KRİPTO VARLIKLARIN SUÇ GELİRLERİNİN AKLANMASINDA KULLANILMASI VE ALINMASI GEREKEN ÖNLEMLER[*]

Prof. Dr. Murat Volkan Dülger[**]

Öz

Teknolojinin her geçen gün kaydetmekte olduğu ilerleme, diğer pek çok alanda olduğu gibi hukuk alanında da hem olumlu hem de olumsuz pek çok gelişmeyi ortaya çıkarmaktadır. Ceza hukuku alanında da kimi zaman yeni suç tipleri meydana gelirken kimi zaman da zaten var olan suç tiplerinde çeşitli düzenlemelere ihtiyaç duyulmaktadır. Bu düzenleme ihtiyacı çoğunlukla suçun işleniş şeklinde kendini göstermektedir. Zira teknolojik gelişme neticesinde çoğunlukla bir suçun işlenebilmesi için yeni yöntemler ortaya çıkmaktadır. Bunun son yıllardaki en yaygın örneği ise suç gelirlerini aklama suçunun hayatımıza bir anda dahil olan kripto varlıklar kullanılması suretiyle işlenmesidir. Bu çalışmamızda kripto varlıkların suç gelirlerinin aklanmasında kullanılıp kullanılmadığı, kripto varlıkların hangi yöntemlerle suç işlemekte kullanıldığı, bu nedenle ortaya çıkan risklerin neler olduğu ve bu durum karşısında ne tür önlemler alınması gerektiği açıklanmıştır. Son olarak ülkemizde yapılan hukuki düzenlemelere yer verilmiştir.

Anahtar Kelimeler: *Kripto varlık, kripto para, kara para aklama, suç geliri, suç gelirlerinin aklanması, blok zincir, dağıtık defter teknolojisi.*

THE USE OF CRYPTO ASSETS IN MONEY LAUNDERING AND THE MEASURES TO BE TAKEN AGAINST LAUNDERING SCHMES ABSTRACT

Abstract

With the advancement of technology day by day, there are many positive and negative developments in the field of law as in many other fields. In the field of criminal law, sometimes new types of offences occur, and sometimes the way in which existing types of offences are committed changes. In recent years, with the inclusion of crypto assets in our lives, the crime of money laundering by using crypto assets is frequently on the agenda. In this study,

[*] Makalenin kaynakçasının düzenlenmesi, düzeltmelerin ve son okumaların yapılmasında katkılarını sunan sayın Av. Gülçin Gümüş'e ve sayın Güldane Kadaş'a çok teşekkür ederim.

[**] İstanbul Aydın Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi. https://orcid.org/0000-0003-4034-5436.

it is explained whether crypto assets are used for laundering the proceeds of crime, the methods by which crypto assets are used to commit crimes, what are the risks arising for this reason and what kind of measures should be taken against this. Finally, the legal arrangements made in our country are included.

Key Words: *crypto asset, crypto money, money laundering, proceeds of crime, laundering of proceeds of crime, blockchain, distributed ledger technology*

GİRİŞ

Kripto varlıkların suç gelirlerinin ya da halk arasında bilinen adıyla kara paranın aklanmasında kullanılması her geçen gün daha çok gündeme gelmektedir. Bu durumda hem akademik yazında hem de suç gelirlerinin aklanmasıyla mücadele eden ulusal ve uluslararası kuruluşların çalışmaları ile düzenlemelerinde bu olgunun sıklıkla yer alması etkili olmaktadır. Bu konudaki bir diğer önemli etki ise ülkemizde son zamanlarda özellikle suç gelirlerinin aklanmasıyla ilgili yürütülen soruşturmalarda kripto varlıkların önemli bir yer tutmasıdır.[1] Ülkemizin pek çok yerinde eş zamanlı olarak suç gelirlerinin aklanması (TCK m. 282), kumar oynanması için yer ve imkân sağlamak (TCK m. 181), kişisel verilerin hukuka aykırı olarak ele geçirilmesi (TCK m. 135) ve aktarılması (TCK m. 136) ve suç işlemek amacıyla örgüt kurma veya örgüte üye olma (TCK m. 220) suçları nedeniyle soruşturmalar yapılmakta ve davalar açılmaktadır. Bu soruşturmalarda çok sayıda şüpheli yakalanıp gözaltına alınmakta, bu kişilerin önemli bir kısmı da tutuklanmakta ve oldukça uzun süreler tutuklu kalmaktadırlar.

Uluslararası alanda da suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadele eden kuruluşların ve diğer uluslararası örgütlerin, kripto varlıkların aklama ve terörizmin finansmanında kullanıldıklarına ilişkin görüşleri ve bu konuya risk temelli yaklaşımları bulunmaktadır. Bu yaklaşımın ve yaratılan algının ise gerçeği ne kadar yansıttığı tartışmalıdır. Ancak kripto varlıklar

[1] Nitekim bu soruşturmaların, ülkemizde suç gelirlerinin aklanmasıyla ciddiyetle mücadele edildiği göstermesi nedeniyle, üç yıldır FATF'nin gri listesinde bulunan Türkiye Haziran 2024 tarihi itibarıyla bu listeden çıkarılmıştır. Bu konuda bir önemli adım da Sermaye Piyasası Kanunu'nda kripto varlıklar hakkında düzenleme yapılmasıdır. Türkiye'nin bu listeye alınması süreci ve nedenleri hakkında ayrıntılı bilgi için bkz: **Hüseyin Işık**, "Mali Eylem Görev Gücü'nün (FATF) Gri Listesi ve Türkiye", International Journal of Public Finance, Vol. 7, No. 2, 2022, s. 414-421.
"Tavsiyelere uyum göstermeyen ülkeler kara listeye, kısmen uyum gösteren ülkeler ise gri listeye alınmaktadır. FATF tavsiyelerini önemli ölçüde uygulayan ülkeler ise herhangi bir listeye alınmamaktadır. Listeye alınmak FATF Tavsiyeleri bakımından ilgili ülkenin bazı zafiyetlerinin bulunduğu anlamına gelmektedir. FATF listesinin açıklanması hem dünya kamuoyunda hem de ülke kamuoyunda ciddi yankı bulmaktadır. Türkiye 2019 yılında karşılıklı değerlendirmeye alınmıştır. Bu değerlendirme sonucu aynı yılın Aralık ayında değerlendirme raporu yayınlanmıştır. Bu raporun ertesinde eleştiri konusu hususların Türkiye tarafından giderilmesi beklenmiştir. Eleştiri konusu hususlarda ilerleme sağlanmadığı belirtilerek 2021 yılı Ekim ayında yapılan FATF genel kurul toplantısında Gri Listeye alınmıştır. Gri listeye alınma ülke kamuoyunda da ciddi düzeyde tartışılmıştır." **Işık**, s. 408.

yoluyla suç gelirlerinin aklanması, dünya çapında hükümetler ve kolluk kuvvetleri için giderek artan bir endişe kaynağı olmaktadır.[2]

Kripto varlıklar, kripto varlıkların özellikleri, bu varlıklara ilişkin regülasyonların nasıl olması gerektiği gibi konularda oldukça çok şey yazılabilir. Ancak bu makalenin konusu, kripto varlıklar ile suç gelirlerinin aklanmasının kesişim kümesinden oluşmaktadır. Bununla birlikte bu kesişim kümesi de her iki konunun çok yönlü olması nedeniyle oldukça geniştir. Bu nedenle makalemizde tartışmak istediğimiz ana konuları şu sorular ile daraltabilir ve makalemizin sınırlarını çizebiliriz.

Bu bağlamda, tek başına kripto varlık bulundurmak, almak, satmak veya halka ilk arz yapmak suç mudur? Bu işlemlerin hukuka aykırı bir yönü var mıdır? Diğer suçlar bir yana kripto varlıklar gerçekten ifade edildiği kadar çok suç gelirlerinin aklanmasında kullanılmakta mıdır? Bu araçlar gerçekten aklama işlemlerini kolaylaştırmakta ve artırmakta mıdır? Bu araçların aklama işlemleriyle birlikte anılması bugünün bir sorunu mudur yoksa geleceğe yönelik bir önlem midir? Ülkemizde bu konuda yapılan soruşturmalarda gerçekten bu araçlar mı hedef alınmaktadır yoksa başka bir amaç var mıdır? Ülkemizde bu konuda ne şekilde bir düzenleme yapılmıştır? İşte bu çalışmamızda tüm bu sorulara yanıt bulmaya çalışacağız.

Kripto Varlıkların Tanımı ve Ortaya Çıkışı

Kripto varlıkların suç gelirlerinin aklanmasını kolaylaştırmak amacıyla nasıl kullanılabileceğine geçmeden önce kripto varlığın ne olduğunu anlamak gerekir.

Kripto varlık *"yalnızca dijital olarak var olan, genellikle merkezi bir ihraç veya düzenleme otoritesi olmayan, bunun yerine işlemleri kaydetmek için merkezi olmayan bir sistem kullanan dijital varlık birimi"* olarak tanımlanabilir. Kripto varlıklar, fiat (itibari)[3] paralardan farklı olarak herhangi bir merkezi otorite tarafından çıkarılmaz ve bunların arkasında herhangi bir devletin güvencesi bulunmaz. Bu da *"alıcı ya da satıcı için herhangi bir koruma olmadığı ve ödeme olarak kullanımının tamamen isteğe bağlı olduğu"* anlamına gelir.[4] Dolayısıyla blok zincir teknolojisi üzerine kurulu bu varlıklar, üzerine kurulu oldukları teknolojinin doğası

[2] **Romel Sharif**, "Digital Bill: An Approach to Minimize Illicit Activities and other Drawbacks of Crypto Currency", Mayıs 2023, (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4434303, (set) 28.07.2024.

[3] Fiat veya diğer ismiyle itibari para, hükümet kararına dayalı olarak çıkartılan, altın, gümüş vs. karşılığı olmayan, altında imzası olan yere ve düzenlendiği kâğıdın taklit edilemeyeceğine güven üzerine kurulmuş, mal ve hizmet alışverişi için kullanılan banka kâğıdı veya kâğıt para demektir. Günümüzde dolaşımda olan paralar bu şekildedir.

[4] **George Forgang**, Money Laundering Through Cryptocurrencies, Unpublished Master of Science Thesis, La Salle University Economic Crime Forensics Capstones 40, 2019, s. 4 (Çevrimiçi) https://digitalcommons.lasalle.edu/ecf_capstones/40, (set) 15.06.2024.

gereği merkeziyetçi bir yapıya sahip değildirler.[5] Bu da işlemler esnasında merkezi bir kayıt tutulmamasına ve yarı anonim bir yapının ortaya çıkmasına neden olmaktadır. İşte bu yarı anonim yapı ve merkeziyetsizlik; bir yandan yakalanmak istemeyen suçluları kendine çekerken diğer yandan adli makamların işini zorlaştırmaktadır. Öte yandan yapılan işlemlerin kontrol edilmesini imkânsız kılacak ölçüde sınırsız hesap oluşturma imkânı, kripto varlık aracı kurumları (borsalar) aracılığıyla kişiden kişiye transfer imkânı ve finansal faaliyetleri saklayabilme imkânı suç gelirlerinin aklanmasında kripto varlıkların tercih edilmesine neden olan diğer unsurlardır.[6]

Kripto varlıklar arasından en eskisi, en bilineni ve en yaygın kullanılanı Bitcoin'dir ve ilk olarak 2008 yılında *Satoshi Nakamoto* tarafından tanıtılmıştır.[7] Ancak bu ismin takma bir ad olduğuna inanılmaktadır. Bitcoin'in tanıtılmasından bu yana geçen yıllarda, geliştirici(ler)in gerçek kimliği veya kimlikleri konusunda önemli miktarda spekülasyon yapılmıştır, ancak *Satoshi*'nin kimliği henüz çözülememiş bir gizem olarak varlığını sürdürmektedir. Bitcoin, 2008 finansal krizinden sonra dünyaya tanıtılmış ve şirketlerin müdahaleleri ile hükümetlerin düzenlemelerinden arınmış, alternatif bir para birimi olması amaçlanmıştır. Bitcoin'e sahip olan bireyler bu para birimini herhangi bir kısıtlama olmaksızın özgürce kullanabilir ve finansal bir aracıya ihtiyaç duymaksızın dünya çapında paralarını hareket ettirebilir. Bu konudaki yaygın efsaneye göre Florida'lı bir adam pizza karşılığında 10.000 Bitcoin teklif etmiştir (o zamanlar Bitcoin bugünkünden çok daha düşük bir değere sahipti). Birleşik Krallık'taki bir kişi bu teklifi kabul etmiş ve iki adet Papa John's pizzasının Florida'daki Bitcoin kullanıcısına teslim edilmesini sağlamıştır.[8] Eğer efsane doğruysa muhtemelen bu pizzalar bugüne kadar dünyada satılan en pahalı pizzalardır. Bu Bitcoin ile yapıldığı bilinen ilk işlemdir. Bu işlem tek başına son derece zararsız ve sıradan olsa da, Bitcoin'in anonimlik özelliği ve hukuk tarafından düzenlenmemiş olması suçluların dikkatini çok kısa bir zaman içinde çekmiş ve kısa süre içerisinde kötü amaçlar için kullanılmaya başlanmıştır.[9] Bitcoin'in ve dolayısıyla kripto varlıkların yaygın şekilde suçla anılması ve sanki yalnızca suç işlemekte kullanılan bir araçmış gibi algılanmasına

[5] **Kerim Çakır**, Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu, 2. Baskı, Adalet Yayınevi, Ankara, 2023, s. 77.

[6] **Murat Balcı/Kerim Çakır**, Kripto Paraların Karapara Aklama Yöntemi Olarak Kullanılması, CHD, Yıl: 16, Sayı: 46, Ağustos, 2021, s. 317.

[7] **Satoshi Nakamoto**, "Bitcoin: A Peer-to-Peer Electronic Cash System", 30 Ekim 2008, (Çevrimiçi) https://bitcoin.org/bitcoin.pdf, (set) 11.07.2024; **Çakır**, s.77; **Berrin Akbulut**, "Kripto Para ve Terörizmin Finansmanı", Karşılaştırmalı Hukukta ve Türk Hukukunda Terörizm, Terör Suçları ve İnfaz Hukuku, Ed. İzzet Özgenç, I. Cilt, Türkiye Bilimler Akademisi, Ankara, 2024, s. 487.

[8] **Alison Griswold**, "The First-Ever Bitcoin Purchase Was Remarkably Inglorious" Slate, 23 Mayıs 2014,https://slate.com/business/2014/05/first-bitcoin-purchase-twopepperoni-pizzas-from-papa-john-s.html

[9] **Forgang**, s. 4, 5. Bitcon özelinde kötüye kullanımlar için bkz. **Sesha Kethineni/Ying Cao/Cassandra Dodge**, "Use of Bitcoin in Darknet Markets: ExaminingFacilitative Factors on Bitcoin-Related Crimes", American Journal of Criminal Justice, Vol. 43, Issue 2, Mayıs 2017.

neden olan olay 2011-2013 yılları arasında faaliyet gösteren "Silk Road"[10] adlı çevrimiçi bir pazar yeridir. Silk Road başta kullanıcılar için anonim ve güvenli bir pazar yeri iken daha sonra kötü niyetli kişilerin uyuşturucu ticareti ve suç gelirlerini (kara para) aklama amacıyla kullandığı bir alan haline gelmiştir.[11] Bu site "dark net" denilen karanlık ağda faaliyet göstermiş ve siteye erişebilen bireylerin çok sayıda yasa dışı malı yakalanma tehdidi olmadan kolayca alıp satabilmesine olanak sağlamıştır. Site faaliyetteyken 100.000'den fazla kullanıcının uyuşturucu, sahte kimlik ve pornografi dahil olmak üzere 200 milyon dolardan fazla değerde yasa dışı mal alıp sattığı tahmin edilmektedir.[12] Kapsamlı bir soruşturmanın ardından web sitesi FBI tarafından kapatılmış ve site yöneticisi Ross Ulbricht kara para aklama ve uyuşturucu kaçakçılığı suçlamalarıyla tutuklanmıştır. Buna ek olarak, ABD Adalet Bakanlığı yaklaşık 3,5 ile 4 milyon dolar arasında Bitcoin'e el koymuştur.[13]

Uyuşturucu ya da silah gibi izinsiz bulundurulması, verilmesi, alımı ve satımı suç olan ürünlerin herhangi bir yasal düzenleme olmaksızın internet üzerinden alınıp satılması tek başına önemli bir sorundur. Buna ek olarak Silk Road olayı yetkililere Bitcoin'in bu şekildeki yasa dışı faaliyetleri kolaylaştırmak için kullanılabileceğini ve bu nedenle yalnızca masum bir yenilik olarak algılanmaması gerektiğini de göstermiştir.[14] Silk Road faaliyetteyken, Bitcoin tek kripto varlık birimi olarak dolaşımdaydı. O zamandan bu yana binlerce yeni kripto varlık birimi piyasaya sürülmüştür. Teknik olarak Bitcoin olmayan tüm kripto para birimleri "altcoin" olarak kabul edilmektedir. Bunlardan Ethereum ve Ripple, Bitcoin'den sonra en yüksek değere sahip diğer iki kripto varlık birimidir ve bu özellikleri görünüşte onları en tanınır, aktarılabilir ve tartışmalı olmakla birlikte meşru kılmaktadır.[15] Ancak günümüzde kripto varlık aracı kurumlarında işlem gören altcoinlerin sayısı binlerle ifade edilmektedir.

Kripto Varlıkların Yapısı

Kripto varlık birimleri, güvenilir üçüncü tarafların aracılığı veya gözetimi olmamasına rağmen, işlem bütünlüğünü ve hızını sağlamak için kriptografik ilkeleri kullanan küresel, kalıcı ve sansürsüz bir dijital ortamda çalışır.

[10] "Silk Road" kavramı "İpek Yolu" anlamına gelmektedir. Özel isim olması sebebiyle makalede "Silk Road" kavramı tercih edilmiştir.
[11] **Balcı/Çakır**, s. 323.
[12] **Corinne Ramey**, "The Crypto Crime Wave is Here" The Wall Street Journal, 26 Nisan 2018, (Çevrimiçi) https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366, (set) 10.07.2024.
[13] **Arnold Greenberg**, (2018, April 23). "The Dark Web's Favorite Currency Is Less Untraceable Than It Seems", Wired, 23 Nisan 2018, (Çevrimiçi) https://www.wired.com/story/monero-privacy/ (set) 10.07.2024.
[14] **Forgang**, s. 5.
[15] **Forgang**, s. 6.

Bu tür kripto varlıklar, eşler arası ("P2P")[16] veri (değer) değer aktarımı için geliştirilmiş genel ve özel anahtarlara dayanır ve her aktarım işlemi kriptografik olarak imzalanır. Ardından çoğaltılmış ve paylaşılan bir veri yapısının fikir birliği mekanizması (blok zincir teknolojisi) aracılığıyla doğrulanır. Buna ek olarak, kripto varlıklarının merkezi olmayan yapısı nedeniyle işlemlerin gözetimine sahip olan ve sorumlu tutulabilecek ve şüpheli işlemlerin ilgili makamlara bildirilmesi gereken banka gibi merkezi bir aracı kurum da yoktur. Aslında, anonim kullanıcılara ve merkezi olmayan yönetime dayalı, hesap verebilirlik olmaksızın, herhangi bir yerden izin almak gerekmeksizin DLT (Distributed Ledger Technology / Dağıtık Defter Teknolojisi) üzerinde çalışan kripto varlıkların, geleneksel ödeme yöntemlerine kıyasla suç gelirlerinin aklanması için kullanılma potansiyeli daha yüksek ve kötüye kullanıma daha açıktır.[17] Kripto varlıklarının sınır tanımayan P2P biçiminde işleyen doğasının çeşitli varlıkların (fonların) mevcut AML/CFT[18] yapısının izleyemeyeceği ve engelleyemeyeceği bir şekilde anında transfer edilmesine izin verdiği ileri sürülmektedir. Söz konusu risk, gönderenlerin ve alıcıların kripto varlık cüzdanlarının adreslerine bağlı herhangi bir gerçek isim olmadığı için kişisel kimlik tespiti gerektirmeyen P2P temelinde kripto aktarım işlemlerini gerçekleştirebilmelerinden kaynaklanmaktadır. Yukarı aktarılanlar göz önünde bulundurulduğunda bu riskin önceliğinin yüksek olduğu görülmektedir.[19]

Kripto varlıkların yapısını ve işleyişini bir örnek üzerinden geleneksel finans sistemiyle karşılaştırarak şu şekilde özetleyebiliriz: Geleneksel finans sisteminde hem X hem de Y bankalarına (Banka A ve Banka B) güvenirler. Bu sistemde fon transferi yapılması, X'in hem Y'nin bankasının tanımlayıcısını hem de Y'nin hesabının tanımlayıcısını bulmasını gerektirir. Bir sonraki adımda fon transferinin gerçekleşmesi için X'in parayı Y'nin hesabına transfer etmek istediğini bankasına bildirmesini gerektirir. X'in bankası bu işlemi kontrol eder ve eğer geçerliyse, tanımlanan tutar kadar hesabından çekim yapılır ve bu tutar A Bankasından B Bankasına iletilir ve Y'nin bankası da bu tutarı onun hesabına alacak olarak kaydeder. Bu yöntemde hem A Bankasının hem de B Bankasının işlemi kontrol edebilecek

[16] "Peer-to-peer (P2P) teknolojisi ise iki 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. Kripto para birimi satın almak veya satmak isteyen bireyler genellikle peer to peer dönüştürücüler veya tacirler olarak anılan bireylerine networküne yönelmektedir." **Balcı/Çakır**, s. 316.

[17] FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks Report, Haziran 2014, 9.

[18] Anti Money Laundering / Counter Financing Terrorism = Suç Gelirlerinin Aklanmasıyla ve Terörizmin Finansmanıyla Mücadele.

[19] **Christopher P. Buttigieg/Christos Efthymiopoulos/Abigail Attard/Samantha Cuyle**, "Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State," Law and Financial Markets Review, Vol. 13, No. 4, 2019, s. 212, 213.

defterleri (ledger) bulunur ve tüm işlemler bu defterlere (günümüzde dijital kayıtlar) kaydedilip saklanır. Her banka hem X'in ve Y'nin işlemlerini hem de gerçekleşmesi olası olağandışı işlemleri raporlayabildiğinden, bu yöntem suç soruşturması bakımından son derece önemli ve yararlıdır.

Ancak internetin yeni yeni yaygınlaştığı ve kamuya açıldığı 1990'ların siberpunkları, özellikle bankaların işlemlerden elde ettiği karlarda, bankaların aracı takası sağlama gerekliliklerini sorgulamaya başladılar. Yaklaşımları, halka açık bir defter olan blok zinciri kullanmak ve ardından işlemleri genel anahtar şifrelemesiyle imzalamaktı. Madenciler (doğrulama için matematiksel işlemler yapan ve ödül olarak belirli miktarda kripto varlık alan kişiler) daha sonra son işlemler için bir fikir birliği oluşturmak için rekabet edebilecek ve kazanan blok zincirine yeni bir blok ekleyecekti. Bitcoin altyapısında X ve Y'nin her biri için özel bir anahtar oluşturulur ve ardından ilişkili bir genel anahtar türetilir. Bu ortak anahtar daha sonra işlemler için genel bir kimlik adresi oluşturmak için kullanılır. X artık Y'ye bir miktar para göndermek istediğinde, onun açık adresini bulur ve ardından ona bir miktar Bitcoin göndermek için bir işlem oluşturur. Bu onun özel anahtarıyla imzalanır ve daha sonra diğer tüm son işlemleri bir araya toplayacak ve işlemlerin blok zincir üzerinde yeni bir bloğa eklenmesi için bir fikir birliği oluşturacak madenciler tarafından alınır. Bunun gerçekleşmesinden önce, X'in hesabında Y'ye ödeme yapmaya yetecek kadar Bitcoin olup olmadığının kontrol edilmesi gerekir. Bu kontrol, işlemlerin halka açık olmasının nedenidir; çünkü X'in Y'ye ödeme yapacak yeterli parası yoksa madenciler işlemi gerçekleştiremez. Daha sonra X'i ve Y'yi genel bir adresle eşleştirmek için sahte bir kimlik kullanılır. Tanımlayıcıları eşleştirmek zor olsa da kolluk kuvvetleri en azından işlemler için bilinen adreslerin izini sürebilir. Ancak bu modelle ilgili endişe, fonların fiat para birimine çevrilmesi söz konusu olmadığı sürece fonların hiçbir zaman bir banka hesabına ulaşmayacağıdır. Dolayısıyla bu tür bir yaklaşım hem vergi toplama yetkililerini hem de kolluk kuvvetlerini endişelendirmektedir. Bu nedenle, dünya çapında birçok hükümet kripto varlıklara yönelik düzenleme yapma ve böylece fon akışlarını denetlemeyi sağlamayı istemektedir. Ancak aşırı düzenleme yapılması halinde bunun da yeni teknolojilerin ortaya çıkmasını engellemesinin mümkün olabileceği endişesi söz konusudur.[20]

Bu işleyişi şu şekilde de tanımlayabiliriz: Tüm işlemlerin açık anahtarları blok zincirinde saklansa da, bunlar herhangi bir kişinin kimliğiyle bağlantılı değildir. Güvenlik uzmanları bu durumu, takma isimle kitap yayınlamaya benzer şekilde takma isimle gizlilik olarak adlandırmaktadırlar. Takma ad sizinle bağlantılı olmadığı sürece gizliliğinizi koruyabilirsiniz. Ancak hile,

[20] **Simon Dyson/William J. Buchanan/Liam Bell**, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime", The Journal of British Blockchain Association, Volume 1, Issue 2, 2018, s. 1, 2.

birisi kitaplarınızdan birine bağlantı verdiği anda ortaya çıkar. Böylelikle yazar, takma ad altında yazdıklarının tamamını kamuya açık hale getirir.[21]

Kripto Varlık Bulundurmak, Almak veya Satmak Suç Mudur?

Kripto başlığı altında incelediğimiz varlıkların (Bitcoin, Etherium, Monero, Zcash vb.) ihraç edilmesi, bulundurulması ve alınıp satılması hukuka aykırı olmayıp suç değildir. Ancak bu konuda 26.06.2024 tarihli ve 7518 sayılı Kanun ile 06.12.2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu'nda yapılan düzenlemelere uygun hareket edilmesi gerektiği unutulmamalıdır. Özellikle kendilerini "Kripto Para Borsası" olarak adlandıran aracı kurumlar (kripto varlık hizmet sağlayıcı) için getirilen bu düzenlemeye uygun davranılmadığında tazminat sorumluluğu, idari yaptırımlar ve suç işlenmesi söz konusu olabilecektir. Ancak aşağıda değineceğimiz üzere bu düzenleme aracı kurumlar için getirilmiştir, kripto varlığın kendisi "doğası gereği" düzenleme altına alınmamıştır. Dolayısıyla bir hukuk normuyla açıkça yasaklanmayan bir konu serbest olduğuna göre kripto varlıklara sahip olmak ve bunlarla işlem yapmak tamamen hukuka uygundur.

Bu konuda dikkat edilmesi gereken bir diğer husus da bu varlıkların ödeme aracı olarak kullanılmasının ülkemizde yasak olmasıdır. 16.04.2021 tarihli ve 31456 sayılı Resmî Gazete'de yayımlanan *"Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik"* uyarınca kripto varlıkların ödemelerde kullanılması yasaklanmıştır. Buna göre kripto varlıkların ödemelerde doğrudan veya dolaylı şekilde kullanılması ve buna yönelik hizmet sunulması yasaktır. Bu bağlamda ödeme hizmeti sağlayıcılarının, ödeme hizmetlerinin sunulmasında ve elektronik para ihracında kripto varlıkların doğrudan veya dolaylı olarak kullanılacağı bir şekilde iş modelleri geliştirmesi ve bu tür iş modellerine ilişkin herhangi bir hizmet sunması söz konusu yönetmelik gereğince hukuka aykırıdır.

O halde Sermaye Piyasası Kanunu'na ve Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik'e uygun hareket edildikten sonra bu varlıkları bulundurmak ve kullanmak hukuka aykırı değildir ve suç oluşturmaz. Kripto varlıkların hukuka aykırı işlemlerde özellikle bazı ekonomik suçların işlenmesinde kullanılması bizatihi bunların çıkarılmasını, bulundurulmasını ve kullanılmasını hukuka aykırı hale getirmez.

Bunları bulundurmak ve işleme tabi tutmak suç olmamakla birlikte, kripto varlıkların neden hep bir şekilde çeşitli suçlarla ilişkilendirildiğini anlayabilmek için kripto varlıklar ve fiat para arasındaki benzerlikleri ve farkları göz önünde bulundurmak gerekir. Aslında fiat para da özellikle nakit formda ise kripto varlıklar gibi büyük ölçüde anonimdir (yalnızca

[21] **Llambi Prendi/Daniel Borakaj/Klarida Prendi**, "The New Money Laundering Machine Through Cryptocurrency: Current and Future Public Governance Challenges", Corporate Law & Governance Review, Vol. 5, Issue 2, 2023, s. 89.

seri numaraları aracılığıyla izlenebilir) ve bu nedenle geleneksel olarak suç işlenmesini ve yasa dışı ticareti kolaylaştırmada önemli bir rol oynamıştır. Bu ikisi arasındaki temel fark, kripto varlıkların kimin yaptığı belli olmadan yani anonim şekilde dijital işlemleri ve e-ticareti mümkün kılmasıdır. Fiat parada bu günümüzde o kadar kolay değildir, zira finans sektörü çok büyük ölçüde regüle edilmiştir. Kripto paranın anonimlik sağlama özelliği ise suçlular tarafından kısa sürede keşfedilmiştir. Bilişim devriminin bir sonucu olarak ortaya çıkan e-ticaret ve dijital ödeme sistemleri perakende ve toptan ticarette devrim yaratmıştır. Çevrimiçi alışveriş, perakendeciliğin yapısını, tüketim kalıplarını, seçimi, pazarlamayı, rekabeti ve nihayetinde arz ve talebi önemli ölçüde etkilemiştir. Ticaretteki bu dijital devrimin etkisi blok zincir teknolojisi ve buna bağlı olarak kripto varlıklar ortaya çıkana kadar büyük ölçüde yasal mal ve hizmetlerle sınırlı kalmıştır, zira kripto varlıklar olmaksızın yapılan ticaretteki dijital ödemeler kolaylıkla izlenebilir. Ancak kripto varlıklar, nakit paranın anonimliğini dijitalleşme ile birleştirerek bu durumu değiştirmiştir; bu da etkin, anonim, çevrimiçi ve sınır ötesi ticareti mümkün kılmıştır. Dolayısıyla kripto varlıklar yasa dışı ürün ve hizmetlerin alışverişinde kullanılan karaborsanın işleyişinde önemli bir yapısal değişime yol açmıştır.

Kripto Varlıkların Suç İşleme Aracı Olarak Kullanılması ve Yöntemleri

1. Araç Olarak Kullanılma

Kural olarak kripto varlıkların bulundurulması ve kullanılması suç oluşturmasa da bu durum, söz konusu varlıkların suç işlemekte kullanılmayacağı anlamına gelmez. Bu araçlar başta ekonomik çıkar amacıyla işlenen suçlar olmak üzere birçok suçun işlenmesinde kullanılabilir. Son günlerde ülkemizde kripto varlıkların sürekli olarak çeşitli suçlarla birlikte anılması da bu yüzdendir.

Blok zincir teknolojisinde fon hareketlerinin izlenmesi ve bu işlemlerin arkasındaki gerçek kişilere erişilmesi oldukça güç olduğundan, yasa dışı faaliyetlerini anonim ve gizli şekilde gerçekleştirmek isteyen suçluların bir kısmı kripto varlıklar üzerinden bu faaliyetlerini sürdürmeye yönelmişlerdir. Kripto varlıklar suç gelirlerinin aklanmasının yanı sıra bilişim hırsızlığı, uyuşturucu ticareti, kaçakçılık, çocuk pornografisi ve fuhuş gibi suçların işlenmesinde de ödeme, saklama ya da aklama aracı olarak kullanılabilir. Dolayısıyla kripto varlıkların suç işlemede, suç gelirlerinin aklanmasında ve terörizmin finansmanında kullanılması potansiyel olarak mümkündür.
Kripto varlıklarla işlenen suçlar için "kripto suç" (crypto crime), "kripto para suçları" (cryptocurrency crimes) ve "kripto parayla bağlantılı suçlar" (crypto currencies related crimes) terimleri kullanılmaktadır. Kripto varlıklar, suç faillerinin ihtiyacı olan anonimlik, merkeziyetsizlik (ve dolayısıyla denetimsizlik) ve aracıya ihtiyaç duymama gibi imkânlar sağlaması nedeniyle suç işlemenin aracı ve geleneksel paranın bir alternatifi olarak kullanılmaktadır. Dolayısıyla "kripto varlık suçu" diye ayrı bir

suç türü bulunmayıp bu varlıkların suç işlemede kullanılması yalnızca saydığımız suçların yeni bir işleniş şeklini (modelini) ifade etmektedir.[22] Bu nedenle biz "kripto varlıklarla işlenen suçlar" ifadesinin daha doğru olduğunu düşünüyoruz.

Kripto varlıklar, yukarıda belirttiğimiz suçlardan daha çok ve sıklıkla suç gelirlerinin aklanması ve terörizmin finansmanı suçlarıyla anılmaktadır.[23] Bunun nedeni ise bu araçların aklama işlemlerinde gerekli olan anonimlik ve takip güçlüğü gibi özellikleri barındırmasıdır. Nitekim kripto varlıkların sağladığı anonimlik ve düzenleme eksikliğinin, suç gelirlerinin aklanması, vergi kaçakçılığı, uyuşturucu kaçakçılığı ve diğer suç faaliyetlerini kolaylaştırdığı yönünde ciddi endişeler söz konusudur.[24] Bu konudaki bir diğer önemli faktör de kripto varlıklarla yapılan işlemlerin tek bir yargı yetkisi alanına girmemesi ve merkezi bir aracının bulunmamasıdır. Bu durum söz konusu teknolojik yenilikten kaynaklanan suç faaliyetlerinin düzgün bir şekilde kontrol altında tutulmasını, kayıt altına alınmasını ve dolayısıyla soruşturulmasını ve yargılamasını zorlaştıran hukuki bir belirsizlik ortamı yaratmaktadır.[25] Tahmin edileceği üzere bu ortam suçlular, özellikle de siber suçlar ve aklama suçu gibi ekonomik suçlar işleyen kişiler için bulunmaz bir fırsattır.

Kripto varlıkların suç gelirlerinin aklanmasını kolaylaştırmak için kullanılmasındaki asıl neden kullanıcılara sağladığı yarı anonimliktir. Bu anonimliğin nedeni, banka hesaplarının aksine kripto varlık adreslerinin bireylerin adına kayıtlı olmamasıdır.[26] Kripto varlık işlemlerinde kullanılan kimlikler yarı (sözde) anonimdir, zira gerçek dünyadaki bireylere veya kuruluşlara açıkça bağlı olmamakla birlikte tüm işlemler tamamen şeffaftır, dolayısıyla izlenebilir niteliktedir ancak gerçek bir kişiyle bağının kurulması

[22] **Murat Volkan Dülger/Onur Özkan**, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi", Prof. Dr. Mehmet Emin Artuk'a Armağan, Ed. Mahmut Koca, Seçkin Yayıncılık, Ankara, 2020, s. 977, 978.

[23] "Terörizmin finansmanında blok zincirinin kullanımının bilindiği kadarıyla çok fazla olmadığı, payının düşük olduğu belirtilmektedir. Her ne kadar Bitcoin ve diğer kripto paraların geniş çapta kullanıldığında dair kanıtlar olmasa da, Avrupa ve Endonezya'daki bir dizi terör saldırısında etkilerinin bulunduğunda dair güçlü kanıtların bulunduğu, 2021 yılında Birleşmiş Milletler Terörle Mücadele Haftası kapsamında yapılan toplantılarda da terör örgütlerinin dijital finansmanına odaklanılarak, bağış toplama fırsatlarını artırdıkları ifade edilmiştir. Kripto para teknolojilerinin yüksek teknik uzmanlık gerektirmesi nedeniyle çok fazla kullanılmasa da, terör örgütlerinin bu teknolojileri kullanmak için teknik kapasitelerini artırmaları halinde kripto paraların terörizmin finansmanında kullanımında artış görüleceği ifade edilmektedir." **Akbulut**, s. 510.

[24] **Garry Jacobs**, "Cryptocurrencies & The Challenge of Global Governance", Cadmus, Vol. 3, Issue 4, Mayıs 2018, (çevrimiçi) https://cadmusjournal.org/, (set) 11.07.2024.

[25] **Elliott Maurice Nathaniel Keech**, "Crime, Innovation, and The Technology of Moneys", Unpublished PhD Thesis, University of York, York Law School, York, 2022, s. 47, 48.

[26] **Rolf van Wegberg/Jan-Jaap Oerlemans/Oskar van Deventer**, "Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin", Journal of Financial Crime, Vol. 25 Issue 2, 2018, s. 422.

çok güçtür.[27] Blok zincir, güvenilir üçüncü tarafın yerini alarak yapılan her işlemin kaydını tutan bir defter görevini üstlenir. Her bir yeni Bitcoin işleminde zincire yeni bir blok eklenir ve kaydedilir. Blok zincir, aleni ve kamuya açık olmasına rağmen düşünülenin aksine oldukça güvenilirdir.[28] Blok zincir teknolojisi dağıtılmış defter teknolojisi (DLT) olarak bilinen bir işlem arşivi oluşturur, her işlem bloğunun bir kopyası dağıtılır ve ağın tüm üyeleri tarafından görülebilir hale getirilir.[29] Bireyler ve suç örgütleri farklı takma adlar kullanarak gerçek kimliklerini gizleyebilirler, bu da işlemlerin yarı anonim olarak yapılmasını sağlar ve işlemlerin arkasındaki gerçek kişilere ulaşmayı çok zor hale getirir. Ayrıca kripto varlıkların bir banka veya güvenilir üçüncü bir taraf aracılığıyla transfer edilmesi gerekmez. Bunun yerine kripto varlık serbestçe ve bağımsız olarak hareket ettirilebilir.[30]

Kripto varlıklar diğer geleneksel para birimlerine göre daha fazla anonimliğe izin verir çünkü halka açık defter üzerinde işlem yapan taraflar yalnızca kendi açık anahtarlarıyla tanımlanır ve kripto varlıkların üzerinde çalıştığı dağıtık defter teknolojisi anonim fonlamaya (nakit fonlama veya fon kaynağını doğru bir şekilde tanımlamayan sanal değiştiriciler aracılığıyla üçüncü taraf fonlama) izin verir. Bunun yanı sıra KYC açısından çok önemli olan fonu gönderenin ve alıcının yeterince tanımlanmadığı anonim transferlere de izin verir.[31] Bunlara ek olarak kripto varlık teknolojisindeki bazı gelişmeler, fon transferlerinin izlenmesini daha da zorlaştırmaktadır. Örneğin, Bitcoin ve diğer bazı altcoin işlemlerinin anonimliğini ortadan kaldırmak için bazı blok zincir analiz araçları mevcut olsa da, gizlilik (mahremiyet) varlıkları (Monero, ZCash, Dash), zincir dışı kanallar (örneğin LightningNetwork, Raiden, Plasma vb.) ve karıştırıcılar/tamburlar (örneğin Shapeshift) KYC için zorluklar oluşturmaktadır. Gizlilik varlıkları açık kaynaklı halka açık DLT'leri kullanarak çalışsa da, aynı görünürlüğü veya tanımlayıcı ayrıntıları sunmazlar. Örneğin, Monero, DLT'sindeki işlemlerin göndericisi, alıcısı veya değeri hakkında görünürlük sağlamaz. Yalnızca gönderenin ve alıcının işlem ayrıntılarına erişebilmesini sağlamak için gizli adresler veya tek seferlik kullanım için oluşturulan yeni adresler kullanır ve ayrıca bir grup kullanıcı arasında işlemlerin imzalanmasını sağlayan halka imzalar oluşturur, böylece imzanın bireysel kullanıcılara atfedilmesini engeller. Öte yandan, Zcash'te gizlilik isteğe bağlıdır ve tarafların bilginin geçerliliği konusunda fikir birliğine varması sağlanarak Zcash ağındaki işlemlerin meşruiyetini garanti altına alan ve aynı zamanda diğer tarafların kimliğinin

[27] **Sarah Meiklejohn/Marjori Pomarole/Grant Jordan/Kirill Levchenko/Damon McCoy/Geoffrey M. Voelker/Stefan Savage**, "A Fistful of Bitcoins: Characterizing Payments among Men with No Names", Communications of the ACM, Vol. 59, Issue 4, Nisan 2016, s. 86.
[28] **Balcı/Çakır**, s. 315, 316.
[29] **David Yermack**, "Corporate Governance and Blockchains", Review of Finance, Vol. 21, Isuse 1, Mart 2017, s. 17.
[30] **Forgang**, s. 6, 7.
[31] FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks Report, Haziran 2014, 9.

şifreli ve korumalı kalmasına izin veren "zero-knowledge proof" (sıfır bilgi kanıtı)[32] özelliğini içermektedir.[33]

Bu nedenle kripto varlıklar suçlular için denetim organları tarafından kontrolü daha zor olan yeni fırsatlar yaratmaktadır. Kripto varlıkların sağladığı yarı anonimlik, görünmez yasa dışı işlemler ile suç gelirlerinin aklanması ve terörizmin finansmanı için giderek daha fazla kullanılmaktadır.[34] Ancak kripto varlıkların bu sıklıkla aklama ve terörizmin finansmanıyla anılma durumu aklama işlemlerinin çoğunluğunun kripto varlıklarla yapıldığı ve hatta aklama işlemlerinin kripto varlıkla birlikte başladığı ya da arttığı anlamına gelmemektedir.[35] Zira suç gelirlerinin aklanması, blok zincir teknolojisinin keşfedilmesi ve bunun Bitcoin ve diğer altcoinlere uygulanmasıyla ortaya çıkmamıştır.[36] Suç gelirlerinin aklanmasının tarihi henüz bilgisayarın icat edilmediği 20. yüzyılın başına kadar gitmektedir.

Kripto varlıkların sıklıkla suç gelirlerinin aklanmasıyla birlikte anılması, asıl olarak blok zincir teknolojisinin sağladığı iki özellik nedeniyledir. Bunlar, küresel ağlardaki işlemlerin merkeziyetçi olmayan (dağıtık) yapısı ve yarı anonimliğinin sağlanmasıdır. Böylelikle uluslararası alanda suç gelirlerinin aklanması için yeni yöntemlerin ortaya çıkması sağlanmıştır.[37] Bu bağlamda kripto varlıklar, blok zincir teknolojisinin sağladığı özellikler nedeniyle aklama suçunun üç aşamasında da kullanılabilir:[38]

a) Yerleştirme Aşaması: Suç geliri, nakit veya diğer finansal araçlar yerine kripto varlık olarak işlem gördüğünde blok zincir teknolojisinin getirdiği aracıya ve doğrulamaya ihtiyaç duymadan tarafların karşılıklı işlem yapabilmesi anlamına gelen eşler arası işlem yapabilme özelliği (P2P) sonucu, bankacılık ve finans sistemlerinin tabi olduğu sıkı denetimden kurtulmayı sağlar.[39] Yerleştirme aşaması, bir kripto varlık borsasından (örn. Bitcoin, Etherum, Litecoin) veya çoğunlukla regüle edilmemiş olan kripto ATM'lerinden nakit veya banka kartı ile birincil kripto varlıkların satın alınmasını içerir. Bu aşamada, aracı kurumlardaki KYC doğrulamasından geçmek için genellikle temiz kayıtlara ve doğrulanmış bilgilere sahip

[32] Sıfır bilgi ispatı, bir kişinin diğer bir kişiye söz konusu bilgiye doğrudan erişim izni vermeden ilgili bilgiye sahip olduğunu teyit ettiği bir yöntemdir.
[33] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 213.
[34] **Keech**, s. 54; **Çakır**, s. 77.
[35] **Ole Bjerg**, "How is Bitcoin Money?", Theory, Culture & Society, Vol. 33, Issue 1, 2016, s. 53-72.
[36] **Malcolm Campbell-Verduyn/Marcel Goguen**, "The Mutual Constitution of Technology and Global Governance: Bitcoin, Blockchains, and the International Anti-money-laundering Regime", in: Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018, s. 72; **Bjerg**, s. 53-72; **Forgang**, s. 14.
[37] **Campbell-Verduyn/Goguen**, s. 74.
[38] **Balcı/Çakır**, s. 324.
[39] **Erdal Durdu**, Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku, Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2018, s. 189; **Campbell-Verduyn/Goguen**, s. 74; **Dülger/Özkan**, s. 989.

"saman adamlar" yani bu işlemin gerçek lehtarı olmayan kişiler kullanılır. Yasa dışı aktörler ayrıca bir İlk Para Arzında ("ICO") kripto varlıkları satın alarak da yasa dışı gelirlerden kaynaklanan fonları temizlemeye çalışabilir. Bir ICO'dan satın alınan coinlerin yeni basılmış olma gibi ek bir avantajı vardır ve işlem geçmişiyle ilişkili riskleri ortadan kaldırır. Bu aşamada, parayı önemsiz miktarlarda ve farklı yerlerde bölmek için genellikle "*şirinleme*"[40] *yöntemi kullanılır.*[41]

b) Ayrıştırma Aşaması: "Karıştırma" (mixing) adı verilen, kimlik takibini önleyen ve işlemleri öngörülemeyen kombinasyonlarla bir araya getiren karmaşık fon hareketleri gerçekleştirilerek, kripto varlıkların suç gelirinin kaynağı ile ilişkisi kopartılabilir ve bu şekilde izi kaybettirilebilir.[42] *Bu bakımdan blok zincir teknolojisi ve ayrıştırma aşamasının bilişim sistemleri üzerinden kripto varlıklarla gerçekleştirilmesi, suç faillerine çeşitli imkanlar sunar.*[43] *Ayrıştırma aşaması, fonların kaynağını gizlemek ve tespit edilmekten kaçınmak için tasarlanmış çeşitli ve sınırsız işlemlerden oluştuğu için en karmaşık aşamadır. Birincil kripto varlıkların izini gizlemek amacıyla, birincil adreslerini geçici cüzdan adresleriyle değiştirmek için karıştırma veya tambur hizmetleri gibi teknikler kullanılır ve böylece bu işlemlerin denetleyici kurumlar tarafından izlenebilirliği engellenir. Kullanılan bir diğer yöntem de alıcı adreslerini kasıtlı olarak tahrif ederek işlemleri yedek adreslere yeniden yönlendirmek ve böylece denetim defterini bozmaktır. Karıştırılan birincil kripto varlıklar daha sonra gizlilik varlıkları satın almak üzere bir kripto varlık aracı kurumuna (örn. Kraken, Binance, Coinbase) aktarılır. Yasa dışı fonlar ya da suç gelirleri etkin bir şekilde temizlenir ve birden fazla gizlilik varlığı, borsa ve dijital adresin izinin takip edilmesini zorlaştıracak şekilde katmanlanması yoluyla geleneksel finansal sisteme entegrasyon için hazırlanır.*[44]

c) Bütünleştirme Aşaması: Suçtan elde edilen malvarlığı değerleri kripto varlık olarak tutulduğunda, yukarıda belirtildiği gibi bu varlıklar ile gerçek ve/veya sanal mal ve hizmetler alınabilir, takas merkezlerinde fiat paralara çevrilebilir. Bu şekilde suçtan elde edilen malvarlığı değerlerinin finans sistemine yasal işlemlerle sokulması mümkün hale gelir.[45] *Bütünleştirme aşamasında, fiat para birimi elde etmek için kripto varlıklardan temizlenmiş fonları çekmek için çeşitli seçenekler bulunur. Gizlilik varlıklarının birincil varlıklarla ve nihayetinde fiat para birimiyle takas edilmesi ya da kripto varlıkların fiziksel olarak istenen herhangi bir yere taşınmak üzere bir*

[40] Şirinleme, suç gelirlerini aklayan birincil kişi adına ve onun yararına işlem yapmak için birkaç kişinin kullanılması yöntemidir. İlerleyen sayfalarda şirinleme yöntemine ilişkin ayrıntılı açıklamalara yer verilmiştir.
[41] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.
[42] **Campbell-Verduyn/Goguen**, s. 80; **Durdu**, s. 189.
[43] **Dülger/Özkan**, s. 989.
[44] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.
[45] **Durdu**, s. 190; **Dülger/Özkan**, s. 989.

donanımsal kripto cüzdanına aktarılması seçeneği vardır.[46] *Böylelikle kripto varlıklar suç gelirlerinin aklanmasının her üç aşamasında hizmet görüşmüş olurlar.*

Suçlular, özellikle bilişim suçlarından elde ettikleri suç gelirlerini, bu konu özelinde ise kripto varlıkları aklamak için güvenli bir nakit çıkış stratejisine ihtiyaç duyarlar. Bilişim suçu işlemiş ve elde ettiği gelirleri aklamak isteyen bir kişi, nakit çıkışına nadiren kripto varlık ile başlar. Bu tür gelirler genellikle avro veya dolar gibi fiat para birimlerinden oluşur. Bilişim suçlarının gelirlerinin kaynağı, niteliği ve büyüklüğü ne olursa olsun, kripto varlık ekosistemi nakit çıkış stratejisinin gerektirdiği anonimleştirme veya katmanlama sürecinin bir parçası olarak kullanılır. Bu gelirlerin kripto varlıklar özellikle de Bitcoin ile takas edilmesiyle birlikte, paranın izi silinmiş olur.[47]

Kripto varlıkların aklanması için kullanılabilecek çeşitli yöntemler kapsamlı ve genellikle karmaşıktır ve özellikle katmanlama süreci AML/CFT yetkilileri için önemli zorluklar teşkil etmektedir. Buna rağmen, bu denetimsel engellerin üstesinden gelmeyi amaçlayan araçlar sürekli olarak geliştirilmektedir.[48]

2. Yöntemler

Suçlular kripto varlıkları kullanarak aklama faaliyetine giriştiklerinde genellikle kripto varlık tamburları (tumbler), karıştırma hizmetleri (mixer), eşler arası ağlar (P2P), OTC brokerleri ve DeFi platformlarının istismarı gibi çeşitli yöntemler kullanmaktadırlar. Yaklaşımları farklı olsa da bu yöntemlerin hepsi aynı amaca, suç gelirlerinin asıl kaynağını gizleyerek kolluk kuvvetlerinin izini sürmesini zorlaştırmaya hizmet etmektedirler. Örneğin, kripto varlık karıştırıcıları ve karıştırma hizmetleri, büyük miktarlardaki kripto varlığı daha küçük, takip edilemez miktarlara ayırırlar. Benzer şekilde, eşler arası ağlar ve OTC brokerleri anonim işlemler için bir platform sağlayarak izleme sürecini daha da karmaşık hale getirirler. Son olarak DeFi platformlarının istismarı, kripto sektöründeki düzenleme ve gözetim eksikliğinden yararlanarak suçluların karmaşık işlem ağları aracılığıyla fonları hareket ettirmesine olanak tanır. Bu yöntemlerin her biri kolluk kuvvetleri için zorluklar oluşturur ve kripto varlıkların aklanması ile mücadele için gelişmiş araç ve tekniklerin sürekli olarak geliştirilmesi ihtiyacını ortaya çıkarır.[49]

---

[46] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.
[47] **n van Wegberg/Oerlemans/van Deventer**, s. 420.
[48] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.
[49] **Financial Crime Academy**, "Understanding Crypto Money Laundering Methods: The Cryptocurrency Crime", (Çevrimiçi) https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/#:~:text=What% 20are%20the%20methods%20of,decentralized%20finance%20(DeFi)%20platforms. (set) 10.06.2024.

Kripto Varlık Tamburları ve Karıştırma Hizmetleri

Kripto varlık tamburları ve karıştırma hizmetleri,[50] birçok aklama işleminde merkezi bir rol oynamaktadır. Bu hizmetler, suçluların suç gelirlerini daha küçük miktarlara bölerek ve bir dizi işlemden geçirdikten sonra yeniden birleştirerek kaynağını gizlemelerine yardımcı olur. Bu işlemlerin sonucunda asıl kaynağına kadar izlenmesi zor olan bir dizi fon ortaya çıkar ve bu da kolluk kuvvetlerinin suç faillerini tespit etmesini ve kovuşturmasını zorlaştırır. Tamburlama (tumbler) ve karıştırma (mixer) hizmetlerinin kullanımı suç gelirlerinin aklanması ile sınırlı değildir, bunlar uyuşturucu kaçakçılığı ve bilişim suçları gibi diğer suç faaliyetlerini kolaylaştırmak için de kullanılabilir.[51]

İlk nesil kripto varlık karıştırıcıları, karıştırma için merkezi bir hizmet olarak çalışmıştır. Bunlar kripto varlıkları karıştırmanın en eski ve en ilkel hizmetleriydi. Bu tür hizmetler aracılığıyla anonimleştirmenin başarısı, kullanıcı sayısı ve kripto varlık miktarına bağlıdır. Bu nedenle bu tür özel hizmetler çok popüler değildir. Benzer amaçlar için kripto varlık aracı kurumları ve diğer ticaret platformları daha sık kullanılmaktadır. Karıştırıcı yeterince büyükse sonuçta yatırılan fonlar kesinlikle diğer kripto varlıklara dönüşür ve hatta bunları satmak ve almak zorunlu değildir. Böylece, komisyon olmadan kripto varlıklar etkili bir şekilde karışır. Ancak böyle bir hizmetin güvenilir olması gerekir. Karıştırma hizmetini verenler kripto varlıkları kendileri sahiplenmemeli, ayrıca bu varlıklar dıştan gelecek hırsızlıklardan ve sistem kırılmalarından korunmalıdır. Bunların yanı sıra hizmetin karıştırma işlemlerinin raporlarını kaydetmediğine, bu tür kayıtları satmayacağına veya kimseyle paylaşmayacağına tam olarak güvenilmesi gerekir. Karıştırıcı hizmeti verenler, kripto varlıkların sahibine geri dönüşünü garanti etse bile yukarıda listelenenlerin hepsini birden sağlamak ve kaygıları gidermek oldukça zordur.[52]

Yine de bu yöntemin oldukça etkili olduğunu belirtmek gerekir. Nitekim *Helix* adlı tambur uygulamasının yaklaşık 300 milyon Dolar değerindeki Bitcoin'i birbirinden ayrılmaz şekilde karıştırdığı ve böylelikle suç gelirlerinin aklanmasını kolaylaştırdığı ifade edilmektedir.[53] Ancak FATF'nin 15 no.lu Tavsiyesi gereğince ülkelerin bu tür hizmet sağlayıcılar için çeşitli yükümlülükler getirmesi, anonimlik perdesinin aralanması için çeşitli önlemler alınması ve bazı şirketlerin geliştirdikleri yazılımlarla açık kaynak blokları takip ederek arkasındaki gerçek kişilere ulaşma imkanının

[50] Karıştırma hizmetleri hakkında deneysel ve ampirik bir çalışma için bkz. **Malte Möser/Rainer Böhme**, "Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques", 2017 IEEE European Symposium on Security and Privacy: Workshops (EuroS&PW), 2017, s. 32-41; ayrıca bkz. **van Wegberg/Oerlemans/van Deventer**, s. 420 vd.

[51] **Financial Crime Academy**, Crypto Money Laundering.

[52] **Sat/Krylov/Bezverbnyi/Kasatkin/Kornev**, s. 246; **Prendi/Borakaj/Prendi**, s. 85.

[53] **Zeynep Esra Tarakçıoğlu**, "Kripto Varlıkları ve Ceza Hukuku Sorumluluğu", Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, C. 11, S. 2, Aralık 2021, s. 342.

sağlanması nedeniyle doğrudan değişim platformlarında kullanılan suç fonlarının küresel ortalamasının 2019 yılında % 47 oranında azaldığı ifade edilmektedir.[54]

Eşler Arası Ağlar, OTC Brokerları ve Off-Chain Kanalları
Eşler arası ağlar ve OTC[55] brokerleri ise suçluların kripto varlıklar aracılığıyla suç gelirlerini aklamaları için başka bir yol sunarlar. Bu platformlar kullanıcıların kimliklerini belirtmeden kripto varlık ticareti yapabilmelerini sağlayarak suçluların görece anonim bir şekilde faaliyet gösterebilecekleri bir ortam sunmaktadırlar. Suçlular bu platformları kullanarak, tespit edilmelerini sağlayacak herhangi bir iz bırakmadan suç gelirlerini aklayabilirler.

Bu sorunu ele almak için düzenleyici kurumlar, eşler arası ağların ve OTC brokerlerinin sıkı KYC/AML[56] politikaları uygulamalarını sağlamak için gerekli önlemleri almalıdır. FATF'nin rehberleri bu önlemlerin neler olduğunu açıklamaktadır. Nitekim devletler ve finans kuruluşları kripto varlıklar ile ilgili suç faaliyetleriyle mücadele etmek için bir dizi adım atmışlardır. Bu adımlar arasında suç gelirlerinin aklanmasını ve terörizmin finansmanını durdurmaya çalışan aklama karşıtı (AML) düzenlemelerin yanı sıra finans kuruluşlarının müşterilerinin kimliğini teyit etmeye zorlayan "müşterini tanı" (KYC) standartları da yer almaktadır.[57] 5549 sayılı Kanun'un 3.maddesine göre yükümlüler, kendileri nezdinde yapılan veya aracılık ettikleri işlemlerde öncelikle, işlemi yapan kişi ile nam ve hesabına işlem yapılan kişinin kimlik bilgilerini tespit etmeli ve gerekli önlemleri almalıdır.[58] Bu önlemler alınarak söz konusu platformlar suç gelirlerinin aklanması ve diğer yasa dışı faaliyetlerin önlenmesine yardımcı olabilir ve aynı zamanda kullanıcılarını potansiyel risklerden koruyabilirler. Ayrıca, kolluk kuvvetleri bu platformların işletmecileri ile iş birliği yaparak bilgi ve kaynak paylaşımında bulunmalı, böylece suç faaliyetlerinin tespit edilmesi ve engellenmesi kolaylaştırılmalıdır.[59]

Off-chain kanallarında (örn. Lightning, Network, Raiden, Plasma vb.) ise açılan bir ödeme kanalı aracılığıyla işlem yapılması ve bu işlemlerin blok zincirde yayınlanmasına gerek kalmadan sürdürülmesi sağlanmaktadır.[60]

Merkezi Olmayan Finans (DeFi) Platformlarından Yararlanma
Merkezi Olmayan Finans (DeFi) platformları, bir dizi yenilikçi finansal

[54] **Cipher Trace**, Cryptocurrency Crime and Anti Money Laundering Report, 2020, 7.
[55] OTC (Over-The-Counter) veya Türkçe olarak tezgâh üstü piyasalar, borsa dışı piyasalardır. BİST, Nasdaq veya NYSE gibi organize piyasalar değillerdir. Daha gevşek kurallara ve denetimlere sahiptir. Bu piyasada alıcılar ve satıcılar herhangi bir aracı olmadan direkt olarak alım satım işlemlerini gerçekleştirirler.
[56] Know Your Customer/Anti Money Laundering = Müşterini Tanı/Suç Gelirlerinin Aklanmasıyla Mücadele.
[57] **Prendi/Borakaj/Prendi**, s. 85.
[58] **Balcı/Çakır**, s. 327.
[59] **Financial Crime Academy**, Crypto Money Laundering.
[60] **Buttigieg/Efthymiopoulos/ Attard/ Cuyle**, s. 213.

ürün ve hizmet sunarak kripto alanında yeni bir fırsat olarak ortaya çıkarmıştır. Ancak DeFi sektöründeki düzenleme ve gözetim eksikliği, bu sektörü suç gelirlerini aklamak isteyenler için cazip hale getirmiştir. Suçlular, bu platformların sunduğu anonimlik ve merkeziyetsizlikten yararlanarak, suç gelirlerini karmaşık işlem ağları aracılığıyla taşıyabilir ve kolluk kuvvetlerinin bunların kaynağını izlemesini zorlaştırabilir. DeFi platformlarının aklama amacıyla kullanılmasıyla mücadele etmek için düzenleyici kurumlar, uygun düzenlemeler ve gözetim mekanizmaları geliştirmeli ve uygulamalı, DeFi platformlarının şeffaf ve güvenli bir şekilde çalışması sağlanmalı ve kullanıcıları suç gelirlerini aklama ve diğer yasa dışı faaliyetlerle ilişkili potansiyel risklerden korumalıdır.[61]

3. Yöntemlerin Suç İşlenmesindeki Rolü

Bu yöntemlerin aklayıcılara temel olarak iki önemli avantaj sağladığı görülür. Bunlar AML rejiminin merkezinde yer alan bankalar gibi güvenilir aracı kurumların atlatılması ve kullanıcılara yarı anonimlik sağlanmasıdır. Suç gelirlerinin aklanmasında geliri elde edenin ve işlemi yapanın anonim kalması son derece önemlidir. Böylelikle gelirin kaynağı olan suçla ilişkisinin kesilmesi, faillerin tespit edilmesi ve suç gelirlerine el konulması riskleri ortadan kalkmış olur. İşte bu noktada kripto varlıkların sağladığı yarı anonimlik aklayıcılara büyük bir fırsat sağlamaktadır. Bu fırsatlar kripto varlıklarla suç gelirlerinin aklanmasını oldukça kolay bir hale getirmektedir.[62] Blok zincir teknolojisi yarı anonimdir, zira blok zincir ile yapılan her işlem bu işlemin yer aldığı tüm bilgisayarlarda görülebilir ve işlem zinciri baştan sona izlenebilir. Bu anlamda tamamen şeffaftır. Öte yandan işlemleri yapanlar yalnızca sayılar ve takma adlardır, merkezi bir kuruluş tarafından kayıt tutulmadığı için kişilerin gerçek kimliğini belirlemeye gerek ve olanak yoktur, güvenliği sağlayan her bir bilgisayarda tutulan işleme ilişkin aynı kayıttır yani bizatihi işlemin kendisidir. Bu yönüyle de blok zincir teknolojisi anonimdir. İşte bu ikisinin bir araya gelmesi sonucunda yarı anonim bir durum ortaya çıkmaktadır. Bu yarı anonimlik gizli kalarak finansal işlem yapmak isteyenlere güzel fırsatlar sunmaktadır. Tabi bu güzel fırsatlar, suçla mücadele edenler açısından çeşitli zorluklar anlamına gelmektedir.

Bunun sonucu olarak, dünya çapında yaygın olarak kullanılabilen ancak merkezi bir yapısı ve düzenleyicisi olmayan ağlarda kullanıcılar arasında doğrudan işlem yapılmasına olanak tanıyan blok zincir teknolojisi uluslararası AML rejiminin merkezinde yer alan bankalar gibi güvenilir üçüncü tarafları saf dışı bırakmakta ve bunlar üzerinden uygulanan AML rejimini atlatmaya yardımcı olmaktadır. Geleneksel merkezi kurumlarda fon alışverişini doğrulamak ve denetlemek için bankalar gibi finans

[61] **Financial Crime Academy**, Crypto Money Laundering.

[62] **van Wegberg/Oerlemans/van Deventer**, s. 432.

kuruluşlarına güvenilirken, kripto varlıklarla yapılan işlemlerde hem karmaşık algoritmalara hem de alışverişlerin geçerliliğini sürekli olarak doğrulayan merkezi olmayan kullanıcı ağlarına güvenilir. Böylelikle kripto varlıklar, kullanıcıların geleneksel güvenilir üçüncü taraflar araya girmeden doğrudan kendi aralarında (P2P = peer to peer = eşler arası) fon transferi yapmalarını sağlar. Fon transferi ya da dönüşümü işlemlerine üçüncü bir kişi girmediği için bu kişi üzerinden kontrol yapılması imkânsız hale gelir. Zira KYC/AML rejiminin yöneldiği ve etkisini gösterdiği en önemli yapı araya giren finans kuruluşlardır. Bunlar aradan çıkarıldığında KYC/AML rejiminin uygulanması neredeyse imkânsız hale gelir. Bu işlemlerin uluslararası AML gerekliliklerini karşılamasını sağlamak için gözetim sağlayacak merkezi kurumlar olmadığından, kripto varlık gibi blok zinciri uygulamalarının *"son 25 yılda geliştirilen çok sayıda kara para aklama karşıtı düzenlemeden düzgün bir şekilde sıyrıldığı"*[63] *ifade edilmektedir.*[64]

Blok zincir teknolojisinin uluslararası AML rejimi üzerinde etki yaratan bir diğer özelliği, yukarıda da bahsetmiş olduğumuz gibi kullanıcılara sağlanan yarı-anonimliktir. Şeffaflık ve anonimlik arzusu arasındaki çatışma, dijital teknolojilerin genel olarak karşı karşıya kaldığı temel bir sorundur ve özellikle blok zincir uygulamalarında kendini göstermektedir. Blok zinciri, kripto varlıkların oluşturulduğu, transfer edildiği ya da saklandığı dijital sicildir. Kripto varlıklar blok zinciri sistemi ile kriptografiyi kullanırlar.[65] *Kullanıcı adreslerine dayalı olarak gerçek dünyadaki bireylerin kimliklerinin tespit edilmesi, blok zincirin temelini oluşturan kriptografik yöntemlerin karmaşıklığı nedeniyle zordur ancak imkânsız değildir. Bu yarı anonimlik nedeniyle finans kuruluşlarının çalışanları için tam olarak kime soru sorulacağını belirlemek zorlaşmaktadır. Bununla bağlantılı olarak, finansçılar ve sektör düzenleyiciler için kripto varlık işlemlerinin hangisinin "atipik" hangisinin "normal" olduğu hakkında bir anlayış geliştirmeleri gerekir. Bu bağlamda şüpheli bir Bitcoin transferinin tam olarak neye benzediğinin finansçılar ve düzenleyici kurumlar tarafından bilinmesi gerekir. Başka bir deyişle, şüpheli blok zincir tabanlı kripto varlık işlemlerinin tipik kullanımlarına ilişkin standart bir referansın belirlenmesi gerekir.*[66]

Sonuç olarak blok zincir teknolojisinin merkezi olmayan yapısı ve yarı anonimlik sağlama özelliği birlikte ele alındığında bu özelliklerin uluslararası AML/CFT rejimi için önemli sonuçları olmaktadır. Kripto varlıklar gibi blok zincir tabanlı işlemler, fon transferi gerçekleştirmek için "ortak güven ve geçiş noktası" olarak klasik bankalara ve finansal

[63] **Robert Stokes**, "Anti-money Laundering Regulation and Emerging Payment Technologies", in: Banking and Financial Services Policy Report, Vol. 32, Issue. 5, 2013, s. 3.
[64] **Campbell-Verduyn/Goguen**, s. 74.
[65] **Akbulut**, s. 489.
[66] **Stokes**, s. 5; **Campbell-Verduyn/Goguen**, s. 74.

kurumlara güvenmez ve bunları kullanmaz. Bunun yerine eşler arası doğrudan işlem sağlar ve teknoloji bu güveni sağlama üzerine kuruludur. Bu nedenle, blok zincir tabanlı işlemlerde yer alan tarafları belirleme yeteneği önemli ölçüde azdır.[67]

Kripto Varlıkların Suç Gelirlerinin Aklanmasında Kullanılma Potansiyeli ve Buna İlişkin Çarpıcı Örnekler

Kripto varlıkların ortaya çıkmasıyla birlikte, finans alanında yatırım için yeni olanaklar da ortaya çıkmıştır. Ancak bu gelişme aynı zamanda suçluların bu dijital ortam ve kripto varlıklar aracılığıyla suç gelirlerini aklamaları için yeni fırsatlar da ortaya çıkarmıştır. Kripto varlıkların kötüye kullanımının tam ölçeği bilinemese de, dolaşımda olan tüm kripto varlık birimlerinin piyasa değeri 2020'de dünya çapında 250 milyar doları aşmış ve 2022'de yaklaşık 1,94 trilyon dolara ulaşmıştır.[68] Bununla birlikte tahminlere göre 2022 yılında 23,8 milyar dolar değerindeki kripto varlık yasa dışı faaliyetlerde kullanılmıştır ve bu meblağ gittikçe büyümektedir.[69] Ayrıca kripto varlık sektöründeki gelirin 2023 yılında yaklaşık 42 milyar dolara ulaştığı ve 2027 yılına kadar yıllık %14,36'lık bir büyüme oranı göstermesinin beklendiği, kullanıcı penetrasyonunun ise 2023'te %3,8 olacağı ve 2027'ye kadar bu oranın %4,4'e ulaşmasının beklendiği ifade edilmektedir.[70] Görüldüğü üzere meblağlar oldukça yüksektir ve gün geçtikçe ivmelenerek artmaktadır.

Yasa dışı kullanıcıların kripto varlık adreslerinin yaklaşık %39,31'ini kontrol ettiği ve kripto varlık işlemlerinin dolar hacminin yaklaşık beşte birini (%23,06) oluşturduğu tahmin edilmektedir. Dolar bazında, yasa dışı kullanıcıların yaklaşık 429 milyar dolar değerinde kripto varlık işlemi gerçekleştirdiği iddia edilmektedir. Yasa dışı kullanıcılar dolar hacmindeki paylarından daha büyük bir işlem payına sahip olduklarından, yasal kullanıcılara göre daha küçük miktarlı işlemler yapma eğilimindedirler. Bu sonuç, yasa dışı kullanıcıların kripto varlıkları bir yatırım veya spekülatif varlık olarak tutmak yerine öncelikle bir ödeme sistemi olarak dolayısıyla suç işlenmesinde ödeme aracı ya da suç gelirlerinin aklanmasında kullanıldığı iddiasıyla tutarlıdır.[71]

Daha önce de değinildiği üzere kripto varlıkların suç gelirlerinin aklanmasında kullanılma potansiyeline ilişkin en önemli ve gerçek örnek, "dark net"te hizmet veren, alışverişlerde yalnızca Bitcoin kabul eden ve yaratıcısı Ross Ulbricht'in suç gelirlerini aklama ve işlediği diğer suçlardan dolayı ömür boyu hapis cezasına çarptırıldığı Silk Road adlı çevrimiçi pazar

[67] **Campbell-Verduyn/Goguen**, s. 75.
[68] **Keech**, s. 48.
[69] **Financial Crime Academy**, Crypto Money Laundering.
[70] **Prendi/Borakaj/Prendi**, s. 85.
[71] **Foley/Karlsen/Putnins**, s. 24.

yeridir.[72] Silk Road özellikle Bitcoin'in suçluların yakalanmasını önleyecek şekilde yasa dışı işlerde kullanılmasının en bariz ve bilinen örneği olmuştur. Bir başka kripto varlıkla aklamanın gerçekleştirildiği yöntem ve ortaya çıkarılan olay ise suç gelirlerini aklayan birincil kişi adına ve onun yararına işlem yapmak için birkaç kişinin kullanılmasıdır. Buna "şirinleme (smurfing)" denilmektedir. Şirinlemenin arkasındaki mantık, farklı yerlerde küçük işlemler yapan birkaç kişinin, önemli miktarda para için tek bir işlem yapan bir kişiden çok daha az şüphe ve dikkat çekmesidir. Şirinleme, suç gelirlerinin aklanmasında eski bir yöntemdir, ancak kripto varlıkların dünya çapında taşınabilmesinin kolaylığı ve hızı nedeniyle küresel bir sorun haline gelmiştir. Bu tür bir yöntem Europol, İspanyol Sivil Muhafızları (Guardia Civil / İspanyol Jandarması), Finlandiya kolluk güçleri ve ABD İç Güvenlik Bakanlığı iş birliği ile yürütülen ortak bir soruşturma sonucunda ortaya çıkarılmıştır. Soruşturma sonucunda 11 kişinin tutuklanması ve 8 milyon avroya el konulmasıyla sonuçlanan karmaşık bir küresel şirinleme planı tespit edilmiştir. Bu yöntem başlangıçta İspanya'da bulunan ve yasa dışı uyuşturucu kaçakçılığından elde edilen gelirleri toplamak ve 174 farklı banka hesabına bölmekle görevlendirilen suçlularla başlamıştır. Suçlular daha sonra Kolombiya'ya gitmiş ve hesaplara bağlı banka kartlarını kullanarak hesaplardaki parayı çekmişlerdir. Ancak suçlular eylemlerinin işlem geçmişlerinden kolayca takip edilebileceğini fark ettiklerinde, plan nakit yerine Bitcoin ve diğer kripto para birimlerinin aklama işlemlerinde kullanılması şeklinde değiştirilmiştir. Suçlular nakit parayı bizzat çekmek yerine, suç gelirlerinin yatırıldığı hesaplar aracılığıyla "yasa dışı gelirlerini kripto varlıklara dönüştürmek için aracı kurumları kullanmışlar, ardından kripto para birimini Kolombiya pesosuna çevirip aynı gün Kolombiya banka hesaplarına yatırmışlardır". Yetkililer kripto varlık aracı kurumunun nerede olduğunu keşfettikten ve aracı kurumun şüpheliler hakkında sahip olduğu tüm kişisel kimlik bilgilerini topladıktan sonra plan çözülmüştür.[73] Bazı araştırmalarda, ABD arama motoru verileri analiz edilerek kripto

[72] Silk Road, 2010'ların başlarında etkin olmuş, yasa dışı madde satışı ile tanınan online karaborsa ve darknet marketiydi. Darknet piyasasının ortaya çıkmasını sağlamıştır. Deep web'de yer alan market, Tor ağı üzerinde ".onion" uzantısı ile hizmet vermiş, bu sayede kullanıcıların siteye anonim ve güvenli bir biçimde ulaşımını sağlamıştır. 2011 Şubat ayında kurulmuş sitenin geliştirilmesine bundan 6 ay önce başlanmıştır. Etkin olduğu dönem boyunca 100.000'i aşkın müşteri sitede yer alan ürünleri satın almıştır. Ekim 2013'te FBI siteyi ele geçirmiş ve kapatmış, Ross Ulbricht'i ise sitenin kurucusu olan "Dread Pirate Roberts" olduğu suçlamasıyla tutuklamıştır. Takip eden ayda Silk Road 2.0 adlı bir site kurulmuş, ancak bu site de 2014 Kasım ayında Onymous Operasyonu adlı operasyon sonucunda kapatılmış ve admini tutuklanmıştır. 2016'da Silk Road 3.0 kurulmuş ancak diğer sitelerin rekabeti nedeniyle eski popülerliğine ulaşamamıştır. Ulbricht site ile ilişkisinden ötürü şartlı tahliye hakkı olmaksızın müebbet hapse mahkûm edilmiştir. Kasım 2020'de ABD hükümeti Silk Road ile ilişkili 1 milyar ABD doları değerinde bitcoin ele geçirmiş olduklarını açıklamıştır. (Çevrimiçi) https://tr.wikipedia.org/wiki/Silk_Road, (set) 04.07.2024.

[73] Europol, "Illegal Network Used Cryptocurrencıes and Credit Cards to Launder more than Eur 8 Million from Drug Trafficking", 9 Nisan 2018, (Çevrimiçi) https://www.europol.europa.eu/media-press/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking, (set) 11.07.2024.

varlıkların kullanılmasıyla yasa dışı faaliyetler arasında bir korelasyonun bulunduğu tespit edilmiştir.[74] Ancak bu örneklerin dışında blok zinciri uygulamalarını gerçek aklama operasyonlarıyla doğrudan ilişkilendiren çok fazla kanıt bulunmamaktadır. Örneğin 2015 tarihli İngiliz Ulusal Risk Değerlendirme Raporu'nda, *"dijital para birimlerinin suç gelirlerinin aklanması için kullanıldığına dair somut sonuçlara varılabilecek sınırlı sayıda vaka çalışması olduğu"* ve *"dijital para birimleriyle ilişkili suç geliri aklama riskinin düşük olduğu"* sonucuna varılmıştır.[75]

Medyanın sansasyonel haberlerine rağmen, kripto varlıkların terörün finansmanında kullanıldığını gösteren çok az kanıt vardır. Paris'te Kasım 2015 tarihinde gerçekleşen terör saldırılarının faillerinin kripto varlıkları kullandığına dair iddiaların asılsız olduğu ortaya çıkmıştır. Teorik olarak kripto varlıkların suç gelirlerinin aklanması ve terörizmin finansmanında kullanılması riski söz konusu olsa da kripto varlıkların bu tür amaçlar için kullanıldığı henüz somut olarak gösterilememiştir.

Kripto varlık güvenlik firması CipherTrace tarafından hazırlanan 2018 tarihli suç gelirlerinin aklanmasına ilişkin rapora göre, internette kripto varlık birimleri aracılığıyla kumar oynamaya izin veren 100 ile 200 arasında kumar sitesi bulunmaktadır.[76] Tıpkı normal bir kumarhanede olduğu gibi, fonlar bahis amacıyla çevrimiçi bir kumarhaneye aktarılabilir, ancak muhtemelen minimum sayıda bahis oynanmadan veya minimum miktarda para harcanmadan da çekilebilir. Rapora göre, çevrimiçi kumarhaneler aracılığıyla suç gelirlerinin aklanmasının izlenmesindeki temel zorluk, bu kumar sitelerinde "Müşterini Tanı" (KYC) düzenlemesinin çok az olması veya hiç olmaması nedeniyle, kolluk kuvvetlerinin bu kumar sitelerinden yapılan transferler hakkında bilgi edinmesinin zor olmasıdır.[77] Kripto varlıkla kumar oynatan siteler hakkında basit bir internet araması yapılması halinde dahi özellikle "https://bitcoinplay.net" sitesinin kumar oynamak için kullanılabilecek farklı sitelerin reklamını yaptığı görülmektedir. Dahası, bu web sitesi anonimliği teşvik etmekte ve potansiyel olarak web sitelerinin suç gelirlerini para aklama faaliyeti için istismar edilmesine izin vermektedir.[78] Ancak görüldüğü üzere bu raporda da kripto varlıkların "potansiyel olarak" suç işlenmesinde kullanılmasından bahsedilmekte ancak doğal olarak buna ilişkin sayısal bir veriye yer verilmemektedir.

---

[74] **Aaron Yelowitz/Matthew Wilson**, "Characteristics of Bitcoin Users: An Analysis of Google Search Data", Applied Economics Letters, Vol. 22, Issue 13, 2015, s. 1-7.

[75] Bkz. HM Treasury and Home Office, UK National Risk Assessment of Money Laundering and Terrorist Financing, 15 Ekim 2015, (Çevrimiçi) https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing, (set) 05.07.2024.

[76] Cryptocurrency Anti-Money Laundering Report, 2018, (Çevrimiçi) https://info.ciphertrace.com/crypto-aml-report-q218, (set) 11.07.2024.

[77] Cryptocurrency Anti-Money Laundering Report, 2018, s. 9.

[78] **Forgang**, s. 15, 16.

Çevrimiçi aklama tarihindeki en büyük vakalardan birisi ise "Liberty Reserve" olayıdır. Mayıs 2013'te ABD Adalet Bakanlığı Kosta Rika'da faaliyet gösteren "Liberty Reserve" şirketinin yedi yöneticisi ile çalışanına karşı çeşitli suçlamalarda bulunmuştur. Söz konusu kişiler, para transferi hizmetleri sağlayarak kayıt dışı ticari faaliyette bulunmak ve 6 milyar ABD dolarını aşan yasa dışı gelirin işleme alınmasına yardım ederek kara para aklamakla suçlanmışlardır. Yapılan açıklamalara göre bu sistem devasa boyutlarda işlemekteydi. Sistemin ABD'deki 200.000 kullanıcısı da dahil olmak üzere tüm dünyada milyonlarca kullanıcısı bulunmaktaydı. Bu sistem içinde yaklaşık 55 milyon işlem gerçekleştirilmiştir ve neredeyse bunların tamamı yasa dışıdır. Sistemin içinde kendi sanal para birimi olan "Liberty Dollars" kullanılmıştır. Ancak işlemin başlangıç ve bitiş noktalarında para dönüştürülmüş ve sabit para biriminde (USD) çevrilmiştir. İyi koordine edilmiş eylemlerin bir sonucu olarak, ABD Maliye Bakanlığı "Liberty Reserve"i suç gelirlerinin aklanması açısından endişe uyandıran finansal kuruluş olarak belirlemiş ve ABD Terörle Mücadele Yasası'nın (Vatanseverlik Yasası) 311. Bölümü gereğince ABD'nin finansal sistemine erişimini tamamen engellemiştir.[79] Görüldüğü üzere burada da belli bir sistem içinde geçerliliği olan bir kripto varlık kullanılmıştır.

Bu konuda bilinen bir diğer güncel gelişme ise Europol'un ilk olarak 12 Ocak 2021'de yayınladığı sonra aynı yılın 18 Kasım'ında güncellendiği bir basın bülteninde, dark web'de o tarihte dünyanın en büyük yasa dışı pazar yeri olan DarkMarket'i çevrimdışı hale getirdiğini duyurmasıdır. Yapılan açıklamada DarkMarket'in 500.000 kullanıcısı, 2.400 satıcısı ve 4.650 Bitcoin ve 12.800 Moneros tutarında 320.000 ödenmemiş işlemin olduğu, toplamda o zamanki kurlarla bunun 140 milyon Avro'dan fazla bir tutara denk geldiği ifade edilmiştir. Europol aynı basın açıklamasında bu olgunun ulaştığı boyutun açık bir işareti olarak dark web'de işlenen suçlarla mücadele için koordineli bir kolluk kuvveti yaklaşımı oluşturmanın gerekliliğini de ifade etmiştir.[80] Bunun kripto varlıklarla işlenen suçlara ilişkin tahminlerle karşılaştırıldığında önemli bir miktar olmadığı ancak bireysel olarak ele geçirilen miktarların sıralamasında muhtemelen önemli bir miktar olduğu ifade edilmektedir.[81] Dolayısıyla söz konusu yasa dışı pazar yerleri ya da bir başka deyişle yeraltı piyasaları, kripto varlık birimlerinin mevcut ve gelecekteki suç gelirlerini aklama planlarında kullanılmasını kolaylaştırıcı bir unsur olarak görülebilir.[82]

---

[79] **Valeriia Dyntu/Oleh Dykyi**, "Cryptocurrency in the System of Money Laundering", Baltic Journal of Economic Studies, Vol. 4, No. 5, 2018, s. 79.

[80] (Çevrimiçi) https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down (set) 18.07.2024.

[81] **Michele Manna**, The Bonfire of Banknotes, Mercati, Infrastrutture, Sistemi di Pagamento (Markets, Infrastructures, Payment Systems) Approfondimenti (Research Papers), No. 25 Banca d'Italia, Rome, 2022, s. 20.

[82] **van Wegberg/Oerlemans/van Deventer**, s. 421.

Bu konudaki en güncel gelişme ise ABD'de gerçekleşmiştir. Darknet'te kripto varlık mikseri hizmeti vererek 2011 tarihinden beri 400 milyon dolar akladığı iddiasıyla yargılanan Roman Sterlingov isimli Rus-İsveç çifte vatandaşı olan bir kişi, Washington'da federal bir jüri tarafından darknet üzerinden uzun süredir devam eden aklama hizmetini yürüttüğü için mahkûm edilmiştir. Roman Sterlingov, suçluların darknet pazar yerlerinden yüz milyonlarca dolarlık yasa dışı fonları aklamasına olanak tanıyan bir kripto para birimi "karıştırma" hizmeti olan Bitcoin Fog'u işletiyordu. Sanık ve müşterileri bu yasa dışı işlemleri gizlemek için Bitcoin Fog'u kullanıyorlardı. Başsavcı Yardımcısı Lisa Monaco yaptığı açıklamada *"...yakalanmadan yüz milyonlarca dolar bitcoin aklamak için internetin gölgelerini kullanabileceğini düşündü ama yanıldı; ajanlar, analistler ve savcılardan oluşan ekibimiz, Sterlingov ve Bitcoin Fog girişiminden hesap sormak için blok zinciri üzerinden bitcoin'i titizlikle takip ederek adalet arayışlarında acımasız davrandılar. Bugün jüri tüm suçlamalarla ilgili olarak suçlu kararı verdi - bu da nerede faaliyet gösterirseniz gösterin, kripto para hizmetiniz ABD'ye ulaşıyorsa, ABD yasalarına uymanız gerektiğini gösteriyor."* demiştir. FBI Direktör Yardımcısı Paul Abbate ise *"FBI'ın siber işgücü, yasa dışı faaliyetleri yürütmek ve kolaylaştırmak için teknolojiden yararlanan suçluların peşini bırakmıyor, bu mahkûmiyet kararı, FBI ile federal ve uluslararası ortaklarımız arasındaki yakın iş birliğinin bir sonucudur ve Bitcoin Fog ve operatörüne kara para aklama faaliyetlerinden dolayı cezai yaptırım uygulanmasını sağlamıştır. FBI, nerede faaliyet gösterirlerse göstersinler, siber suçlulara bedel ödetmek için mevcut tüm araçları ve kaynakları kullanmaya devam edecektir."* şeklinde açıklamada bulunmuştur. Mahkeme belgelerine ve duruşmada sunulan kanıtlara göre, 35 yaşındaki Roman Sterlingov, 2011'den 2021'e kadar Bitcoin Fog'un işletilmesinde yer almıştır. Bitcoin Fog, yasa dışı gelirlerini kolluk kuvvetlerinden gizlemek isteyen suçlular için bir suç gelirlerini aklama hizmeti olarak ün kazanan, en uzun süre faaliyet gösteren kripto para birimi karıştırıcısı olarak hizmet vermiştir. Bitcoin Fog, on yıl süren operasyonu boyunca, işlemler sırasında yaklaşık 400 milyon dolar değerinde olan 1,2 milyondan fazla Bitcoin işlemi yapmıştır. Bu kripto varlığın büyük bir kısmı darknet pazarlarından gelmiş ve yasa dışı narkotik, bilişim suçları, kimlik hırsızlığı ve çocuklara yönelik cinsel istismar materyalleriyle bağlantılı olduğu görülmüştür. Jüri, Sterlingov'u her biri azami yirmi yıl hapis cezası gerektiren "kara para aklama komplosu" ve "gizli kara para aklama suçlarından" ve her biri azami beş yıl hapis cezası gerektiren Columbia Bölgesi'nde ruhsatsız para aktarma işi yapmak ve ruhsatsız para aktarma suçlarından mahkûm etmiştir. Bu davanın ve öncesindeki soruşturmanın önemli bir özelliği de soruşturmanın kurumların ulusal ve uluslararası iş birliğiyle bu suçların ortaya çıkarılması ve failin cezalandırılabilmesidir. Bu soruşturmada AB'den IRS-CI District of Columbia Siber Suçlar Birimi ve FBI Washington Saha Ofisi birlikte asıl soruşturmayı yapmışlardır. ABD Adalet Bakanlığı'nın Uluslararası İlişkiler

Ofisi ve FBI'ın Sanal Varlık Birimi soruşturma ekiplerine yardım etmiştir. Europol, İsveç Ekonomik Suçlar Kurumu, İsveç Savcılık Kurumu ve İsveç Polis Kurumu ile Romanya Polisi Genel Müfettişliği, Organize Suçlarla Mücadele Müdürlüğü ve Organize Suç ve Terörizm Araştırma Müdürlüğü tarafından ek yardım sağlanmıştır.[83]

Buradan hareketle kripto varlıklar kullanılmak suretiyle yapılan aklama işlemlerine ilişkin tahminlerin somut bir kanıta dayanmadan, çeşitli öngörüler ve hesaplamalar kullanılarak yapıldığı rahatlıkla söylenebilir. Var olan örneklerin de geneli yansıtamayacak kadar az sayıda olduğu görülmektedir. Nitekim bazı hukukçular kripto varlıkların suç gelirlerinin aklanmasında kullanılmasının gerçek olmaktan çok algılanan fırsatlar olabileceği konusunda uyarıda bulunmuşlardır.[84] Benzer şekilde, pek çok teknoloji uzmanı kripto varlıkların suç gelirlerinin aklanması için kullanılma riskinin "şişirilmiş" olduğunu iddia etmektedirler. Bununla birlikte uluslararası AML rejimindeki kilit aktörler blok zincir teknolojilerinin suç gelirlerinin aklanması ve terörizmin finansmanını önlemeye yönelik çabalarını zora soktuğu görüşündedirler.[85]

Bizce kripto varlıkların suç gelirlerinin aklanmasına kullanılması yönelik önemli bir potansiyeli vardır. Ancak bu, potansiyelin gerçeğe dönüştüğü anlamına gelmemektedir. Yukarıda verdiğimiz örneklerin toplamı tüm aklanan gelirlerinin yanında nokta düzeyinde kalmaktadır. Bu nedenle kripto varlıklar için KYC uygulanmalı AML/CFT rejimi devreye alınmalı ancak bu teknolojinin ve kripto varlık ekosisteminin varlığı ve gelişimi sırf bu potansiyel nedenden dolayı engellenmemeli ve yok edilmemelidir. Ayrıca bu tür bir teknolojinin tamamen yasaklanması halinde bunun yer altına inebileceği gerçeği de unutulmamalıdır.

FATF'nin Düzenlemeleri

Dünyada suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadelede öne çıkan ve öncü rol üstlenen kuruluş FATF'dir. Bu nedenle FATF, çalışmaları ve bu alana özgü çıkarttığı rehberler ile tüm dünyada suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadele konusunda mevzuat yapıcı ve uygulayıcılar açısından yol göstericidir. FATF üstlendiği bu rol ve bundan aldığı güçle kripto varlıkların suç gelirlerinin aklanmasında ve terörizmin finansmanında kullanılmasına ilişkin çeşitli rehberler yayınlamıştır. FATF'nin bu rehberlerinden varılan sonuç, kuruluşun kendisinin de açıkça ifade ettiği üzere kripto varlıklara "risk temelli" yaklaşmaktır. Bu yaklaşım dünyada da yankı bulmuş ve sanki

[83] (Çevrimiçi) https://www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy, 14 Mart 2024, (set) 18.07.2024.

[84] **Steven David Brown**, "Cryptocurrency and Criminality: The Bitcoin Opportunity", The Police Journal, Vol. 89, Issue 4, 2016, s. 332; **Stokes**, s. 5.

[85] **Campbell-Verduyn/Goguen**, s. 75.

bu riskler gerçekleşmiş gibi bir algı oluşmuş bunun sonucunda da kripto varlıklar suç gelirlerinin aklanması ve terörizmin finansmanıyla birlikte anılır olmuştur. Ancak kripto varlıklar şu anda bu yasa dışı uygulamayla mücadeleye yönelik küresel çabalar için daha az tehdit ve daha çok fırsat sunmaktadır.[86] Risk temelli yaklaşım doğru olmakla birlikte yukarıda da ifade ettiğimiz üzere bu varlıkların "yalnızca suç işlemekte kullanıldığı" bir gerçeklik değildir. Dolayısıyla FATF'nin bu yaklaşımı gerçekleşmesi mümkün olan riskler olarak algılanmalı ve henüz risk gerçekleşmeden bunlara karşı önlemler alınmalıdır. Ancak bu durum kripto varlıkların ve hatta blok zincir teknolojisinin yasaklanmasına bir gerekçe oluşturmamalı, blok zincir teknolojisinin gelişiminin önü tıkanmamalıdır.

FATF, bu konuda ilk olarak Haziran 2014 tarihli raporunda[87] sanal para birimlerini ve barındırdığı riskleri tanımlama yönünde bir çalışmada bulunmuş ve bir yıl sonra, Haziran 2015 tarihinde ise sanal para birimlerine risk temelli yaklaşım rehberini yayımlamış[88] ve söz konusu bu ikinci rehberi Ekim 2021'de güncellemiştir.[89] FATF'nin 15 no.lu Tavsiyesi, suç gelirlerinin aklanması ve terörizmin finansmanı (AML/CFT) önlemlerini sanal varlıklara (VA) ve sanal varlık hizmet sağlayıcılarına (VASP'ler) uygulamak için 2019 yılında güncellenmiştir. Buna göre:

"15. Yeni teknolojiler: Ülkeler ve finansal kuruluşlar (a) Yeni dağıtım mekanizmaları da dahil olmak üzere yeni ürünlerin ve yeni iş uygulamalarının geliştirilmesi ve (b) Hem yeni hem de önceden var olan ürünler için yeni veya gelişen teknolojilerin kullanılması ile ilgili olarak ortaya çıkabilecek kara para aklama veya terörün finansmanı risklerini belirlemeli ve değerlendirmelidir. Finansal kuruluşlar söz konusu olduğunda, bu tür bir risk değerlendirmesi yeni ürünlerin, iş uygulamalarının veya yeni ya da gelişmekte olan teknolojilerin kullanılmaya başlanmasından önce yapılmalıdır. Bu riskleri yönetmek ve azaltmak için uygun tedbirleri almalıdırlar.

Sanal varlıklardan kaynaklanan riskleri yönetmek ve azaltmak için ülkeler, sanal varlık hizmet sağlayıcılarının AML/CFT amaçları doğrultusunda düzenlendiğinden, lisanslandığından veya tescil edildiğinden ve FATF Tavsiyelerinde öngörülen ilgili tedbirlere uyumu izlemek ve sağlamak için etkili sistemlere tabi olduğundan emin olmalıdır."

FATF 15 no.lu Tavsiye Kararı ve Yorumlayıcı Notu (R.15/INR.15) ile uyumuna ilişkin beşinci güncellemeyi Temmuz 2024'te yayınlamış olduğu

[86] **Malcolm Campbell-Verduyn**, "Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance" Crime, Law and Social Change V. 69, No. 2, March 2018, s. 299.
[87] FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, Haziran 2014.
[88] FATF, Guidance for a Risk-Based Approach to Virtual Currencies, Haziran 2015.
[89] FATF, Updated Guidance for a Risk-Based Approach to Virtual Currencies Ekim 2021.

raporunda sunmaktadır.[90] Nitekim Türkiye'nin SPK'ya eklediği maddeler ile kripto varlıkları ve kripto varlık hizmet sağlayıcıları düzenlemesi FATF'nın güncellenmiş 15 no.lu Tavsiye Kararı ile uyumun sağlanması için yapılmıştır.

Blok zincir teknolojilerinin iki temel özelliği - ademi merkeziyetçilik ve yarı anonimlik - uluslararası AML rejiminin kalbinde yer alan FATF'nin tepkisini şekillendirmiştir. FATF ilk olarak, yarı anonim kripto varlık kullanıcıları tarafından gerçekleştirilen merkezi olmayan işlemlerin izlenmesi ve tanımlanmasındaki zorluklara işaret etmiştir. 2015 tarihli raporda belirtildiği üzere, *"soruşturma amacıyla ... hedef alınacak", "merkezi bir konum veya kuruluşun"* olmaması, *"ülkelerin etkili ve caydırıcı yaptırımlar uygulama kabiliyetini zayıflatmakta"* ve *"kolluk kuvvetlerinin aklanan yasa dışı gelirlerin izini sürme kabiliyetine önemli bir zorluk teşkil etmektedir"*.[91]

FATF, kripto varlık kullanıcılarını hedef almak yerine, kripto varlık aracı kurumlarına (borsalarına) ve merkezi olmayan blok zincir tabanlı sistemlerdeki diğer "düğüm noktalarına" odaklanılmasını tavsiye etmiştir. Bunlar, faaliyetleri FATF'nin "düzenlenmiş fiat para finansal sistemi" olarak tanımladığı sistemle önemli şekillerde kesişen kilit kurumlardır. FATF böylece uluslararası AML çabalarının odağını, "üst dünyaların" devlet destekli ulusal para birimlerinden, küresel ekonominin "yeraltı dünyalarına" transfer edildikten sonra kripto varlıkları "gönderen, alan ve saklayan" merkezi kurumlara doğru yöneltmiştir.[92]

FATF, devlet ve devlet dışı aktörler arasında zorlayıcılığı az olan "koordinasyon mekanizmalarına" ihtiyaç olduğunu vurgulamıştır. Bu tür

[90] FATF, Targeted Update on Implementatıon of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, Haziran 2024. "Bu rapor, yetki alanlarının FATF'nin 15 sayılı Tavsiye Kararı ve Yorumlayıcı Notu (R.15/INR.15) ile uyumuna ilişkin beşinci güncellemeyi sunmaktadır. Tavsiye 15, suç gelirlerinin aklanması ve terörle mücadele finansmanı (AML/CFT) önlemlerini sanal varlıklara (VA) ve sanal varlık hizmet sağlayıcılarına (VASP'ler) uygulamak için 2019 yılında güncellenmiştir. Raporda ayrıca, suç gelirlerinin aklanması, terörün finansmanı ve bu finansmanın çeşitliliği için VA'ların kullanımıyla ilgili ortaya çıkan riskler ve piyasa gelişmeleri hakkında güncellemeler de yer almaktadır. FATF'nin raporu, bazı yargı bölgelerinin AML/CFT düzenlemelerini yürürlüğe koyma konusunda ilerleme kaydetmiş olmasına rağmen, küresel uygulamanın hala gecikmekte olduğunu ortaya koymaktadır. Sektörü düzenlemek için henüz önemli adımlar atmamış olan çok sayıda hükümet bulunmaktadır ve bu ülkelerin acil olarak Standartları tam olarak uygulamaya öncelik vermeleri gerekmektedir. Revize edilmiş R.15/INR.15'in 2019'da kabul edilmesinden bu yana 130 FATF karşılıklı değerlendirme ve takip raporuna göre, yargı bölgelerinin %75'i FATF gereklilikleriyle yalnızca kısmen uyumludur veya uyumlu değildir; bu oran Nisan 2023'tekiyle aynıdır (%75 kısmen uyumlu veya uyumsuz yargı bölgeleri; 98'in 73'ü) ve ihmal edilebilir bir iyileşme göstermektedir." (Çevrimiçi) https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html, 9 Temmuz 2024, (set) 19.07.2024.

[91] FATF, 2015: 8-11.

[92] **Petrus C. van Duyne/Klaus von Lampe/Nikos Passas**, (eds.) Upperworld and Underworld in Cross-Border Crime, Wolf Legal Publishers, Nijmegen, 2002; FATF, 2015: 6; **Campbell-Verduyn/ Goguen**, s. 76, FATF, 2015: 6.

tedbirler arasında bilgi ve enformasyon paylaşımı, "benzer risk profillerine sahip benzer ürün ve hizmetler için benzer AML/CFT uygulamalarını" formüle etme ve benimseme çabaları ve ülkeler arasında ya varlıklara el koyma ya da kara para aklama suçlarıyla itham edilen kişileri potansiyel olarak iade etme konusunda karşılıklı hukuki yardımlaşma yer almaktadır. Yine de FATF, yalnızca bu tür önlemlerin yetersiz olduğu kanıtlandığında, blok zincir tabanlı faaliyetlerin tamamen yasaklanmasını da içeren "bir dizi etkili, orantılı ve caydırıcı yaptırım" dahil olmak üzere daha zorlayıcı stratejilerin dikkate alınmasını önermektedir.[93]

FATF'nin risk temelli yaklaşımını yerinde bulduğumuzu ifade etmeliyiz. Ancak bu bakış açısı FATF açısından bir yasaklama anlamına gelmediği gibi FATF'nin bu konudaki yaklaşım ve tavsiyelerine uyum sağlayacak ülkeler açısından yasakçı bir zihniyete dönüşmemelidir. Risk temelli yaklaşım doğrudur zira günümüzde kripto varlıklar suç gelirlerinin aklanmasında abartıldıkları kadar yoğun kullanılmamaktadır ancak kontrol altına alınmaz ise bu potansiyeli taşıdığı bir gerçektir. Bundan dolayı FATF bu potansiyel duruma yönelik risk temelli bir yaklaşım geliştirmiştir. Nitekim bu konudaki son derece önemli ve ufuk açıcı makalesi *Campell-Verduyn*'da bunu ifade etmektedir:

"…bazı eksikliklerine rağmen, kara para aklamayla mücadele çabalarının koordinasyonunda yer alan önde gelen küresel düzeydeki kuruluş olan Mali Eylem Görev Gücü (FATF) tarafından formüle edilen risk temelli yaklaşım, kripto varlıkların şu anda sunduğu mevcut tehditler ve fırsatlar arasında etkili bir denge sağlamaktadır. FATF'nin daha gevşek, merkezi olmayan yönetişim ağlarını teşvik etmesi, hızlı ve öngörülemeyen teknolojik değişim çağında yenilikçi ve nihayetinde geleneksel merkezi zorlama biçimlerinden daha etkili olarak kabul edilmektedir."[94]

Ancak FATF'nin son tahlilde gerekirse kripto varlık faaliyetlerinin tamamen yasaklanmasına ilişkin aşırı yaklaşımını benimsemediğimizi ifade etmeliyiz. Bunun iki nedeni bulunmaktadır: Birincisi bu tür yasaklama teknolojinin önüne ket vurmak anlamına gelir. Bu ise inovasyonu ve daha iyi ve refah içinde yaşamının yollarını arayışa ilişkin çalışmaların yapılmasını engeller. Bu yasaklamalar bir kere başladı mı çeşitli gerekçelerle her yerde görülmeye başlar, bu ise bilimin, teknolojinin ve insanlığın gelişiminin engellenmesi anlamına gelir. İkinci olarak bu şekilde normatif bir yasaklamanın gerçek yaşamda bir karşılığının olmayacağıdır yani bu tür yasaklayıcı bir norm sosyal etkililik açısından başarısız olmaya mahkûmdur. Cin şişeden bir kere çıkmıştır! Artık blok zincir ve kripto varlık kullanımı ve geliştirilmesinin hukuk kurallarıyla engellenmesi mümkün değildir. Bu tür bir yasak tüm kripto varlık sektörünü yer altına inmeye zorlayacaktır. Bu ise çok daha

[93] FATF, 2015: 9-11.

[94] **Campbell-Verduyn**, s. 284.

fazla sayıda suçun işlenmesine ve tam bir kontrolsüzlüğe yol açacaktır. Bu nedenle yasaklamak yerine sektörün kontrol altına alınmasına ilişkin çalışmaların ve düzenlemelerin yapılması bize göre çok daha yerinde bir yaklaşım olacaktır.

Blok zincir teknolojisinin ve uygulamalarının uluslararası AML rejimine meydan okuma teşkil ettiğine dair yaygın algı, uluslararası kuruluşların tepkisinin yönünü belirlemiştir. Birleşmiş Milletler Uyuşturucu ve Suç Ofisi, kara para aklamaya karışan kripto varlıkların tespit edilmesi ve ele geçirilmesi için ayrıntılı bir kılavuz hazırlamıştır. UNODC, Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) ile birlikte, yetkilileri kripto varlıklar aracılığıyla kara para aklamayı araştırmak için eğitmeye başlamıştır (Birleşmiş Milletler Uyuşturucu ve Suç Ofisi, 2017). Interpol ve Europol, "sanal para birimlerinin cezai işlemler ve kara para aklama için kötüye kullanılmasına karşı" polis faaliyetlerini koordine eden bir ortaklık kurmuştur.[95] Ayrıca Avrupa Birliği'nin bu konuda Direktifleri bulunmaktadır. FATF için getirdiğimiz eleştiriler, bu kurumlar tarafından yapılan düzenlemeler bakımından da geçerlidir.

Ortaya Çıkan Riskler, Tehditler ve Zorluklar

Kripto varlıkların suç gelirlerinin aklanmasında ve terörizmin finansmanında kullanılmasının büyüyen bir tehdit olduğu tartışmasız bir gerçektir. Bu tehdit nedeniyle bir yandan finans dünyası bu zorlukla boğuşurken, diğer yandan kolluk kuvvetleri de suç gelirlerinin kaynağını izlemek ve yasa dışı fonların oluşturulmasında rol oynayan suç faillerini tespit etmek gibi zorlu bir görevle karşı karşıyadır. Zaten zor bir süreç olan aklama işlemlerini tespit etmek kripto varlıkların ortaya çıkmasıyla daha da zor hale gelmiştir. Suç gelirlerini aklayanlar çeşitli suç faaliyetlerinden elde ettikleri fonları aklamak için kripto varlıkları giderek daha fazla kullanmaktadırlar. Bu yasa dışı fonları kaynağına kadar takip etmek, kolluk kuvvetleri için zorlu bir görev haline gelmiştir çünkü kolluk güçleri genellikle kripto varlıkların özelliklerine uygun olmayan geleneksel soruşturma yöntemlerini kullanmaktadırlar. Nitekim suç gelirlerini aklamanın; yerleştirme, katmanlama ve bütünleme aşamalarında kripto varlıkların kullanılması aklama işlemlerini daha da karmaşık ve takibi zor hale getirmektedir. Suçlular, haksız kazançlarının kaynağını gizlemek için kripto varlık tamburları (tumbler) ve karıştırma hizmetlerinden (mixer) yararlanmakta, bu da kolluk güçlerinin paranın izini takip etmesini ve suç faillerini belirlemesini zorlaştırmaktadır.[96]

Kripto varlıklar içinde Bitcoin, merkezi yönetim organları veya aracılar olmaksızın kullanıcıları tarafından hizmet verilen ilk merkezi olmayan P2P

[95] **Campbell-Verduyn/Goguen**, s. 76. Bkz. Europol Interpol Cybercrime Conference makes the case formultisector cooperation. Retrieved 02.10.2015 (Çevrimiçi) https://www.europol.europa.eu/media-press/newsroom/news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-for-greater-multisector-cooperation, (set) 10.08.2024.

[96] **Financial Crime Academy**, Crypto Money Laundering.

ödeme ağıdır. Kullanıcıların bakış açısından Bitcoin, nakit paraya benzerlik gösterir ancak sadece internette geçerlidir. Sistemin merkezsizleşmesi ve anonimlik kripto varlıklara özgüdür ve içerisinde suç gelirlerinin aklanması ve terörizmin finansmanı için kullanılma riskini artırır. Bitcoin hesaplarında, hesap sahipleri hakkında kimlik bilgileri yer almadığından ve sistemde merkezi bir sunucu veya hizmet sağlayıcı bulunmadığından bu sistem aklama işlemlerini yapmayı kolaylaştırmaktadır. Bitcoin protokolü, gerçek dünyada olduğu gibi, kişilerin kontrol edilmesini veya geçmiş dönemdeki işlemlere ilişkin verilerin oluşturulmasını ve tutulmasını talep etmez ve sağlamaz. Ayrıca merkezi bir denetim otoritesi yoktur ve günümüzde suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadele için şüpheli işlemlerin şemalarını izlemeyi ve ortaya çıkarmayı mümkün kılacak tam ve eksiksiz bir yazılım bulunmamaktadır. Sonuçta, kredi ve banka kartları ve elektronik ödeme sistemleri (e-cüzdanlar) bakımından imkânsız olan yüksek düzeyde anonimlik sağlamaktadır. Kripto varlıklar ile ilgili ana mesele bunların özünde gizlidir. Zira kripto varlıklar yerleşik finansal kurumların ve finansal düzenlemelerin tamamen dışındadır.[97]

Kullanıcı açısından bakıldığında Bitcoin bir elektronik para sistemidir. İnternete erişimi olan ve bilgisayarında gerekli miktarda bellek bulunan herhangi bir kişi bu elektronik paranın kullanıcısı olabilir. Bitcoin kullanmaya başlamanın ilk adımı, "bitcoin.org" sitesinden bir cüzdan seçilmesi ve ardından bunun kurulmasıdır. Bir cüzdan oluşturulduktan sonra Bitcoin adresi otomatik olarak oluşturulur. Bu cüzdanı kullanarak kullanıcı herhangi bir işlem yapabilir. Bitcoinlerin bir kullanıcından diğerine aktarılması, Bitcoinlerin bir adresten diğerine aktarılması yoluyla yapılır. Bu adres rakam ve harflerin bir kombinasyonu gibi göründüğü için sahibine tam bir anonimlik sağlar, örn. "1D5wZqCjxNuPqfUN3RMFsxxxtqRBwiAeTZ". Her Bitcoin cüzdanı, belirli bir kullanıcıya ait olan herkesin Bitcoin adresinin özel anahtarları hakkında sınıflandırılmış bilgileri içerir. Bu nedenle, işlem için tasarlanan bir Bitcoin adresinden özel bir anahtara sahip olunduğunda işlem yapılabilir. Bu sistem oldukça güvenli olmasına rağmen, site yöneticileri mümkün olduğunca çok sayıda Bitcoin adresi, yani her işlem için yeni bir Bitcoin adresi kullanılmasını önermektedir. Bitcoin sisteminde özel anahtarın geri yüklenmesi gibi bir işlev bulunmamaktadır, bu nedenle özel anahtarın kaybedilmesi durumunda kullanıcı bu adreste saklanan tüm fonları kaybeder. Özel anahtarın çalınması da depolanan Bitcoinlerin kaybına yol açar. İşlemlere ilişkin veriler, adresin kullanıcısı hakkında bilgi ifşa edilmeksizin açık erişimli dağıtık veri tabanında saklanır. Aynı Bitcoinlerin iki kez harcanabileceği durumları önlemek için Satoshi Nakamoto, veri tabanının özel bloklar zincirine bölündüğü bir

[97] **Diana Mergenovna Sat/Grigory Olegovich Krylov/Kirill Evgenyevich Bezverbnyi/Alexander Borisovich Kasatkin/Ivan Aleksandrovich Kornev**, "Investigation of Money Laundering Methods Through Cryptocurrency", Journal of Theoretical and Applied Information Technology, Vol. 83, No. 2, January 2016, s. 245.

zaman etiketi sistemi (timestamp server) geliştirmiştir. Her blok bir önceki bloğun hash'ini (sağlama toplamı) ve seri numarasını içerir. Yeni blok, işlemlerin tamamlandığının onaylanmasıyla oluşturulur ve Bitcoinlerle yapılan önceki işlemler hakkında bilgi içerir. Başka bir deyişle, her Bitcoin daha önce nasıl kullanıldığı bilgisine sahiptir ve kullanıcılar Bitcoinleri alırken "dijital imza" ve bir sonraki sahibin açık anahtarını bırakırlar. Bir bloğun içindeki verilere müdahale edildiğinde HASH değeri değiştiği için diğer bloklar bu farklı HASH değerini onaylamamakta dolayısıyla da veriler değiştirilememektedir.[98] Tüm işlemlerin Bitcoin adresleri ile bağlantısı vardır ve internette bulunabilen bir Bitcoin blok zincirinde bu işlemlerin izi sürülebilir. Bu nedenle, şüphelinin bilgisayarında bulunan Bitcoin adreslerinin bilgileri, şüpheliyle bağlantılı Bitcoin adreslerine yapılan transferlerden önce ve sonra hangi işlemlerin yapıldığının tespit edilmesi açısından incelenebilir.[99]

Teknolojinin küresel yönetişim üzerindeki etkileri genellikle birbiriyle çelişen iki görüşü ortaya çıkarmıştır. Bir yanda teknolojideki ilerlemelerin yönetişimi geliştireceğine dair olumlu fikirlere dayanan iyimser görüşler söz konusuyken;[100] diğer yanda ise yeni teknolojilerin yönetişim açısından olumsuz sonuçları olacağına dair fikirlere dayanan distopya hikayelerinin yer aldığı kötümser görüşler bulunmaktadır.[101] Bunlardan ilki, teknolojik gelişmelerin ekonomik verimliliğin artmasına ve insani yaşam koşullarının iyileşmesine yol açacağını varsayar. İkinci görüş ise daha çok nükleer silahlar, zehirli partiküller gibi teknolojik ilerlemenin neden olduğu felaketlere ve bekleyen yok olma risklerine odaklanmaktadır. Her iki görüş de teknoloji ve yönetişim arasındaki çok daha karmaşık iç içe geçmiş ilişkinin aşırı basitleştirilmiş halidir.[102] Oysa işler ne iyi ne de kötü yönde bu kadar basit bir biçimde ilerlememektedir. Teknoloji, insanların gündelik yaşamlarındaki güç yapısına gömülüdür ve her zaman değişmektedir. Teknolojinin "iki hikayesinin" sınırlandırılması bizi yüzeysel araçsallığın ötesine ve teknoloji ile hükümetler, işletmeler, bireyler vb. arasındaki daha derin ilişkiye odaklanmaya yönlendirmektedir.[103]

---

[98] **Akbulut**, s. 490.

[99] **Sat/Krylov/Bezverbnyi/Kasatkin/Kornev**, s. 245, 246.

[100] **Ray Kurzweil**, The Singularity is Near: When Humans Transcend Biology, Penguin, London, 2005; **Roger Pielke Jr./Tom Wigley/Christopher Green**, Dangerous Assumptions Nature, 452, 2008, s. 531–532.

[101] **Steve Matthewman**, Technology and Social Theory, Palgrave Macmillan, London, 2011.

[102] **Maximilian Mayer/Mariana Carpes/Ruth Knoblich**, (eds.), The Global Politics of Science and Technology – Vol. 1, Concepts from International Relations and Other Disciplines, Springer, New York, 2014; **Maximilian Mayer/ Mariana Carpes/Ruth Knoblich**, (eds.), The Global Politics of Science and Technology – Vol. 2, Perspectives, Cases and Methods, Springer, New York, 2014.

[103] **Kai Jia/Falin Zihang**, "Between Liberalization and Prohibition Prudent Enthusiasm and the Governance of Bitcoin/blockchain Technology", in: Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018, s. 88.

Bitcoin ve blok zincir teknolojilerinin ortaya çıkışı bu güç dinamiklerini örneklemektedir. Bir yandan, bireylerin merkezi kurumlar olmadan doğrudan işlem yapabilmelerini sağlayan aracısızlaştırma, insanları hükümetlerin veya merkez bankalarının kontrolüne karşı güçlendirmektedir. Öte yandan, merkezi kurumlar bu teknoloji tarafından tamamen devre dışı bırakılmamaktadır. Aksine, hükümetlerin politik tepkileri özel olarak kripto varlıkların ve genel olarak blok zincir teknolojilerinin gelişim yolunu etkilemektedir.[104]

Bu konuda Bitcoin üzerinden ampirik bir çalışma yapan *van Wegberg/ Oerlemans/van Deventer* suç gelirlerini aklamanın pratikte düşünülebilir bir kavram olduğu, kripto varlıklarla aklama işlemi yapmanın günümüzde ve gelecekteki aklama işlemlerine eklemlenebilecek biçimde günümüzdeki klasik yöntemlerle yüksek derecede benzerliğe sahip olduğu sonucuna varmışlardır. Yazarlar, ortaya çıkan son vakalar ve Europol raporlarının, Bitcoinlerin siber suçlular tarafından aklama amacıyla kullanıldığı sonucunu desteklediğini ifade etmektedirler. Yazarların en önemli bulduğu konu ise kripto varlıklarla yapılan aklama işlemlerinin daha fazla anonimlik sağlarken aklama maliyetini düşürme kabiliyetinin bu yöntemi suçlular için daha çekici bir aklama tekniği haline getirmesidir. Yazarlar bu bağlamda, bunun suç işleme modellerinin karlılığı için ne anlama geldiği sorusunu sormaktadırlar ve bu soruyu yanıtlarken öncelikle bu yöntemi kullanan suçlular hakkında sınırlı bir genel bakışa sahip olduklarını, bununla birlikte, bu küçük ölçekli deneyden, en azından teoride Bitcoin kullanılarak yapılan aklamanın maliyetinin düşürülebileceğini, bunun da bazı suç işleme modellerini potansiyel olarak daha karlı hale getirebileceğini, bunun da siber suç girişimleri için cazip olduğunu ifade etmektedirler.[105]

Kripto varlıklar, iyilik için olduğu kadar kötülük için de kullanılmaktadır. Kripto varlıkların yargı bölgeleri arasında en yaygın iki yasa dışı kullanımı dijital karaborsalar (yasa dışı pazar yerleri) ve suç gelirlerinin aklanmasıdır. Küresel bir ağ olan internet üzerinden anonimlik sağlanmak suretiyle suçtan elde edilmiş gelirlerin ülkelerin fiziksel sınırlarının ötesine transfer edilmesi bu teknoloji sayesinde oldukça kolaylaşmıştır. Konuya teorik olarak yaklaşıldığında kripto varlıkların suç gelirlerini aklamak isteyenler için göründüğü kadar cazip bir seçenek olmadığı düşünülebilir. Zira ilk olarak, kripto varlıkların işlem kapsamı sınırlıdır. İkincisi, tüm işlem kayıtları halka açık ve erişilebilirdir. Her ne kadar kullanıcıların adresleri ve kimlikleri şifreleme teknolojisi ile korunuyor olsa da özellikle Silk Road vakasında görüldüğü gibi Bitcoin'ler belirli fiat para birimleri ile takas edildiğinde, kolluk kuvvetlerinin şüphelileri teyit etmesi hala mümkündür. Üçüncüsü, Avrupa Birliği'nde görüldüğü üzere aklama karşıtı kayıt tutma ve raporlama gerekliliklerine uyma baskısı altında olan Bitcoin borsalarına kademeli

[104] **Jia/Zihang**, s. 89.
[105] **van Wegberg/Oerlemans/van Deventer**, s. 431.

olarak hukuki düzenlemeler getirilmektedir.[106] Ancak bu çekinceler yine de aklama için kripto varlıkların elverişli potansiyelini yok etmemektedir. Kolluk kuvvetlerinin kripto varlıkların aklamada kullanılmasına karşı mücadelelerinde karşılaştıkları zorunluklardan bazıları şunlardır: İlk zorluk kripto varlıkların merkezi olmayan bir yapıya sahip olmasıdır. Geleneksel para birimlerinin aksine, kripto varlıklar herhangi bir merkezi otorite tarafından kontrol edilmezler ve işlemlerin hükümet veya finans kurumlarının gözetimi dışında gerçekleşmesine izin verirler.[107] Bu merkeziyetsiz ve dağıtık yapı, kolluk kuvvetlerinin yasa dışı fonları takip etmesini ve izlemesini önemli ölçüde zorlaştırır. Ayrıca küresel düzenleyici bir yapının olmaması suç soruşturmalarını daha da zorlaştırır. Bunlara ek olarak, kripto varlık işlemlerinin takma isimle anonim olarak gerçekleştirilmesi bir başka karmaşıklık katmanı oluşturur. Tüm işlemler blok zincirine kaydedilirken, varlık transferleri kriptografik adreslerle yapılır, bu da işlemlerin gerçek dünyada bu işlemleri yapan kişilerin kimlikleriyle ilişkilendirilmesini zorlaştırır. Bu durum, suçlular tarafından istismar edilebilecek bir anonimlik sağlayarak kolluk kuvvetlerinin çalışmalarını engeller. Kripto varlıkların, bankalar gibi aracı kurumlara ihtiyaç duymadan gerçekleştirilmesi, sınır ötesi işlemlere olanak tanıyan yapısı ve bu yapıya küresel erişim sağlanabilmesi kolluk güçlerinin suçluların izini sürmesi bakımından bir başka zorluk oluşturmaktadır. Böylelikle bir ülkedeki suç gelirleri başka bir ülkeye kolayca aktarabilir ve bu da suçluların belirlenmesi ve soruşturulmasını önemli ölçüde zorlaştırır.[108]

Bu alandaki bir başka zorluk da bazı kripto varlıkların ekstra gizlilik sağlamasıdır. Bunun en göze çarpan örnekleri Monero ve Zcash gibi gizlilik altcoinleridir. Gizlilik varlıkları (coinleri) olarak adlandırılan bu kripto varlıklar, bir kullanıcının bilgilerini ve bir işlemle bağlantılı ilgili ayrıntıları maskelemek için özel olarak tasarlanmışlardır. Bu varlıklar, halka açık defterlere sahip olmaları anlamında halka açıktırlar ancak işlem bilgileri son kullanıcıların gizliliğini korumak için çeşitli derecelerde gizlenmiştir. Sonuç olarak, Monero ve Zcash gibi gizlilik varlıkları, suçlulara fayda sağlayabilecek ek bir anonimlik katmanı sağlarken, aynı zamanda kolluk kuvvetlerinin soruşturmalarını da engellemektedirler. Gizlilik varlıkları, kripto varlıkları izlemek için geliştirilen yazılımları/araçları (tool) da atlatabilmektedir, dolayısıyla bunların varlığı riski artıran bir faktördür.[109] Bunlardan Monero, işlem imzaları büyük bir grup insan tarafından paylaşıldığı için işlemde yer alan tarafların izlenmesini zorlaştırmakta ve

[106] **Aaron van Wirdum**, "New EU directive may impose anti-money laundering regulations on Bitcoin wallet providers". Bitcoin Magazine, (2016), (Çevrimiçi) https://bitcoinmagazine.com/articles/new-eu-directive-may-impose-anti-money-laundering-regulations-on-bitcoin-wallet-providers-1468424029/ (set) 09.08.2024; **Jia/Zihang**, s. 95, 96.
[107] **Çakır**, s. 78; **Akbulut**, s. 489.
[108] **Financial Crime Academy**, Crypto Money Laundering.
[109] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.

böylelikle belirli kullanıcıları bir işlemle ilişkilendirmek oldukça zor bir hale gelmektedir. Zcash ise biraz daha farklı işlemektedir, işlem gerçekleştikten sonra işlem geçmişinin "silinmesi" sonucunda gizlilik sağlanmaktadır.[110] Bu nedenle, sektörün dinamik yapısı ve bu alandaki işletmeciler tarafından geliştirilen (geliştirilecek) özel teknolojilerin görünürlüğünün olmaması göz önüne alındığında, bir genel yasağın ileriye dönük en uygun yol olup olmayacağı tartışılmaktadır.[111]

Gizlilik kripto varlıkları, suç gelirlerini aklayanlar için oldukça elverişli görünse de bu varlıkların asırlık bir suçu çağdaşlaştırmak için yirmi birinci yüzyıl teknolojisini manipüle etme niyetiyle geliştirilmediğini belirtmek gerekir. Bunun yerine, gizlilik varlıkları dijital çağda bireylere ek bir gizlilik, güvenlik ve anonimlik katmanı sunmak üzere tasarlanmıştır. Aslında Monero çoğu insanın yasal olarak kullanması için geliştirilmiştir, bunun geliştirilmesindeki amaç sadece başkalarının kendisinin kahve mi yoksa araba mı aldığını bilmelerini istememesine ilişkin mahremiyetini sağlamaktadır.[112] Ne var ki, çoğu teknolojik gelişme gibi mucitler iyi niyetli olabilir ancak bazı kişiler her zaman teknolojiyi kötü amaçlar için kullanmanın bir yolunu bulacaktır. Bununla birlikte, Monero ve Zcash gibi gizlilik varlıkları kötüye kullanılma potansiyelleri nedeniyle hem pek çok kolluk kuvvetinin hem de uluslararası düzenleyicilerin dikkatini çekmektedir.[113]

Sonuç olarak bu alanda çalışma yapanların genel düşüncesi ifade eden *Keech* mevcut tehditler ile kripto varlıkların sağladığı fırsatlar arasında bir denge kurulması gerektiğidir.[114] Benzer şekilde *Campbell-Verduyn* suç gelirlerini aklamayı önleme adımlarının, kripto varlıkları yasa dışı kullanım için kullanmak yerine, kripto para birimlerinin temelini oluşturan blok zincir teknolojisine doğru kaymaya başlaması gerektiğini kabul etmektedir.[115]

Alınması Gereken Önlemler

1. Genel Olarak

Kripto varlıklar, inovasyon ve yatırım için sunduğu yeni fırsatlarla finans dünyasında bir devrim yaratmıştır. Bu dijital devrim faydalarının yanı

[110] **Forgang**, s. 7. Ayrıca bkz. Nasdaq, "Know Your Coins: Public vs. Private Cryptocurrencies", 22 Eylül 2017, (Çevrimiçi) https://www.nasdaq.com/articles/know-your-coins-public-vs-private-cryptocurrencies-2017-09-22, (set) 10.07.2024.

[111] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.

[112] **Olga Kharif**, "Bitcoin is being dropped by criminals in favour of privacy coins like monero", Independent, 2 Ocak 2018, (Çevrimiçi) https://www.independent.co.uk/news/business/analysis-and-features/bitcoin-latestupdates-price-privacy-coins-cryptocurrency-monero-digital-currency-pricea8137901.html, (set) 10.07.2024.

[113] **Shaurya Malwa**, "$1.2 Billion in Cryptocurrency Laundered Through Bitcoin Tumblers, Privacy Coins", 6 Temmuz 2018, (Çevrimiçi) https://finance.yahoo.com/news/1-2-billion-cryptocurrency-laundered-224521652.html, (set) 11.07.2024; **Forgang**, s. 8, 9.

[114] **Keech**, s. 57.

[115] **Campbell-Verduyn**, s. 283.

sıra karanlık bir tarafın da ortaya çıkmasına neden olmuştur. Karanlık tarafta kripto varlıklar çeşitli suçların işlenmesinde ve suç gelirlerinin aklanmasında kullanılmaktadır. Suçlular kripto varlıkların anonimliğinden ve dağıtık yapısından yararlanmak için giderek daha sofistike yöntemler geliştirirken; kolluk kuvvetlerinin, kural yapıcıların ve kripto endüstrisinin bu büyüyen tehditle mücadele etmek için birlikte çalışmaları gerekir.

Kripto varlıkların küresel yapısı, kripto varlık aklama ile etkin bir şekilde mücadele etmek için koordineli bir uluslararası müdahaleyi ve mücadeleyi birlikte gerektirir. Yaptıkları işlemleri daha karmaşık hale getirmek isteyen suçlular, soruşturma makamlarının önüne geçmek için tekniklerini sürekli geliştirmektedirler. Teknolojideki hızlı ilerlemeler, sınırlı kaynaklar ve uzmanlıkla birleştiğinde, yetkililerin sürekli değişen kripto varlık aklama ortamına ayak uydurmasını zorlaştırır. Sonuç olarak, kolluk kuvvetleri bu büyüyen tehditle etkin bir şekilde mücadele etmek için uyum sağlamalı ve yeni stratejiler geliştirmelidir.[116]

Suçlular hem klasik yöntemlerde hem de kripto varlıkları ve dijital dünyayı kullandıkları yöntemlerde suç işleme ve suç gelirlerini aklama teknik ve yöntemlerini sürekli geliştirerek, kolluk kuvvetlerinin suç gelirlerinin aklanmasıyla etkin bir şekilde mücadele etmesini ve teknolojinin gelişimine ayak uydurmasını giderek zorlaştırmaktadırlar. Suçluların kullandığı teknikleri anlamak, kripto para aklamayla etkin bir şekilde mücadele etmek için hayati bir adımdır. Kolluk kuvvetleri ve düzenleyici kurumlar bu teknikleri ortaya çıkararak aklama faaliyetlerine karşı koymak ve kripto endüstrisinin güvenirliğini korumak için stratejiler ve araçlar geliştirmelidir.[117]

2. Aklamayla Mücadelede Kripto Varlık Aracı Kurumların (Borsaların) Rolü

Kripto varlık borsaları olarak da bilinen kripto varlık aracı kurumları, suç gelirlerinin aklanması ile mücadelede ilk aşamada yer alan ve son derece önemli konumda bulunan kurumlardır. Kripto ekosisteminin önemli bir bileşeni olan bu kurumlara ekosistemin düzgün işlemesinin sağlanması yanında suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadele edilebilmesi için çeşitli yükümlülükler getirilmelidir. Bu kurumlar sıkı KYC/AML politikaları uygulamak, şüpheli faaliyetleri tespit etmek ve bildirmek, soruşturma makamları ile iş birliği yapmak gibi yükümlülüklere tabi tutulmalıdırlar.[118] Nitekim ülkemizde MASAK yakın tarihte kripto varlık aracı kurumları için bu yükümlülükler getirmiştir.

Kripto varlıklar geleneksel finansal kurumlar tarafından ihraç edilmez ve bu nedenle aynı düzenlemelere tabi değildir. Bireyler finansal bir aracıya

[116] **Financial Crime Academy**, Crypto Money Laundering.
[117] **Financial Crime Academy**, Crypto Money Laundering.
[118] **Financial Crime Academy**, Crypto Money Laundering.

ihtiyaç duymadan serbestçe kripto varlık alışverişi yapılabilirken, kripto varlık aracı kurumları suç gelirlerini aklama faaliyetlerini kolaylaştırmak için de kullanılabilir. Aracı kurumlar esasen kripto varlıkların yasal olarak alınıp satılabildiği, hem geleneksel paraların kripto varlık birimlerine dönüştürülmesine hem de tam tersinin yapılmasına ve bir kripto varlık biriminin diğeriyle takas edilmesine olanak tanıyan ticaret platformlarıdır. Bazı aracı kurumlarda suç gelirlerini aklamayı önleme protokolleri mevcut olsa da hala istismar edilebilecek zayıflıklar olduğu belirtilmelidir. Sonuçta, en büyük ve en sıkı denetime tabi finansal kurumlar bile aklama faaliyetlerine açıktır. Bu kurumların uyum departmanlarına sahip olması ve aklamayı önleme görevlileri istihdam etmesi, suç gelirlerinin aklama faaliyetlerinin gerçekleşmeye devam etmediği anlamına gelmez.[119]

Bu kurumlar arasında KYC/AML'ye uyumlu olanlar ve olmayanlar şeklinde bir ayrım yapılabilir. Uyumlu aracı kurumlar, KYC/AML yükümlülükleri ile ilgili yasa ve yönetmeliklere bağlı olan ve bunlara uygun işlem yapan kurumlardır. Bu uyum sayesinde aracı kurumlar bir yandan suç gelirlerinin aklanması ve diğer yasa dışı faaliyetlerin önlenmesi açısından soruşturma makamlarına yardımcı olurken diğer yandan kullanıcılarını potansiyel risklerden korurlar. Bu kurumlar sorumluluklarını ciddiye alarak kullanıcılarının kimliklerini doğrulamak, şüpheli faaliyet belirtilerine karşı işlemleri izlemek ve olası sorunları ilgili makamlara bildirmek için sağlam sistem ve prosedürlere sahip olduklarından emin olmalıdırlar. Bu yalnızca kripto ekosisteminin bütünlüğünü korumaya yardımcı olmakla kalmaz, aynı zamanda şeffaf ve etik bir şekilde faaliyet göstermeye kararlı olduklarını göstererek kullanıcıları ve geniş halk kitleleri nezdinde güven oluşturmalarını sağlar. Buna karşılık, uyumlu olmayan borsalar sıkı KYC/AML politikaları uygulamazlar, bu da onları suç faaliyetlerine ve yetkililer tarafından olası kapatmalara karşı daha savunmasız hale getirir. Uyumlu ve uyumsuz borsalar arasındaki ayrım, kripto sektöründe düzenlemenin ve gözetimin önemini vurgulamaktadır. Düzenleyiciler, borsaların sıkı KYC/AML gerekliliklerine uymasını sağlayarak suç gelirlerinin aklanması ve diğer yasa dışı faaliyetlerin önlenmesine yardımcı olmalı ve aynı zamanda kripto ekosisteminin bütünlüğünü korumalıdırlar. Bu da kullanıcılar, yatırımcılar ve sektördeki diğer paydaşlar arasında daha fazla güven uyanmasını sağlar.[120]

Blok zinciri uygulamalarının suç işlemede kullanılmasının tespit edilmesi ve takip edilmesi içerisinde çeşitli zorluklar barındırmaktadır. Bu zorluklara verilen yanıt ise merkezi olmayan ve esnek uluslararası kuralların devreye alınmasıdır (yumuşak hukuk kuralarının devreye alınması). Yani devletler ve devlet dışı aktörler bu zorlukların üstesinden gelebilmek için çeşitli

[119] **Forgang**, s. 7.
[120] **Financial Crime Academy**, Crypto Money Laundering.

AML uyumlu faaliyetlerin geliştirilmesini teşvik etmişlerdir. Bir yandan, dünyanın çeşitli bölgelerindeki yargı mercileri kendilerini AML uyumlu blok zincir faaliyetleri için meşru merkezler olarak ayırt etmeye çalışmıştır. Örneğin, ABD'de New York Eyaleti, "yıllık risk değerlendirmeleri, tüm işlemlerin on yıllık kayıtları, şüpheli faaliyet raporları, müşteri tanımlama programı, kontroller ve uyumluluk, yıllık iç veya dış denetimler ve raporlamadan kaçınmak veya kimliği gizlemek için yapılandırma yapmamak" taahhütlerini yerine getiren aracı kuruluşlara verilen bir "Bitlicense" geliştirmiştir. Singapur gibi rakip bölgeler de AML uyumlu blok zincir tabanlı faaliyetleri çekmeye çalışmıştır. Singapur'da Şüpheli İşlem Raporlama Ofisi kullanıcı kimliklerini aktif olarak doğrulamakta ve şüpheli işlemleri izlemektedir. İngiliz Kanalı adası Alderney kendisini AML uyumlu bir blok zincir merkezi olarak tanıtmakta ve Man Adası ile "Bitcoin Adası" unvanını almak için rekabet etmektedir. Bunlara benzer olarak bazı kripto varlık aracı kurumlarının da KYC/AML rejimine tabi olmayı gönüllü olarak kabul ve beyan ettikleri ifade edilmektedir.[121]

Kripto varlık aracı kurumları son birkaç yılda KYC/AML'nin benimsenmesinde önemli ölçüde değişiklik göstermişlerdir. Eskiden bir hesaba kaydolmak ve e-posta adresi dışındaki borsalarda çok az ayrıntı tutularak veya hiç bilgi tutulmadan para girişi ve çıkışı mümkündü. Ancak aracı kurumlar artık çok büyük ve kârlı işletmeler haline geldiğinden, gerekli özeni göstermek ve benzer finansal kuruluşlarla uyum sağlamak bu kuruluşlar açısından daha mantıklı hale gelmiştir. Kripto varlık sektörünün üzerinde halen bu alanın düzenlenmemiş olması ve kripto varlık biriminin Silk Road'dan ve karanlık ağdaki erken kullanımlardan kaynaklanan yasa dışı işlerde kullanıldığı algısı halen bulunmaktadır. Sektörün genişlemesine bağlı olarak, büyük finansal kurumlar yatırım yaparken ve artık kripto varlıklar finans endüstrisinde faaliyet gösterirken, öz düzenleme ve düzenli raporlama doğru yönde atılmış bir adım olacaktır. Merkezi borsalar, AML mevzuatının yüksek standartlarına sahip KYC/AML dostu ülkelerde bulunan borsalara dönüşmüştür. Bu alanlarda faaliyet gösteren borsalar, beklenen standartlara uymamanın zorlayıcı düzenleme ihtimalini artıracağının bilincindedir. Aracı kurumlar özenli bir şekilde çalıştırılmamaları halinde müşterilerini riske maruz bırakmaktadırlar. Bu borsalar, nispeten yeni bir borsa olan Binance'ın da gösterdiği gibi, çok büyük miktarda müşteri çekmekte ve aynı dönemde Almanya'nın en büyük bankasının kazandığından (200 milyon dolar) daha yüksek kar açıklamaktadır.[122] Bu nedenle KYC/AML düzenlemelerine uymak kripto varlık aracı kurumların güvenilirlikleri, müşteri çekmek kapasiteleri ve dolayısıyla karlılıkları açısından son derece önemlidir.

[121] **Campbell-Verduyn/Goguen**, s. 78.
[122] **Dyson/Buchanan/Bell**, s. 3.

Suç gelirlerinin aklanmasına karşı ilk savunma hattı olarak kripto varlık hizmet sağlayıcılarının, işletmelerini ve müşterilerini mali suçlardan korumak için sağlam önlemler almaları gerekir. Bunlardan ilki güçlü KYC/AML politikalarının uygulanmasıdır. Güçlü müşterini tanı (KYC) ve suç gelirlerini aklamayı önleme (AML) politikaları uygulamak, aklama risklerini azaltmak isteyen kripto varlık aracı kurumları için önemli bir adımdır. Bu kurumlar, müşterilerini doğru bir şekilde tanımlayıp doğrulayarak ve risk profillerini değerlendirerek, istemeden aklama faaliyetlerini kolaylaştırmadıklarından veya suç faaliyetlerine karışan kişilere hizmet sağlamadıklarından emin olmalıdırlar. Güçlü KYC/AML politikaları, aracı kurumları bir yandan çeşitli idari yaptırımlardan korurken, diğer yandan suç gelirlerinin aklanmasının önlenmesi ile ilgili düzenlemelere uyulması konusunda kararlılık gösterilmesi, müşteriler, yatırımcılar ve diğer paydaşlar arasında güven oluşturur.[123]

İkinci önlem, çalışan eğitimleri ve farkındalık programlarının hayata geçirilmesidir. Çalışan eğitimi ve farkındalık programları, kapsamlı bir aklamayla mücadele stratejisinin önemli bir bileşenidir. Kripto varlık aracı kurumları, personellerinin aklama riskleri hakkında bilgi sahibi olmalarını ve tehlike işaretlerini tespit edebilmelerini sağlayarak hizmetlerinin yasa dışı amaçlarla kullanılma olasılığını en aza indirebilirler.[124]

Bir diğer önlem ise şüpheli faaliyetlerin proaktif izlenmesi ve raporlanmasıdır. Şüpheli faaliyetlerin proaktif olarak izlenmesi ve raporlanması, etkili bir kara para aklamayla mücadele stratejisinin önemli bir parçasıdır. İşlemleri yakından izleyerek ve olağandışı kalıpları veya davranışları belirleyerek, kripto varlık kurumları potansiyel aklama planlarını tespit edebilir ve bunların gerçekleşmesini önlemek için uygun önlemleri alabilirler.[125]

Bu bağlamda kripto varlık alanındaki kilit oyuncular arasında kripto varlık kullanıcıları, kripto varlıklarının ihraççıları/yöneticileri, kripto varlık borsaları, cüzdan sağlayıcıları, ticaret platformları ve kripto madencilik havuzları yer almaktadır. Kripto varlıklarla ilişkili AML/CTF risklerini yeterince azaltmak için, kripto varlık işlemlerinde yer alan belirli kilit oyuncuların düzenlenmeye başlaması ve KYC uygulaması yürütmek, işlemleri izlemek ve gerektiğinde geleneksel finansal araçlar için kullanılan prosedürde olduğu gibi yüksek riskli işlemleri işaretleyen Şüpheli İşlem Raporları düzenlemek için AML/CFT gerekliliklerine tabi olunması hayati bir önem taşımaktadır.[126]

Kripto varlık aracı kurumları, şüpheli faaliyet belirtileri için işlemleri yakından inceleyerek potansiyel aklama işlemlerini tespit etmeli ve

[123] **Financial Crime Academy**, Crypto Money Laundering.
[124] **Financial Crime Academy**, Crypto Money Laundering.
[125] **Financial Crime Academy**, Crypto Money Laundering.
[126] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.

bunların gerçekleşmesini önlemek için uygun önlemleri almalıdır. Aracı kurumlar şüpheli işlemlerin ilgili makamlara bildirilmesi ve ilgili varlıkların dondurulması için bu konudaki yükümlülüklere uymalıdır. Kurumlar ayrıca işlemleri etkin bir şekilde izlemek ve tehlike işaretlerini tespit etmek için gelişmiş araç ve teknolojilere yatırım yapmalı, karmaşık işlem verilerini analiz etmek ve yorumlamak için gerekli uzmanlık seviyesine ulaşmalıdır. Ayrıca bu kurumlar bilgi ve kaynakları paylaşmak için kolluk kuvvetleri ve kripto sektöründeki diğer paydaşlarla iş birliği yapmalıdır. Bu sayede, fonların aklanması ve aklanan fonların izinin sürülebilmesi de dahil olmak üzere aklama faaliyetlerinin tespit edilmesi ve engellenmesi daha kolay olacaktır.[127]

Bu bağlamda kripto varlıklarla yapılan fon işlemlerinin izlenmesi ve şüpheli işlem uyarılarının (kırmızı bayrakların) belirlenmesi, etkili bir aklama karşıtı stratejide mutlaka bulunması gereken unsurlardır. Kripto varlıklara ilişkin suç gelirleriyle mücadele tipolojilerinin oluşturulması, etkin ve verimli AML/CFT uyumluluğu amacıyla şüpheli ve yüksek riskli kripto işlemlerini gösteren kırmızı bayrakların oluşturulmasına yardımcı olacaktır.[128]

Kripto varlık aracı kurumları ve kolluk kuvvetleri arasındaki iş birliği, kripto varlık aklama vakalarının etkili bir şekilde soruşturulması ve kovuşturulması için çok önemlidir. Aracı kurumlar birlikte çalışarak kolluk kuvvetlerine değerli bilgiler ve destek sağlayabilir ve aynı zamanda bu kurumların uzmanlık ve kaynaklardan faydalanılabilirler. Bilgi ve kaynak paylaşımına ek olarak, kripto varlık aracı kurumları ve kolluk kuvvetleri arasındaki iş birliği, şeffaflığı teşvik eden ve yasa dışı faaliyetlere karşı koruma sağlayan politika ve düzenlemelerin şekillendirilmesine de yardımcı olabilir. Her iki taraf da birlikte çalışarak kripto varlık aklama ile ilgili riskleri ve zorlukları daha iyi anlayabilir ve bu büyüyen tehditle mücadele etmek için stratejiler ve araçlar geliştirebilirler.[129]

3. Suç Gelirlerini Belirlemeye Yönelik Soruşturma Araçları ve Teknikleri

Kolluk kuvvetleri, kripto varlıklar aracılığıyla aklama işlemleri ile etkin bir şekilde mücadele edebilmek için suç gelirlerinin izini sürmek ve suç faillerini belirlemek için son teknoloji araçlara ve tekniklere erişmelidir. Kripto varlıkların benzersiz doğası, merkezi olmayan yapıları ve kullanıcılara sağlayabildikleri anonimlik göz önüne alındığında bu husus özellikle çok önemlidir. Suç gelirlerinin izini sürmeye ve takip etmeye yönelik geleneksel yöntemler, bu zorluklar karşısında genellikle yetersiz kalmakta ve kripto alanına özel olarak uyarlanmış gelişmiş soruşturma

[127] **Financial Crime Academy**, Crypto Money Laundering.
[128] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 214.
[129] **Financial Crime Academy**, Crypto Money Laundering.

tekniklerinin geliştirilmesini ve benimsenmesini gerektirmektedir.[130]

Bu araçlar ve teknikler, şüpheli işlem modellerini belirleyebilmeli, potansiyel yasa dışı faaliyetleri saptamalı ve hatta gelecekteki tehditleri tahmin etmek için karmaşık blok zinciri verilerini analiz edebilmelidir. Ayrıca kripto varlık işlemlerinin anonim şekilde yapılması nedeniyle genellikle karmaşık bir süreç olan blok zinciri işlemlerini gerçek dünya kimliklerine bağlamak için bir araç sağlamalıdırlar. Bu araçların kripto teknolojilerinin ve aklama yöntemlerinin hızlı evrimine ayak uydurmak için dinamik ve uyarlanabilir olması gerekir. Suçlular kripto sistemini istismar etmek için yenilikler yapmaya ve yeni stratejiler benimsemeye devam ettikçe, kolluk kuvvetleri soruşturma araçlarının ve tekniklerinin yalnızca güncel değil, aynı zamanda ileriye dönük, ortaya çıkan tehditleri öngörebilecek ve bunlara karşı koyabilecek nitelikte olmasını sağlamalıdır.[131] Bu durum, özellikle yeni müşterileri kabul eden kripto varlık aracı kurumlarının müşterini tanı protokollerinin yetersiz olması halinde geçerlidir. Eğer aracı kurumlar müşterileri hakkında yeterli kayıt tutmuyorsa ya da bilgileri doğrulamak için makul bir girişimde bulunmuyorsa, o zaman kolluk kuvvetlerinin herhangi bir şüpheli faaliyeti araştırmak için yeterli kaynağı olmayacaktır.[132] Nitekim Wall Street Journal'da yer alan bir makaleye göre, *"teknoloji meraklısı suçlular, ABD yasalarına uymayan denizaşırı borsalarda sahte isimlerle giderek daha fazla hesap açmaktadır"*. Hatta Adalet Bakanlığı'ndan eski bir ABD savcısına göre, *"Araştırmacılar blok zinciri analiz ederek fonları takip edebilseler de, bu fonları gerçek dünyadaki bir suçluya bağlayamayabilirler. Mahkeme celplerinde '123 Main Street' adresinde ikamet eden 'Mickey Mouse'un adının yer alması mümkündür"*.[133]

Bu gelişmiş araç ve tekniklere ek olarak, kolluk kuvvetlerinin kapsamlı ve zamanında bilgiye erişmesi gerekir. Bu da kripto varlık aracı kurumları, finans kurumları, düzenleyici kurumlar ve diğer ilgili paydaşlarla yakın iş birliğini gerektirir. Bilgi paylaşımı ve ortak çabalar sayesinde, daha şeffaf ve güvenli bir kripto ortamı yaratılarak suçluların suç gelirlerini aklama ve diğer yasa dışı faaliyetler için istismar etmeleri zorlaştırılabilir.[134]

Kripto varlıklara yapılan aklama işlemlerinin başlangıç ve bitiş noktası (genellikle) para birimlerindeki değişimi içerir. Kolluk kuvvetleri bu alışverişlerde kanıt toplayabilir. Mevcut polisiye tedbirler bunu yapmak için yeterli araçlar sağladığından müdahale etme olasılığı bulunur. Kolluk

[130] **Financial Crime Academy**, Crypto Money Laundering.
[131] **Financial Crime Academy**, Crypto Money Laundering.
[132] **Forgang**, s. 13.
[133] **Corinne Ramey**, "The Crypto Crime Wave is Here: From stickups and drug deals to white-collar scams, cryptocurrency-related crime is soaring—and law enforcement is scrambling to keep up", The Wall Street Journal, 26 Nisan 2018, (Çevrimiçi) https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366, (set) 11.07.2024.
[134] **Financial Crime Academy**, Crypto Money Laundering.

kuvvetleri kripto varlık transferlerinin izini sürmek amacıyla bu varlıkların adreslerini tespit etmeli ve tespit edilen suçluların kripto varlık cüzdanlarına el koymalı ve bunları analiz etmelidir.[135]

Blok zincir analizi ve adli bilişim, kolluk kuvvetlerinin suç gelirlerinin izini sürmesine ve kurtarmasına yardımcı olmada kritik bir rol oynayabilir. Soruşturmacılar blok zincir verilerini inceleyerek şüpheli işlemleri ve kalıpları belirleyebilir ve hatta suç faaliyetlerine karışan kişileri tespit edebilir. Bu, kripto varlık aklama vakalarının yanı sıra diğer mali suç türlerinin soruşturulması ve kovuşturulmasında da çok değerlidir. Bununla birlikte, blok zincir teknolojisinin karmaşıklığı, mevcut veri standartları ve uzman eksikliği de dahil olmak üzere, blok zincir analizi ve adli bilişim ile ilgili bir dizi zorluk vardır. Bu zorlukların üstesinden gelmek için kolluk kuvvetleri gerekli araçlara ve eğitime yatırım yapmalı, bilgi ve kaynakları paylaşmak için kripto endüstrisi ile yakın bir şekilde çalışmalıdır.[136]

Blok zincir tabanlı girişimler, belirli kripto varlık adresleriyle ilişkili kişileri tanımlamada büyük veri analizinden yararlanarak kripto varlık kullanıcılarının profillerini oluşturmada kullanılabilirler. Bitcoin ağı zorunlu olarak şimdiye kadar yapılan tüm işlemlerin geçmişini yayınladığından, bu verilerin analizi belirli düğümler ve bunların işlemsel faaliyetleri hakkında açıklayıcı bilgiler ortaya çıkarabilir. BlockTrail ve Coinanalytics gibi şirketler, belirli kullanım modellerini tespit ederek Europol ve Interpol gibi hükümetler arası polis teşkilatlarının kripto varlık işlemlerini bireysel profillerle eşleştirme becerisini geliştirmektedirler. İşlem akışları, bilgisayar bilimcileri tarafından geliştirilen kripto varlıklara ilişkin adli bilişim araçlarından yararlanılarak belirli kullanıcılarla eşleşen kimliklerle ilişkilendirilir. Bu ve diğer girişimler, blok zincir teknolojilerinin küresel AML yönetişiminin bilgi ve kimlik belirleme çabalarını zayıflatmak yerine katkıda bulunmaya yönelik "işlev gördüğünü" göstermektedir. Ayrıca, yeni teknolojilerin düzenleyici çabalara sadece meydan okumakla kalmayıp aynı zamanda onları nasıl destekleyebileceğini de daha geniş bir şekilde örneklendirmektedir. Bu nedenle blok zincir teknolojisinin paradoksu, AML çabalarının bir yandan "kimliklerin kusurlu bilgisiyle uğraşması" gerekirken, diğer yandan da *"tüm işlemlerin mükemmel bilgisinden yararlanabilmesidir"*.[137]

Kriptografik koruma ve sürekli güncellenen bir kaydı birçok tarafla paylaşma yeteneği DLT'nin birincil yeniliğidir. Blok zinciri gibi dağıtılmış ağlar, tüm ağ faaliyetlerinin şeffaf ve güvenli bir kaydını içeren ortak bir veri tabanı sunar, çünkü kripto varlık işlemlerinin geçmişi deftere kaydedilir, bu işlem değişmezdir (tüm sistemin %51'lik bölümüne yapılan bir saldırı

[135] **van Wegberg/Oerlemans/van Deventer**, s. 431.
[136] **Financial Crime Academy**, Crypto Money Laundering.
[137] **Campbell-Verduyn**, s. 298.

tarafından etkilenmedikçe ki bunun gerçekleşmesi imkansıza yakındır) ve kalıcı kayıtlara yol açar. Bu, halka açık defterlerden büyük miktarda veri toplama yeteneği sağlar ve her işlem adresi ilgili DLT'de, örneğin Bitcoin blok zincirinde aranabilir. Dağıtık defterdeki bilgiler daha sonra kripto varlık adreslerini kripto varlık sahibinin dijital kimliğiyle ilişkilendirmek ve kripto fonlarının kaynağını, faaliyetini ve hedefini araştırmak için kullanılabilir ancak bu DLT analiz yazılımının varlığı halinde mümkün olabilir. DLT analiz yazılımı, adreslerin belirli kullanıcılara atfedilmesine olanak tanır ve fon kaynağı hakkında kapsamlı raporlar sağlar. AML/CFT ve KYC gereklilikleri için kontroller ve risk değerlendirmeleri oluştururken, aynı zamanda diğer ekonomik suçların soruşturulmasına da yardımcı olur. Bu teknolojinin kullanılması, aklama modellerinin (tipolojilerin) geliştirilmesinde ve kırmızı bayrak göstergelerinden oluşan bir havuzun oluşturulmasında kilit rol oynamakta ve kripto varlıklar alanında önleme, gözetim ve adli soruşturmaya yardımcı olmaktadır.[138]

Kripto varlıklar yasa dışı ticareti kolaylaştırmanın yanında, aynı zamanda blok zincirin kamuya açık yapısı nedeniyle yasa dışı faaliyetlerin tespit edilmesini de kolaylaştırmaktadır. Özellikle Bitcoin'in yasa dışı faaliyetlerde yaygın olarak kullanılmış olmasına rağmen bazı yazarlar, her ne kadar kripto varlığın anonim bir yapısı olsa da blok zincirinin aslında kolluk kuvvetlerinin yasa dışı faaliyetleri tespit etmesini kolaylaştırdığını savunmaktadırlar, bu yazarlar bilgisayarlardan blok zincirine aktarılan işlemleri izleyerek, bireysel işlemleri gönderenin IP adresine bağlayabildiklerini göstermişlerdir. [139] Başka araştırmacılar tarafından da blok zincirindeki bir Bitcoin hırsızlığının Bitcoin borsalarına kadar izlenmesinin ve bu yöntemin failleri potansiyel olarak tespit etmek için nasıl kullanılabileceğini açıklamaktadırlar.[140] Bir başka yazar ise Bitcoin'in artan popüleritesinin kaçınılmaz olarak anonimleştirme teknolojileri için büyüyen bir pazara yol açacağını ve bunun da blok zincir ile işlem yapan kullanıcıların şeffaflığının artmasına neden olacağını varsaymaktadır.[141]

---

[138] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 215.

[139] **Philip Koshy/Diana Koshy/Patrick McDaniel**, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic", 18th International Conference on Financial Cryptography and Data Security, Ed: Reihaneh Safavi-Naini/Nicolas Christin, Springer Verlag, Heidelberg, 2014, s. 469-485. Yazarlar makalelerinin özetinde aynen şu ifadeye yer vermişlerdir: "Son 4 yılda, merkezi olmayan bir P2P kripto para birimi olan Bitcoin yaygın bir ilgi görmüştür. Bitcoin kullanarak sözde anonim finansal işlemler oluşturma yeteneği, para birimini gizliliklerine önem veren kullanıcılar için cazip hale getirmiştir. Önceki çalışmalar Bitcoin'in sunduğu anonimlik derecesini kümeleme ve akış analizi kullanarak analiz etmiş olsa da, hiçbiri Bitcoin adreslerini doğrudan IP verileriyle eşleştirme yeteneğini göstermemiştir. Bu tür eşleştirmeleri yalnızca 5 ay boyunca toplanan gerçek zamanlı işlem trafiğini kullanarak oluşturmak ve değerlendirmek için yeni bir yaklaşım öneriyoruz. Bitcoin adresleri ve IP adresleri arasındaki sahiplik ilişkilerini tanımlamak için sezgisel yöntemler geliştirdik. Bu ilişkilerin hangi koşullar altında belirgin hale geldiğini tartışıyor ve anormal aktarım davranışından yararlanarak yaklaşık 1.000 Bitcoin adresinin olası sahip IP'leriyle nasıl eşleştirilebileceğini gösteriyoruz."

[140] **Meiklejohn/Pomarole/Jordan/Levchenko/McCoy/Voelker/Savage**, s. 86-93.

[141] **Yermack**, s. 7–31.

Gelişmiş ve gizleyici kripto stratejilerinin kullanılmasına rağmen, Regtech gibi bazı adli bilişim şirketleri tarafından otomatik DLT analiz yazılım çözümlerinin geliştirilmesi sonucunda karmaşık veri analitiği kullanılarak, yasa dışı karmaşık işlemler izlenerek, kripto varlık işlemleriyle ilgili anonimliğin ortaya çıkarılmasına yardımcı olan güçlü istihbarat araçları setleri sunulmaktadır. Böylelikle kripto varlık işlemleri, AML/CFT ve KYC uyum yükümlülüklerine yardımcı olmak için faaliyet izleme raporları yayınlayan, şüpheli işlemlerin kaynağını ve hedefini görselleştirmeye ve araştırmaya yardımcı olan, şüpheli faaliyetleri ve karanlık ağdan ortaya çıkan tehditleri tespit etmeye yardımcı olan blok zincir analizi çözümleri kullanılarak izlenebilir ve bir bireyin açık anahtar adresine bağlanabilir.[142] Bu görüşlere yanıt olarak, kripto varlık birimleri tarafından sağlanan anonimliğin destekçileri, kolluk kuvvetlerinin tespit yöntemlerine meydan okuyan yeni para birimlerini geliştirmektedirler. Bunlar arasında, kullanıcının açık anahtarlarını aynı tutarı içeren bir grup açık anahtar ("halka imzalar" olarak bilinen)[143] arasında gizleyen Monero[144] ve göndereni, alıcıyı ve işlem tutarını gizleyerek kanıt bırakmayan Zcash[145] bulunmaktadır, nitekim sonuncusunun "Z" harfi "sıfır" anlamına gelen "zero"dan kaynaklanmak ve sıfır bilgi verdiği anlamına gelmektedir.[146]

---

[142] **Buttigieg/Efthymiopoulos/Attard/Cuyle**, s. 215.

[143] "Halka imza, veri gizliliği ve kullanıcı kimliği gizliliği sağlar. Halka imza, mesajları imzalamak için asimetrik anahtarlarla sağlanan bir grup kullanıcıya (halka olarak adlandırılır) dayanan bir kriptografik dijital imza türüdür. Bir mesaj imzalandıktan sonra, yalnızca halka imza ile şifresi çözülebilir ve grup içinde mesajın gerçek imzacısını tespit edemeyiz. Uygulama örneği olarak, Ring CryptoNote protokolü, merkezi olmayan kripto para birimi Monero'daki işlem ayrıntılarını (örneğin, miktar, kaynak, hedef) gizler. Ancak halka imza, kullanıcı kimliklerini yönetmek için bir TTP (Trusted Third Party / Güvenilir Üçüncü Taraf) gerektirir ve dijital sertifikalar nedeniyle halka imzanın hem üretim hem de doğrulama maliyeti artar. Kimlik tabanlı halka imza bu sorunların üstesinden gelir ve kullanıcıların gizliliğini artırır. Ayrıca tam anahtar açığa çıkarma saldırısına karşı da önlem alır". Bkz. **Sidra Aslam/ Aleksandar Tošić/Michael Mrissa**, "Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions", Journal of Cybersecurity and Privacy, Vol. 1, 2021, s. 171.

[144] Ayrıntılı bilgi için bkz. **Shen Noether**, "Ring Signature Confidential Transactions for Monero". IACR Cryptology ePrint Archive, 2015, (Çevrimiçi) https://eprint.iacr.org/2015/1098, (set) 16.07.2024.

[145] Ayrıntılı bilgi için bkz. **Eli Ben Sasson/Alessandro Chiesa/Christina Garman/Matthew Green/ Ian Miers/Eran Tromer/Madars Virza**, "Zerocash: Decentralized Anonymous Payments from Bitcoin", IEEE Symposium on Security and Privacy, 2014, (Çevrimiçi) https://ieeexplore.ieee.org/document/6956581, (set) 16.07.2024. "Bu kripto varlık da adını tam olarak "zero knowledge proof (ZKP)" kavramından almaktadır. Sıfır bilgi kanıtı (ZKP), bir varlığın (kanıtlayıcı) başka bir varlığa (doğrulayıcı), kanıtın kendisinin doğru olması dışında herhangi bir bilgi vermeden belirli bir değerin doğru olduğunu kanıtlamasına olanak tanır. Zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), her iki taraf (kanıtlayan ve doğrulayan) arasında herhangi bir etkileşim olmadan bilginin doğru hesaplandığını kanıtlamaya izin veren bir ZKP'dir. ZKP tabanlı çözümler özellikle veri bütünlüğü ve kimlik doğrulama için ilgi çekicidir, çünkü bir ifadenin kanıtını o ifadeyi ifşa etmeden sağlarlar. Ayrıca hassas veriler için anonimliği korurlar ve TTP'ye dayanmazlar. Bununla birlikte, kanıtları doğrulamak ve oluşturmak için diğer çözümlere kıyasla hesaplama açısından oldukça yoğundurlar." Bkz. **Aslam/Tošić/ Mrissa**, s. 171; **van Wegberg/Oerlemans/van Deventer**, s. 423, 424.

[146] **Foley/Karlsen/Putnins**, s. 8, 9.

Foley, *Karlsen* ve *Putnins* araştırmalarının sonuçlarının yer aldığı makalelerinde, kolluk güçlerine yardımcı olacağını ifade ettikleri teknikleri açıklamaktadırlar. Buna göre, ağ kümesi analizi ve tespit kontrollü tahmin tekniklerinden yararlanarak Bitcoin'deki yasa dışı faaliyetlerin belirlenmesine yönelik yeni yaklaşımların geliştirilmesi ve bu yöntemlerin kolluk kuvvetleri tarafından gözetim faaliyetlerinde kullanılması mümkündür. Örneğin, bu yöntemler yeni bloklar oluşturuldukça blok zinciri verilerine uygulanabilir ve yetkililerin Bitcoin'deki yasa dışı faaliyetleri izlemelerini sağlayabilir. Bu tür bilgiler, hali hazırda son derece az olan düzenleme ve uygulama kaynaklarının daha etkin kullanılmasına yardımcı olabilir. Yazarlar araştırmalarını yaparken, "gizlilik coinleri" olarak da bilinen Monero, Dash ve Zcash gibi bir dizi kripto varlık birimi ortaya çıkmış ve yasa dışı kullanıcılar arasında bir dereceye kadar benimsenmiştir. Örneğin, bazı darknet pazarları ödemeler için Monero'yu kabul etmeye başlamış bu da yazarların tahminine göre Bitcoin'deki yasa dışı faaliyet miktarını azaltmıştır. Yazarlar gizlilik coin'lerinin daha da geliştirilmesinin, yasa dışı faaliyetleri tespit etmeyi zorlaştıracağını ifade etmekle birlikte, bugüne kadar başlıca gizlilik coin'lerinin kullanıcılarına tam bir gizlilik sunmakta yetersiz kaldığını belirtmektedirler. Bilgisayar bilimi araştırmacıları, çeşitli sezgisel yöntemler ve kümeleme algoritmaları kullanarak Monero ve ZCash gibi popüler gizlilik coinlerinde kullanıcı düzeyinde kayıtları ve işlem faaliyetlerini yeniden oluşturabilmiştir. Bu tür bulgulara dayanarak, gizlilik coinlerinin belki de amaçlandıkları kadar gizlilik sağlamadığı görülmektedir. Bu nedenle yazarlar, yasa dışı faaliyetler Monero ve Zcash gibi popüler gizlilik coinlerine kaymaya devam etse bile, kolluk kuvvetleri ve araştırmacıların gizlilik coinleri ve Bitcoin Cash, Litecoin ve Ethereum gibi gizlilik içermeyen coinler de dahil olmak üzere çeşitli kripto varlıklarla işlenen suçların araştırılması için kendi yaklaşımlarını kullanabileceklerini iddia etmektedirler.[147]

Blok zincir analizine ek olarak, suç gelirlerini aklama planlarını ortaya çıkarmak ve bu faaliyetlerden sorumlu kişileri belirlemek için mali soruşturmalar ve geleneksel teknikler de kullanılabilir. Araştırmacılar mali kayıtları analiz ederek, işlemlerin izini sürerek ve şüphelilerle görüşerek suç gelirlerini aklama planlarının altında yatan karmaşık işlemler ağını bir araya getirebilir ve suçluları adalete teslim edebilir. Ancak, mali soruşturmaların ve geleneksel tekniklerin kullanılması, kripto varlık yoluyla aklamanın yarattığı zorlukların üstesinden gelmek için tek başına yeterli olmayabilir. Bu tehditle etkin bir şekilde mücadele edebilmek için kolluk kuvvetlerinin yeni araç ve teknolojileri de benimsemesi gerekir, bu tekniklere şunlar örnek verilebilir: Blok zincir analizi, makine öğrenimi algoritmaları, veri analitiği ve yapay zekâ yazılımları. Ayrıca, kripto varlığı aklamayı önlemek ve tespit etmek için yenilikçi çözümler geliştirmenin yanı sıra bilgi ve kaynakları

[147] **Foley/Karlsen/Putnins**, s. 33, 34.

paylaşmak için kripto endüstrisi ile iş birliği çok önemlidir.[148]

Kripto varlık hizmet sağlayıcıları, cüzdan sağlayıcıları ve diğer hizmet sağlayıcıları gibi kripto sektörü paydaşlarıyla iş birliği, kripto varlık yoluyla aklama vakalarının etkili bir şekilde soruşturulması ve kovuşturulması için çok önemlidir. Kolluk kuvvetleri ve kripto endüstrisi birlikte çalışarak aklama faaliyetlerini tespit etmek ve engellemek için kaynaklarını ve uzmanlıklarını bir araya getirebilir ve sorumlu kişilerin adalete teslim edilmesini sağlayabilir. Bilgi ve kaynak paylaşımına ek olarak, kolluk kuvvetleri ve kripto endüstrisi arasındaki iş birliği, yasa dışı fonların izini sürmek ve suç gelirlerinin aklanmasıyla mücadele etmek için yeni araç ve tekniklerin geliştirilmesine de katkıda bulunabilir. Kripto ekosisteminin şeffaf, güvenli ve suç faaliyetlerinden uzak kalması sağlanabilir.[149]

Sonuç olarak, kripto varlıkların aklanması finans dünyası için önemli bir tehdittir ve bununla ancak kolluk kuvvetleri, düzenleyiciler ve kripto endüstrisinin ortak çabalarıyla etkin bir şekilde mücadele edilebilir. Sağlam KYC/AML politikaları uygulayarak, şüpheli faaliyetler için işlemleri izleyerek, bilgi ve kaynakları paylaşmak için birlikte çalışarak, kripto ekosisteminin şeffaf, güvenli ve suç faaliyetlerinden uzak kalması sağlanabilir. Kripto varlık dünyası sürekli gelişirken, suç gelirlerini aklamayı önleme ve finansal sistemin bütünlüğünü koruma çabalarında uyanık ve proaktif olmak çok önemlidir.[150]

Ülkemizde Yapılan Düzenleme

Bu makalenin konusunu suç gelirlerinin aklanmasında kripto varlıkların kullanılması oluşturduğu için daha fazla ayrıntıya girmiyoruz, zira bu düzenleme bir başka makalenin konusunu oluşturacak genişlikte ve önemdedir. Ancak biz ülkemiz kanun koyucusunun kripto varlıkların gelişimi konusunda duyarsız kalmadığını ortaya koymak için kısa bir bilgi vermeyi tercih ettik.

Ülkemizde giriş kısmında da bahsettiğimiz üzere 26.06.2024 tarihli ve 7518 sayılı Kanun ile 06.12.2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu'nda (SPK) yapılan düzenleme ile kripto varlıklar ve kripto varlık aracı kurumları düzenlenmiştir.

SPK'nın 3. maddesine eklenen bentler ile "cüzdan, kripto varlık, kripto varlık hizmet sağlayıcı, kripto varlık saklama hizmeti, platform" gibi kripto varlık sektörüne ilişkin kavramlar tanımlanmıştır. Buna göre cüzdan, *"kripto varlıkların transfer edilebilmesini ve bu varlıkların ya da bu varlıklara ilişkin özel ve açık anahtarların çevrim içi veya çevrim*

[148] **Financial Crime Academy**, Crypto Money Laundering.
[149] **Financial Crime Academy**, Crypto Money Laundering.
[150] **Financial Crime Academy**, Crypto Money Laundering.

dışı olarak depolanmasını sağlayan yazılım, donanım, sistem ya da uygulamalar"; kripto varlık, *"dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan ve değer veya hak ifade edebilen gayri maddi varlıklar"*; kripto varlık hizmet sağlayıcı, *"platformları, kripto varlık saklama hizmeti sağlayan kuruluşları ve bu Kanuna dayanılarak yapılacak düzenlemelerde kripto varlıkların ilk satış ya da dağıtımı dâhil olmak üzere kripto varlıklarla ilgili olarak hizmet sağlamak üzere belirlenmiş diğer kuruluşları"*; kripto varlık saklama hizmeti, *"platform müşterilerinin kripto varlıklarının veya bu varlıklara ilişkin cüzdandan transfer hakkı sağlayan özel anahtarların saklanmasını, yönetimini veya Kurulca belirlenecek diğer saklama hizmetlerini"*, platform, *"kripto varlık alım satım, ilk satış ya da dağıtım, takas, transfer, bunların gerektirdiği saklama ve belirlenebilecek diğer işlemlerin bir veya daha fazlasının gerçekleştirildiği kuruluşlar"* olarak tanımlanmıştır. Böylelikle hukukumuzda kripto varlıklarla ilgili temel hususlar bu konudaki yerleşik bilgi birikimiyle uyumlu bir şekilde tanımlanmıştır.

Bu tanımların dışında özellikle SPK'ya eklenen 35/B maddesi ile kripto varlık aracı kurum açmanın ve işletmenin şartları sıkı bir şekilde düzenlenmiş, bu kuruluşların açılmasının ve denetlenmesinin Sermaye Piyasası Kurulu tarafından yapılacağı belirtilmiş, bu kuruluşların açılması için gerekli olan asgari standartlar belirlenmiştir. Kanun'a eklenen 35/C maddesiyle bu kripto varlık işlemlerinin nasıl gerçekleştirileceği düzenleme altına alınmıştır. Ayrıca diğer maddelerin yanı sıra 99/A ve 99/B maddeleri ile izinsiz faaliyetlerde bulunanlara ilişkin yaptırımlar ile bu kuruluşların denetiminin nasıl yapılacağı düzenlenmiştir.

Söz konusu düzenlemenin ceza hukuku ile ilgili boyutu ise SPK'nın 109/A maddesinde düzenlenen "İzinsiz kripto varlık hizmet sağlama suçu" ve 110/A maddesinde düzenlenen "Kripto varlık hizmet sağlayıcılarda zimmet suçu" ile gerçekleşmiştir. Dolayısıyla bu Kanun'un yürürlüğe girdiği andan itibaren bu eylemleri gerçekleştirenler yukarıdaki suçlardan cezalandırılacaklardır. Böylelikle bu konuda öğreti de uygulama yer alan tartışmalara ve özellikle suçta ve cezada kanunilik ilkesine aykırı uygulamalara bir son verilmek istenmiştir.

Görüldüğü üzere bu Kanun'da kripto varlıkların suç gelirlerinin aklanmasında kullanılmasına ilişkin bir düzenleme bulunmamaktadır, zira buna gerek de yoktur. TCK'nın 282. maddesinde yer alan aklama suçu zaten kapsam bakımından elverişlidir ve her hareketi içerek kadar geniş düzenlenmiştir. Ayrıca kripto varlıkların bu suçun işlenmesinde kullanılması yeni bir suç değil mevcut bir suçun yeni bir işleniş modelidir. Ancak SPK'da yapılan düzenlemeler ile kripto varlıkların arzının, işleyişinin ve aracı kurumların düzenleme altına alınması ve özellikle denetim ve gözetim organı olarak Sermaye Piyasası Kurulu'nun belirlenmesi potansiyel suç

gelirlerinin aklanması eylemlerinin takip edilmesi bakımından son derece önemlidir. Zira böylelikle MASAK, Sermaye Piyasası Kurulu aracılığıyla ve tabii ki kendisi doğrudan bu aracı kurumlar üzerinde KYC/AML rejimini uygulayabilecektir. Bu nedenle bu Kanun'u hem kripto varlık sektörüne bir düzen getirerek geçmişte yaşanmış büyük mağduriyetlerin önlenmesi hem de suç gelirlerinin aklanması ve terörizmin finansmanın önlenmesi rejimine ilişkin kuralların uygulanabilmesi açısından son derece yerinde ve olumlu bulduğumuzu ifade etmeliyiz.

Suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadelede kilit konumda olan ve KYC/AML rejimin uygulanmasını sağlayan düğüm noktaları yukarıda da ifade ettiğimiz üzere fon transferi ya da işlemlerini sağlayan aracı kurumlardır. Bunlar hukukumuzda daha geniş bir alanı kapsayacak şekilde "yükümlüler" olarak tanımlanmaktadır. 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. maddesinde belirlenmiştir. Tedbirler Yönetmeliğinin 4. maddesinin 1. fıkrasına 01.05.2021 tarihli ve 31471 sayılı Resmî Gazete'de yayımlanan Yönetmelik değişikliği ile eklenen (ü) bendine göre, "kripto varlık hizmet sağlayıcılar" anılan tarih itibarıyla yükümlüler arasına alınmıştır.

Nitekim yükümlülerin *"suçla mücadelede Mali Suçları Araştırma Kurulunun en önemli paydaşı konumunda"* olduğu MASAK'ın kripto varlık hizmet sağlayıcıları için çıkardığı Mayıs 2021 tarihli "Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklere İlişkin Temel Esaslar" başlıklı rehberinde[151] açıkça ifade edilmektedir.

Kripto varlık hizmet sağlayıcıların tabi oldukları yükümlülükler; müşterinin tanınması, şüpheli işlem bildirimi, bilgi ve belge verme, devamlı bilgi verme ile muhafaza ve ibrazdır. Bu yükümlülüklerin yerine getirilmemesi çeşitli idari para cezalarını gerektirmektedir.

Görüldüğü üzere kripto varlıkların ve aracı kurumların Kanun ile düzenlenmesinden önce MASAK aracı kurumları yükümlüler kapsamına almıştır. Bu varlıkların ve aracı kurumların Kanun ile düzenlemesinden sonra MASAK'ın getirdiği bu yükümlülükler daha ciddi bir şekilde uygulanabilecektir.

SONUÇ

Kripto varlıklar yalnızca dijital olarak var olan, genellikle merkezi bir ihraç veya düzenleme otoritesi olmayan, bunun yerine işlemleri kaydetmek için merkezi olmayan bir sistem kullanan dijital varlık birimidir. Kripto varlık

[151] (Çevrimiçi) https://masak.hmb.gov.tr/rehberler, (set) 17.07.2024, s. 6.

birimleri, güvenilir üçüncü tarafların aracılığı veya gözetimi olmamasına rağmen, işlem bütünlüğünü ve hızını sağlamak için kriptografik ilkeleri kullanan küresel, kalıcı ve sansürsüz bir dijital ortamda çalışır. Aslında, anonim kullanıcılara ve merkezi olmayan yönetime dayalı, hesap verebilirlik olmaksızın, herhangi bir yerden izin almak gerekmeksizin DLT üzerinde çalışan kripto varlıkların, geleneksel ödeme yöntemlerine kıyasla suç gelirlerinin aklanması için kullanılma potansiyeli daha yüksektir ve kötüye kullanıma daha açıktır.

Kural olarak kripto varlıkların bulundurulması ve kullanılması suç oluşturmamakla birlikte, bu ifade söz konusu varlıkların suç işlemekte kullanılmayacağı anlamına gelmez. Bu araçlar başta ekonomik çıkar amacıyla işlenen suçlar olmak üzere birçok suçun işlenmesinde kullanılabilir. Nitekim son günlerde ülkemizde kripto varlıkların sürekli olarak çeşitli suçlarla birlikte anılması da bu yüzdendir.

Kripto varlıklar, daha çok ve sıklıkla suç gelirlerinin aklanması ve terörizmin finansmanı suçlarıyla anılmaktadır. Bunun nedeni ise bu araçların aklama işlemlerinde gerekli olan anonimlik ve takip güçlüğü gibi özellikleri barındırmasıdır. Nitekim kripto varlıkların sağladığı anonimlik ve düzenleme eksikliğinin, suç gelirlerinin aklanması, vergi kaçakçılığı, uyuşturucu kaçakçılığı ve diğer suç faaliyetlerini kolaylaştırdığı yönünde ciddi endişeler söz konusudur. Bu konudaki bir diğer önemli faktör de kripto varlıklarla yapılan işlemlerin tek bir yargı yetkisi alanına girmemesi ve merkezi bir aracının bulunmamasıdır. Bu durum söz konusu teknolojik yenilikten kaynaklanan suç faaliyetlerinin düzgün bir şekilde kontrol altında tutulmasını, kayıt altına alınmasını ve dolayısıyla soruşturulmasını ve yargılamasını zorlaştıran hukuki bir belirsizlik ortamı yaratmaktadır.

Suçlular kripto varlıkları kullanarak aklama faaliyetine giriştiklerinde genellikle kripto varlık tamburları (tumbler), karıştırma hizmetleri (mixer), eşler arası ağlar (P2P), OTC brokerleri ve DeFi platformlarının istismarı gibi çeşitli yöntemleri kullanmaktadırlar. Yaklaşımları farklı olsa da bu yöntemlerin hepsi aynı amaca, suç gelirlerinin asıl kaynağını gizleyerek kolluk kuvvetlerinin izini sürmesini zorlaştırmaya hizmet etmektedirler.

Kripto varlıkların suç gelirlerinin aklanmasına kullanılması yönelik önemli bir potansiyeli vardır. Ancak bu, potansiyelin gerçeğe dönüştüğü anlamına gelmemektedir. Bu nedenle teknolojinin ve kripto varlık ekosisteminin varlığı ve gelişimi sırf bu potansiyel nedenden dolayı engellenmemeli ve yok edilmemelidir. Ayrıca bu tür bir teknolojinin tamamen yasaklanması halinde bunun yer altına inebileceği gerçeği de unutulmamalıdır.

Dünyada suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadelede öne çıkan ve öncü rol üstlenen kuruluş FATF'dir. Bu nedenle FATF, çalışmaları ve bu alana özgü çıkarttığı rehberler ile tüm

dünyada suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadele konusunda mevzuat yapıcı ve uygulayıcılar açısından yol göstericidir. FATF üstlendiği bu rol ve bundan aldığı güçle kripto varlıkların suç gelirlerinin aklanmasında ve terörizmin finansmanında kullanılmasına ilişkin çeşitli rehberler yayınlamıştır. FATF'nin bu rehberlerinden varılan sonuç, kuruluşun kendisinin de açıkça ifade ettiği üzere kripto varlıklara "risk temelli" yaklaşmaktır.

FATF'nin risk temelli yaklaşımını yerinde bulduğumuzu ifade etmeliyiz. Ancak bu bakış açısı FATF açısından bir yasaklama anlamına gelmediği gibi FATF'nin bu konudaki yaklaşım ve tavsiyelerine uyum sağlayacak ülkeler açısından yasakçı bir zihniyete dönüşmemelidir. Risk temelli yaklaşım doğrudur zira günümüzde kripto varlıklar suç gelirlerinin aklanmasında abartıldıkları kadar yoğun kullanılmamaktadır ancak kontrol altına alınmaz ise bu potansiyeli taşıdığı bir gerçektir. Bundan dolayı FATF bu potansiyel duruma yönelik risk temelli bir yaklaşım geliştirmiştir.

FATF'nin son tahlilde gerekirse kripto varlık faaliyetlerinin tamamen yasaklanmasına ilişkin aşırı yaklaşımını benimsemediğimizi ifade etmeliyiz. Bunun iki nedeni bulunmaktadır: Birincisi bu tür yasaklama teknolojinin önüne ket vurmak anlamına gelir. Bu ise inovasyonu ve daha iyi ve refah içinde yaşamının yollarını arayışa ilişkin çalışmaların yapılmasını engeller. Bu yasaklamalar bir kere başladı mı çeşitli gerekçelerle her yerde görülmeye başlar, bu ise bilimin, teknolojinin ve insanlığın gelişiminin engellenmesi anlamına gelir. İkinci olarak bu şekilde normatif bir yasaklamanın gerçek yaşamda bir karşılığının olmayacağıdır yani bu tür yasaklayıcı bir norm sosyal etkililik açısından başarısız olmaya mahkûmdur.

Suç gelirlerini aklayanlar çeşitli suç faaliyetlerinden elde ettikleri fonları aklamak için kripto varlıkları giderek daha fazla kullanmaktadırlar. Bu yasa dışı fonları kaynağına kadar takip etmek, kolluk kuvvetleri için zorlu bir görev haline gelmiştir çünkü kolluk güçleri genellikle kripto varlıkların özelliklerine uygun olmayan geleneksel soruşturma yöntemlerini kullanmaktadırlar. Nitekim suç gelirlerini aklamanın; yerleştirme, katmanlama ve bütünleme aşamalarında kripto varlıkların kullanılması aklama işlemlerini daha da karmaşık ve takibi zor hale getirmektedir. Suçlular, haksız kazançlarının kaynağını gizlemek için kripto varlık tamburları (tumbler) ve karıştırma hizmetlerinden (mixer) yararlanmakta, bu da kolluk güçlerinin paranın izini takip etmesini ve suç faillerini belirlemesini zorlaştırmaktadır.

Kolluk kuvvetleri, kripto varlıklar aracılığıyla aklama işlemleri ile etkin bir şekilde mücadele edebilmek için suç gelirlerinin izini sürmek ve suç faillerini belirlemek için son teknoloji araçlara ve tekniklere erişmelidir. Kripto varlıkların benzersiz doğası, merkezi olmayan yapıları ve kullanıcılara sağlayabildikleri anonimlik göz önüne alındığında bu husus özellikle çok önemlidir. Suç gelirlerinin izini sürmeye ve takip etmeye

yönelik geleneksel yöntemler, bu zorluklar karşısında genellikle yetersiz kalmakta ve kripto alanına özel olarak uyarlanmış gelişmiş soruşturma tekniklerinin geliştirilmesini ve benimsenmesini gerektirmektedir.

Bu gelişmiş araç ve tekniklere ek olarak, kolluk kuvvetlerinin kapsamlı ve zamanında bilgiye erişmesi gerekir. Bu da kripto varlık aracı kurumları, finans kurumları, düzenleyici kurumlar ve diğer ilgili paydaşlarla yakın iş birliğini gerektirir. Bilgi paylaşımı ve ortak çabalar sayesinde, daha şeffaf ve güvenli bir kripto varlık ortamı yaratılarak suçluların suç gelirlerini aklama ve diğer yasa dışı faaliyetler için istismar etmeleri zorlaştırılabilir. Ülkemizde 26.06.2024 tarihli ve 7518 sayılı Kanun ile 06.12.2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu'nda (SPK) yapılan düzenleme ile kripto varlıklar ve kripto varlık aracı kurumları düzenlenmiştir. Söz konusu düzenlemenin ceza hukuku ile ilgili boyutu ise SPK'nın 109/A maddesinde düzenlenen "İzinsiz kripto varlık hizmet sağlama suçu" ve 110/A maddesinde düzenlenen "Kripto varlık hizmet sağlayıcılarda zimmet suçu" ile gerçekleşmiştir. Dolayısıyla bu Kanun'un yürürlüğe girdiği andan itibaren bu eylemleri gerçekleştirenler yukarıdaki suçlardan cezalandırılacaklardır. Böylelikle bu konuda öğreti de uygulama yer alan tartışmalara ve özellikle suçta ve cezada kanunilik ilkesine aykırı uygulamalara bir son verilmek istenmiştir.

Görüldüğü üzere bu Kanun'da kripto varlıkların suç gelirlerinin aklanmasında kullanılmasına ilişkin bir düzenleme bulunmamaktadır, zira buna gerek de yoktur. TCK'nın 282. maddesinde yer alan aklama suçu zaten kapsam bakımından elverişlidir ve her hareketi içerek kadar geniş düzenlenmiştir.

Suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadelede kilit konumda olan ve KYC/AML rejimin uygulanmasını sağlayan düğüm noktaları fon transferi ya da işlemlerini sağlayan aracı kurumlardır. Bunlar hukukumuzda daha geniş bir alanı kapsayacak şekilde "yükümlüler" olarak tanımlanmaktadır. Tedbirler Yönetmeliğinin 4. maddesinin 1. fıkrasına 01.05.2021 tarihli ve 31471 sayılı Resmî Gazete'de yayımlanan Yönetmelik değişikliği ile eklenen (ü) bendine göre, "kripto varlık hizmet sağlayıcılar" anılan tarih itibarıyla yükümlüler arasına alınmıştır

Kripto varlık hizmet sağlayıcıların tabi oldukları yükümlülükler; müşterinin tanınması, şüpheli işlem bildirimi, bilgi ve belge verme, devamlı bilgi verme ile muhafaza ve ibrazdır. Bu yükümlülüklerin yerine getirilmemesi çeşitli idari para cezalarını gerektirmektedir.

Özetle hem fırsatlar hem de riskler barındıran kripto varlıkların bir yandan suç gelirlerinin aklanmasında ve terörizmin finansmanında kullanılması önlenmeye çalışılmalı bir yandan da bu teknolojik gelişimin ve bundan sağlanan faydaların önü tıkanmamalıdır. Şu ana kadar ülkemiz mevzuatının bu görüşümüz doğrultusunda şekillendiğini görmek memnuniyet vericidir.

KAYNAKÇA

1. **Akbulut,** Berrin, "Kripto Para ve Terörizmin Finansmanı", Karşılaştırmalı Hukukta ve Türk Hukukunda Terörizm, Terör Suçları ve İnfaz Hukuku, ed. İzzet Özgenç, I. Cilt, Türkiye Bilimler Akademisi, Ankara, 2024.
2. **Aslam,** Sidra / Tošić, Aleksandar / Mrissa, Michael, "Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions", Journal of Cybersecurity and Privacy, Vol. 1, 2021.
3. **Balcı,** Murat / Çakır, Kerim, Kripto Paraların Karapara Aklama Yöntemi Olarak Kullanılması, CHD, Yıl: 16, Sayı: 46, Ağustos, 2021.
4. **Brown,** Steven David, "Cryptocurrency and Criminality: The Bitcoin Opportunity", The Police Journal, Vol. 89, Issue 4, 2016.
5. **Buttigieg,** Christopher P. / Efthymiopoulos, Christos/Attard, Abigail /Cuyle, Samantha, "Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State," Law and Financial Markets Review, Vol. 13, No. 4, 2019.
6. **Çakır,** Kerim, Suçtan Kaynaklana Malvarlığı Değerlerini Aklama Suçu, 2. Baskı, Adalet Yayınevi, Ankara, 2023.
7. **Campbell-Verduyn,** Malcolm, "Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance" Crime, Law and Social Change V. 69, No. 2, March 2018.
8. **Durdu,** Erdal, Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku, Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2018.
9. **Duyne,** Petrus C. van / Lampe, Klaus von / Passas, Nikos, (eds.) Upperworld and Underworld in Cross-Border Crime, Wolf Legal Publishers, Nijmegen, 2002; FATF, 2015: 6.
10. **Dülger,** Murat Volkan / Özkan, Onur, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi", Prof. Dr. Mehmet Emin Artuk'a Armağan, Ed. Mahmut Koca, Seçkin Yayıncılık, Ankara, 2020.
11. **Dyntu,** Valeriia / Dykyi, Oleh, "Cryptocurrency in the System of Money Laundering", Baltic Journal of Economic Studies, Vol. 4, No. 5, 2018.
12. **Dyson,** Simon / Buchanan, William J. / Bell, Liam, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime", The Journal of British Blockchain Association, Volume 1, Issue 2, 2018.
13. **Forgang,** George, Money Laundering Through Cryptocurrencies, Unpublished Master of Science Thesis, La Salle University Economic Crime Forensics Capstones 40, 2019, s. 4 (Çevrimiçi) https://digitalcommons.lasalle.edu/ecf_capstones/40, (set) 15.06.2024.

14. **Greenberg,** Arnold, (2018, April 23). "The Dark Web's Favorite Currency Is Less Untraceable Than It Seems", Wired, 23 Nisan 2018, (Çevrimiçi) https://www.wired.com/story/monero-privacy/ (set) 10.07.2024.

15. **Griswold,** Alison, "The First-Ever Bitcoin Purchase Was Remarkably Inglorious" Slate, 23 Mayıs 2014, https://slate.com/business/2014/05/first-bitcoin-purchase-twopepperoni-pizzas-from-papa-john-s.html.

16. **Işık,** Hüseyin, "Mali Eylem Görev Gücü'nün (FATF) Gri Listesi ve Türkiye", International Journal of Public Finance, Vol. 7, No. 2, 2022**.**

17. **Jacobs,** Garry, "Cryptocurrencies & The Challenge of Global Governance", Cadmus, Vol. 3, Issue 4, Mayıs 2018, (çevrimiçi) https://cadmusjournal.org/, (set) 11.07.2024.

18. **Jia,** Kai / Zihang, Falin, "Between Liberalization and Prohibition Prudent Enthusiasm and the Governance of Bitcoin/blockchain Technology", in: Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018.

19. **Kharif,** Olga, "Bitcoin is being dropped by criminals in favour of privacy coins like monero", Independent, 2 Ocak 2018, (Çevrimiçi) https://www.independent.co.uk/news/business/analysis-and-features/bitcoin-latestupdates-price-privacy-coins-cryptocurrency-monero-digital-currency-pricea8137901.html, (set) 10.07.2024.

20. **Keech,** Elliott Maurice Nathaniel, "Crime, Innovation, and The Technology of Moneys", Unpublished PhD Thesis, University of York, York Law School, York, 2022.

21. **Kethineni,** Sesha / Cao, Ying / Dodge, Cassandra, "Use of Bitcoin in Darknet Markets: ExaminingFacilitative Factors on Bitcoin-Related Crimes", American Journal of Criminal Justice, Vol. 43, Issue 2, Mayıs 2017.

22. **Koshy,** Philip / Koshy, Diana / McDaniel, Patrick, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic", 18th International Conference on Financial Cryptography and Data Security, Ed: Reihaneh Safavi-Naini/Nicolas Christin, Springer Verlag, Heidelberg, 2014.

23. **Kurzweil,** Ray, The Singularity is Near: When Humans Transcend Biology, Penguin, London, 2005.

24. **Malwa,** Shaurya, "$1.2 Billion in Cryptocurrency Laundered Through Bitcoin Tumblers, Privacy Coins", 6 Temmuz 2018, (Çevrimiçi) https://finance.yahoo.com/news/1-2-billion-cryptocurrency-laundered-224521652.html, (set) 11.07.2024.

25. Manna, Michele, The Bonfire of Banknotes, Mercati, Infrastrutture, Sistemi di Pagamento (Markets, Infrastructures, Payment Systems) Approfondimenti (Research Papers), No. 25 Banca d'Italia, Rome, 2022.

26. Matthewman, Steve, Technology and Social Theory, Palgrave Macmillan, London, 2011.

27. Mayer, Maximilian / Carpes, Mariana / Knoblich, Ruth, (eds.), The Global Politics of Science and Technology – Vol. 1, Concepts from International Relations and Other Disciplines, Springer, New York, 2014.

28. Mayer, Maximilian / Carpes, Mariana / Knoblich, Ruth, (eds.), The Global Politics of Science and Technology – Vol. 2, Perspectives, Cases and Methods, Springer, New York, 2014.

29. Meiklejohn, Sarah / Pomarole, Marjori / Jordan, Grant / Levchenko, Kirill / McCoy, Damon / Voelker, Geoffrey M. / Savage, Stefan, "A Fistful of Bitcoins: Characterizing Payments among Men with No Names", Communications of the ACM, Vol. 59, Issue 4, Nisan 2016.

30. Möser, Malte / Böhme, Rainer, "Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques", 2017 IEEE European Symposium on Security and Privacy: Workshops (EuroS&PW), 2017.

31. Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 30 Ekim 2008, (Çevrimiçi) https://bitcoin.org/bitcoin.pdf, (set) 11.07.2024 **.**

32. Nasdaq, "Know Your Coins: Public vs. Private Cryptocurrencies", 22 Eylül 2017, (Çevrimiçi) https://www.nasdaq.com/articles/know-your-coins-public-vs-private-cryptocurrencies-2017-09-22, (set) 10.07.2024.

33. Noether, Shen, "Ring Signature Confidential Transactions for Monero". IACR Cryptology ePrint Archive, 2015, (Çevrimiçi) https://eprint.iacr.org/2015/1098, (set) 16.07.2024.

34. Prendi, Llambi / Borakaj, Daniel / Prendi, Klarida, "The New Money Laundering Machine Through Cryptocurrency: Current and Future Public Governance Challenges", Corporate Law & Governance Review, Vol. 5, Issue 2, 2023.

35. Pielke Jr., Roger / Wigley, Tom / Green, Christopher, Dangerous Assumptions Nature, 452, 2008.

36. Ramey, Corinne, "The Crypto Crime Wave is Here: From stickups and drug deals to white-collar scams, cryptocurrency-related crime is soaring—and law enforcement is scrambling to keep up", The Wall

Street Journal, 26 Nisan 2018, (Çevrimiçi) https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366, (set) 11.07.2024.

37. **Ramey,** Corinne, "The Crypto Crime Wave is Here" The Wall Street Journal, 26 Nisan 2018, (Çevrimiçi) https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366, (set) 10.07.2024.

38. **Sasson,** Eli Ben / Chiesa, Alessandro / Garman, Christina / Green, Matthew / Miers, Ian / Tromer, Eran / Virza, Madars, "Zerocash: Decentralized Anonymous Payments from Bitcoin", IEEE Symposium on Security and Privacy, 2014, (Çevrimiçi) https://ieeexplore.ieee.org/document/6956581, (set) 16.07.2024.

39. **Sat,** Diana Mergenovna / Krylov, Grigory Olegovich / Bezverbnyi, Kirill Evgenyevich / Kasatkin, Alexander Borisovich / Kornev, Ivan Aleksandrovich, "Investigation of Money Laundering Methods Through Cryptocurrency", Journal of Theoretical and Applied Information Technology, Vol. 83, No. 2, January 2016.

40. **Sharif,** Romel, "Digital Bill: An Approach to Minimize Illicit Activities and other Drawbacks of Crypto Currency", Mayıs 2023, (Çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4434303, (set) 28.07.2024.

41. **Stokes,** Robert, "Anti-money Laundering Regulation and Emerging Payment Technologies", in: Banking and Financial Services Policy Report, Vol. 32, Issue. 5, 2013.

42. **Tarakçıoğlu,** Zeynep Esra, "Kripto Varlıkları ve Ceza Hukuku Sorumluluğu", Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, C. 11, S. 2, Aralık 2021.

43. **Verduyn,** Malcolm Campbell / Goguen, Marcel, "The Mutual Constitution of Technology and Global Governance: Bitcoin, Blockchains, and the International Anti-money-laundering Regime", in: Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance, Ed. Malcolm Campbell-Verduyn, Routledge, London and New York, 2018.

44. **Wegberg,** Rolf van / Oerlemans, Jan-Jaap / Deventer, Oskar van, "Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin", Journal of Financial Crime, Vol. 25 Issue 2, 2018.

45. **Wirdum,** Aaron van, "New EU directive may impose anti-money laundering regulations on Bitcoin wallet providers". Bitcoin Magazine, (2016), (Çevrimiçi) https://bitcoinmagazine.com/articles/new-eu-directive-may-impose-anti-money-laundering-regulations-on-bitcoin-wallet-providers-1468424029/ (set) 09.08.2024.

46. Yelowitz, Aaron / Wilson, Matthew, "Characteristics of Bitcoin Users: An Analysis of Google Search Data", Applied Economics Letters, Vol. 22, Issue 13, 2015.

47. Yermack, David, "Corporate Governance and Blockchains", Review of Finance, Vol. 21, Isuse 1, Mart 2017.

Çevrimiçi Kaynaklar

Financial Crime Academy, "Understanding Crypto Money Laundering Methods: The Cryptocurrency Crime", (Çevrimiçi) https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/#:~:text=What%20are%20the%20methods%20of,decentralized%20finance%20(DeFi)%20platforms. (set) 10.06.2024.

(Çevrimiçi) https://tr.wikipedia.org/wiki/Silk_Road, (set) 04.07.2024.

Europol, "Illegal Network Used Cryptocurrencıes and Credit Cards to Launder more than Eur 8 Million from Drug Trafficking", 9 Nisan 2018, (Çevrimiçi) https://www.europol.europa.eu/media-press/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking, (set) 11.07.2024.

HM Treasury and Home Office, UK National Risk Assessment of Money Laundering and Terrorist Financing, 15 Ekim 2015, (Çevrimiçi) https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing, (set) 05.07.2024.

Cryptocurrency Anti-Money Laundering Report, 2018, (Çevrimiçi) https://info.ciphertrace.com/crypto-aml-report-q218, (set) 11.07.2024.

(Çevrimiçi) https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down (set) 18.07.2024.

(Çevrimiçi) https://www.justice.gov/opa/pr/bitcoin-fog-operator-convicted-money-laundering-conspiracy, 14 Mart 2024, (set) 18.07.2024.

(Çevrimiçi) https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html, 9 Temmuz 2024, (set) 19.07.2024.

Europol Interpol Cybercrime Conference makes the case formultisector cooperation. Retrieved 02.10.2015 (Çevrimiçi) https://www.europol.europa.eu/media-press/newsroom/news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-for-greater-multisector-cooperation, (set) 10.08.2024.

(Çevrimiçi) https://masak.hmb.gov.tr/rehberler, (set) 17.07.2024.