

SUÇ GELİRLERİNDE KRİPTO PARALARIN KULLANIMI VE ANONİM İŞLEMLERE DAİR DEĞERLENDİRMELER

ASSESSMENTS OF THE USE OF CRYPTOCURRENCIES IN CRIMINAL PROCEEDS AND ANONYMOUS TRANSACTIONS



Doğançan AKATA*

ÖZ

Çalışmada, kripto paralar ile gerçekleştirilen işlemlerin anonim olması ile suç gelirleri arasındaki ilişki değerlendirilmiştir. Kripto paralar ile gerçekleştirilen işlemlerin muhteviyatı itibarıyla anonim bir yapıda olması takibi imkansızlaştırır- sa da, kanuni paraya dönüştürülmesi ya da tam tersi durumun, oluşabilecek anomalilerin analiz ve tespiti için gerekli bilgilerin edinilmesini sağlayacak görüşler tartışılacaktır. Bu noktada anomali denilerek kastedilen: Kara para aklama ve terörün finansmanı gibi yasa dışı durumların finansmanının perdelenmeye çalışılması, oluşabilecek olağanüstü finansal hareketlerdir. Bu çerçevede mali istihbarat birimleri ile uluslararası finansal kuruluşların bilgi edinmesi, var olan mevzuatlarda boşlukların doldurulması, uygulamaların standardizasyonu, finans sistemin bilgi ağına entegrasyonu ve Mali Suçları Araştırma Kurulu

ABSTRACT

In the study, the relationship between the anonymity of transactions with cryptocurrencies and the proceeds of crime was evaluated. Although the anonymous nature of the transactions made with cryptocurrencies makes it impossible to follow up, opinions that will enable the acquisition of necessary information for the analysis and detection of anomalies that may occur in case of conversion to legal money or vice versa will be discussed. At this point, what is meant by anomaly is: Trying to conceal the financing of illegal situations such as money laundering and financing of terrorism and extraordinary financial movements that may occur. In this context, evaluations were made within the scope of the information acquisition of financial intelligence units and international financial institutions, filling gaps in existing legislation, standardization of

* Doktora Öğrencisi, İzmir Katip Çelebi Üniversitesi, Sosyal Bilimler Enstitüsü, Maliye ve Mali Yönetim Anabilim Dalı, dogancan.akt@gmail.com, ORC-ID: 0000-0003-4597-4928.

Akata, D. (Eylül 2021). Suç Gelirlerinde Kripto Paraların Kullanımı ve Anonim İşlemlere Dair Değerlendirmeler, *Vergi Raporu*, 264, (91-104).

Makale Türü: Derleme Makalesi

M.G.T.: 03.06.2021 / M.K.T.: 25.08.2021

Başkanlığı (MASAK) tarafından yayımlanan Tedbirler Yönetmeliği kapsamında değerlendirmeler yapılmıştır. Söz konusu değerlendirmeler gerçekleştirilirken, ilgili kuruluşlar tarafından yayımlanan bildiri, direktif, rehber ve yasal mevzuat baz alınmıştır.

Anahtar Kelimeler: Kripto Para, Suç Gelirleri, Mali İstihbarat Birimleri.

JEL Sınıflandırma Kodları: F53, H20, K34.

GİRİŞ

Günümüzde hemen hemen herkes kripto para kavramı ile ilgili, günlük hayatta ya da çeşitli yayın organlarındaki haberler vasıtası ile bir aşinalık kazanmıştır. Kısa vadede “aşırı” yüksek kazanç getirmesi birçok yatırımcıyı kendine çekmektedir. Hatta kripto paraları kolay kazanç olarak görüp, kulaktan dolma tavsiyelerle birikimlerini bu alana yatıran kişilerin sayısı gün geçtikçe artmaktadır. Ancak kripto paraları günümüzdeki yatırım çılgınlığının ötesinde, muhteviyatı itibarıyla yasadışı ticaretin bir unsuru olarak da nam salmış bir kavramdır. Anonimlik, merkezi bir yapıya ait olmaması yasadışı kullanımı cazip kılmaktadır. Bir taraftan kazançlı bir “yatırım” unsuru olarak görülmesinin dışında, suç ile ilişkili kişi/örgüt gibi art niyetli çevrelerce “para” olarak kabul görmektedir. Bu açıdan kripto paralar devletlerin mali istihbarat birimleri tarafından son yıllarda mercek altına alınmıştır. Çalışmada ilk olarak kripto para kavramı ardından suç gelirleri kavramı ve kapsamı açıklanmıştır. Üçüncü kısımda kripto paraların suç gelirlerinde finansal

practices, integration of the financial system into the information network and the measures regulation published by the Financial Crimes Investigation Board (FCIB). While making the said evaluations, the documents, directives, guidelines and legal legislation published by the relevant organizations were taken as a basis.

Keywords: Cryptocurrency, Proceeds Of Crime, Financial Intelligence Units.

JEL Classification Codes: F53, H20, K34..

araç olarak kullanılmasının önüne geçmeye yönelik mali istihbarat birimleri ve diğer uluslararası kuruluşlarca getirilen öneriler belirtilmiştir. Dördüncü kısımda ise MASAK’nın aldığı önlemler değerlendirilmiştir.

1- KRIPTO PARA KAVRAMI

Kripto para birimleri, merkezi olmayan, halka açık dağıtık defterlere kaydedilen dijital varlıklardır¹. Dağıtık Defter teknolojisi (Distributed Ledger Technology), aslında birden çok mekan, coğrafya veya kurumdan oluşan, senkronize edilmiş fikir birliği sunarak bir ağda paylaşılabilen varlık veritabanıdır². Kayıt sistemi olarak bilinen bu defterin en bilineni Blok Zincir (Blockchain)’dir. Blok zincir, belirli kurallara uyularak, bilgilerle inşa edilmiş bir dijital ağ sistemidir. Bu teknoloji, sisteme dahil olan tüm insanların kayıt tutmaya (muhasibeye) katılmasının bir şekli olarak ifade edilebilir³. Genellikle merkezi düzenleme veya düzeltme yetkisi olmayan ancak bunun yerine işlemleri kaydetmek ve yeni birimlerin verilmesini yönetmek için merkezi olmayan bir sistem kul-

¹ Dennis CHU. “Broker-Dealers For Virtual Currency: Regulating Cryptocurrency Wallets And Exchanges”. Columbia Law Review. Sayı: 118/8. 2018. s. 2326.

² Government Office for Science. “Distributed Ledger Technology: beyond block chain”. A report by the UK Government Chief Scientific Adviser. 2016. s. 4

³ Alan T. SHERMAN ve diğerleri. “On the Origins and Variations of Blockchain Technologies”. IEEE Computer and Reliability Societies. Sayı: 17/1. 20 Mart 2019. s. 72-77.

lanmaktadır. Bu sistem sahtecilik ve hileli işlemleri önlemek için kriptografiye dayanmaktadır⁴. Kripto paraların herhangi bir merkeze bağlı olmayışı, para otoritesinin kontrolünü ve herhangi bir coğrafi sınıra bağlı olmayı ortadan kaldırmaktadır⁵. Oluşturulan blok zincirin doğruluğunun kanıtı ile kripto madencilerin bloklar eklemesi ve yeni para üretmesi için İş Kanıtı (PoW) protokolleri düzenlenmiştir. PoW tipik bir şifreleme senaryosunda, bir taraf (kanıtlayıcı) başka bir tarafı (doğrulamayı) belirli bir formun sırrına sahip olduğuna veya belirli bir matematiksel ifadenin doğru olduğuna ikna etmeyi amaçlar⁶. Doğruluğu kanıtlanan işlem yeni “blok” olarak blok zincire eklenir ve işlemin gerçekleşmesi ile madenciye verilen komisyon para arzını oluşturur.

Kripto para birimine sahip olmak, özel bir anahtara sahip olmayı gerektirir. Bu özel anahtar, halka açık blok zinciri ile eşleştirildiğinde, sahiplerin kendi kripto para birimlerine erişmesine ve

başka bir kişiye aktarmasına olanak tanır⁷. Bu sistemin amacı, izlenebilir olmayan ödemelerin gerçekleştirilmesine izin verirken, bu süre zarfında kişisel gizlilik sağlanması olarak özetlenebilir⁸. Kripto paraların “eşler arası bir teknoloji”⁹ olması ve kimliklerin gizliliği; anonimlik unsurunu kapsamaktadır. İşlemlerin genellikle hassas doğası göz önüne alındığında, bir finansal sistem için önemli bir özelliktir¹⁰. Kriptografi vasıtasıyla veriler ile belirli bir kişi arasındaki bağı ve mahremiyeti korumaktan ziyade, o bağı kurulmasının önüne geçmeye yönelik gerçekleştirilen bir eylemdir¹¹.

Kripto paralar genel olarak sanal para kapsamında değerlendirilmektedir¹². Sanal para birimleri ise dijital paraların regüle edilmemiş (kanunlar tarafından kontrol edilmeyen veya denetlenmeyen) bir türüdür. Avrupa Merkez Bankası (ECB)¹³, Uluslararası Para Fonu (IMF)¹⁴, Avrupa Menkul Kıymetler ve Piyasalar Otoritesi (ESMA)¹⁵, Avrupa Bankacılık Otoritesi (EBA)¹⁶,

⁴ Merriam-Webster. “Cryptocurrency”. (<https://www.merriam-webster.com/dictionary/cryptocurrency>). Erişim tarihi: 17 Nisan 2021.

⁵ James ALTUCHER. *Crypto-Currencies 101*. Laissez Faire Books. Maryland. 2017. s. 14.

⁶ Marcus JAKOBSSON ve Ari JUELS. *Proof of Work and Bread Pudding Protocols*. (ed. Bart Preneel). Secure Information Networks - Communications and Multimedia Security -IFIP TC6/IC11 Joint Working Conference on Communications and Multimedia Security (CMS'99) September 20-21, 1999 Leuven, Belgium. Springer Science+Business Media. Germany. 1999. s. 259-261.

⁷ Dennis CHU. a.g.m. s. 2326.

⁸ David CHAUM. “Blind Signature For Untraceable Payments” (<https://scweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF>). Erişim tarihi: 02 Mayıs 2021.

⁹ Whitfield DIFFIE ve Martin E. Hellman. “Multiuser Cryptographic Techniques”. National Computer Conference. 1976. s. 109.

¹⁰ Giulia FANTI ve diğerleri. *Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees*, Proc. ACM Meas. Anal. Comput. Syst., Sayı: 2/2. Haziran 2018. s. 30.

¹¹ Anon Collective, Book of Anonymity - Big Data's End Run around Anonymity and Consent, (<https://punctumbooks.com/titles/book-of-anonymity/>), Erişim tarihi: 19 Mayıs 2021.

¹² Oktay ÜSTÜN. *Açıklamalı İngilizce - Türkçe Karapara Terimleri ve Kavramları Sözlüğü*. Türkiye Bankalar Birliği. Matsis Matbaası. İstanbul. 2016. s. 39.

¹³ European Central Bank. “Virtual Currency Schemes”. (<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>). Erişim tarihi: 16 Nisan 2021.

¹⁴ IMF Staff Discussion Note, “Virtual Currencies and Beyond: Initial Considerations”, (<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>), Erişim tarihi: 16 Nisan 2021.

¹⁵ ESMA, EBA & EIOPA, “Warning on the risks of Virtual Currencies”. (https://www.esma.europa.eu/sites/default/files/library/esma501641284_joint_esas_warning_on_virtual_currencies.pdf). Erişim tarihi: 16 Nisan 2021.

¹⁶ Andrea ENRIA, Chairperson of EBA, “Designing a Regulatory and Supervisory Roadmap for FinTech”. (<http://www.eba.europa.eu/documents/10180/2151635/Andrea+Enria%27s+speech+on+FinTech+at+Copenhagen+Business+School+090318.pdf>). Erişim tarihi: 16 Nisan 2021.

Kara Paranın Aklanmasının Önlenmesine Yönelik Mali Eylem Görev Gücü (FATF)¹⁷, ABD Gelir İdaresi (IRS)¹⁸ gibi mali istihbarat birimleri ve uluslararası finansal kuruluşlar kripto paraları sanal para olarak kategorize etmektedir. Bunun yanı sıra, dijital para biriminin alt birimi olarak da kategorize edilmektedir. Örnek olarak; Dünya Bankası kriptografik tekniklere dayanan dijital para birimleri olarak kabul etmektedir¹⁹. Ulusla-

rarası Ödemeler Bankası'nın (BIS) bir organı olan Ödemeler ve Piyasa Altyapıları Komitesi (CPMI) de dünya bankası ile aynı görüştedir²⁰. Son olarak Türkiye Cumhuriyet Merkez Bankası, kripto paraları yerine kripto varlık olarak ifade etmiş ve itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıklar olarak kabul etmiştir²¹.

Tablo 1: Para Matrisi

		FORMAT	
		FİZİKSEL	DİJİTAL
YASAL STATÜ	DÜZENSİZ	Bazı Yerel Para Birimleri	Sanal Paralar
	DÜZENLİ	Banknotlar ve Madeni Paralar	Dijital Paralar
			Ticari Bankalardaki Mevduat Hesabı

Kaynak: European Central Bank. "Virtual Currency Schemes". (<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>). Erişim tarihi: 16 Nisan 2021.

2- SUÇ GELİRLERİ

Suç gelirleri, doğrudan veya dolaylı olarak suç yoluyla elde edilen para / varlıkları ifade eder. Genellikle, suç işlemekten kazanılan para, varlık satın almak için kullanılır ve söz konusu varlıkları suç gelirine dönüştürür²². Kara para aklama ve Terörün Finansmanı bu kapsamda değerlendirilen suç unsurlarıdır.

2.1- Kara Para Aklama

Kara para aklama, parayı elde eden kişilerin

kimliğini gizleyerek ve bunu meşru bir kaynaktan gelmiş gibi görünen varlıklara dönüştürmesi, böylece yasadışı faaliyetten elde edilen paranın kullanılması olarak tanımlanabilir²³. Kara para aklama fikri prensip olarak basittir. Bir tür haksız (yasa dışı) kazanç elde eden kişi bu fonları, uygunsuz davranışlar sonucu elde edildiğini fark ettirmeden piyasada kullanımını sağlamasıdır. Meşru ve gayri meşru fonları karıştırarak, miktarın tamamı potansiyel olarak meşru görünebilir ve bu nedenle kara para aklayanın hedeflerine

¹⁷ FATF, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", (<http://www.fatfgafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>), Erişim tarihi: 16 Nisan 2021.

¹⁸ IRS, "Notice 2014-21". (<https://www.irs.gov/pub/irs-drop/n-14-21.pdf>). Erişim tarihi: 18 Nisan 2021.

¹⁹ World Bank Group, "Distributed Ledger Technology (DLT) and blockchain", (<http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>), Erişim tarihi: 16 Nisan 2021.

²⁰ CPMI, "Digital currencies". <https://www.bis.org/cpmi/publ/d137.pdf>. Erişim tarihi: 16 Nisan 2021.

²¹ Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik. (www.resmigazete.gov.tr). Erişim tarihi: 17 Nisan 2021.

²² India WENTWORT, "What are the Proceeds of Crime?". <https://www.delta-net.com/compliance/anti-money-laundering/faqs/what-are-the-proceeds-of-crime#:~:text=Proceeds%20of%20crime%20refer%20to,said%20assets%20proceeds%20of%20crime>. Erişim tarihi: 17 Nisan 2021.

²³ John MADINGER, Money Laundering: A Guide for Criminal Investigators. CRC Press. New York. 2012. s. 4.

ulaşarak aklanmış olabilir. Fonlar meşru işlerden gelmiş gibi görünse de fonların bir kısmı aslında bir tür suç faaliyetinden kaynaklanmıştır²⁴. Yasadışı fonları gizlemek ve bunları kayıtlı ekonomiye sokmak amacıyla üç geniş kategori bulunmaktadır. Birincisi, finansal kurumların kullanımı yoluyla; ikincisi, bir ülkeden veya yetki alanından diğerine fiziksel olarak büyük miktarda nakit para kaçırmak; üçüncüsü ise malların ticaret yoluyla transferidir²⁵.

Para aklamak için, failler parayı standart finansal kurum sistemi üzerinden hareket ettirmeli ve varlığını haklı çıkarmak için makul bir kağıt izi oluşturmalıdır. Aslında, faillerin çoğu parayı hareket ettirmek için basit, kolay anlaşılır finansal süreçler kullanır. Hızla değişen finansal ortamdaki teknoloji, para aklayıcılar için en önemli faktör olan hem yetenekler hem de uygulama kontrolü açısından bu hareketi kolaylaştırır²⁶. Bahsi geçen para ya da varlıklara, devletin el koyması, vergilendirmesi veya her iki durumun birleşiminden kaynaklanan durumlarından kaçınılması söz konusudur. Bu durumlara ek olarak hukuki davalarda yargılanma ve diğer suçlardan kaynaklanan paraların da izlenmesi sayılabilir. Özet olarak kara para aklama kavramı, bankacılık ve ticaret alanlarıyla iç içe geçmiş bir kavram olarak değerlendirilebilir²⁷.

2.2- Terörün Finansmanı

Terörizm; siyasi, dini veya ideolojik bir inancı yaymak amacıyla hükümeti, uluslararası bir kuruluşu veya halkı sindirmek için tasarlanmış, hukuka aykırı eylem tehdididir. Terörizmin finansmanı, terör eylemlerini finanse etmek için bir kişi veya gruba fon sağlama sürecidir²⁸. Herhangi bir insan teşebbüsü gibi, terörist faaliyetler de finansman gerektirir. Silah ve malzeme satın almak için fonlara ihtiyaç vardır. Terör örgütüne yeni katılanlar için eğitim, propaganda malzemeleri, işbirliği için mali teşvikler sağlamak, seyahat ve diğer lojistik giderleri bu fonlar ile karşılanır²⁹. Terörist faaliyetleri finanse etmek için kullanılacak araçlar para veya mülkleri içerir. Fonlar ve mülk, meşru veya cezai kaynaklardan olabilir. Küçük miktarlarda olabilirler³⁰. 11 Eylül saldırılarından bu yana, terörün finansmanına karşı koymaya yönelik uluslararası girişimler hızlanmıştır. Bu kurumsallaşmanın, özellikle ulusal yasal çerçevelerin oluşturulması veya iyileştirilmesi, idari altyapının oluşturulması veya güçlendirilmesi, çeşitli farklı düzenleyici önlemlerin getirilmesi ve kullanılması ve uygulama kanıtları ile ölçüldüğünde, ulusal düzeyde somut etkileri olmuştur³¹.

Kara para aklama genel çerçevede gri ekonomi unsuru olarak değerlendirilirken terörün finansmanı yasal çizginin daha da bulanıklaştığı

²⁴ Dennis COX. *Handbook of Anti Money Laundering*. John Wiley & Sons Ltd. United Kingdom. 2014. s. 6.

²⁵ John A. CASSARA. *Trade-Based Money Laundering The Next Frontier in International Money Laundering Enforcement*. John Wiley & Sons, Inc. New Jersey. 2016. s. 2

²⁶ Jonathan E. Turner. *Money Laundering Prevention: Deterring, Detecting, And Resolving Financial Fraud*. John Wiley & Sons, Inc. New Jersey. 2011. s. 89.

²⁷ Nigel MORRIS-COTTERILL. "A Brief History Of Money Laundering". (<http://www.counter.moneylaundering.com/public/content/brief-history-money-laundering>). Erişim tarihi: 18 Nisan 2021.

²⁸ Central Bank of Trinidad & Tobago. *Guideline on Anti-Money Laundering and Combatting of Terrorism Financing*. 13 Nisan 2018. s. 2.

²⁹ Yuliya ZABYELINA. *The Industry of Terror: Criminal Financing of the North Caucasus Insurgency*. (ed. Kimberley L. Thachuk ve Rollie Lal). Terrorist Criminal Enterprises - Financing Terrorism through Organized Crime. Praeger. California. 2018. s. 2018.

³⁰ Asian Development Bank. *Handbook On Anti-Money Laundering And Combatting The Financing Of Terrorism For Nonbank Financial Institutions*. Mandaluyong City, Philippines: Asian Development Bank, 2017. s. 6.

³¹ Thomas J. BIERSTEKER ve diğerleri. *International Initiatives To Combat The Financing Of Terrorism*. (Ed. Thomas J. Biersteker and Sue E. Eckert). Countering the Financing of Terrorism. Routledge. London. 2008. s. 234

karanlık ekonominin unsuru kabul edilmektedir. İnsan kaçakçılığı, uyuşturucu kaçakçılığı, silah kaçakçılığı, gasp, zorlama / gözdağı, fidye için adam kaçırma, yolsuzluk ve siber suç dahil olmak üzere temel olarak uluslararası organize suçun çeşitli yönlerine odaklanmaktadır³².

3- MALİ İSTİHBARAT BİRİMLERİ VE DİĞER ULUSLARARASI KURULUŞLARCA GETİRİLEN ÖNERİLER

Günümüzde kripto para dünyası, gelişmekte olan bir sanal para hobisi ortamından çıkıp multi-milyar dolarlık bir endüstriye dönüşmeye başlamıştır. Geçmişte nakit olarak yapılan yeraltı ekonomisi işlemleri hızla çevrimiçi ve karanlık ağa (dark web) taşınmaya başlamıştır. Bu yeni mecra hız, gizlilik, geniş kitlelere erişim gibi birçok olanak sunmaktadır. Bu süreç nihayetinde, gri ve karanlık ekonomi için yeni finansal alana dönüşmüştür³³.

Kara paranın aklanmasını önlemek ve terörizmin finansmanı ile mücadele etmek için tasarlanmış bir önlem, yasadışı faaliyetin finansmanında en yoğun kullanılan kaynaklar ve yöntemler hedeflediğinde etkili olmaktadır. Bu, ancak ülkedeki kara para aklama ve terör finansmanı risklerinin iyi bir analizi ve anlaşılması

yoluyla yapılabilir³⁴. G20 ülkelerinin desteğiyle son dönemlerde FATF, kara para aklama ve terörün finansmanı için sanal varlıkların kötüye kullanılmasını önlemek için küresel çapta, bağlayıcı standartlar yayınlamaktadır. Konuyla ilgili görüşler, kanuni para birimlerinin dijital temsilini içermeyecek şekilde düzenlenmiştir. Sanal varlıkların birçok potansiyel faydası olduğu, ancak uygun düzenlemeler olmadan, suçluların ve teröristlerin finansal işlemleri için sanal bir güvenli liman olma riski taşıdıkları vurgulanmıştır. Küresel çapta, yasal düzenleyici sistemdeki var olan yasal boşluklar, suçluların ve teröristlerin suistimal etmesi için önemli fırsatları beraberinde getirdiği üzerinde durulmuştur. Günümüzde birçok sanal varlık hizmet sağlayıcısı, “riskli iş” olarak algılanmakta, banka hesaplarına ve diğer düzenli finansal hizmetlere erişimi reddedilmektedir. FATF’in gereksinimlerini uygulamak sektör için zor olsa da, değer aktarmanın sağlam ve uygulanabilir bir yolunun arkasındaki temel yapı olarak, nihai blok zincir teknolojisine olan güveni artırması hedeflenmiştir³⁵. Blok zincir teknolojisinin yapısı itibarıyla işlemler anonim gerçekleştirilmektedir. Fakat sanal hizmet sağlayıcılar (kripto para borsaları) ilgili mali istihbarat birimleri ile koordinasyonu ve şeffaflık sağlayacak bilgi akışının oluşturulması önem arz etmektedir.

³² Colin P. Clarke. *Terrorism, Inc. The Financing of Terrorism, Insurgency, and Irregular Warfare*. Praeger. California. 2015. s. 6.

³³ Sultan OZ. *Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s*. The Cyber Defense Review. Sayı: 4/1. 2019. s. 55.

³⁴ The World Bank, “Risk Assessment Support for Money Laundering/Terrorist Financing”, (<https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support#1>). Erişim tarihi: 06 Mayıs 2021.

³⁵ FATF. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, France 2012-2020*.

(<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>). Erişim tarihi: 18 Nisan 2021.

Tablo 2: FATF'a Göre Ülkelerin ve Sanal Değer Sağlayıcılarının Üzerine Düşen Görevler

ÜLKELER	SANAL DEĞER HİZMET SAĞLAYICILARI
Sektörün karşı karşıya olduğu kara para aklama ve terör finansmanı risklerini anlaması	Müşteri durum tespiti, kayıt tutma ve şüpheli işlemlerin bildirilmesi dahil olmak üzere finansal kurumlarla aynı önleyici tedbirleri uygulanması
Sanal değer hizmet sağlayıcılarını lisanslanması veya kaydedilmesi	Transfer yaparken gönderici ve lehtar bilgilerini alınması ve bu bilgilerin saklanıp güvenliğinin sağlanması
Söz konusu sektörün, diğer finans kuruluşlarını denetler gibi denetlenmesi	

Kaynak: FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, France 2012-2020.

(<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>). Erişim tarihi: 18 Nisan 2021.

ABD Finansal Suçları Engelleme Ağı'na (FinCen); blok zincir analizi, blok zincir ağının ölçeği, eşler arası etkinliğin kapsamı, işlem bilgilerini gizlemek için anonimleştirme teknolojilerinin kullanımı ile belirli işlemlerde transferlerin ve alıcıların kimliğine ilişkin bilgi eksikliği gibi bir dizi faktörü denetimi zorlaştıran unsur olarak değerlendirmiştir. Bu kapsamda FinCen, anonimlik ile geliştirilmiş kripto para birimi türlerinin (örneğin, Monero, Zcash, Dash, Komodo ve Beam) popüleritesi artmakta ve denetim mekanizmasının hem blok zincir verilerini kullanarak işlem faaliyetlerini belirleme hem de bu faaliyeti gerçek kişiler tarafından yürütülen yasadışı faaliyetlere ilişkilendirme yeteneğini engelleyen çeşitli teknolojiler olarak görmektedir. Geliştirilen bir önlem olarak, Bank Secrecy Act'a göre; bankaların ve FinTech'lerin, sahipsiz cüzdan (un-hosted wallet) içeren sanal hizmet platformlarında yapılan 10.000 \$ 'ın üzerindeki herhangi bir kripto para birimi işleminde FinCen'e belirli müşteri bilgilerini rapor etmelerini gerektireceğini belirtmiştir³⁶. Bu uygulama bilgi edinimi koordinasyo-

nun temini için önemli bir örnektir. Fakat kripto paralar yerel çapta değerlendirilebilecek bir olgu değildir. Uluslararası boyutta bir işbirliği gerekmektedir.

Finansal İstihbarat Birimleri'nin (Financial Intelligence Units - FIUs), kara para aklama ve terörist finansmanı ile mücadelede güvenli uzmanlık ve finansal istihbarat alışverişi için bir platform sunan Egmont Grubu, 19 Haziran 2018 tarihli Official Journal of the European Union'da yer alan direktifte: "*Uluslararası kurallar standardının eksikliğinden dolayı, FIUs'lar işlevleri, yeterlilikleri ve yetkileri bakımından önemli farklılıkları sürdürmektedir. Üye Devletler, sanal para birimlerinin kötüye kullanılması ile ilgili olanlar da dahil olmak üzere terörizmle ilgili mali soruşturmaları ele almak için daha verimli ve koordineli bir yaklaşım sağlamaya çalışmalıdır. Bununla birlikte, mevcut farklılıklar bir FIUs'nun faaliyetini, özellikle de istihbarat, soruşturma ve adli faaliyetlerden ve uluslararası işbirliğinden sorumlu tüm yetkilileri desteklemek için önleyici analizler geliştirme kapasitesi etkilememelidir.*

³⁶ Financial Crimes Enforcement Network. Federal Register. Sayı: 85, No. 247. Proposed Rules. <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/FR-2020-12-23.pdf>. Erişim tarihi: 08 Mayıs 2021.

Görevlerini yerine getirirken, FIUs'lar bilgiye erişebilmeli ve yasa uygulayıcı makamlarla uygun işbirliği de dahil olmak üzere herhangi bir engel olmadan bilgi alışverişinde bulunabilmelidir. Suçtan şüphelenilen tüm vakalarda ve özellikle de terörizmin finansmanı ile ilgili durumlarda, bilgiler gecikmeden doğrudan ve hızlı bir şekilde akmalıdır. Bu nedenle, FIUs'ların yetkilerini ve işbirliğini netleştirerek FIUs'ların etkinliğini ve verimliliğini daha da arttırmak önemlidir.” ifadede yasal düzenlemelerin eksikliği, sınıflandırma ile ilgili belirsizlikler ve işbirliği konuları vurgulanmıştır³⁷. Gerekli önlemlerin hayata geçirilmesi ve işbirliği içinde uygulanması, kripto paraların kötü amaçla kullanımının önüne geçmek bu finansal eylemlerin anonimlik vasıtasıyla perdelenmesini önlemek amacıyla gerçekleştirilmelidir.

Avrupa Komisyonu'nun hazırladığı çalışmada; kanun yaptırımı açısından bakıldığında, kripto para kullanıcılarının hesap verebilirlik mekanizmalarının tanıtılması ve bu teknolojinin büyük ölçüde yasa dışı amaçlar için kullanılmasının engellenmesi gerektiğini savunmaktadır. Ancak Komisyon, gerçekleşen teknolojik yeniliklerin önüne geçilmemesi gerektiğini de belirtmiştir. Bu noktada amaç, yasadışı davranışlar ele alınırken gerçekleştirilen eylemlerin teknolojik yeniliğe ket vurmamasıdır. Kripto para birimleri cezai amaçlar için kullanılıyorsa, bu nedenle ele alınması gereken unsurun teknolojinin olmamasıdır³⁸. 2018 yılında Avrupa Komisyonu tarafından yayımlanan Beşinci Kara Para Aklamayı Önleme Yönergesi (AMLD5) Kara paranın aklanmasının önlenmesi ve terörizmin finansmanının önlen-

mesi amacıyla yetkili makamlar, yükümlü kuruluşlar aracılığıyla sanal para birimlerinin kullanımını izleyebilmesi gerektiğini öne sürmektedir. Sanal para birimlerinin yapısındaki anonimliğin, potansiyel olarak kötü niyetli kullanıma olanak sağlayacağını savunmaktadır. Anonimlikle ilgili risklerle mücadele etmek için, ulusal Finansal İstihbarat Birimleri (FIU'lar), sanal para birimi adreslerini sanal para biriminin sahibinin kimliğiyle ilişkilendirmelerine olanak tanıyan bilgileri elde edebilmesi gerektiği belirtilmiştir³⁹. Mali istihbarat birimleri ile sanal hizmet sağlayıcıları arasında gerçekleştirilmesi planlanan bu bilgi alışverişinin, finansal sistemin temel taşı olan bankalar ile desteklenmesi en sağlıklı yaklaşım olacaktır.

Güney Kore hükümeti, 30 Ocak 2018 tarihinden itibaren yalnızca, Gerçek İsim Sanal Banka Hesabı (Real Name Virtual Bank Account) kripto para alım satımına izin veren bir kural uygulamaya koymuştur. Kripto para satıcılarının, kripto para birimi alım-satımlarıyla ilgili bankalarla sözleşmeleri olması gerekmektedir. Bankalar, bu tür sözleşmeleri imzalamadan önce satıcıların yönetim ve siber güvenlik sistemlerini incelemektedir. Bir kripto para birimi alım-satımında e-cüzdan üzerinden işlem yapmak için, kripto para birimi alıcısının ve satıcısının bir bankada hesabı olması gerekmektedir. Anonim kripto para birimi kullanıcıları, kripto para birimi hesaplarından para çekebilir ancak yeni bir para yatırma işlemi yapamazlar. Küçüklerin ve yabancıların, ikamet ettikleri yerden bağımsız olarak, kripto para birimi ticareti yapmaları yasaktır⁴⁰.

³⁷ Official Journal of the European Union. “Directive 2018/843/EU”. (<https://eur-lex.europa.eu/oj/direct-access.html>) Erişim tarihi: 18 Nisan 2021.

³⁸ Robby HOUBEN ve Alexander SNYERS. “Cryptocurrencies and Blockchain: Legal Context And Implications For Financial Crime, Money Laundering And Tax Evasion”. The European Parliament. Requested by the TAX3 committee. Haziran 2018.

³⁹ Directive (Eu) 2018/843 Of The European Parliament and Of The Council. (<https://eur-lex.europa.eu/>). Erişim tarihi: 9 Mayıs 2021.

⁴⁰ Library of Congress. Regulation of Cryptocurrency Around the World. (<https://www.loc.gov/law/help/cryptocurrency/world-survey.php>). Erişim tarihi: 12 Mayıs 2021.

4- MASAK'NUN ALDIĞI ÖNLEMLER

Türkiye'de aklama suçuyla mücadele, 1996 yılında yürürlüğe giren 4208 sayılı Kara paranın Aklanmasının Önlenmesine Dair Kanunla hukuki kimlik kazanmıştır. Söz konusu suçla mücadele esas itibarıyla, 17 Şubat 1997 tarihinde Maliye Bakanlığı bünyesinde ana hizmet birimi statüsünde, doğrudan Maliye Bakanına bağlı olarak görev yapmaya başlayan MASAK tarafından yürütülmektedir. Aklama suçuyla mücadelede ulusal ve uluslararası standartlar ve ihtiyaçların değişmesi mevzuatın ve uygulamanın revize edilmesini gerektirmiştir. Bu kapsamda anılan Kanun yerine 18 Ekim 2006 tarihinde yürürlüğe giren 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun aklama suçuyla mücadele sistematığı içerisine terörizmin finansmanı suçuyla mücadeleyi de ekleyerek yürürlüğe girmiştir⁴¹. MASAK aynı zamanda FATF ve şüpheli eylem bildirim konusundaki çalışmalarıyla ön plana çıkan Egmont Grubu ile işbirliği içerisindedir. Bunun dışında konvansiyon (Viyana, Palermo) ve sözleşmelerde (Strazburg ve Varşova) taraf olarak uluslararası alanda mücadelesini sürdürmektedir. Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun'un uygulanma-

sına yönelik olarak; suç gelirlerinin aklanmasının ve terörün finansmanının önlenmesi amacıyla yükümlüler, yükümlülükler, yükümlülüklerle uyumun denetimi, gümrük idaresine açıklama yapılması ve diğer tedbirlere ilişkin usul ve esasları belirlemek amacıyla, "Suç Gelirlerinin Aklanmasının Önlenmesine Dair Tedbirler Yönetmeliği (Tedbirler Yönetmeliği)" yayımlanmıştır.

Tedbirler Yönetmeliği baz alınarak MASAK tarafından yayımlanan "Kripto Varlık Hizmet Sağlayıcılar Rehberi"nde kripto varlık hizmet sağlayıcıların müşterinin tanınması, şüpheli işlem bildirim, bilgi ve belge verme, devamlı bilgi verme ile muhafaza ve ibraz olarak tabi oldukları yükümlülükler sayılmıştır. 5549 sayılı Kanunun 13'üncü maddesinin birinci fıkrasına göre; müşterinin tanınması yükümlülüğü, devamlı bilgi verme yükümlülüğü ve şüpheli işlem bildirim yükümlülüğünün ihlallerinin tespiti halinde, MASAK tarafından Kanunda belirtilen miktarlarda ve işlem başına idari para cezası verilmesini öngörmüştür⁴². Hazine ve Maliye Bakanı'nın yaptığı açıklamada, Kripto Varlık Hizmet Sağlayıcılarının 10 bin liranın üzerinde işlem yapanları MASAK'a bildirme zorunluluğu getirildiğini açıklamıştır⁴³.

⁴¹ Mali Suçları Araştırma Kurulu Başkanlığı. "Mali Suçları Araştırma Kurulu Başkanlığı Faaliyet Raporu 2019". (https://ms.hmb.gov.tr/uploads/sites/12/2021/01/FAALIYET_RAPORU_2019-FINAL-1.pdf). Erişim tarihi: 18 Nisan 2021.

⁴² Mali Suçları Araştırma Kurulu Başkanlığı. Kripto Varlık Hizmet Sağlayıcılar Rehberi. (<https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf>). Erişim tarihi: 11 Nisan 2021.

⁴³ TRT Haber. "Kripto para için MASAK'a denetleme yetkisi". (<https://www.trthaber.com/haber/ekonomi/kripto-para-icin-masaka-denetleme-yetkisi-578917.html>). Erişim tarihi: 23 Mayıs 2021.

Tablo 3: Kripto Varlık Hizmet Sağlayıcıları Yükümlülükleri ve Cezaları

	Yükümlülük	Tek Bir İhlal İçin Verilecek İdari Para Cezası (TL)	İdari Para Cezası Üst Limit Tutarı (TL)
Müşterinin Tanınması	-Yükümlüler, müşterinin tanınmasına ilişkin esaslar kapsamında; kendileri nezdinde yapılan veya aracılık ettikleri işlemlerde işlem yapılmadan önce, işlem yapanlar ile nam veya hesaplarına işlem yapılanların kimliklerini tespit etmek ve gerekli diğer tedbirleri almak zorundadır.	30.000	4.000.000
Şüpheli İşlem Bildirimi	-Yükümlüler nezdinde veya bunlar aracılığıyla yapılan veya yapılmaya teşebbüs edilen işlemlere konu malvarlığının yasa dışı yollardan elde edildiğine veya yasa dışı amaçlarla kullanıldığına dair herhangi bir bilgi, şüphe veya şüpheli gerektirecek bir hususun bulunması halinde bu işlemlerin yükümlüler tarafından Başkanlığa bildirilmesi zorunludur. -Yükümlüler, Başkanlığa şüpheli işlem bildiriminde bulunulduğunu, yükümlülük denetimi ile görevlendirilen denetim elemanları ile yargılama sırasında mahkemeler dışında, işleme taraf olanlar dahil hiç kimseye açıklayamazlar. (ihlali halinde bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.)	50.000	4.000.000
Devamlı Bilgi Verme	-Yükümlüler taraf oldukları veya aracılık ettikleri işlemlerden, Bakanlıkça belirlenecek tutarı aşanları Başkanlığa bildirmek zorundadırlar.	30.000	4.000.000

Kaynak: 5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun. (www.mevzuat.gov.tr). Erişim tarihi: 11 Mayıs 2021.

Kripto paralar Türkiye’de ve dünyanın birçok ülkesinde yasal bir para birimi olarak kabul görmemektedir. Bu sebeple, kripto para vasıtasıyla elde edilmiş suç gelirlerinin finansal sisteme karışmasında sanal hizmet sağlayıcılarının yanı sıra bankaların göz önünde bulundurulması gerekmektedir. Kripto paranın herhangi bir kanuni paraya dönüşmesi sanal hizmet sağlayıcılarındaki hesaplardan ve ilişkili banka hesapları vasıtasıyla gerçekleşmektedir. Gerçekleştirilen

işlemlerin anonimliğinin sona erdiği sınır bu kısmıda ortadan kalkmaktadır. Bu doğrultuda, Tedbirler Yönetmeliği 18. maddesi kapsamında, “Yükümlüler karmaşık ve olağandışı büyüklükteki işlemler ile görünürde makul hukuki ve ekonomik amacı bulunmayan işlemlere özel dikkat göstermek, talep edilen işlemin amacı hakkında yeterli bilgi edinmek için gerekli tedbirleri almak ve bu kapsamda elde edilen bilgi, belge ve kayıtları istenildiğinde yetkililere sunmak üzere mu-

hafaza etmek zorundadır.” hükmü mevcuttur⁴⁴. Müşterini tanı tedbirleri kapsamında; “teknolojik risklere karşı tedbir alınması, riskli ülkelerle ilişkiler ve sıkılaştırılmış tedbirler şeklindeki tedbirler hem finansal kuruluşlarca hem de finansal olmayan belli iş ve mesleklerce yerine getirilmeli iken gibi üçüncü tarafa güven ilişkisi, muhabirlik ilişkisi ve elektronik transferlere yönelik tedbirler sadece finansal kuruluşlarca yerine getirilmelidir. Bunların dışında kalan basitleştirilmiş tedbirler, işlemin reddi ve iş ilişkisinin sona erdirilmesi, kimlik tespiti gibi müşterini tanı tedbirleri bütün yükümlülere yerine getirilmelidir”⁴⁵ şeklinde ifade edilmiştir. Bu hükümlerin kapsamı günümüz koşulları göz önünde bulundurulduğunda kripto paraları kapsayacak şekilde genişletilmesi, kripto para borsalarına sağlanan nakit akışının takibi ve ilgili makamlarının bilgilendirilmesi gerekmektedir. Son olarak, Teknolojik Risklere Karşı Tedbir Alınması, Tedbirler Yönetmeliği 19. maddesi kapsamında, “Finansal kuruluşlar, yeni ve gelişen teknolojilerin getirdiği imkânların aklama ve terörün finansmanı amacıyla kullanılması riskine karşı özel dikkat göstermek ve bunu önlemeye yönelik uygun tedbirleri almak zorundadır.” hükmü verilmiştir. Yine aynı kanun maddesinin devamında; “Finansal kuruluşlar yüz yüze olmayan işlemler yapılmasını mümkün kılan sistemleri kullanarak gerçekleştirilen hesaba para yatırma, hesaptan para çekme ve elektronik transfer gibi işlemlere özel dikkat göstermek, müşterinin mali profiline ve faaliyetlerine uygun olmayan veya faaliyetleriyle ilgisi bulunmayan işlemleri yakından izlemek, tutar ve işlem sayısı limiti belirlemek de dâhil uygun ve etkili tedbir-

leri almak zorundadır.” şeklinde açıklanmıştır⁴⁶. Kripto paraların günümüzde popüler bir teknoloji olması ve suç gelirlerinin finansmanı riskleri göz önünde bulundurulması suretiyle ilgili hüküm çerçevesinde tedbirlerin alınması gerekmektedir.

SONUÇ

Teknoloji yaşantımızda geniş çapta değişikliklere yol açmıştır. Finans dünyası, bu değişikliklerin etkilerini yoğun olarak hisseden alanlardan biri olmuştur. Elektronik para ve türevi birçok kavram artık günlük hayatta bir şekilde (yatırım-değişim aracı) kullanılmaktadır. Fiziki olarak kullanımda kabul görmüş banknot ve madeni paralar artık dijital varlıklara yerini bırakmaya başlamıştır. İlk kez kaydi para olarak bilgisayar ekranlarında gördüğümüz paralar artık dijital, sanal ve kripto olarak popülerlik kazanmaya başlamıştır. Bu durum suç gelirlerine de bir araç olarak kullanılmasının da önünü açmıştır. Bu kapsamda yapılan değerlendirmede;

- Sanal varlık hizmet sağlayıcılarına karşı duyulan güvensizlik ortamı ve birçok ülkede yasal düzenlemelerin yeni uygulamaya konulması, bu yeni finansal mecralarda gerçekleştirilen işlemlerin takip ve denetimine olanak vermemiştir. Kripto para olarak gerçekleştirilen işlemlerin anonim olması sebebiyle takip edilememesi, ilgili kuruluşlarca kanuni paraya dönüştürülmesinde önemli yerlerden biri olan kripto para borsalarının önemini arttırmış durumdadır. Bu açıdan sanal hizmet merkezlerinin yasal çerçevede tanınıp, bilgi alışverişini sağlayacak düzenlemelerin hayata geçiril-

⁴⁴ Suç Gelirlerinin Aklanmasının Önlenmesine Dair Tedbirler Yönetmeliği. (www.masak.hmb.gov.tr). Erişim tarihi: 18 Nisan 2021.

⁴⁵ Mali Suçları Araştırma Kurulu Başkanlığı. “Yükümlülükler”. (https://masak.hmb.gov.tr/yukumlulukler). Erişim tarihi 18 Haziran 2021.

⁴⁶ Suç Gelirlerinin Aklanmasının Önlenmesine Dair Tedbirler Yönetmeliği. (www.masak.hmb.gov.tr). Erişim tarihi: 18 Nisan 2021.

mesi önem arz etmektedir. MASAK, Kripto Varlık Hizmet Sağlayıcılar Rehberi vasıtasıyla tedbirler yönetmeliği çerçevesinde müşterinin tanınması yükümlülüğü, devamlı bilgi verme yükümlülüğü ve şüpheli işlem bildirimi yükümlülüğü hayata geçirilmiştir. TCMB tarafından yasal olarak tanımlanması ve MASAK tarafından atılan adımlar temel nitelikte olup kripto paraların gelecek perspektifte gelişimi göz önünde bulundurularak geliştirilmesi gerekmektedir.

- Suç gelirleri ile kripto para kullanımının arasındaki ilişki yerel boyutta değerlendirilecek bir mesele değildir. Anonim gerçekleştirilen işlemlerin, özellikle suç unsuru barındırdığı şüphesi varsa, geniş bir coğrafyayı kapsayacak şekilde takibi gerekmektedir. Sanal hizmet sağlayıcılarının verilenin paylaşılması karşılaştırarak analizinin yapılması gerekmektedir. Herhangi bir devletin kendi sınırları içerisinde uygulaya koyacağı bir düzenleme yeterli olmayacaktır. Bu açıdan mücadelenin uluslararası alanda yürütülmesi gerekmektedir. Mali istihbarat birimlerinin koordineli bir şekilde hareket etmesi için uygulamalara standardizasyon getirilmelidir. MASAK bu açıdan FATF ile koordineli bir şekilde çalışmaktadır.
- Kripto borsalarda gerçekleştirilen işlemlerin belirli bir miktarın üstünde olması durumunda bildirilmesi tek başına çözüm olmayacaktır. İşleme konu olan miktar sınır belirlemeksizin Tedbirler Yönetmeliği kapsamında özel dikkat gerektiren işlemler ve Teknolojik Risklere Karşı Tedbir hükümlerinin de devreye girmesi gerekmektedir.
- Kripto para işlemlerine yönelik yalnızca sanal hizmet sağlayıcılarından bilgi edinilmesi yeterli olmayacaktır. Çünkü kripto para borsalarında kripto para alımı ya da sahip olunan kripto paraların kanuni paraya dönüştürülmesi neticesinde gerçekleştirilen iş-

lemler finansal sisteme nüfus edecektir. Bu kapsamda finansal sistemin temel taşı olan bankalardan, kripto para borsalarıyla ilişkili olan mevduat bilgilerinin ilgili makamlarca edinilmesi gerekmektedir. Türkiye’de, bilgi edinme ve bilgi akışında koordinasyonun sağlanmasında MASAK’la beraber TCMB, Sermaye Piyasası Kurulu, Bankacılık Düzenleme ve Denetleme Kurumu’nun ortak hareket etmesi gerekmektedir.

KAYNAKÇA

- ALTUCHER, J. (2017). *Crypto-Currencies 101*. Laissez Faire Books. Maryland.
- Anon Collective, “*Book of Anonymity - Big Data’s End Run around Anonymity and Consent*”, (<https://punctumbooks.com/titles/book-of-anonymity/>), Erişim tarihi: 19 Mayıs 2021.
- Asian Development Bank. (2017). *Handbook On Anti-Money Laundering And Combating The Financing Of Terrorism For Non-bank Financial Institutions*. Mandaluyong City, Philippines: Asian Development Bank,
- BIERSTEKER, T. J., ECKERT, S. E, ROMANIUK, P. (2008). *International Initiatives To Combat The Financing Of Terrorism*. (Ed. Thomas J. Biersteker and Sue E. Eckert). *Countering the Financing of Terrorism*. Routledge. London.
- CASSARA, J. A. (2016). *Trade-Based Money Laundering The Next Frontier in International Money Laundering Enforcement*. John Wiley & Sons, Inc. New Jersey.
- Central Bank of Trinidad & Tobago. (2018). *Guideline on Anti-Money Laundering and Combatting of Terrorism Financing*.
- CHAUM, D. “*Blind Signature For Untraceable Payments*” (<https://scweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF>). Erişim tarihi: 02 Mayıs 2021.

- CHU, D. (2018). *"Broker-Dealers For Virtual Currency: Regulating Cryptocurrency Wallets And Exchanges"*. Columbia Law Review. Sayı: 118/8.
- COX. D. (2014). *Handbook of Anti Money Laundering*. John Wiley & Sons Ltd. United Kingdom.
- CPMI. *"Digital currencies"*. <https://www.bis.org/cpmi/publ/d137.pdf>. Erişim tarihi: 16 Nisan 2021.
- DIFFIE, W. ve HELLMAN, M. E. (1976). *"Multiuser Cryptographic Techniques"*. National Computer Conference.
- Directive (Eu) 2018/843 Of The European Parliament and Of The Council. (<https://eur-lex.europa.eu/>). Erişim tarihi: 9 Mayıs 2021.
- ENRIA, A. *"Designing a Regulatory and Supervisory Roadmap for FinTech"*. (<http://www.eba.europa.eu/documents/10180/2151635/Andrea+Enria%27s+speech+on+FinTech+at+Copenhagen+Business+School+090318.pdf>). Erişim tarihi: 16 Nisan 2021.
- ESMA, EBA & EIOPA. *"Warning on the risks of Virtual Currencies"*. (https://www.esma.europa.eu/sites/default/files/library/esma501641284_joint_esas_warning_on_virtual_currenciesl.pdf). Erişim tarihi: 16 Nisan 2021.
- European Central Bank. *"Virtual Currency Schemes"*. (<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>). Erişim tarihi: 16 Nisan 2021.
- FATF. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, France 2012-2020*. (<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>). Erişim tarihi: 18 Nisan 2021.
- FATF. *"Virtual Currencies – Key Definitions and Potential AML/CFT Risks"*, (<http://www.fatfgafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>), Erişim tarihi: 16 Nisan 2021.
- FANTI, G., VENKATAKRISHNAN, S. B., BAKSHI, S., DENBY, B., SHRUTI, B., MILLER, A., VISWANATH, P. (2018). *"Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees"*. Proc. ACM Meas. Anal. Comput. Syst. Sayı: 2/2.
- Financial Crimes Enforcement Network. Federal Register. Sayı: 85, No. 247. Proposed Rules. <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/FR-2020-12-23.pdf>. Erişim tarihi: 08 Mayıs 2021.
- Government Office for Science. (2016). *"Distributed Ledger Technology: beyond block chain"*. A report by the UK Government Chief Scientific Adviser.
- HOUBEN, R. ve SNYERS, A. (2018). *"Cryptocurrencies and Blockchain: Legal Context And Implications For Financial Crime, Money Laundering And Tax Evasion"*. The European Parliament. Requested by the TAX3 committee.
- IMF Staff Discussion Note, *"Virtual Currencies and Beyond: Initial Considerations"*, (<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>), Erişim tarihi: 16 Nisan 2021.
- IRS. *"Notice 2014-21"*. (<https://www.irs.gov/pub/irs-drop/n-14-21.pdf>). Erişim tarihi: 18 Nisan 2021.
- JAKOBSSON, M. ve JUELS, A. (1999) *Proof of Work and Bread Pudding Protocols*. (ed. Bart Preneel). Secure Information Networks - Communications and Multimedia Security -IFIP TC6/C11 Joint Working Conference on Communications and Multimedia Security (CMS'99) September 20-21, 1999 Leuven, Belgium. Springer Science+Business Media. Germany.
- Library of Congress. Regulation of Cryptocurrency Around the World. (<https://www.loc.gov/congressional-reporting/summary.aspx?docId=113547>)

- www.loc.gov/law/help/cryptocurrency/world-survey.php). Erişim tarihi: 12 Mayıs 2021.
- MADINGER, J. (2012). *Money Laundering: A Guide for Criminal Investigators*. CRC Press. New York.
 - Mali Suçları Araştırma Kurulu Başkanlığı. "Mali Suçları Araştırma Kurulu Başkanlığı Faaliyet Raporu 2019". (https://ms.hmb.gov.tr/uploads/sites/12/2021/01/FAALIYET_RAPORU_2019-FINAL-1.pdf). Erişim tarihi: 18 Nisan 2021.
 - Mali Suçları Araştırma Kurulu Başkanlığı. *Kripto Varlık Hizmet Sağlayıcılar Rehberi*. (<https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf>). Erişim tarihi: 11 Nisan 2021.
 - Mali Suçları Araştırma Kurulu Başkanlığı. "Yükümlülükler". (<https://masak.hmb.gov.tr/yukumlulukler>). Erişim tarihi 18 Haziran 2021.
 - Merriam-Webster Dictionary. "Cryptocurrency". (<https://www.merriam-webster.com/dictionary/cryptocurrency>). Erişim tarihi: 17 Nisan 2021.
 - MORRIS-COTTERILL, N. "A Brief History Of Money Laundering". (<http://www.countermoneylaundering.com/public/content/brief-history-money-laundering>). Erişim tarihi: 18 Nisan 2021.
 - Official Journal of the European Union. "Directive 2018/843/EU". (<https://eur-lex.europa.eu/oj/direct-access.html>). Erişim tarihi: 18 Nisan 2021.
 - OZ, S. (2019). *Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s*. The Cyber Defense Review. Sayı: 4/1.
 - Ödemelerde Kripto Varlıkların Kullanılmasına Dair Yönetmelik. (www.resmigazete.gov.tr). Erişim tarihi: 17 Nisan 2021.
 - SHERMAN, A. T., JAVANI, F., ZHANG, H., GOLASZEWSKI, E. (2019). "On the Origins and Variations of Blockchain Technologies". IEEE Computer and Reliability Societies. Sayı: 17/1.
 - Suç Gelirlerinin Aklanmasının Önlenmesine Dair Tedbirler Yönetmeliği. (www.masak.hmb.gov.tr). Erişim tarihi: 18 Nisan 2021.
 - ÜSTÜN, O. (2016). *Açıklamalı İngilizce - Türkçe Karapara Terimleri ve Kavramları Sözlüğü*. Türkiye Bankalar Birliği. Matsis Matbaası. İstanbul.
 - WENTWORT, I. "What are the Proceeds of Crime?". (<https://www.delta-net.com/compliance/anti-moneylaundering/faqs/whataretheproceedsofcrime#:~:text=Proceeds%20of%20crime%20refer%20to,said%20assets%20proceeds%20of%20crime>). Erişim tarihi: 17 Nisan 2021.
 - World Bank Group. "Distributed Ledger Technology (DLT) and blockchain", (<http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>). Erişim tarihi: 16 Nisan 2021.
 - The World Bank, "Risk Assessment Support for Money Laundering/Terrorist Financing", (<https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support#1>). Erişim tarihi: 06 Mayıs 2021.
 - TRT Haber. "Kripto para için MASAK'a denetleme yetkisi". (<https://www.trthaber.com/haber/ekonomi/kripto-para-icin-masaka-denetleme-yetkisi-578917.html>). Erişim tarihi: 23 Mayıs 2021.
 - ZABYELINA, Y. (2016). *The Industry of Terror: Criminal Financing of the North Caucasus Insurgency*. (ed. Kimberley L. Thachuk ve Rollie Lal). Terrorist Criminal Enterprises - Financing Terrorism through Organized Crime. Praeger. California.