

KRİPTO PARALARIN KARAPARA AKLAMA YÖNTEMİ OLARAK KULLANILMASI^(*)

Prof. Dr. Murat BALCI^(**)
Dr. Öğr. Üyesi Kerim ÇAKIR^(***)

Öz: Ekonomi ve finans dünyasındaki gelişmelere paralel olarak, suç işleyerek gelir elde eden kimseler karaparayı kripto para birimleri aracılığıyla aklamaya başlamıştır. Kripto para birimlerinin kendine özgü bir varlık değerinin bulunması ve uçtan uca şifreleme yöntemi ile transfer edilebilme imkanı, son yıllarda suç gelirlerinin nakde çevrilmesinde kripto para birimlerinin tercih edilme sebebi olmuştur.

Karapara aklama, yeni aklama yöntemleri ile sürekli gündemde olan bir suç tipidir. Bu çalışmanın konusunu da karapara aklama yöntemlerinden biri haline gelen kripto paralarla karapara arasındaki ilişki oluşturmaktadır. Suç işlenerek elde edilen malvarlığı değerlerine bugün itibariyle sanal malvarlığı olarak kripto paralar da dahildir. Kripto para birimlerinin anonim ve küresel olması, merkezi bir otoriteye tabi olmaması karapara aklamayı kolaylaştırıcı özellikler olarak karşımıza çıkmaktadır. Çalışmamızda da kripto para birimlerinin karapara aklamayı kolaylaştırıcı özellikleri, kripto para dolandırıcılığı ve hırsızlığı gibi karapara aklama suçunun varlık sebebi olan öncül suçlar ve bu suçlardan elde edilen gelirlerin Türk Ceza Kanunu'nun 282'nci maddesinde düzenlenen karapara aklama suçuna konu olması incelenecektir.

Anahtar Kelimeler: Karapara Aklama, Kripto Para, Suç Geliri, Bitcoin, Blokszincir.

USING CRYPTOCURRENCIES AS A MONEY LAUNDERING METHOD

Abstract: In parallel with the developments in the world of economy and finance, people who earn income by committing crimes have started to launder money through cryptocurrencies. Cryptocurrencies have a unique asset value and the possibility of transferring them with end-to-end encryption method has been the reason why cryptocurrencies are preferred in cashing the proceeds of crime in recent years.

Money laundering is a type of crime that is constantly on the agenda with new laundering methods. The subject of this study is the relationship between crypto money, which has become one of the money laundering methods, and money. As of today, cryptocurrencies as virtual assets are included in the assets obtained by committing crimes. The fact that

^(*) Makalenin Gönderim Tarihi: 15.07.2021,
Makalenin Birinci Hakem Tarafından Kabul Tarihi: 05.08.2021,
Makalenin İkinci Hakem Tarafından Kabul Tarihi: 13.08.2021.

^(**) Fatih Sultan Mehmet Vakıf Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Usul Hukuku, Öğretim Üyesi,
E-posta: balci53@hotmail.com; Orcid no: <https://orcid.org/0000-0002-8506-7911>.

^(***) Marmara Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Usul Hukuku Anabilim Dalı, Öğretim Üyesi,
E-posta: kerimcakir@marmara.edu.tr; Orcid no: <https://orcid.org/0000-0003-1821-9935>.

cryptocurrencies are anonymous and global and not dependent on a central authority are the features that facilitate money laundering. In our study, money laundering facilitating features of cryptocurrencies, precursor crimes such as crypto money fraud and theft, which are the reason for the existence of money laundering crime, and the revenues obtained from these crimes will be examined in the money laundering crime regulated in Article 282 of the Turkish Penal Code.

Keywords: Money Laundering, Cryptocurrency, Proceeds of Crime, Bitcoin, Blockchain.

Giriş

Günümüz teknolojisi kripto para birimleri marifetiyle karapara aklamayı kolaylaştırmaktadır. Kripto para adresleri ve protokolleri müşteri kimliği gerektirmediğinden, gerçek kişi ile sanal para hesabı arasındaki bağları ortadan kaldırmak mümkün hale geldiğinden suç işlenerek elde edilen değerler (suç gelirleri) kripto paralarla aklama faaliyetine konu olmaya başlamıştır.

Kripto para birimlerinin ve blokzincir teknolojisinin pazar hacmi küçük olsa da bir ödeme ve yatırım aracı olarak önemleri giderek artmaktadır. Kripto paraların da karaparalar gibi kriminal bir alan olduğu ve kripto para birimlerinin gelir elde edilen suç faaliyetlerini anımsattığı yaygın bir kanaat haline gelmiştir. Ancak başlangıçta belirtelim ki kripto paraları ve bu paraların işlem gördüğü platform ve borsaları doğrudan suçla ilişkilendirmek ve özellikle karapara aklama faaliyetine konu olduğunu iddia etmek doğru değildir. Kripto paralara yatırım yapmak, alım satımı ile meşgul olmak ya da ticari platformlarda veya borsalarda işlem yapmak suç teşkil eden fiiller değildir. Bu sebeple kripto paraların meşru olmayan ve suça konu olan para birimleri gibi değerlendirilmesi yerinde olmayacaktır. Esasında kripto paraların karapara aklama suçu ile birlikte değerlendirilmesinin sebebi kripto paraların özelliklerinin kullanıcılara sunduğu avantajlardır.

Kripto paralar, suç işlemek veya terörizmi desteklemek amaçlı işlemlerde doğrudan kullanılabilmesi gibi yasa dışı eylemlerle ilişkili finansal faaliyetleri gizlemek veya teşvik etmek için de kullanılabilir. Suç işleyerek gelir elde eden kişiler yasa dışı gelirlerini aklamak için kripto para birimini giderek daha fazla kullanmaktadırlar.

Kripto paralar finans kuruluşlarının hiçbir müdahalesi olmaksızın kullanılabilir. Son yıllarda kullanımı hızla arttığından karapara aklama ile ilgili riskler hakkında finans kurumları uyarılarda bulunmaya başlamıştır. Özellikle karapara aklama ve kripto para birimleri analiz edilerek örneğin, ilk kripto para birimi olan Bitcoin'in gerçekten karapara aklamaya ne ölçüde uygun olduğu, kripto para biriminin hangi özelliklerinin karapara aklama için bir katalizör olarak işlev gördüğü ve bundan hangi yeni karapara aklama tekniklerinin ortaya çıktığı karapara aklama suçuyla mücadele bakımından önemlidir. Ayrıca siber suçlarda özellikle kritik altyapılara yönelik hacker saldırıları ve dijital şantajlar hız kazandığından Bitcoin gibi yeni ödeme yöntemlerinin sadece fırsatlar değil, aynı zamanda riskler getirdiği de ortadadır.

I. Karapara ve Kripto Para

Karapara, yasadışı yollardan sağlanan kazançtır. Karapara terimine karşılık olarak İngilizce’de “dirty money” (kirli/karapara) veya “proceeds of crime” (suç geliri) terimleri kullanılmaktadır.¹ Meşru yollardan elde edilmeyen, kirli işlerden kazanılan para veya suç kaynaklı, kaçakçılık, eroin satışı, kadın ticareti vb. yasa dışı faaliyetlerden elde edilen para anlamlarında da kullanılmaktadır.

Ceza hukuku anlamında karapara, yasa dışı faaliyetlerle diğer bir deyişle konusu suç teşkil eden fiillerin işlenmesiyle elde edilen para, mal, gelir veya sair değerleri ifade eder.² Kısacası karapara, kaynağı yasadışı olan paradır. Her türlü kriminal aktiviteden elde edilen kazanç da karapara olarak tanımlanabilir.

Kripto para ise işlemleri güvenceye almak için kriptografi yani şifreleme kullanan, çalışma şekli nakite alternatif bir değişim aracı olarak tasarlanmış varlık değeri bulunan bir sanal para birimidir. Kripto paralar, merkezi elektronik para ve merkezi bankacılık sistemlerin aksine tümüyle merkeziyetsizlerdir. Her bir kripto para biriminin merkeziyetsizliği, veri tabanı olarak işlev gören bir blokzincirinden (Blockchain) gelmektedir.³ 2009’da Satoshi Nakamoto tarafından oluşturulan Bitcoin, ilk merkeziyetsiz kripto paradır. O zamandan beri birçok farklı kripto para ortaya çıkmıştır. Bitcoin dışındaki kripto para birimlerine genel olarak altcoin denilir ki bu kısaltma alternatif ve coin yani madeni para’nın birleşimidir.⁴

Kripto paralar online (çevrimiçi) işlem gören ve diğer para birimlerine dönüştürülen, merkezileştirilmemiş, Peer-to-Peer⁵ network-tabanlı bir sanal para

¹ https://tr.wikipedia.org/wiki/Para_aklama, (Erişim tarihi: 10.06.2021).

² “Karapara” terimi mevzuatımıza ilk defa 4208 Sayılı Kanun ile girmiş ve suç tipi de “karapara aklama suçu” olarak isimlendirilmiştir. Karapara terimi, hukuki bir nitelik taşımasa da madde metninde kullanılarak hukuki bir nitelik kazandırılmaya çalışılmıştır. Doktrinde de yaygın kanaat, karapara kavramının hukuki bir kavram olmadığı yönündedir. 5237 Sayılı Türk Ceza Kanunu’nda, “suçtan kaynaklanan malvarlığı değerlerini aklama” ifadesinin, 5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunu’nda da “suç geliri” ifadesinin kullanılmasıyla “karapara” kavramının kullanımı azalmıştır. Nitekim 5549 sayılı Kanunun 26. maddesinin 3. fıkrasında da mevzuatta yer alan “karapara” ibaresinden “suçtan kaynaklanan malvarlığı değeri”, “karapara aklama suçu” ibaresinden “aklama suçu”nun anlaşılması gerektiği belirtilmiştir. 4208 sayılı Kanun’un 2-a maddesinde, karaparanın tanımına yer verilmekteydi. Buna göre, karapara “... fiillerin işlenmesi suretiyle elde edilen para veya para yerine geçen her türlü kıymetli evrakla, mal veya gelirleri veya bir para biriminden diğer bir para birimine çevrilmesi de dahil, sözü edilen para, evrak, mal veya gelirlerin birbirine dönüştürülmesinden elde edilen her türlü maddi menfaat ve değeri” ifade etmekteydi. Gbi bkz. Çakır, Kerim, *Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu*, Ankara 2016, s. 11 vd.

³ Tahan, Özge, *Kripto Paraların Türk ve Alman Ceza Hukuku Düzenlemeleri Yönünden Değerlendirilmesi*, Suç ve Ceza Dergisi, Cilt: 14, Sayı: 1, Mart 2021, s. 108.

⁴ https://tr.wikipedia.org/wiki/Kripto_para, (Erişim tarihi: 10.06.2021).

⁵ Peer-to-peer ya da P2P olarak tanımlanır. Peer eş, denk demektir. İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür. Eşler, sunucuları veya sabit bilgisayarlar tarafından merkezi koordinasyon ihtiyacı olmadan, işlemci gücü, disk depolama veya ağ bant genişliği gibi kendi kaynaklarının bir kısmını, doğrudan diğer ağ katılımcıları için kullanılabilir yapabilir. Sadece sunucuların tedarikçi ve istemcilerin tüketici olduğu geleneksel istemci-sunucu modelinin aksine, eşler, hem tedarikçi hem de tüketicidir. Peer-to-peer yazılımlarıyla, kullanıcılar her türlü diji-

birimidir.⁶ Sistem, bir algoritma ile otomatik olarak yönetilen Peer-to-Peer networküne dayanmaktadır.⁷

Merkezi bir otoriteye bağlı olmayan kripto para birimleri esasında kullanıcılarına birçok avantaj sunar. Merkez bankalarından, devletlerden ve kredi kuruluşlarından bağımsız olarak doğrudan kullanıcılar arasında alınıp satıldığından, neredeyse tamamen hükümet müdahalesinin ötesinde, küresel bir erişime sahiptir. Bu durum suçlulara cazip gelirken idari makamlar düzenleyici işlemler yapma konusunda; adli makamlar ise kripto paralar marifetiyle işlenen suçların önlenmesi konusunda zorluklarla karşılaşmaktadırlar. Bu sebeple ülkeler kripto para üretimi, ihracı ve ticareti konusunda bu varlıkların ödemelerde kullanılmaması, ödeme hizmetinin sunulmaması yahut elektronik paralarla birlikte işlem görmemesi konusunda düzenlemeler yapmaktadır.⁸

Kripto paraların ceza hukuku ile ilişkisi bakımından suçta konu olduğu alanlardan biri ise suç işlenerek elde edilen malvarlığı değerlerinin aklanmasıdır. Günümüzde hukuk ve teknolojinin gelişiminin büyük ölçüde farklılaştığı ortadadır. Teknoloji hızla gelişirken hukukun bu gelişmenin hızını yakalayamadığı ve teknolojinin gerisinde kaldığını söylememiz gerekir. Bununla birlikte hem ulusal hem de uluslararası düzenlemelerde suç işlemenin gelir kaynağı olarak görülmemesi ve kişilerin suç işleyerek kazanç elde etmesinin önüne geçmek için çaba gösterilmektedir. Kripto paraların karapara aklamanın aracı olduğu düşüncesi önceleri internet için de tartışılmıştı.⁹ Özellikle 2000'li yılların başında internetin karapara aklamanın aracı olacağı ve küresel ölçekte suçun sınırının tespit ve tayin edilemeyeceği belirtilmekteydi.¹⁰

tal içeriklerini uygulamaları kullananlarla paylaşabilirler. Bu işlem bu tanımıyla yasal olsa da, paylaşılan içerikler telif haklarıyla korunan ve parayla satılan içerikler olduğunda (ticari müzik albümleri, prodüksiyonlu filmler, lisanslı yazılımlar vesaire) bu içeriklerin paylaşılması ve paylaşan kişilerden edinilmesi illegal hale gelir. Ancak yasadışı hale gelen yazılımlar ve teknoloji değil, bunun kötüye kullanımınıdır. Bkz. <https://tr.wikipedia.org/wiki/Peer-to-peer> (Erişim tarihi: 07.05.2021).

⁶ Avrupa Merkez Bankası'nın (ECB), Ekim 2012'de konuya ilişkin hazırladığı raporda sanal para birimi "Genellikle geliştiricileri tarafından ihraç ve kontrol edilen, belli bir sanal ortamın üyeleri tarafından kabul edilen ve kullanılan, kanunlarla düzenlenmemiş dijital bir para çeşidi" şeklinde tanımlanmıştır. (ECB, 2012, s. 5) Bkz. Üzer, Betül, *Sanal Para Birimleri*, Uzmanlık Yeterlik Tezi, Türkiye Cumhuriyet Merkez Bankası Ödeme Sistemleri Genel Müdürlüğü, Ankara 2017, s. 9.

⁷ Chia Huang, Chung-Trangle, Asher, *Anti-Money Laundering and Blockchain Technology*, CSP023, May 2020, s. 21; Sicignano, Gaspare Jucan, *Money Laundering using Cryptocurrency: The Case of Bitcoin!*, Athens Journal of Law, Volume 7, Issue 2, April 2021, s. 256.

⁸ Türkiye Cumhuriyet Merkez Bankası 16 Nisan 2021 tarih ve 31456 sayılı Resmi Gazete'de "Ödemelerde Kripto Varlıklarının Kullanılmamasına Dair Yönetmelik" yayımlanmış ve bahse konu yönetmelik 30 Nisan 2021 tarihinde yürürlüğe girmiştir.

⁹ Kripto paraların suç işlemek amacıyla üretildiğini ve kullanıldığını iddia etmek doğru değildir. İnternet sayesinde bilgisayar ve bilişim uzmanları 1990'lı yıllardan (Cypherpunks) itibaren dijital para projesi üzerinde çalışmaktadır.

¹⁰ Grzywotz, Johanna, *Virtuelle Kryptowährungen und Geldwäsche, Internetrecht und Digitale Gesellschaft*, Band 15, Berlin 2019, s. 110.

İlk kripto para birimi olarak karşımıza çıkan Bitcoin'in temeli blockchain'dir. Bitcoin blockchain'i, bitcoin kripto para birimi için merkezi olmayan bir banka gibi çalışmaktadır. Bitcoin işlemleri doğrudan bitcoin adresleri arasında yapılır.¹¹ Bu anlamda, blockchain halka açık ve doğrulanabilir bir defter olarak görülür. Tüm işlemler blokzincirine kaydedilir ve blockchain.info ve diğer açık kaynaklı internet siteleri gibi herkese açık internet siteleri aracılığıyla denetlenebilir. Herhangi biri, herhangi bir yerde gerçek zamanlı olarak bir bitcoin adresinden diğerine yapılan tüm bitcoin işlemlerini görebilir. Bir bitcoin adresindeki bitcoin miktarının mevcut bakiyesi de blokzincirinde görülebilir. Açıklığına rağmen, bitcoin sistemi yüksek düzeyde anonimlik sağlar. Bu anonimliğin nedeni, banka hesaplarının aksine bitcoin adreslerinin şahıslara kayıtlı olmamasıdır.¹² Bu düzeyde anonimlik, Bitcoin'in yasadışı faaliyetlerde neden bu kadar popüler hale geldiğini açıklamaktadır.

Bir bitcoin işlemi birkaç unsurdan oluşur. Bitcoin işlemleri birbirine bağlı olduğundan, her girdi otomatik olarak önceki bir işlemin çıktısıdır. Bu şekilde bitcoin çıktısının değeri, önceki işlemlere kadar izlenebilir.¹³

Kripto paralarla ilgili blokzincir (blockchain) ve peer to peer teknolojisinden de bahsedilmesi gerekmektedir. Önemli bir teknoloji olan blokzincir, işlem kayıtlarını bir bloğa yerleştiren veri tabanı çeşididir. Her bir blok, şifresel bir imza kullanılarak bir sonraki bloğa zincirlenir. Bu ağ içerisinde veriler sıralı bir şekilde bloklara kaydedilir.¹⁴ Blokzincir teknolojisi, Bitcoin işlemleri bakımından halka açık defter biçiminde 2009 yılında kullanılmaya başlamıştır. Blokzincir teknolojisi aynı Bitcoin'in iki defa aynı kişi tarafından işlem görmemesi için, iki Bitcoin hesabı arasındaki işlemi doğrulayabilme görevi görür. Çünkü Bitcoin, geleneksel finansal sistemin dışında ve işlemleri yürütmek için banka gibi güvenilir bir üçüncü taraf kullanmadan, para birimlerinin değişiminin bir yolu olarak tasarlanmıştır.¹⁵

Blokzincir, güvenilir üçüncü tarafın yerine geçerek ve her bir işlemin kaydını yapan defter görevini üstlenir. Ödeme geçmişini doğrulayabilecek ve herhangi bir zamanda her bir Bitcoin sahibinin hesabıyla ilişkilendirilmiş Bitcoin'lerin sayısı blokzincir teknolojisi ile tespit edilir. Bitcoin için, bu blokzincir defteri eş zamanlı olarak dünyaya yayılmış binlerce bilgisayarda aynı şekilde mevcut olup kamuya açık hale getirilir. Her bir yeni Bitcoin işlemi "zincire" diğer bir "blok" eklenerek kaydedilir ve daha sonra her bir internet düğümü tarafından paylaşı-

¹¹ Wegberg, Rolf van - Oerlemans, Jan Jaap - Deventer, Oskar van, *Bitcoin Money laundering*, Journal of Financial Crime Vol. 25 No. 2, 2018 (419-435), s. 423.

¹² Wegberg - Oerlemans - Deventer, s. 422; Chia Huang-Trangle, s. 13.

¹³ Wegberg - Oerlemans - Deventer, s. 423; Chia Huang-Trangle, s. 13.

¹⁴ Üzer, s. 24.

¹⁵ Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>, s. 1 vd. (Erişim tarihi: 07.06.2021).

larak kamuya açık defterde yansıtılır.¹⁶ Aleni ve kamuya açık olmasına rağmen, blokzincir zannedilenin aksine son derece emniyetli ve güvenilirdir.¹⁷

Peer-to-peer (P2P) teknolojisi ise iki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür.¹⁸ Eşler, sunucuları veya sabit bilgisayarlar tarafından merkezi koordinasyon ihtiyacı olmadan, işlemci gücü, disk depolama veya ağ bant genişliği gibi kendi kaynaklarının bir kısmını, doğrudan diğer ağ katılımcıları için kullanılabilir yapabilir. Sadece sunucuların tedarikçi ve istemcilerin tüketici olduğu geleneksel istemci-sunucu modelinin aksine, eşler, hem tedarikçi hem de tüketicidir.¹⁹ Kripto para birimi satın almak veya satmak isteyen bireyler genellikle peer to peer dönüştürücüler veya tacirler olarak anılan bireylerin networküne yönelmektedir.²⁰

P2P dönüştürücüler genel olarak merkezi operatörü olmayan online borsa platformlarını veya web sitelerini kullanırlar. Her ne kadar P2P borsa platformlarının birçoğu, merkezileştirilmiş sanal malvarlığı borsaları tarafından sunulan hizmetlere benzer hizmetler sunsalar da P2P borsa platformları, geleneksel finans kuruluşlarını kullanmadan kripto paraların platformlar arası ticaretine imkan sunmaktadır.²¹

II. Kripto Paraların Karapara Aklamayı Kolaylaştıran Özellikleri

Kripto paraların suç gelirlerinin aklanmasını neden ve nasıl kolaylaştırdığını açıklığa kavuşturmak için kripto para ekosisteminin özellikleri incelenmelidir. Kripto paralar herhangi bir coğrafi kısıtlamaya maruz kalmadığından online olarak sınır ötesi işlem yapmaya imkan sağladığından suç işleyerek gelir elde eden ve bu gelirleri kripto paralar marifetiyle aklayarak yasal ekonomik sisteme dahil etme konusunda suçlulara birçok avantaj sunmaktadır.²² Kripto paralarla suç işlenmesi, bu paraların suça konu olması ve Blockchain teknolojileri, adli ve idari makamları yeni mücadelelerle karşı karşıya bırakmaktadır.²³

¹⁶ Dyntu, Valeriia - Dykyi Oleh, *Cryptocurrency in the System of Money Laundering*, Baltic Journal of Economic Studies Vol. 4, No. 5, 2018, (75-81), s. 77; Chia Huang-Trangle, s. 9.

¹⁷ Dyntu - Dykyi, s. 77; Chia Huang-Trangle, s. 9.

¹⁸ Peer-to-Peer File Sharing: A Guide for Business, Federal Trade Commission, s. 1. Bkz. <https://www.ftc.gov/system/files/documents/plain-language/bus46-peer-peer-file-sharing-guide-business.pdf>, (Erişim tarihi: 20.06.2021).

¹⁹ Peer-to-peer ya da P2P olarak tanımlanır. Peer eş, denk demektir. Bkz. <https://tr.wikipedia.org/wiki/Peer-to-peer>, (Erişim tarihi: 03.06.2021).

²⁰ Peer-to-Peer File Sharing: A Guide for Business, Federal Trade Commission, s. 3.

²¹ Chia Huang-Trangle, s. 9.

²² Heine, Sonja, *Bitcoins und Botnetze - Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining*, NSTZ 2016, s. 441; Rückert, Christian, *Vermögensabschöpfung und Sicherstellung bei Bitcoins*, MMR 5/2016, s. 295.

²³ Broadhead, Stearns, *The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments*, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), (1180-1196), s. 1181, 1182.

Kripto para birimlerinin en önemli özelliği merkezi bir otoriteye bağlı olmamasıdır. Yapılan işlemler herhangi bir merkezi otoritenin denetimine tabi değildir. Bu sebeple aracı kurum niteliğindeki finans veya banka gibi kurumlara ihtiyaç duyulmaz. Kripto para birimlerinin büyük çoğunluğu merkezileştirilmemiştir. Bu sebeple kripto para birimini ihraç etmek ve ödeme defterlerini sürdürmek için merkezi bir idare söz konusu değildir.

Kripto paraların bir başka özelliği ve karapara aklamayı kolaylaştıran yönü, tüm işlemleri kontrol etmeyi imkansız kılan sınırsız miktarda hesap oluşturmanın kripto paralar için mümkün olmasıdır.

Kripto paralar, kripto varlık borsaları aracılığıyla kişiden kişiye transfer edilebilmektedir. Kripto para biriminin saklanması tipik olarak, sanal hesaba benzeren bireysel cüzdan ile ilişkilendirilir. Cüzdanlar, blokzincirler ile bağlantı kurabilir ve kripto para birimini göndermek ve almak için kullanılan ortak anahtarları (PIN veya şifre gibi işlev gören) ve özel anahtarları oluşturabilir ve/veya saklayabilir.²⁴

Kripto paraların karapara aklamayı kolaylaştıran özelliklerinden bir diğeri finansal faaliyetleri saklayabilmeleridir. Finans sistemde fonların online ve anonim olarak, bir kripto para biriminden diğer bir kripto para birimine veya kripto para biriminden itibari para birimine dönüştürülmesi oldukça kolaydır. Gerçekten de kripto para birimini kullanan online piyasalar ve borsalar, suçlulara finansal ayak izlerini saklama ve yasa dışı kazançlarının menfaatlerinden yararlanma konusunda elde ettikleri paranın transfer edilmesine imkan sağlamaktadır.²⁵ Uyuşturucu kartelleri dahil olmak üzere uluslararası suç örgütleri özellikle finansal faaliyetleri saklamak ve tespit edilmeden sınırlar ötesine yüksek meblağlardaki parayı transfer etmek için kripto para birimlerinden yararlanmaktadırlar.²⁶ Bu konuda lisanssız, tescilsiz veya usule uygun faaliyet göstermeyen borsalar ve platformlar kullanılmaktadır.²⁷ Hatta, usule uygun tescilli borsalar bile belirsiz kurallarla faaliyet göstererek veya karapara aklamayla mücadele protokollerine uymayarak suç işlenmesini kolaylaştırmaktadırlar. Aslında karapara aklama ile mücadele protokollerinde “müşterinizi tanıyınız, nakit ve şüpheli işlemleri bildiriniz” şeklinde tescilli borsalar işlem bilgileri elde etmektedir. Ancak, bu yükümlülükleri uymaktan kaçınan borsalar, suçlulara yasa dışı finansal faaliyetlerini, adli ve idari makamlardan saklama imkanı sağlamaktadır.

Yukarıda belirttiğimiz hususlar dışında kripto paralar küresel alanda güvenli, çok hızlı ve düşük maliyetli işlem yapabilme imkanına sahiptir. Ancak kripto para

²⁴ Wegberg - Oerlemans - Deventer, s. 425.

²⁵ Chia Huang-Trangle, s. 38, 39.

²⁶ Report of the Attorney General's Cyber Digital Task Force, October 2020, s. 13.

²⁷ Wegberg - Oerlemans - Deventer, s. 422.

birimlerini bir ödeme aracı olarak tanımadan, yasal ekonomik sisteme dahil etmeden, merkezi bir otoriteye tabi kılmadan ve bu konuda uluslararası iş birliği yapmadan bu paraların karapara aklama faaliyetine konu olmasını engellemek oldukça güçtür.²⁸

III. Karapara Aklama Suçu (TCK m.282)

Suçtan kaynaklanan malvarlığı değerlerinin nakde çevrilmesinde kripto paraların potansiyel bir risk oluşturduğunu söylememiz gerekir.²⁹ Bu riskin suç teşkil edecek davranışlara dönüşmesiyle ilgili 5237 sayılı Türk Ceza Kanunu'nun 282'nci maddesinde "suçtan kaynaklanan malvarlığı değerlerini aklama" suçu düzenlenmiştir. Madde; "(1) 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 maksadıyla, çeşitli işlemlere tâbi tutan kişi, üç yıldan yedi yıla kadar hapis ve yirmibin güne kadar adli para cezası ile cezalandırılır. (2) Birinci fıkradaki suçun işlenmesine iştirak etmeksizin, bu suçun konusunu oluşturan malvarlığı değerini, bu özelliğini bilerek satın alan, kabul eden, bulunduran veya kullanan kişi iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. (3) Bu suçun, kamu görevlisi tarafından veya belli bir meslek sahibi kişi tarafından bu mesleğin icrası sırasında işlenmesi halinde, verilecek hapis cezası yarı oranında artırılır. (4) Bu suçun, suç işlemek için teşkil edilmiş bir örgütün faaliyeti çerçevesinde işlenmesi halinde, verilecek ceza bir kat artırılır. (5) Bu suçun işlenmesi dolayısıyla tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur. (6) Bu suç nedeniyle kovuşturma başlamadan önce suç konusu malvarlığı değerlerinin ele geçirilmesini sağlayan veya bulunduğu yeri yetkili makamlara haber vererek ele geçirilmesini kolaylaştıran kişi hakkında bu maddede tanımlanan suç nedeniyle cezaya hükmolünmaz" şeklindedir.

Buna göre, suç işlenerek elde edilen malvarlığı değerleri kripto paralarla gizlenebilir veya çeşitli işlemlere tabi tutulabilir. Suç işlenerek elde edilen malvarlığı değerleri kripto paraya yatırılabilir veya dönüştürülebilir ya da kripto paralar bir yatırım aracına çevrilebilir veya üçüncü bir kimseye devredilebilir. Madde metnine ve gerekçesine bakıldığında, bugün itibarıyla kripto paraların suç işlenerek elde edilen malvarlığı değerlerini aklama suçunda önemli bir yöntem olduğu anlaşılabacaktır.³⁰

²⁸ Dyntu - Dykyi, s. 78.

²⁹ Broadhead, s. 1181.

³⁰ Suçtan kaynaklanan malvarlığı değerlerini aklama suçu, Türk Ceza Kanunu'nun İkinci Kitabının, "Millete ve Devlete Karşı Suçlar ve Son Hükümler" başlıklı İkinci Bölümü'nde "Adliye Karşı Suçlar" kısmında, 282. maddede yer almaktadır. Madde Gereği; "Suçtan kaynaklanan malvarlığı değerlerine meşruiyet görüntüsü verilerek ekonomik sisteme sokulması, suç işlemenin kazanç elde etme açısından cazip bir yol olarak görülmesine neden olmaktadır. Suç işlemek suretiyle veya dolayısıyla elde edilmiş olan ekonomik değerlerin meşruiyet görüntüsü kazandırılarak ekonomik sisteme sokulması, aynı zamanda suç delillerinin değiştirilmesi, gizlenmesi ve dolayısıyla suçlunun kayırılması sonucunu doğurmaktadır. Bu düşüncelerle, suçtan kaynaklanan malvarlığı

Suç işlenerek elde edilen her türlü malvarlığı değerini meşrulaştırmak maksadıyla yapılan eylemler, karapara aklama suçunun fiil unsurunu oluşturur. Suçtan kaynaklanan malvarlığı değerleri ifadesi, “*sanal varlıkları*” da kapsar niteliktedir.³¹

5237 sayılı TCK'nın 282'nci maddesine göre, karapara aklama suçuna sebebiyet veren eylemler, suç işlenerek elde edilen gelirleri yurt dışına çıkarma veya gayrimeşru kaynağını gizleme veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla, çeşitli işlemlere tâbi tutmadır.

İlk seçimlik hareket suçtan elde edilen malvarlığı değerlerinin yurtdışına çıkarılmasıdır. Suç kaynaklı malvarlığı değerinin yurt dışına çıkarılması yasal bir yol kullanılarak gerçekleştirileceği gibi yasal olmayan yollarla da gerçekleştirilebilir. Elde edilen suç gelirleri yatırım amaçlı kripto paralara dönüştürüldükten sonra bu paraları hukuken tanıyan ve işlem yapılmasına imkan sağlayan ülkelere transfer edilebilir ve bu sayede aklanabilir. Böylece suç işlenerek elde edilen karapara kripto paralar marifetiyle başka bir ülkeye transfer edilmiş olur.

Karapara aklama suçunun oluşmasına sebebiyet veren bir diğer seçimlik hareket, öncül suçun işlenmesiyle ortaya çıkan malvarlığı değerlerini, sanki meşru yollardan elde edilmiş bir değer niteliğine sahip olduğunu gösterecek şekilde çeşitli işlemlere tabi tutarak aklanmasına sebebiyet vermedir. Bu konuda özellikle takas işlemi yapan firmalar, kripto para borsaları ve platformları veya sırf cüzdan hizmeti sunan kuruluşlar karaparayı kripto paralar üzerinden çeşitli işlemlere tabi tutarak aklayabilirler.

Kanun koyucu çeşitli işlemlere tabi tutma ifadesiyle hem gayri meşru kaynağı gizleme hem de meşru bir yolla elde edildiği konusunda kanaat uyandırma maksadıyla hareket etmeyi aramaktadır. Belirtelim ki suçtan elde edilen malvarlığı değerlerinin meşru bir yolla elde edildiği konusunda kanaat uyandırma, gayrimeşru kaynağı gizlemeyi de kapsamaktadır. Kişilerde bu kazancın meşru bir kazanç olduğu noktasında kanaat uyandırmak isteyen, aynı zamanda gayrimeşru kaynağı da gizleme maksatlı eylemler gerçekleştirir. Dolayısıyla suç kaynaklı malvarlığı değerlerine meşru yollardan elde edilmiş kazanç izlenimi verme, bu gelirlerin gayrimeşru kaynağını gizleyici eylemleri de kapsar niteliktedir. Bu hareket şeklinde suç gelirlerini gizlemenin ötesine geçilmekte, sanki bu gelirler yasal yollardan elde edilmiş gelir gibi gösterilmeye çalışılmaktadır. Buradaki işlemler kripto paralarla yapılan işlemlere tatbik edilebilmekte ve suç işlenerek elde edilen kazanç rahatlıkla meşruiyet kazandırılabilir. Örneğin, suç işlenerek elde edilen parayla kripto para satın alınır ve daha sonra bu para hizmet sağlayıcılar marifetiyle tekrar satılarak itibari paraya dönüştürülebilir. Bu sayede

değerlerinin, yurt dışına transfer edilmesi veya bunların gayrimeşru kaynağını gizlemek ve meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla çeşitli işlemlere tabi tutulması, ayrı bir suç olarak tanımlanmıştır” şeklindedir.

³¹ Report of the Attorney General's Cyber Digital Task Force, s. 2.

hukuka aykırı bir şekilde elde edilmiş olan para çeşitli işlemlere tabi tutularak meşru bir yolla elde edilmiş gelir gibi gösterilebilir.³²

Kripto paralar, geleneksel madeni ve kağıt para birimi gibi, değiş tokuş aracı olarak işlev gören değerlerin temsilidir. Yani bu para birimi alınıp satılabilir, transfer edilebilir ve ödeme veya yatırım aracı olarak kullanılabilir. Sanal para birimi, geleneksel para birimlerinin, menkul kıymetlerin ve diğer geleneksel finansal malvarlıklarının dijital temsililerinden ayrı ve farklı olarak, “sanal malvarlığı” türüdür.³³ Malvarlığı terimi karapara aklamalarının tespitinde önemli bir rol oynamaktadır. Madde metninde yer alan malvarlığı ibaresine “sanal mülkiyet” de dahildir.³⁴ Dahası itibari para birimi, gerçek para birimi veya ulusal para birimi olarak da anılan “geleneksel para biriminin” aksine, sanal para birimi herhangi bir ülkede veya hükümete veya diğer alacaklıda yasal arz statüsünde değildir.³⁵ Bunun yerine, belirli sanal para biriminin dönüşüm değeri genellikle kendi topluluğundaki kullanıcılar arasındaki sözleşmeye veya güvene dayanır.

Karapara aklama suçunda üzerinde durulması gereken en önemli husus öncül suçtur. Karaparanın varlığından bahsedilebilmesi için daha önce işlenmiş ve gelir elde edilmiş bir suçun varlığı şarttır. Bu sebeple öncül suç, aklama suçunun varlık sebebidir. Hem öncül suçun hem de karapara aklama suçunun konusunu kripto para birimleri oluşturabilir. Öncül suç kapsamında kripto paralarla bağlantılı olarak işlenen suçların başında yine kripto paraların konu olduğu dolandırıcılık ve hırsızlık gelmektedir. Dijital şantaj ve dolandırıcılığın kripto paralar aracılığıyla işlenmesi dikkat çekicidir.³⁶

Kripto paraların karapara aklamaya konu olması bakımından işlendiğinde gelir elde edilen ve ağırlıklı olarak uyuşturucu madde ticareti ile yasa dışı faaliyetlerin konu olduğu suçlar ön plana çıkmaktadır. Kripto varlık hizmet sağlayıcılarının güvenlik açıklarını bilerek kripto para platformlarına ve borsalarına siber saldırıda bulunan kişiler, cüzdanlardaki ve borsalardaki güvenlik açıklarını kullanarak kripto parayı çalabilir.³⁷ Dijital hırsızlığa ek olarak, piyasa manipülasyonu ile kripto para birimleriyle dolandırıcılık suçu da işlenebilir.

Bilişim suçları içerisinde mütalaa edilen kripto para dolandırıcılığı kripto varlık hizmet sağlayıcısı olan platformların ve borsaların işlem yapıldığı internet

³² Dülger, Murat Volkan-Özkan, Onur, *Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi*, in: Prof. Dr. Mehmet Emin Artuk'a Armağan (Editör, Mahmut Koca), Ankara 2020, s. 989; Tahan, s. 132.

³³ Report of the Attorney General's Cyber Digital Task Force, s. 2.

³⁴ Grzywotz, s. 331.

³⁵ Report of the Attorney General's Cyber Digital Task Force, s. 31.

³⁶ Grzywotz, s. 333.

³⁷ Kamu raporları 2018 yılında, asgari 1.7 milyar \$ tutarında kripto para biriminin çalındığını veya hortumlandığını, bu çalınan tutarın 950 milyon \$'dan fazlasının ise kripto para birimi borsalarından çalınmış olduğunu tahmin etmektedir. 2019 yılında, önceki senenin kaybının iki katından fazla olan, 4.5 milyar \$ tutarındaki kripto para biriminin hırsızlık veya dolandırıcılıktan ötürü kaybedildiği rapor edilmiştir. Bkz. Report of the Attorney General's Cyber Digital Task Force, s. 15.

sitelerinin taklidi yapılarak işlenmektedir. Yaptıkları kopya sitelerle kullanıcının “kullanıcı adı ve şifresi” ele geçirilir. Bir diğer kripto para dolandırıcılığı, sahte kripto para borsaları ve hizmet sağlayıcılarıdır. Sahte kripto para siteleri üzerinden özellikle yabancı kripto para borsalarına benzeyen içerikler kullanılarak kişiler dolandırılmaktadır. Her geçen gün yeni bir kripto para birimi ile karşılaşıldığından sahte ve hiç var olmayan kripto paralarla da kişilerin dolandırılması mümkündür.³⁸ Benzer şekilde sahte madencilik siteleri ile kullanıcılara kısa vadede yüksek kazanç elde edecekleri vaat edilerek kripto para dolandırıcılığı karapara aklama suçunda öncül suç olarak işlenebilmektedir.

Kripto paralarla karapara aklama suçu arasındaki ilişkide TCK'nın 282'nci maddesinin ikinci fıkrasının da değerlendirilmesi gerekir. Karapara aklama suçunun işlenmesine iştirak etmeksizin, aklama suçunun konusunu oluşturan malvarlığı değerlerini bu özelliğini bilerek satın alma, kabul etme, bulundurma veya kullanma cezalandırılmaktadır. Kripto varlık hizmet sağlayıcılarında, kripto varlık borsalarında veya platformlarında işlem yapan kişinin bu fıkra bağlamında öncül suçtan elde edilen gelire kripto parayı satın almaktan, kabul etmekten, bulundurmaktan veya kullanmaktan sorumlu tutulabilmesi kripto para birimlerinin özellikleri de (*kripto paraların anonimliği, izini sürmede yaşanan güçlükler ve blokzincir teknolojisi*) dikkate alındığında düşüncemize göre mümkün gözükmemektedir. Ayrıca TCK'nın 282'nci maddesinin ikinci fıkrasında yer alan seçimlik hareketlerin kripto paralar bakımından uygulanabilmesi de ayrı bir sorundur. Şayet kişi, suç gelirlerini aklamak için kripto paraları kullanmış ve karapara aklama suçunu işlemişse, bahse konu suçların işlenişine iştirak ettiğinden artık TCK'nın 282'nci maddenin birinci fıkrasına göre cezalandırılır.

Burada son olarak, karapara aklama suçu bakımından öncül suç niteliği haiz olmayan,³⁹ fakat benzer nitelikli görülen vergi kaçırma faaliyetlerinden de bahsetmek gerekir. Karapara aklamada olduğu gibi, kripto para birimi işlemlerinin izlenmesindeki potansiyel zorluklar vergi kaçırma da kolaylaştırır.⁴⁰ Kişi, kripto para satışından veya diğer tasarruflardan elde ettikleri sermaye kazançlarını ve kripto para biriminden elde ettiği işletme gelirini raporlamayarak kripto para birimi üzerinden vergi kaçırılabilir. Piyasada kripto para birimleri ortaya çıktıkça ve dalgalandıkça raporlanmamış sermaye kazançlarından kaynaklanan vergi ziyayı da önemli ölçüde artar.⁴¹

³⁸ Dülger-Özkan, s. 988.

³⁹ TCK'nın 282'nci maddesinde suçtan kaynaklanan malvarlığı değerinden bahsedilmektedir. Vergi suçlarında elde bulunan malvarlığı, yasal ve meşru yollardan elde edilmiştir. Burada kişiler devlete ödenmesi gereken belirli meblağların bir şekilde kayda girmesini engelleyerek kazanç elde etmektedir. Vergi kaçaklığına konu olan eylemlerde, devlete belirli bir oranda vergi olarak verilmesi gereken meblağ aslında anapara olarak meşru yollardan elde edilmektedir. Dolayısıyla temelinde suç işlenerek elde edilmiş bir malvarlığı değeri bulunmamaktadır. Bkz. Çakır, s. 305, 306.

⁴⁰ Chia Huang-Trangle, s. 3.

⁴¹ Chia Huang-Trangle, s. 3.

IV. Karapara Aklama Yöntemi Olarak Kripto Para Kullanımı

Karapara aklayanlar adli mercilerin takibinden kaçmakla birlikte, suçtan elde ettikleri değerleri de korumak isterler. Bu sebeple kripto paralar hem adli takipten kaçmak hem de suç gelirlerini korumak için tercih edilen önemli bir karapara aklama yöntemi haline gelmiştir. Karaparanın kaynağını gizlemek için işlemleri katmanlaştırmanın bir yolu olarak yasadışı gelirleri sanal para birimlerine aktarma organize suçluluk ve terörizmin finansmanı bakımından da hızla yayılmaya başlamıştır.⁴²

Suçtan kaynaklanan malvarlığı değerleri çoğu zaman nakittir. Aklama faaliyetini gerçekleştiren kimseler aklama yöntemlerinden birini kullanarak ellerindeki nakit parayı yasal ekonomi içerisinde eritmeye çalışırlar. Özellikle organize suçluluk veya uyuşturucu ticaretinden elde edilen değerler dikkate alındığında suç işlenerek elde edilen nakit paranın aklanma nedeni daha iyi anlaşılacaktır.

Karapara aklama faaliyetinde yapılması gereken en önemli iş, öncül suçtan elde edilen değerlerin izinin sürülmesini engellemektir. Eldeki malvarlığının nereden kaynaklandığının bilinmemesi gerekir. Kripto paralar da öncül suçla karapara arasındaki bağı kesme ve adli makamların olayı aydınlatmasına mani olma açısından önemli avantajlar sağlamaktadır.

Kripto paralarla karapara aklamının çeşitli şekilleri vardır. Bunlardan biri; “enstrümental kripto para aklama” diğeri “online kripto para aklama”dır.

Enstrümental kripto para aklamada, para aklamının üç aşamasından (yerleştirme, ayırıştırma ve bütünleştirme) birisinin dijital olarak gerçekleştirilmesi söz konusudur. Bitcoin aracılığıyla gerçekleştirilen enstrümental kripto para aklamının tipik örneği, suçtan elde edilen nakdi gelirler ile kripto para satın alınmasıdır.⁴³

Online kripto para aklamada ise karapara aklamının tüm aşamaları dijital olarak gerçekleşir. Aklanacak para zaten dijital şekilde mevcuttur ve karapara aklama süreci hızlıca gerçekleşir.⁴⁴ Online kripto para aklama, zaten sanal olan para ile sanal para satın alınırken gerçekleşir.

İnternette takip edilmek istemeyenlerin tercih ettiği ve ilk sanal para birimi Bitcoin ile adını duyuran darknet de (*dark web - deep web*) kripto paralarla karapara aklamının yöntemlerinden biri olarak kullanılmıştır.⁴⁵ Başlangıçta çevrim içi bir pazar yeri olarak kullanıcılarına anonim ve güvenli bir ortam sunan, ancak daha sonra kötü niyetli kimselerin uyuşturucu ticareti ve karapara aklama

⁴² National Strategy for Combating Terrorist and Other Illicit Financing, 2020, s. 18. Ayrıca bkz. Tahan, s. 116, 117.

⁴³ Sicignano, s. 259.

⁴⁴ Sicignano, s. 259.

⁴⁵ Broadhead, s. 1192. Ayrıca bkz. FATF REPORT, Virtual Currencies Key Definitions and Potential AML/CFT Risks June 2014, s. 6.

faaliyetleri için kullandığı “Silk Road” konuya ilişkin güzel bir örnek teşkil etmektedir.⁴⁶ Silk Road, 2011 yılında çevrimiçi bir alışveriş sitesi olarak kurulmuş ve kullanıcılarına gerçek kimliklerini saklayarak anonim kalma imkanı sağlamıştır. 2013 yılında FBI, karmaşık ve gelişmiş teknoloji ile internet üzerinden başta uyuşturucu ticareti ve kötü amaçlı yazılımlarla suç işlendiğinden bahisle siteyi kapatmıştır.⁴⁷ Bu süreçte adli makamlar “darknet”te faaliyet gösteren kişileri, bitcoin transferleri üzerinden takip etmiş ve bulmuştur.

Suç işlenerek elde edilen karapara kripto paraların işlem gördüğü *kiosklar*’da da aklanmaya çalışılmaktadır.⁴⁸ Yaygın olarak “Bitcoin ATM’leri” olarak anılan kripto para birimi kioskları; kullanıcılara itibari para birimini Bitcoin’e ve diğer kripto para birimlerine veya tersine dönüştürmeye izin veren dış makinelerdir. Kripto para birimi kioskları, sanal malvarlığı değişimi için kolay kullanılabilen fiziki erişim noktalarıdır.⁴⁹ Kişi cep telefonunu kullanarak bu makinelerden kripto para alıp satabilir.

Kiosklar gibi karıştırıcılar (mixer, laundry service, tumbler)⁵⁰ da kripto paraların nihai varış yerine teslimatından önce birden fazla kullanıcının kripto para birimini karıştırarak kripto para biriminin belirli birimlerinin kaynağını veya sahibini gizleyebilirler.⁵¹ Ücret karşılığında, müşteri karıştırıcı tarafından kontrol edilen belirli bir adrese kripto para birimini gönderir. Karıştırıcı, bu isteği talep edilen alıcı adrese göndermeden önce diğer müşterilerden gelen fonlar ile bu kripto paraları karıştırır.⁵² Karıştırıcılar, işlem zincirini gizleyen bir tür anonimleştiricidir. Aynı bitcoin adresindeki tüm işlemleri birbirine bağlayarak blokzincirde başka bir adresten gönderilmiş gibi görünmelerini sağlar.

⁴⁶ FATF REPORT, s. 11.

⁴⁷ Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals, April 3, 2019, s. 6. Ayrıca bkz. Mutluoğlu, Derya, *Kripto Para Birimleri ve Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu*, Ankara 2020, s. 61; Tahan, s. 119.

⁴⁸ 22 Temmuz 2020 tarihinde, ABD Adalet Bakanlığı, Kaliforniya’lı bir adamın, şahsi işlemler ve Bitcoin ATM- tipi kioskların networkü aracılığı ile -suç faaliyeti gelirleri dahil olmak üzere- 25 milyon \$’a kadar dönüştüren Herocoin olarak adlandırılan yasa dışı sanal para birimi para hizmetleri işlettiği için suçlu bulunmayı kabul ettiğini açıkladı. Kiosklar, Kaliforniya genelinde AVM’lere, petrol ofislerine ve dükkanlara yerleştirilmişti ve müşterilere nakit parayı bitcoin dönüştürmeye ve tersi işlemi yapmaya izin vermişti. Kişi, bilerek ve isteyerek Herocoin’i FinCEN nezdinde tescil etmediğini, karapara aklama programı uygulamadığını, 10,000 \$’ı aşan değişimler için para birimi işlem raporları sunmadığını, müşteri hakkında durum tespiti yapmadığını ve şüpheli faaliyet raporları sunmadığını kabul etmiştir. Bitcoin ATM networküne ilişkin olarak, sanık ayrıca, 3,000 \$’a kadar birden fazla işlem yapan müşteriler için kimlik elde etme veya işlemi gerçekleştiren kişiyi fiilen yansıtan herhangi bir kimlik doğrulama programı uygulamadığını da itiraf etmişti. Bkz. Report of the Attorney General’s Cyber Digital Task Force, s. 40.

⁴⁹ Report of the Attorney General’s Cyber Digital Task Force, s. 39, 40.

⁵⁰ FATF REPORT, s. 6.

⁵¹ Grzywotz, s. 111.

⁵² Wegberg - Oerlemans - Deventer, s. 423.

Karapara aklamanın anlaşılmasını engellemek maksadıyla mümkün olduğu kadar yasal işlem türlerine benzer nitelikli işlemler yapılması önem arz etmektedir. Birçok ülke kripto para birimlerini tanımasa da bu para birimlerinin kendine özgü borsalarda ve ticari platformlarda işlem gördüğü ve bu konuda kripto varlık hizmet sağlayıcılarının da etkin rol oynadığı ortadadır. Öyle ki kripto varlık hizmet sağlayıcılarının da ülkemizde “yükümlüler” arasına alınması bu durumun göstergesidir.⁵³

Mevcut ekonomik ve mali sistemde kendine yer bulmaya çalışan kripto para birimleri yasal işlem türlerine benzerliği ile karapara aklamak isteyenlere cazip gelmektedir. Teknolojinin gelişmesiyle çok daha teknik ve hızlı yöntemler suç işlenerek elde edilen karaparanın aklanmasını kolaylaştırmaktadır. Karapara aklama faaliyetinde süreç gizli yürütülmekte, yasadışı kaynak veya yasadışı uygulamalarla elde edilen gelirlere meşru yollardan kazanılmış gelir görünümü verilmeye çalışılmaktadır. Olağan işlemlerde göze çaracak kadar büyük miktarlar, tekrar eden adreslere aktarılırsa, yetkililerin dikkatini çekebilir. Belki bu sayede yetkililer, kripto varlık hizmet sağlayıcısı tarafından uyarılır. Ancak merkezi olmayan hizmetlerin kullanılmasıyla kripto paraların gerçek göndericisi ve alıcısı arasındaki bağlantıyı gizleyebildiği de göz ardı edilmemelidir.⁵⁴

Karapara aklama suçunda hangi yöntem kullanılırsa kullanılsın genel olarak aklama faaliyeti üç aşamada gerçekleşir. Bunlar; yerleştirme, ayırıştırma ve bütünleştirme aşamalarıdır.⁵⁵ Karaparanın aklanması için belirli aşamalara ihtiyaç vardır. Kripto paralarda ise bu aşamaların tümü hızla geçilir ve karaparanın izini sürmek zorlaşır. Bu aşamalarda aklanmış ve yasal yolla elde edildiği izlenimi verilen malvarlığı değeri mali sisteme entegre edilmiş olur.

Suç kökenli malvarlığı değerlerine yasal yolla elde edilmiş malvarlığı görünümü kazandırma kripto paralar vasıtasıyla rahatlıkla geçilebilmektedir. Karapara ne kadar ayırıştırılır ve parçalara bölünürse, adli makamların bu gelirlerin izini sürmesi ve bulması o kadar zorlaşır, failerin yakalanma riski de o nispette azalır.⁵⁶

Kripto para, varlığı daha hızlı adımda ve daha düşük masrafla transfer edebilme imkanı vermektedir. Ayrıca yoğun denetim altında olan geleneksel ban-

⁵³ Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmeliğin 4'üncü maddesinin birinci fıkrasının (ü) bendine “Kripto varlık hizmet sağlayıcılar” eklenmiş ve yükümlüler arasında kripto varlık hizmet sağlayıcıları da dahil edilmiştir. (Ek: RG-1/5/2021-31471-C.K-3941/1 md.)

⁵⁴ Report of the Attorney General's Cyber Digital Task Force, s. 13.

⁵⁵ Gerek ulusal gerekse de uluslararası hukukta suçtan kaynaklanan malvarlığı değerlerini aklamaya ilişkin aşamaları üç başlık halinde ele alınmaktadır. Herzog, Flix-Achtelik, Olaf, *Geldwäschegezet* *Kommentar*, 2. Auflage, 2014, s. 5 vd.

⁵⁶ Herzog-Achtelik, s. 7.

kacılık sistemine kıyasen, kripto para birimine sahip suçlular varlıklarını diğer kullanıcılara kimliklerini ifşa etmeden transfer edebilirler. Kripto para birimi, uyuşturucu ve silah gibi yasa dışı malların ticaretinde de kullanılabilir. Bu durum, karapara aklamanın yerleştirme aşamasına olan ihtiyacı ortadan kaldırır. Belirtilim ki karapara aklama faaliyeti sırasında en riskli olan aşama bu aşamadır. Çünkü yasal olmayan yollardan elde edilen bu para görünür haldedir ve adli makamların dikkatini çekebilecek durumdadır.

Kripto para borsasında ve platformlarında aklanan karapara yasal yolla elde edildiği izlenimi verilen malvarlığı değeri olarak mali sisteme entegre edilir. Buna bütünleştirme (entegrasyon) aşaması denilir. Bu aşamada suç işlenerek elde edilen malvarlığı değerlerinin tespiti oldukça güçtür. Artık suç kökenli malvarlığına, yasal yolla elde edilmiş malvarlığı görünümü kazanmıştır.⁵⁷

Karapara aklama yöntemi olarak kripto para kullanımı suç gelirlerinin müsaderesini engelleme imkanı da vermektedir. Suçtan kaynaklanan malvarlığı değerlerinin kripto paralarla aklanmaya çalışılması, eldeki suç gelirlerine adli makamların elkoymasını zorlaştırır. Adli makamlar bireylerin cüzdanlarının şifrelerine veya kriptografi anahtarlarına sahip değilse kripto paraları ele geçirmek mümkün değildir. Böylesi bir koruma suç işleyerek gelir elde eden kişilere cazip gelmekte ve sıcak veya soğuk cüzdanlarda muhafaza edilen kripto paralara adli ve idari makamların erişimi engellenmektedir.⁵⁸ Kripto paralarda elkoyma tedbirini uygulamak zordur. Bireysel şifrelerin adli makamlarda mevcut olmaması halinde failin iş birliği yapması beklenir. Kişinin kriptografik şifreleri paylaşmaya ve sahibi olduğu cüzdanlara erişim sağlamaya icbar edilmesi ise hukuka aykırıdır. Şüpheli veya sanık suçla bağlantılı arama yapılmasına ve elkoyma işlemlerinin uygulanmasına katlanmak durumunda olsa da şifreleri bildirmekle veya deşifre konusunda iş birliği yapmakla yükümlü tutulamaz.⁵⁹

V. Kripto Paralarla Karapara Aklamada Mali Eylem Görev Gücü

Karaparanın aklanması, terörizmin finansmanının önlenmesi ve siber suçla mücadelede olduğu gibi kripto paraların da suça konu olması halinde uluslararası iş birliğinin zorunlu olduğunu belirtmemiz gerekir. İş birliği, ekonomik büyümeyi teşvik edeceği gibi uluslararası güvenliği de güçlendirir.⁶⁰ Bununla ilgili kripto paralarla suç işlenmesine engel olmak ve ülkelerin mali yapısını korumak için Birleşmiş Milletler bünyesinde faaliyet gösteren Mali Eylem Gö-

⁵⁷ Herzog-Achtelik, s. 7.

⁵⁸ Grzywotz, s. 111.

⁵⁹ Simmler, Monika-Selman, Sine-Burgermeister, Daniel, *Beschlagnahme von Kryptowährungen im Strafverfahren*, AJP/PJA 8/2018, s. 976.

⁶⁰ National Strategy for Combating Terrorist and Other Illicit Financing, 2020, s. 52.

rev Gücü (Financial Action Task Force-FATF) başta olmak üzere, benzer kurum ve kuruluşlarla mücadelenin nasıl ve ne şekilde olacağı belirlenmeye çalışılır. FATF, suç gelirlerinin aklanması ve terörizmin finansmanı ile mücadele adına kurulmuş olan ve bu konuda standartları belirleyen ve etkin bir şekilde uygulanmasını teşvik eden önemli bir kuruluş olup, düzenleyici önlemler ve tavsiye kararları almaktadır.⁶¹

Mali Eylem Görev Gücü (FATF) kripto para birimleriyle karaparanın aklanması ve terörizm finansmanına engel olmak için tavsiye kararları almakta ve üye ülkelerden bu tavsiyelere uygun düzenlemeler yapmalarını ve uluslararası iş birliği beklemektedir.⁶²

FATF, 2014 yılında, sanal malvarlığına dayalı faaliyetleri kendi kapsamına alma ihtiyacını fark etmiş⁶³ ve 2015 yılında, sanal malvarlığı ödeme ürünleri ve hizmetleri ile ilişkili karapara aklama ve terörizmin finansmanı risklerini ele alan küresel bir kılavuz yayınlamıştır. Temmuz 2018’de, FATF, sanal malvarlıklarını içeren yasa dışı finansal tehditleri değerlendiren bir raporu G20 Maliye Bakanları ve Merkez Bankaları Yöneticileri toplantısında yayınlamıştır.⁶⁴

FATF, Ekim 2018’de, sanal malvarlığı faaliyetlerindeki uygulamalarını açıklığa kavuşturmak için “15 No.lu Tavsiye Kararı’ni” tadil ederek “*sanal malvarlığı*” ve “*sanal malvarlığı hizmet sağlayıcısı*” tanımlarına tavsiye kararında yer vermiş⁶⁵ ve 21 Haziran 2019’da, ülkelerin ve yükümlü kuruluşların, sanal malvarlıklarının, karapara aklama ve terörizmin finanse edilmesi ve yaygınlaştırılması amacıyla kötüye kullanımını engellemek için ilgili Tavsiye Kararlarına nasıl uygunluk sağlamak zorunda olduklarını açıklamıştır.

⁶¹ FATF’in aldığı kararlar tavsiye niteliğindedir. Ancak taraf olan devletlerden tavsiye kararları doğrultusunda düzenleme yapmaları beklenmektedir. Birleşmiş Milletler de üye devletleri FATF’in almış olduğu tavsiye kararlarını uygulamaya davet etmektedir. Alınan tavsiye kararlarının uluslararası hukukta bağlayıcılığı olmasa da üye devletlere politik ve ekonomik yönlü baskı yapılması, alınan kararların uygulanmasını zorunlu kılmaktadır. Bkz. Herzog-Achtelik, s. 26.

⁶² FATF’in amaçları karapara aklama, terörizmin finansmanı, kitle imha silahlarının yaygınlaşması ve uluslararası finansal sistemin bütünlüğüne yönelik diğer ilgili tehditler ile mücadele için standartlar koymak, yasal, düzenleyici ve operasyonel tedbirlerin verimli tatbikini teşvik etmektedir. Standart koyucu ve yasa düzenleyici bir organ olarak, FATF, yargı yetkileri arasında mümkün olan en geniş şekilde uyumluluğun sağlanması, hedeflenen ulusal yasama ve düzenleyici reformlar gerçekleştirilmek için teknik bir anlayışı ve gerekli bir siyasi iradeyi oluşturmaya çalışır. Bkz. Herzog-Achtelik, s. 26.

⁶³ <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, (Erişim tarihi 08.06.2021).

⁶⁴ Güncellenen metinde, sanal varlık; “dijital olarak alınıp satılabilen değerler dijital bir temsilidir veya devredilebilir ve ödeme veya yatırım amaçlı kullanılabilir. Sanal varlıklar fiat para birimlerinin, menkul kıymetlerin ve diğer finansal varlıkların dijital temsillerini içerir” şeklinde tanımlanmıştır. Bkz. FATF, s. 130.

⁶⁵ Ayrıca ülkelerden sanal malvarlığı hizmet sağlayıcılarının AML (Anti-Money Laundering) /CFT (Countering the Financing of Terrorism) amaçlarına ve FATF Tavsiye Kararlarında uygun hareket etmeleri istenmiştir. FATF, s. 17.

Son olarak FATF, Ekim 2020’de güncellenen 19 no.lu Tavsiye Kararı’nda, ülkelerin sanal varlıkları “mülk”, “gelir”, “fon”, “fonlar veya diğer varlıklar” veya diğer “karşılık gelen değer” olarak değerlendirmeleri gerektiğini belirtmiş ve bununla ilgili önlemlerin alınmasının ve sanal varlık hizmet sağlayıcılarının da bu önlemleri uygulamasının önemini vurgulamıştır.⁶⁶

Konuyla ilgili iç hukukta da 1 Mayıs 2021 tarihli 31471 sayılı Resmi Gazetede yayımlanan ve aynı tarihte yürürlük bulan Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmeliğin 4’üncü maddesinin birinci fıkrasının (ü) bendine “Kripto varlık hizmet sağlayıcılar” eklenmiş ve yükümlüler⁶⁷ arasına kripto varlık hizmet sağlayıcıları da dahil edilmiştir.⁶⁸

Kripto varlık hizmet sağlayıcılarının tabi oldukları yükümlülüklerin başında müşterinin tanınması gelmektedir. 5549 sayılı Kanunun 3’üncü maddesine göre 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 zorundadırlar.⁶⁹

Bir diğer yükümlülük şüpheli işlem bildirimidir. Şüpheli işlem; “yükümlüler nezdinde veya bunlar aracılığıyla yapılan veya yapılmaya teşebbüs edilen işleme konu malvarlığının; yasa dışı yollardan elde edildiğine veya yasa dışı amaçlarla kullanıldığına, bu kapsamda terörist eylemler için ya da terör örgütleri, teröristler veya terörü finanse edenler tarafından kullanıldığına veya bunlarla ilgili ya da bağlantılı olduğuna dair herhangi bir bilgi, şüphe veya şüpheliyi gerektirecek bir

⁶⁶ International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation the FATF Recommendations Updated October 2020, s. 76.

⁶⁷ “Yükümlüler”, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 2/1-d maddesi ile Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmeliğin (Tedbirler Yönetmeliği) 4/1’inci maddesinde belirlenmiştir. Tedbirler Yönetmeliğinin 4’üncü maddesinin birinci fıkrasına 01 Mayıs 2021 tarihli ve 31471 sayılı Resmi Gazete’de yayımlanan Yönetmelik değişikliği ile eklenen (ü) bendine göre, “kripto varlık hizmet sağlayıcılar” anılan tarih itibarıyla yükümlüler arasına alınmıştır. Bkz. Ek: RG-1/5/2021-31471-C.K-3941/1 md.

⁶⁸ Yönetmelikle kripto varlık hizmet sağlayıcıları yükümlüler arasına dahil edilse de bu hizmet sağlayıcılarının kimler olduğu belirsizdir. Düşüncemize göre örneğin, “takas işlemi yapan firmalar, kripto para borsaları ve platformları veya sırf cüzdan hizmeti sunan kuruluşlar” bu kapsamda hizmet sağlayıcı olarak değerlendirilebilir.

⁶⁹ Kripto varlık hizmet sağlayıcıları; sürekli iş ilişkisi tesisi dışında, -Şüpheli işlem bildirimini gerektiren durumlarda tutar gözetmeksizin, -Daha önce elde edilen müşteri kimlik bilgilerinin yeterliliği ve doğruluğu konusunda şüphe olduğunda tutar gözetmeksizin, -İşlem tutarı ya da birbiriyle bağlantılı birden fazla işlemin toplam tutarı yetmişbeşbin TL veya üzerinde olduğunda, kimlik tespiti yapmak zorundadırlar. Kimlik tespitinin, iş ilişkisi tesisinden veya işlem yapılmadan önce tamamlanması gerekmektedir. Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, Mali Suçları Araştırma Kurulu Başkanlığı, Mayıs 2021, s. 7.

hususun bulunması halidir.⁷⁷⁰ Ayrıca hizmet sağlayıcıların bilgi ve belge verme,⁷¹ devamlı bilgi verme⁷² ile muhafaza ve ibraz⁷³ yükümlülükleri de bulunmaktadır.⁷⁴

⁷⁰ Kripto Varlık Hizmet Sağlayıcıların Şüpheli İşlem Bildirimlerini Kim Gönderecektir? Bu sorunun cevabı, Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar da şu şekilde verilmiştir. “Şüpheli işlem bildirimi yükümlülüğü, tüzel kişi yükümlünün kanuni temsilcileri tarafından yerine getirilir. Bu kişiler şüpheli olabilecek işlemler hakkında, yetki ve imkânları ölçüsünde araştırma yaparak edinilen bilgi ve bulguları değerlendirmek ve şüpheli olduğuna karar verdiği işlemleri MASAK Başkanlığına bildirmekle sorumludur. Şüpheli işlem bildirimini <https://masak.hmb.gov.tr/> sektorel-sib-rehberleri adresinden (Diğer Yükümlüler) şüpheli işlem bildirim formu (EK: 1) indirilip doldurulularak ıslak imzalı şekilde elden veya taahhütlü posta yoluyla Başkanlığa gönderilebilir. Şüpheli işlem bildirimini faks yoluyla Başkanlığa gönderilmesi halinde faksla gönderilen ŞİB formunun aslı, taahhütlü posta yoluyla ya da elden Başkanlığa intikal ettirilir. Form doldurulmadan Başkanlığa gönderilen yazılar imzalı olsa dahi şüpheli işlem bildirim olarak kabul edilmez. Şüpheli işlem bildirimlerinin elektronik ortamda gönderimi de mümkün bulunmaktadır. Elektronik ortamda şüpheli işlem bildirim, Başkanlık tarafından yükümlülerin erişimine sunulan EMIS.ONLINE sistemi kullanılarak (<https://online.masak.gov.tr/>) yapılacaktır. EMIS.ONLINE sistemine erişim yapılabilmesi için kripto varlık hizmet sağlayıcısı tüzel kişinin kanuni temsilcisi tarafından “Elektronik Ortamda Şüpheli İşlem Bildirimi Taahhüt Formu” (EK: 2) düzenlenerek ıslak imzalı olarak Başkanlığa iletilecektir. Söz konusu Taahhüt Formu ile birlikte kanuni temsilciye ilişkin yetki belgesinin de Başkanlığa gönderilmesi gerekmektedir. Taahhüt formunun Başkanlığa iletmesini müteakip Başkanlık tarafından başvuruda bulunan kanuni temsilcisi için EMIS.ONLINE sistemi içerisinde bir kullanıcı hesabı açılacak ve bu hesaba erişim için gerekli şifre kanuni temsilcisi tanımlaması yapıldıktan sonra, sistem tarafından kanuni temsilcinin kurum uzantılı e-posta adresine otomatik olarak gönderilecektir. Kanuni temsilci, kendisine iletilen şifre ile EMIS.ONLINE sistemine ilk erişiminde şifresini zorunlu olarak değiştirecektir. Yükümlülerin kanuni temsilcilerinin değişmesi hâlinde yeni yetkilendirilen kanuni temsilci tarafından “Elektronik Ortamda Şüpheli İşlem Bildirimi Taahhüt Formu” yeniden düzenlenerek ıslak imzalı olarak Başkanlığa gönderilecektir.” Bkz. Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, s. 11, 12.

⁷¹ 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 7’nci maddesine göre; kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlar, Başkanlık ve denetim elemanları tarafından istenilecek her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtları, bu kayıtlara erişimi sağlamak veya okunabilir hale getirmek için gerekli tüm bilgi ve şifreleri tam ve doğru olarak vermek ve gerekli kolaylığı sağlamakla sorumludur. Bkz. Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, s. 13, 14. Konuyla ilgili ABD Hazinesi de en az 10.000 dolarlık kripto para biriminin İç Gelir Servisi’ne bildirilmesinin bir gereklilik olduğunu belirtti. Bkz. <https://www.bloomberg.com/news/articles/2021-05-20/treasury-calls-for-crypto-transfers-over-10-000-reported-to-irs>. (Erişim Tarihi, 10.06.2021).

⁷² 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 6’nci maddesine göre, yükümlüler, taraf oldukları veya aracılık ettikleri işlemlerden, Bakanlıkça belirlenecek tutarı aşanları Başkanlığa bildirmek zorundadırlar. Bkz. Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, s. 14.

⁷³ 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 8’inci maddesine göre, yükümlüler, anılan Kanunla getirilen yükümlülüklerle ve işlemlerine ilişkin her türlü ortamdaki; belgeleri düzenleme tarihinden, defter ve kayıtları son kayıt tarihinden, kimlik tespitine ilişkin belgeleri ise son işlem tarihinden itibaren sekiz yıl süreyle muhafaza ve istenmesi halinde yetkililere ibraz etmekle yükümlüdür. Bkz. Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, s. 14.

⁷⁴ Ayrıca bkz. FATF, s. 130.

Sonuç

Kripto paralar bir varlık değeri olarak hayatımıza girmekle birlikte terörizmin finansmanı, uyuşturucu madde ticareti ve karapara aklama şeklindeki suç faaliyetlerine de konu olmaktadır. Bu sebeple hem ulusal hem de uluslararası hukuk bakımından adli-idari makamların tedbir alması zorunlu bir hal almıştır.

Dijital ödeme yöntemlerinin hem bir fırsat hem de bir risk oluşturduğu ortadadır. Bu sebeple ceza hukukunun dijital çağın gereksinimlerine uygun olarak güncellenmesi gerekmektedir. Bu konuda kripto varlık hizmet sağlayıcılarının yükümlülüklerini yerine getirip getirmediğini kontrol edebilecek teknik alt yapının önemli olduğunu vurgulamamız gerekir. Öyle ki yeni teknolojiler geliştikçe, finans kurumlarının karapara aklama ile mücadele yasalarına uyum sağlamalarına yardımcı olmak amacıyla bir dizi yeni kurulmuş şirket, blokzincir teknolojilerini kullanarak kripto paralarla karapara aklanmasına mani olmaya çalışmaktadır.

Kripto para birimlerinin son yıllarda karaparayı aklama yöntemi olarak kullanıldığı görülse de bu para birimlerinin doğrudan doğruya karapara aklamak için kullanılmadığını, ancak önemli bir risk oluşturduğunu belirtmemiz gerekir. Kripto para birimleri suçlular ve karapara aklayıcılar için aslında bir Truva atı görevi görmektedir.

Kripto paraların transferi basit olduğundan ve finans kurumları aracılığıyla da ticari faaliyetlere konu edilebildiğinden karapara aklama yöntemi olarak kullanılabilir. Kripto para birimlerinin özellikleri ve bütün olarak kripto para birimi piyasasının anonimliği bu paraları karapara aklamanın aracı haline getirmiştir. Günümüz piyasası, kullanıcılara mallar, hizmetler ve değeri olan diğer kaynakların alım satımı için küresel ölçekte sanal para birimi transferi imkanı sunan, binlerce kripto para birimi içermektedir. Kripto para borsaları ve platformları, işlemlerin doğrulanması ve kolaylaştırılması için finansal araçlara olan ihtiyacı elimine ederek, kripto para biriminin işlem masraflarını asgariye indirmeye çalışmaktadır. Bu para birimlerinin kullanımı geliştikçe ve genişledikçe, yasa dışı kullanımları da artmakta ve sadece kamu düzeni değil aynı zamanda ulusal ve uluslararası güvenlik de tehdit edilmektedir.

Kripto paraların merkezileştirilmemiş yapısı adli ve idari mercilerin gözetimini ve denetimini zorlaştırmaktadır. Özellikle FATF'ın uluslararası alanda yaptığı çalışmalar ve aldığı kararlar devletler tarafından iç hukukta uygulamaya konulsa da çoğu ülke kripto paraları bir para birimi olarak tanımadığından, müşteri tanıma ve şüpheli işlemlerin bildirilmesi gibi kurallar ve düzenlemeler kripto para birimleri üzerinden işlem yapan gerçek ve tüzel kişilerin faaliyetlerini gizleyebilmektedir. Bir bankada hesap açılması için, müşterinin devlet tarafından basılı ve fotoğraflı kimlik kartı veya diğer kimlik doğrulayıcı belgeleri sunması gerekmektedir. Oysa kripto para hesabı oluşturmak için, kripto varlık hizmet sağlayıcı platform ve borsalarda müşterinin yalnızca bir telefon numarası ve e-mail

adresi kullanarak kaydolması yeterli olabilmektedir. Bu durum yasa dışı işlemlerin tespitini, takibini ve yaptırım uygulanmasını zorlaştırmaktadır.

Teknolojinin ve uluslararası ticaretin gelişimi ve bunun sonucunda dünya çapında sermaye likiditesi, karapara aklama suçu ile mücadele konusunda kanuni düzenleme yapmayı ve önleyici tedbirler almayı zorunlu kılmıştır. Karapara aklama suçu uluslararası boyutu olan, ortak hareket ve iş birliği ile mücadele edilmesi gerekli olan bir suç tipidir. Bu konuda Birleşmiş Milletler ve OECD (Organisation for Economic Co-operation and Development) bünyesinde faaliyet gösteren FATF'a ve ülkemiz özelinde MASAK'a önemli görevler düşmektedir. Suçtan kaynaklanan malvarlığı değerlerinin izini takip etme, şüpheli işlemler hakkında bilgi verme, nakit işlemlerde bildirim zorunluluğuna uyma ve müşteri tanıma sistemlerinin geliştirilmesi ve teknolojinin sunduğu imkanlarla yükümlülerin bu işlemleri yapıp yapmadığı takip edilmelidir.

Kripto para piyasası, bir algoritma ile otomatik olarak yönetilen peer-to-peer networküne dayalı olduğundan her devletin bu paranın izini sürmesi ve yasa dışı faaliyete konu olduğunu belirlemesi son derece güçtür. Devletlerin tüm şüpheli işlem bildirimlerini isteyebileceği herhangi bir kurum yoktur. Bu sebeple kripto varlık platformlarında veya borsalarında işlem yapan kimselerin müşteri tanıma sistemi olarak kimlik bilgilerinin tespiti sağlanmalıdır. Hizmet sağlayıcılar şüpheli işlemleri adli ve idari makamlara iletmelidir. Yükümlülüklerini yerine getirmeyen veya getiremeyecek kripto varlık hizmet sağlayıcılarının faaliyet izni iptal edilmelidir.

Ayrıca hizmet sağlayıcıları aracılığıyla işlem yapan vatandaşları bilgilendirici ve koruyucu düzenlemelere de ihtiyaç vardır.

Son olarak kripto para birimlerinin özellikleri ve gizliliği işlenen suçlarda adli makamlar için önemli zorluklar ihtiva etse de bu para birimlerinin faydalı olabileceğinin altını çizmemiz gerekir. Örneğin, daha geniş anonimlik, geleneksel bankacılık ve kredi sistemlerinin kullanımında yaşanan hesap veya kimlik hırsızlığı riskini azaltabilir.

Kaynakça

- Broadhead, Stearns. *The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments*, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), (1180-1196).
- Chia Huang, Chung-Trangle, Asher, *Anti-Money Laundering and Blockchain Technology*, CSP023, May 2020.
- Çakır, Kerim, *Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu*, Ankara 2016.
- Dülger, Murat Volkan-Özkan, Onur, *Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi*, in: Prof. Dr. Mehmet Emin Artuk'a Armağan (Editör, Mahmut Koca), Ankara 2020.
- Dyntu, Valeriia-Dykyi Oleh, *Cryptocurrency in the System of Money Laundering*, Baltic Journal of Economic Studies Vol. 4, No. 5, 2018, (75-81).
- FATF REPORT, Virtual Currencies Key Definitions and Potential AML/CFT Risks June 2014.
- Grzywotz, Johanna, *Virtuelle Kryptowährungen und Geldwäsche*, Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2019.
- Heine, Sonja, *Bitcoins und Botnetze - Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining*, NSTZ 2016.
- Herzog, Flix-Achtelik, Olaf, *Geldwäschegesetz Kommentar*, 2. Auflage, 2014.
- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation the FATF Recommendations Updated October 2020.
- Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, Mali Suçları Araştırma Kurulu Başkanlığı, Mayıs 2021.
- Mutluoğlu, Derya, *Kripto Para Birimleri ve Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu*, Ankara 2020.
- Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>.
- National Strategy for Combating Terrorist and Other Illicit Financing, 2020.
- Report of the Attorney General's Cyber Digital Task Force, October 2020.
- Rückert, Christian, *Vermögensabschöpfung und Sicherstellung bei Bitcoins*, MMR 5/2016.
- Sicignano, Gaspare Jucan, *Money Laundering using Cryptocurrency: The Case of Bitcoin!*, Athens Journal of Law, Volume 7, Issue 2, April 2021.
- Simmler, Monika-Selman, Sine-Burgermeister, Daniel, *Beschlagnahme von Kryptowährungen im Strafverfahren*, AJP/PJA 8/2018.
- Tahan, Özge, *Kripto Paraların Türk ve Alman Ceza Hukuku Düzenlemeleri Yönünden Değerlendirilmesi*, Suç ve Ceza, Cilt: 14, Sayı: 1, Mart 2021.
- Üzer, Betül, *Sanal Para Birimleri*, Uzmanlık Yeterlik Tezi, Türkiye Cumhuriyet Merkez Bankası Ödeme Sistemleri Genel Müdürlüğü, Ankara 2017.

Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals, April 3, 2019.

Wegberg, Rolf van - Oerlemans, Jan Jaap - Deventer, Oskar van, *Bitcoin Money laundering*, Journal of Financial Crime Vol. 25 No. 2, 2018 (419-435).

<https://www.bloomberg.com/news/articles/2021-05-20/treasury-calls-for-crypto-transfers-over-10-000-reported-to-irs>.

<https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

Peer-to-Peer File Sharing: A Guide for Business, Federal Trade Commission, <https://www.ftc.gov/system/files/documents/plain-language/bus46-peer-peer-file-sharing-guide-business.pdf>.