ANADOLU AKADEMİ SOSYAL BİLİMLER DERGİSİ

KRİPTO PARALAR İLE TERÖR VE DİĞER İLLEGAL AKTİVİTELERİN FİNANSMANI*

Deniz TURAN[1]

Cem DEMİRCAN[2]

Özet

Blok zinciri teknolojilerinde barındırılan kripto para birimlerinin sağladığı anonimlik ve görünüşte anonimlik, bu platformları suç aktörlerinin kara para aklama ve terörizmin finansmanı gibi yasadışı faaliyetlerde kullanması için giderek daha çekici araçlar haline getirdi. Blok zinciri teknolojisi henüz emekleme aşamalarında olduğundan dolayı tam olarak anlaşılmamış ve düzgün bir yasal düzenlemeye tabi tutulmamıştır. Bu durum son yıllarda suçlarının artarak yararlandığı gri alana yol açmaktadır. Çalışmanın amacı, blok zinciri teknolojisini ve ardından kripto para birimlerini inceleyerek, bunların yarattığı fırsatlar ve zorluklar ile kara para aklamanın yanı sıra terörizmin finansmanında ki rolünü açığa kavuşturmaktır. Kripto paralar ve blok zincirlere yönelik işlemlerin takip ve denetiminde uluslararası alanda var olan hukuksal boşluklar ile teknik bilgi ve donanım yetersizliğinin giderilmesinin, bu sanal varlıkların kara para aklama ve terörizm finansmanında kullanımının engellenmesinde önem arz ettiği sonucuna ulaşılmıştır.

Anahtar kelimeler: Blok Zinciri, Kripto Para, Terörizmin Finansmanı

FINANCING of TERROR and OTHER ILLEGAL ACTIVITIES with CRYPTO MONEY

Abstract

The anonymity and pseudo-anonymity provided by cryptocurrencies hosted on blockchain technologies has made these platforms increasingly attractive tools for criminal actors to use for illicit activities such money laundering and financing of terrorism. Since blockchain technology is in its infancy, it has not been fully understood and properly regulated. This situation leads to the gray area where crimes have increasingly benefited in recent years. The aim of the study is to examine blockchain technology and then cryptocurrencies, to reveal the opportunities and challenges they create and their role in money laundering as well as in financing terrorism. It has been concluded that the legal gaps that exist in the international arena as well as the lack of technical knowledge and equipment in the monitoring and control of cryptocurrencies and blockchains are important in preventing the use of these virtual assets in money laundering and terrorism financing.

Keywords: Blockchain, Cryptocurrency, Financing of Terrorism

[1] Doç. Dr., Polis Akademisi Başkanlığı, Güvenlik Bilimleri Enstitüsü, Suç Araştırmaları ABD, ahmetdenizturan@gmail.com, ORCID:0000-0002-6697-2721

[2] Doktora Öğrencisi, Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Sivil Havacılık Anabilim Dalı, cemdemircan@live.com, ORCID:0000-0002-8476-8353

* Bu çalışma Anadolu Üniversitesi Bilimsel Araştırma Projeleri Birimi (BAP) tarafından desteklenen 1907E129 nolu proje kapsamında hazırlanmıştır. Desteği için Anadolu Üniversitesi BAP'a teşekkür ederiz.

Giriş

Toplumların refahını olumsuz etkileyen ve sınırötesi negatif dışsallıklara sahip terör ve suç örgütlerinin faaliyetleri ve finansal yapıları günümüzde sıkı denetim altına alınmaya başlanmıştır. Bu durum terör ve suç örgütlerinin finansman kaynaklarında dönüşüm yaşanmasına ve para izi takibinin daha zor olduğu kripto paraların illegal faaliyetlerin finansmanında ve para aklamada kullanımının yaygınlaşmasına yol açmıştır.

Son yıllarda ana akım medya ve haber platformları tarafından blok zinciri (blockchain) ve kripto para terimlerinin moda sözcükler haline getirilmesi, gerçek anlamlarının kamuoyu tarafından anlaşılmasının önüne geçmesine yol açmıştır. Böylelikle aslında katılımcılar tarafından bağımsız olarak tutulan ve güncellenen bir veritabanı olan blockchain (distributed ledger technology), veri tabanlarını global bir ağ üzerinde dağıtarak sansür ve müdahalelere karşı dirençli bir ağ oluşturma amacını genel olarak aktaramamış ve sonuçta blok zincirinin başka kullanım alanları olmasına rağmen yalnızca elektronik para olabileceği kanısı yaygınlaşmıştır. Bu nedenle blok zinciri ve kripto para terimlerinin gerçekte ne anlam ifade ettiğinin açıklanması ve kripto paraların yasa dışı aktivitelerde kullanımlarının incelenmesi önem arz etmektedir.

Çalışmanın amacı, terör ve diğer illegal aktivitelerin finansmanında ve kara para aklamada blok zinciri teknolojisini ve ardından kripto para birimlerinin rolünü açığa kavuşturmaktır. Literatürde bulunan diğer çalışmalardan farklı olarak makalede öncelikle blok zinciri ve kripto paraların, teknik detaylara girmeden kavram olarak ne oldukları açıklanacak ve şeffaf ve gizlilik odaklı kripto paraların fonksiyonları, dağıtılmış defter teknolojisinin ne olduğunu ve neden müdahaleye ve sansüre dirençli olduğu bu temeller üzerinde izah edilecektir. Bunu takiben terör ve illegal faaliyetlerin finansmanı ve para aklamada kripto paraların rolü ve bunlara karşı alınabilecek önlemler ele alınacaktır.

Blok Zinciri Teknolojisi

Bu başlık altında blok zinciri teknolojisi, sınırlı bilgisayar bilimleri teknik bilgisi ile anlaşılabilir olmasını sağlayacak şekilde, finansal kullanım alanı perspektifinden tanımlamayı amaçlamaktadır. 2017 yılında Bitcoin'in işlem değerinde yaşanan büyük artış dikkatleri blockchain teknolojisine ve kripto paraların üstüne çekmiş, akabinde konunun uzmanı olmayan ancak büyük takipçilere sahip haber platformları tarafından blockchain ve kripto para kavramları moda kelimeler haline gelmiştir ancak teknoloji olarak Blockchain tarihi daha eskiye dayanmaktadır. 1980'lerin sonlarında ve 1990'ların başlarında ağ mühendisleri güvenliği ihlal edilmiş veya güvenilmez bilgisayarların olduğu ağlarda yaşanılan güvenlik sorunlarını çözmeye yönelik fikirler üretmeye çalışıyorlardı. Bu sorunu çözmeye yönelik en eski adım, Leslie Lamport'un "The Part Time Parliament" isimli eserinde yer almaktadır (1998, s.133–169). Lamport'un geliştirdiği "Paxos algoritması" kavramı daha sonra Bitcoin'in yapı taşlarından birisi olacaktır (Yaga vd., 2018, s. 2).

Blok zinciri teknolojisi, Iansiti ve Lakhani (2017, s.118-127) tarafından, büyük ve merkezi olmayan yani tek bir varlığın kontrol etmediği, halka açık bir ağ içinde eşzamanlı olarak kullanılabilen ve paylaşılabilen bilgileri (finansal işlem kayıtları gibi) içeren dijital bir veri tabanı olarak tanımlanmıştır. Her biri mesajı diğerlerine gönderen düğümler aracılığıyla eşler arası iletişim sağlayan blok zinciri işlemleri programlanabilir ve blok zinciri tarafından oluşturulan kayıtlar kalıcıdır.

Her blok zinciri kullanıcısı, 30 artı karakterli bir adresle tanımlanır. Teknolojinin temelinde işlevlerin tutarlılığını sağlamak amacıyla "kriptografik karma işlevi" (cryptographic hash function, CHF) adı verilen işlem kullanılır. Makalede bundan sonra hash fonksiyonu olarak adlandırılacak bu fonksiyon ile dokümandan yazılara kadar değişebilen her girdiye özel bir çıktı hesaplanmaktadır. En basit anlamıyla girdi verisi (message) CHF ile tekrar hesaplanarak bir çıktı (digest) elde edilmektedir. Blok zinciri uygulamasında en çok rastlanan uygulamalardan biri olan Secure Hash Algorithm 2 (SHA-2), Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı (NSA) tarafından geliştirilmiş ve SHA-256 ve SHA-512 olmak üzere bit cinsinden iki çıktı düzenine sahiptir. 1 bayt 8 bit olduğu göz önüne alındığında SHA-256 32 bayt çıktı vermekte ve bu çıktı 64 karakter yazı olarak görüntülenmektedir. Blockchain yazısı bu algoritma üzerinden hesaplandığında çıktı şöyledir: *EF7797E13D3A75526946A3BCF00DAEC9FC9C9C4D51DDC7CC5DF888F74DD434D1*. 1 bit 0 ve 1 olmak üzere 2 farklı duruma sahip olduğu için toplamda 2256 ya da 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936 olası kombinasyona sahip SHA-256 algoritması, günümüzde kullanılan çoğu bilgisayar sistemi ile uyumlu olması nedeniyle birçok blok zinciri uygulaması tarafından tercih edilmektedir (Yaga vd., 2018, s. 7). Yukarıda verilen kombinasyonun büyüklüğü göz önüne alındığında çıktıdan girdiyi elde etmeye çalışmak günümüz teknolojisiyle mümkün değildir. Bu durum, işlemlerin güvenirliğinin ağdaki paydaşlar tarafından doğrulandığı dağıtılmış, şeffaf, değiştirilemez ve güvenli bir veri yapınsa sahip blok zinciri teknolojisine güven duyulmasında en büyük etkenlerden biridir (Reyna vd., 2018, s.173-190).

Ekonomik ve sosyal sistemlerimiz için yeni temeller yaratma potansiyeline sahip blok zinciri teknolojisinde kullanılan CHF yöntemini, benzersiz tanımlayıcılar oluşturmak, cüzdan adresleri oluşturmak, blok başlıklarında önce bloğun digest değerini saklamak gibi birçok farklı işlemde kullanmaktadır. Her ne kadar uygulamalar arasında farklılıklar olsa da genel olarak kriptografik algoritmaların birleşimi olan blok zincirleri bu şekilde işlemektedirler (Yaga vd., 2018, s. 8).

Kripto Para Kavramı

Blockchain'e çok benzer şekilde, kripto para birimleri, kriptografi tekniğini kullanan çok çeşitli teknolojik gelişmeleri ifade eden bir "moda sözcük" haline geldi. Basit bir ifadeyle, kriptografi, bilgiyi yalnızca gizli bir anahtara sahip biri tarafından deşifre edilebilen (veya şifresi çözülebilen) okunamayan bir biçime dönüştürerek (yani şifreleyerek) koruma tekniğidir. Bitcoin gibi kripto para birimleri, ustaca bir genel ve özel dijital anahtar sistemi kullanılarak bu teknikle güvence altına alınır (Houben ve Snyers, 2018, 20). Kripto para, eşler arasında geçerli, devlet destekli yasal ödeme aracına alternatif olarak, herhangi merkezi bir bankadan bağımsız olarak genel amaçlı değiş tokuş aracı olmak üzere, kriptografi adı verilen sistemle güvenliği sağlanan, yasal ödeme araçlarıyla değiş tokuş edilebilen bir değerin dijital temsilidir (Houben ve Snyers, 2018, s. 23).

Ocak 2021 dönemi itibariyle piyasa değerine göre ilk on sıralamadaki kripto paralar ve dolaşım miktarları Tablo 1'de verilmiştir. Ocak 2021 tarihi itibariyle CoinMarketCap adlı kripto paraların takip edilmesine yarayan web sayfası toplamda 3981 farklı kripto para çeşidinin işlem gördüğünü göstermektedir.

Tablo 1: Piyasa Değerlerine Göre İlk On Sıradaki Kripto Paralar (Ocak 2021)

İSİM	PİYASA DEĞERİ	DOLAŞAN MİKTAR
Bitcoin (BTC)	$636,201,099,684	18,614,718 BTC
Ethereum (ETH)	$156,504,395,713	114,465,286 ETH
Tether (USDT)	$26,365,837,774	26,341,141,890 USDT
XRP (XRP)	$15,816,112,994	45,404,028,640 XRP
Palkadot(DOT)	$15,123,587,425	905,477,183 DOT
Cardano (ADA)	$10,947,640,550	31,112,484,646 ADA
Chainlink (LINK)	$9,334,564,697	404,009,556 LINK
Litecoin (LTC)	$8,941,326,396	66,382,415 LTC
Bitcoin Cash (BCH)	$7,667,140,181	18,641,100 BCH
Stellar (XLM)	$6,985,510,753	22,253,501,805 XLM

Kaynak*:* CoinMarketCap, Ocak 2021.

Her ne kadar Bitcoin dijital parayı ana akım haline getirmiş olsa da, bu alandaki ilk örnek değildir. Bitcoin takip edilemez elektronik ödeme kolaylığı ile tanınmadan önce, aynı sonuçları elde etmek için başka girişimler de bulunmaktadır. David Chaum "Blind Signatures for Untraceable Payments" adlı eserinde ileride Bitcoin ve diğerlerine temel oluşturacak elektronik ödeme sistemini öne sürmüştür (Chaum, 1983). Chaum'un fikri eCash adı altında gerçekliğe kavuşmuş ancak güvenilir üçüncü bir kişi tarafından kullanıcılarının bilgisayarlarındaki paranın varlığını kanıtlamasını gerekli kılmıştır ve gerekli başarıya ulaşamamıştır. Chaum'un çalışması, izlenemeyen para transferleri sağlamak üzerine inşa edilmiş olsa da, sadece fonların doğrulanması için üçüncü bir tarafa güvenmek zorunda kalmak, Satoshi Nakamoto takma adını kullanan Bitcoin'in geliştiricisi tarafından 2008'de yayınlanan makalesinde kabul edilemez görüldü. Nakamoto'ya göre, tüccarları dolandırıcılık ve işlemin tersine çevrilmesi olasılığı ile yüzyüze bırakan güvene dayalı bir sistem zayıftı. Nakamoto'ya göre elektronik ödeme sistemleri "güven yerine kriptografik kanıta" dayanmalıydı (Nakamoto, 2008, s. 1).

İzinsiz yani herhangi bir düğümün istediği herhangi bir zamanda herhangi bir merkezi otoritenin iznine dayanmaksızın ağa girip çıkabildiği blok zincir uygulamalarının en çok bilinen örneği olan Bitcoin, açık kaynak kodlu bir blok zincirinde kanıta dayalı uzlaşma (proof-of-work consensus) yöntemiyle çalışmaktadır. Buna göre ağda bir blok yayımlayabilmek için düğümler hesaplama açısından yoğun bir bulmacayı çözmek zorundadırlar. Bitcoin'in yapımcısı Satoshi Nakamoto, ağdaki blok yayımlama hızını saatte ortalama sayıda tutacak bir zorluk seviyesi belirlemiş ve ağda hesaplama gücü arttıkça artacak şekilde programlamıştır (Nakamoto, 2008, s. 3). Bu da yüksek düzeyde elektrik tüketimini ortaya çıkarttığı için kanıta dayalı uzlaşma bazlı blok zinciri uygulamalarının en çok eleştirildiği yönüdür. Bitcoin'i duyurduğu yazısında Nakamoto bunun bir saldırganın hesaplama gücü üzerinde tekel kurmasını önlemek ve ağın devamlılığını sağlamak için mutlak gerekli olduğunu savunmaktadır (Nakamoto, 2008, s. 3). Yukarıda bahsedilen bulmaca çözme işlemine kripto uzayında madencilik (mining) denmektedir. Bu bulmacayı çözerek blok yayımlayan düğüm ise o blok zinciri uygulamasının kendi kripto parası ile ödüllendirilmektedir ve böylelikle ağın devamlılığını sağlayacak aktörlerin katılımı teşvik edilmektedir.

Nakamoto'nun ortaya koyduğu sistemin sağladığı yarı anonimlik, blok zinciri teknolojisi hakkında yeterli bilgi sahibi olunmadığı için kitle medya araçları ve haber platformlarınca tüm kripto paraların takibinin imkânsız olduğu kanısının ortaya çıkmasına neden oldu. Dizaynı itibariyle Bitcoin, ağda gerçekleşen tüm

işlemlerin halka açık ve herkes tarafından doğrulanabilir olması üzerine kuruludur. Ancak tüm kripto paralar bu saydamlık ilkesine dayanmamaktadır. Bu tür kripto paralardan olan Monero ve Monero'nun yasa dışı aktivitelerin finansmanındaki yerine ilerleyen bölümlerde değinilmiştir. Saydam blok zincirlerine dönecek olursak, saydam blok zincirleri ağda bulunan tüm hesapların, bu hesaplardaki fonların ve bu hesaplar arasındaki işlemlerin herkesin görebileceği şekilde defterde tutulmasına dayanmaktadır. Ancak buna rağmen, hesaplar sahiplerine dair hiçbir veriye sahip değildirler ve yeni hesap edinmek oldukça kolaydır.

Kripto Para Dünyasının Aktörleri

Kripto para biriminin kendi oyuncuları bulunmaktadır ve her oyuncu, bu büyük ölçüde yasal düzenlemeden yoksun piyasada farklı bir rol oynamaktadır. Bu başlık altında, bazı kilit aktörler ve oynadıkları roller ele alınacaktır.

- ***Kullanıcılar***

Kripto para kullanıcıları, mal ve hizmet satın almak, ödeme yapmak veya yatırım amacıyla kripto para birimleri elde eden gerçek veya tüzel kişilerdir. Kullanıcılar kripto para birimlerini çeşitli şekillerde edinebilir.

- Kanıta dayalı uzlaşma ağlarında kripto para biriminin yeni birimleri madencilik ile edinilebilir. Yeni blok yayımlayan düğümler genellikle 'kriptografik bulmacalarını' çözerek devamlılığını sağladıkları blok zinciri tarafından o zincirin para birimiyle ödüllendirilmektedir.

- Kullanıcılar kripto paralara devlet destekli para birimleri ile kripto paraların değiş tokuş yapıldığı borsalardan gerçek para vererek satın alabilirler. Bu genel olarak çoğu kullanıcının kripto para dünyasına ilk adımıdır. Bir kullanıcı bir çeşit kripto para birimine sahip olduğunda, söz konusu para birimini o platformda listelenen diğer herhangi bir kripto para birimine dönüştürmek için merkezi olmayan borsalara aktarabilirler.

- Kullanıcı ayrıca, "İlk Para Teklifi (Initial Coin Offering, ICO)" gibi şemalardaki belirli kripto para biriminin kaynağından doğrudan kripto para birimini edinebilir.

- Kullanıcı mal veya hizmet satıyorsa, ödemeyi kripto para biriminde almayı tercih edebilir.

- Kullanıcının halihazırda bir blok zincirinde kripto para birimine sahip olduğunu varsayarsak, genellikle blok zincirinin eski versiyonunun desteklemediği yeniliklerin kabul edildiği durumlarda gerçekleşen "hard-fork" ile yeni blok zincirinde de aynı miktarda para birimine sahip olurlar. Bitcoin (BTC), Bitcoin Cash (BCH) veya Bitcoin Satoshi Vision (BSV) birçok kez "hard-fork" geçirmiş ve farklı blok zincirlerine sahiptir.

- Bir kullanıcı başka bir kullanıcıdan hediye olarak kripto para alabilir (Houben ve Snyers, 2018, s. 25).

- ***Madenciler***

Kanıta dayalı uzlaşı ağlarında blok zincirinin devamlılığını yeni blok üretmek için sunulan kriptografik bulmacayı çözerek sağlayan madenciler, o blok zincirinin kripto parasıyla ödüllendirilir ve böylelikle blok zincirinin devamlılığını sağlamak için teşvik edilirler. Madenciler elektrik harcanarak oluşturulan hesaplama gücünü kripto para edinmek için harcarlar. Kanıta dayalı uzlaşı yöntemlerinin temel noktası olan bu değiş tokuş bireysel olabildiği gibi Çin'de örnekleri bulunan 'maden çiftliği' kurulabilecek kadar büyük boyutlarda da olabilir (Houben ve Snyers, 2018, s. 25-26).

- ***Borsalar***

Yerine getirdikleri role bağlı olarak, iki yaygın kripto para birimi borsa türü vardır. Birincisi, borsada yer alan ve kullanıcıların istekleri doğrultusunda devlet destekli para birimlerinin yanı sıra kripto paraların da alım satımının yapıldığı merkezi borsalardır. CoinBase, Gemini, Binance gibi borsalar merkezi borsalara örnek olarak gösterilebilirler. İkincil tip borsalar ise merkezi olmayan, yalnızca yazılım tarafından kontrol edilen ve alıcılar ile satıcılar arasında köprü rolü kuran borsalardır. Merkezi borsalara yasal düzenleme getirilerek bulundukları devlet sınırları içinde belli finansal standartlara uymaları sağlanabilirken merkezi olmayan borsalarda yasal düzenleme yapılması mümkün olmamaktadır (Houben ve Snyers, 2018, s. 26-27).

- ***Kripto Para Üreticileri***

Kripto para birimi üreticileri, blok zinciri tabanlı bir kripto para biriminin ve onun kural setinin omurgasını oluşturan ve genellikle geliştirici olarak adlandırılan bir grup bireydir. Bu kişilerin kimlikleri her durumda kamuya açık olmayabilir. Bu kişiler ilk blok zincirini oluşturmuş olabilir, ancak blok zincirinin başlatılmasından sonraki herhangi bir değişiklik, çoğunluk tam düğümlerin bu sürüme güncellenmesini gerektirir. Bu da geliştiricilerin ürettikleri blok zinciri uygulaması üstündeki güçlerini kısıtlamaktadır (Houben ve Snyers, 2018, s. 28).

- ***Kripto Para Teklifçileri***

Geliştiriciler ürettikleri kripto paraları belli bir ücretten satar ya da ücretsiz olarak sunarlarsa kripto para teklifçileri olarak sınıflandırılırlar. Kanıta dayalı uzlaşma blok zincirlerinde belirli bir miktar para daha üreticilerin inisiyatifinde kullanılmak amacıyla önceden basılabilir (Houben ve Snyers, 2018, s. 28).

Kripto Para Çeşitleri

Kripto para birimleri şeffaf ve gizlilik odaklı kripto para birimleri olarak iki kısma ayrılmaktadır. Terörizm ve illegal faaliyetlerin finansmanında kripto paraların rolünün açığa kavuşturulması açısından bu tasnif önem taşımaktadır.

- ***Şeffaf Kripto Para Birimleri***

Bitcoin ve bugün dolaşımdaki en popüler blok zinciri uygulamalarından bazıları, halihazırda blok zincirinde saklanan tüm bilgileri halk açık bir şekilde saklamaktadırlar. Bu da, gelen veya giden tüm işlemlerin, fonların kendisinin ilk oluşturulma noktasına kadar hesaplar arasında kolayca izlenebileceği anlamına gelir. Satoshi, elektronik paraya güven ihtiyacını ortadan kaldırmaya ve ağ çapında yayınlanmış

işlemlerle çifte harcamayı çözmeye çalışmış olabilir ancak, Bitcoin ve benzer blok zincirleri tarafından sağlanan sözde anonimlik, şüpheli fonların takibini nispeten kolaylaştırır.

- *Bitcoin*

Avrupa Polis Teşkilatı'nın 2017'de yayınlanan "Internet Organized Crime Threat Assessment" raporuna göre gizlilik odaklı kripto para birimleri popülerlik kazanırken, Bitcoin hala dark-web piyasalarında ve diğer yasa dışı faaliyetlerde en çok tercih edilen ödeme yöntemidir (Europol, 2017, s. 13). Daha önce de belirtildiği gibi, adres sahiplerinin gerçek bilgileri blok zincirinin kendisi aracılığıyla tespit edilemese de, Bitcoin blok zincirinin şeffaf yapısı nedeniyle yasa dışı faaliyetlerle ilişkili bilinen adresler ve aralarında aktarılan fonlar kolayca izlenebilir. Vergilendirme açısından Bitcoin, para birimi yerine mülk olarak kabul edilir ve bu gelir yalnızca Bitcoin devlet destekli para birimlerinden birine dönüştürüldüğünde ortaya çıkar. Bu nedenle Bitcoin, yetkililer tarafından "sanal bir off-shore vergi cenneti" olarak görülmektedir (Engle, 2016, s. 379).

- *Ethereum*

Nakamoto tarafından gerçekleştirilen güvensiz sistemin izinden giden Ethereum, akıllı sözleşmeler (smart contracts) ile kripto para birimlerine yeni bir özellik getirdi. Başlangıç olarak 1994 yılında, kripto para biriminin önde gelen aktörlerinden Nick Szabo tarafından "bir sözleşmenin şartlarını yerine getiren bilgisayarlı bir işlem protokolü" olarak tanımlandı (Yaga vd., 2018, s. 32). Ethereum'un akıllı sözleşme tasarım uygulaması, ortak sözleşme yükümlülüklerini yerine getirmek için kötüye kullanılabilecek veya kazara oluşabilecek durumlara karşı, güvenilir üçüncü taraflara ve istisnalara olan ihtiyacı en aza indirmeye çalışır. Ethereum, kanıta dayalı uzlaşma altyapısına sahip izinsiz bir blok zinciri olduğundan, sözleşmeyi düzenleyen kullanıcı, blok yayınlamanın düzgünlüğünü korumak için, işlevsellik açısından sınırlı olan ve belirli yürütme süresi kurallarına uyması gereken akıllı sözleşme kodunun zincir üstünde yürütülmesi için ödeme yapmalıdır. Ethereum, tıpkı Bitcoin gibi, akıllı sözleşmeyi yürüten tüm düğümlerin aynı sonuca ulaşmasını sağlamak için akıllı sözleşmeleri ve kodlarını içeren şeffaf bir blok zincirine sahiptir, böylelikle blok zincirinin deterministik yönünü korur (Yaga vd., 2018, s. 33).

- ***Gizlilik Odaklı Kripto Para Birimleri***

Bir kripto para biriminin gizlilik odaklı bir kripto para birimi olarak görülmesi için bir dizi hedefe ulaşması gerekir. Gizlilik odaklı en yaygın kripto para birimlerinden ikisi olan Monero (XMR) ve ZCash (ZEC) şu ortak hedeflere sahiptir:

- ✓ Gizlilik: Bir işlemde aktarılan tutar kamuya açıklanmayacaktır,
- ✓ İzlenemezlik: Harcanmış para birimi, üretildiği yere bağlanamaz,
- ✓ Bağlantısızlık: Bir saldırgan, bir ağa ait iki adresin aynı kullanıcıya ait olup olmadığını belirleyemez,
- ✓ Kullanıcı Anonimliği: Bir kullanıcının adresini bilen bir düşman, o kullanıcının ağa nasıl bağlandığını belirleyememelidir (Tramèr vd., 2019, s. 4-5).

- *Monero (XMR)*

2014 yılında izinsiz blok zinciri üzerinde çalışan ve kanıta dayalı uzlaşma altyapısını kullanmak üzere başlatılan Monero, hem gönderme hem de alma adreslerini ve transfer miktarını kriptografik olarak koruyarak kullanıcı işlemlerinin tamamen anonim olmasını sağlayan bir kripto para birimi formudur. DEAŞ, dark-web de yer alan web sayfasında, tercih ettiği bağış yöntemini Monero olarak değiştirmiş ve artık Bitcoin kabul etmediğini belirtmiştir (Harper, 2020). 2018'deki bir siber saldırıyla olan ilişkileri nedeniyle Amerika Birleşik Devletleri Yabancı Varlık Kontrol Bürosu'nun (OFAC) iki İran vatandaşına ait Bitcoin hesaplarını kara listeye almasından görülebileceği gibi, bazı kripto paralar terörizm, kara para aklama ve kumar gibi yasa dışı faaliyetlerle ilişkili olarak izlenebilir ve bu hesaplar devletlerce kara listeye alınabilir (Möser ve Narayanan, 2019, s. 1). Monero'nun anonim doğası göz önüne alındığında, bu tür etkinlikleri izlemek imkânsız olmaktadır ve bu nedenle yasa dışı aktivitelerle ilişkili belirli XMR birimlerini kara listeye almak da teknik olarak mümkün görülmemektedir (Houben & Snyers, 2018, s. 46).

- *Verge (XVG)*

Yine 2014'te ortaya çıkan ve başlangıçta DogeDarkCoin olarak piyasaya sürülen, 2016'da Verge olarak yeniden adlandırılan Verge, kullanıcıların anonimliğini bir adım öteye taşımış ve TOR ile The Invisible Internet Project'i (I2P) yazılımında aktifleştirerek, kullanıcılarının İnternet Protokolü (IP) adreslerinin toplanmasına karşı önlemler almaya çalışmıştır. Invisible Internet Project, TOR'a bir alternatif olarak ortaya çıkmış ve internet üzerindeki diğer bilgisayarlarla iletişim kurarken kullanıcıları anonim hale getirmek için tasarlanmış bir anonim ağdır. TOR, devlet aktörü temelli İnternet sansürüne ve filtrelere çok daha dirençli iken I2P, kullanıcılarına benzer anonimlik sağlamak için az bilinen ve az saldırıya uğrayan bir anonim ağ olmasının getirdiği güvenliğe güvenmektedir (The Invisible Internet Project, 2018). Bu iki anonimlik teknolojisinin eklenmesi ile Verge, daha fazla kimlik koruması sunarak rakiplerinin önüne geçmeye çalışmıştır (Koerhuis vd., 2020, s. 3). Ancak buna rağmen Europol'ün 2017 raporunda Verge'den bahsedilmemiş ancak Bitcoin başta olmak üzere Monero'nun yasa dışı faaliyetlerde kullanımında bir artış gözlendiğine vurgu yapılmıştır (Europol, 2017, s. 13).

Blok Zinciri Teknolojisinin Yarattığı Fırsatlar ve Zorluklar

Blok zinciri teknolojisinin tedarik zinciri yönetimi, güvenlik ve gizlilik, nesnelerin interneti, müşteri tanıma, oy kullanma sistemleri, tapu kayıt- eğitim- enerji- küresel ödeme işlemleri, dijital kimlik yönetimi, kamu ve sağlık kayıtları ile ihaleler (Zheng vd., 2018, s.354), bağış toplama ve yönetimi, mal ve kaza sigortası tazmin süreci gibi bireysel ve toplumsal refahı artıracak potansiyel farklı kullanım ve uygulama alanları bulunmaktadır.

Blok zincirinin kendisi gerçekten yeni bir teknoloji olmasa da en yaygın bilinen kripto para birimlerinden biri olan Bitcoin'deki son fiyat sıçramaları, teknolojinin kendisine daha fazla dikkat çekmiştir. Kripto paralar ve blok zincirlerinin global olarak yasal düzenlemeler çerçevesine oturtulmamış olması ve yasa dışı

faaliyetlerde çok kullanılması, teknolojiyi çevreleyen alanda suçluların türemesine ve barınmasına olanak tanımaktadır. Bu bölümde blok zinciri teknolojisinin yarattığı fırsatlar ve zorluklar ele alınarak, yasal alandan yetersiz yönetişimin yarattığı problemlere değinilecektir.

- ***Değişmezlik Efsanesi***

Blok zinciri teknolojisinin en önemli avantajlarından birisi müdahalelere karşı dirençli olmasıdır. Bu noktada belirtmek gerekir ki, müdahaleye karşı dirençli olmak ile müdahale edilemez olmak tamamen farklı şeylerdir (tamper-resistant, tamper-proof). Bir blok zincirine müdahale edebilmek oldukça maliyetlidir. Genel olarak çoğunluk saldırısı ya da %51 saldırısı olarak bilinen bu saldırı, devlet düzeyindeki aktörler için ulaşılamaz değildir. İzin gerektirmeyen blok zinciri uygulamaları için %51 saldırısı blok zincirinde blok üretiminin bir saldırganın tekeline geçmesi anlamına gelmektedir. Yeterli hesaplama gücüyle bir saldırgan ele geçirdiği blok zincirinde gerçekleşen işlemleri olmamışçasına geriye çevirebilir ya da bazı hesapların harcama yapma kapasitesini engelleyerek ödemelerin aksamasını ve blok zincirine olan güvenin yok olmasına neden olabilir (Greenspan, 2017).

Bitcoin ağı örneğine bakıldığında ağda blok üretiminde kullanılan en yaygın bilgisayar birimleri "Uygulamaya Özel Entegre Devreler (Application Specific Integrated Circuits, ASICs)" olarak bilinen devrelerle yapılmaktadır. Bu devrelerin hesaplama yöntemleri halihazırda devletlerin sahip olduğu süper bilgisayarlardan farklıdır. Bu da devletlerin kaynak harcaması yapmadan blok zincirlerine müdahale etmelerini zorlaştırmaktadır (Yaga vd., 2018, s. 34). İzne dayalı blok zinciri uygulamalarında, Nakamoto'nun karşı olduğu güvenilen bir üçüncü parti yer aldığı için %51 saldırısını yapmak dışarıdaki bir taraf için daha zordur. Blok üretimi blok zincirinin yöneticilerinin yönetimi dahilinde gerçekleştiği için herhangi bir saldırıya karşılık verilmesi görece olarak kolaylaşmaktadır.

- ***Blok Zincirlerinin Sahipleri Yoktur***

Yaygın yanılgılardan biri, izinsiz blok zincirlerinin herhangi bir kuruluşa ait olmadığı ve çalışan madenciler olduğu sürece hayatta kalacakları inancıdır. Blok zincirlerinin ölümü gerçekleşebilen bir durumdur ve örnekleri mevcuttur ancak bu makalenin konusu dışında kaldığı için değinilmemiştir.

Herhangi bir blok zinciri için etkileşim içinde olan üç farklı aktör kategorisi vardır. Blok zincirini kullanan kullanıcıları, blok zinciri üzerindeki kripto para birimini gönderir ve alırlar. İkinci aktör, blok zincirinin kodunu yazan, güncelleyen ve sürdüren yazılım geliştiricilerdir. Son aktör ise yeni bloklar oluşturarak, işlemlerin kayıtlarını tutarak, işlemleri doğrulama yeteneği olan bir blok zincirinin devamlılığını sağlayan madenciler olarak bilinen düğümlerdir. Yazılım geliştiricileri tarafından blok zincirinin kodunda yapılan herhangi bir ek özellik ya da değişiklik, blok zinciri programını yeni bir sürüme güncelleyerek düğümler tarafından kabul edilmelidir. Bu değişikliklerin düğümlerden yeterince destek alamaması durumunda (yeni sürüme güncelleme yapılmadığı takdirde), blok zinciri 'hard-fork' ile ikiye bölünecektir. Ayrılma noktasından sonra farklı işlemlere sahip iki farklı blok zinciri ortaya çıkmaktadır. Bu, esasen blok zincirlerinin genellikle iki farklı aktör tarafından yönetildiği ve zinciri canlı tutmak için bu iki aktörün iş birliği yapmak zorunda oldukları anlamına gelir (Yaga vd., 2018, s. 35).

- ***Blok Zincirleri Anonim Oldukları İçin Yasal Düzenlemelerden Muaftırlar***

Kullanıcı gizliliğini en önemli koşul olarak nitelendiren blok zincirlerinin yasa dışı faaliyetler için sağlayacağı faydalarla başa çıkmak için şu ana kadar kullanılan ve Mali eylem Görev gücü (FATF) tarafından güncellenen kara para aklama ve terörizmin finansmanıyla mücadele yöntemleri yetersiz kalmaktadır. Sanal varlıklar olarak nitelendirilen kripto paraların statüsüne dair global bir görüşün yer almayışı, devletleri ve devletlerarası örgütleri bu tip sanal varlıklara bireysel düzenlemeler getirmeye zorlamıştır. Bu düzenlemede yer alan boşluklar, kripto para hesaplarına yönelik kimlik tespit ve takibinin yüksek maliyetli analizler gerektirmesi (Yurdakul, 2019, s.433), zayıf finansal kontrolün olduğu ülkelerde var olan kripto para borsaları aracılığıyla kara para aklama ve terörizm finansmanı risklerini artırmaktadır (Poskriakov vd., 2020).

FATF'in yayımladığı öneri niteliği taşıyan raporlara göre sanal varlık hizmet sağlayıcıları yani kripto paraların alınıp satılabildiği borsalar, finansal kurumların tabi olduğu kara para aklama ve terörizm finansmanı önlemlerini etkinleştirmekle yükümlü kılınmalıdır (FATF, 2020, s. 16). Bu nedenle, finansal kurumların başlattığı müşterilerini tanımak amacıyla kişisel bilgilerinin toplanması ve elde tutulması uygulaması, kripto para borsalarında son dönemde artarak uygulamaya başlamıştır. FATF bu önlemlerin kara para aklama, vergi kaçırma ve terörizmin finansmanı gibi yasa dışı faaliyetlerin önüne geçilmesi için gerekli olduğu savunmaktadır. Ancak buna rağmen asıl zorluk, zaten finansal olarak düzenlemelerin ve kanun yaptırımlarının yetersiz kaldığı bölgelerde kurulan kripto para borsalarının bu düzenlemelere uymayarak kripto para ile devlet destekli paralara değiş tokuşa olanak sağlamasından kaynaklanmaktadır (Salami, 2017, s. 972). Ayrıca devlet destekli paralarla değiş tokuş olanağı sağlamayan kripto para borsalarında yapılan sanal varlık değiş tokuşlarında kolaylıkla yasal düzenleme yapılamayışı problemi artırmaktadır (Adenyanju, 2019). Chainalysis'in 2020 raporunda yer alan verilere göre yasa dışı faaliyetlerde kullanılan kripto paralar FATF'in önerilerini hayata geçirmiş büyük borsalarda işlem görmekte ve devlet destekli para birimlerine bu borsalarda var olan ve gerçek dünyada aleni satışla (Over-the-counter, OTC) kripto para birimleri satan satıcılar sayesinde dönüştürülmektedir (Chainalysis, 2020, s. 12).

Bütün bu zorluklar Bitcoin gibi şeffaf bir blok zinciri uygulamasında yaşanmaktadır. Monero örneğinde ise hiçbir işlem kamu açık olarak görülemediği için takibi oldukça zordur. Bu yüzden 2020 Eylül ayında Amerika Birleşik Devletleri Gelirler İdaresi (IRS), Monero'da işlem takibinin sağlanmasına yönelik açtığı 625.000$ ödüllü ihalesini Integra FEC LLC ve Chainalysis Inc. Şirketlerine vermiştir (U.S. Internal Revenue Service, 2020).

- ***Blok Zinciri Teknolojisi Halen Tam Olarak Anlaşılmamıştır***

Blockchain bir teknoloji olarak şu anda tam olarak anlaşılmamış ve tamamlanmamıştır. Blok zinciri, dağıtılmış defter teknolojisinin bir biçimi olsa da, kripto para birimi bu teknolojinin yalnızca tek bir uygulamasıdır. Teknolojinin kendisi için pek çok meşru kullanım durumu olabilir, ancak Attaran ve Gunasakeran (2019, s. 10-11) tarafından bu teknolojinin benimsenmesinin önündeki bazı engelleri detaylandırmışlardır. Attaran ve Günasekaran'a göre mevcut blok zinciri teknolojisi tam olarak bilinmiyor ve güvenilmiyor. Blok zincirinin tamamlanmadığı veya tam olarak anlaşılmadığı göz önüne alındığında,

kurumsal düzeyde uygulamayı birçok şirketin bütçesinin ötesinde büyük ve riskli bir yatırım haline getirmektedir.

Blok zincirinin benimsenmesinin önündeki önemli engellerden birisi de siber güvenlik açısından blok zincirinin yeteneklerinin tam olarak kanıtlanmamasıdır. Finansal uygulamalar olmasa bile, merkezi olmayan mülkiyet konuları, teknolojiyi benimsemek isteyen kurumsal düzeydeki aktörler için belirli yasal zorlukları çözmeleri gerekeceği anlamına gelmektedir. Bunların yanı sıra blok zinciri teknolojisin en büyük eksisi olarak işlem hızı kapasitesi görülmektedir. Daha önceki veritabanı teknolojilerine kıyasla, Bitcoin örneğinde, bütün ağın İrlanda kadar elektrik tüketmesine rağmen sonuç olarak saniyede ortalama 7 işlem yapabilirken finans sektöründe liderlerden Visa saniyede 1700 işlem yapabilmektedir (Attaran ve Gunasekaran, 2019, s. 10-11).

Terör ve Diğer İllegal Aktivitelerin Finansmanında Kripto Paraların Rolü

Devlet destekli para birimlerine kıyaslandığında kripto para birimleri merkezi bir otorite tarafından desteklenmemektir. TOR veya I2P gibi bazı araçlarla internette anonim kalmak daha kolay hale gelmiştir ancak kripto para söz konusu olduğunda gerekli olan teknik uzmanlık ihtiyacı artmaktadır. Bitcoin ve diğer kripto para birimlerinin çoğu kullanıcılarına sözde anonimlik sunabilmektedirler ancak bu fonlar anonim olarak edinilmiş veya bu bölümde açıklaması yapılacak olan karıştırıcılar aracılığıyla aklanmış olsa bile, bu kripto para birimlerini itibari para birimine dönüştürmek en büyük zorluk haline gelmektedir. Yasal düzenleyiciler için blok zincirlerini analiz etmek ve işlemleri izlemek için bir araç sunduğunu iddia eden Chainalysis Şirketi tarafından yayınlanan bir rapora göre, terörizmin finansmanında blok zincirinin kullanımı hala emekleme aşamasında iken, kara para aklama ve kripto paraların son dönemdeki popülerliklerinden faydalanarak hızlıca zengin olmak isteyenleri hedefleyen dolandırıcılar, blok zincirindeki suç faaliyetinin en büyük bölümünü oluşturur. Rapora göre 2020 Ağustos sonunda ABD Adalet Bakanlığı'nca yürütülen ortak operasyonla son verilen İzzeddin el-Kassam Tugayları'nın bağış kampanyası, blok zincirinde şu ana kadar görülmüş en sofistike terörizm finansmanı kampanyasını oluşturuyor (Chainalysis, 2020, s. 73).

Dark-web üstünde ateşli silahlardan çocuk pornosuna, uyuşturucudan sahte kimliklere kadar büyük bir kara borsanın varlığının yanı sıra, teröristlerin davalarına militan topladıkları ve eğitim materyalleri yayınladıkları bir yer haline gelmiştir (Weimann, 2016, s. 196). 2015 yılında ABD Hazine Bakanlığı'nın yayımladığı Terörün Finansmanı Risk Değerlendirme Raporunda kripto paraların mali işlemler yürütmek için çekiciliğine vurgu yapılmış ve terörist grupların bu yeni ödeme sistemlerini Amerika Birleşik Devletleri'nde toplanan fonları terörist gruplara ve onların ABD dışındaki destekçilerine transfer etmek için kullanması olasılığına dikkat çekilmiştir (U.S. Department of the Treasury, 2015).

2020 Ağustos ayında ABD Adalet Bakanlığı terörizm finansmanında kullanılan 155 Bitcoin hesabını ele geçirildiğini ve bu hesaplarla bağlantılı olarak üç farklı terörist gruba finansman sağlamak amacıyla oluşturulmuş yardım kampanyalarının durdurduğunu belirtmiştir. İzzeddin el-Kassam Tugayları'na bağış toplamak üzere oluşturulan ilk yardım kampanyasında ABD kolluk kuvvetlerince ele geçirilen bilgisayar ekipmanları, İzzeddin el-Kassam Tugayları sempatizanlarını belirlemek için kullanılmıştır. İkinci yardım kampanyasında ise El-Kaide ve buna bağlı örgütlerin "terörist hedeflerini ilerletmek için kripto para birimi

bağışları talep etmek için Telegram kanallarını ve diğer sosyal medya platformlarını kullanan bir Bitcoin kara para aklama ağı" işletilmekteydi (U.S. Department of Justice, 2020). Üçüncü kampanyada, Murat Çakar adında DEAŞ üyesi bir bilgisayar korsanı, Covid-19 salgını sırasında DEAŞ'ı finanse etmek için dünya çapındaki müşterilere sahte kişisel koruyucu ekipman satmayı planlıyordu. Dava dosyalarında geçen bazı Bitcoin adreslerinin açık kaynak istihbarat ile toplanan bilgilerle terörizmle bağlantılı oldukları kamuoyunca biliniyordu.

Bitcoin, yakın tarihe kadar suç dünyasında kullanılan tek kripto para ödeme aracıydı ancak Europol Raporu'na göre (2017, s. 13) son yıllarda suçluların Monero'yu benimsemeye başladığını belirtmiştir. Bitcoin'in şeffaf bir blok zincirinde olması, işlemlerin izlenmesini ve halka açık kayıt tutulması nedeniyle fidye veya kara para aklama gibi yasa dışı faaliyetlerle bağlantılı olan paraları ayırt etmeyi mümkün kılmaktadır. Kripto paralar arasında mikser görevi gören Tumblers adlı araç, lekelenmiş kripto paralardan etkin bir şekilde "lekeyi temizleyebilen" ve onları devlet destekli para birimleri ile takas etmelerini kolaylaştırmak için temiz paralarla karıştırabilen bir hizmet sunmaktadır. DarkLaunder, BitLaunder, CoinMixer ve CoinJoin gibi hizmetler, Bitcoin kullanıcılarına paralarını küçük bir ücret karşılığında temiz paralarla karıştırma olanağı sunmaktadır (de Balthasar ve Hernandez-Castro, 2017, s. 297-299).

Kripto para aklama süreci, kirli kripto paralar olarak adlandırılanlarla karıştırılacak temiz kripto paraların akışına bağlıdır. Yasa dışı faaliyetlerde bulunmamış olsalar bile Bitcoin ağında anonimliklerini iyileştirmek isteyen kullanıcıların yanı sıra yasadışı faaliyetlerde bulunan ve bilinen cüzdan adresleri, devlet destekli para birimine dönüştürebilmek için bu hizmetleri kullanabilir. Hem temiz hem de 'lekeli' kripto paralar, karıştırma servisinin cüzdanında toplanır ve işlem onayından sonra, kullanıcılar kripto paralarını, seçtikleri bir zamanda işlem ve işlem ücretleri düşüldükten sonra belirledikleri yeni bir cüzdanda alırlar. Karıştırma hizmetinin kullanılmasından sonra, eski Bitcoin cüzdanı atılabilir ve bu da işlemleri izleyen yetkililer için bir çıkmaz yaratır (de Balthasar ve Hernandez-Castro, 2017, s. 299). Ancak tüm süreç, bu hizmetlerin güvenilirliğini doğrulamak için gerekli teknik uzmanlığa sahip bireyler gerektirmektedir ve kripto paraların terörizmin finansmanında kullanımı bu kapsamda beyaz yaka suçluluğu olarak kabul edilmektedir.

Gizlilik odaklı kripto para birimleri, suçluların ve teröristlerin faaliyetlerini gizlice finanse etmeleri için mükemmel bir örtü sağlar. Anonimliğin yanı sıra, bu yasadışı kullanım durumlarında kullanılabilmeleri için kripto para birimlerinin ihtiyaç duyduğu bazı temel faktörler vardır. Dion-Schwarz vd. tarafından yapılan çalışmada (2019, s. 23-31) kripto paraların özellikleri açısından terörist finansman faaliyetlerinde kullanılabilirliği incelenmiş ve kripto paraların altı ortak özelliği (anonimlik, kullanılabilirlik, güvenlik, geçerlilik, güvenilirlik, hacim) belirterek belirli yasadışı faaliyetlerde bu özelliklerin yeterliliklerini karşılaştırmışlardır. Kripto para birimlerinin şu anda büyük çapta terörizmin finansmanı için yeterince güvenli olmadığı, çünkü siber uzayda bulundukları için siber saldırılara karşı savunmasız olduklarını savunulmuştur. Bu kapsamda bir sonraki başlıkta, kripto para biriminde terörizmin finansmanını ve diğer yasadışı faaliyetleri aksatabilecek kripto para kullanımına karşı temel siber saldırılar ele alınmıştır.

Kripto Para Çerçevesinde Ortaya Çıkan Yasadışı Eylemlere Karşı Geliştirilebilecek Önlemler

Terörizmin ve kara para aklamanın finansmanında kripto para biriminin olası rolü üzerine yapılan araştırmalar, bu tür araçların daha yüksek bir teknik uzmanlık gerektirmesi nedeniyle, ancak terör örgütleri bu teknolojileri kullanmak için teknik kapasitelerini artırdıktan sonra bu araçların terörizmin finansmanında kullanımında bir artış görüleceği öne sürülmektedir (Brantly, 2014, s. 4). ABD Adalet Bakanlığı'nın yayımladığı dava raporuna göre İzzeddin el-Kassam Tugayları, El-Kaide ve IŞİD'in finansmanına yönelik bağış kampanyaları teröristlerin bu teknik altyapıya ulaştığı yönündedir. Bu son bölümde, terörizmin ve diğer yasadışı faaliyetlerin finansmanında kripto para biriminin artan kullanımıyla mücadele etmek için alınabilecek önlemler ele alınacaktır. Yasal düzenlemelerin zorlukları ve suçluların kripto paraları devlet destekli paralara dönüştürmesinde zorluk yaşamayışı göz önüne alındığında, belli bir noktadan sonra kripto paralara yönelik devlet destekli aktörlerce olası siber saldırı ihtimali artacaktır.

Dion-Schwarz vd. tarafından kripto para birimlerinin aslında terörizmin finansmanında güvenilmez bir yol olduğunun savunulduğu çalışmalarında (2019, s.38), *kripto para kullanımına karşı dört farklı siber saldırıdan bahsetmektedirler. Bunlar; anonimliği ortadan kaldırma, harcama engeli, hırsızlık ve sistemsel saldırılardır.* Anonimliği ortadan kaldırma yönteminde, kripto para kullanıcıların anonimliğinin ortadan kaldırılarak kimliklerinin belirlenmesi eylemi tarif edilmektedir. Harcama engeli yöntemi ise bazı harcamaların blok zincirinde engellenerek belirlenen yasa dışı aktivitelere karışmış hesapların blok zincirinde işlem yapmasının önüne geçilmesi amaçlanmaktadır. Hırsızlık yönteminde ise kripto paraların tutulduğu cüzdanların özel anahtarlarının (private key) elde edilerek paraların başka hesaba geçirilmesi ve dolayısıyla çalınmasıdır. Son olarak sistemsel saldırı yöntemi ise bütün ağı sona erdirerek tüm kullanıcılar tarafından kullanılamaz hale getirilmesine yönelik alınan aksiyonların bütünüdür (Dion-Schwarz vd., 2019, s. 38). Bu sayılan siber saldırı ihtimalleri, kripto paralara ve blok zinciri teknolojisine güven duyulmamasının başlıca nedenleri arasında gelmektedir. Blok zincirinde işlemlerin geriye döndürülememesi ve destek alınabilecek bir otoritenin eksikliği, genel kullanım örnekleri için bu teknolojiyi çekici kılmamaktadır.

Bunlara rağmen, FATF kripto paraları para olarak görmemekte, sanal varlıklar olarak tanımlamaktadır. FATF raporunda (2020) kripto paraların sanal varlıklar olduğu ve bu varlıkları devlet destekli para birimleriyle değiş tokuş eden borsaları ise sanal varlık hizmet sağlayıcıları olarak nitelendirmektedir. FATF'in ortaya koyduğu yönergelere göre bu hizmet sağlayıcılar ve kripto paraların transferini yapan finansal kurumlar, kara para aklama ve terörizmin finansmanına karşı önlem almakla yükümlüdürler. Aynı raporda ise FATF eşler arası (peer-to-peer, P2P) gerçekleştirilen ve bir sanal varlık hizmet sağlayıcısı veya finansal kuruluşunun kullanımı ve katılımı olmaksızın sanal varlıkların devrinin, revize edilmiş FATF Standartları kapsamındaki karaparanın aklanmasının önlenmesi ve terörizmin finansmanı ile mücadele (AML/CFT) yükümlülüklerine açıkça tabi olmadığı hükmü yer almaktadır (FATF, 2020, s. 16-17). Bunun anlamı, FATF'in, standartlarında bir değişikliğe gidebilmesi için eşler arası sanal varlık transferleriyle yapılan kara para aklama/terörizm finansmanı faaliyetlerinde riskin yeterli derecede yüksek olduğunu düşünmediğidir. Buna karşılık FATF'ın blok zinciri teknolojisi tarafından sağlanan sanal varlıkların kara para aklama ve terörizmin finansmanında kullanabileceği riskini ciddiye aldığı söylenebilir.

Blok zinciri teknolojisi şu anda anlaşılabilir ve güvenilen bir teknoloji değildir ve FATF tarafından önerilen tüm yönergeler, yargı bölgelerinin yasama kabiliyetine bağlı olduğu için efektif denetim, devletlerin kendi iç kanunlarını ne kadar uygulayabildiğini bağlıdır.

Sonuç

Günümüzde uluslararası barış ve güvenlik için ciddi bir tehdit halini almış olan terörizm ve suç örgütlerinin illegal faaliyetlerinin finansman yapılarının tespiti ve mücadele edilmesinde para izinin takip edilmesi giderek zorlaşmaktadır. İllegal yapıların, finansman sağlamada ve para transferlerinde, tespit edilmesi zor hatta bazen imkânsız olan kripto paraları sıklıkla kullanmaya başladıkları görülmektedir. Diğer taraftan sanal varlıkların anonimliği ve sınır ötesi özellikleri illegal örgütler için çekici görünse de gerçekte blok zincirinde anonim kalmak için ileri düzeyde uzmanlığa ihtiyaç duyulması, blok zinciri teknolojisinin terörizmin finansmanında kullanımında bir caydırıcılık unsuru taşımaktadır.

Monero'nun geleneksel halka açık blok zincirlerinde kullanılabilen blok zinciri gözetim tekniklerine kesinlikle dirençli olması, işlemlerin izlenmesini zorlaştırmaktadır ancak Monerove ve Verge gibi çok daha gizlilik sağlayan alternatiflerin mevcut olmasına rağmen, Bitcoin'in blok zincirinde terörizmin finansmanı için hala yaygın olarak tercih edilen araçtır. Kirli kripto paralar ile temiz paraları karıştıran mikser programların kullanılmaya başlanmasının ise kirli paranın takibini imkânsız hale getirdiği görülmektedir.

Görülmektedir ki kullanıcı gizliliğini en önemli koşul olarak nitelendiren blok zincirlerinin illegal faaliyetlerin finansmanında kullanımına karşı geliştirilen yöntemler ve hukuksal altyapı yetersiz kalmaktadır. Sadece sanal varlıkların eşler arası transferi üzerine değil, aynı zamanda nakit paranın dijitalleşmesini sağlayan dağıtılmış defter teknolojisi ekosistemini daha iyi anlamak için akademisyenler, yazılım uzmanları ve mühendislerle blok zinciri teknolojisi üzerinde daha fazla ortak araştırmaya ihtiyaç duyulduğu gerçeği her türlü izahtan varestedir.

KAYNAKÇA

Adenyanju, C. (17.05.2019). What Crypto Exchanges Do to Comply With KYC, AML and CFT Regulations. *Cointelegraph,* Erişim Tarihi: 22 Aralık 2020, https://cointelegraph.com/news/what-crypto-exchanges-do-to-comply-with-kyc-aml-and-cft-regulations

Attaran, M., ve Gunasekaran, A. 2019. *Applications of Blockchain Technology in Business: Challenges and Opportunities*. Springer International Publishing.

Brantly, A. (2014). Financing Terror Bit by Bit. *Combatting Terrorism Center at West Point: CTC Sentinel*, 7(10), 1-20.

Chainalysis. (2020). The 2020 State of Crypto Crime. *Chainalysis*. Erişim Tarihi: 12 Aralık 2020, https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

Chaum, D. (1983). Blind Signatures for Untraceable Payments. İçinde: Chaum D., Rivest R.L., Sherman A.T. (eds) *Advances in Cryptology*. Springer, Boston, 199-203.

CoinMarketCap. (2021, January). Erişim Tarihi: 25 Ocak 2021, https://coinmarketcap.com/

de Balthasar, T., ve Hernandez-Castro, J. (2017). An Analysis of Bitcoin Laundry Services. *Nordic Conference in Secure IT Systems,* Tartu:Estonia. s. 297-312. Erişim Tarihi: 25 Kasım 2020, https://kar.kent.ac.uk/63502/193/An%20Analysis%20of%20Bitcoin%20Mixers.pdf

Dion-Schwarz, C., Manheim, D., ve Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Santa Monica:RAND Corporation. Erişim Tarihi: 25 Ekim 2020, https://www.rand.org/pubs/research_reports/RR3026.html

Engle, E. (2016). Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting (CCC). *Journal of High Technology Law*, 16(2), 340-393.

Europol. (2017). *Internet Organized Crime Threat Assesment* (IOCTA). Erişim Tarihi: 15 Ekim 2020. https://globalinitiative.net/wp-content/uploads/2018/06/Internet-Organised-Crime-Threat-Assessment-IOCTA-Europol-2017.pdf.

FATF. (2020). *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*. Erişim Tarihi: 15 Aralık 2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

Greenspan, G. (2017). *The blockchain immutability myth.* Private Blockchains.[blog] MultiChain. Erişim Tarihi: 05 Aralık 2020. https://www.multichain.com/blog/2017/05/blockchainimmutability-myth

Harper, C. (25.06.2020). ISIS shuns Bitcoin, embraces privacy coin Monero for donations.Decrypt.co. Erişim Tarihi: 15 Ekim 2020. https://decrypt.co/33562/isis-shuns-bitcoin-privacy-coin-monero

Houben, R., ve Snyers, A. (2018). *Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*. Strasbourg: European Parliament - Policy Department for Economic, Scientific and Quality of Life Policies. Erişim Tarihi: 15 Kasım 2020. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Iansiti, M. ve Lakhani, K. R. (Ocak – Şubat 2017). The Truth About Blockchain, *Harvard Business Review* , 95:1, s. 118-127.

Koerhuis, W., Kechadi, T., ve Le-Khac, N.A. (2020). Forensic Analysis of Privacy-Oriented Cryptocurrencies. *Forensic Science International: Digital Investigation*, 33, 1-10.

Lamport, L. (1998). The part-time parliament. *ACM Transactions on Computer Systems*,16(2), 133–169.

Temmuz 2020. https://www.merriam-webster.com/dictionary/blockchain

Möser, M., ve Narayanan, A. (2019). *Effective Cryptocurrency Regulation Through Blacklisting*. s.1-24. Erişim Tarihi: 05 Ekim 2020. https://maltemoeser.de/paper/blacklisting-regulation.pdf

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org: Erişim Tarihi: 13 Ekim 2020. https://bitcoin.org/bitcoin.pdf

Poskriakov, F., Chiriaeva, M., ve Cavin, C. (2020). *Blockchain Laws and Regulations 2021, 10 Cryptocurrency compliance and risks: A European KYC/AML Perspective*, Global Legal Insights (GLI). Erişim Tarihi: 13 Ekim 2020. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/10-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective

Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M. (2018). "On blockchain and its integration with IoT Challenges and opportunities, *Future Generation Computer Sysems*, 88, 173–190.

Salami, I. (2017). Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?, *Studies in Conflict & Terrorism*, 41(12), 968-989.

The Invisible Internet Project. (2018). *Intro-I2P*. Erişim Tarihi: 12 Aralık 2020. https://geti2p.net/en/about/intro

U.S. Department of Justice. (13.08.2020). *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns.* Erişim Tarihi: 10 Aralık 2020. https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

U.S. Internal Revenue Service. (20. 09.2020). *Pilot IRS Cryptocurrency Tracing Award Notice*. Erişim Tarihi: 10 Kasım 2020. https://beta.sam.gov/opp/5ab94eae1a8d422e88945b64181c6018/view

U.S. Department of the Treasury. (2015). *National Terrorist Financing Risk Assessment*. Erişim Tarihi: 05 Kasım 2020. https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

Tramèr, F., Boneh, D., ve Paterson, K. G. (2019). *Remote Side-Channel Attacks on Anonymous Transactions.* Stanford University, 1-29, Erişim Tarihi: 05 Ekim 2020. https://eprint.iacr.org/2020/220.pdf

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, 39(3), 195-206.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. United States Department of Commerce: National Institute of Standards and Technology Internal Report 8202. Erişim Tarihi: 08 Kasım 2020. https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf

Yurdakul, A. (2019). Küreselleşme ve Yeni Vergi Cennetleri Sorunu: Kripto Para, *Küreselleşmenin Krizi Yeni Güç Dengeleri*, Eds. Murat Ercan, Ali Ayata. Efe Akademi Yayınları, s.411- 441.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., ve Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, 14(4), 352-375.