ULUSLARARASI AFRO-AVRASYA ARAŞTIRMALARI DERGİSİ
INTERNATIONAL JOURNAL OF AFRO-EURASIAN RESEARCH (IJAR)
E-ISSN 2602-215X
VOLUME 8- ISSUE 16- JUNE 2023 / CİLT 8 – SAYI 16 – HAZİRAN 2023

KARA PARANIN AKLANMASINDA DİJİTAL PARALARIN ETKİSİ: BİTCOİN ÖRNEĞİ

Cumhur ŞAHİN
cumhur.sahin@bilecik.edu.tr
0000-0002-8790-5851

Araştırma Makalesi
Research Article

Geliş Tarihi
Received: 10.02.2023

Kabul Tarihi
Accepted: 15.03.2023

THE EFFECT OF CRYPTO-CURRENCIES ON MONEY LAUNDERING: BITCOIN EVIDENCE

ÖZ *Kara paranın aklanması, yasa dışı yollardan elde edilen illegal kazançların suç faaliyeti ve yasa dışı fonlar arasındaki bağlantıyı gizlemek için sistemden saklanması olarak tanımlanabilir. Kara para aklama genellikle ikincil bir eylem olup, öncesinde yasa dışı bir eylem, diğer bir ifadeyle öncül suç gelmektedir. Kara para aklama küresel anlamda ciddi bir sorundur çünkü yıkıcı ekonomik etkileri bulunmaktadır aynı zamanda terörün finansmanıyla da yakından ilgilidir. Kara para aklama suçu her ne kadar yeni olmasa da kara paranın aklanmasında dijital paraların kullanılması oldukça yenidir. Bitcoin, Litecoin, Liberty Reserve, Perfect Money ve WebMoney gibi sanal paraların son on yılda popülerlik kazandığı görülmektedir. 2009 senesi kripto paralar için son derece önemli bir yıldır çünkü bir ödeme şeklinde yaratılan Bitcoin çarpıcı bir biçimde artan fiyatı ile finans dünyasında ilgi odağı oldu. Bu ödeme biçimi Satoshi Nakamoto kod adlı kişi veya grup tarafından Bitcoin: A peer-to peer Electronic Cash System (Eşler arası bir elektronik nakit sistemi) adlı makale ile dünyaya tanıtıldı. Bilindiği üzere Bitcoin bir merkez bankasına ihtiyaç duyulmaksızın işlemlerin yapılabildiği sanal bir paradır. Bitcoin'in anonim, neredeyse izlenemez doğası, kaçınılmaz bir şekilde suçluları bu para birimine çekmiş, dolayısıyla kara paranın aklanmasında Bitcoin başta olmak üzere dijital paralar önem kazanmıştır. Bu çalışmada kara paranın aklanmasında Bitcoin özelinde kripto paraların rolü hakkında bilgi verilmeye çalışılacaktır. Bu çalışmanın amacı kripto paraların yasa dışı elde edilen paraların kullanılmasında ne derece önemli olduğu hakkında literature bir katkı sunulmasıdır.*

Anahtar Kelimeler: Kara Para Aklama, Dijital Para, Bitcoin, Finans, Finansal Piyasalar

ABSTRACT *Money laundering can be defined as stocking revenues in system in order to hide the link of illegal revenues from crime operations. Money laundering is a secondary act. The first act becomes crime or illegal operation. Money laundering is a serious crime and results in devastating economic effects with terror financing. Money laundering is an old concept. However, using crypto-currencies in money laundering is new phenomenon. It is found that Bitcoin, Litecoin, Liberty Reserve, Perfect Money and WebMoney have become popular among crypto-currencies in recent years. The year 2009 is a quite important year for cryptocurrencies because Bitcoin, which was formed as a payment, has been a limelight in the financial world with its dramatically increasing price. This form of payment was introduced to the world by a person or group codenamed Satoshi Nakamoto with an article called 'Bitcoin: A peer-to-peer Electronic Cash System'. Bitcoin, as it is known, is a virtual currency in which transactions can be made without the need for a central bank. The anonymous, almost untraceable nature of bitcoin has inevitably attracted criminals to this currency; hence digital coins, particularly Bitcoin, have become important in laundering money. In this study, it is going to be tried to present information about the role of cryptocurrencies, in particular about Bitcoin, in laundering money. The aim of this study is to contribute to the literature on how important cryptocurrencies are in the use of illegally obtained money.*

Keywords: *Money Laundering, Cryptocurrency, Bitcoin, Finance, Financial Markets*

GİRİŞ

Eski bir söz "her seviyede yeni bir şeytan ortaya çıkar" demektedir. Günümüzde teknoloji; toplumun siber suçların mücadele edilmesi gereken yeni bir şeytan olduğunu gözler önüne sermektedir. Siber suçlar, yalnızca yerel suçların sanal ortamda ortaya çıkışı değildir; yeni zorluklar sunan yeni özelliklere sahiptir. Bununla birlikte, bazı siber suçlar sadece sanal ortamda işlenebilse de, bazıları da zaten var olan yerel suçların kıvrımları arasına gizlenmiştir. Bazı yerel suçlar teknolojik gelişmeleri benimsemekte ve araçlarını geliştirmek için bunları kullanmaktadır. Bu tür suçlar örneğin; kara para aklama şeklinde ve daha fazla başarı ve hatta daha az tespit edilme amacıyla sanal para birimlerini benimseme şeklinde ortaya çıkmaktadır. (Mabunda, 2018:1)

ABD İç Güvenlik ve Devlet İşleri Bakanlığı'na sunulan kolluk kuvvetlerinin çıkarlarını öngören yasalardan birincisinde; suç veya terörü finanse etme faaliyetlerinde, kara para aklama amacıyla kullanılmış parayı taşımak veya saklamak için sanal para kullanan suçluları caydırmaya ve kovuşturmaya yönelik çabalar; ve ikincisinde; yasa dışı kara para aklama planlarını ve kara para aklamayı önlemeyi amaçlayan yasaları ihlal eden sanal para birimi hizmetlerinin de araştırılması ele alınmaktadır. (M. Raman, 2013)

ABD Gizli Servisi, aşağıdakileri sağladığı için sanal para birimlerinin suçlular tarafından tercih edildiğine inanmaktadır: 1. Hem kullanıcılar hem de işlemler için en yüksek derecede anonimlik. 2. Yasadışı gelirlerin bir ülkeden diğerine hızlı ve güvenli bir şekilde aktarılabilmesi yeteneği. 3. Düşük kur riski ile sonuçlanan düşük oynaklık, dijital para biriminin serveti iletmek ve depolamak için verimli bir araç olma yeteneğini arttırması. 4. Suçlu yeraltı dünyasının yaygın olarak benimsenmesi. 5. Güvenilirlik (Lowery III, 2013).

Bu çalışmada sırasıyla kara para aklama kavramının yanısıra, kara paranın aklanmasında Bitcoin'in rolü ve önemi, kara para aklamada kripto paraların kullandığı bir takım taktik ve yöntemler, kripto para birimleri kullanarak doğrudan perakende satın alımlar, gizlilik coin'leri ve paravan olarak madencilik konuları hakkında bilgi verilmektedir. Bu araştırmanın motivasyonu, özellikle Türkiye'de kara para aklanmasında kripto paraların rolü ve önemi hakkında yeterince çalışma olmamasıdır. Bu çalışmanın sözkonusu alandaki boşluğu bir nebze olsun dolduracağı düşünülmektedir.

KARA PARA AKLAMA

Kara para aklama, orijinal suç faaliyetleri ile yasadışı fonlar arasındaki bağlantıyı gizlemek için yolsuzluk veya yasadışı faaliyetlerden elde edilen gelirlerin gizlenmesi sürecidir. Kara para aklama genelde sadece ikincil bir eylemdir ve öncesinde yasa dışı bir eylem, yani öncül suç gerçekleşmektedir. (Ajello, 2015:444)

Kara para aklama, yıkıcı ekonomik etkileri olduğu için ve aynı zamanda terörün finansmanıyla yakından bağlantılı olduğu için ciddi bir küresel endişe kaynağıdır. Kara para aklama, doğrudan yabancı yatırımı caydırırken aynı zamanda uluslararası sermaye akışlarını bozacak bir şekilde finansal kurumların bütünlüğünü ve istikrarını ve ülkelerin ekonomik istikrarını baltalamaktadır.(National Drug Intelligence Center, 2008).

Kara para aklama modeli üç aşamalı bir süreçtir; yerleştirme (placement), katmanlama (layering) ve entegrasyon. Yerleştirme aşaması, yasadışı olarak kazanılan paranın küçük bir işletme gibi meşru bir işletmeye veya gayrimenkule yatırılarak para ile öncül suç arasında ilk mesafenin oluşturulduğu aşamadır. Katmanlama aşamasında para, birçok yasal işlemde onunla ilgili suç eylemi arasında daha fazla mesafe yaratmak için kullanılmaktadır. Bu işlem, meşru küçük işletmeler için ekipman alıp satma şeklinde olabilir.

Son aşama, paranın meşru finansal sisteme geri enjekte edildiği entegrasyon sürecidir. Bu işlem, ekipman veya gayrimenkul satışından elde edilen gelirin bir bankaya yatırılması şeklinde yapılabilir. Bu aşamalar arasında, özellikle yerleştirme ve katmanlama süreçlerinde genellikle bir örtüşme bulunmaktadır.(Ajello, 2015:444)

Geleneksel olarak bankalar ve diğer finansal kurumlar kara para aklama için tercih edilen araçlardır, ancak sanal para biriminin büyümesiyle birlikte çevrimiçi kara para aklama popülerlik kazanmaktadır. (National Drug Intelligence Center, 2008).

Kara para aklama yeni bir suç olgusu değildir. Güncellenen işleyiş biçimleri ve gelişen iş modelleri ile sürekli değişen bir suç olgusudur (Savona, 2014:1). Suç teşebbüsü için makul bir para çekme stratejisine ulaşılması kolay değildir. Bu tür gelirleri aklama araçları olmadan suç gelirleri, yalnızca yaşam tarzı harcamaları için yapılmadığı sürece, suç işlemeyi kârsız bir hale getirecektir. Geleneksel olarak, suç parasının aklanması para taşıyıcıları (money mules), offshore hesaplar veya lüks ürünler, yani sanat eserleri, evler, tekneler veya bunların bir kombinasyonun alım satımı ile kolaylaştırılmaktadır (Levi ve Reuter, 2006:289, Aston vd., 2009, Florencio ve Herley, 2010, Levi, 2015:275). Western Union veya Perfect Money gibi alternatif ödeme yöntemlerinin kara para aklama şemalarında önemli bir yer aldığı iddia edilmektedir. Ön ödemeli kredi kartları, hediye çekleri veya diğer kolayca değiştirilebilen geleneksel-olmayan değerli öğeler de genellikle suç parasının aklanmasıyla ilişkilendirilmektedir. Günümüzde, sözde yeni-ödeme yöntemleri gerçek kara para aklama planlarında daha önemli bir faktör haline gelmektedir (Europol, 2015a, 2015b, 2015c; FATF, 2015). Yeni-ödeme yöntemleri kategorisinde kripto para birimleri öne çıkmaktadır. Suçluların, suç gelirlerinin nakde çevrilmesinde kripto para birimlerini daha sık kullandığı bir değişim belirgindir (FATF, 2015).

Bitcoin'ler ayrıca suçlular arasında popüler bir ödeme şeklidir. Europol (2015b: 46) tarafından, siber suç soruşturmalarında, Bitcoin'in “belirlenen tüm suçludan suçluya yapılan ödemelerin yüzde 40'ından fazlasını oluşturduğu” bildirilmektedir. Bu bildirimin, öne çıkan “suçlu” ödeme yöntemi olarak Bitcoin kullanımında bir akış olduğuna dair bir kanıt olarak ne ölçüde görülebileceği henüz net değildir.

Yeraltı piyasaları, mevcut ve gelecekteki kara para aklama planlarında kripto para birimlerinin kullanılması için bir kolaylaştırıcı olarak görülebilirler. Bu durum yeraltı pazarlarına kolaylıkla erişilebilmesi ayrıca suç faaliyetlerinin yerleştirilmesi ve kurulması için (siber) suçlular arasında popülerlik kazanabilir. Genel halk için anonim tarama Tor-protokolü (onion router) kullanılarak uygulanabilir bir hale gelebilir. Tor sistemi, internet trafiğini birkaç Tor düğümüne yönlendirerek aralarındaki ağ trafiğini şifreleyebilir (Dingledine vd., 2004:21). Bağlanan bir bilgisayar yalnızca zincirdeki daha önceki Tor-düğümünün IP adresini görebilir. Bu nedenle Tor sistemi, bir bilgisayar kullanıcısı tarafından İnternet'e erişmek için kullanılan bilgisayarın orjinal IP adresini açıklamadan İnternet'in kullanılmasını mümkün kılar.(Chakravarty ve Barbera, 2014)

Bu şekilde, faaliyetlerini Dark-Web'e taşımanın avantajlarını arayan giderek artan sayıda suçluyu cezbeden sözde Dark-Web kanalları ortaya çıkmıştır. Dark-Web'teki nicel araştırmalar, tüm içeriğin yüzde 50'den fazlasının yasa dışı olduğunu göstermektedir (Moore ve Rid, 2016: 21).

Suçlular tüm iş modellerini kurarlar ve yepyeni bir çevrimiçi yeraltı ekonomisi yaratırlar (Christin, 2013:213, Holt, 2013:155). Böylece İnternette suç teknikleri ve hizmetlerini alıp satmaya dayalı kayıt dışı bir ekonomi ortaya çıkmıştır (Holz vd., 2009, Motoyama vd., 2011). “Hırsızlar arasında namus yoktur” atasözünde söylendiği gibi, suçlular, birbirlerini dolandıranlar bile platforma akın etmişlerdir. Bu tür dolandırıcılık riskini

azaltmak için örneğin eBay ile karşılaştırılabilir bir inceleme sistemi devreye alınmıştır (DécaryHétu ve Dupont, 2013:175, Holt vd., 2015:81). Bu inceleme sistemi, hizmetlerin gözden geçirilerek - doğrulanmış ve çalışır durumda olduğu veya dolandırıcılık olabileceği veya dikkatli olunması gerektiği - şeklinde işaretlendiği, yeraltı piyasalarında itibar-mekanizmasının en öne çıkan unsuru olarak görülebilir.(Wegberg vd., 2018:422)

Daha sonra gerçekleşen araştırmalar, bu pazar yerlerinin suçlular tarafından yasa dışı mal ve hizmetleri satın almak ve sunmak için yaygın olarak kullanıldığını göstermektedir. Eeten ve Bauer, bireylerin bir siber-suç planı içinde belirli bir işlevi yerine getiren hizmetleri satın alıp sunabilecekleri belirli bir siber-suç yeraltı ekonomisinin ortaya çıktığını, (2008) de, belirtmişlerdir. Örneğin, bazı suçlular, diğer kişilerin bilgisayarlarına bulaşarak ve kişisel veya finansal bilgilerini çalmak için kullanabileceği kötü amaçlı yazılımlar yazarlar (Eeten ve Bauer, 2008; Anderson vd., 2012). Bu yazılımların birçoğu daha sonra Dark-Web'te bireylerin satın alabileceği veya kiralayabileceği bir kit olarak sunulur (Sood ve Enbody, 2013:28). Diğer suçlular, Bitcoin karıştırma ve yer altı takas hizmetleri sunarak siber-suç yoluyla elde edilen gelirlerin aklanması konusunda uzmanlaşmışlardır (Möser vd., 2013:1). Europol (2015a: 31), "suç örgütleri için değerli olan bilgisayar becerilerine veya diğer becerilere sahip kişilere kripto-para birimlerinde ödeme yapmak için hizmetlerinin reklamını yapmalarının beklediklerini" tahmin etmektedir.

Açıklanmaya çalışılan bu hususlar, sözkonusu pazar yerlerinin çoğunun suç faaliyetleriyle ilgili olduğu ve ödeme yöntemi ve kara para aklamayı kolaylaştırıcı olarak bitcoin kullanımının siber suçlular arasında popüler olduğu imajını desteklemektedir. Bu nedenle araştırmamız, sanal para biriminin kullanımıyla kara para aklama sürecini ve bunların suçlular tarafından kullanılan nakit-çıkışı stratejilerine katılımları hakkında bilgi sağlamayı amaçlamaktadır. Bitcoin, siber suçlular arasında muhtemelen tercih edilen kripto para birimi olduğu için ilgi çeken bir sanal para birimi olarak seçilmiştir (Europol, 2015b). Yine de, siber suç yoluyla elde edilen suç gelirlerini aklamak için Bitcoin kullanan nakit-çıkışı stratejileri hakkında çok az şey bilinmektedir.

BİTCOİN ÜZERİNDEN KARA PARA AKLANMASI

Bu bölümde; Bitcoin'in siber-suç gelirlerinin aklanmasını neden ve nasıl kolaylaştırdığını netleştirmek için Bitcoin ekosisteminin özellikleri anlatılmaktadır. Blok-zinciri (blockchain) Bitcoin'in temelidir. Bitcoin blok-zinciri, Bitcoin kripto para birimi için merkezi olmayan bir banka olarak çalışmaktadır (Nakamoto, 2008). Bu durum; Bitcoin'lerle kişilerarası işlemlerde Bankaların artık gerekli olmadığı anlamına gelmektedir. Sonuç olarak Bitcoin işlemleri doğrudan Bitcoin adresleri arasında yapılmaktadır (Decker ve Wattenhofer, 2013). Bu anlamda, blok-zinciri halka açık ve doğrulanabilir bir defter olarak görülebilir. Tüm işlemler blok-zincirine kaydedilir ve blockchain.info ve diğer açık kaynaklı web siteleri gibi halka açık web siteleri aracılığıyla denetlenebilir. Herkes, herhangi bir yerde, bir Bitcoin adresinden diğerine yapılan tüm Bitcoin işlemlerini gerçek zamanlı olarak görebilir. Bir Bitcoin adresindeki Bitcoin miktarının mevcut bakiyesi de blok-zincirinde görülebilir. Açıklığına rağmen, Bitcoin sistemi yüksek düzeyde bir anonimlik sağlamaktadır. Bu anonimliğin nedeni, Bitcoin adreslerinin banka hesaplarının aksine şahıslara kayıtlı olmamasıdır. Numaralandırılmış İsviçre banka hesaplarıyla karşılaştırılabilir şekilde, Bitcoin adresinin kendisi, özgün bir tanımlayıcı görevi görür ve hesaba yalnızca Bitcoin cüzdanına giriş ayrıntılarına sahip olan gerçek sahibi tarafından erişilebilir.

Ancak, Bitcoin adresine ve cüzdanına hiçbir isim bağlı değildir. Yüksek anonimlik derecesine ilave olarak, Bitcoin anında yeni Bitcoin adreslerinin oluşturulmasına dayanmaktadır. Bu durum, hesabına isim vermek için kişisel bilgilerinin zorunlu olarak kaydedilmesinin yanı sıra, kurulması zaman alan banka hesaplarıyla

keskin bir tezat oluşturmaktadır. Bu anonimlik düzeyi, Bitcoin'in yasa dışı faaliyetlerde neden bu kadar popüler bir hale geldiğini açıklamaktadır. Bununla birlikte - suç açısından bakıldığında - toplam sistemin bir "dezavantajı" bulunmaktadır. Blok-zinciri konsepti sayesinde, herhangi bir Bitcoin adresi ve işlem bilgisi hakkındaki tüm geçmiş bilgiler, kolluk kuvvetleri için sadece bir mouse tıklaması kadar uzaktır (UNODC, 2014).

KARA PARA AKLAMADA KRİPTO PARA BİRİMİNİN KULLANIMINA İLİŞKİN ARAŞTIRMA

Sınırlı sayıda araştırma, kara para aklama veya terörün finansmanında kripto para biriminin kullanımına yöneliktir. Wegberg vd., 2018:422 suç faaliyetlerinden elde edilen gelirlerin çeşitli karanlık ağ hizmetleri (Dark-Web) aracılığıyla aklanabileceğini göstermektedir ve Dark-Web'te bulunan beş karıştırma ve takas hizmetini araştırmaktadır. Deneyleri, nakit-çıkışı stratejilerinde işlemleri gerçekleştirebilen itibara-dayalı hizmetler olduğunu ortaya koymaktadır. Yazarlar, Bitcoin'in "zaten nispeten anonim" olduğunu ve sanal paralardaki daha fazla yeniliğin kara para aklamayı daha fazla kolaylaştırabileceğini savunmaktadırlar. Ancak, kripto para biriminin yasa dışı kazançların aklanması için kullanılabileceği mekanizmalar hakkında değerli bilgiler sağlarken, Dark-Web hizmetlerini kullanan bu tür nakit-çıkışı stratejilerinin, uluslararası suç örgütlerinin ve terör gruplarının gerektirdiği şekilde büyük miktarlarda paranın aklanmasını kolaylaştırması için yeterli olup olmadığını değerlendirmemişlerdir. (Dupuis ve Gleason, 2021:63).

KAÇINMA TAKTİKLERİ: AÇIK KAPILAR

Düzenleyici diyalektiğin öngördüğü gibi, düzenleyiciler, suçluların inovasyonuna karşı sürekli bir savaş halindedir. Kara para aklayıcıların parayı temizlemek için kullanabilecekleri altı "açık-kapı" nın özellikleri aşağıda açıklanmaktadır: (Dupuis ve Gleason, 2021:66).

MANDALLAR

Mandallar, kriptodan kripto/fiyat para aklamaya yönelik önde gelen araçlardan birisidir ve ağırlıklı olarak Bitcoin, Litecoin veya Ethereum gibi en önemli para birimlerine odaklanmaktadır. Karıştırma hizmetleri olarak da bilinirler ve Clearnet (Smartmixer, Bitcoin Mixer, JoinMarket, vb.) üzerindeki web sitelerinden veya Tor (Dream-market, artık lağvedilmiş Alphabay, vb.) aracılığıyla Dark-net üzerindeki web sitelerinden çalışırlar. Karıştırıcılar, meşru Bitcoin transferlerini yasa dışı kazançlarla tam anlamıyla harmanlayarak ve ortaya çıkan sanal fonları yeni bir adrese göndererek cüzdanlar arasındaki işlemsel bağlantıyı etkili bir şekilde bozarlar. Servis ücretleri kesildikten sonra aklanan paralar Paypal veya Western Union aracılığıyla nakde çevrilirler. Fiyat eşiğine eklenen boyut sınırlamaları, Mandallama sistemlerinin *(*tumbling facilities*)* etkinliğini sınırlar, ancak coin'ler temizlendikten sonra, işlemler artık şüpheli olmadığından diğer nakit-çıkışı yolları açılır. Ayrıca, kripto-için-kripto para alım satımları için herhangi bir boyut sınırı uygulanmaz. Son zamanlarda, Çin dolandırıcılığı Plus Token aracılığıyla elde edilen ve toplamı 3 milyar ABD Dolarını aşan fonlar, ceza görmeden izlenen çoklu Bitcoin cüzdanlarından bir tumbling facility hizmetine taşınmış ve izleri kaybolmuştur. Bu coin'ler Ağustos 2019'da tasfiye edildiğinde meşru borsalara giden yolu bulduğuna ve BTC fiyatında bir düşüşe neden olduğuna inanılmaktadır. Kolluk kuvvetleri ve ABD Adalet Bakanlığı yasa dışı ticareti aktif olarak hedef almaya başlayarak kısa bir süre önce Larry Harmon adlı kişiyi Bitcoin kullanarak 300 milyon dolar aklama ile suçlamıştır. Bununla birlikte, bugüne kadar, çevrimiçi kaynakları ve Dark-Neti yasalaştırmanın zorluğu nedeniyle karıştırıcılar üzerindeki düzenleyici yanıt nispeten sessiz kalmıştır. Mart 2020'de ABD kolluk kuvvetleri, lisanssız kripto-sermaye akışlarının kullanımıyla mücadele etmek için kripto-para birimi istihbarat programını kurmuştur, ancak sorunun basitçe tanımlanması bir çözüm

sunmamaktadır; Örnek olarak, offshore cennetlerini kullanarak vergi kaçakçılığı yapılması onlarca yıldır kabul edilmektedir, ancak önlenememiştir. (https://paypers.com).

TEZGAH ÜSTÜ PİYASALAR

Kriptodan itibari paraya (veya tersi) işlemler için, OTC (tezgah üstü piyasalar) pazarını yenmek zordur. Tezgah üstü işlem hacminin, resmi piyasaların çıktısının üç veya dört katı olduğu tahmin edilmektedir. OTC işlemleri için iki ana yol bulunmaktadır; bir komisyoncu aracılığıyla (Kraken, Bitstocks, Genesis Trading, vb.) aracılığıyla veya kişiden-kişiye. Riskten korunma hedge fonları ve madenciler - boyut, likidite ve hız gibi bariz nedenlerle, aracıları tercih etme eğilimindedir. Bu işlemler için çıkış rampası Kriptodan-itibari paraya (veya tersi) işlemler için yine de bir bankacılık ilişkisi gerektirir, bu nedenle madeni paralar komisyoncuya ulaşmadan önce aklanmadığı sürece kara para aklayıcılar için daha az ilgi çekicidir. Kripto işlemleri organize bir değiş tokuş gerektirmediğinden, iki kişi kriptodan-kriptoya ticareti tamamlamak için genel anahtarları değiştirebilirler (swap public keys*)* [veya hızlı yanıt (QR) kodunu tarayabilir]. Fiyat dönüşümleri, masada nakit ile yüz yüze bir toplantı gerektirir ve OTC hizmet sağlayıcıları, hizmetleri için genellikle %3 ila %8 arasında bir ücret alırlar. Araştırmacılardan birisi OTC piyasalarını kullanma konusunda ilk elden deneyime sahiptir. Bu yasal işlem 2017 yılında Dubai'de gerçekleşmiş olup formatı tüm dünyada aynıdır. Araştırmacı, satıcıyı localbitcoins.com 'da bulmuştur. Bu küresel web sitesi, potansiyel işlem yapan taraflar, derecelendirmeler ve bireyler için tamamlanan işlemlerin sayısı, emanet hizmetleri, oranlar, maksimum işlem tutarları ve iletişim ayrıntıları için kapsamlı bilgiler sunmaktadır. Araştırmacı, satıcıyı arayarak, halka açık ama sessiz bir kafede bir buluşma ayarlamıştır. Toplam satın alma tutarı, yaklaşık 100.000 ABD Doları olarak, nispeten düşük, ancak iyi ilişkileri sürdürmek için yeterli olan %3'lük bir pazarlık ücretiyle kararlaştırılmıştır. Bir sonraki adım, BAE'de şaşırtıcı derecede kolay bir iş olan sermayeyi bankadan çekmektir. Banka memuru parayı 15 dakikada hazırlamıştır. Satıcı kafede akıllı telefonunu çıkartarak, o sırada kabaca 6,000 dolar olan fiyatı sabitlemek için Bitfinex borsasına girmiştir. Bu arada yazar, Exodus cüzdanına giriş yapmıştır ve hesabı için Bitcoin'in "receive" genel anahtarını ve QR kodunu almıştır. Para masanın üzerinde dururken satıcı, alıcının QR kodunu taramış ve telefonundaki "send" düğmesine basmıştır. Kahveler yudumlanırken ve para sayılırken işlem Bitcoin blok zincirine kaydedilmiştir, her iki tarafça da doğrulanmıştır ve birkaç dakika sonra *ilave* BTC16.2 olarak araştırmacının cüzdan bakiyesinde görünmüştür. Satıcı ayrıca BTC0.0005'lik normal transfer ücretini de ödemiştir. Ticaret tamamlanmıştır, içinde nakit para bulunan zarf masadan alınmış ve her iki taraf da kafeden ayrılmıştır. Görüldüğü üzere işlem bu kadar basittir. (Dupuis ve Gleason, 2021:68)

Kripto işlemleri için OTC piyasasını kullanmak için birçok meşru neden bulunmaktadır. Büyük siparişler, sipariş defteri görünür olduğunda organize borsalarda önemli bir fiyat etkisine sahip olabilirler, bunun yanında OTC masaları likidite aramada etkilidir. Ayrıca, kripto borsalarının itibari para yatırma ve ticaret konusunda yasaklayıcı haftalık limitleri vardır. Standart bir hesapla 100.000 ABD Doları tutarında bir satın alma işlemi yapmak 10 hafta sürebilir ve bilindiği üzere Bitcoin fiyatı Aralık 2017'de hızlı hareket ederek 19.000 ABD Dolarının üzerine çıkmıştır. Bu şartlar altında 10 hafta bir yaşam süresidir. Ayrıca, ücretler karşılaştırılabilir; fiyatı organize bir piyasaya taşımak, BTC0.005 transfer maliyetine ilave olarak bankacılık ücretlerini, %2'lik bir piyasa ücretini (fiyat mevduatı) ve borsadaki alım satım spreadini gerektirecektir. Kara para aklamanın sonuçları açıktır; araştırmacı parayı bankadan çekmiş olsa da, kaynak kolayca uyuşturucu satışı veya başka herhangi bir suç faaliyeti olabilir. Burada, büyük miktarlar bir sorun gibi görünmüyor ve küçük bir önlemle, işlem tüm bireylerin erişimine açıktır. Yasadışı olsun veya olmasın, başka yollar da

(bloglar, sohbet odaları vb.) bir işlem düzenlemek için kullanılabilir. Yakın tarihli bir haber makalesinde, OTC anlaşmalarına düzenleyici tepki vurgulanmaktadır. https://www.coindesk.com/markets/2020/03/11/us-homeland-security-charges-localbitcoins-seller-with-money-laundering/

Mart 2020'de ABD İç Güvenlik Soruşturma Departmanı, bir kişiyi lisanssız para aktarma işi yürütmek ve fon aklamakla suçlayarak tutuklamıştır. Gizli ajanlar, tüccarla yerel Bitcoin'ler aracılığıyla temasa geçmiştir ve iddiaya göre, işlem insan kaçakçılığından elde edilen gelirlerden kaynaklanmıştır, ancak sonuç alınamamıştır, satıcıyla birden fazla anlaşma yapılmıştır. Bu durum, bir tutuklama ve mahkûmiyetin ilk örneği değildir, ancak vaka bazında müdahale sıkıcı, pahalı ve göreceli olarak verimsizdir, bu nedenle uygulama yaygın olmaya devam ederken ve OTC pazarları hala gelişirken uygulama doğal olarak sınırlıdır.

GİZLİLİK COİN'LERİ

2008 krizine yanıt olarak Nakamoto (2008), dış kontrolden yoksun şeffaf bir para birimi sunar; tabi ki tüm dünya tarafından Bitcoin olarak bilinmektedir. Şimdiye kadar, bu devrim niteliğindeki çaba nispeten başarılıydı, ancak Bitcoin'in izlenebilirliği, bazı tutucuları bir kırılganlık duygusu ile karşı karşıya bıraktı. Geliştiriciler kısa sürede alternatif bir çözüm bulmak için iş başındaydı ve 2014'ten 2016'ya kadar; Monero, Dash ve Zcash gibi coinler tek bir amaç göz önünde bulundurularak yaratıldı: anonimlik. Bu coinler, herhangi bir tüccarın iletebileceği, ancak kaynağın, miktarın ve varış yerinin gizli olduğu, gizlenmiş bir kamu defterini aktif olarak uygulamaktadır. Zcash ve Dash, Bitcoin blok zincirinin sert çatallarıdır, dolayısıyla benzer güvenlik açıklarını paylaşırlar. Güvenilirlik, bu kripto para birimleriyle ilişkili gizliliğin sağlam olduğudur, ancak gerçek şu ki, önemli sayıda ticaret izlenebilir. Koruma, intifa hakkı sahibinin aktif müdahalesini gerektirebilir ve çok azı gerekli bilgiye sahiptir. Quesnelle, 2017 ve Kappos vd, 2018, Zcash adreslerinin yalnızca %3,5'inin korumalı olduğunu ve bunların %31,5'inin gelişmiş analitik araçlar kullanılarak izlenebileceğini göstermektedir. Bu durum, Zcash işlemlerinin %98,9'unu takibe açık bırakır, vaat ettiği gizlilik pek mümkün değildir. Monero, açık ara en popüler gizlilik madeni parası olmaya devam ediyor - gizli adreslerin ve halka gizli işlem protokolünün birleşimi, bu kripto para birimini neredeyse izlenemez hale getiriyor. Möser vd. 2018, tüm Monero işlemlerinin yaklaşık %25'inin yasa dışı olduğunu tahmin ediyorlar. Ayrıca, 2017 öncesi bazı işlemlerin ileri matematiksel analizlerle izlenebileceğini gösteriyorlar, ancak durumun hala böyle olup olmadığı belirsizliğini koruyor. Popüler inanç, kripto para birimlerinde gizliliğin mümkün olduğu yönündeyken, teori bunun bir illüzyondan başka bir şey olmadığını öne sürüyor. 2019'da Mali Eylem Görev Gücü (FATF), sanal para birimleri hakkında bir kılavuz belge yayınlayarak, tüm yetki alanlarının kripto para birimlerini içeren finansal ve finansal olmayan faaliyetlere AML gereklilikleri getirmesini tavsiye ederek, kripto endüstrisi üzerinde etkili bir şekilde geniş bir ağ oluşturdu. Ne yazık ki, uygulama, egemen düzenleyici kurumların ayrıcalığıdır ve şimdiye kadar uygulanmaya devam etmektedir. Bazı küçük borsalar (OKEx, BitBay, vb.) FATF'nin baskısı altında boyun eğdi ve şüpheli paraları listeden çıkardı, ancak daha büyük pazarların çoğu onları ilk etapta listelemedi. Örneğin Coinbase, Zcash için likidite sağlarken Monero veya Dash için likidite sağlamamıştır.(Dupuis ve Gleason, 2021:69).

MERKEZİ OLMAYAN BORSALAR

Standart organize piyasalar, nihai olarak düzenleyici kurumlara uyumdan sorumlu olan ve bu nedenle sorumlu tutulan bir kurumsal varlık olarak bir emanetçinin gözetimi altında çalışır. Bu borsaların kayda değer bir dezavantajı bulunmaktadır; Bu anahtarlar saklayıcı tarafından kontrol edilen konsolide bir depoda tutulduğu için kullanıcıların özel anahtarlarına erişimi yoktur. Ayrıca, merkezi borsalar bilgisayar korsanları

tarafından sürekli saldırı altındadır ve bazıları başarılı olmaktadır. Örneğin, Japon ticaret platformu Coincheck 2018'de 230 milyon NEM (530 milyon ABD doları) piyasa değerinde soyulmuştur. (https://news.bitcoin.com/tokyo-police-arrest-2-men-for-buying-cryptocurrency-tied-to-530m-coincheck-hack/) Son zamanlarda yeni bir borsa türü ortaya çıkmıştır; DEX'ler . (https://coinsutra.com/decentralized-exchange-cryptocurrency) Lin (2019), DEX'leri "dağıtılmış defter protokolleri ve kullanıcıların, kripto para birimlerinin ticaretinde bir aracı veya emanetçi olması için merkezi bir varlığa güvenmeye gerek kalmadan kripto para birimlerinde işlem yapmalarını sağlayan uygulamalar" olarak tanımlamaktadır. Bu pazarlar, zincir-üzerinden akıllı sözleşmeler kullanarak çevrimiçi olarak anonim olarak çalışırlar ve bir işlemi tamamlamak için bir e-posta adresi bile gerektirmezler. DEX'ler, kullanıcıların kendi özel anahtarlarını kontrol etmelerine olanak tanırlar, potansiyel tek bir hata noktasından (sunucu kapalı kalma süresinde) etkilenmeyerek, üçüncü şahıslar içermeyecek, karşı taraf riski olmayacak ve hükümetler tarafından kapatılamayacak şekilde dağıtılırlar. Kripto kullanıcıları özünde, kendi bankaları olurlar.

Madalyonun öbür yüzünde ise, DEX'ler ana şirketlerinden bağımsız olarak çalışırlar ve düzenlenmeleri zordur. Kullanıcı dostu değildirler, genellikle destekten yoksundurlar ve fiyat dışı hizmetler sunmazlar. Bu hizmetlerin çoğu (Uniswap, Bancor, Cryptobridge, WavesDEX, AirSwap, vb.) yakın zamanlarda kripto-dünyasına girmişlerdir ve bazıları hala proje geliştirme aşamasındadır. Bu nedenle, henüz düzenleyici bir yanıt verilmemiştir. Shapiro (2018:3), IRS'nin gözetim dışı finansal işlemleri izleme yeteneğinden yoksun olduğunu ve potansiyel bir çözüm sunduğunu öne sürmektedir; IRS, "stopaj yükümlüsü" tanımını kontrol yerine kâr kavramını içerecek şekilde güncellemelidir. Yine de, kriptodan-kriptoya kara para aklama için tercih edilen bir araç haline gelmeleri beklenilmektedir.

KRİPTO PARA BİRİMLERİ KULLANARAK DOĞRUDAN PERAKENDE SATIN ALIMLAR

Kripto para aklamada en çok korunan portal çıkış yolu süreçtir; diğer bir ifadeyle dijital coin'den Dolar, Euro veya Yen gibi itibari paraya geçiştir. Çoğu durumda, suçtan elde edilen gelirlerin hacmi, nakit parayı kullanışsız hale getirir ve doğrudan banka mevduatları ise arkalarında bir iz bırakırlar. Yaygın bir uygulama, büyük varlıkları (gayrimenkul, araba, mücevher, sanat eseri, şarap vb.) yasadışı gelirlerle nakit olarak satın almak ve ardından varlığı açık piyasada yeniden satmaktır. Konuyla ilgili literatür oldukça geniştir (De Sanctis, 2017, Thiemann, 2014:1203, Tiwari vd., 2020:271). Bugün bile, bir ev satın almak için bir bavul dolusu dolar getirmek, bazı pazarlarda hala uygulansa da, dikkat çekmektedir. Araştırmacılardan biri, İstanbul'da bir kat mülkiyeti satmıştır ve tüm tarafların haberi olmadan, alıcı bir çanta dolusu lirayla gelmiştir. Hiç etkilenmeyen avukatlar, işlemi gözlerini kırpmadan hallettiler. Yine de, benzer bir durum muhtemelen ABD'de veya diğer gelişmiş pazarlarda bu kadar sorunsuz gitmeyecektir. Aynı süreç, negatif damgalama hariç kripto alımları için de geçerlidir. Bu durum hala devam ederken, Bitcoin ile emlak satın almak olumlu bir şekilde yenilikçi ve dikkate değer olarak kabul edilmektedir. Uygulama o kadar popülerlik kazanmıştır ki, Bitcoin RealEstate günümüzde bir web sitesi geliştirmektedir. Dubai emlak geliştiricileri artık kripto para birimini kabul etmektedirler ve konut ile ilgili popüler dergilerde konuyla ilgili makaleler yayınlanmaktadır. (www.hgtv.com/lifestyle/real-estate/how-to-buy-real-estate-with-bitcoin).

PARAVAN OLARAK MADENCİLİK

Bu, dünya çapında kullanılan iyi-bilinen taktiğin yeniden yapımıdır; yasadışı fonları nakit yoğun bir işe aktarın, ortaya çıkan vergileri ödeyin ve durulanan parayı boş zamanlarında harcayın. Bu tür aklamaya karşı en yaygın önlem, şüpheli işletmeler için nakit akışlarının analizinden oluşmaktadır, ancak bu yöntemin etkili

olabilmesi için, sanal para birimi madenciliği gibi nispeten yeni bir alan için büyük olasılıkla eksik olan istatistiksel verilere dayanmaktadır. Bu işlemler, dış kuruluşların verimlilik, hash-oranı ve piyasa koşullarına bağlı çıktıyı değerlendirmesi nispeten zor olduğundan, geliri gizlemek için çok uygundur. Yasadışı Coin'ler, normal madencilik gelirleriyle kolayca karışır ve ayırt edilemez hale gelirler, böylece aklama döngüsü tamamlanır. (Dupuis ve Gleason, 2021:71).

SONUÇ

En yalın ifadesiyle kara para, kanunlar ile men edilmiş etkinliklerin neticesi olup ekonomiye dâhil edilmesi söz konusu olmayan bir gelir çeşididir. Diğer yandan kara para aklama, illegal faaliyetler sonucunda sağlanan kazancın, yasal bir faaliyet neticesinde kazanılmış gibi gösterilmesi ve ekonomik sisteme katılması sürecidir. Bu sayede aklanan paralar, genellikle yine kanun dışı olarak değerlendirilmektedir. Mevzuatın sıkılaştırılması nedeniyle kara para aklama araçlarına olan talep arttıkça, mali suçlular yasa dışı faaliyetlerinden elde ettikleri gelirleri aklayabilecekleri açık kapılar ararlar. Dijital para birimlerinin icadı iki ucu keskin bir kılıç olmuştur. Bir yandan internet üzerinden güvenli bir şekilde işlem yapmayı kolaylaştırırken, diğer yandan sayısız siber suçları kolaylaştırmak ve suçluların gelirlerini güvenli bir şekilde aklamasına yardımcı olmak için istismar edilmiştir. Bitcoin, anonimliği, güvenliği, geri döndürülemezliği ve yerinden yönetilebilmesi nedeniyle istismar edilen bir kripto para birimi örneğidir.

Bu çalışmada, kara paranın aklanmasında bitcoin özelinde dijital paraların oynadığı rol ve etkileri hakkında bilgi verilmeye çalışılmıştır. Dijital para birimlerinin kara paranın aklanmasında ve terörle ilgili faaliyetlerin finansmanında kullanılabilmesindeki en önemli etken, klasik finansal sisteme uygulanan legal düzenleme ve önlemlerin haricinde yer almasıdır. Kara paranın dijital para birimleriyle aklanmasının önüne geçilebilmesi için gerekli önlemler ve öneriler olarak şunlar sayılabilir: Hukuk mevzuatında özellikle bilişim suçlarıyla ilgili olarak dijital paralarla ilgili düzenlemelerin süratle hayata geçirilmesi faydalı olacaktır. Yine, teknik bilgi gerektiren bu konularla ilgili olarak alanında uzman, ihtisaslaşmış personel bulundurmak son derece önemli ve gereklidir. Benzer biçimde şüpheli işlemleri belirleme yeteneğine sahip gelişmiş aygıtların temin edilmesi bu tür risklerin ortadan kaldırılması için elzemdir. Bu çalışmanın sınırlılıkları, kripto paraların yürürlüğe girdiği 2008 yılı ile 2021 yılı arasındaki dönemdeki çalışmaları esas almaktadır. Dolayısıyla 2022 ve 2023 yılına ilişkin çalışmalar yer almamaktadır. Bu çalışma, Oral ve Yeşilkaya'nın (2021) çalışmasına Bitcoinin finansal bir teknoloji olarak sınıflandırılması ve düzenlemenin öncelikle özel sektör kuruluşlarına dayandırılması gerekliliği konusunda benzerlikler taşımaktadır. Yine Savaş ve Danacı'nın (2014) çalışmasında olduğu gibi bu çalışmada da ulusal bazda yeterli ölçüde yasal düzenleme bulunmaması, mevcut mevzuatımızın bu sistem hakkında müeyyidelerde bulunmasını mümkün kılmamakta şeklinde bir değerlendirme yapmak mümkündür. Yönetimsel ve sektörel olarak kara paranın aklanmasında en çok kullanılan sektörlerden özellikle gayri menkul sektörüne odaklanılması faydalı olabilecektir.

KAYNAKÇA

AJELLO, N.J. 2015. "Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination", *Brooklyn Law Review*, 80(2):434-461.

ANDERSON, R., BARTON, C., BOEHME, R., CLAYTON, R., EETEN, M.V., LEVİ, M., MOORE, T. ve SAVAGE, S. 2012. "Measuring the cost of cybercrime", Workshop on the Economics of Information Security.

ASTON, M., McCCOMBİE, S., REARDON, B. ve WATTERS, P. 2009. "A preliminary profiling of internet money mules: an Australian perspective", Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing.

CHAKRAVARTY, S. ve BARBERA, M. 2014. "On the effectiveness of traffic analysis against anonymity networks using flow records", PAM, doi: 10.1007/978-3-319-04918-2

CHRİSTİN, N. 2013. "Traveling the silk road: a measurement analysis of a large anonymous online marketplace", *World Wide Web*, 213-224.

DE SANCTİS, F.M. 2017. "Money laundering through real estate", International Money Laundering through Real Estate and Agribusiness, Springer, Cham.

DECARY-HETU, D. ve DUPONT, B. 2013. "Reputation in a dark network of online criminals", *Global Crime,* 14(2-3): 175-196, doi: 10.1080/17440572.2013.801015.

DECKER, C. ve WATTENHOFER, R. 2013. "Information propagation in the Bitcoin network", IEEE P2P 2013-Proceedings 13th IEEE International Conference on Peer-to-Peer Computing, pp. 1-10, doi: 10.1109/P2P.2013.6688704.

DİNGLEDİNE, R., MATHEWSON, N. ve SYVERSON, P. 2004. "Tor: the second-generation onion router", SSYM'04 Proceedings of the 13th Conference on USENIX Security Symposium, Vol. 13, pp. 21, doi: 10.1.1.4.6896.

DUPUİS, D. ve GLEASON, K. 2021. "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Journal of Financial Crime*, 28(1): 60-74.

EETEN, M.V. ve BAUER, J. 2008. "Economics of malware: security decisions, incentives and externalities", Report. OECD Science, Technology and Industry Working Papers.

EUROPOL 2015a. "Exploring tomorrow's organised crime", available at: www.europol.europa.eu/sites/default/files/Europol_OrgCrimeReport_web-final.pdf

EUROPOL 2015b. "The internet organised crime threat assessment", available at: www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf

EUROPOL 2015c. "Why cash is still King?", available at: www.europol.europa.eu/sites/default/files/publications/europolcik.pdf

FATF 2015. "Virtual currencies: key definitions and potential AML/CFT Risks", available at: http://fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks. Pdf

FLORENCİO, D. ve HERLEY, C. 2010. "Phishing and money mules", International Workshop on Information Forensics and Security (WIFS).

HOLT, T.J. 2013. "Exploring the social organisation and structure of stolen data markets", Global Crime, 14(2-3): 155-174, doi: 10.1080/17440572.2013.787925.

HOLT, T.J., SMİRNOVA, O., CHUA, Y.T. ve COPES, H. 2015. "Examining the risk reduction strategies of actors in online criminal markets", *Global Crime*, 16(2): 81-103, doi: 10.1080/ 17440572.2015.1013211.

HOLZ, T., ENGELBERTH, M. ve FREİLİNG, F. 2009. "Learning more about the underground economy: a case-

study of keyloggers and dropzones", Computer Security-ESORICS.

KAPPOS, G., YOUSAF, H., MALLER, M. ve MEİKLEJOHN, S. 2018. "An empirical analysis of anonymity in zcash", Working Paper, available at: www.researchgate.net/publication/ 325034106_An_Empirical_Analysis_of_Anonymity_in_Zcash.

LEVİ, M. 2015. "Money for crime and money from crime: financing crime and laundering crime proceeds", *European Journal on Criminal Policy and Research*, 21(2): 275-297.

LİN, L. 2019. "Deconstructing decentralized exchanges", *Stanford Journal of Blockchain Law and Policy*, available at: https://stanford-jblp.pubpub.org/pub/deconstructing-dex.

LOWERY III, E. W. 2013. "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. (Mar. 18, 2013)

MABUNDA, S. 2018. Cryptocurrency: The New Face of Cyber Money Laundering. International conference on advances in big data, computing and data communication systems (icabcd).

MOORE, D. ve RİD, T. 2016. "Cryptopolitik and the darknet", *Survival. Routledge*, 58(1):7-38, doi: 10.1080/00396338.2016.1142085.

MOTOYAMA, M., McCOY, D., LECCHENKO, K., SAVAGE, S. ve VOELKER, G.M. 2011. "An analysis of underground forums", ICM

MÖSER, M., BÖHME, R. ve BREUKER, D. 2013. "An inquiry into money laundering tools in the bitcoin ecosystem", Procedings of the 2013 e-Crime Researches Summit, pp. 1-14, doi: 10.1109/ eCRS.2013.6805780.

MÖSER, M., SOSKA, K., HEİLMAN, E., LEE, K., HEFFAN, H., SRİVASTAVA, S., HOGAN, K., HENNESSEY, J., MİLLER, A., NARAYANAN, A. ve CHRİSTİN, N. 2018. "An empirical analysis of traceability in the monero blockchain", Proceedings on Privacy Enhancing Technologies.

NAKAMOTO, S. 2008. "Bitcoin: a peer-to-peer electronic cash system", Consulted, pp. 1-9, doi: 10.1007/ s10838-008-9062-0.

NATIONAL DRUG INTELLIGENCE CENTER. 2008. "Money laundering in digital currencies," U.S. Department of Justice, No. 2008-R0709-003, June 2008.

ORAL, B.G. ve YEŞİLKAYA, Y. 2021. "KRİPTO PARA İKİLEMİ: KARAPARA AKLAMA ve BİTCOİN", *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 39(1): 209-239.

QUESNELLE, J. 2017. "On the linkability of zcash transactions", available at: https://arxiv.org/pdf/ 1712.01210.pdf.

RAMAN, M. 2013. Department of Justice, Press Release (Nov. 18, 2013), available at http://www.justice.gov/criminal/pr/speeches/2013/crm-speech-131118.html.

SAVAŞ, D.O. ve DANACI, Ö. 2014. "DİJİTAL PARA BİTCOİN; BİR ÖDEME ARACI MI YOKSA KARA PARA AKLAYICILARIN YENİ SIĞINAĞI MI?", *Gümrük ve Ticaret Dergisi*, 4, 72-85.

SAVONA, E. 2014. "Organised crime numbers", *Global Crime*, 15, 1-2, 1-9, doi: 10.1080/ 17440572.2014.886512.

SHAPİRO, D. 2018. "Taxation and regulation in decentralized exchanges", *Journal of Taxation of Investments*, 36(1): 3-13.

SOOD, A.K. ve ENBODY, R.J. 2013. "Crimeware-as-a-service—a survey of commoditized crimeware in the underground market", *International Journal of Critical Infrastructure Protection*, 6(1): 28-38.

THİEMANN, M. 2014. "In the shadow of basel: how competitive politics bred the crisis", *Review of International Political Economy*, 21(6): 1203-1239.

TİWARİ, M., GEPP, A. ve KUMAR, K. 2020. "A review of money laundering literature: the state of research in key areas", *Pacific Accounting Review*, 32(2): 271-303.

UNODC .2014. Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies.

WEGBERG, R.V., OERLEMANS, J.J., ve DEVENTER, O.V. 2018. "Bitcoin money laundering: mixed results?", *Journal of Financial Crime*, 25(2): 419-435.

https://paypers.com (31.12.2022)

https://www.coindesk.com/markets/2020/03/11/us-homeland-security-charges-localbitcoins-seller-with-money-laundering/ (28.12.2022)

https://news.bitcoin.com/tokyo-police-arrest-2-men-for-buying-cryptocurrency-tied-to-530m-coincheck-hack/) (02.01.2023)

https://coinsutra.com/decentralized-exchange-cryptocurrency (03.01.2023)

www.hgtv.com/lifestyle/real-estate/how-to-buy-real-estate-with-bitcoin (04.01.2023)