risklere de açık olduğu uyarısını yaparak riskleri kamuoyuyla paylaşmıştır.[22]

Sermaye Piyasası Kurulu (SPK), Kurul Karar Organı'nın 27/09/2018 tarih ve 47/1102 sayılı Kararı Uyarınca kripto para uygulamalarının birçoğunun Kurul'un gözetim ve denetimi dışında kaldığını belirterek ilk para arzlarının (*initial coin offering (ICO)*) risklerine dikkat çekmiş, kitle

DRAFT-TASLAK

[17] U.S. Internal Revenue Service (IRS), 'Notice 2014-21. Internal Revenue Service' (2014) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> Erişim 13 Kasım 2020.
[18] U.S. Securities and Exchange Commission (SEC), 'U.S. Securities and Exchange Commission: Statement on Cryptocurrencies and Initial Coin Offerings' (2017) <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11> Erişim 13 Kasım 2020.
[19] U.S. Commodity Futures Trading Commission, 'Bitcoin Basics. U.S. Commodity Futures Trading Commission' (2019) <https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf> Erişim 13 Kasım 2020.
[20] Crypto-Currency Act of 2020, H.R.6154, 116th Cong. (2020), <https://www.congress.gov/bill/116th-congress/house-bill/6154/text> Erişim 6 Temmuz 2021.
[21] 20.06.2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun (RG. 27.06.2013/28690.
[22] Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), '25 Kasım 2013 tarih ve 2013/32 sayılı Basın Açıklaması' (2013) <https://www.bddk.org.tr/Duyuru/EkGetir/510?ekId=530> Erişim 6 Temmuz 2021.

Electronic copy available at: https://ssrn.com/abstract=4083129

fonlaması (*crowdfunding*) adı altında gerçekleştirilmesi muhtemel kripto varlık satışlarına yatırımcılar tarafından itibar edilmemesi uyarısında bulunmuştur.[23]

16 Nisan 2021 tarih ve 31456 sayılı Resmî Gazete'de 30 Nisan 2021 tarihinde yürürlüğe girmek üzere yayımlanan Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik m.3(1) ile kripto varlık (*cryptoasset*) tanımı yapılmıştır.[24] Yönetmeliğin uygulanmasında 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 ifade edilmektedir. Tanımda, kripto para yerine kripto varlık ifadesi kullanılmış; bu varlıkların ne olduğundan çok ne olmadığı üzerinde durulmuştur. Kripto varlık, kapsayıcı, başka bir deyişle "şemsiye" bir tabirdir.[25] Kripto varlığın, şifreleme yöntemiyle güvence altına alınmış sanal varlıklar olduğu ve her kripto para kripto varlık olsa bile, her kripto varlık kripto para olmadığı kabul edilmektedir.[26] Kripto varlık tanımının sınırlarına yönelik farklı görüşler bulunsa da bunlar varlığın kullanım amacından ziyade (ödeme/değişim belirteçleri (*token*), menkul kıymet belirteçleri, karma amaçlı belirteçler, hizmet belirteçleri) oluşturulma ve transfer edilme teknolojiyle alakalıdır.[27] Yönetmelikteki tanım, kripto varlıklar sadece kripto paralardan ibaret olmadığından, ödeme, menkul kıymet ve diğer sermaye piyasası aracı olarak kullanılma yasağının kapsamını tüm kripto varlıklar bakımından geniş yorumlanmasına neden olabilecektir. Bununla birlikte yönetmelik, kripto para borsaları, kripto varlıkların vergilendirilmesi ve terörizmin finansmanı gibi konularda düzenleme getirmemektedir.

Sanal paralar, esas itibariyle devletler tarafından basılan ulusal para birimleri ile aynı işlevi görmeyi hedefler. Sanal paralar, ağırlıklı olarak, yerel para birimi olarak işlem görmese de ekonomik değere sahip varlıklar olarak kabul edilmektedir. Ancak devletler giderek farklı yaklaşımlar benimsemektedir. El Salvador, Bitcoin yasası ile şirketlere mal ve hizmet karşılığında Eylül 2021 itibariyle Bitcoin'in ödeme aracı olarak kabul etme gerekliliği getirmiştir.[28] Kara paranın aklanması

[23] Sermaye Piyasası Kurulu (SPK), '27/09/2018 tarih 2018/42 sayılı Sermaye Piyasası Kurulu Bülteni' (2018) https://spk.gov.tr/Bulten/Goster?year=2018&no=42

[24] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik (RG. 16.04.2021/31456).

[25] Apolline Blandin ve ark., 'Global Cryptoasset Regulatory Landscape Study' Cambridge Centre for Alternative Finance 2020) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf> Erişim 15 Haziran 2021.

[26] Global Blockchain Business Council, 'Global Standard Mapping Initiative (GSMI): Insight Report' (2020) <https://gbbcouncil.org/wp-content/uploads/2020/10/GSMI-Legal-Regulatory-Report.pdf> Erişim 15 Haziran 2021.

[27] Blandin ve ark. (n 25).

[28] Nelson Renteria, Tom Wilson, Karin Strohecker, 'In a world first, El Salvador makes bitcoin legal tender' *Reuters* (Americas, 10 Haziran 2021) <https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/> Erişim 1 Temmuz 2021.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

ve terörizmin finansmanına yönelik endişeler, bu yasadışı eylemlerin ABD doları ile gerçekleştirildiği açıklamasıyla giderilmeye çalışılmıştır.[29] El Salvador'un Bitcoin yasasını takiben Tanzanya başkanı da merkez bankasına kripto paralara yönelik değişikliklere hazırlıklı olması yönünde açıklamada bulunmuştur.[30] Öte yandan belirtildiği üzere Türkiye, kripto varlıkların ödeme aracı olarak kullanılmasını yasaklamıştır.[31] Kripto paraların nitelendirilmesine yönelik sorunlar, hem var olan hukuki çerçeveye oturtulmaları hem de gerekli yeni düzenlemelerin yapılmasını zorlaştırmaktadır.

Tartışmasız olan nokta, niteliğinin ne olduğundan bağımsız olarak, kripto paraların gerçek anlamda finansman sağlayabilmesi için bir noktada ulusal para birimlerine dönüştürülmesi gerektiğidir.[32] Bunun için sanal para borsa (*exchange*) siteleri kullanılmaktadır. Ancak son zamanlarda sanal ve gerçek para arasındaki çizgi ortadan kalkmaya başlamıştır. Örneğin, çok fazla sayıda kullanıcısı olan çevrimiçi oyunlarda elde edilen sanal gelirler, aracı siteler üzerinden doğrudan gerçek para birimlerine aktarılmaya başlanmıştır.[33] Kendi sanal para birimi olan Second-life gibi oyun platformları sanal paraların kullanım alanını genişletmektedir.[34] Bu, sanal paraların kullanımlarının yaygınlaştığını ve geçerli ekonomik değere dönüştüğünü göstermekte, sanal paraların ulusal para birimlerine dönüştürülmeden para aktarım aracı olarak kullanılabileceği anlaşılmaktadır. İnternet üzerinden yapılan işlemlerde kullanılan sanal paralar gibi gelişen yeni teknolojiler terörist kullanımları kolaylaştırmakta, devletler tarafından terörist eylemlerin takibini zorlaştırmaktadır.[35]

## 2. Terör Örgütlerinin Finansman İhtiyaçları ve Finansmanın Sağlanması

### 2.1. Terörizmin Finansmanı

Terör örgütleri ihtiyaçlarını karşılayabilmek, eylemlerine devam edebilmek, silah edinmek ve hareket edebilmek için önemli miktarda finansmana ihtiyaç duymaktadır.[36] Terörizmin finansmanı

[29] ibid
[30] Samuel Haig, 'Tanzanian president urges central bank to prepare for crypto' (*Cointelegraph*, 14 Haziran 2021) <https://cointelegraph.com/news/tanzanian-president-urges-central-bank-to-prepare-for-crypto> Erişim 1 Temmuz 2021); Robert Hart, 'Tanzania considers crypto and boosts bitcoin as nations line upbehind El Salvador to embrace decentralized finance' (*Forbes,* 14 Haziran 2021) <https://www.forbes.com/sites/roberthart/2021/06/14/tanzania-considers-crypto-and-boosts-bitcoin-as-nations-line-up-behind-el-salvador-to-embrace-decentralized-finance/?sh=64fc2a944fc3> Erişim 1 Temmuz 2021.
[31] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik (n 24).
[32] Brill (n 9) 11.
[33] Angela Irwin, Jill Slay, 'Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft' (International Cyber Resilience Conference, Perth Western Australia: Edith Cowan University, 2010) <http://ro.ecu.edu.au/icr/5> Erişim 1 Aralık 2020) 43.
[34] Michael Jacobson, 'Terrorist Financing and the Internet' (2010) 33 Studies in Conflict & Terrorism 353, 360.
[35] ibid
[36] Brigitte L. Nacos, *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post-9/11 World* (Pearson Education Inc. 2008) 226.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

başlı başına suç teşkil etmekte, bu suçun oluşması için öncül bir eylem veya finanse edilen eylemin gerçekleşmiş olması şartları aranmamaktadır.[37] Bu nedenle terörün finansmanı

> Bir terör suçunun işlenmesinde katkısı olacağını bilerek ve/veya terörist saldırıda kullanılmasını isteyerek, amaçlanan terör eylemi gerçekleştirilmiş olsun veya olmasın; terör örgütüne, örgüt üyesine veya örgüt üyesi olmasa bile terör suçunu işleyecek olan faile ulaşması kastıyla, para ve/veya taşınır taşınmaz, hak, alacak, gelir, menfaat gibi karşılığı para ile ölçülebilen ya da paraya tahvil edilebilen her türlü iktisadi değerin herhangi bir yöntemle toplanması veya temin edilmesi

şeklinde tanımlanabilmektedir.[38]

Terör örgütleri, maddi kaynaklarını hem yasal hem de yasa dışı yollarla elde edebilmektedir. Terörün finansmanında başvurulan dört ana yöntemin devlet sponsorluğu, özel kuruluşların desteği veya bireysel bağışlar, terör örgütlerinin yasal işler aracılığıyla elde ettikleri gelirler ve yasadışı faaliyetlerle elde edilen gelirler olduğu belirtilmektedir.[39] Devlet sponsorluğuyla, genellikle dolaylı yolla yapılmakta, teröristlere yaşam ve eğitim alanlarının sağlanması, silah temini, nakit akışının sağlanması gibi konularda destek verilmesi amaçlanır. İran'ın Hizbullah'a verdiği destek bunun örneği olarak gösterilmektedir.[40]

Özel kuruluşların desteği veya bireysel bağışlar, terör örgütünün amaçlarının bu kuruluş ve bireyler tarafından benimsenmesiyle paralellik göstermektedir. Genellikle örgütlerin en az zarar verdiği veya örgütlerin ortaya çıktığı bölgelerdeki kuruluş veya kişilerce desteklenmektedir. Filistin Hamas örgütünün eğitim imkanları, sağlık yardımı ve diğer sosyal hizmetleri sunarken, silahlı güçlerinin terörist eylemlerde bulunduğu bilinmektedir.[41] Kripto paralar, kişilerin anonim kalmasını temin ettiğinden, kimliklerini belli etmekten çekinen bireysel bağışçıların veya özel kuruluşların desteğiyle para toplanması için uygun bir ortam sağlamaktadır. Örneğin, 2017'de El-Kaide ile bağlantılı sosyal medya hesapları üzerinden Suriye'de eylemlerini sürdüren Sadaka adlı örgüt, Bitcoin, Monero ve Dash gibi kripto paralar aracılılığıyla destek toplamıştır.[42]

---

[37] Mehmet Gödekli, *Terörizmin Finansmanı Suçu* (Seçkin Yayınları 2017) 55.
[38] ibid
[39] Nacos (n 36) 227.
[40] Cynthia Dion-Schwarz, David Manheim, ve Patrick B Johnston, *Terrorist Use of Cryptocurrencies* (RAND Corporation 2019) <https://www.rand.org/pubs/research_reports/RR3026.html> Erişim 15 Haziran 2021), xii.
[41] Lara Pham, 'Terrorism and charity: defining Hamas' (*World Policy,* 8 Ağustos 2014) <http://worldpolicy.org/2014/08/08/terrorism-and-charity-defining-hamas/> Erişim 13 Şubat 2021.
[42] Tom Keatinge, David Carlisle, Florence Keen, 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses' (European Parliament 2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf> Erişim 13 Kasım 2020) 34.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Terör örgütlerinin yasal iş ve işletmeler aracılığıyla finansmanın sağlanması en olağandışı yöntem olarak görülse de çeşitli eşyaların çevrimiçi yollarla satışı ile finansman sağladıkları görülmektedir.[43] Kripto paralarla ödeme yasağı, kısıtlı da olsa bu tür eylemlerin önüne geçilmesinde etkili olabilecektir.

Yasadışı faaliyetlerle elde edilen gelirler ise terör örgütlerinin banka soygunları, fidye için adam kaçırma, tehdit ve uyuşturucu kaçakçılığı, kara para aklama gibi yasadışı eylemlerine dayanmaktadır. Kripto paraların aklanması ise bu gruba dahil olarak yeni bir yasadışı finansman yöntemi olarak karşımıza çıkmaktadır. Kara paranın aklanması ve terörün finansmanı suçlarında faillerin saikleri arasında farklılık bulunabilir.[44] Terör amacı olmadan bireysel çıkarlar için kara paranın aklanması söz konusu olabilir. Ancak, her iki durumda da faillerin kullandıkları yöntemler benzerdir. Bu nedenle kara paranın aklanması ve terörün finansmanının engellenmesi ile genellikle birlikte mücadele edilmeye çalışılır. Kripto paralar da hem kara para aklama hem de terörün finansmanında kullanılabileceğinden bu iki kavramın birlikte ele alınması gerekliliği doğmuştur.

Terörün finansmanında önemli diğer bir nokta, belirtilen yöntemlerle temin edilen fonların transferinin gerçekleştirilmesidir. Fon transferinde para kuryeleri, gayri-resmi aktarım sistemleri, para hizmet sağlayıcıları, resmi bankacılık, sahte ticari faturalama ve yüksek meblağlı eşyaların yaygın şekilde kullanıldığı belirtilmektedir.[45] Sivil toplum örgütleri ve vakıflar, ön ödemeli araçlar, mobil ve kripto para gibi sanal ödeme sistemleri de bunlara eklenmektedir.[46] Fonların aktarılması sırasında kullanılacak yöntem, aktarılabilecek paranın hacmi, denetim mekanizmalarıyla karşılaşma riski, kişilerin bulundukları konuma göre uygunluk, atılacak adımların azlığı ve kolaylığı, transfer masrafları ve aktarım hızına göre seçilmektedir.[47] Kripto paralar fonların transferinde aranan bu özellikleri kolaylaştırdığı veya desteklediğinden terörün finansmanıyla temin edilen fonların aktarımı için kullanılmalarında etkili olmaktadır. Kripto paraların olumlu ekonomik ve sosyal etkileri olsa da yasadışı kullanımlarının önüne geçilmesi için tedbirler alınması gerektiği anlaşılmaktadır.

DRAFT-TASLAK

[43] Cohen-Almagor R, 'Jihad Online: How Do Terrorists Use the Internet?' F Freire, X Araújo Rúas, Fernández V Martínez, X García (ed.) *Media and Metamedia Management: Advances in Intelligent Systems and Computing* (Springer 2017) 5.
[44] Nacos (n 36).
[45] Michael Freeman, Ruehsen Moyara, 'Terrorism Financing Methods: An Overview' (2013) 7 Perspectives on Terrorism 5, 7-20.
[46] Dion-Schwarz (n 40) 12.
[47] Freeman (n 45) 7.

Electronic copy available at: https://ssrn.com/abstract=4083129

## 2.2.Kripto Paraların Terörizmin Finansmanında Kullanılması

### 2.2.1. Kripto paraların özellikleri ve tercih edilmesindeki etmenler

11 Eylül olaylarından sonra terörizmle mücadele kapsamında terörizmin finansmanın önüne geçilmesi için tedbirler sıkılaştırılmaya başlanmış, bankacılık sektöründe de denetim artırılmıştır.[48] Bunun üzerine teröristler, finansman sağlanmak için daha gizli ve denetimden uzak mekanizmalar aramaya başlamıştır.[49] Örneğin, 2011 yılında Norveç'te terörist Anders Behring Breivik'in saldırısı neticesinde 77 kişinin ölüp 242 kişinin yaralandığı olayda birden çok kredi kartı vasıtasıyla şirketin kıyı ötesi banka hesaplarındaki fonlardan para temin edildiği ortaya çıkarılmıştır.[50] Bu saldırı resmi bankacılığın denetiminden sıyırılarak gerçekleştirildiğinden terörün finansmanda kullanılabilecek alternatif yöntemler dikkatleri üzerine çekmiştir.

Kripto paraların sahaya çıkması ve her geçen gün yeni tür kripto paranın piyasaya sürülmesiyle terörün finansmanın takibi önemli ölçüde zorlaşmıştır.[51] 2015 tarihli rapora göre Avrupa'daki yasadışı işlemlerin %40'ında kripto paraların kullanıldığı tespit edilmiştir.[52] Takibi oldukça zor olan ve yüzlerce çeşidi bulunan kripto paralar, terörün finansmanın kontrol altına alınması bakımından endişe uyandırmaktadır.[53] Kripto paraların bunların yanında kendilerine has bazı özellikleri terörün finansmanında benimsenen konvansiyonel yöntemlere tercih edilmelerine neden olmaktadır.

Kripto paraların tercih edilmesini sağlayan başlıca özellikleri, anonim olmaları (*anonimity*), kullanılabilirlik (*usability*), güvenlik (*security*), geçerlilik (*acceptance*), güvenilirlik (*reliability*) ve işlem hacmi (*volume*) olarak belirtilmektedir.[54] Kripto paraların anonim olması, kullanıcının kimliğinin korunması ve/veya saklanabilmesini ifade etmektedir.[55] Anonim olmak, teröristler, kara para aklama suçluları ve diğer yasadışı işlerin failleri için her ne kadar gerekli olsa da tek başına suç işlendiğini kanıtlamamaktadır.[56] Sıradan vatandaşlar da birtakım eylemleri bakımından anonim olmanın güvencesine sığınmak istemektedir. Örneğin, Ukrayna'dason zamanlarda, hem hükümeti

[48] Iwa Salami, 'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?' (2018) 41 Studies in Conflict and Terrorism 968, 969.
[49] ibid
[50] Matthew Taylor, 'Norway gunman claims he had nine-year plan to finance attacks' *The Guardian* (Norveç, 25 Temmuz 2011) <https://www.theguardian.com/world/2011/jul/25/norway-gunman-attack-funding-claim> Erişim 14 Kasım 2020.
[51] Salami (n 48); Pankaj C. Patel, Igor Pereira, 'The Relationship between Terrorist Attacks and Cryptocurrency Returns' (2020) *Applied Economics* 1, 2.
[52] European Law Enforcement Agency (EUROPOL), 'The Internet Organised Crime Threat Assessment (IOCTA) 2015' (20 Haziran 2017) <https://op.europa.eu/s/pkP9> Erişim 14 Kasım 2020) 46.
[53] Salami (n 48); Pankaj (n 47).
[54] Dion-Schwarz (n 40) 23.
[55] ibid
[56] Brill (n 9) 14.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

destekleyen hem de muhalif vatandaşların "fişlenmemek" adına politik görüşlerini savunmak için internet ortamında anonim kalmayı tercih etmesi, anonim kalmanın sadece suç teşkil eden fiillerin gerçekleştirilmesinde değil; vatandaşların yasal yollarla görüşlerini savunmaları sırasında da duyulan birihtiyaç olduğunu göstermektedir.[57]

Anonimliğin sağlanması tek başına terör eylemi gerçekleştirildiğinin belirteci olmasa da, terör eylemlerinde anonimlik önem arz etmektedir. ABD tarihinin en büyük kara para aklama vakası olarak tanımlanan Liberty Reserve davası buna örnek olarak verilmektedir.[58] Liberty Reserve, elektronik ödeme sistemi olan PayPal[59] ile benzer bir işlev yürüten merkezi sanal para hizmet sağlayıcısı olarak kullanıcıların birbirlerine sadece isim, eposta adresi ve doğum tarihi girerek para transfer etmelerini sağlamış; kullanıcıların kimlikleri araştırılmamış veya doğrulanmamıştır.[60] Kullanıcılar, banka hesaplarından parayı üçüncü taraf borsalara aktarmışlardır. Bu borsalar, tam anlamıyla denetlenmeyen para iletimi sağlayan işletmelerdir. Borsa, kendisine havale edilen parayı kripto paraya çevirerek takip edilemez duruma getirmiştir. Sanal para Liberty Reserve'deki hesaba yatırılmış ve bu şekilde para aklanmıştır. Kripto para teknolojisi kullanıldığından, tüm işlemler tek taraflı ve geri dönüştürülemez şekilde gerçekleştirilmiştir.[61]

Diğer bir özellik olarak kullanılabilirlik, kullanıcının işlemleri yerine getirmesi ve parasını yönetmesindeki kolaylıktır.[62] Kripto paranın tercih edilmesi için teknik bilgi sahibi olmayan kişiler tarafından da kolaylıkla kullanılabilir olması gerekmektedir. Bu noktada borsalar son kullanıcıya ulaşılmasına önem arz etmektedir. Aynı zamanda kullanılabilirlik açısından komisyon miktarının olabildiğince az olması ve bu sayede hem büyük hem de küçük meblağlı transferlerin yapılabilmesi sağlanmalıdır.[63] Ancak, kripto paraların transferinde artan komisyon miktarları, bunun neticesinde yavaşlayan işlemler kripto paraların kolay kullanılması veya erişilmesinin önünde engel teşkil edebilecektir.[64]

DRAFT-TASLAK

[57] ibid
[58] Salami (n 48) 969-7.
[59] PayPal para gönderme ve talep etmeyi sağlayan çevrimiçi ödeme kuruluşudur. 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun uyarınca ödeme kuruluşlarının izin alması gerekmektedir. PayPal'in alt düzenlemelere dayanarak yaptığı izin başvurusu reddedilmiş, kuruluş 2016 yılından itibaren Türkiye'deki faaliyetlerini durdurmuştur. bkz. 6493 sayılı Kanun (n 21).
[60] Salami (n 48) 969-7.
[61] ibid
[62] Dion-Schwarz (n 40) 23.
[63] Brill (n 9) 14.
[64] Bitcoin işlem ücretlerinin en yüksek meblağa ulaştığı hakkında bkz. Colin Harper, 'Bitcoin transaction fees more expensive than ever' (*Coindesk,* 21 Nisan 2021) <https://www.coindesk.com/bitcoin-transaction-fees-more-expensive-than-ever> Erişim 1 Temmuz 2021.

Electronic copy available at: https://ssrn.com/abstract=4083129

Güvenlik ise işlemlerin ve kullanıcı hesaplarının gizliliği, bütünlüğü ve doğruluğunun ne derecede sağlandığı ile ilgilidir.[65] Geçerlilik, kullanıcı topluluğu tarafından ne derece kabul edildiği ve bu topluluğun ne derece büyük olduğunu ifade etmektedir.[66] Güvenilirlik kullanıcıların gözünde işlemlerin hızı ve erişilebilirliğini göstermektedir.[67] İşlem hacmi ise kripto para alt yapısında gerçekleşen ortalama zaman dilimindeki toplam işlem sayısıdır.[68] Tüm bu özellikler kripto paraların yasal veya yasadışı amaç güden tüm kullanıcılar tarafından ulusal para birimlerine karşı tercih edilmesinde etkili olan unsurlar olarak karşımıza çıkmaktadır. Anonimlik başta olmak üzere, kullanım kolaylığı, işlemlerin güvenli ve hızlı şekilde gerçekleştirilmesiyle daha çok kişi tarafından kullanılmaya başlaması da terör finansörlerinin ilgisini çekmektedir.[69]

### 2.2.2. Kripto paraların dezavantajları

Kripto paraların tercih edilmesini sağlayan özelliklerinin yanında birtakım dezavantajları bulunmaktadır. Yasal kullanıcıların karşılaştıkları risk ve sorunlarla terörist oluşumlar da karşılaşmaktadırlar. Kripto paraların tercih etmelerinin önüne geçen faktörlerden bazıları şu şekilde sırlanmaktadır: Kripto paranın değeri sürekli ve öngörülmeyen şekillerde değişebilmektedir. Kripto paraların tutulduğu cüzdanlar çalınabilir veya *hack*'lenebilir. Ulusal ve uluslararası düzeyde hükümet yetkilileri ve kolluk tarafından sanal paraların takibindeki uzmanlığın artması da teröristlerin kripto paraları tercih etmemelerinde etkili olmaktadır.[70] Ek olarak, teröristlerin yeterli düzeyde madencilik (*mining*) yapamayacakları; bu nedenle finansman aracı olarak kripto paraları tercih etmeyecekleri de düşünülmektedir.[71] Her ne kadar yeterli teknik alt yapılarının bulunmaması teröristlerin kripto paraları tercih etmeyeceklerini düşündürse de teknik desteği dışarıdan sağlayabilecekleri savunulmaktadır.[72] Nitekim, 2015 yılında Amerikalı bir genç IŞİD'e Twitter üzerinden Bitcoin kullanarak nasıl fon sağlayabileceklerine ilişkin önerilerde bulunmuş; bu nedenle hapis cezası almıştır.[73]

Kripto paraların tercih edilmesini engelleyen bir diğer unsur kolluk tarafından yapılabilen siber saldırılardır. Kolluk tarafından çevrimdışı saldırılar, pasif veya aktif saldırılar, açık saldırılar

---

[65] Dion-Schwarz (n 40) 23.
[66] ibid
[67] ibid
[68] ibid
[69] Daniel Eisermann, 'Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges' (Berlin Risk 2020) <https://www.counterextremism.com/sites/default/files/Cryptocurrencies%20as%20Threats%20to%20Public%20Security%20and%20Counter-Terrorism_ENG%20Translation_April%202020.pdf> Erişim 5 temmuz 2021) 223.
[70] Brill (n 9) 15.
[71] Carmona (n 3) 132.
[72] ibid
[73] Eisermann (n 69) 24.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

veya karmaşık teknik bilgi gerektiren yöntemler kullanılarak terörist grupların kripto paraları kullanmasının önüne geçilebilmektedir.[74] Ancak birçok ülkede kolluk güçlerinin teknik bilgisinin yetersiz kaldığı ve gerekli korumanın sağlanamadığı görülmektedir. Ayrıca kripto paraların yaygınlaşması ve anonim şekilde kullanılması, düzenleme ve denetimlerin yetersiz kalması, Bitcoin dışında alternatif para birimlerinin sağladığı pazarın genişlemesinin terör örgütlerinin kripto paraları finansman aracı olarak kullanmalarını artıracağı öngörülmektedir.[75] Yasadışı oluşumların yıllara göre arttığı tespit edilmiştir.[76]

Bitcoin en yaygın kripto para olsa da Bitcoin dışında birçok kripto para türü bulunmaktadır. Gizlilik özellikleri nedeniyle Zcash, Monero, ve Dash gibi kripto paraların blokzincir analiz teknikleri kullanılarak tespit ve takip edilmesi daha zordur.[77] Özellikle Monero'nun, karanlık ağ pazarında daha çok benimsenmeye başlandığı bilinmektedir.[78] Kripto paraların terör örgütlerinin finansman ihtiyaçlarının tamamına cevap vermeyeceğini savunan görüşün aksine sanal paralar aracılığıyla terör finansmanı sağlanmasının gerçek bir tehdit olduğu da anlaşılmaktadır.[79] Şu anda kripto paraların genel bir ödeme yöntemi olarak kabul edilmemesi nedeniyle borsalar (*exchanges*) aracılığıyla ulusal paraya dönüştürülebiliyor olması para akışının takibini bir nebze kolaylaştırmaktadır; ancak ülkelerin veya kuruluşların El Salvador örneğinde olduğu gibi kripto paraların doğrudan harcanabilir para birimleri olarak kabul etmeleri durumunda paranın akışının takip edilmesinin engelleneceği düşünülmektedir.[80] Bu konuda terazinin iki farklı kolundaki kripto paraların geçerli para birimleri olarak kabul edildiği ve ödeme aracı olarak yasaklandığı ülkelerdeki gelişmelerin yakından takip edilmesi önemlidir. Her geçen gün daha karmaşık protokollerle gelişen ve takibi zorlaşan kripto paraların dikkatle irdelenmesi ve düzenlenmelerin daha temkinli yapılması gerektiği anlaşılmaktadır.

### 2.2.3. Terör örgütlerinin kripto para aracılığıyla fon toplama etkinlikleri

Şu anda kullanılan hiçbir kripto paranın terör örgütlerinin yukarıda açıklanan finansal ihtiyaçlarını karşılamaya elverişli olmadığı düşülmektedir.[81] Ancak belirtilen finansal aktiviteler arasından bağış toplama için Bitcoin gibi kripto paraların kullanıldığı bilinmektedir.[82] Borsalar

[74] Dion-Schwarz (n 40) 45.
[75] ibid 45-55.
[76] Yaya J. Fanusie, Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (Elliptic/Foundation for Defense of Democracies, 2018) <https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf> Erişim 14 Kasım 2020) 4.
[77] ibid 13.
[78] ibid
[79] Salami (n 48) 985.
[80] Rumer Ramsey, 'An Examination of the Challenges Posed by Cryptocurrencies to AML/CTF Regulation' (2020) 12 Amsterdam Law Forum 1, 3.
[81] Dion-Schwarz (n 40) 35.
[82] ibid

DRAFT TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

(*exchanges*), karıştırıcılar (*mixers/tumblers*) ve kumar siteleri, Bitcoin'in aklandığı başlıca platformlardır.[83] 2013-2016 yılları arasında kamuya açık Bitcoin blokzinciri üzerinde yapılan analize göre yarım milyonun üzerinde Bitcoin'in yasadışı kaynaklardan dönüştürme sağlayıcılarına (*conversion providers*) aktarılmıştır.[84] Yasadışı Bitcoin işlemlerinin bu sayıdan daha fazla olduğu düşünülmektedir.[85]

Yasadışı eylemlerin fonlanması için sanal paraların kullanılmasında en önemli olaylardan biri Silk Road davasıdır. Silk Road, uyuşturucu, silah, çalınmış kimlik bilgileri ve diğer yasadışı eşyaların satışı için tasarlanmış internet sitesidir.[86] Silk Road olayında Bitcoin "karanlık ağ" üzerinden yetkililer tarafından fark edilmeyecek şekilde aktarılmıştır.[87] Kullanıcılar işlemlerinde Bitcoin aracılığıyla gerçekleştirildiğinden kimliklerini saklayabilmişlerdir.[88] Buna ek olarak, kullanıcılar her bir işlem için yeni bir Bitcoin adresi edinebildiğinden ve site aynı zamanda karıştırıcı (*mixer/tumbler*) kullandığından kullanıcı ile Bitcoin arasındaki bağın kurulması engellenmiştir.[89] Yaklaşık 1,2 milyar dolar toplanan ve Şubat 2011'de açılan site, 2013'te kapatılmıştır.[90] Yasadışı oluşumların %90'ının Silk Road'dan kaynaklandığı görülmüştür.[91]

Bir diğer finansal aktivite olan fonların transferinde de kripto paraların tercih edildiği görülmektedir. Western Express International adlı uluslararası suç örgütü, çalıntı kredi kartı ve kişisel bilgi kaçakçılığı amacıyla anonim sanal paralar kullanmıştır.[92] Western Express, kripto para borsası (*exchange*) olarak kurulan bir şirkettir. Toplamda sanal para karşılığı 35 milyon doların transferini gerçekleştirmiştir.[93] Örgütsel oluşumların yanında, IŞİD için para aklarken Bitcoin'den yararlanılması gibi bireysel olarak gerçekleştirilen eylemlerde de kripto paraların kullanıldığı da görülmektedir.[94]

## 3. Kara Para Aklama ve Terörün Finansmanının Önlenmesi Hakkındaki Düzenlemeler ile Bunların Kripto Paralar Bağlamında Eksiklikleri

[83] Fanusie (n 76) 6.
[84] ibid 3.
[85] ibid 4.
[86] Lawrence Trautman, 'Virtual Currencies. Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox' (2014) 20 Richmond Journalof Law & Technology 1, 92.
[87] Salami (n 48) 970.
[88] FATF (n 4) 11.
[89] Trautman (n 86).
[90] FATF (n 4) 11; Salami (n 48) 970.
[91] Fanusie (n 76) 4.
[92] FATF (n 4) 12.
[93] ibid
[94] Dan Mangan, 'New York woman pleads guilty to using bitcoin to launder money for terror group ISIS' *CNBC* (2020) <https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html> Erişim 14 Kasım 2020.

DRAFT - TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Terörizmin finansmanı ve kara paranın aklanması hakkında ulusal ve uluslararası düzenlemeler bulunmaktadır. Bu düzenlemeler kripto paraları kapsayacak şekilde yorumlanabilecek olsa da kripto para kullanıcılarının ve kullanma şekillerinin takibinde yetersiz kalmaktadır.

Terörizmin finansmanı suç olarak kabul edilmiş ve önlenmesi için çeşitli düzenlemeler yapılmıştır. Terörizmin finansmanının önlenmesindeki en önemli düzenlemelerden biri Birleşmiş Milletler Genel Kurulu tarafından 9 Aralık 1999'da kabul edilen Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme'dir ("BM TFÖ Sözleşmesi").[95] Sözleşme m.2'de her ne suretle olursa olsun, tümüyle veya kısmen, aynı maddede sayılan eylemlerin gerçekleştirilmesinde kullanılması niyetiyle veya kullanılacağını bilerek, doğrudan veya dolaylı olarak, yasa dışı bir şekilde ve kasten, fon sağlanmasını ihlal olarak saymaktadır. Sözleşme m.1'de fon kavramının içine her türlü kıymeti ve bunların elektronik veya dijital şekilleri de dahil edilmiştir.[96] Kripto paraların yasadışı yollarla kullanımının Sözleşme kapsamına gireceği şüphesizdir. Ancak kripto paraların kullanımının kendisi yasa dışı olmadığından ve takipleri zor olduğundan hangi noktada "yasa dışı fon sağlanması"na katkı sağladıkları belirlenemeyecektir.

6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun uyarınca,[97] bir halkı korkutmak veya sindirmek ya da bir hükûmeti veya uluslararası kuruluşu herhangi bir eylemi gerçekleştirmeye veya gerçekleştirmekten kaçınmaya zorlamak amacıyla, kasten öldürme veya ağır yaralama fiilleri, 3713 sayılı Terörle Mücadele Kanunu[98] kapsamında terör suçu olarak kabul edilen fiilleri ve Türkiye'nin taraf olduğu terörün önlenmesine yönelik uluslararası antlaşmalarda suç olarak kabul edilen fiilleri gerçekleştirmek amacıyla fon sağlanması ve toplanması yasaklanmıştır. Fon ise para veya değeri para ile temsil edilebilen her türlü mal, hak, alacak, gelir ve menfaat ile, bunların birbirine dönüştürülmesinden hasıl olan menfaat ve değer olarak tanımlanmıştır. BM TFÖ Sözleşmesi'nden farklı olarak dijital ifadesine yer verilmese de hükmün oldukça geniş olduğu bu nedenle ekonomik değeri olan kripto paraların da bu kanun kapsamında fon sayılabileceği düşünülebilir.

---

[95] Birleşmiş Milletler Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme (*International Convention for the Suppression of the Financing of Terrorism*) (kabul tarihi 9 Aralık 1999 BM Genel Kurul Kararı No A/RES/59/109, yürürlük tarihi 10 Nisan 2002, 2178 UNTS 197) (BM TFÖ Sözleşmesi). BM TFÖ Sözleşmesi, Türkiye adına, 27 Eylül 2001 tarihinde imzalanmış, 10 Ocak 2002'de kabul edilen 4738 sayılı Kanun ile onaylanması uygun bulunmuş ve 1 Nisan 2002 tarihli Resmi Gazete'de yayımlanmıştır.

[96] ibid m.1. ("Fon her ne suretle edinilmiş olursa olsun, maddi veya gayri maddi, menkul veya gayrimenkul, her türlü kıymeti ve bu kıymetler üzerinde bir mülkiyet hakkı veya çıkarı kanıtlayan, elektronik veya dijital şekilleri dahil olmak üzere, her türlü görünüşteki belge ve yasal araçları ve bu çerçevede banka kredilerini, seyahat çeklerini, para havalelerini, hisse senetlerini, teminatları, tahvilleri, kredi mektuplarını, işbu tadat sınırlayıcı olmaksızın kapsar.")

[97] 07.02.2013 tarihli ve 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun (RG. 16.02.2013/28561)

[98] 12.04.1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu (RG. 12.04.1991/20843).

DRAFT TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Terörün finansmanını engellemeye yönelik düzenlemelerle yetinilmeyerek, terörle mücadelede klasik yöntemlerin işe yaramadığının anlaşılması üzerine, terör örgütlerini gelirlerinden mahrum bırakmak için kara para aklama fiili de açıkça suç olarak tanınmış ve terörün finansmanını engellemeye yönelik adımlar atılmaya başlanmıştır.[99] Türk Ceza Kanunu'nun m.282 atfıyla[100] 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun uyarınca "*Alt sınırı altı ay veya daha fazla hapis cezasını gerektiren bir suçtan kaynaklanan malvarlığı değerlerini, yurt dışına çıkaran veya bunların gayrimeşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak*" ifadesiyle kara para aklama da suç olarak kabul edilmiştir.[101]

Kara paranın aklanması ve terörün finansmanı eylemleri geleneksel olarak finansal işlemlerin katı şekilde bildirimi gerektiren prosedürlerin uygulanması sayesinde belirlenip soruşturulabilmektedir.[102] Bu prosedürler şüpheli konuların, olağandışı anlaşmaların ve uluslararası havalelerin tespit edilmesini amaçlamaktadır.[103] Terörizmin finansmanı ile mücadelede terör örgütünün fon toplamasının engellenmesi, kullanılan fonların tespit edilmesi ve bunlara el konulması, fonların aktarılma yollarının takibinin de engellenmesi hedeflenmektedir.[104] BM TFÖ Sözleşmesi m. 8.1 uyarınca da bu adımların takip edilmesi gerekmektedir.[105]

Amerika Birleşik Devletleri Hazinesi'ne bağlı olan Finansal Suçlar İnfaz Ağı (*Financial Crimes Enforcement Network* (*FinCen*)) kara para aklama suçunu yasadışı yollarla edinilmiş gelirlerin yasal gibi gösterilmesi süreci olarak tanımlamakta ve bunun için üç adımın benimsenmiş olabileceğini belirtmektedir: 1) kara paranın yasal finansal sisteme yerleştirilmesi (*yerleştirme (placement)*), 2) kaynağını örtmek için ek işlemler yapılması (*ayrıştırma (layering)*) ve 3) yasal olarak gözükmesi için daha fazla işlemle finansal siteme entegre edilmesi (*bütünleştirme (integration)*).[106] T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu (MASAK) da genellikle aynı adımların izlendiğini belirtmektedir.[107]

Buradan yola çıkıldığında, klasik anlamda kara para aklama ve terör finansmanın tespitinde şu aşamaların bulunduğu belirtilmektedir: Yasadışı yollarla elde edilen fonlar finansal bir kuruluşa

[99] Gödekli (n 37) 54.
[100] 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu (RG. 12.10.2004/25611).
[101] 11.10.2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun (RG. 18.10.2006/26323).
[102] Irwin (n 33) 44.
[103] ibid
[104] Gödekli (n 37) 54.
[105] BM TFÖ Sözleşmesi (n 95) m.8.1: "Her Taraf Devlet, gerektiğinde müsadere edilebilmeleri amacıyla., 2. maddede belirtilen suçların işlenmesi için kullanılan, veya kullanılması için oluşturulan fonların veya bu suçlardan temin edilen kazançların tespiti, bulunması, dondurulması, el konulması için iç hukuku uyarınca gerekli tedbirleri alır."
[106] U.S. Department of the Treasury, 'Financial Crimes Enforcement Network: History of Anti-Money Laundering Laws' <https://www.fincen.gov/history-anti-money-laundering-laws> Erişim 13 Kasım 2020.
[107] TC Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu (MASAK), 'Aklamanın Aşamaları' <https://masak.hmb.gov.tr/aklamanin-asamalari> Erişim 1 Aralık 2020.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

yerleştirilmeye çalışılır. Finansal kuruluş bu işlemden şüphelenir ve bunun araştırılması için ilgili devlet kurumuna yönlendirilir. Kolluk ve yargı merciinin sürece dahil olması ileşüpheli sorgulanır ya da yargılanır.[108] Halihazırda yürürlükte olan düzenlemeler sanal ortamlara uzanmamaktadır. Bu nedenle sanal ortamda gerçekleştirilen kara para aklama ve terörün finansmanında yasadışı yollarla elde edilen fonlar finansal bir kuruluşa yerleştirilmeye çalışılır.[109] Ancak finansal kuruluşların kontrol eksikliği ve kripto paralara yönelik yasal düzenlemelerin olmaması nedeniyle klasik yöntemler izlenememekte, sanal ortamdaki kara para aklama ve terörün finansmanının önüne kolaylıkla geçilememektedir.[110] Kripto paralar takip edilemediğinden malvarlıklarının dondurulması, fon toplamasının engellenmesi, kullanılan fonların tespit edilmesi ve bunlara el konulması gibi tedbirler uygulanamamaktadır.[111]

Ek olarak, kripto paraların dayandığı blokzincir teknolojisi sınır ötesi nitelik taşımaktadır. Teknoloji, farklı ülkelerde bulunan birden çok bilgisayarın dağınık şekilde verileri işlemesi mantığına dayandığından herhangi bir devletin yetki beyanında bulunup kendi kanunlarını uygulaması da sorun teşkil etmektedir. BM TFÖ Sözleşmesi, yetki tesis edilen durumlarda nasıl hareket edilmesi gerektiğine ilişkin hükümler içermektedir. Örneğin, BM TFÖ Sözleşmesi m. 3, 7, 11, 16, 22'de devletlerin yetkisine ilişkin hükümler bulunmaktadır. Yetki tesisinde ülkesellik ve vatandaşlık ilkelerinin benimsendiğini söylememiz mümkündür. Bununla birlikte BM TFÖ Sözleşmesi siber uzayda yetkinin nasıl tesis edileceğini belirlemediğinden bu husus açıkta kalmaktadır. Aynı şekilde kripto paralar ve blokzincir dağıtık şekilde farklı ülkelerde bulunduklarından ve veriler sürekli hareket halinde olduğundan hangi ülkenin yetkisi altında olacağı sorusuna şu anki düzenlemeler cevapsız kalmaktadır. Sonuç itibariyle, kripto paraların terörizmin finansmanında kullanılması, belirtilen düzenlemelerin kapsamına girecek şekilde yorumlanabilir. Ancak düzenlemeler kripto paraların kullanıcılarının ve kullanma şekillerinin takibinde yetersiz kalmakta; bu sorunlar aşılsa dahi sınır ötesi yetki kullanma meselesiyle karşılaşılmaktadır.

Siber uzayın düzenlenmemiş olmasının hızla değişmeye başladığı ve yakın zamanda katı kurallar ve düzenlemelerin getirileceği öngörülmektedir.[112] Kara para aklama ve terörün finansmanı özellikle finansal düzenlemeleri ile yasalarının yaptırım gücünün zayıf olduğu ülkeler ile ilişkilendirildiğinden ülkelerin ulusal düzeyde birtakım düzenlemeler yapmaları önerilmektedir.[113] Bu ülkelerde başlangıç olarak sanal paralar kullanılarak yasadışı eylemlerin gerçekleştirilmesi için

[108] Irwin (n 33) 46.
[109] ibid
[110] Eisermann (n 69) 23.
[111] ibid
[112] Irwin (n 33108) 48.
[113] Salami (n 48) 968.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

fon sağlanmasının, sanal ortamlar dışında gerçekleştirilen kara para aklama ve terör finansmanı fiillerinin tabi olduğu kanun hükümlerince suç kabul edilmesi gerekmektedir.[114] Bir sonraki aşamada, sanal ortamın gerekliliklerine göre ek düzenlemelerle desteklenerek kripto paralar aracılığıyla terörün finanse edilmesinin önüne geçilmesi ve her halükarda ulusal düzenlemelerin uyumlu hale getirilmesi gerekmektedir. Bunun için uluslararası düzeyde düzenleme ihtiyacı olsa da ülkelerin bu konuda farklı görüşleri bulunmaktadır. Bazı ülkeler uluslararası düzenleme vurgusu yaparken, bazıları buna ihtiyaç olmadığı görüşündedir.[115] Ülkeleri aynı masanın etrafında toplamak zor da olsa, internet üzerinden terörizmin finansmanını ülkelerin ayrı ayrı çözmelerinin mümkün olmadığı; kolektif, tutarlı ve global bir yaklaşımın benimsenmesi gerektiğinin altı çizilmektedir.[116] Dolayısıyla bu yönde yapılan çalışmalara ağırlık verilmesi önem arz etmektedir.

## 4. Kripto Paraların Terörizmin Finansmanında Kullanılmasının Önüne Geçilmesine Yönelik Çalışmalar

Kripto paraların terörizmin finansmanında kullanılmasının önüne geçilmesindeki yetersizliğin temel nedenleri kripto paraların alışılagelmiş finansal araçlardan farklı olması ve mevcut ulusal ve uluslararası düzenin revizyona ihtiyaç duymasıdır. Kripto paralar birçok ülkede yasal düzenlemelere tabi değildir.[117] Yukarıda açıklandığı üzere, kripto paraların niteliği ve nasıl düzenlenmesi gerektiği konusunda görüş birliği bulunmamaktadır. Kripto paranın niteliği konusunda aynı ülke içerinde bile yeknesaklık olmadığı gibi terörizmin finansmanında kripto paraların kullanımı açısından herhangi bir düzenleme söz konusu değildir. Bu çok başlılık kripto paralara yönelik düzenleme yapılmasını zorlaştırmaktadır. Danimarka ve Polonya kripto paraların şu aşamada düzenlenmesine ihtiyaç olmadığını ileri sürerek daha liberal bir yaklaşım sergilemektedir.[118] Tayland, Çin Halk Cumhuriyeti, Endonezya, Danimarka ve Rusya ise sanal paraların kullanımına yönelik tedbirler almışlardır.[119] Finansal düzenlemelerin yetersizliği nedeniyle kripto paraların terörizmin finansmanında kullanılabileceğinin öngörüldüğü yüksek risk grubu ülkeler ise Afganistan, Kenya, Irak, Nijerya, Somali, Sudan ve Suriye olarak belirtilmektedir. [120]

[114] Fanusie (n 76) 3.
[115] Jacobson (n 34) 360.
[116] ibid
[117] Bazı ülkelerin yapmış oldukları düzenlemeler için bkz. Asian Development Bank (ADB), *Distributed Ledger Technology and Digital Assets: Policy and Regulatory Challenges in Asia* (ADB 2019) <https://www.adb.org/publications/distributed-ledger-technology-digital-assets-asia> Erişim 12 Şubat 2021.
[118] Choo (n 11) 302.
[119] Salami (n 48) 977.
[120] ibid

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Bununla birlikte, coğrafi olarak bakıldığında, belirlenebilir bölgeler dışından aktarılan yasadışı Bitcoin miktarının en çok olduğu bölgenin Avrupa olduğu tespit edilmiştir.[121] Gerçekten de, Avrupa'daki yasadışı Bitcoin aktivitesinin Kuzey Amerika'dan beş kat daha fazla olduğu görülmüştür.[122] Yasadışı Bitcoin aktarılan dönüştürme hizmetleri sağlayıcılarının (*conversion services*) büyük bir kısmı faaliyet ülkelerini gizlediğinden kara para aklama kanunlarının uygulanacağı ülkenin tespit edilmesi de ayrıca zorlaşmaktadır.[123] Buna ek olarak, kolluk ve infaz kurumları tarafından tespit edilemeyen ve sınır ötesi gerçekleştirilen Liberty Reserve ve Silk Road olaylarındaki yasadışı işlemlerden sonra uluslararası düzenlemelerin ve işbirliğinin önemi anlaşılmıştır.[124] Her ne kadar henüz ortak bir sonuca varılmamış olsa da kripto paraların tanımı, niteliği ve nasıl ele alınması gerektiği konusunda uluslararası örgütlerin çalışmaları bulunmaktadır.[125]

Kripto paralara ilişkin düzenlemeler bakımından bu zamana kadar genellikle aracı kuruluşlara odaklanıldığı görülmektedir.[126] Örneğin, ABD'nin New York Eyaleti, sanal para işleriyle uğraşan gerçek ve tüzel kişilerin "Bitlicense" denilen lisansı almalarını zorunlu kılmaktadır.[127] Buna göre, (1) işlemin finansal olmayan amaçlarla gerçekleştirildiği ve nominal miktardan fazla sanal para biriminin transferini içermediği durumlar dışında, sanal para biriminin iletilmesi veya iletilmesi için sanal para biriminin alınması; (2) başkaları adına sanal para biriminin saklanması, tutulması veya muhafazası veya kontrolü; (3) müşteri için sanal para birimi alıp satmak; (4) müşteri için değişim hizmetleri gerçekleştirmek; veya (5) bir sanal para birimini kontrol etmek, yönetmek veya vermek olarak tanımlanan sanal para işlerinin yapılabilmesi için lisans alınması gerekmektedir.[128] Sadece yatırım amaçlı sanal parayı elinde tutmak isteyen tüketiciler lisansa tabi değildir. Bununla birlikte, lisans almanın koşulları oldukça sıkı olduğundan çok az kişiye lisans verilmektedir.[129] Bitlicense düzenlenmesinin en önemli noktası, aracı kuruluşlara getirilen kayıt yükümlülüğüne ek olarak, sanal parayla uğraşan gerçek ve tüzel kişilere kara paranın aklanmasının önlenmesi yükümlülüğü getirmesidir.[130] Bu kişiler iç denetimlerini düzenli olarak gerçekleştirmek, kara paranın aklanmasının

[121] Fanusie (n 76) 2.
[122] ibid
[123] ibid
[124] Salami (n 48) 984; Morton (n 8) 131.
[125] Morton (n 8) 131.
[126] Ibrahim (n 2) 3.
[127] New York Codes, Rules and Regulations, 23 NYCRR 200.3, <https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I7444ce80169611e594630000845b8d3e&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)&bhcp=1> Erişim 1 Temmuz 2021.
[128] ibid 200.2(q).
[129] Bu zamana kadar lisans verilen kişilerin listesi için bkz. New York State Department of financial Services, 'Regulated Entities' <https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/regulated_entities> Erişim 1 Temmuz 2021.
[130] 23 NYCRR 200.15.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

önlenmesine yönelik yazılı politikalar oluşturmak, günlük uyumları denetleyecek kişileri belirlemek, kayıt tutmak, müşterinin tanınması ve şüpheli işlemlerin bildirilmesi mekanizmalarını işletmek zorundadır.[131]

Avrupa Komisyonu, blokzincir temelli uygulamalara ilişkin konulardaki yasal kesinlik ve açık düzenlemelerin gerekliliğini tanımıştır.[132] Kısaca 5. Kara Para Aklamanın Önlenmesi Direktifi olarak anılan Avrupa Parlamentosu ve Avrupa Komisyonu'nun 30 Mayıs 2018 tarihli Direktifi ("5. Direktif") ile sanal paraların ve cüzdan sağlayıcıları ile ön ödemeli kartların anonim olmasına sınır getirilmiştir.[133] Yükümlü kuruluş olarak belirlenen borsa ve cüzdan sağlayıcılarına sicile kaydolma, müşteriyi tanımak için gerekli işlemleri yapma ve şüpheli işlemleri yetkili birimlere bildirme yükümlülükleri getirilmiştir. Böylelikle sanal paraların tercih edilmesinde belki de en önemli unsur olan anonimliğin ortadan kaldırılmasında ilk adım atılmıştır. Bu Direktifin AB üye ülkeleri tarafından kabul edilmesinin ardından yasadışı aktivitelere karşı merkezi kuruluşlara önemli yetkiler sağlayacağı düşünülmektedir.[134] Avrupa Bankacılık Otoritesi (*European Banking Authority (EBA)*) ve Avrupa Menkul Kıymetler ve Piyasalar Otoritesi (*European Securities and Markets Authority (ESMA)*), AB karar alıcılarının FATF'nin kara para aklama ve terörizmin finansmanını engellemeye yönelik rehber ilkeleriyle 5. Direktif'in kripto para borsalarına ve ilk para arzı sağlayıcılarına uygulanmasını göz önünde bulundurmaya davet etmektedir.[135]

Avustralya da kara paranın aklanmasının ve terörün finansmanın önlenmesine yönelik yasasını sanal paraları kapsayacak şekilde değiştirmiştir. Sanal para borsalarına sicile kaydolma, uyum ve kayıt tutma yükümlülükleri getirilmiştir.[136]

Türkiye'de ise aracı kuruluşlara yönelik özel bir düzenleme getirilmemekle birlikte kara paranın aklanması ve terörün finansmanın önlenmesine yönelik düzenlemelerin kripto varlıkları kapsayacak şekilde genişletildiği söylenebilir. Daha önce belirtilmiş olduğu üzere, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile kara paranın aklanması ve terörizmin finansmanı suçlarına değinilmektedir. Bu kanunun 2. maddesinin 1(d) fıkrasında bankacılık,

---

[131] ibid.

[132] European Commission, 'Legal and regulatory framework for blockchain' (2020) <https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain> Erişim 13 Kasım 2020.

[133] European Parliament and the Council Directive (EU) 2018/843 of the of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43 (5. Direktif).

[134] Morton (n 8) 134.

[135] European Securities and Markets Authority (ESMA), 'Advice - Initial Coin Offerings and Crypto-Asset' (ESMA 2019) <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> Erişim 1 Temmuz 2021) 36.

[136] Anti-Money Laundering and Counter-Terrorism Financing Amendment Act (No 130) 2017 <https://www.legislation.gov.au/Details/C2017A00130> Erişim 15 Haziran 2021.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

sigortacılık, bireysel emeklilik, sermaye piyasaları, ödünç para verme ve diğer finansal hizmetler ile posta ve taşımacılık, talih ve bahis oyunları alanında faaliyet gösterenler; döviz ile iştigal edenler veya bu faaliyetlere aracılık edenler başta olmak üzere kanun uyarınca yükümlü kişiler belirtilmektedir. Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik (Tedbirler Hakkında Yönetmelik) m.4(1)'de de benzer kişilere yer verilmiş ve 5549 sayılı kanuna ek olarak kripto varlık hizmet sağlayıcılar yönetmelikte yükümlü kişiler arasında sayılmıştır.[137] Kripto varlık hizmet sağlayıcılar ne bu yönetmelikte ne de Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik'te tanımlanmaktadır.[138] Dolayısıyla her ne kadar aracı kuruluşların açıkça düzenlenmediği görülse de yapılacak bir tanımla kara paranın aklanması ve terörün finansmanın önlenmesine ilişkin kurallara tabi olacak yükümlülerin kapsamı genişletilip daraltılabilecektir. Bu konuda mevzuatta karışıklığa neden olunmaması adına kripto varlık sağlayıcısı ifadesinden ne anlaşılması gerektiğinin ivedilikle düzenlenmesi önem arz etmektedir.

5549 sayılı kanunda kripto varlık sağlayıcılara yer verilmemiş olsa da Tedbirler Hakkında Yönetmelik m.1'de bu yönetmeliğin amacının 5549 sayılı kanunun uygulanmasına yönelik olarak yükümlüler, yükümlülükler, yükümlülüklere uyumun denetimi, gümrük idaresine açıklama yapılması ve diğer tedbirlere ilişkin usul ve esasları düzenlemek olduğu belirtilmektedir. Buradan hareketle kripto varlık sağlayıcılarının da hem 5549 sayılı kanun hem de Tedbirler Hakkında Yönetmelik kapsamındaki yükümlülüklere tabi olacağını söylememiz mümkündür. Buradan hareketle, kripto varlık sağlayıcıları 5549 sayılı kanun m.3 ile Tedbirler Hakkında Yönetmelik'in üçüncü bölümü (m.3-26) uyarınca müşterinin tanınması ve kimlik tespiti yükümlülüğünü yerine getirmek zorunda olacaktır. MASAK, kripto varlık sağlayıcılarının müşteri/kullanıcı ile yüz yüze gelmediği durumlarda kimlik tespitini yaparken Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik'te yer alan destek hizmetine ilişkin şartlardan ve Sermaye Piyasası Kurulu tarafından yayımlanan Yatırım Kuruluşlarının Kuruluş ve Faaliyet Esasları Hakkında Tebliğ'in Aracı Kurumların Dışarıdan Hizmet Alımına İlişkin Esaslar başlıklı Dokuzuncu Bölümü'nde yer alan dışarıdan hizmet alımına ilişkin şartlardan yararlanılabileceğini belirtmektedir.[139] Aynı şekilde, MASAK "Faaliyetlerini Münhasıran Elektronik Ortamda Gerçekleştiren Yükümlüler" olarak kripto varlık hizmet sağlayıcılarının 5 No'lu

[137] Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik (RG. 09.01.2008/26751). Kripto varlık sağlayıcılarının yönetmelikteki yükümlü tanımına eklenmesine ek olarak 5549 sayılı kanuna eklenmesinin karışıklık yaratmaması adına faydalı olacağı düşünülmektedir.
[138] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik (n 24).
[139] TC Hazine ve Maliye Bakanlığı, Mali Suçları Araştırma Kurulu (MASAK), 'Kripto Varlık Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklere İlişkin Temel Esaslar' 10 (MASAK 2021) <https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf> Erişim 15 Haziran 2021.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Mali Suçları Araştırma Kurulu Genel Tebliği'nin 2.2.10 maddesinde belirtilen şartları tamamlamaları halinde Basitleştirilmiş Tedbirlere ilişkin hükümlerden yararlanabilmesi mümkün olduğunu; ancak, bunun için ilgili maddede yer verilen şartların tamamlanması gerektiğinin altını çizmektedir.[140]

Bunlara ek olarak, kripto varlık sağlayıcılar 5549 sayılı kanun m.4 uyarınca şüpheli işlem bildiriminde bulunmalıdır. Şüpheli işlemlerin bildirilmesine yönelik esaslar tedbirler hakkında yönetmeliğin dördüncü bölümünde (m.27-30) düzenlenmektedir. Kripto varlık sağlayıcıların 5549 sayılı kanun m.7 uyarınca bilgi ve belge verme (Tedbirler Hakkında Yönetmelik, Beşinci Bölüm – m.31-34); m.8 uyarınca muhafaza ve ibraz (Tedbirler Hakkında Yönetmelik, Sekizinci Bölüm – m.46); m.6 uyarınca devamlı bilgi verme yükümlülüğü (Tedbirler Hakkında Yönetmelik, m.32-34) de bulunmaktadır. Bu yükümlülüklerin ihlali neticesinde 5549 sayılı kanun m.13 uyarınca müşterinin tanınması yükümlülüğü, devamlı bilgi verme yükümlülüğü ve şüpheli işlem bildirimi yükümlülüğünün ihlallerinin tespiti halinde idari para cezaları, m.14 uyarınca şüpheli işlem bildiriminin mahkemeler dışında paylaşılmaması yükümlülüğü ile bilgi ve belge verme, muhafaza ve ibraz yükümlülüklerinin ihlali halinde adli ceza öngörülmektedir.

Buradaki önemli husus, yükümlülüklerin tüzel kişi yükümlünün kanuni temsilcileri tarafından yerine getirilmesinin öngörülmüş olmasıdır.[141] Bu noktada, merkezileşmemiş ve arkasında bir tüzel kişi olmayan kripto varlık sağlayıcılarının denetiminin açıkta bırakıldığı görülmektedir. Düzenlemelerin en azından bu sağlayıcılar açısından yetersiz kalacağı anlaşılmaktadır.

Devletlerin benimsedikleri yaklaşımlar değerlendirildiğinde genellikle borsalar gibi aracı kuruluşların ele alındığı ancak bunun yeterli olmadığı, düzenlemelerde kullanıcılar, madenciler ve geliştiricilere yoğunlaşılması gerektiği belirtilmektedir.[142] Aynı zamanda suç teşkil eden işlemlerdeki kamuya açık adreslerin veya güvenilir kullanıcıların listesinin yayınlanması önerilmektedir.[143] Belli bir düzenlemeye konu olan borsalar ise sadece merkezileşmiş borsalardır. Merkezileşmemiş, belirli adresi, kurucusu, ortağı olmayan sadece merkezi olmayan borsalar tamamen göz ardı edilmektedir. Bu bağlamda kara paranın aklanması ve terörün finansmanın önlenmesine ilişkin kuralların ne derece uygulanabileceği soru işareti yaratmaktadır.[144] Ne şekilde yapılırsa yapılsın denetim ve gözetim mekanizmalarının ve kurumların yetkilerinin açık bir şekilde belirlenmesi gerekmektedir. Örneğin,

[140] ibid (MASAK bu şartları kısaca şu şekilde özetlemektedir: Türkiye'de mukim bankayla, sunulan mal veya hizmete ilişkin tahsilat ve ödeme işlemlerinin elektronik ortam üzerinden gerçekleştirileceğine dair sözleşme yapılmış olması, kimliğe ilişkin bilgilerin İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü veri tabanı kullanılarak sorgulanması yoluyla teyit edilmesi.)
[141] MASAK (n 139).
[142] Blandin (n 25) 50; Ramsey (n 80) 4.
[143] Ramsey (n 80) 4.
[144] Blandin (n 25) 52.

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

kara paranın aklanması veya terörün finansmanın önlenmesiyle ilgili bir kurumdan alınacak lisans ile sermaye piyasası kurumundan alınacak lisans farklılık arz edecektir.[145]

Kripto paraların regüle edilmesi konusunda hem devletlerin hem de devletlerin kurumlarının görüş birliğinin sağlanması zor olabilir. Bazı ülkelerde siber işlemlerin düzenlenmesi ulusal güvenlik açısından önem taşıdığından devletin bireysel işlemleri gerçekleştiren kişilerin bilgilerine ulaşmasını sağlayan yasal dayanaklar bulunmaktadır.[146] Bazı ülkelerde ise ulusal güvenlik unsurunun gizlilik ve verilerin korunması hakları arasında denge sağlanması için siber alanın düzenlenmesine daha temkinli yaklaşılmaktadır.[147] Kara paranın aklanması ve terörün finansmanı açısından benzer yaklaşımlar getirmeleri, ortak zeminde buluşmalarının imkansız olmadığını göstermektedir. Keza, ülkelerin ortak sorunlarına odaklanılarak uluslararası düzenlemeler yapılması gerektiği savunulmaktadır.[148] BM TFÖ Sözleşmesi her ne kadar doğrudan kripto paraların yarattığı sorunlara cevap veremese de terörün finansmanının önlenmesi için uluslararası işbirliği yapılması konusunda taraf devletlere sorumluluk yüklemektedir.[149] Yeni düzenlemeler sınır ötesi sanal para işlemlerine ilişkin yasaların/düzenlemelerin uyumlu hale getirilmesini, sanal para ile ilgili kuruluşlar üzerinden kara paranın aklanması suretiyle terörizmin finansmanın sağlanmasının önüne geçilmesini öngörmelidir.[150]

Bu bakımdan, yeni düzenlemenin karşılayacağı ihtiyaçların belirlenmesi için öncelikle finansal kuruluşların dolaylı da olsa kripto paralar aracılığıyla kara para aklanmasını sağlayıp sağlamadıklarını ve eğer sağlıyorlarsa bunun kaynaklarını tespit etmeleri gerekmektedir.[151] Finansal riskin belirlenmesinde yapay zeka ve blokzincir analiz tekniklerinin kullanılması ve özellikle kripto paralar için dönüşüm hizmeti sağlayan finansal kuruluşların bu risk değerlendirmesini yapmaları önerilmektedir.[152] Örneğin Elliptic adlı blokzincir şirketi kripto cüzdanların ve sanal varlık hizmeti sağlayıcılarının risklerini değerlendirerek dolandırıcılığı en aza indirmeye çalışmakta; kara paranın aklanması ve terörizmin finansmanın önlenmesine yönelik düzenlemelerin otomasyonunu sağlayarak kripto işlemleri denetlemektedir.[153] Blokzincir teknolojisini kullanan Chainalysis adlı başka bir şirket özellikle kamu kurumlarına ve finansal kuruluşlara kripto paralarla ilgili veri sağlamakta, dönüşüm

[145] ibid 54.
[146] Salami (n 48) 985.
[147] ibid
[148] Ramsey (n 80) 6.
[149] Örneğin bkz. BM TFÖ Sözleşmesi (n 95) Başlangıç Hükümleri, m. 18.
[150] Salami (n 48) 985.
[151] Fanusie (n 76) 3.
[152] ibid
[153] Elliptic, <https://www.elliptic.co > Erişim 1 Temmuz 2021.

DRAFT - TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

hizmetlerine yönelik saldırılar, fidye yazılım saldırıları, kara paranın aklanması gibi durumların incelenmesini kolaylaştırmaktadır.[154]

Riskin yoğunluğuna göre ülkelerdeki finansal otoritelerin, karıştırıcıların (*mixers*) ve çevrimiçi kumar siteleri üzerindeki kara paranın önlenmesine yönelik yasaların uygulanmasına yönelik adımlar atması; kolluğun bu tür sitelerin açıklarına yoğunlaşması gerekmektedir.[155] Ancak tüm bunların etkili şekilde yapılabilmesi için ortak standartlar getirilebilmesi adına uluslararası işbirliğine ve uyumlu düzenlemelere ihtiyaç duyulmaktadır.[156] Böyle bir uluslararası düzenleme olmadan teröristlerin yasa açığından yararlanmaya devam edecekleri öngörülmektedir.[157]

Bu yasa açıklarını kapatmak aynı zamanda teknolojinin gelişimini teşvik etmek için geliştirilen yöntemlerden biri kum havuzu tekniğidir. Kum havuzları henüz düzenlemenin olmadığı teknolojik altyapıların geliştirilmesinde yazılımcıları, şirketleri ve yasa koyucuları bir araya getiren, tamamen işlevsel olan ancak teknolojinin test edilmesi amacıyla oluşturulan izole ortamlardır. Bu ortamlar sayesinde teknolojilerin gelişmesi engellenmeden oluşabilecek güvenlik açıkları belirlenmekte ve düzenlemeler buna göre şekillendirilebilmektedir. Kum havuzları fintek alanında blokzincir, dağıtık defter teknolojiler ve kripto paralar özelinde kullanılmaya başlanmıştır. Avrupa Komisyonu'nun kurmuş olduğu Avrupa Blokzincir Ortaklığı AB'nin blokzincir stratejinin belirlenmesi ve kamu hizmetlerinde blokzincir altyapının kullanılması amacıyla kurulmuş olup kum havuzu yöntemiyle hem teknolojinin hem de düzenlemelerin geliştirilmesini sağlamaktadır.[158] Kripto paralar hakkında finansal araç olan ve olmayan kripto varlıklar ayrımı yapılarak yeni düzenlemeler önerilmiştir.[159] Bu kurallar kripto varlıkları finansal araç olarak kullanan pazar altyapılarını düzenlemekte; kara paranın aklanması ve terörizmin finansmanın önlenmesi hakkında hüküm içermemektedir.[160] Bununla birlikte, Avrupa Komisyonu yukarıda anılan 5. Direktifin kripto-varlıkların kara paranın aklanması ve terörizmin finansmanında kullanılmasını içerdiğini hatırlatmakta, ancak zamanla bu düzenlemenin de gözden geçirileceğini vurgulamaktadır.[161]

DRAFT-TASLAK

[154] Chainalysis, <https://www.chainalysis.com> Erişim 1 Temmuz 2021.
[155] Fanusie (n 76) 12.
[156] Morton (n 8) 142.
[157] İbid.
[158] Eurpean Commission, 'European Blockchain Partnership' <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership> Erişim 5 Temmuz 2021.
[159] Eurpean Commission (n 132).
[160] European Commission, 'Questions and Answers: Digital Finance Strategy' <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1685> Erişim 5 Temmuz 2021.
[161] ibid

Electronic copy available at: https://ssrn.com/abstract=4083129

Birleşik Krallık, Finansal Yönetim Kurumu (*Financial Conduct Authority – FCA*) tarafından yönetilen finansal gelişmeleri destekleyen kum havuzu oluşturmuştur.[162] Kum havuzunda blokzincir ve dağıtık defter teknolojilerine dayalı elektronik ödeme sistemi sağlayan şirketler de yer almaktadır.[163] Ayrıca, FCA, kum havuzuna dahil ettiği son grup şirketlerin sağladığı hizmetler arasında dolandırıcılığın tespiti ve önlenmesine yönelik teknolojilerin olması şartını aramıştır.[164]

Kum havuzlarının yaygınlaştırılması hem teknolojinin gelişimini ağır kurallar ve uyum yükümlülüklerle engellemeyecek hem de sektörün düzenleme ihtiyaçlarını gözlemlenmesine yardımcı olarak düzenlemelerin yetersizliğinin giderilmesine ve en güvenli kuralların konulmasına yardımcı olacaktır. Birçok devletin benimsediği şekilde kara paranın aklanması ve terörün finansmanın önlenmesi kurallarının yeni gelişen finansal teknolojilere ve dolayısıyla kripto varlıklara etki edecek şekilde genişletilmesine rağmen, ileride revize edilmek üzere düzenlemelerdeki eksikliklerin giderilmesi adına da kum havuzları önem arz etmektedir. Düzenlemelerdeki açıkların tespit edilmesine ek olarak, kripto varlıklar bakımından kanunlarla uyum sağlanmasına katkı sağlayacak teknolojilerin de bu havuzlarda denenmesi etkili sonuçlar doğuracaktır.

**SONUÇ**

Terörizmin finansmanında yeni finansman aracı olarak kripto paralar karşımıza çıkmaktadır. Kripto paralar, takiplerinin neredeyse imkansız oluşu ve kullanıcılara anonim kalma imkanı sağlaması gibi özellikleri nedeniyle terör örgütleri tarafından tercih edilmeye başlanmıştır. Ülkelerin ulusal düzeyde terörizmin finansmanı ve kara paranın engellenmesine yönelik düzenlemeleri ve çalışmaları bulunmaktadır. Bu düzenlemeler genel itibariyle kripto paraların terörün finansmanında kullanılmasını da kapsayacak şekilde yorumlanabilmektedir. Ancak bu düzenlemeler, kripto paraların doğası gereği sınır ötesi nitelikte olması nedeniyle yeterince etkili olmamaktadır. Her devletin kripto paralara yönelik düzenlemesi olmadığı gibi olan düzenlemeler eşit düzeyde koruma sağlamakta veya farklı alanları düzenlemektedir. Kripto paraların dayandığı blokzincir teknolojisinin uluslararası niteliği sonucunda birbiriyle uyumlu olmayan ve farklı düzeylerde koruma getiren ulusal düzenlemeler yetersiz kalmaktadır. Devletlerin siber alanın düzenlenmesi konusunda tutumları farklı olsa da, terörizmin finansmanının önlenmesinde adım atmaları gerekmektedir. Ulusal düzeyde yasa açıklarının bulunmasında gelişen teknolojilerden faydalanılmalı, kum havuzu tekniği gibi yöntemlerle kripto para ve blokzincir teknolojilerinin gelişiminin önü açılırken düzenlemelerin

[162] Financial Conduct Authority (FCA), 'Applying to the regulatory sandbox' <https://www.fca.org.uk/firms/innovation/regulatory-sandbox-prepare-application> Erişim 5 Temmuz 2021.
[163] Financial Conduct Authority (FCA), 'Regulatory sandbox – cohort 6'<https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-6> Erişim 5 Temmuz 2021.
[164] Financial Conduct Authority (FCA) (n 162).

DRAFT - TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

eksiklikleri test edilmelidir. Farklı alanlarda faaliyet gösteren devlet kurumları iletişimde kalmalı ve birbirleri ile tutarlı düzenlemeler ortaya çıkarmalıdır. Son aşamada, uluslararası örgütlerin yaptıkları çalışmalar ışığında, kripto paraların teknik özellikleri de dikkate alınarak uluslararası iş birliği gerçekleştirilmeli ve bir sonraki aşamada uluslararası düzenlemelere gidilmelidir.

**KAYNAKÇA**

**Düzenlemeler**


07.02.2013 tarihli ve 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun (RG. 16.02.2013/28561)

11.10.2006 tarihli ve 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun (RG. 18.10.2006/26323)

12.04.1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu (RG. 12.04.1991/20843)

26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu (RG. 12.10.2004/25611)

Anti-Money Laundering and Counter-Terrorism Financing Amendment Act (No 130) 2017 <https://www.legislation.gov.au/Details/C2017A00130> Erişim 15 Haziran 2021

Birleşmiş Milletler Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme (*International Convention for the Suppression of the Financing of Terrorism*) (kabul tarihi 9 Aralık 1999 BM Genel Kurul Kararı No A/RES/59/109, yürürlük tarihi 10 Nisan 2002, 2178 UNTS 197)

Crypto-Currency Act of 2020, H.R 6154, 116th Cong. (2020), <https://www.congress.gov/bill/116th-congress/house-bill/6154/text> Erişim 6 Temmuz 2021

European Parliament and of the Council Directive (EU) 2018/843 of the of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJL 156/43

New York Codes, Rules and Regulations, 23 NYCRR 200.3, <https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I7444ce80169611e594630000845b8d3e&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)&bhcp=1> Erişim 1 Temmuz 2021

Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik (RG. 16.04.2021/31456)

Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik (RG. 09.01.2008/26751)


DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

**Kitap ve Makaleler**


Freeman M, Moyara R, 'Terrorism Financing Methods: An Overview' (2013) 7 Perspectives on Terrorism 5

Brill A, L Keene, 'Cryptocurrencies: The Next Generation of Terrorist Financing?' (2014) 6 Defence Against Terrorism Review

Carmona A, 'The Bitcoin The Currency of the Future, Fuel of Terror' (2015) 63 Advances in Information Security 127

Choo KKR, 'Chapter 15 - Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?' David Lee Kuo Chuen (ed.), *Handbook of Digital Currency*: *Bitcoin Innovation, Financial Instruments, and Big Data* (Academic Press 2015)

Cohen-Almagor R, 'Jihad Online: How Do Terrorists Use the Internet?' F Freire, X Araújo Rúas, Fernández V Martínez, X García (ed.) *Media and Metamedia Management: Advances in Intelligent Systems and Computing* (Springer 2017)

Gödekli M, *Terörizmin Finansmanı Suçu* (Seçkin Yayınları 2017)

Ibrahim SA, 'Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering' (2019) 2 *Stratagem*

Irwin A, J Slay, 'Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft' (International Cyber Resilience Conference, Perth Western Australia: Edith Cowan University, 2010) <http://ro.ecu.edu.au/icr/5> Erişim 1 Aralık 2020

Jacobson M, 'Terrorist Financing and the Internet' (2010) 33 Studies in Conflict & Terrorism 353

Morton DT, 'The Future of Cryptocurrency: An Unregulated Instrument in an Increasingly Regulated Global Economy' (2020) 16 Loyola University Chicago International Law Review 129

Nacos BL, *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post-9/11 World* (Pearson Education Inc. 2008)

Patel PC, I Pereira, 'The Relationship between Terrorist Attacks and Cryptocurrency Returns' (2020) *Applied Economics* 1

Ramsey R, 'An Examination of the Challenges Posed by Cryptocurrencies to AML/CTF Regulation' (2020) 12 Amsterdam Law Forum 1

Salami I,'Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?' (2018) 41 Studies in Conflict and Terrorism 968


DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Trautman L, 'Virtual Currencies. Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox' (2014) 20 Richmond Journalof Law & Technology 1

**Rapor ve Çalışmalar**

Asian Development Bank (ADB), *Distributed Ledger Technology and Digital Assets: Policy and Regulatory Challenges in Asia* (ADB 2019) <https://www.adb.org/publications/distributed-ledger-technology-digital-assets-asia> Erişim 12 Şubat 2021

Blandin A ve ark., 'Global Cryptoasset Regulatory Landscape Study' (Cambridge Centre for Alternative Finance 2020) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf> Erişim 15 Haziran 2021

Global Blockchain Business Council, 'Global Standard Mapping Initiative (GSMI): Insight Report' (2020) <https://gbbcouncil.org/wp-content/uploads/2020/10/GSMI-Legal-Regulatory-Report.pdf> Erişim 15 Haziran 2021

Keatinge T, David Carlisle, Florence Keen, 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses' (European Parliament 2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf> Erişim 13 Kasım 2020

Dion-Schwarz C, D Manheim, ve PB Johnston, *Terrorist Use of Cryptocurrencies* (RAND Corporation 2019) <https://www.rand.org/pubs/research_reports/RR3026.html> Erişim 15 Haziran 2021

Eisermann D, 'Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges' (Berlin Risk 2020) <https://www.counterextremism.com/sites/default/files/Cryptocurrencies%20as%20Threats%20to%20Public%20Security%20and%20Counter-Terrorism_ENG%20Translation_April%202020.pdf> Erişim 5 temmuz 2021

European Law Enforcement Agency (EUROPOL), *The Internet Organised Crime Threat Assessment (IOCTA)* (2015) <https://op.europa.eu/s/pkP9> Erişim 14 Kasım 2020

Fanusie YJ, T Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services' (Elliptic/Foundation for Defense of Democracies 2018) <https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf> Erişim 14 Kasım 2020

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Financial Action Task Force (FATF), 'Virtual Currencies – Key Definitions and Potential AML/CFT Risks' (FATF-OECD 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> Erişim 14 Ekim 2020

Şirin P ve ark, 'Blokzinciri Teknolojisi Terminoloji Çalışması' (Türkiye Bilişim Vakfı 2019) <https://bctr.org/dokumanlar/Blokzinciri_Teknoloji_Terminoloji.pdf> Erişim 10 Haziran 2021

TC Hazine ve Maliye Bakanlığı, Mali Suçları Araştırma Kurulu (MASAK), 'Kripto Varlık Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklere İlişkin Temel Esaslar' (MASAK 2021) <https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf> Erişim 15 Haziran 2021

**İnternet Siteleri**

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), '25 Kasım 2013 tarih ve 2013/32 sayılı Basın Açıklaması' (2013) <https://www.bddk.org.tr/Duyuru/EkGetir/510?ekId=530> Erişim 6 Temmuz 2021

Chainalysis, <https://www.chainalysis.com> Erişim 1 Temmuz 2021

Elliptic, <https://www.elliptic.co > Erişim 1 Temmuz 2021

European Commission, 'Legal and regulatory framework for blockchain' (2020) <https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain> Erişim 13 Kasım 2020

European Commission, 'Questions and Answers: Digital Finance Strategy' <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1685> Erişim 5 Temmuz 2021

European Securities and Markets Authority (ESMA), 'Advice - Initial Coin Offerings and Crypto-Asset' (ESMA 2019) <https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets> Erişim 1 Temmuz 2021

Eurpean Commission, 'European Blockchain Partnership' <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership> Erişim 5 Temmuz 2021

Financial Conduct Authority (FCA), 'Applying to the regulatory sandbox' <https://www.fca.org.uk/firms/innovation/regulatory-sandbox-prepare-application> Erişim 5 Temmuz 2021

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

Haig S, 'Tanzanian president urges central bank to prepare for crypto' (*Cointelegraph*, 14 Haziran 2021) <https://cointelegraph.com/news/tanzanian-president-urges-central-bank-to-prepare-for-crypto> Erişim 1 Temmuz 2021

Harper C, 'Bitcoin transaction fees more expensive than ever' (*Coindesk,* 21 Nisan 2021) <https://www.coindesk.com/bitcoin-transaction-fees-more-expensive-than-ever> Erişim 1 Temmuz 2021

Hart R, 'Tanzania considers crypto and boosts bitcoin as nations line upbehind El Salvador to embrace decentralized finance' (*Forbes,* 14 Haziran 2021) <https://www.forbes.com/sites/roberthart/2021/06/14/tanzania-considers-crypto-and-boosts-bitcoin-as-nations-line-up-behind-el-salvador-to-embrace-decentralized-finance/?sh=64fc2a944fc3> Erişim 1 Temmuz 2021

Institute for the Unification of the Private Law UNIDROIT, 'Study LXXXII – Digital Assets and Private Law Project'<https://www.unidroit.org/work-in-progress/digital-assets-and-private-law> Erişim 6 Temmuz 2021

Mangan D, 'New York woman pleads guilty to using bitcoin to launder money for terror group ISIS' *CNBC* (2020) <https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html> Erişim 14 Kasım 2020

New York State Department of Financial Services, 'Regulated Entities' <https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/regulated_entities> Erişim 1 Temmuz 2021

Pham L, 'Terrorism and charity: defining Hamas' (*World Policy,* 8 Ağustos 2014) <http://worldpolicy.org/2014/08/08/terrorism-and-charity-defining-hamas/> Erişim 13 Şubat 2021

Renteria N, T Wilson, K Strohecker, 'In a world first, El Salvador makes bitcoin legal tender' *Reuters* (Americas, 10 Haziran 2021) <https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/> Erişim 1 Temmuz 2021

Taylor M, 'Norway gunman claims he had nine-year plan to finance attacks' *The Guardian* (Norveç, 25 Temmuz 2011) <https://www.theguardian.com/world/2011/jul/25/norway-gunman-attack-funding-claim> Erişim 14 Kasım 2020

TC Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu (MASAK), 'Aklamanın Aşamaları' <https://masak.hmb.gov.tr/aklamanin-asamalari> Erişim 1 Aralık 2020

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129

U.S. Commodity Futures Trading Commission, 'Bitcoin Basics. U.S. Commodity Futures Trading Commission' (2019) <https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf> Erişim 13 Kasım 2020

U.S. Department of the Treasury, 'Financial Crimes Enforcement Network: History of Anti-Money Laundering Laws' <https://www.fincen.gov/history-anti-money-laundering-laws> Erişim 13 Kasım 2020

U.S. Internal Revenue Service (IRS), 'Notice 2014-21. Internal Revenue Service' (2014) <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> Erişim 13 Kasım 2020

U.S. Securities and Exchange Commission (SEC), 'U.S. Securities and Exchange Commission: Statement on Cryptocurrencies and Initial Coin Offerings' (2017) <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11> Erişim 13 Kasım 2020

DRAFT-TASLAK

Electronic copy available at: https://ssrn.com/abstract=4083129