Prof. Dr. Murat BALCI*
Dr. Öğr. Üyesi Kerim ÇAKIR**

YASA DIŞI KRİPTO PARA MADENCİLİĞİNDE CEZA SORUMLULUĞU

CRIMINAL LIABILITY IN ILLEGAL CRYPTO MINING

ÖZET

Kripto para madenciliği, blok zincir üzerinde yapılan işlemleri doğrulamak ve yeni kripto para birimleri oluşturmak anlamına gelen bir faaliyettir. Kripto para madencileri özel donanıma sahip bilgisayarlarla yeni bir kripto para değeri elde eder ve bunun karşılığında kripto para ile ödüllendirilir. Esasında bireysel veya toplu halde yapılan kripto para madenciliği suç teşkil etmez. Ancak kripto para madenciliğinin yüksek elektrik maliyeti ve madenciliğin güçlü donanıma sahip bilgisayarlar gerektirmesi kötü niyetli kişilerin zararlı yazılımlar marifetiyle bilişim alanında birtakım suçları işlemesine neden olur.

Çalışmada, bilişim sistemleri üzerinden yapılan yasa dışı kripto para madenciliğinin suç teşkil eden yönleri ele alınıp konu, 5237 sayılı Türk Ceza Kanunu'nda yer alan bilişim sistemine girme suçu ile sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu temelinde tartışılacaktır.

Anahtar Kelimeler: Kripto para, kripto para madenciliği, bilişim sistemi, veri, zararlı yazılım.

ABSTRACT

Cryptocurrency mining is an activity which means verifying transactions on the blockchain and creating new cryptocurrencies. Cryptocurrency miners get a new cryptocurrency value with specially equipped computers and are rewarded with cryptocurrency in return. In fact, individual or collective cryptocurrency mining does not constitute a crime. However, the high electricity cost of cryptocurrency mining and the fact that mining requires computers with powerful hardware cause malicious people to commit some crimes in the field of informatics by means of malicious software.

In the study, the criminal aspects of illegal cryptocurrency mining through information systems will be reviewed and the matter will be discussed based on the crime of accessing a data processing system and the crime of preventing the functioning of a system and deletion, alteration or corrupting of data in the Turkish Penal Code numbered 5237.

Keywords: Cryptocurrency, cryptocurrency mining, IT system, data, malware.

Araştırma Makalesi
Makale Geliş Tarihi: 22.02.2022 **Kabul Tarihi:** 30.05.2022
* **Prof. Dr. Murat Balcı ORCID ID:** https://orcid.org/0000-0002-8506-7911
Fatih Sultan Mehmet Vakıf Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Usul Hukuku Anabilim Dalı Öğretim Üyesi, balci53@hotmail.com;
** **Dr. Öğr. Ü. Kerim Çakır ORCID ID:** https://orcid.org/0000-0003-1821-9935
Marmara Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Usul Hukuku Anabilim Dalı Öğretim Üyesi, kerimcakir@marmara.edu.tr;

Giriş

Kripto paralar, madencilik olarak bilinen kriptografik görevlerin çözülmesi ile ortaya çıkar[1] ve kripto para birimi kodunda belirtilen algoritma temelinde madenciler tarafından oluşturulur[2]. Bu faaliyette bulunan kimseler madenci (miner) olarak isimlendirilir. Kripto para madenciliğinde karmaşık algoritmaları çözerek işlemleri doğrulama ve bu hizmetten ötürü ödeme alma ve blok zincire (Blockchain) doğrulanmış işlemler ekleme söz konusudur[3]. Burada işlemlerin doğrulanması ve onaylanması için çok hızlı matematik problemleri çözen bilgisayarlara ihtiyaç vardır. Karmaşık matematiksel formüllerin bilgisayar gücü ile çözülmesi süreci madencilik olarak isimlendirilir[4]. Yeni kripto paraların üretilmesinin tek yolu budur.

Kripto paralar, dünya çapında kullanılabilen merkezi bir otoritenin olmadığı sanal para biriminin adıdır. Kripto para aktarımı, bilgisayarların internet üzerinden birbirine bağlanması ile ve özel bir eşler arası uygulama yardımıyla, banka olarak hizmet veren merkezi bir katılım olmadan gerçekleşir[5]. Örneğin, Bitcoin'ler blok zinciri adı verilen kamuya açık bir işlem kaydında saklanır. Katılımcılara tahsis edilmeleri, kişisel dijital cüzdanlar üzerinden gerçekleşir[6].

1 Müller, Eckhart-Schlothauer, Reinhold-Knauer, Christoph, Münchener Anwalts Handbuch Strafverteidigung, 3. Auflage 2022, § 50, kn.7.

2 Wenger, Tobias-Tokarski, Kim Oliver, Kryptowährungen, (Jochen Schellinger, Kim Oliver Tokarski, Ingrid Kissling-Näf Digitale Transformation und Unternehmensführung Trends und Perspektiven für die Praxis), Springer Gabler, 2020, s.269.

3 Report of the Attorney General's Cyber Digital Task Force, s. 4.

4 Bozkurt Yüksel, Armağan Ebru, Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış, İÜHFM, C. LXXIII, S. 2, (173-220), Yıl: 2015, s. 201; Agin, Nurşen Selen, Türk Ceza Hukuku'nda Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu (TCK md.158/1-f), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2019, s. 75.

5 BGH: Illegales Bitcoinschürfen, NStZ, 2018, s. 401.

6 Bitcoin madenciliği, sisteme yeni Bitcoin arz etmenin, hileli işlemleri engellemenin, olmayan Bitcoin'leri harcatmamanın ve çifte harcamayı engellemenin yoludur. Henüz onaylanmış Bitcoin transfer işlemlerinin, Blok-Zincir'e yani küresel hesap defterine işlenmesini Bitcoin madencileri yaparlar. Blok-Zincir›de bir bloğa yazılmış olan bir işlem onaylanmış demektir ve artık transfere konu olan alıcı tarafından kendisine gönderilen Bitcoin kullanılabilir durumdadır. Blok-Zincir'e bloğunu ekletecek olan madenci, yeni blokla arz edilen parayı ve Bitcoin işlemlerindeki işlem masrafını alarak ödüllendirilir. Bkz. Çarkacıoğlu, s. 46; Stabile, Daniel T.-Prior, Kimberly A.- Hinkes, Andrew M., Digital Assets and Blockchain Technology: U.S. Law and Regulation, Edward Elgar Publishing, USA 2020, s. 17.

Kendine özgü bir yapıya sahip olan kripto paralar, kendi borsalarında ve platformlarında işlem görür. Kripto para birimlerinin ilki olan Bitcoin somut bir para birimi olmayıp kriptografik verilerden oluşmaktadır. Ne yeni Bitcoin'lerin oluşturulması ne de işlemlerin yürütülmesi merkezi bir otorite gerektirmez. Yetkilendirme de kriptografik teknikler kullanılarak gerçekleştirilir[7]. Kripto para sisteminin geleneksel para sistemine kıyasla farklı bir güven düzeyi gerektirdiği açıktır. Merkez bankalarının itibari para biriminin işleyişi için kefil olma görevi, kripto para sisteminde kripto para birimi kodu ve kriptografik prosedür kripto para madenciliği tarafından yerine getirilir. Böylece kripto para sisteminde sosyal güvenin bir kısmı teknolojik güven düzeyine kaydırılmış olur[8].

Yukarıdaki bilgiler ışığında, kripto paraların üretilmesi ve piyasada bulundurulması bakımından kripto para madenciliğinin yasal olduğunu belirtmemiz gerekir. Yüksek performansa sahip özel yazılımlı bilgisayarlarla kripto para madenciliği yapmak mümkündür. Kripto para madenciliği konusunda tartışmalara neden olan husus, enerji kaynaklarının hızla tükendiği bir dünyada kripto para madenciliği için çok fazla enerji tüketilmesi ve bu enerjinin bazı ülkelerin enerji ihtiyaçlarına ve tüketimlerine eşdeğer olmasıdır[9]. Bu durum ülkeleri kripto para madenciliği konusunda tedbirler almaya ve enerjiden tasarruf edilmesi konusunda düzenlemeler yapmaya sevk etmektedir.

I. Kripto Para Madenciliği

Kripto para madenciliği özel donanımlı, yüksek performanslı ve güçlü ekran kartına sahip bilgisayarlar marifetiyle üretilir. Madencilikle blok zincir oluşturulur ve yeni blok zinciri için matematiksel tabanlı işlemleri çözmek gerekir[10.] Diğer bir ifadeyle kripto para madenciliği, blok

7 Goger, Thomas, Bitcoins im Strafverfahren-Virtuelle Währung und reale Strafverfolgung, MMR 2016, s. 433; Bozkurt Yüksel, s. 200.

8 Lewis, Antony, The Basics of Bitcoins and Blockchains, USA 2018, s. 21; Wenger-Tokarski, Kryptowährungen, s.276.

9 Tahan, Özge, Kripto Paraların Türk ve Alman Ceza Hukuku Düzenlemeleri Yönünden Değerlendirilmesi, Suç ve Ceza Dergisi, Cilt: 14, Sayı: 1, Mart 2021, s. 122.

10 Çarkacıoğlu, Abdurrahman, Kripto-Para Bitcoin, Sermaye Piyasası Kurulu Araştırma Dairesi Araştırma Raporu, 2016, s.13; İmamoğlu, Deniz Alp, Kripto Para Birimleri Ve Türk Hukukunda Düzenlenmesi, 2. Baskı, Ankara 2021, s. 52. Ayrıca bkz. https://www.chip.com.tr/haber/mining-kripto-para-madenciligi-nedir-nasil-yapilir-turleri-nelerdir_96470.html

zincirine yeni bloklar eklemek için çeşitli şifreleme yöntemini çözme işidir. Blok zincirin oluşturulmasına katkı sunan kullanıcılar kripto para ile ödüllendirilir[11]. Kripto paralar, transfer işlemlerini doğrulama aşamalarına katılarak (madencilik faaliyetiyle kazılan ödül), başka bir kripto para sahibinden doğrudan kripto para alarak ya da kripto para borsaları veya platformlarını aracı kılarak elde edilir[12].

Kripto para madenciliği için çözülmesi gereken algoritmalar, artan kripto para sayısı ile giderek daha karmaşık bir hal alır ve giderek daha fazla hesaplama zamanı ve performansı gerektirir. Kullanılan bilgisayarın performansı ne kadar yüksek olursa, doğru sonuca ulaşma imkanı o nispette artar. Ancak burada dikkat çeken husus, ortaya çıkan elektrik masraflarının yeni üretilen kripto paraların değer artışını azaltmasıdır.

Madencilik faaliyetinde, blok zincire yeni bloklar ekleyebilmek için bir tür kriptografik bulmaca çözülmesi gerekmektedir. Bu işlemde, sistemde kayıtlı bulunan önceki verilerden yararlanılır. Önceki verilerin kullanılması, çok daha fazla miktarda verinin hesaplanmasını gerektirdiğinden işlemler daha da karmaşık bir hal alır. Bu karmaşık işlemleri ve eldeki verileri hesaplama sırasında da çok fazla elektrik enerjisine ihtiyaç duyulur[13].

Yapılan işlemleri sisteme entegre etmek, blok zinciri veya Bitcoin ağındaki blokları güvence altına almak ve senkronize etmek amacıyla yapılan madecilikte bilgi işlem gücü önemli bir yere sahiptir. Bu kapsamda örneğin, Bitcoin blok zincirindeki blokların en az %99'u madencilik havuzları tarafından oluşturulmaktadır[14].

11 Goger, s. 433. Ayrıca bkz. https://www.chip.com.tr/haber/mining-kripto-para-madenciligi-nedir-nasil-yapilir-turleri-nelerdir_96470.html

12 Tomrukçu, Tuğçe, Kripto Varlıkların Konu Olduğu Dolandırıcılık Suçları, Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022, s. 265.

13 Balcı, Umut, Kripto Paraların Ceza Hukuku Boyutu ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri, TBB Dergisi 2021 (155), s. 210.

14 Wenger-Tokarski, Kryptowährungen, s.7.

Cambridge Üniversitesinin son verilerine göre Amerika Birleşik Devletleri, Çin'in yerine geçerek Bitcoin madenciliğinde hakim ülke konumuna gelmiştir. Son yayımlanan rapora göre, ülkelere göre dağılımı yapılan Bitcoin hash oranı[15] verileri, ABD'nin en büyük pazar payına sahip olduğunu göstermektedir.

Cambridge Alternatif Finans Merkezi (Cambridge Center for Alternative Finance-CCAF) tarafından yayımlanan Ağustos (2021) dönemi Bitcoin madencilik haritası, ABD'nin yüzde 35,4 oranında aylık ortalama hash oranına sahip olduğunu göstermektedir. Çin hükümetinin 2021 yılında madencilik faaliyetlerine yasak getirmesinin ardından başlayan madencilik göçü neticesinde Kuzey Amerika kıtası, ABD önderliğinde Bitcoin madenciliğinde hakim bölge konumu haline geldi[16]. Geçen yılın aynı dönem verilerine göre ise ABD, hash oranı payında Ağustos 2020'de sadece yüzde 4,2'lük bir paya sahipti. Güncel verilere göre yüzde 35,4'lık oranla ABD, pazar payını 8 kat artırmıştır. Aynı dönemde Bitcoin madenciliğinin hakim ülkesi Çin, pazarın yüzde 66,86'sına sahipti. Çin'in madencilik hakimiyeti, 2021 yılının ikinci çeyreğine kadar yüzde 34 seviyelerine kadar azalarak devam ettikten sonra Temmuz ayıyla birlikte Çinli madencilerin toplu halde faaliyetlerini sonlandırdığı görülüyor. CCAF'nın son olarak Ağustos ayı verilerine dayanarak hazırladığı Bitcoin madencilik haritasına göre ABD'yi sırasıyla yüzde 18,1 pazar payı oranıyla Kazakistan, yüzde 11,23 ile Rusya ve yüzde 9,55 ile Kanada izliyor. Türkiye ise hash oranına göre gösterilen dağılımda toplam madencilik pazarının sadece yüzde 0,06'sını oluşturmaktadır[17].

II. Yasa Dışı Kripto Para Madenciliğinin Yapılışı

Kripto para birimi oluşturmak için başkasına ait bir bilgisayarın yetkisiz olarak kullanılması, yasa dışı kripto para madenciliği (crypto-

15 Bitcoin ağında bir blok üretmenin zorluk derecesini de belirleyen 'hash oranı' Bitcoin ağının anlık işlemci gücünü gösteren bir ölçme sistemidir. Bkz. https://www.barimeks.com/sss/hash-orani-nedir Ayrıca bkz. Lewis, Antony, The Basics of Bitcoins and Blockchains, USA 2018, s. 136.

16 Bkz. https://ccaf.io/cbeci/mining_map

17 Bkz. https://tr.investing.com/news/cryptocurrency-news/abd-bitcoin-madenciliginde-lider-konuma-yukseldi-turkiyenin-pay-ne-kadar-2203532

jacking) olarak adlandırılmaktadır[18]. Bu işlem sıklıkla üçüncü taraf bilgisayarının kripto madencilik kodunu çalıştırmasına neden olan zararlı yazılım[19] veya gizliliği ihlal edilmiş web sitelerinin kullanımı aracılığıyla gerçekleştirilir[20]. Üçüncü kişilerin veya kuruluşların bilgisayarının gizlice kullanılmasındaki nispi kolaylığa kıyasla kripto para birimlerinin (özellikle Bitcoin) değeri göz önüne alındığında yasa dışı kripto para madenciliğinin kötü niyetli kişilere cazip geldiğini söylememiz gerekir[21]. Yasa dışı kripto para madenciliği üçüncü taraf bilgisayarları kullanılarak veya üçüncü tarafın bulut erişimini kullanarak yapılmaktadır. Bu işlemler çoğu zaman çok yüksek bilgi işlem gücüne sahip üçüncü taraf bilgisayarlarında veya sunucularında gerçekleşir[22]. Fail, komuta ve kontrol sunucusuna (Command-and-Control-Server) bağlandığında madencilik faaliyeti başlamış olur[23].

Madencilik olarak adlandırılan kripto para üretiminde, kriptografik görevlerin çözülmesi gerektiğinden yüksek bilgi işlem gücüne ihtiyaç duyulur.

Yeni Bitcoin'lerin üretimi büyük bilgisayar gücü gerektirir. Bu nedenle, Bitcoin madenciliği (mining) yüksek elektrik fiyatları ve pahalı donanımlar yüzünden oldukça masraflı hale gelir. Kötü niyetli kimseler kripto para üretimi için veri değişikliğine sebebiyet vererek girdikleri bilgisayarları üçüncü tarafın bilgisi olmaksızın gizlice kullanmaya başlar. Bu durum verilere karşı suç işlenmesi sonucunu doğurur[24]. Üçüncü taraf

18 Tahan, s. 122.

19 Zararlı yazılım, bilgisayar ve mobil cihazların işlevlerini bozmak, kritik bilgileri toplamak, özel bilgisayar sistemlerine erişim sağlamak ve istenmeyen reklamları göstermek amacı ile kullanılan yazılımdır. Bkz. https://tr.wikipedia.org/wiki/Malware

20 Balcı, Umut, Kripto Paraların Ceza Hukuku Boyutu ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri, TBB Dergisi 2021 (155), s. 218.

21 Report of the Attorney General's Cyber Digital Task Force, s.16.

22 Grzywotz, Johanna, Virtuelle Kryptowährungen und Geldwäsche, Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2019, s.180, 181.

23 Grzywotz, s.165.

24 Boehm, Franziska– Pesch Paulina, Bitcoin: Bir İlk Hukuki Analiz- Alman ve Birleşik Devletler- Amerikan Hukuku, (Çeviren, Doğa Satı), Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022, s. 87.

bilgisayarları Botnet'ler (robot network)[25] yardımıyla kötüye kullanılır[26]. *Botnet*, bilgisayarlar aracılığıyla birbirine bağlanan bir grup zararlı yazılımı ifade eder. Bilgisayar sahipleri çoğu zaman bilgisayarlarının bir Botnet'in parçası olduğunu ve Botnet'lerin kripto para madenciliği için kullanıldığını bilmezler[27]. Böylece bot gözetmeni[28] bağlı bilgisayarları uzaktan kontrol edip kendi amaçları için kullanabilir. Botnet'ler genellikle bilgisayar kullanıcıları tarafından, Truva Atı (Trojan)[29] adında kamufle edilmiş zararlı bir yazılımı açarak, bilinçsiz bir şekilde kurulur veya işletim sistemindeki, web tarayıcısındaki veya programdaki bir güvenlik boşluğu ile bilgisayara bulaşmış olur[30].

İnternetten indirilen müzik, video veya program dosyaları şeklinde kamufle edilmiş olan Truva Atı niteliğindeki zararlı yazılımlarla üçüncü

25 Botnet (robot network) bilgisayar bilimciler tarafından kullanılan bir sözcüktür. Botnetler birçok yazılım ajan programından oluşur. Her yazılım ajan programı uzaktan kontrol edilir. Botnetler bir birim olarak hareket etme yeteneklerine sahiptir. Bir botnet tekrarlanan görevleri ve hedeflerini tamamlamak için bir çaba ile diğer benzer makinelerle iletişim kuran internet bağlantılı bilgisayarların bir dizisidir. Bkz. https://tr.wikipedia.org/wiki/Botnet Botnet sözcüğü, "robot" ve "network" (ağ) sözcüklerinin birleşiminden türetilmiştir. Siber suçlular, çok sayıda kullanıcının bilgisayar güvenliğini ihlal etmek, her bir bilgisayarın kontrolünü ele geçirmek ve tüm virüslü makineleri suçlunun uzaktan yönetebildiği bir "bot" ağı halinde organize etmek için özel Truva atı virüsleri kullanır.
Bkz. https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks

26 Grzywotz, Johanna- Köhler, Olaf- Rückert, Christian, Cybercrime mit Bitcoins– Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention, Strafverteidiger, 2016, s. 753; Beukelmann, Stephan, Virtuelle Währungen, NJW-Spezial 2019, s. 184.

27 Müller-Schlothauer-Knauer, § 50, kn.7; Heine, Sonja, Bitcoins und Botnetze– Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining, NStZ 2016, s. 444. Ayrıca bkz. Heine, Sonja, Bitcoinler ve Botnetler- Yasadışı Bitcoin Madenciliğinde Cezalandırılabilirlik ve Malın Müsaderesi (Çev. Mehmet Karatepeli), Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022, s. 250.

28 Botnet, aynı kişi veya gruplarca yönetilen bir bot hesabı ağıdır. Botnet yöneten bu kişilere, botların yayılması öncesinde gerekli özgün insan girdisini sağladıkları için bot gözetmeni denir. Bkz. https://medium.com/dfrlab/trolltracker-bots-botnets-and-trolls-31d2bdbf4c13

29 Truva yazılımları ismini "Truva Atı"ndan almaktadır. Bir bilgisayar programına bağlanarak saklanan, tahribatını yaparken ise, programın olağan çalışmasına izin veriyormuş gibi gözüken virüslere "Truva atı" denir. Truva atları çoğunlukla, bulaştıkları bilgisayarlarda kullanılan şifre, kullanıcı adı gibi özel bilgileri ele geçirmek amacıyla kullanılır. Bkz. Dolandırıcılık Eylemleri ve Korunma Yöntemleri, Türkiye Bankalar Bilirliği, Aralık 2015, s.14. Truva atı (Trojan), bilgisayar yazılımı bağlamında Truva atı zararlı program barındıran veya yükleyen programdır. (Bazen "zararlı yük" veya sadece "truva" ibareleriyle de nitelendirilmektedir.) Terim klasik Truva Atı mitinden türemiştir. Truva atları masum kullanıcıya kullanışlı veya ilginç programlar gibi görünebilir ancak yürütüldüklerinde zararlıdırlar. https://tr.wikipedia.org/wiki/Truva_at%C4%B1_(bilgisayar)

30 BGH: Illegales Bitcoinschürfen, s. 401.

taraf bilgisayarına erişim sağlanır[31]. Aslında bu durum Botnet'lerin yasa dışı kripto para madenciliğindeki etkisini ve rolünü gösterir niteliktedir[32]. Bu noktada güvenlik duvarlarının önemi de ortaya çıkmaktadır. Güvenlik duvarı, kullanıcının bilgisayarında internetten gelen saldırıları önlemeye yarayan ağ erişim korumasıdır. Belirtelim ki bilişim sistemine girme suçu bakımından bilişim sistemine erişimin bazı tedbir veya uygulamalarla sınırlandırılmış olması önem arz eder[33]. Kullanıcının kendisi tarafından indirilen bu zararlı yazılım bir müzik, video veya program dosyası olarak gizlenmemiş olsaydı komuta ve kontrol sunucusunun bilgisayara erişmesine izin veren program, güvenlik duvarı tarafından denetime tabi tutulup erişim reddedilebilirdi[34].

Belirtelim ki yasa dışı kripto para madenciliğiyle elde edilen malvarlığı değeri, aslında suçtan kaynaklanan bir malvarlığı değeridir. Bu sebeple bahse konu gelirin kaynağını gizlemek amacıyla çeşitli işlemlere tabi tutulması gerekir. Kripto para ekosisteminin özellikleri incelendiğinde suç gelirlerinin aklanmasını nasıl kolaylaştırdığı anlaşılacaktır. Herhangi bir coğrafi kısıtlamaya maruz kalmayan ve online olarak sınır ötesi işlem yapma imkanı sağlayan kripto paralar, suç işleyerek gelir elde eden ve bu gelirleri kripto paralar marifetiyle aklayarak yasal ekonomik sisteme dahil etmek isteyen kişilere önemli avantajlar sunmaktadır[35].

Yasa dışı kripto para madenciliğinden elde edilen gelirle terörizmin finanse edildiği de görülmektedir. Madencilik, terörü desteklemek amaçlı işlemlerde doğrudan kullanılabileceği gibi yasa dışı eylemlerle ilişkili finansal faaliyetleri teşvik etmek için de kullanılabilir. Terörizmin finansmanının önlenmesi ve siber suçla mücadele için yasa dışı kripto para madenciliğine engel olmak gerekmektedir.

31 BGH: Illegales Bitcoinschürfen, s. 401.

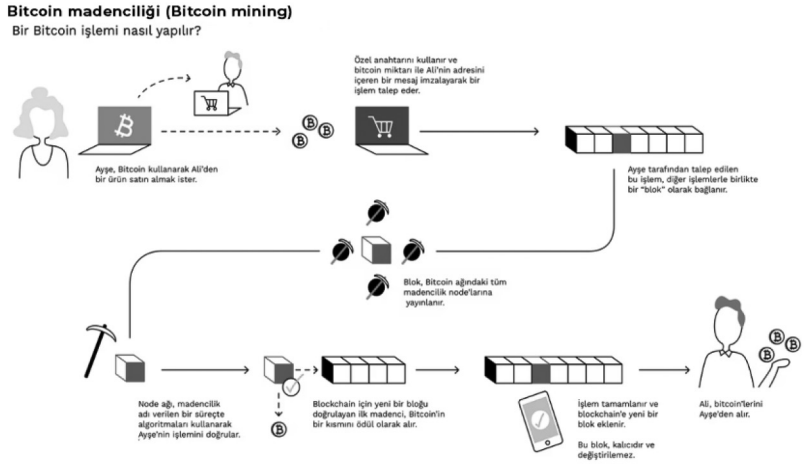
32 BGH: Illegales Bitcoinschürfen, s. 401.

33 Özbek, Veli Özer-Doğan, Koray-Bacaksız, Pınar, Türk Ceza Hukuku Özel Hükümler, 16. Baskı, Ankara 2021, s. 960.

34 BGH: Illegales Bitcoinschürfen, s. 402. Söz konusu olayda 86 adet şifrelenmemiş Bitcoin'e el konulurken, 1,730 Bitcoin geçici olarak güvence altına alınabilmiştir, çünkü erişimleri şifre ile korunuyordu ve sanık şifreyi açıklamadığı için deşifre edilmeleri mümkün değildi.

35 Gbi bkz. Balcı, Murat- Çakır, Kerim, Kripto Paraların Karapara Aklama Yöntemi Olarak Kullanılması, Ceza Hukuku Dergisi, Cilt: 16, Sayı:46, Ağustos 2021, (ss. 311-332), s. 316 vd.

Aşağıda kripto para madenciliğinin işleyişi Bitcoin üzerinden şematik olarak gösterilmiştir[36].



III. Başlıca Kripto Para Madenciliği Yöntemleri

1. Toplu Madencilik: Kripto paraların bireysel olarak üretilmesi mümkündür. Ancak karmaşık problemlerin çözülmesi için yüksek donanımlı bilgisayarlara ihtiyaç duyulduğundan çoğu zaman bilgisayarların güçlerinin birleştirildiği toplu madencilik faaliyetlerine rastlanır. Toplu madencilik, madencilerin gücünü birleştiren bir sunucudur. Burada madencilerin gücünü birleştiren bir sunucu ve yeni blokların oluşturulmasıyla uğraşan ortak bir bilgi işlem ağı mevcuttur[37]. İlgi gören kripto para birimlerinin artan ağ karmaşıklığı toplu halde yapılan kripto para madenciliğini teşvik etmektedir.

2. ASIC Madenciliği: ASIC (Application Specific Integrated Circuit)[38], yani Uygulamaya Özel Entegre Devreler, kripto para maden-

36 Şema için bkz. https://www.bitpanda.com/academy/tr/dersler/bitcoin-madenciligi-nedir-ve-madencilik -nasil-calisir/ Erişim tarihi: 12.01.2022.

37 https://www.chip.com.tr/haber/mining-kripto-para-madenciligi-nedir-nasil-yapilir-turleri-nelerdir_96470.html

38 ASIC, bilgisayar programcılığında kullanılan özel entegre devrenin adıdır. Açılımı, "Application Specific Integrated Circuit" olan tanımlanın dilimizdeki karşılığı, "Uygulamaya özel tümleşik devre"dir. Bkz. https://www.paribu.com/blog/sozluk/asic-nedir/

ciliği odaklı sistemlerdir. İçlerindeki yazılım ve özel donanımlar, bu devreleri kripto para madenciliği gerçekleştirmek üzere özel birer donanım haline getirmektedir. Çok sayıda işlemciden oluşan ASIC cihazlar, yüksek hesaplama kapasitesine sahip olmalarına rağmen çok fazla enerji tüketmektedir. Bu nedenle ASIC cihazlar ile madencilik yapan madencilerin elektrik tüketimini karşılayacak güçlü elektrik altyapılarına ihtiyacı vardır. Bitcoin, Litecoin gibi kripto paralar yüksek hesaplama kapasitesi ihtiyacı nedeniyle artık sadece ASIC madencilik cihazları ile üretilmektedir.

3. GPU Madenciliği: GPU madenciliği de ekran kartlarının hesaplama yaparak işlemleri doğruladığı madencilik türüdür. Grafik kartlarının işlemcileri, bilgisayarların işlemcilerine göre çok daha güçlüdür ve hesaplama odaklıdır. Bu nedenle Ethereum, Zcash gibi kripto paraların işlemlerinin doğrulanmasında grafik kartları kullanılmaktadır.

4. CPU Madenciliği: Merkezi işlem birimiyle yani bilgisayarlarımızdan bildiğimiz ismiyle işlemci ile yapılan madenciliğe verilen isimdir. Bu madencilik türünde transferler için kullanılan matematiksel denklemler CPU ile çözülür. Evlerde kullanılan bilgisayarlara bir madencilik yazılımı kurarak kolaylıkla CPU madenciliği yapılabilmektedir. Ancak günümüzde bu yöntem, diğer yöntemlere göre çok düşük performanslı olması sebebiyle artık neredeyse hiç kullanılmamaktadır. Popüler kripto paraların büyük çoğunluğu için işlemcilerle madencilik yapmak imkansız hale gelmiştir. Bu madencilik türünde, yazılımın çalışması için ihtiyaç duyulan şey ise sanal kripto para cüzdanında belirli bir miktar kripto para bulunmasıdır.

5. Bulut Madenciliği: Kripto para madenciliğini yapmak için kullanıcıların bir diğer tercihi de bulut madenciliğidir. Bulut madenciliğini genellikle teknik donanımı ve zamanı kısıtlı olan kullanıcılar tercih eder. Bulut madenciliği yapmak isteyen kullanıcılar bazı şirketler tarafından satışa sunulan işlem gücünü kiralayarak belirli oranda bir komisyon ücreti öder ve şirket kullanıcılar adına kripto para madenciliği yapar. Bulut madenciliği en az 12 ay süreli sözleşmeler ile güvence altına alınır

ve kripto para madenciliğinde bu yöntem sıklıkla tercih edilmektedir. Bulut madenciliği, kripto para madenciliği yapmak isteyen ancak yeterli donanım, zaman, bilgi birikimi ya da sermayesi olmayanlar için sunulan alternatif bir madencilik yöntemidir.

IV. Yasa Dışı Kripto Para Madenciliğiyle İlgili Suç Tipleri

1. Genel Olarak

Yasa dışı kripto para madenciliği bilişim sistemlerinin kullanılması suretiyle yapıldığından, TCK bakımından öncelikle "bilişim sistemine girme" (m. 243) suçu oluşur. Bununla birlikte bilişim sistemindeki işlemlere veri niteliği atfedildiğinden "verileri değiştirme" suçu (m. 244) ile yüksek donanımlı bilgisayarlara duyulan ihtiyaç sebebiyle "yasak cihaz veya programlar" suçu (m. 245/A) da yasa dışı kripto para madenciliğinde önem taşır. Madencilik faaliyetinde ciddi miktarda enerji kullanımı söz konusu olduğundan malvarlığına karşı suçlar arasında yer alan "karşılıksız yararlanma" suçunun da (m. 163) üzerinde durulması gerekir.

Bu kapsamda aşağıda yasa dışı kripto para madenciliğiyle işlenen suçlar değerlendirilecektir.

2. Bilişim Sistemine Girme Suçu (TCK m. 243)

5237 sayılı TCK'nun 243'üncü maddesine göre, bir bilişim sisteminin[39] bütününe veya bir kısmına, hukuka aykırı olarak giren veya

39 Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik madde 3/1-b'ye göre, bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem, "bilişim sistemi"ni ifade eder. Avrupa Konseyi Siber Suç Sözleşmesi'nin "Tanımlar" başlıklı 1. maddesine göre bilişim sistemi; bir veya birçok unsuru, bir programın işleyişi aracığıyla verilerin otomatik olarak işleme tabi tutulmasını sağlayan, birbirine bağlanmış veya benzeşen tek veya toplu tertibattır. YCGK'nun 2.3.2021 tarih ve 23-51/68 sayılı kararında bilişim sistemiyle ilgili; "Bilişim teknolojisi, yazılım, donanım, hizmetler ve ekipmanlar gibi 4 temel kategoriden oluşur. Öğretide yer alan bu bilgilere göre bilişim sitemi şöyle tanımlanabilir: Yazılım, donanım, hizmetler ve ekipmanlardan oluşan teknolojiyi içinde barındıran sisteme bilişim sistemi denir. Bu tanıma göre bilişim sistemi alet veya cihazdan ibaret olmayıp birden fazla bileşenden oluşur. Dikkat edilirse hem TCK'nın 243. maddesinin gerekçesinde hem de Avrupa Konseyi Siber Suç Sözleşmesi'nde yer alan tanımlarda bir alet, makine veya teçhizattan söz edilmeyip, sistem ve tertibat kavramlarına yer verilmektedir. Bu nedenle bilişim sisteminin kullanılması, bilişim sistemine dahil olan bileşenlerin bir kaçının kullanılmasından yahut bilişim

orada kalmaya devam eden kimse suç işlemiş olur[40]. Bilişim sistemine girmenin ne şekilde gerçekleştiğinin önemi bulunmamaktadır[41]. Bununla birlikte çoğu zaman zararlı yazılımlarla bilişim sistemine girildiği görülmektedir. Suçun oluşabilmesi için failin bilişim sistemine girdiğini bilincinde olması gerekir. Kanun koyucu, madde metninde sisteme "hukuka aykırı olarak giren veya orada kalmaya devam eden" şeklinde bir ifadeye yer verdiğinden fiilinin haksızlık teşkil ettiğini bilmesi gerekir. Bu sebeple suç tipi doğrudan kastla işlenebilir[42].

Suç teşkil eden bu fiil, Alman Ceza Kanunu'nun (StGB) 202a maddesinde "veri casusluğu" başlığı altında düzenlenmiştir. Suçun oluşması bakımından mutlaka sistemdeki verilerin ele geçirilmesi aranmamaktadır[43]. Bahse konu hükümler, tasarruf hakkına sahip kişinin saklanan veya iletilen verilerinin kullanım hakkını korur44. Ayrıca bu düzenleme tasarruf sahibinin gizlilik menfaatini45, bilişim sisteminin güvenliğini, özel hayatını, haberleşme hürriyetini ve şahsiyetini de korumaktadır[46].

teknolojisini barındıran bir aletin kullanılmasından ibaret olmayıp, sistemi oluşturan temel bileşenlerin kullanılmasıyla oluşur" denilmektedir.

40 TCK'nın 243'üncü maddesine göre, *"(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. (4) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."*
Söz konusu suç tipi Alman Ceza Kanunu'nun "veri casusluğu" başlıklı 202a maddesinde düzenlenmiştir. Madde, *"(1) Her kim, yetkisi olmaksızın, kendisinin bilgisine sunulmuş olmayan ve hak sahibi olmayanların girişine karşı özel olarak korunmuş bulunan verileri bu korumayı aşarak kendisine veya bir başkasına giriş yapma olanağı sağlarsa, üç yıla kadar hapis cezası veya adlî para cezası ile cezalandırılır. (2) Birinci fıkrada belirtilen veriden, sadece elektronik, manyetik veya sair doğrudan doğruya algılanamayacak bir şekilde kaydedilmiş veya aktarılmış olan veriler anlaşılır"* şeklindedir.

41 Koca, Mahmut-Üzülmez, İlhan, Türk Ceza Hukuku Özel Hükümler, 7. Baskı, Ankara 2020, s. 901.

42 Koca-Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 903.

43 Tezcan, Durmuş-Erdem, Mustafa Ruhan-Önok, R. Murat, Teorik ve Pratik Ceza Özel Hukuku, 19. Baskı, Ankara 2021, s. 1148.

44 Heine, s. 444.

45 BGH: Illegales Bitcoinschürfen, s. 403.

46 Tezcan-Erdem-Önok, s. 1148, 1149; Özbek-Doğan-Bacaksız, s. 956; Erdoğan, Yavuz, Bilişim Sistemine Girme ve Kalma Suçu, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 12, Özel S., 2010, s.1363-1433 (Basım Yılı: 2012), s. 1364.

243'üncü maddeye göre cezalandırılan ve bilişim sistemine girme olarak ifade edilen hareket, hukuka aykırı olarak bir bilişim sisteminin bir kısmına veya bütününe girmektir. Madde gerekçesinde bilişim sistemi; *"verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağını veren manyetik sistem"* şeklinde açıklanmıştır. TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçunun madde gerekçesinde ifade edildiği üzere, sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır. Hukuki nitelikleri konusunda tartışmalar[47] bulunsa da blok zincir üzerinde işlem gören kripto paralar da veri olarak değerlendirilebilir[48].

Kripto para madenciliğinde gerekli bilgi işlem gücü, "Botnetwork" adı verilen bir sistem aracılığıyla sağlanır. Birkaç bilgisayarın bilgi işlem gücü bir araya getirilerek, bireysel cihazların tüm bilgi işlem gücüne sahip bir tür bilgi işlem ağı, merkezi olmayan bir şekilde oluşturulur. Böyle bir Botnet, örneğin dosyalara Truva atları gizlenerek kurulabilir. Truva atı daha sonra mağdurun bilgisayarını failin istediği amaçlar için kullanmasına imkan verir[49]. Bilgisayar donanımlarının kullanılması ile mağdurun kullandığı elektrik enerjisinin ciddi şekilde arttığı görülür. Bu işlem dolayısıyla madencilik faaliyeti kapsamında 243'üncü maddedeki suç tipi ihlal edilmiş olur. Örneğin, e-posta yoluyla gönderilen zararlı yazılım casus bir program barındırıyor ve böylece doğrudan bilişim sistemine girmek mümkün oluyorsa, 243'üncü maddedeki bilişim sistemine girme suçu oluşur[50].

47 Kripto paraların hukuki niteliğiyle ilgili görüş ve değerlendirmeler için bkz. Balcı, Murat-Çakır, Kerim, Kripto Paralara El Konulması ve Kripto Paraların Müsadere Edilmesi, Mali Hukuk Dergileri, 17.198 (2021), (1503-1534), s. 1512 vd.; Özdemir, Gençer, Kripto Paraların Eşya Niteliği, SDÜHFD C: 11, S: 1, Y: 2021, s. 302; Durdu Erdal, Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul 2018, s. 11; Turanboy, Asuman, Kripto Paraların Ortaya Çıkmaları ve Hukuki Nitelikleri, Banka ve Ticaret Hukuku Dergisi, Cilt: 35, Sayı:3, Eylül 2019, s. 47. Ayrıca bkz. Simmler, Monika-Selman, Sine-Burgermeister, Daniel, Beschlagnahme von Kryptowährungen im Strafverfahren, AJP/PJA 8/2018, s.968.

48 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un tanımlar başlıklı 2'nci maddesine göre de veri, "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri*" ifade eder.

49 Heine, s. 445. Ayrıca bkz. Baier, Johannes, Kriminalpolitische Herausforderungen durch Bitcoin und andere Kryptowährungen – Teil 1, CCZ 2019, s. 128.

50 Tezcan-Erdem-Önok, s. 1153.

Bir başkasının bulut erişimini[51] kullanarak kripto para madenciliği yapılması halinde de bilişim sistemine girme suçu işlenir. Bilişim sistemi üzerinden üçüncü taraf bilgisayarının kimliği kullanılır ve bulut erişimiyle kripto para madenciliği yapılırsa 243'üncü maddede yer alan bilişim sistemine girme suçu oluşur.

3. Verileri Değiştirme Suçu (TCK m. 244)

TCK'nun 244'üncü maddesinin 2'nci fıkrasında yaptırıma bağlanan fiil; "*bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek"*tir. Fıkrada belirtilen seçimlik hareketlerden herhangi birinin yapılması ile suç tamamlanır. Verilerin değiştirilmesi şeklindeki seçimlik harekette, verinin içeriğinin değiştirilmesi, bir verinin yerine başka bir verinin konması, verinin başka biçimlere sokulması, niteliğinin değiştirilmesi ya da verinin başka bir görünüme sahip olması söz konusudur. Diğer bir ifadeyle veriler üzerinde manipülasyon yapılmaktadır[52]. Değiştirme ancak orijinal verilerde söz konusudur. Kopya olan verilerin değiştirilmesi bu madde kapsamında cezalandırılmaz[53].

Kripto para madenciliği yapanlar alınan tedbirlere rağmen yüksek maliyetlere katlanmamak için üçüncü kişilerin bilgisayarlarına zararlı yazılımlarla girmekte ve bu bilgisayarların işlem gücünü yetkisiz olarak kullanmaktadır[54]. Suçun faili ise veriler üzerinde tasarruf yetkisi bulunmayan kişidir[55].

51 Grzywotz, s. 181. Bulut bilişim (İngilizce: Cloud computing), bilgisayarlar ve diğer cihazlar için, istendiği zaman kullanılabilen ve kullanıcılar arasında paylaşılan bilgisayar kaynakları sağlayan, internet tabanlı bilişim hizmetlerinin genel adıdır. Bulut bilişim bu yönüyle bir ürün değil, hizmettir; temel kaynaktaki yazılım ve bilgilerin paylaşımı sağlanarak, mevcut bilişim hizmetinin; bilgisayarlar ve diğer aygıtlardan elektrik dağıtıcılarına benzer bir biçimde bilişim ağı üzerinden kullanılmasıdır. Bkz. https://tr.wikipedia.org/wiki/Bulut_bili%C5%9Fim

52 Koca- Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 918; Akbulut, Berrin, Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Yıl 2016, Cilt 24, Sayı 2, (ss. 7- 55), s. 34; Alp, Barış Emre, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu, Ankara 2019, s. 94.

53 Akbulut, Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme, s. 35.

54 Tahan, s. 123.

55 Akbulut, Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme, s. 19. Ayrıca bkz. "(…) suç

Kripto paralar belli algoritmalarla matematiksel işlemler sonucunda üretilen ve benzeri bulunmayan veriler olarak bilişim sistem araçlarında tutulmaktadır[56]. Veriler, etkinleştirilmiş güvenlik duvarı ile yetkisiz erişime karşı özel olarak korunur. Verilerin değiştirilmesinden bahsedebilmek için üçüncü tarafın verilere erişimini engelleyecek veya en azından bunu önemli ölçüde zorlaştıracak şekilde kurgulanmış bir erişim emniyetinin mevcut olması gerekir[57]. Veri değişikliği sonucunda, ilgili bilgisayar sistemi üzerinde internet aracılığıyla komuta kontrol sunucusuna bağlanılmış olur[58].

Kötü niyetli kişiler kripto para madenciliğinde, üçüncü taraf bilgisayarlarını kullanarak 244'üncü madde uyarınca veri değiştirme suçunu da işlemiş olabilir[59]. Belirtelim ki bu durum fidye yazılımlar60 vasıtasıy-

ile var olan sistem ve sistemdeki verilerin korunması, hem sistemin hem de sistem içerisindeki verilerin zarar görmemesi amaçlanmıştır, ancak sistemdeki verilere zarar verme dışında bu maddede tehlike suçu olarak nitelendirilebilecek iki seçimlik hareket daha düzenlenmiştir. Bunlar, sisteme veri yerleştirmek veya sistemdeki mevcut verilerin başka yere gönderilmesidir. Sistemdeki verilere müdahale niteliğindeki bu eylemleri gerçekleştiren kişiyi (faili) tespit için ise; mülkiyet, tasarruf ve kullanım yetkisine bakmak gerekecektir. Sisteme veri yerleştirme suçunun oluşması için; hukuka aykırı olarak girilen sisteme, veri sağlayıcısı tarafından izin verilmeyen şekilde veri girişi yapmak ya da veri taşıma araçları ile yükleme yapmak gerekir. Fail ise açıklandığı gibi veriler üzerinde tasarruf yetkisine sahip olmayan, sisteme hukuka aykırı olarak giren kişidir" (Yarg., 11. CD., 18.3.2021, 6165/2805).

56 Değirmenci, Olgun, Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi, Yaşar Hukuk Dergisi, C.1, S.2, Temmuz 2019, s.197.

57 BGH: Illegales Bitcoinschürfen, s. 403.

58 2017 yılında Almanya'da *Kempten Eyalet Mahkemesi,* iki kişinin Bitcoin ile para kazanmak için Botnet aracılığıyla başkalarının bilgisayarlarını kötüye kullandığı bir davaya bakmıştır. Sanıklar 29.10.2014 tarihinde StGB 202a, 303a ve 263a maddeleri uyarınca üç yıl hapis cezasına mahkum edilmiştir. Bkz. BGH: Illegales Bitcoinschürfen, s. 401 vd.

59 TCK'nın "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" başlıklı 244üncü maddesi, *"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, alt*ı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir ç*ıkar sa*ğlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur" şeklindedir.

60 Fidye yazılımı, şantaj yazılımı veya fidye virüsü (İngilizce): ransomware) olarak adlandırılan fidye yazılımlarına verilen genel bir addır. Fidye virüsleri bulaştığı bilişim sistemleri üzerinde dosyaları erişimi engelleyerek kullanıcılardan fidye talep eden zararlı yazılımlardır. Bkz. https://tr.wikipedia.org/wiki/Fidye_vir%C3%BCs%C3%BC

la mağdurun bilişim sistemine veri yerleştirilmesine benzemektedir. Başlangıçta fidye yazılım mağdur tarafından indirildiğinde herhangi bir suçun oluşmadığı düşünülse de verinin başkasının sistemine yerleştirilmesiyle birlikte örneğin, zararsız bir elektronik posta görüntüsü ile 244'üncü maddenin ikinci fıkrasındaki sisteme veri yerleştirme suçu oluşacaktır[61].

244'üncü maddede yer alan suçun konusunu bilişim sistemindeki veriler oluşturmaktadır. Verilerin sağlıklı kullanımını engellemeye yönelik bu fiil, 244'üncü maddesinin ikinci fıkrası uyarınca cezalandırılır. TCK'nun 244'üncü maddesinin 2'nci fıkrasında; *"Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen ki*şi, (…) cezalandırılır" denilmektedir. Verilere müdahaleyi yaptırım altına alan bu hüküm, Alman Ceza Kanunu'nun 303a maddesinde "verilerin değiştirilmesi" başlığı altında düzenlenmiştir. Buna göre, hukuka aykırı olarak verileri silen, erişilmez veya kullanılmaz hale getiren veya değiştiren kişi iki yıla kadar hapis veya para cezası ile cezalandırılır.

Bilişim sistemine zararlı yazılım içeren dosya veya e-posta gönderilmesi halinde bilişim sistemine girme (m. 243) değil, veri gönderimi söz konusu olduğundan 244'üncü maddedeki veri değiştirme suçu oluşur[62]. Kripto para madenciliği bakımından da fidye yazılımlarla ya da phising (oltalama) tuzakları ile bilgisayara zarar veriliyorsa fail 244'üncü maddeye göre cezalandırılır.

Bilişim sistemine girme suçunun işlenmesinden sonra (m. 243) fail ayrıca veri değiştirme suçunu da işlerse fikri içtima hükümlerinin uygulanması gerekir[63]. Gerçekten de bilişim sistemine girme fiili ile verileri

61 Değirmenci, s.193; Dülger, Murat Volkan, Bilişim Suçları Ve İnternet İletişim Hukuku, 8. Baskı, Ankara 2020, s. 122.

62 Tezcan-Erdem-Önok, s. 1153.

63 Koca- Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 906; Akbulut, Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme, s. 44.

değiştirme fiili, tek fiil kapsamında örtüşmektedir[64]. Kripto para madenciliğinde üçüncü taraf bilgisayarındaki verileri bozarak veya değiştirerek kriptografik şifreyi çözen ve özel anahtarları ele geçiren kişi de 244'üncü maddenin 2nci fıkrası uyarınca sorumlu tutulur[65].

Verilere yönelik müdahale bilişim sisteminin işleyişini engeller veya bozarsa 244'üncü maddenin birinci fıkrası uygulama alanı bulur[66]. Verilerin değiştirilmesinden bilişim sistemindeki verilerin niteliklerinin değiştirilmesi veya verilere yeni içerik kazandırılması anlaşılmalıdır. Kripto para madenciliğinde bilişim sistemindeki verilerde manipülasyon yapılmakta ve veriler başka biçimlere sokulmaktadır[67]. Kripto para madenciliğinde sistemin işleyişini engelleme ve bozma söz konusu olmadığında, fail 244'üncü maddenin ikinci fıkrası uyarınca cezalandırılır. Aslında burada verinin kullanım amacı dışında başka bir formata dönüştürülmesi söz konusudur[68].

Burada üzerinde durulması gereken bir diğer husus, virüs bulaştırılan bilgisayarın işletim sistemine kayıt defteri üzerinden giriş yapılması gerektiğidir. Kayıt defteri, işletim sistemi için merkezi bir öneme sahiptir. Merkezi bir öneme sahip kayıt defterine giriş yapıldıktan sonra bilgisayar kullanıcısının bir Botnet Truva atının işlevselliğini fark etmeksizin failin komuta kontrol sunucusu ile gizlice internet bağlantısı kurması gerekir[69]. Aksi halde, Truva Atı sisteminin kayıt defterine girişi ile veri değişikliği suçu işlenmiş olmaz. Bunun nedeni, bir veri tabanına başka bir girişin eklenmesinin mevcut verileri veya bir bilgisayar programını değiştirmemesi, yalnızca veri tabanını bütünüyle büyütmesi ve artırmasıdır[70].

64 Koca- Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 906.

65 Aksoy Retornaz, E. Eylem, "Ceza Hukuku Perspektifinden Blokzincir." Gelişen Teknolojiler ve Hukuk I: Blokzincir, 2020, ss. 307-309, s. 309.

66 Tezcan-Erdem-Önok, s. 1169.

67 Grzywotz, s. 334.

68 Özbek-Doğan-Bacaksız, s. 976.

69 Heine, s. 445.

70 Heine, s. 445.

Kişi, üçüncü taraf bilgisayarına kripto para madenciliği yapılabilecek bir yazılım yerleştirir ve bu bilgisayarın hem işlemci gücünü hem de elektrik enerjisini kullanırsa 244'üncü maddenin 4'üncü fıkrası tatbik edilir[71]. Fıkrada, bilişim sisteminin işleyişini engellemek, bozmak, sistemde yer alan verileri bozmak, yok etmek, değiştirmek, erişilmez kılmak, sisteme ek veriler yerleştirmek, var olan verileri başka bir yere göndermek suretiyle kendisi veya başkasının yararına haksız menfaat sağlanması yaptırıma bağlanmıştır.

Kripto para madenciliği yapmak maksadıyla bilişim sistemde yer alan verilere erişimi engelleyen ve bu suretle mağdurdan menfaat temini etmeye çalışan kişinin 244'üncü maddenin dördüncü fıkrasından sorumlu tutulması gerekir[72]. Kanun koyucu 244'üncü maddenin dördüncü fıkrasındaki suçu tamamlayıcı tali bir norm olarak düzenlemiş ve maddede tanımlanan fiillerin başka bir suç oluşturmaması halinde bu hükmün uygulanması gerektiğini belirtmiştir[73].

4. Yasak Cihaz veya Programlar Suçu (TCK m. 245/A)

Yasa dışı kripto para madenciliğinde "yasak cihaz veya programlar"ın kullanılması suçunun işlenmesi de mümkündür. 2016 yılında 6698 sayılı Kanunla TCK'nın bilişim alanında suçlar başlıklı onuncu bölüme eklenen 245/A maddesi[74], münhasıran bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlardan bahsederek TCK kapsamında bilişim suçlarının işlenmesinde kullanılan cihazların veya bilgisayar programlarının yapılmasını, oluşturulmasını, başkalarına verilmesini veya bulundurulmasını yaptırım altına almıştır.

71 Aksoy Retornaz, s. 309.

72 Değirmenci, s.194, 195.

73 Tezcan-Erdem-Önok, s. 1170.

74 TCK'nun "Yasak cihaz veya programlar" başlıklı 245/A maddesinde; *"(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır"* denilmektedir.

Bireysel veya toplu halde bilişim teknolojisi ile yapılan yasa dışı kripto para madenciliğinde yüksek donanıma sahip bilgisayarların kötü amaçlı yazılımlarla tehdit edildiği ortadadır. Bilgisayarları koruma amaçlı olan programların güvenlik duvarlarını aşabilmesi yasak cihaz veya programlarla mümkün olabilmektedir[75]. Bir linkin tıklanmasıyla ya da bir verinin bilgisayara indirilmesi veya kaydedilmesiyle bilgisayara zarar verilmekte ve bu sayede yasa dışı kripto para madenciliği yapılmaktadır. Bu fiilin birden fazla kişi tarafından irade ve fikir birlikteliği ile yapılması halinde müşterek fail olarak sorumluluktan bahsedilir.

245/A maddesi kapsamında bilgisayar teknolojisiyle ilgili unsurların yasa dışı faaliyetlerde kullanılması cezalandırılmaktadır. Yasa dışı kripto para madenciliği için bir cihazın, programın, şifre veya sair güvenlik kodunun üretilmesi halinde, kişi 245/A maddesi uyarınca cezalandırılır. Özellikle kripto para madenciliğinde tarayıcı seviyesinde çalışan program ve uygulamalarla kullanıcının sistemine erişilmekte ve üçüncü taraf bilgisayarının işlemci gücünün kullanılması mümkün olmaktadır[76].

Kişi, 245/A maddesinde yasaklanan fiillerden biri ile kripto para madenciliği yaparsa hem yasak cihaz veya program suçundan hem de 244'üncü maddede yer alan verileri değiştirme suçundan gerçek içtima hükümleri uyarınca ayrı ayrı cezalandırılır.

5. Karşılıksız Yararlanma Suçu (TCK m. 163)

Yasa dışı kripto para madenciliğinde, TCK'nun "Malvarlığına Karşı Suçlar" bölümünde yer alan "karşılıksız yararlanma" suçunun da tartışılması gerekir[77].

75 Özbek-Doğan-Bacaksız, s. 1021.

76 Kaya, Mehmet Bedii, Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim (Siber Güvenlik ve Savunma: Problemler ve Çözümler), (Editörler; Şeref Sağıroğlu, Mustafa Şenol), Ankara 2019, s. 227.

77 Bilişim sistemleri kısmında yaptığımız açıklamalarda bilişim sistemine girmekle kripto paraların veri olarak değerlendirilmesi ve veri değişikliği suçuna konu olduğunu belirtmiştik. Buradan hareketle kripto paraların malvarlığına karşı suçların konusunu oluşturduğunu da söylememiz gerekir. Bu konuda ayrıca bkz. Değirmenci, s. 197, 198. Yargıtay 6. CD'nin, 7.7.2020 tarih ve 1158/2598 sayılı kararında kripto paraların hukuki niteliğini tartışmasa da yağma suçuna konu olabileceğini belirtmiştir. Söz konusu kararda, *"Oluş ve dosya içeriğine göre; kendilerini polis olarak tanıtan ve silah gösteren sanıklar ... ve ...>ın dijital para borsası sahibi mağdur ...>i zorla araca bindirip, ellerini kelepçeledikten sonra bir otoparka götürdük-*

Belirtelim ki, TCK'nun 141'inci maddesinin ikinci fıkrasında *"ekonomik bir değer taşıyan her türlü enerji de taşınır sayılır"* şeklindeki hükümle maddi varlığı bulunmasa da her türlü enerjinin hırsızlık suçunun konusunu oluşturabileceği kabul edilmiş ve suçun elektrik enerjisi hakkında işlenmesi daha ağır cezayı gerektiren nitelikli hal olarak düzenlenmişti. Ancak 02.07.2012 tarih ve 6352 sayılı Kanunla bahse konu hüküm yürürlükten kaldırılmış ve elektrik enerjisinin sahibinin rızası olmaksızın kullanılması hırsızlık suçu olmaktan çıkarılmıştır. Değişiklikle eş zamanlı olarak 163'üncü maddenin üçüncü fıkrasına *"Abonelik esasına göre yararlanılabilen elektrik enerjisinin, suyun veya doğal gazın sahibinin rızası olmaksızın ve tüketim miktarının belirlenmesini engelleyecek şekilde tüketilmesi halinde kişi hakkında bir yıldan üç yıla kadar hapis cezasına hükmolunur"* şeklinde bir hüküm eklenmiştir. Buna göre, abonelik esasına göre yararlanılabilen elektrik enerjisi hırsızlık suçunun değil, karşılıksız yararlanma suçunun konusunu oluşur[78].

TCK'nın 163'üncü maddesinin üçüncü fıkrasına göre, abonelik esasına göre yararlanılabilen elektrik enerjisinin, sahibinin rızası olmaksızın ve tüketim miktarının belirlenmesini engelleyecek şekilde tüketilmesi suçtur[79]. Gerçekten de üçüncü taraf kişi ve kuruluşlara ait bilgisa-

leri, telefonda görüştükleri ...'ın da yönlendirmesi ile mağdura ait dizüstü bilgisayar ve cep telefonunu alıp beklemeye başladıkları, sanıklar ... ve ...>un başka bir araba ile otoparka geldikleri, sanık ...>ın mağdurdan zorla bilgisayar şifresi ile bitcoin işlemlerinde kullandığı şifreleri aldığı ve mağdura ait bilgisayar ile işlem yapmaya çalıştığı, internet bağlantısının zayıflığı nedeniyle işlem yapmakta zorlanınca internet bağlantısının daha güçlü olduğu bir mekana gitmek istediği, bu sırada mağdurun içinde bulunduğu aracın da başka bir otoparka geçerek beklemesini kararlaştırdıkları, mağdurun kaçırıldığı aracın izinin sürülememesi için sanık ...'un aracın plakalarını değiştirdiği, sanık ...'la birlikte internet bağlantısı kuvvetli bir mekana giderek ...'ın işlem yapmasını beklediği" denilmektedir.

78 Konuyla ilgili Alman Ceza Kanunu'nun StGB, § 248c maddesinde de hüküm bulunmaktadır. Maddede, bir "iletken" vasıtasıyla enerji çekme suç olarak düzenlenmiştir. Kablo ve metal gibi akımı iletmeye uygun olan şeyler iletken olduğundan kötü amaçlı yazılımlarla yapılan yasa dışı kripto para madenciliğinde § 248c maddesindeki suç oluşmaz. Bkz. Tahan, s. 124, 125.

79 TCK'nın "Karşılıksız yararlanma" başlıklı 163'üncü maddesinde, *"(1) Otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanan kişi, iki aydan altı aya kadar hapis veya adlî para cezası ile cezalandırılır. (2) Telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. (3) Abonelik esasına göre yararlanılabilen elektrik enerjisinin, suyun veya doğal gazın sahibinin rızası olmaksızın ve tüketim miktarının belirlenmesini engelleyecek şekilde tüketilmesi halinde kişi hakkında bir yıldan üç yıla kadar hapis cezasına hükmolunur"* denilmektedir.

yarlarda izinsiz olarak kripto para madenciliğinin yapılması karşılıksız yararlanma suçunu gündeme getirir. Ancak kripto para madenciliğinde üçüncü taraf bilgisayarının izinsiz kullanımı ile enerji tüketimi için failin enerjinin tüketim miktarının belirlenmesini engelleyecek şekilde hareket etmesi şarttır. Bu şart mevcut değilse karşılıksız yararlanma suçu oluşmaz[80].

Karşılıksız yararlanma bağlı hareketli bir suçtur. "*Engelleme*" ve "*tüketme*" şeklindeki iki fiil gerçekleşmeden eylem suç teşkil etmez. Fail, sahibinin rızası olmadan bir düzenek vasıtasıyla kendi tüketim miktarının belirlemesini bir takım manipülatif hareketlerle engellemelidir[81]. Yasa dışı kripto para madenciliğinde failin enerjinin tüketim miktarının belirlenmesini engelleyecek şekilde hareket etmesi şart olduğundan pratikte bu fiilin işlenmesinin çok güç olduğunu belirtmemiz gerekir. Bu şart gerçekleşmeksizin üçüncü taraf kişi ve kuruluşlara ait bilgisayarlarda izinsiz olarak yapılan kripto para madenciliği karşılıksız yararlanma suçunu oluşturmaz.

Sahibinin rızası olmaksızın ve tüketim miktarının belirlenmesini engelleyici hareketlerle elektrik enerjisinin tüketim miktarını gösteren sistem, tüketilen miktarı hiç göstermez veya olandan daha az gösterirse, yasa dışı kripto para madenciliği bakımından karşılıksız yararlanma suçu oluşur. Bu halde fail hem bilişim sistemine girme hem de karşılıksız yararlanma suçundan ayrı ayrı cezalandırılır. Belirtelim ki, fail tüketim miktarını engelleyici bir hareket yapmaksızın elektrik enerjisinden karşılıksız olarak yararlanırsa 163'üncü maddedeki suç oluşmaz. Bu ihtimalde özel hukuk uyuşmazlığı niteliğinde bir haksız fiilden bahsedilir.

80 Fail, enerjinin yetkisiz kullanımı için fiziksel bir iletken kullanmadığından Alman CK'nun 248c maddesi uyarınca, elektrik enerjisinde maliyet yaratan artış nedeniyle kendisini kovuşturmaya maruz kalmaz. Bkz. Baier, Johannes, Bitcoin ve Diğer Kripto Para Birimlerinden Kaynaklanan Suç Politikası Zorlukları- Bölüm 1, (Çeviren, Yener Ünver), Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022, s. 159.

81 Yılmaz, Zahit- Apiş, Özge, Karşılıksız Yararlanma Suçu (TCK m.163), Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Yıl 2013, Cilt 19, Sayı 2, s. 1761; Tahan, s. 125.

Sonuç

Kripto para madenciliği konusunda tartışmalara neden olan husus, enerji kaynaklarının hızla tükendiği bir dünyada kripto para madenciliği için çok fazla enerji tüketilmesi ve bu enerjinin bazı ülkelerin enerji ihtiyaçlarına ve tüketimlerine eşdeğer olmasıdır. Bu durum ülkeleri kripto para madenciliği konusunda tedbirler almaya ve enerjiden tasarruf edilmesi konusunda düzenlemeler yapmaya sevk etmektedir. Kötü niyetli kimseler artan elektrik masraflarına katlanmamak için üçüncü taraf bilgisayarları üzerinden yasa dışı kripto para madenciliği yapar. Ancak bu durum bilişim suçlarının işlenmesi sonucunu doğurur.

Bilişim sistemine girilerek değiştirilen veriler, hukuki tanımlamaya uygun olarak elektronik, manyetik veya başka bir şekilde hemen algılan(a)mayacak bir biçimde saklanan veya iletilen türden suç objeleridir. Bilgisayar kullanıcısı farkına varmadan zararlı yazılım otomatik olarak başlatılır. Bunun sonucunda, aslında internete kapalı olan bir erişim açılmış ve bunun üzerinden bilgisayar sistemi yasa dışı kripto para madenciliği yapmaya başlamış olur. Böylece fail tarafından işletim sistemindeki komuta ve kontrol sunucusu ele geçirilir ve veriler veri bankasına aktarılır. Bu şekilde hareket eden fail, TCK'nun 243'üncü maddede yer alan bilişim sistemine girme suçunu işler. Üçüncü tarafın bilgisayarına girilmesi ve kripto para üretilinceye kadar diğer bir ifadeyle kripto para madenciliği süresince bilişim sisteminde kalınması 243'üncü madde kapsamında bilişim sistemine girme suçunu oluşturur. Sisteme bir Truva atı yüklenmesi, ancak verilerin değiştirilmemesi halinde ise bilişim sistemindeki verilerin değiştirilmesi suçu oluşmaz.

Zararlı yazılımlarla sisteme girilmesi ve sonrasında üçüncü tarafın fark etmeyeceği bir biçimde bilgisayarın komuta ve kontrol sunucusuna bağlanılması verilerin değiştirilmesi suçuna da sebebiyet verir. Kripto para madenciliğinde sistemin işleyişini engelleme ve bozma söz konusu olmadığında, fail 244'üncü maddenin ikinci fıkrası uyarınca cezalandırılır. Aslında burada verinin kullanım amacı dışında başka bir formata dönüştürülmesi söz konusudur.

Kötü niyetli kimseler, kripto para madenciliği yapmak için üçüncü taraf bilgisayarına 245/A maddesinde yer alan seçimlik hareketler marifetiyle bir cihaz veya programla erişim sağladıklarında yasak cihaz veya programlar suçundan ayrıca cezalandırılır.

Karşılıksız yararlanma suçu bakımından ise failin enerjinin tüketim miktarının belirlenmesini engelleyecek şekilde hareket etmesi şarttır. Bu şart gerçekleşmeksizin üçüncü taraf kişi ve kuruluşlara ait bilgisayarlarda izinsiz olarak yapılan kripto para madenciliği karşılıksız yararlanma suçunu oluşturmaz.

Sonuç olarak, zararlı yazılım kullanarak kripto para madenciliğinin yapılması halinde öncelikle teknik analiz yapılmalı ve bu kapsamda fiil, TCK'nun 243 ve/veya 244'üncü maddeleri uyarınca değerlendirilmelidir.

Kaynakça

Agin, Nurşen Selen, Türk Ceza Hukuku'nda Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu (TCK md.158/1-f), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2019.

Akbulut, Berrin, Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Yıl 2016, Cilt 24, Sayı 2.

Aksoy Retornaz, E. Eylem, "Ceza Hukuku Perspektifinden Blokzincir." Gelişen Teknolojiler ve Hukuk I: Blokzincir, 2020.

Alp, Barış Emre, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu, Ankara 2019.

Baier, Johannes, Bitcoin ve Diğer Kripto Para Birimlerinden Kaynaklanan Suç Politikası Zorlukları- Bölüm 1, (Çeviren, Yener Ünver), Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022.

Baier, Johannes, Kriminalpolitische Herausforderungen durch Bitcoin und andere Kryptowährungen – Teil 1, CCZ 2019.

Balcı, Murat-Çakır, Kerim, Kripto Paralara El Konulması ve Kripto Paraların Müsadere Edilmesi, Mali Hukuk Dergileri, 17.198 (2021), (1503-1534).

Balcı, Murat- Çakır, Kerim, Kripto Paraların Karapara Aklama Yöntemi Olarak Kullanılması, Ceza Hukuku Dergisi, Cilt: 16, Sayı:46, Ağustos 2021, (ss. 311-332).

Balcı, Umut, Kripto Paraların Ceza Hukuku Boyutu ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri, TBB Dergisi 2021 (155).

Beukelmann, Stephan, Virtuelle Währungen, NJW-Spezial 2019. BGH: Illegales Bitcoinschürfen, NStZ, 2018.

Boehm, Franziska– Pesch Paulina, Bitcoin: Bir İlk Hukuki Analiz- Alman ve Birleşik Devletler- Amerikan Hukuku, (Çeviren, Doğa Satı), Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022.

Bozkurt Yüksel, Armağan Ebru, Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış, İÜHFM C. LXXIII, S. 2, (173-220), 2015.

Çarkacıoğlu, Abdurrahman, Kripto-Para Bitcoin, Sermaye Piyasası Kurulu Araştırma Dairesi Araştırma Raporu, 2016.

Değirmenci, Olgun, Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi, Yaşar Hukuk Dergisi, C.1, S.2, Temmuz 2019.

Dolandırıcılık Eylemleri ve Korunma Yöntemleri, Türkiye Bankalar Bilirliği, Aralık 2015.

Durdu Erdal, Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul 2018.

Dülger, Murat Volkan, Bilişim Suçları Ve İnternet İletişim Hukuku, 8. Baskı, Ankara 2020.

Erdoğan, Yavuz, Bilişim Sistemine Girme ve Kalma Suçu, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 12, Özel S., 2010, s.1363-1433 (Basım Yılı: 2012).

Goger, Thomas, Bitcoins im Strafverfahren-Virtuelle Währung und reale Strafverfolgung, MMR 2016.

Grzywotz, Johanna- Köhler, Olaf- Rückert, Christian, Cybercrime mit Bitcoins– Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention, Strafverteidiger, 2016.

Heine, Sonja, Bitcoinler ve Botnetler- Yasadışı Bitcoin Madenciliğinde Cezalandırılabilirlik ve Malın Müsaderesi (Çev. Mehmet Karatepeli), Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022.

Heine, Sonja, Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining, NStZ 2016.

https://tr.investing.com/news/cryptocurrency-news/abd-bitcoin-madenciliginde-lider-konuma-yukseldi-turkiyenin-pay-ne-kadar-2203532

https://www.chip.com.tr/haber/mining-kripto-para-madenciligi-nedir-nasil-yapilir-turleri-nelerdir_96470.html

İmamoğlu, Deniz Alp, Kripto Para Birimleri Ve Türk Hukukunda Düzenlenmesi, 2. Baskı, Ankara 2021.

Kaya, Mehmet Bedii, Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim (Siber Güvenlik ve Savunma: Problemler ve Çözümler), (Editörler; Şeref Sağıroğlu, Mustafa Şenol), Ankara 2019.

Koca, Mahmut-Üzülmez, İlhan, Türk Ceza Hukuku Özel Hükümler, 7. Baskı, Ankara 2020.

Lewis, Antony, The Basics of Bitcoins and Blockchains, USA 2018.

Müller, Eckhart-Schlothauer, Reinhold-Knauer, Christoph, Münchener Anwalts Handbuch Strafverteidigung, 3. Auflage 2022.

Özbek, Veli Özer-Doğan, Koray-Bacaksız, Pınar, Türk Ceza Hukuku Özel Hükümler, 16. Baskı, Ankara 2021.

Özdemir, Gençer, Kripto Paraların Eşya Niteliği, SDÜHFD C: 11, S: 1, Y: 2021.

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

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

Stabile, Daniel T.-Prior, Kimberly A.-Hinkes, Andrew M., Digital Assets and Blockchain Technology: U.S. Law and Regulation, Edward Elgar Publishing, USA 2020.

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

Tezcan, Durmuş- Erdem, Mustafa Ruhan- Önok, R. Murat, Teorik ve Pratik Ceza Özel Hukuku, 19. Baskı, Ankara 2021.

Tomrukçu, Tuğçe, Kripto Varlıkların Konu Olduğu Dolandırıcılık Suçları, Kripto Para ve Ceza Hukuku, (Editörler; Yener Ünver, Kayıhan İçel, Kerem Öz), Ankara 2022.

Turanboy, Asuman, Kripto Paraların Ortaya Çıkmaları ve Hukuki Nitelikleri, Banka ve Ticaret Hukuku Dergisi, Cilt: 35, Sayı:3, Eylül 2019.

Wenger, Tobias-Tokarski, Kim Oliver, Kryptowährungen, (Jochen Schellinger, Kim Oliver Tokarski, Ingrid Kissling-Näf Digitale Transformation und Unternehmensführung Trends und Perspektiven für die Praxis), Springer Gabler, 2020.

Yılmaz, Zahit-Apiş, Özge, Karşılıksız Yararlanma Suçu (TCK m.163), Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Yıl 2013, Cilt 19, Sayı 2.