KRİPTO VARLIKLAR VE CEZA HUKUKU SORUMLULUĞU[*1]

Arş. Gör. **Zeynep Esra TARAKÇIOĞLU**[*2]

Öz

İnsanlar tarafından kurulan para sistemleri zaman içinde yetersiz kalarak yerini farklı ödeme sistemlerine bırakmıştır. Kullanılan ödeme yöntemleri, özellikle teknolojinin gelişmesiyle birlikte büyük oranda değişmeye başlamıştır. Bu değişikliğin gerçekleşmesinde, itibari paranın elektronik ortamda kullanılmasına imkân tanıyan elektronik ödeme sistemleri önemli bir rol oynamıştır. En radikal değişim ise kripto varlıkların ortaya çıkmasıyla yaşanmıştır. Kripto varlıkların yaygınlaşmasıyla zamandan ve mekândan bağımsızlaşan, fiziki ve coğrafi sınırlamalardan kurtulan paralar kullanılmaya başlanmıştır. Esasında kripto varlıklar, mahremiyeti ve işlem şeffaflığını kripto şifreleme yöntemiyle koruyarak aracısız ve güvenli veri transferi yapılmasını sağlayan yazılımlardır. Ancak bu varlıklar, verilerin değişim ve yatırım amacıyla kullanılmasına olanak sağladığı için para ile özdeşleştirilmektedir.

Bitcoin'in ortaya çıkmasıyla hayatımıza dahil olan kripto varlıklar, güvenlik, mahremiyet ve hız gibi birçok konuda kişilere büyük avantaj sağlamaktadır. Parasal bir değerin dünyanın bir ucundan diğer bir ucuna daha hızlı, daha güvenli ve daha ucuz şekilde transfer edilebilmesi, bu varlıkların önemli ölçüde yaygınlaşmasına neden olmuştur. Fakat bu teknolojinin sağladığı avantajlar, suç işlemek için yeni fırsatlar arayan suçluların da dikkatini çekmektedir. Üstelik kripto varlıkların ortak kabul gören hukuki bir kimliği bulunmadığından hem ulusal hem de uluslararası alanda yasal boşluklar ortaya çıkabilmektedir. Bu durum, suç işlemek isteyen kişilerin daha yoğun bir şekilde bu alana yönelmesine sebep olmaktadır. Suçlular, kripto varlıkların sağladığı anonimlikten faydalanarak hırsızlık, dolandırıcılık, uyuşturucu ve uyarıcı madde ticareti, silah ticareti, suçtan kaynaklanan malvarlığı değerlerinin aklanması, vergi kaçakçılığı, terörizmin finansmanı gibi birçok suç tipini daha korkusuz ve kolay şekilde işlemektedir. Bu nedenle konunun cezai ve hukuki açıdan mercek altına alınması önem taşımaktadır. Özellikle mevcut ceza hukuku düzenlemelerinin, kripto varlıkların sanal, anonim ve kompleks yapısıyla mücadele etmek için yeterli olup olmadığının değerlendirilmesi gerekmektedir. Bu kapsamda ilk olarak konuyla ilgili temel kavramlar hakkında bilgi verilmiş, sonrasında Bitcoin üzerinden kripto varlıkların sistemsel özellikleri somutlaştırılmaya çalışılmıştır. Çalışmanın ikinci ve son bölümünde ise konunun ceza hukuku bakımından yansımaları ele alınarak, hırsızlık, yağma, dolandırıcılık ve suçtan elde edilen malvarlığı değerlerinin aklanması suçu özelinde Türk ceza hukuku bakımından ayrıntılı bir inceleme yapılmıştır.

Anahtar Kelimeler

Sanal Para Birimleri, Elektronik Para, Kripto Varlıklar, Bitcoin, Hırsızlık, Dolandırıcılık, Suçtan Elde Edilen Malvarlığı Değerlerinin Aklanması.

[*1] Makalenin Dergiye Geliş Tarihi: 16.11.2021 - Makalenin Kabul Edildiği Tarih: 8.12.2021, DOI No: 10.54704/akdhfd.1024708.

[*2] Hacettepe Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Hukuk Bilimleri Anabilim Dalı / Ankara - Türkiye.
E-posta: zeynepdilek@hacettepe.edu.tr,
Orcid Id: https://orcid.org/0000-0002-6641-3225.

CRYPTOASSETS AND CRIMINAL LIABILITY

Abstract

The monetary systems established by people became insufficient over time and left their place to different payment systems. The payment methods used have started to change significantly, especially with the development of technology. Electronic payment systems, which allow the use of fiat money in electronic form, played an essential role in realizing this change. The most radical change has been experienced with the emergence of crypto assets. With the spread of crypto assets, money that becomes independent of time and space, free from physical and geographical limitations, has begun to be used. In fact, crypto assets are software that provides unmediated and secure data transfer by protecting the privacy and transaction transparency with crypto encryption. However, these assets are identified with money because they allow data to be used for exchange and investment purposes.

Crypto assets, which have become part of our lives with the emergence of Bitcoin, provide a great advantage to people in many areas such as security, privacy, and speed. The fact that a monetary value can be transferred from one part of the world to the other faster, safer, and cheaper has led to the widespread use of these assets. However, the advantages of this technology also attract the attention of criminals who are looking for new opportunities to commit crimes. Moreover, since crypto-assets do not have a common legal identity, legal gaps emerge nationally and internationally. This situation causes people who want to commit crimes to tend to this area more intensely. Criminals commit many crimes such as theft, fraud, drug trafficking, arms trade, money laundering, tax evasion, financing of terrorism more fearlessly and effortlessly by taking advantage of the anonymity provided by crypto assets. Therefore, it is crucial to examine the issue from a criminal and legal perspective. In particular, it is necessary to evaluate whether the current criminal law regulations are sufficient to combat the virtual, anonymous, and complex structure of crypto assets. In this context, the basic concepts related to the subject were provided, and then the systematic features of crypto assets via Bitcoin were tried to be concreted. In the second and last part of the study, the subject's reflections in terms of criminal law were discussed, and a detailed examination was carried out in Turkish criminal law, especially for the crime of theft, looting, fraud, and money laundering.

Keywords

Virtual Currencies, Electronic Money, Crypto Assets, Bitcoin, Theft, Fraud, Money Laundering

Extended Abstract

The monetary systems established by people became insufficient over time and left their place to different payment systems. The payment methods used have started to change significantly, especially with the development of technology. Electronic payment systems, which allow the use of fiat money in electronic form, played an essential role in realizing this change. The most radical change has been experienced with the emergence of crypto assets. With the spread of crypto assets, money that becomes independent of time and space, free from physical and geographical limitations, has begun to be used. In fact, crypto assets are software that provides unmediated and secure data transfer by protecting the privacy and transaction transparency with crypto encryption. In other words, crypto-assets transform money from tangible physical objects such as paper or coins into the software. However, these assets are identified with money because they allow data to be used for exchange and investment purposes. Therefore, even if the phrase currency is used, it should be stated that they are different from fiat money and do not have the same legal character.

Today, there are thousands of crypto-asset types produced from different software. Since the software that forms the basis of crypto assets differs, the systemic features and the level of anonymity may vary. Bitcoin is an important example of understanding the systemic features, as it constitutes the origin of many crypto assets. The most well-known example of its kind, Bitcoin, is a digital finance protocol that ensures reliable transfer of monetary value by protecting user privacy with cryptographic encryption and making transaction records transparent with Blockchain structure. The smooth operation of this protocol depends on the existence of some systemic features and actors. In this context first feature to dwell on is cryptographic encryption techniques. In the issuance and circulation of Bitcoin, encryption (cryptographic) techniques are used, which converts transactions into an unreadable format so that only certain people can decrypt them. These encryption techniques play a vital role in ensuring transaction

security. Nevertheless, the use of these techniques is not capable of preventing all risks. In order to prevent problems such as double payment, fake Bitcoin production, there is a need for a private recording system that will enable the tracking of transactions. At this point, the Blockchain system comes to the fore, allowing users to remain anonymous while enabling the tracking of the transactions. However, since there is no centralized structure in the Bitcoin system, people are needed to follow and verify the transactions. For this reason, actors known as miners are included in the system that ensures the verification of transactions. All these mentioned elements are essential in terms of ensuring the continuity and security of the Bitcoin system.

Crypto assets, which have become part of our lives with the emergence of Bitcoin, provide a great advantage to people in many areas such as security, privacy, and speed. The fact that a monetary value can be transferred from one part of the world to the other faster, safer, and cheaper has led to the widespread use of these assets. However, the advantages of this technology also attract the attention of criminals who are looking for new opportunities to commit crimes. Moreover, since crypto-assets do not have a common legal identity, legal gaps emerge nationally and internationally. This situation causes people who want to commit crimes to tend to this area more intensely. Criminals commit many crimes such as theft, fraud, drug trafficking, arms trade, money laundering, tax evasion, financing of terrorism more fearlessly and effortlessly by taking advantage of the anonymity provided by crypto assets. In addition, since it can be easily converted into real money, crypto-assets can also be used as financing for committing certain crimes or obtaining the necessary criminal tools. Therefore, it is crucial to examine the issue from a criminal and legal perspective. In particular, it is necessary to evaluate whether the current criminal law regulations are sufficient to combat the virtual, anonymous, and complex structure of crypto assets. In this context, the basic concepts related to the subject were provided, and then the systematic features of crypto assets via Bitcoin were tried to be concreted. In the second and last part of the study, the subject's reflections in terms of criminal law were discussed, and a detailed examination was carried out in Turkish criminal law, especially for the crime of theft, looting, fraud, and money laundering.

GİRİŞ

Günlük hayatın her alanında yaygın olarak kullanılan madeni ve kâğıt formundaki paralar, evrensel olarak kabul edilen değişim araçlarıdır. Ancak paranın madeni para ve kâğıt para formuna sahip olması uzun bir tarihsel süreç sonrasında gerçekleşmiştir. Önceleri kendinden bir değere sahip olan pirinç, sığır ve deniz kabuğu gibi mallar bir çeşit para formu olarak kullanılırken, daha sonraları emtiaya dayalı paralar ortaya çıkmış ve daha büyük miktarlarda paranın el değiştirmesi kolaylaşmıştır.[1] Günümüzde gelinen nokta itibariyle, merkezi bir otorite tarafından kontrol edilen ve hukuk ürünü olan itibari paralar kullanılmaktadır. Bu bakımdan, paranın gelişimi ile insanlığın, sosyal, ekonomik ve teknolojik gelişimi arasında bir bağlantı kurulması mümkündür. Başka bir ifadeyle para, meydana gelen değişimlere kendini uyarlama potansiyeline sahip bir değer olarak tarihsel süreç içerisinde önemli ölçüde değişikliğe uğramıştır.

Paranın geçirdiği süreçler göz önüne alındığında, özellikle teknolojik gelişmelerin bu süreç içinde ayrı bir yere sahip olduğu anlaşılmaktadır. Teknolojide meydana gelen gelişmelerle birlikte elektronik ödeme yöntemleri yaygınlık kazanmış ve para transferleri elektronik ortamda gerçekleştirilmeye başlanmıştır. Bunun sonucunda fiziksel bir varlığa sahip olan dolayısıyla eller hissedilebilir ve gözle görülebilir olan paranın bir veri olarak elektronik ortamda tedavül etmesi mümkün hale gelmiştir. Teknolojide

[1] European Central Bank, Virtual Currency Schemes, 2012, 9.

yaşanan süratli gelişmeler karşısında uyum sağlama yetisine sahip olan para, niteliksel değişikliğe uğrayarak soyutlaşmaya, zamandan ve mekândan bağımsızlaşmaya başlamıştır. Ancak kripto varlıkların ortaya çıkması, para kavramına olan bakış açısını kökten değiştirerek yeni bir dönemin kapısını aralamıştır. Henüz hukuki olarak aydınlatılmayan bu yeni dönem kripto varlıkların suç işlemek için cazibe merkezi haline gelmesine neden olmuştur. Dolayısıyla kripto varlıkların irdelenmesi ve hukuki olarak aydınlatılması, bir savunma mekanizması oluşturulması bakımından önem taşımaktadır.

"Kripto Varlıklar ve Ceza Hukuku Sorumluluğu" başlıklı bu çalışma ile kripto varlıkların hangi suçlara konu edilebileceği ve bu suçların Türk hukukundaki hangi düzenlemeler kapsamında ele alınabileceği sorularına cevap verilmesi amaçlanmaktadır. Temel olarak Türk mevzuatı göz önüne alınarak değerlendirme yapılacak ise de uluslararası hukuk ve yabancı hukuk düzenlemelerinden ve uygulamalarından da örnekler verilecektir. Bu kapsamda ilk olarak konuyla ilgili temel kavramlar hakkında bilgi verilecek, sonrasında kripto varlıkların sistemsel özellikleri açıklanmaya çalışılacaktır. Ancak sayısı binleri aşan kripto varlıkların kullandığı sistemler ve taşıdığı özellikler farklılık gösterdiği için konunun sınırlandırılması gerekmektedir. Söz konusu çalışmada, en yaygın kullanılan ve en büyük ticaret hacmine sahip olan Bitcoin üzerinden bir somutlaştırma yapılacak, konuyla ilişkili olduğu ölçüde diğer kripto varlıklara da değinilecektir. Çalışmanın ikinci ve son bölümünde ise konunun ceza hukuku bakımından yansımaları ele alınarak; hırsızlık, yağma, dolandırıcılık ve suçtan elde edilen malvarlığı değerlerinin aklanması suçu özelinde Türk ceza hukuku bakımından ayrıntılı bir inceleme yapılacaktır.

I. SANAL PARA BİRİMLERİ

A. GENEL OLARAK

Kripto varlıkların ne olduğuna ilişkin genel bir çıkarım yapabilmesi için bu varlıkların dahil olduğu kapsayıcı küme hakkında da bilgi sahibi olunması gerekmektedir. Genel kabule göre kripto varlıklar, sanal paranın bir alt kategorisini oluşturmaktadır.[2] Dijital bir temsili ifade eden sanal paralar, merkezi bir geliştiriciye sahip olmayan tarafların bunları kullanmayı kabul ettiği müddetçe kullanılabilen ve elektronik olarak elde edilebilir, saklanabilir, erişilebilir ve işlem yapılabilir nitelikle olan değerlerdir.[3] Benzer nitelikteki tanımlamaları,

[2] Avrupa Merkez Bankası (ECB), Uluslararası Para Fonu (IMF), Uluslararası Ödemeler Bankası bünyesinde ödeme sistemleri konusunda çalışmalarını sürdürmekte olan Ödemeler ve Piyasa Altyapıları Komitesi (CPMI), Avrupa Bankacılık Otoritesi (EBA), Avrupa Menkul Kıymetler ve Piyasalar Kurulu (ESMA), Dünya Bankası, Mali Eylem Görev Gücü (FATF) gibi önemli teşkilatlar, kripto varlıkları sanal paranın bir alt kümesi olarak değerlendirmektedir. Konuya ilişkin benzer değerlendirmelere yer veren raporlar için bknz.: U.S Department of Justice, Cryptocurrency Enforcement Framework, Report of Attorney Generals Cyber Digital Task Force, 2020, 3.

[3] Dong He; Karl Habermeier; Ross Leckow; Vikram Haksar; Yasmin Almeida; Mikari Kashima; Nadim Kyriakos-Saad; Hiroko Oura; Tahsin Saadi Sedik; Natalia Stetsenko and Concepcion Verdugo-Yepes, Virtual Currencies and Beyond: Initial Considerations, IMF Staff Discussion Note,

uluslararası kuruluşların düzenlemelerinde ve yabancı hukuk mevzuatlarında da görmek mümkündür. Avrupa Merkez Bankası 2015 yılında yayınlamış olduğu bir analizde sanal para birimlerini, merkez bankası, kredi kuruluşu ve elektronik para kuruluşları tarafından ihraç edilmeyen ve bazı durumlarda paraya alternatif olarak kullanılabilen değerin dijital temsili olarak tanımlamıştır.[4] Mali Eylem Görev Gücü -Financial Action Task Force (FATF) ise sanal para birimlerini, dijital ortamda değişim aracı, hesap birimi olarak işlev gören ve bir değerin depolanmasına olanak sağlayan ancak yasal bir statüye sahip olmayan bir değer olarak tarif etmiş ve sahip olunan fonksiyonlar üzerinden bir tanım geliştirmiştir.[5] 2015/849/EC sayılı Direktif'de ise sanal paralar, merkez bankası veya bir kamu otoritesi tarafından basılmayan ve garanti edilmeyen, yasal olarak düzenlenen bir para birimine bağlı olması gerekmeyen ve yasal bir para birimi statüsünde de olmayan, elektronik ortamda transfer edilebilen, saklanabilen, alınıp satılabilen ve bir mübadele aracı olarak kabul edilen değer şeklinde ifade edilmiştir. Sanal para kavramına ilişkin yabancı hukukta yapılan tanımlara ise Amerika'dan ve Litvanya'dan örnek verilmesi mümkündür. Litvanya Para Aklanmasının ve Terörizmin Finansmanının Önlenmesi Hakkında Kanun'da (*Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing*) sanal para birimlerinin tanımı; banknot, madeni para, elektronik para ve yasal bir ödeme aracı olarak tanımlanamayan ancak dijital olarak transfer edilebilen, depolanabilen, işlem gören ve değişim aracı olarak fonksiyon gören değerin dijital bir temsili şeklinde yapılmıştır. Washington ise Para Hizmetleri Kanunu'nun (*Uniform Money Services Act*) 19.230.10 numaralı bölümünde sanal para kavramını; değişim aracı, hesap birimi veya değer depolanması için kullanılan ancak Amerika Birleşik Devletleri Hükümeti tarafından tanınan yasal bir statüye sahip olmayan değerin dijital bir temsili olarak ele almıştır. Yapılan bu tanımlardan hareketle sanal paraların üç temel özelliği bulunduğu söylenebilir. Bunlar; sanal para birimlerinin yasal bir statüye sahip olmaması, bir değişim aracı olması ve ancak dijital ortamda işlev görebilmesidir.

Bu noktada, sanal para ile elektronik para kavramlarının birbirinden ayrılması önem arz etmektedir. Her ne kadar sanal parayı elektronik paranın bir alt grubu olarak değerlendiren görüşler bulunsa da esasında sanal paralar birçok özelliğiyle

2016, 7. Sanal para kavramına ilişkin yapılan diğer tanımlar için bknz: U.S Department of Justice, Cryptocurrency Enforcement Framework, 2.

4 European Central Bank, Virtual Currency Schemes - A Further Analysis, 2015, 25; Avrupa Bankacılık Otoritesi de benzer şekilde sanal para birimlerini, bir merkez bankası ve kamu otoritesi tarafından basılması ve itibari para ile zorunlu bir ilişkisi bulunması gerekmeyen ancak gerçek veya tüzel kişiler tarafından bir değişim aracı olarak kullanılan ve elektronik olarak aktarılabilen, saklanabilen veya işlem görebilen dijital bir değer olarak tanımlamıştır. İlgili tanım için bknz: Europe Banking Authority, Opinion on Virtual Currencies, 2014, 11.

5 Financial Action Task Force (FATF), Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014, 4.

elektronik paradan ayrılmaktadır. Elektronik paralar dijital ortamda itibari parayı temsil ederken, sanal paraların gerçek hayatta temsil ettiği somut bir değer bulunmamaktadır.[6] Sanal paranın temsil ettiği değer, sistemin kendine özgü olan soyut bir değerdir. Bu durum, hukuki açıdan da elektronik para ile sanal para arasında bir ayrım yapılmasını gerektirmektedir. İtibari para yasal olarak düzenlenen ve evrensel olarak korunan bir değer olduğundan, elektronik paralar bakımından da benzer düzenlemeler yapılması söz konusu olmaktadır. Ancak sanal paraların düzenlenmesi ve korunması noktasında karşımıza böyle evrensel bir koruma mekanizması bir yana kapsamlı yasal bir koruma dahi çıkmamaktadır. Dolayısıyla, elektronik para ile sanal para arasında bir değeri dijital olarak temsil etme özelliği ile sınırlı bir benzerlik bulunmaktadır. Bu nedenle, sanal paraların elektronik para kapsamında incelenmesinin ne kadar doğru bir yaklaşım olduğunun sorgulanması gerekmektedir. Konuya ilişkin hem Türk doktrininde hem de yabancı hukuk doktrininde bazı tartışmalar yapıldığını ve sanal paraların itibari para olarak kabul edilmemesi yönünde genel bir eğilim bulunduğunu görmekteyiz.[7] Nitekim Avrupa Merkez Bankası, 2015 yılında yayımlamış olduğu analizinde daha önce yaptığı sanal para birimi tanımından[8] "*money*" ifadesini çıkarmış ve bu değişikliğe sanal para birimlerinin likit bir varlığı olmamasını ve paranın sahip olması gereken kabul seviyesine ulaşmamasını gerekçe olarak göstermiştir.[9] Mali Eylem Görev Gücü de ilk yayımlamış olduğu raporlarda "*sanal para (virtual currency)*" kavramını kullanmaktayken, 2018 yılında güncellediği Tavsiye Kararı'nda "*sanal varlık (virtual assets)*" ifadesine yer vermiştir. Benzer şekilde Japonya'da da Ödeme Hizmetleri Kanunu'nda (*Payment Services Act*) 2019 yılında değişikliğe gidilerek, "*sanal para*" kavramı yerine "*sanal varlık*" kavramının kullanması tercih edilmiştir. Netice olarak, bünyesinde para ifadesini barındırsa bile sanal para birimlerinin elektronik paradan farklı bir kavram olduğu ve aynı hukuki niteliğe sahip bulunmadığı ifade edilmelidir. Bu eğilimin bir yansıması olarak, söz konusu çalışmada "*kripto para*" kavramı yerine "*kripto varlık*" ifadesinin kullanılması tercih edilmiştir.

Yapılan tanımlar göz önüne alındığında, sanal para birimlerinin internet kuponları, uçak milleri ve kripto varlıklar gibi birçok kümeyi kapsadığı anlaşılmaktadır. Buna karşın, sanal para birimlerini kendi içinde farklı ayrımlara tabi tutmak

---

6 Abdurrahman Çarkacıoğlu, Kripto-Para Bitcoin, Sermaye Piyasası Kurulu Araştırma Raporu, 2016, 7.

7 Michael Abramowicz, "Cryptocurrency-Based Law," Arizona Law Review 58, S.2 (2016): 361; Osman Gazi Güçlütürk, "Türk Hukukunda Kripto Varlıkların Para ve Elektronik Para Niteliğinin İncelenmesi," Regesta Ticaret Hukuku Dergisi 4, S.3 (2019): 387.

8 Avrupa Merkez Bankası 2012 yılında yayımlamış olduğu analizinde sanal para birimlerini, geliştiricileri tarafından kontrol edilen ve tedavül ettirilen, belirli bir sanal topluluğun üyeleri arasında geçerli olan ve hukuki olarak düzenlenmemiş dijital para olarak tanımlamıştı. Görüldüğü gibi sanal para alanında meydana gelen değişimler, yapılmış olan bir tanımın sadece 3 yıl içerisinde geçerliliğini kaybetmesine yol açmıştır. 2012 tarihinde yapılan bu tanım için bknz: European Central Bank, Virtual Currency Schemes, 13.

9 European Central Bank, Virtual Currency Schemes - A Further Analysis, 25.

mümkündür. Bu kapsamda en yaygın şekilde kullanılan ayrım, kullanılan sistemin merkezi mi yoksa hibrit nitelikte mi olduğuna ilişkindir. Daha sonra da ayrıntılı inceleneceği üzere, Bitcoin, Litecoin, Namecoin gibi birçok kripto varlık katılımcıların başrol oynadığı merkezi olmayan bir sistem kullanmaktayken, Linden Doları gibi bazı kripto varlıklar merkezi bir sisteme sahip bulunmaktadır. Bununla birlikte bazı işlemlerin katılımcılar, bazı işlemlerin merkezi bir otorite tarafından yürütüldüğü hibrit sistemler de kullanılabilmektedir.[10] Bu sistemi kullanan kripto varlıklara ise işlem güvenliğinin ve geçerliliğinin tamamen olmasa da büyük oranda Ripple Labs tarafından sağlandığı Ripple (*XRP*) örnek olarak verilebilir.[11]

Sanal paralar bakımından yapılan diğer önemli bir ayrım ise mal, hizmet ve gerçek para birimlerine dönüştürebilirlik düzeylerini esas almaktadır. Dönüştürebilirlik düzeyini esas alan bu ayrımda sanal para birimleri; kapalı sistem, tek yönlü akışa sahip sistem ve çift yönlü akışa sahip sistem olarak üçlü bir başlık altında incelenmektedir. Kapalı sistemi kullanan sanal para birimleri, sadece ait olduğu sanal ortamda kullanılabildiği için gerçek hayat ile bağlantısı önemli ölçüde sınırlandırılmış bir yapıya sahip bulunmaktadır. Bu sisteme en iyi örnek, sanal para birimi kullanan oyunlardan biri olan World of Warcraft'dır. Bu oyunda kazanılan sanal paralar (*World of Warcraft Gold*) gerçek ekonomik bir değere sahip olmadığı gibi sadece oyun platformu içinde kullanılabilmektedir.[12] Ekonomik değere sahip olan araçlarla alınmasına karşın tekrardan bunlara dönüştürülemeyen sanal para birimleri bakımından ise tek yönlü akışa sahip sistem karşımıza çıkmaktadır. Bu sistemde tek yönlülük, gerçek paranın sanal para birimine dönüştürülebilirken, sanal para biriminin gerçek para birimine dönüştürülememesinden kaynaklanmaktadır.[13] Bu kapsamda, gerçek para karşılığı alınmasına karşın tekrardan gerçek para birimlerine dönüştürülemeyen Facebook Credits ve Project Entropia Dollars örnek olarak verilebilir.[14] Çift yönlü akışa sahip sanal para birimlerinde

---

10 He, Habermeier, Leckow, Haksar, Almeida, Kashima, Kyriakos-Saad, Oura, Sedik, Stetsenko and Verdugo-Yepes, Virtual Currencies and Beyond: Initial Considerations, 8.

11 Ripple hakkında ayrıntılı bilgi için bknz: Frederik Armknecht; Ghassan O. Karame; Avikarsha Mandal; Franck Youssef and Erik Zenner, "Ripple: Overview and Outlook, Trust and Trustworthy Computing," in Lecture Notes in Computer Science, ed. Mauro Conti, Matthias Schunter, Ioannis Askoxylaki (Cham: Springer, 2015), 171; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 5; Adrian Blundell Wignall, The Bitcoin Question: Currency versus Trust-less Transfer Technology, OECD Working Papers on Finance, Insurance and Private Pensions No: 37, 2014, 15; European Central Bank, Virtual Currency Schemes - A Further Analysis, 11-12; Derya Mutluoğlu, "Kripto Para Birimleri ve Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu," (Yüksek Lisans Tezi, Ankara Üniversitesi, 2020), 37 vd.

12 Ioannis Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," (Doctoral Thesis, School of Information and Communication Technology Royal Institute of Technology, 2015), 18.

13 Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 18.

14 FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 4; Armağan Ebru Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış," İÜHFM 73, S.2 (2015): 198.

ise sanal paranın tekrardan gerçek paraya dönüştürülmesi mümkündür. Başka bir ifadeyle, çift yönlü akışa sahip sanal paralar hem gerçek parayla alınabilen hem de gerçek paraya dönüştürülebilen bir niteliği haiz bulunmaktadır. Bu bakımdan çift yönlü akışa sahip sanal para birimleri, ekonomik bir değeri temsil etmekte ve bu değer yerine kullanılabilmektedir. Bu sistemi kullanan sanal paraların en önemli örneğini ise kripto varlıklar oluşturmaktadır. Bitcoin, Linden Doları, Ethereum gibi birçok kripto varlık, çift yönlü akışa sahip bir dönüştürülebilirlik düzeyine sahip bulunmaktadır. Ancak dikkat edilmesi gerekirse, sanal para birimleri yasal bir statüye sahip olmadığından yalnızca tarafların bunları kullanmayı kabul ettiği müddetçe dönüştürülebilir niteliktedir.[15]

B. KRİPTO VARLIKLAR

1. Genel Olarak

Sanal paraların bir alt grubunu oluşturan kripto varlıkların farklı bakış açıları ışığında tanımlanması mümkündür. Bir kullanıcı açısından kripto varlıklar, telefon veya bilgisayara indirilerek mal ve hizmet satın alınması, yatırım yapılması, fon sağlanması gibi çeşitli amaçlarla kullanılabilen dijital değişim araçlarını ifade etmektedir. Teknik bir bakış açısından ise kripto varlıkların verileri değişim aracı olarak kullanmaya imkân sağlayan yazılımlar olduğunu söyleyebiliriz. Başka bir deyişle, kripto varlıklar parayı kâğıt veya madeni para gibi elle tutulur fiziki nesneler olmaktan çıkartıp birer yazılıma dönüştürmektedir.[16] Kripto varlıkların genel kabul görmüş hukuki bir tanımı bulunmamakla birlikte sanal paraya ilişkin farklı kuruluşların yaptığı tanımlardan faydalanılabilmektedir. Ancak bu tanımlara önemli bir unsurun da eklenmesi gerekmektedir. Kripto varlıkların ihracında ve tedavül etmesinde, işlemleri okunamayan bir biçime dönüştürerek yalnızca belirli kişilerin bu işlemleri deşifre edebilmesine imkân tanıyan şifreleme (*kriptografik*) teknikleri kullanılmaktadır. Bu nedenle, bu varlıklara kripto veya kriptografik varlık denmektedir.[17] Nitekim Dünya Bankası tarafından kripto varlıklar, katılımcılar arasında konsensüsü sağlamak için kriptografik teknikler kullanan dijital para birimleri olarak tanımlanmıştır.[18] Avrupa Bankacılık Otoritesi'ne göre ise kripto varlıklar, temel olarak kriptografi ve dağıtık defter teknolojisine veya benzer bir teknolojiye bağlı olan, herhangi bir merkez bankası ve kamu otoritesi

15 FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 4.

16 Muhammet Şahin, "Kripto Para Yeni Bir Vergi Sığınağı mı? Bilişim Teknolojilerindeki Gelişmeler Temelinde Bir Değerlendirme," Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, S.34 (2019): 174; Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 18.

17 Şahin Çetinkaya, "Kripto Paraların Gelişimi ve Para Piyasalarındaki Yerinin Swot Analizi ile İncelenmesi," Uluslararası Ekonomi ve Siyaset Bilimleri Akademik Araştırmalar Dergisi 2, S.5 (2018): 13.

18 World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, FinTech Note No. 1, 2017, IV.

tarafından ihraç ve garanti edilmeyen, değişim, yatırım veya bir mal ve hizmete erişim amacıyla kullanılabilen bir değeri ifade etmektedir.[19] Bu itibarla kripto varlıklar, kriptografi olarak bilinen yöntem ile güvence altına alınan, iki yönlü olarak paraya dönüştürülebilen ve bir değişim aracı olarak paraya alternatif şekilde eşler arası kullanılabilen bir değere karşılık gelmektedir.[20]

Kripto varlıkların ortaya çıkmasına sebep olan gelişmelerin başında, dijital mahremiyet taraftarı bir grup bilişim uzmanının kurduğu "*Cypherpunk*" hareketi bulunmaktadır.[21] Kendilerini mahremiyeti koruyucu sistemler kurmaya adayarak sosyal ve politik bir değişim gerçekleştirmek isteyen bu kriptografi ve bilgisayar uzmanları, mahremiyetin kriptografik teknikler kullanarak sağlanabileceğini öne sürmüştür.[22] Cypherpunk hareketine göre kırılgan bir yapıya sahip olan mahremiyet, ona değer vermeyen merkezi yapıların elinde kolayca kaybolabileceğinden, bilginin daha önce devletin silahı olan kriptografinin araç olarak kullanılması suretiyle korunması gerekmektedir.[23] Kriptografiyi ön plana çıkaran bu gruba, Wikileaks'in kurucusu Julian Assange, Bittorent'in kurucusu Bram Cohen, Bit Gold'un ve akıllı sözleşme kavramının mucidi Nick Szabo, Zcash'in kurucusu Zooko Wilcox-O'Hearn gibi önemli isimler dahil bulunmaktadır. Ayrıca 2009 yılında[24] "*Bitcoin: Eşler Arası Elektronik Ödeme Sistemi (Bitcoin: A Peer to Peer*

---

19 Europe Banking Authority, Report with Advice for the European Commission on Crypto-Assets, 2019, 10-11.

20 Kripto varlıklar hakkında yapılan diğer tanımlar için bknz: European Parliament, Cryptocurrencies and Blockchain, 2018, 23; Greeshma K V., "Crypto Currencies and Cybercrime," International Journal of Engineering Research & Technology (IJERT) 3, S.30 (2015): 1; Selman Musab Çeker, "Kripto Paralar ve Ekonomik Etkileri," (Bitirme Tezi, Yıldız Teknik Üniversitesi, 2018), 2; Erdal Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," (Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2018), 12; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 5; Sherena Sheng Huang, "Crypto Assets Regulation in the UK: An Assessment of the Regulatory Effectiveness and Consistency," Journal of Financial Regulation and Compliance 29, S.3 (2021): 338.

21 World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, 4; Sesha Kethineni and Ying Cao, "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity," International Criminal Justice Review, 30, S.3 (2020): 337. Bu noktada Cypherpunk ile Crypto-anarchy'nin farklı yaklaşımlar olduğuna dikkat edilmesi gerekmektedir. Cypherpunk, mahremiyeti korumak için kriptografik tekniklerin kullanılmasını savunan bir yaklaşımken, Crypto-anarchy kriptografi dışında hiçbir yasanın özgürlük sağlamayacağını düşünen ve mevcut yasaları tanımayan politik bir görüştür. Ayrıntılı bilgi için bknz: Lana Swartz, "What Was Bitcoin, What Will It be? The Techno-Economic Imaginaries of a New Money Technology," Cultural Studies 32, S.4 (2018): 625-627.

22 Eric Hughes, "A Cypherpunk's Manifesto," Erişim Tarihi: Ekim 25, 2020, https://www.activism.net/cypherpunk/manifesto.html.

23 Swartz, "What Was Bitcoin, What Will It be? The Techno- Economic Imaginaries of a New Money Technology," 626.

24 Cypherpunk hareketi ile oluşturulacak yeni bir sistemde dijital paranın önemli bir yapı taşı olacağı düşünüldüğü için böyle bir paranın üretilmesi için daha önce de çeşitli girişimlerde bulunulmuştur. Bu bakımdan kripto varlık üretme fikri 1985'li tarihlere kadar götürülebilmektedir. Bu girişimler kapsamında "eCash", "CryptoCredits", "b-money" gibi kriptografik varlıklar üretilmiş ancak hiçbiri Bitcoin kadar başarılı olamamıştır. Konuya ilişkin ayrıntılı bilgi için bknz: Sarah Jeong, "The Bitcoin Protocol as Law, and the Politics of a Stateless Currency," Erişim Tarihi: Kasım 18, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 2294124.

Electronic Cash System)" makalesi ile Bitcoin'i tüm dünyaya duyurarak yeni bir dönemin kapısını aralayan Satoshi Nakamoto'nun da bu gruba dahil olduğu ileri sürülmektedir.[25]

Kripto varlıklar, sanal para birimlerinin belki de en kapsamlı gruplarından birini oluşturmaktadır. Bugün, binden fazla kripto varlık türünden bahsedilebilmekte ve bu sayı sürekli artmaya devam etmektedir.[26] Bu kripto varlıklardan bazıları Bitcoin'e ait açık erişimli yazılımdan türetilirken (*altcoin*), bir kısmı ise tamamen farklı yazılımlardan (*metacoin*) türetilmiştir.[27] Mesela Namecoin, Peercoin, Dogecoin, Zerocoin ve Litecoin Bitcoin'den türetilmiş bir yazılıma sahipken, Ethereum[28] ve Ripple gibi kripto varlıklar kendi yazılımlarına sahip bulunmaktadır.[29] Dolayısıyla kripto varlıkların temelini oluşturan yazılımlar farklılık göstermektedir. Bu durum, kripto varlıklar arasında sistemsel ve zamansal farklılıklar doğmasına ve anonimlik seviyesinin değişkenlik göstermesine yol açmaktadır. Bitcoin, birçok kripto varlığın kökeni oluşturması sebebiyle öncü olarak değerlendirilmesi yanında halen en geniş ticaret hacmine ve piyasa değerine sahip bulunan kripto varlık türüdür. Bu nedenle, kripto varlıkların işleyişinin somutlaştırılması ve daha iyi anlaşılabilmesi için Bitcoin üzerinden bir inceleme yapılması yararlı olacaktır.

2. Bitcoin

Bitcoin, herhangi bir kamu kurumuna ya da özel sektöre bağlı olmadan kullanıcıların katılımıyla işlemlerin doğrulanmasını sağlayan, dağıtık bir muhasebe sistemine sahip olan, transfer işlemlerinde mahremiyet ve şeffaflığın esas alındığı bir yazılımdır.[30] Başka bir ifadeyle, kullanıcı mahremiyetini kriptografik şifreleme ile koruyup, işlem kayıtlarını şeffaflaştırarak parasal bir değerin aracısız ve güvenli şekilde transfer edilmesini sağlayan dijital bir finans protokolüdür. Hukuki bir tanım yapılması noktasında ise Adalet Divanı tarafından Bitcoin'e ilişkin

---

25 Swartz, "What Was Bitcoin, What Will It be? The Techno-Economic Imaginaries of a New Money Technology," 628.

26 Kripto varlık türleri hızlı bir şekilde artış göstermektedir. Aylar önce bu sayı yaklaşık 4902 iken, 06.12.2021 tarihi itibariyle 7982'ye çıkmıştır. Kripto varlık türlerinin güncel sayısı, değeri ve market hacmi için bknz: "Today's Cryptocurrency Prices by Market Cap," Coinmarketcap, Erişim Tarihi: Kasım 15, 2021 https://coinmarketcap.com/1/.

27 K V, "Crypto Currencies and Cybercrime," 1; European Parliament, Cryptocurrencies and Blockchain, 29.

28 Ethereum, akıllı sözleşmeler ve tokenlar gibi çeşitli formatların oluşturulabileceği dijital bir platformdur. Ethereum üzerinden türetilen tokenların listesine ulaşmak için bknz: "Token Tracker," Etherscan, Erişim Tarihi: Ocak 27, 2021, https://etherscan.io/tokens.

29 Armknecht, Karame, Mandal, Youssef and Zenner, "Ripple: Overview and Outlook, Trust and Trustworthy Computing," 163; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 6.

30 Murat Volkan Dülger ve Onur Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," in Prof. Dr. Mehmet Emin Artuk'a Armağan, ed. Mahmut Koca (Ankara: Seçkin Yayınevi, 2020), 968.

verilen önemli bir karardan yararlanılması mümkündür. Adalet Divanı Skatteverket v. David Hedqvist kararında, Bitcoin'in çek gibi diğer kıymetli evrakların aksine sadece onu kabul edenler arasında kullanılabilen ve sözleşmeden kaynaklanan doğrudan bir ödeme yöntemi olduğunu ifade etmiştir.[31] Bu ödeme yöntemi vasıtasıyla işleme konu edilen ve elektronik olarak depolanabilen değer birimi ise Bitcoin (BTC) olarak adlandırılmaktadır.[32] Her Bitcoin, kriptografik gizli anahtarlar tarafından oluşturulan bir imza dizisini temsil etmektedir.[33] Dolayısıyla ağda yer alan ve bir imza dizisini temsil eden Bitcoinler esasında birer veriye karşılık gelmektedir. Ancak bu veriler diğer birçok veriden farklı olarak ekonomik bir değer taşımakta, yatırım ve değişim aracı olarak kullanılabilmektedir. Bu bakımdan Bitcoin'in internet ortamında kullanılan nakit paraya benzetilmesi mümkündür.[34] Nitekim Bitcoin'in günlük hayattaki kullanım alanlarına bakıldığında, nakit para gibi işlev gördüğü açıkça anlaşılmaktadır. Bir ödeme aracı olarak bu sistemin kullanıldığı ilk olay, 2010'da "*Laszlo*" lakaplı bir kişinin 10.000 Bitcoin karşılığında iki adet pizza satın almasıyla gerçekleşmiştir.[35] Bu olay sonrasında Bitcoin, mal ve hizmet alımlarında bir ödeme aracı olarak yaygın şekilde kullanılmaya başlanmıştır.[36] Günümüzde gelinen nokta itibariyle, Bitcoin ile bazı üniversitelerin eğitim ücreti ödenebilmekte, Tesla ve Lamborgini'ye ait bazı araba modelleri alınabilmekte, Greenpeace ve Wikileaks gibi kuruluşlara bağış yapılabilmekte, Burger King, KFC ve Subway gibi zincirlerde yemek yenebilmekte ve Microsoft, Amazon, Dell gibi şirketlerden ürün satın alınabilmektedir.[37]

---

31 Judgment of 22 Octotober 2015, Skatteverket v David Hedqvist, C-264/14, EU:C:2015:718, §42. Söz konusu karar, üye devletlerin vergi hukuku bakımından önem taşıyan bir karardır. Adalet Divanı verdiği kararda, Bitcoin alım ve satımına ilişkin faaliyetin Katma değer Vergisi'ne ilişkin 2006/112/EC sayılı Avrupa Birliği Direktifi'nin kapsamına girebileceğini ancak aynı Direktif'in 135/1-e maddesi uyarınca ödemeden muaf tutulabileceğini belirtmiştir.

32 Fatih Kaplanhan, "Kripto Paranın Türk Mevzuatı Açısından Değerlendirilmesi "Bitcoin Örneği," Vergi Sorunları Dergisi, S.353 (2018): 106.

33 Scott D. Hughes, "Cryptocurrency Regulations and Enforcement in the U.S," Western State Law Review 45, S.1 (2017): 4.

34 Mehmet Ata Sarıkatipoğlu; Timur Arif Çapkın ve Fatma Karaalioğlu, "Bitcoin: Bir Sanal Para Birimi Olarak Regülasyonu ve Kara Para Aklanması Bakımından Durumu," GSI Dergisi, (2015): 91.

35 John O. Mcginnis and Kyle Roche, "Bitcoin: Order without Law in the Digital Age," Indiana Law Journal 94, S.4 (2019): 54; Çarkacıoğlu, Kripto-Para Bitcoin, 17; Swartz, "What Was Bitcoin, What Will It be? The Techno-Economic Imaginaries of a New Money Technology," 637; Blundell Wignall, The Bitcoin Question: Currency versus Trust-less Transfer Technology, 7.

36 Avrupa Merkez Bankası'na göre, kripto varlıkların değerindeki hızlı değişimler nedeniyle bir değişim aracı olma işlevinden ziyade yatırım ve spekülasyon aracı olma özelliği daha ön plana çıkmaktadır. İlgili görüş için bknz: European Central Bank, Virtual Currency Schemes - A Further Analysis, 23.

37 Vivian A. Maese; Alan W. Avery; Benjamin A. Naftalis; Stephen P. Wink and Yvette D. Valdez, "Cryptocurrency: A Primer," Banking Law Journal 133, S.8 (2016): 469; Bilgi Teknolojileri ve İletişim Kurumu (BTK), Kripto Para Araştırma Raporu, 2020, 14; Murat Yıldırım, "Blok Zincir Teknolojisi, Kripto Paralar ve Ülkelerin Kripto Paralara Yaklaşımları," Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 10, S.20 (2019): 272; Kethineni and Cao, "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity," 325-326.

Bitcoin'in yaygınlık kazanmasında, dünyanın bir ucundan diğer bir ucuna hızlı, güvenli ve ucuz transfer gerçekleştirilebilmesinin ve kullanıcılara sağlanan mahremiyetin önemli bir yeri bulunmaktadır. Ayrıca merkezi otoritelerin kontrolü altında bulunan paralara duyulan güvensizliğin bir sonucu olarak da bu paraya alternatif nitelikte görülen Bitcoin'e başvurulması söz konusu olabilmektedir.[38] Nakit paraya benzetilmesine karşın Bitcoin, güvenlik, mahremiyet, hız gibi birçok konuda daha avantajlı bir niteliğe sahip bulunmaktadır.[39] Bu avantajlar, Bitcoin'in kullandığı sistemin temel özelliklerinden ileri gelmektedir. Aynı zamanda bu özellikler, Bitcoin'i hem sanal paradan hem de elektronik paradan önemli ölçüde ayırmaktadır. Bu nedenle, söz konusu temel özelliklerin ayrı başlıklar altında genel hatlarıyla incelenmesi gerekmektedir.

a. Kriptografi

Bitcoin sisteminde, transfer işlemlerinin yapılması, yapılan işlemlerin doğrulanması, gizliliğin sağlanması ve hatta Bitcoin arzının gerçekleşmesinde şifreleme teknikleri kullanılmaktadır.[40] Bitcoin transferi gerçekleştirmek isteyen her kişiye biri açık, biri kapalı olmak üzere iki anahtar ve bir adres tahsis edilmektedir. Tahsis edilen adres Bitcoin biriktirilmesine, anahtarlar ise Bitcoin'in işleme tabi tutulmasına hizmet etmektedir.[41] Bu bakımdan Bitcoin adresi banka hesabına, anahtarlar ise banka şifresine veya PIN numarasına benzetilmektedir.[42] Fakat banka hesabı ve şifresinden farklı olarak bunlar hash şifreleme tekniğiyle oluşturulmaktadır. Bitcoin adresi açık anahtardan, açık anahtar ise gizli anahtardan tek yönlü fonksiyon ile türetilmektedir.[43] Fonksiyonun tek yönlü olması işlemin tersi yöne işleyememesi anlamına gelmektedir. Diğer bir ifadeyle, adresten açık anahtara, açık anahtardan ise gizli anahtara ulaşılması mümkün değildir. Anahtarların oluşturulması yanında işlemlerin gizliliği de bu şifreleme teknikleri ile sağlanmaktadır. Açık anahtar ile şifrelenen bir mesaj, sadece açık anahtarla ilişkili olan gizli anahtar ile deşifre edilebilmektedir.[44] Bu nedenle Bitcoin trans-

38 Bu durumun en güzel örneklerinden biri Çin'de yaşanmıştır. Baskıcı rejim nedeniyle 2013-2017 yılı arasında Çin'de, dünyanın geri kalanından daha fazla Bitcoin işlemi gerçekleştirilmiştir. Konuya ilişkin ayrıntılı bilgi için bknz: Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 12-13.

39 Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış," 194.

40 Edward V. Murphy; M. Maureen Murphy and Michael V. Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues (2015), Congressional Research Service Report R43339, 1.

41 Çarkacıoğlu, Kripto-Para Bitcoin, 28; Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 71; Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 64.

42 Michele R. Korver; C. Alden Pelker and Elisabeth Poteat, "Attribution in Cryptocurrency Cases," United States Attorneys' Bulletin 67, S.1 (2019): 234.

43 Çarkacıoğlu, Kripto-Para Bitcoin, 24; Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 64; Blundell Wignall, The Bitcoin Question: Currency versus Trust-less Transfer Technology, 8.

44 Swartz, "What Was Bitcoin, What Will It be? The Techno-Economic Imaginaries of a New Money Technology," 629; Jeong, "The Bitcoin Protocol as Law, and the Politics of a Stateless Currency," 3.

feri yapmak isteyen bir kişinin alıcıdan açık anahtarını temin etmesi, alıcının ise kendisine ulaşan şifreli mesajı gizli anahtarı ile deşifre etmesi gerekmektedir. Bu itibarla, açık anahtarın Bitcoin sisteminde ikili bir işlev gördüğü söylenebilir. Açık anahtar hem Bitcoin adresinin türetilebilmesi için kaynak işlevi görmekte hem de göndericinin kimliğinin doğrulanmasına imkân tanımaktadır.

Anahtarların kriptografi ile oluşturulması ve korunması söz konusu olduğu için hesaptaki Bitcoinler'in başkası tarafından harcanması veya başka bir işleme konu edilmesi, gizli anahtar ele geçirilmediği sürece mümkün değildir. Dolayısıyla gizli anahtar güvenli bir ortamda saklanmalı ve başkalarıyla paylaşılmamalıdır.[45] Aksi taktirde para dolu bir cüzdanın çalınmasına benzer sonuçlar ortaya çıkabilecek ve adreste bulunan Bitcoinler ile istenilen işlemler yapılabilecektir. Gizli anahtar ele geçirilmediği sürece Bitcoinler'in harcanamaması, sistemin güvenliğini sağlama noktasında şifreleme tekniklerinin çok önemli bir rol oynadığını göstermektedir.[46] Bu bakımdan, sistemin dolandırıcılığa ve hırsızlığa karşı güvenilir olduğu ifade edilmektedir.[47] İleri sürülen bu görüşe karşı çıkanlar da bulunmakla beraber yaşanan hırsızlık ve dolandırıcılık olaylarına bakıldığı takdirde, bunların Bitcoin sisteminden ziyade cüzdan ve değişim hizmeti sunan site ve uygulamaları hedef aldığı görülmektedir. Buna rağmen, Bitcoin sisteminin de siber saldırılara maruz kalması mümkündür.[48] Henüz Bitcoin ağına karşı böyle bir saldırının gerçekleştirilmemiş olması, bu ağın mutlak güvenlik sağladığı şeklinde yorumlanmamalıdır.[49]

b. Eşitler Arası (Peer to Peer) Prensibi

Devlet adına paranın kontrol edilmesi için oluşturulan merkezi otoriteler, para ve kur politikalarının yönetilmesinden sorumlu baş aktörler olup yaptıkları iş mahiyeti gereği güven gerektirmektedir.[50] Ancak modern para, bir hukuk ürünü olduğu için manipüle edilebilmekte ve devletler tarafından baskı aracı olarak kullanılabilmektedir.[51] Bu niteliği dolayısıyla merkezi otoriteye bağlı sistemler, krizin bir parçası hatta kaynağı olarak algılanmakta ve kişilerin güven kaybı yaşamasına yol açmaktadır.[52] Bitcoin'in mucidi Nakamoto'ya göre, aracılar vasıtasıyla

45 Henry S. Zaytoun, "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft," North Carolina Law Review 97, S.2 (2019): 406.

46 Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 21; Çeker, "Kripto Paralar ve Ekonomik Etkileri," 2.

47 Eveshnie Reddy and Anthony Minnaar, "Cryptocurrency: A Tool and Target for Cybercrime," Southern African Journal of Criminology 31, S.3 (2018): 72.

48 Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış," 203.

49 Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 38.

50 European Central Bank, Virtual Currency Schemes, 9-10.

51 Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 7.

52 Pauline W.J. van Esterik Plasmeijer and W. Fred van Raaij, "Banking System Trust, Bank Trust, And Bank Loyalty," International Journal of Bank Marketing 35, S.1 (2017): 97; Swartz, "What Was Bitcoin, What Will It be? The Techno-Economic Imaginaries of a New Money Technology," 629.

işlemlerin gerçekleştirilmesini sağlayan mevcut sistemler, güvene dayandığı için bu güven ilişkisinden doğan bazı zafiyetlere sahip bulunmaktadır. Bu sebeple, güven ilişkisine dayanan bir sistemden ziyade kriptografik şifreleme tekniklerine dayanan bir elektronik ödeme sistemi oluşturularak, güvenilir üçüncü bir kişiye ihtiyaç duymadan işlem yapılması sağlanmalıdır.[53] Söz konusu amacı gerçekleştirebilmek için Bitcoin sisteminde işlemlerin yapılmasına aracılık eden merkezi bir yapıdan yararlanılmamıştır. Kişiler ile merkezi otorite arasında bulunan güven ilişkisi yerine kriptografik teknikler koyularak, katılımcıların hem aktör hem de seyirci olarak hareket etmesine imkân sağlayan bir yazılım geliştirilmiştir.[54] Bu sistemde transfer işlemlerinin yapılması, yapılan işlemlerin doğrulanması ve sisteme Bitcoin arz edilmesi gönüllü katılımcılar tarafından gerçekleştirilmektedir.[55] Bu itibarla, Bitcoin'in kullandığı sistem "peer to peer (*eşitler arası*)"[56] prensibine dayanmaktadır. Fakat bu prensip özellikle kullanıcılar açısından olumsuz sonuçlar doğurabilecek niteliktedir. Merkezi bir yapı bulunmadığından, yaşanan olumsuz durumlar karşısında şikâyet ve itiraz yolunun işletilmesi mümkün değildir. Dolayısıyla Bitcoin kullanıcıları, merkezi yapıya sahip bir sistemde yer alan kullanıcılara kıyasla daha savunmasız bir pozisyonda bulunmaktadır.

Merkezi yapıyı kaldırarak kullanıcıları aktör haline getiren eşitler arası prensibinin, paraların yasal bir düzenlemeye sahip olması gerektiği fikrine bir başkaldırı niteliğinde olduğu ileri sürülmektedir.[57] Gerçekten de Bitcoin'in işleyişine bakılırsa, ne sistemi regüle etmek amacıyla konulan kurallar ne de konulan kuralları uygulayabilecek merkezi bir otorite bulunmaktadır. Halbuki her para biriminin arkasında paranın hukuki olarak regüle edilmesi gerektiği fikri yatmaktadır. Bu nedenle Bitcoin başta gelmek üzere kripto varlıklar, para birimlerinin hukuki bir alt yapıya sahip olması gerektiği fikrini kökten değiştirmiştir. Para birimleri hukuk düzenine ait bir ürünken, Bitcoin gibi kripto varlıklar kanunsuz bir düzenin ürünüdür.[58]

c. Anonimlik

Kripto varlıklar bakımından anonimlik, kullanıcıların gerçek kimliklerini açıklamak zorunda kalmadan sisteme girebilmelerini ve işlemlerini gerçekleştirebilmelerini ifade etmektedir. Daha önce de belirtildiği üzere, Bitcoin ile işlem

---

53 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 1, Erişim Tarihi: Kasım 27, 2020 https://bitcoin.org/bitcoin.pdf.

54 Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 1.

55 Dülger ve Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," 966.

56 Peer to peer sisteminin farklı şekillerde kullanımı için bknz: Abramowicz, "Cryptocurrency-Based Law," 404 vd.

57 Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 4; Jeong, "The Bitcoin Protocol as Law, and the Politics of a Stateless Currency," 17.

58 Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 4.

yapmak isteyen herkese banka hesabı gibi işlev gören bir adres tahsis edilmektedir. Tahsis edilen bu adres, banka hesabından farklı olarak hiçbir kişisel bilgi kullanılmadan kriptografik tekniklerle üretilmektedir. Başka bir ifadeyle, Bitcoin adresleri, "1" veya "3" sayısıyla başlayan, sadece harf ve rakamlardan oluşan bir dizi ya da bir QR kodu olup, isim, soy isim ve doğum tarihi gibi hiçbir kişisel bilgi içermemektedir.[59] Bundan dolayı hem sistemdeki kullanıcıların hem de 3. kişilerin, işlemi yapan adresin kime ait olduğunu bilmesi mümkün değildir. Bitcoin adreslerinden gerçek kişilere teknik yollarla ulaşılması da ciddi engellerin ve zorlukların aşılmasını gerektirmektedir. Bu zorluklara rağmen, bir Bitcoin adresinin kime ait olduğu biliniyorsa Blokzincir yapısının sağlamış olduğu şeffaflık nedeniyle bu adresin yapmış olduğu tüm işlem ve transferlerin takip edilmesi olanaklıdır.[60] Hatta bu niteliğinden dolayı Bitcoin'in anonim değil, "*pseudonymity*"[61] özelliğine sahip olduğu ileri sürülmektedir.[62] Bu bakımdan, Bitcoin sisteminin mutlak bir anonimlik sağlaması söz konusu değildir. Buna karşın kullanıcıların alacağı ek önlemlerle bu seviyeyi yükseltmesi imkân dahilindedir. Daha üst bir seviyede anonimlikten yararlanmak isteyen kişilerin, sahip olduğu Bitcoin adresini bir defa kullanması alınabilecek bu önlemlerin başında gelmektedir.

d. Blokzincir Sisteminin Kullanılması

Bitcoin, kullanıcıların anonim kalmasına imkân tanırken yapılan transferlerin aleni bir şekilde takip edilmesini mümkün kılmaktadır. Bu şeffaflığı veri depolama sistemi olarak nitelendirebileceğimiz Blokzincir sistemi ile sağlamak-

---

59 Hughes, "Cryptocurrency Regulations and Enforcement in the U.S," 5; Çarkacıoğlu, Kripto-Para Bitcoin, 12.

60 Steven David Brown, "Cryptocurrency and Criminality: The Bitcoin Opportunity," Police Journal 89, S.4 (2016): 331; Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 18; K V, "Crypto Currencies and Cybercrime," 1; Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 78.

61 Pseudonymity (takma ad), bireylerin kimliklerini açıklamadan başkalarına kendileri hakkında bilgi vermelerini veya işlemi yapanın kendileri olduğunu kanıtlamalarını sağlayan bir yöntemdir. Kullanılan bu takma ad sayesinde kişilerin kimliğine ilişkin bilgilere ulaşılamayacak ancak bu takma ad altında yapılan bütün işlemler bu adı kullanan kişi ile ilişkilendirilebilecektir. Bu nedenle Bitcoin sistemi anonim olmaktan ziyade pseudonymity özelliğine sahip bulunmaktadır. Zira Bitcoin hesabından kişilerin kimliğine ilişkin bir çıkarım yapılması mümkün olmamasına karşın yapılan işlemlerin belli bir hesap ile ilişkilendirilmesi mümkündür. Konu hakkında ayrıntılı bilgi için bknz: Miranda Mowbray, "Implementing Pseudonymity," SCRIPT-ed 3, S.1 (2006).

62 Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," SSRN Electric Journal, (2015): 19; Rustem Magizov; Sergey Kuznetsov; Venera Garipova; Muhamat Gilmanov; Anastasia Kasatova and Aleksey Kuznetsov, Criminal, Problems of Criminal Responsibility for Illegal Circulation of Cryptocurrency, 12th International Conference on Developments in eSystems Engineering, 2019, 997; Murphy, Murphy and Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues, 1; Reddy and Minnaar, "Cryptocurrency: A Tool and Target for Cybercrime," 71; European Parliament, Cryptocurrencies and Blockchain, 33; Ghassan O. Karame; Elli Androulaki and Srdjan Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," Cryptology ePrint Archive IACR Report No.248, 2012, 2; European Central Bank, Virtual Currency Schemes - A Further Analysis, 22.

tadır.[63] Blokzincir sistemi, verilerin depolandığı açık ve dağıtık bir kayıt defterine benzemektedir. Ancak bir kayıt defterinden farklı olarak, veriler sayfalar halinde değil bloklar halinde depolanmaktadır.[64] Diğer bir deyişle, bu sistemde veriler her on dakika içerisinde gerçekleştirilen işlemlerin blok şeklinde şifrelenmesi ile saklanmaktadır.[65] Bu blokların birbirine bağlanması ile de zincir yapısı ortaya çıkmaktadır. Ortaya çıkan bu zincir yapısı aleni olduğu için işlemlerin blok blok geçmişe giderek incelenmesine olanak tanımaktadır.[66]

Zincir yapısının şeffaflık dışında sağladığı diğer bir avantaj ise bölünemezlik ve değiştirilemezliktir.[67] Bir zincirde yer alan halkaların değiştirilmesi için nasıl tüm zincirin parçalanması gerekiyorsa, Blokzincir sisteminde yer alan işlemlerin değiştirilebilmesi veya silinebilmesi için de ondan sonraki tüm blokların geriye dönük bir şekilde değiştirilmesi gerekmektedir. Bu nedenle, bir işlemin ve blokun Blokzincir'e eklendikten sonra geri alınması ve değiştirilmesi mümkün değildir. Hata sonucu yapılan bir işlemin olumsuz sonuçlarını önlemek adına başvurulabilecek tek yol, alıcının yeni bir işlem yaparak geri alınmak istenen işlem tutarını göndericiye geri göndermesidir.[68] Fakat alıcının böyle bir işlem yapmasını zorunlu kılan bir düzenleme olmadığı gibi her işlemin olumsuz sonucu telafi edilebilir nitelikte değildir. Mesela gönderilen bir mal karşılığı ödenecek Bitcoin tutarının hiç ödenmediği veya eksik ödendiği bir durumda, satıcı açısından ortaya çıkan olumsuz sonuçların ortadan kaldırılması mümkün olmayabilecektir. Dolayısıyla Bitcoin kullanıcılarının sadece güvenilen ve bilinen kişilerle işlemlerini gerçekleştirmesi gerekmektedir.

Bitcoin sisteminin Blokzincir şeklinde aleni ve şeffaf bir yapı kullanması, sistemsel bir gereksinim olarak karşımıza çıkmaktadır. Şöyle ki, yapılan işlemlerin doğrulanması ve blok olarak zincire eklenmesi merkezi bir yapı olmadığından katılımcılar tarafından gerçekleştirilmektedir. Bu doğrulama işlemi, düğüm (*node*) olarak adlandırılan uçlar tarafından konsensüs mekanizması ile yapılmaktadır. Düğümlerin çoğunluğu tarafından onaylanmayan bir transfer işlemi, zincir yapıya katılmamaktadır. Bu bakımdan Blokzincir sisteminde sadece doğrulanmış işlemler yer almaktadır. Düğümler tarafından bu doğrulama işleminin yapılabilmesi için veri depolama sisteminin aleni olması ve işlemleri denetlemeye imkân vermesi gerekmektedir. Nitekim Bitcoin'in kurucusu Nakamoto da ele aldığı makalesinde,

63 European Parliament, Cryptocurrencies and Blockchain, 15.

64 Betül Üzer, "Sanal Para Birimleri," (Uzmanlık Yeterlik Tezi, Türkiye Cumhuriyet Merkez Bankası Ödeme Sistemleri Genel Müdürlüğü, 2017), 24.

65 Mesut Serdar Çekin, "Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var mı?," İstanbul Hukuk Mecmuası 77, S.1 (2019): 321-322.

66 Aleni olmayan özel nitelikte Blokzincir ağları da bulunmaktadır. Konuya ilişkin ayrıntılı bilgi için bknz: Mutluoğlu, "Kripto Para Birimleri ve Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu," 25-26.

67 Çeker, "Kripto Paralar ve Ekonomik Etkileri," 2.

68 Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 21.

güven duyulan merkezi bir yapı bulunmadığından işlemlerin doğrulanabilmesi için bunların bilinmesi gerektiğine dikkat çekmiştir.[69] Nakamoto'ya göre ancak bu sayede işlemlerin doğrulanabilmesi ve çifte harcamanın[70] önüne geçilmesi olanaklı hale gelmektedir.[71] Bitcoin'in öncü olarak değerlendirilmesine yol açan ve özel bir yerde konumlandırılmasını sağlayan temel neden de Blokzincir sisteminin kullanılmış olmasıdır. Zira elektronik paralara özgü sistemsel sorunlar Blokzincir sistemi kullanılarak büyük oranda aşılmıştır. Bu noktada önemle belirtmek gerekir ki, Blokzincir sadece ödeme sistemleri bakımından değil, kamu ve özel sektör için de büyük bir potansiyele sahip bulunmaktadır.[72] Sağlık, bankacılık, finans, yönetim, iletişim gibi alanlarda da Blokzincir sisteminden faydalanılabilmektedir.[73] Kısacası, veri değişimi olan her alanda Blockzincir sisteminin kullanılması mümkündür. Bu nedenle, söz konusu sistem para transferlerinin yapılması ile sınırlı görülmemelidir.

3. Bitcoin Sisteminde Yer Alan Temel Aktörler

a. Bitcoin Kullanıcıları

Bitcoin sisteminde kullanıcılar, kendilerine tahsis edilen anahtarları mal ve hizmet satın almak, kişisel ödemelerini gerçekleştirmek veya yatırım yapmak amacıyla kullanan kişilerdir.[74] Herhangi özel bir şart gerekmeden Bitcoin'e ait açık erişimli yazılımın bilgisayar ve telefon gibi sistemlere yüklenmesi ile kullanıcı olunabilmektedir. Ayrıca özel olarak geliştirilen bazı uygulamalar ile Bitcoin yazılımı indirilmeden dahi kullanıcı olarak işlem yapmak mümkündür.[75] Ancak kullanıcı olarak işlem yapılabilmesi için Bitcoin satın alınması, ödeme olarak Bitcoin kabul edilmesi ve madencilik yapılması gibi çeşitli yöntemlerle Bitcoin'in elde edilmesi gerekmektedir.

---

69 Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2.

70 Aynı Bitcoin'in birden fazla harcanmasına çifte harcama denmektedir. Yapılan bir işlemin onaylanması zaman aldığı için çifte harcama yapılma olasılığı bulunmaktadır. Bunu önlemek adına zaman damgası ve madencilik sistemi kullanılarak Bitcoin'lerin kopyalanması ve birden fazla kullanımı engellenmek istenmiştir. Çifte harcamanın ne olduğu, nasıl önlenebildiği ve Bitcoin'in halen çifte harcama tehlikesi altında olup olmadığına ilişkin ayrıntılı bilgi için bknz: Karame, Androulaki and Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," 1 vd.; Çarkacıoğlu, Kripto-Para Bitcoin, 40; Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış," 201.

71 Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2; European Parliament, Cryptocurrencies and Blockchain, 18.

72 Blockzincir teknolojisinin, akıllı sözleşmeler ve merkezi olmayan (özerk) kuruluşlar aracılığıyla yönetilen bir dünya ve Lex Cryptographia olarak adlandırılan yeni bir hukuk düzenine yol açabileceği görüşü için bknz: Wright and Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," 44 vd.

73 Zaytoun, "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft," 397. Blokzincir sisteminin kripto varlıklar dışındaki çeşitli uygulamaları için bknz: World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, 21 vd.

74 European Central Bank, Virtual Currency Schemes - A Further Analysis, 8.

75 FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 6.

b. Cüzdan Sağlayıcıları

Cüzdan sağlayıcıları, kripto varlık kullanıcılarına Bitcoinler'i tutmak, saklamak ve kullanmak için tahsis edilen anahtarları depolayan veya üreten programlardır.[76] Mevcut olan anahtarların bu cüzdanlarda saklanması mümkün olduğu gibi, anahtarı olmayan bir kişiye uygulama vasıtasıyla anahtar tahsis edilmesi de olanaklıdır. Bu kapsamda; online cüzdan (*hotstorage*), offline cüzdan (*coldstorage*), mobil cüzdan (*mobile wallet*), masaüstü cüzdanı (*desktop wallet*), kâğıt cüzdan (*paper wallet*) gibi çeşitli cüzdan uygulamalarından faydalanılabilmektedir.[77] Bu noktada şunu ifade etmek gerekir ki, Bitcoin kullanımı için cüzdan uygulamalarından yararlanılması zorunluluk teşkil etmemektedir.[78] Cüzdanlar, Bitcoinler'in saklanması ve harcanması noktasında kullanıcılara yardımcı olarak işlemlerin daha kolay bir şekilde gerçekleştirilmesine hizmet etmektedir.[79] Dolayısıyla cüzdanlar, teknik alt yapıya sahip olmayan veya daha pratik şekilde işlemlerini gerçekleştirmek isteyen kullanıcılar tarafından tercih edilmektedir. Ancak bu durumda, kullanıcıların anahtarların güvenliği konusunda cüzdan sağlayıcılarına güven duyması önem arz etmektedir. Zira cüzdan sağlayıcılarının, teknik sorunlar ve sistemin hacklenmesi gibi sebeplerle anahtarları kaybetme tehlikesi bulunmaktadır. Ayrıca kötü amaçlı programlanan bir yazılım tarafından oluşturulan anahtarların, kullanıcıların iradesi dışında kullanılması da mümkündür.[80] Bu nedenle, kullanıcılara birbiriyle bağlı olmayan birden fazla kurumsal cüzdandan veya offline cüzdan uygulamalarından yararlanması önerilmektedir.[81]

c. Değişim Hizmeti Sunanlar

Değişim hizmeti sunanlar, belli bir komisyon karşılığında Bitcoin gibi kripto varlıkların satın alınmasına, gerçek para birimlerine veya sanal para birimlerine dönüştürülmesine imkân sağlayan platformlardır.[82] Bu platformların birçoğu, ihraççıya veya 3. bir kişiye bağlı finansal olmayan şirketler tarafından işletilmekte-

---

76 Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 23; European Central Bank, Virtual Currency Schemes - A Further Analysis, 8; Çetinkaya, "Kripto Paraların Gelişimi ve Para Piyasalarındaki Yerinin Swot Analizi ile İncelenmesi," 16; Korver, Pelker and Poteat, "Attribution in Cryptocurrency Cases," 234; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 8.

77 U.S Department of Justice, Cryptocurrency Enforcement Framework, 3.

78 European Central Bank, Virtual Currency Schemes - A Further Analysis, 8.

79 Güçlütürk, "Türk Hukukunda Kripto Varlıkların Para ve Elektronik Para Niteliğinin İncelenmesi," 389; Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 72; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 8.

80 European Central Bank, Virtual Currency Schemes - A Further Analysis, 13.

81 Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 73. Offline cüzdan uygulamalarıyla birlikte biyometrik kimlik doğrulama teknolojisinin kullanılmasının güvenlik sorunlarını sona erdireceğini düşünen görüş için bknz: David Orme, "Is Biometrics the Answer to Crypto-Currency Crime?," Biometric Technology Today, S.2 (2019): 9.

82 Zaytoun, "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft," 406; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 7.

dir.[83] Türkiye'de hizmet gören değişim platformlarına BTCTurk, Paribu, Binance gibi örnekler verilmesi mümkündür. Bu platformlardan bazılarının kullanıcılara cüzdan sağlaması da söz konusu olabilmektedir. Dolayısıyla değişim platformları, borsa ve döviz bürosu gibi işlev görmesinin yanında cüzdan sağlayıcı olarak da hizmet verebilmektedir. Bu itibarla, Bitcoin aktörleri birbirinden bağımsız olarak düşünülmemelidir.

Değişim hizmeti sunan aktörler bakımından vurgulanması gereken en önemli husus, kullanıcılara hizmet verebilmek için kişisel bilgi talep edebilmesidir. Bu platformlara kayıt esnasında isim, soy isim, doğum yılı hatta kimlik numarası gibi bilgilerin girilmesi gerekebilmektedir. Bu bakımdan değişim hizmeti sunan aktörler, Bitcoin'in sağladığı anonimliğin yumuşatılmasında ve kullanıcıların takip edilmesinde önemli bir rol oynamaktadır. Bu önem dolayısıyla Amerika, Japonya, İsrail, Fransa gibi bazı ülkeler, yapmış olduğu düzenlemelerle para borsalarında olduğu gibi kripto varlık değişim platformlarında da kişisel bilgi talebini zorunlu tutmaktadır. Anonimliğin aşılmasında önemli bir araç olabilmesine karşın, değişim hizmeti sunan platformlar bazı güvenlik zafiyetlerine sahip bulunmaktadır. Bitcoin'lerin çalınması, anahtarların başkaları tarafından ele geçirilmesi, cüzdanların hacklenmesi gibi birçok eylem bu aktörleri hedef alarak gerçekleştirilmektedir.[84] Genellikle merkezi bir yapının bulunduğu bu platformlarda kullanıcılar dolandırıcılık, hırsızlık ve iflastan kaynaklanan maddi kayıplara maruz kalabilmektedir. Konuya ilişkin en bilinen örneklerden birini "MT GOX" platformu oluşturmaktadır. En büyük değişim platformlarından biri olan MT GOX, 2014 yılında hacklenmiş ve 473 milyon dolar değerindeki Bitcoin'in çalınmasından sonra iflas etmiştir.[85] Verilen bu örnekten de anlaşılacağı üzere, değişim platformlarının regüle edilmemesi ve denetlenmemesi hem kullanıcıların kendisi hem de kamu düzeni bakımından büyük bir risk oluşturmaktadır.[86]

d. Ticari Platformlar

Ticari platformlar, Bitcoin alıcıları ile satıcılarını bir araya getirerek teklif yoluyla anlaşma yapılmasına olanak sağlamaktadır. Merkezi bir yapıya sahip bulunmayan bu platformlar, geliştirilen yazılım aracılığıyla alıcıya ve satıcıya uygun bir ortam oluşturma amacı taşımaktadır.[87] Bu niteliği itibariyle söz konusu platformlar adeta Bitcoin pazarı gibi işlev görmektedir. Ancak değişim hizmeti sunan aktörlerden farklı olarak bu platformların kendisi Bitcoin alımı ve satımı ile uğraşmamaktadır.[88]

---

83 European Central Bank, Virtual Currency Schemes - A Further Analysis, 8.

84 Zaytoun, "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft," 407.

85 Murphy, Murphy and Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues, 8; European Central Bank, Virtual Currency Schemes - A Further Analysis, 21.

86 U.S Department of Justice, Cryptocurrency Enforcement Framework, 15.

87 European Parliament, Cryptocurrencies and Blockchain, 27.

88 European Central Bank, Virtual Currency Schemes - A Further Analysis, 8.

e. Madenciler (Miners)

Bitcoin sisteminde merkezi bir yapı bulunmadığından işlemlerin doğrulanması katılımcılar tarafından gerçekleştirilmektedir. Katılımcıların yapılan işlemleri doğrulayabilmesi ise konsensüs mekanizmasına bağlı bulunmaktadır.[89] Bir işlem ancak katılımcıların çoğu tarafından onaylanması halinde geçerlilik kazanabilmektedir. İşte Bitcoin sisteminde işlemlerin doğrulanmasını bu konsensus mekanizması ile gerçekleştiren kişilere madenci (*miners*) denmektedir.[90] Yeryüzünden değerli bir mineral çıkarmak amacıyla zaman ve enerji harcayan insanlara benzediği için bu kişilere madenci denmektedir.[91] Madenciler yeni yapılan işlemleri bir araya toplayarak ve zamansal olarak sıralayarak blok haline getirmekte, her yeni blokun daha önceki blokların şifresel çıkarımını içermesini özel bir algoritmayla (SHA-256) sağlamaya çalışmaktadır.[92] Bu bakımdan madencilik, bir işlem kayıt hizmeti olarak da görülebilir.[93] Fakat Blokzincir de yer alan veriler her geçen gün artarak büyük miktarlara ulaştığından, daha önceki blokların şifresel çıkarımının yapılması zorlaşmakta ve daha çok vakit almaktadır.[94] Ayrıca böyle bir işlemin yapılması çok büyük miktarda bilgisayar gücü de gerektirmektedir. Bu nedenle, özellikle elektriğin ucuz olduğu yerlerde madencilik faaliyetine rastlanmaktadır. Gene aynı nedenle bireysel çalışmak yerine "*mining pools*" olarak bilinen madenci havuzlarına katılarak kollektif bir çalışma yapılması tercih edilmektedir.

Blokzincire yeni bir blokun eklenmesi için madencinin işlemleri sadece doğrulaması yeterli olmamakta ayrıca bu işlemlerin kendisi tarafından doğrulandığının da ağa kanıtlanması gerekmektedir. Bu sisteme iş kanıtı "*Proof of Work (PoW)*" denmektedir.[95] Proof of work sisteminde bir madencinin iş kanıtı su-

---

89 Simon Dyson; William J. Buchanan and Liam Bell, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime," The Journal of the British Blockchain Association 1, S.2 (2018): 1; Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 27; European Parliament, Cryptocurrencies and Blockchain, 18; Çekin, "Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain," 321-322.

90 Madencilik sisteminin, yasal olmayan mekanizmaların geleneksel bir hükümet işlevini nasıl tamamlayabileceğine ve hatta yerini alabileceğine iyi bir örnek teşkil ettiğini düşünen görüş için bknz: Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 30.

91 European Central Bank, Virtual Currency Schemes - A Further Analysis, 7.

92 Üzer, "Sanal Para Birimleri," 32.

93 Üzer, "Sanal Para Birimleri," 32.

94 European Parliament, Cryptocurrencies and Blockchain, 18; Blundell Wignall, The Bitcoin Question: Currency versus Trust-less Transfer Technology, 8; Isaac Kfir, "Cryptocurrencies, National Security, Crime and Terrorism," Comparative Strategy 39, S.2 (2020): 116.

95 Bu sistemin alternatifi olan Proof of Stake (PoS) sisteminde ise iş kanıtı değil kullanıcılar tarafından sahip olunan birim sayısı göz önünde bulundurulmaktadır. Böylece PoW sisteminde söz konusu olan manipülasyon tehlikesi ve yüksek enerji tüketimi sorunu aşılmaya çalışılmıştır. Bu sistemleri hibrit şekilde kullanan Peercoin, Blackcoin gibi kripto varlık türleri de olduğunu belirtmek gerekir. Konuya ilişkin ayrıntılı bilgi için bknz: European Central Bank, Virtual Currency Schemes - A Further Analysis, 10.

nabilmesi için bazı şifresel bulmacaları çözmesi zorunluluk arz etmektedir. Bu kapsamda, daha önceden belirlenmiş bir formatı[96] sağlamak için her türlü girdi deneme yanılma yoluyla test edilmekte ve bu formata uygun şifresel bir özet bulunmaya çalışılmaktadır.[97] Bulunacak özet, daha fazla girdinin daha kısa sürede denenmesine bağlı olduğundan her madencinin ödülü alabilme şansı mevcuttur. İstenilen bu formatı sağlayan ilk madenci, yeni bir bloku zincire eklemeye hak kazanmakta ve belli bir miktar Bitcoin ödemesi ile ödüllendirilmektedir. Madencilere teşvik amaçlı verilen bu ödüller aynı zamanda sistemin kendi içindeki Bitcoin arzını da sağlamaktadır.[98] Bu durum, itibari paralar ile kripto varlıklar arasında önemli bir fark yaratmaktadır. Para birimlerinde arz merkez bankaları aracılığıyla gerçekleştirilirken, Bitcoin sisteminde bu sistemin katılımcısı olan madenciler tarafından gerçekleştirilmektedir.[99] Tasarlanan yazılım gereği madenciler aracılığıyla arz edilen Bitcoin miktarı her 210.000 blokta yarılanarak azalmaktadır.[100] Başlangıçta 50 Bitcoin ödül olarak verilirken, günümüz itibariyle bu miktar 6,25 Bitcoin'e kadar düşmüş bulunmaktadır. Dolayısıyla belli bir süre sonra Bitcoin sistemine yapılacak olan arzın bitme noktasına gelecek kadar azalması söz konusu olacaktır. Netice olarak, madenciler ancak belli aşamalardan geçerek doğrulama işlemlerini tamamlayabilmektedir. Bu aşamaları kısaca; kullanıcılar tarafından yapılan işlemlerin madenciler tarafından bir blok içinde toplanması, her madencinin işlemleri topladığı bir blok için işlem kanıtı bulmaya çalışması, bulunan işlem kanıtının çoğunluk tarafından onaylanabilmesi için tüm düğümlere yayımlanması, eğer işlemler geçerli ise ve çifte harcama söz konusu değilse blokun düğümler tarafından onaylanarak zincire eklenmesi şeklinde sıralayabiliriz. Doğrulama işleminin tamamlanması belli bir süre aldığı için farklı içeriklere sahip blokların onaylanması ve zincirin çatallaşması mümkündür.[101] Bu halde çoğunluk kararını, en büyük iş kanıtını içeren en uzun zincir temsil etmektedir.[102]

Madenciler tarafından yapılan doğrulama ve onaylama işlemleri sonucunda yaklaşık 10 dakikada bir zincire yeni bir blok eklenmekte, böylece sistemin kendi

96 Söz konusu format algoritmanın kendisi tarafından tanımlanmakta ve bir madencinin çözümü bulması için gereken süreyi dikkate alarak her 2016 blokta yenilenmektedir.

97 Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 19; Jeong, "The Bitcoin Protocol as Law, and the Politics of a Stateless Currency," 4; Karame, Androulaki and Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," 2; World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, 6.

98 Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 4.

99 Ayşe Esra Pirinççi, "Yeni Dünya Düzeninde Sanal Para Bitcoin'in Değerlendirilmesi," Uluslararası Ekonomi Siyaset İnsan ve Toplum Bilimleri Dergisi 1, S.1 (2018): 47-48.

100 Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 19.

101 Doğrulama süresinin yeterince kısa olmamasını, farklı kripto varlıkların ortaya çıkmasında temel bir neden olarak değerlendiren görüş için bknz: Kounelis, "Secure and Trusted Mobile Commerce System Based on Virtual Currencies," 21.

102 Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 3.

içinde devamı ve güvenliği sağlanmaktadır.[103] Madenciler olmadan sistem doğru bir şekilde işleyemeyeceğinden çifte harcama ve sahte Bitcoin oluşturulması gibi sorunlarla karşılaşılabilecektir.[104] Bu bakımdan Bitcoin'in belki de en önemli aktörlerinden birini madenciler oluşturmaktadır. Ancak Bitcoin'e güvenlik bakımından getirilen eleştirilerin başında da madencilik faaliyetinin ve konsensus mekanizmasının yer aldığı belirtilmelidir. Konsensus mekanizması nedeniyle kötü niyetli madencilerin sistemi belli hallerde manipüle etmesi mümkündür.[105] Genel kabul gören görüş, sistemin manipüle edilebilmesi için kötü niyetli madencilerin bilgisayar gücünün çoğunluğuna sahip olması gerektiğini vurgulayarak sistemin güvenli olduğunu ileri sürmektedir.[106] Bu görüşe göre Blokzincire, ancak sistemdeki tüm bilgisayar gücünün %51'ini oluşturan madenciler bir araya gelerek (*%51 attack*) sahte işlemlerden oluşan bloklar ekleyebilecektir. Sistemin %51'den daha az bilgisayar gücü ile manipüle edileceğini belirten görüşler de bulunmakla beraber konuya ilişkin şu çıkarımın yapılması mümkündür: Bitcoin sistemi mutlak güvenlik sözü verilebilecek bir sistem olmayıp belli hallerde manipüle edilebilecek bir niteliği haizdir.

II. KRİPTO VARLIKLARIN HUKUKİ NİTELİĞİ

A. GENEL OLARAK

Ceza hukuku bakımından doğru bir değerlendirme yapılabilmesi için öncelikle kripto varlıkların hukuki niteliği üzerinde durulması gerekmektedir. Eğer kripto varlıklar elektronik para, emtia veya menkul kıymet gibi kategorilere dahil edilebilirse, bu kategorilere ilişkin düzenlemelerin söz konusu varlıklar hakkında da uygulanması mümkün olabilecektir. Konuyu bir örnekle açıklayacak olursak; kripto varlıkların emtia olduğu kabul edilirse üzerinde sahiplik iddiası kurulabilecek bir mal söz konusu olacağından hem mülkiyet hakkının sonuçlarından yararlanılabilecek hem de konusu mal olan, mala zarar verme, hırsızlık, yağma gibi suçların işlenmesi olanaklı hale gelecektir.[107] Dolayısıyla hukuki niteliğine ilişkin yapılacak yorum, kripto varlıklara uygulanacak kuralları da belirleyecektir. Bununla birlikte, kripto varlıklar bizzat devlet eliyle desteklenmesi halinde önemli ölçüde yaygınlaşma potansiyeline de sa-

---

103 Madenciler tarafından her 10 dakikada bir yapılan işlemler bir araya getirilerek bir blok içinde sıralanmaktadır. Alıcı ve satıcının yaptıkları transferlerin daha erken işleme alınması için işlem ücreti teklif etmesi mümkün olduğu gibi madencinin de böyle bir ücret talep etmesi mümkündür. İşlem ücretleri genellikle toplam işlem değerinin %0,1 altındadır. İşlem ücretinin alınması noktasında ise girdi değeri ile çıkış değeri arasındaki fark göz önünde tutulmaktadır. Konuya ilişkin ayrıntılı bilgi için bknz: Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 26.

104 European Central Bank, Virtual Currency Schemes - A Further Analysis, 7.

105 Christopher P. Buttigiegh, "Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State," Law and Financial Markets Review 13, S.4 (2019): 212.

106 Şahin, "Kripto Para Yeni Bir Vergi Sığınağı mı? Bilişim Teknolojilerindeki Gelişmeler Temelinde Bir Değerlendirme," 173; Mcginnis and Roche, "Bitcoin: Order without Law in the Digital Age," 27; Jeong, "The Bitcoin Protocol as Law, and the Politics of a Stateless Currency," 5.

107 Kaplanhan, "Kripto Paranın Türk Mevzuatı Açısından Değerlendirilmesi "Bitcoin Örneği," 113.

hip bulunmaktadır. Dünya geneline baktığımız zaman; Singapur, İsveç, Çin, Meksika ve Rusya gibi bazı ülkelerin merkez bankaları aracılığıyla kripto varlık üretmek için faaliyete başladığı görülmektedir.[108] Türkiye de böyle bir faaliyette bulunmayı planlayan ülkeler arasında yer almaktadır. Cumhurbaşkanlığı Hükümet Sistemi'nin ilk kalkınma planı olan 11. Kalkınma Planı'nda, Blokzincir tabanlı dijital merkez bankası parası çıkartılması kararı bulunmaktadır.[109] Bu nedenle, kripto varlıkların hukuki bir kimliğe ihtiyacı daha belirgin bir şekilde ortaya çıkmaktadır. Buna rağmen kripto varlıkların hukuki niteliğine ilişkin genel geçer bir yorum yapılması şu an için mümkün gözükmemektedir. Kripto varlıklara karşı olan tutum, dünya genelinde önemli ölçüde farklılık göstermektedir. Japonya, Singapur, Almanya, Amerika, İngiltere gibi bazı ülkeler bu varlıkları desteklerken; Rusya, Çin gibi bazı ülkeler önemli kısıtlamalar getirmekte, Bolivya, Lübnan, Bangladeş gibi bazı ülkeler ise yasaklayıcı bir tutum sergilemektedir.[110] Diğer birçok ülke ise bu konudaki tarafsızlığını korumaktadır. Ayrıca bu varlıkları destekleyen ülkeler arasında da konu oldukça tartışmalıdır. Bu kapsamda kripto varlıkları, para birimi olarak kabul edenler bulunduğu gibi; emtia, sanal emtia, mal, menkul kıymet[111] ve hatta bir ürün (*production*)[112] olarak değerlendiren görüşler de bulunmaktadır. Aynı ülkede dahi kripto varlıkların hangi niteliğe sahip olduğu tartışmalıdır. Konunun en karmaşık şekilde ele alındığı ülkelerden biri olan Amerika'da, yürütülen faaliyetle ilişkili olarak farklı nitelendirmeler yapılmaktadır. Kripto varlıklar, Menkul Kıymetler Borsa Komisyonu'na (SEC) göre menkul kıymet,[113] mali istihbarat birimi FİNCEN'e göre para, Gelirler İdaresi'ne (IRS) göre

---

108 Rustem Magizov; Sergey Kuznetsov; Venera Garipova; Muhamat Gilmanov; Anastasia Kasatova and Aleksey Kuznetsov, Problems of Legal Regulation of Cryptocurrencies, 12th International Conference on Developments in eSystems Engineering, 2019, 958; Craig Calcaterra; Wulf A. Kaal and Vadhindran Rao, "Stable Cryptocurrencies," Washington University Journal of Law & Policy 61, S.1 (2020): 205-206.

109 11. Kalkınma Planı'nın onaylandığına dair karar 23.07.2019 tarihli 30840 sayılı Resmî Gazete'de yayımlanmıştır.

110 Magizov, Kuznetsov, Garipova, Gilmanov, Kasatova and Kuznetsov, Criminal, Problems of Criminal Responsibility for Illegal Circulation of Cryptocurrency, 997; Kfir, "Cryptocurrencies, National Security, Crime and Terrorism," 114; Svitlana Kostenko; Vitalii Strilchuk; Roman Chernysh and Anna Buchynska, "The Threats to National Security of Ukraine and Poland Inassisting to the Development of the Crypto-Asset Market: Legal Aspect," Management Theory and Studies for Rural Business and Infrastructure Development 43, S.2 (2021): 231.

111 Eric Engle, "Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting," Journal of High Technology Law 16, S.2 (2016): 374.

112 Magizov, Kuznetsov, Garipova, Gilmanov, Kasatova and Kuznetsov, Problems of Legal Regulation of Cryptocurrencies, 956.

113 SEC'in Kurumsal Finans Bölüm Direktörü William Hinman tarafından yapılan bir konuşmada, Bitcoin ve Ethereum'un artık menkul kıymet olarak değerlendirilemeyeceği yönünde bir görüş ileri sürülmüştür. Bu açıklamaya dayanılarak oluşturulan "Hinman Test" Amerikan doktrininde büyük tartışmalara yol açmıştır. İlgili açıklama metni için bknz: William Hinman, "Digital Asset Transactions: When Howey Met Gary (Plastic)," (SEC transcribed speech, 14 Haziran 2018), Erişim Tarihi: Ocak 20, 2021, https://www.sec.gov/news/speech/speech-hinman-061418. Kripto varlıkların menkul kıymet olarak değerlendirilemeyeceği yönünde ileri sürülen diğer bir görüş için bknz: Irina Cvetkova, "The Legal Definition of Cryto Assest," BRICS Law Journal 5, S.2 (2018): 136.

mal (*property*), Vadeli Emtia İşlemleri Komisyonu'na[114] (CFTC) göre ise emtia niteliğindedir.[115] Söz konusu kuruluşlar arasındaki görüş ayrılığına ek olarak mahkeme kararları arasında da içtihat birliği bulunmamaktadır. Kripto varlıkların para birimi, menkul kıymet ve fon olduğunu ifade eden mahkeme kararları bulunduğu gibi emtia olarak değerlendirildiği kararlar da mevcuttur.[116] Bu nedenle, kripto varlıkların hangi niteliğe sahip olduğundan ziyade hangi niteliğe sahip olmadığını belirlemek şu an için daha doğru bir yaklaşım olarak görünmektedir. Daha önce de belirtildiği gibi, kripto varlıkların dahil olduğu sanal para birimleri "*itibari para*" olarak değerlendirilmemektedir. Bu bakımdan, itibari paraya ilişkin mevzuatın kripto varlıklar için uygulanamayacağı açıktır.

Kripto varlıkların niteliğine ilişkin hukuki değerlendirmenin, öncelikle elektronik para üzerinden yapılması gerekmektedir. Avrupa Birliği 2009/110 sayılı Elektronik Para Kuruluşlarının Kurulması, Faaliyetlerinin Sürdürülmesi Denetimi Direktifi konuya ilişkin en önemli hukuki metinlerden biri olup; birçok ülke mevzuatında yer alan düzenlemelere kaynak teşkil etmektedir.[117] Bu Direktif'in 2. maddesinde elektronik para; ödeme işlemlerinin yerine getirilmesi amacıyla fon karşılığı çıkarılan, ihraççısı dışındaki gerçek veya tüzel kişiler tarafından da kabul edilen ve elektronik olarak onu ihraç edene karşı bir talepte temsil edilmek üzere elektronik veya manyetik olarak depolanan parasal değer şeklinde tanımlanmıştır. Avrupa Merkez Bankası ise elektronik para kavramını geniş bir şekilde yorumlamış, bu kavramın ihraççı dışındaki kuruluşlara ödeme yapmak için kullanılabilen ve teknik bir cihazda elektronik olarak depolanabilen parasal bir değeri ifade ettiği belirtilmiştir.[118] Elektronik paranın tanımlanması noktasında

---

114 Kripto varlıklar üzerinde en güçlü yasal otoriteye CFTC'nin sahip olduğunu düşünen görüş için bknz: Tyler C. Lee, "Decrypting Crypto: Issues Plaguing Today's Hottest Regulatory Nightmare," New York University Journal of Law and Business 16, S.2 (2020): 565.

115 FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019, 50-51; Gabrielle Chasin Velkes, "International Anti-Money Laundering Regulation of Virtual Currencies and Assets," New York University Journal of International Law and Politics 52, S.3 (2020): 895; Türkiye Bilişim Vakfı (TBV), Kripto Para ve ICO Raporu, 2020, 22; Lee, "Decrypting Crypto: Issues Plaguing Today's Hottest Regulatory Nightmare," 561; Kfir, "Cryptocurrencies, National Security, Crime and Terrorism," 120; Kethineni and Cao, "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity," 331.

116 Konuya ilişkin önemli bazı kararlar için bknz: CFTC v. My Big Coin Pay, Inc., 2018; CTFC v. McDonnell, 2018; Audet v. Fraser, 2017; U.S v. Coinbase, Inc., 2017; Balestra v. ATBCoin LLC, 2019; Hodges v. Harrison, 2019; SEC v. Blokvest LLC, 2018; SEC v. Plexcorps, 2017; U.S v. Anthony Murgio, 2017; State of Florida v. Michell Abner Espinoza, 2016; Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, 2013. Konu hakkında ayrıntılı bilgi için bknz: Hughes, "Cryptocurrency Regulations and Enforcement in the U.S," 8; Pavlo Bartusiak, "'Judicial Finding' of the Legal Nature of Cryptocurrency," Ehrlich's Journal 2, S.1 (2018): 32.

117 AB, Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC (2009), OJ L 267/7.

118 European Central Bank, "Electronic Money," Erişim Tarihi: Şubat 7, 2021, https://www.ecb.europa.Eu/stats/money_credit_banking/electronic_money/html/index.en.html.

karşılaştırmalı hukuktan da yararlanılması mümkündür. İngiltere Elektronik Para Yönetmeliği'nin (*Electronic Money Regulations*) 2. maddesine göre elektronik para, elektronik ve manyetik olarak depolanabilen parasal bir değerdir. Ancak bu parasal değerin ödeme yapmak amacıyla fon karşılığı çıkarılmış olması, ihraççı dışındaki kişiler tarafından da kabul edilmesi ve kanuni düzenlemelerden hariç tutulmamış olması gerekmektedir.

Elektronik paraya ilişkin uluslararası ve karşılaştırmalı hukukta yapılan tanımlar göz önüne alındığında, temel olarak üç noktaya parmak basıldığı söylenebilir. Bunlar; parasal değerin temsili olması, bu temsilin elektronik veya manyetik olarak depolanabilmesi ve ihraççı dışındaki diğer kişiler tarafından da kabul edilmesidir. Bu bakımdan elektronik paralar, itibari paranın elektronik ortamdaki bir temsilinden ibaret olup genel kabul gören ödeme yöntemleri arasında yer almaktadır.[119] Başka bir deyişle, elektronik paranın bir karşılığı, temsil ettiği somut bir değer bulunmaktadır. Elektronik paranın transfer edilmesi, ilgili miktarın adeta banka kasasından başka bir banka kasasına aktarılması gibi sonuç doğurmaktadır. Kripto varlıkların ise temsil ettiği somut bir değer bulunmadığı gibi, ihraççısı dışındaki diğer kişiler tarafından da kabul görmesi söz konusu değildir. Bu nedenle, elektronik paraya ilişkin yasal düzenlemelerin kripto varlıklar için uygulama alanı bulması mümkün değildir. Ancak değeri ülke paraları, altın gibi çeşitli değerlere endekslenebilen ve "*stable coin*" olarak adlandırılan kripto varlıklar da bulunmaktadır.[120] Bazı yazarlara göre, somut olayın şartlarına göre stable coinlerin elektronik para olarak kabul edilmesi mümkündür.[121] Henüz bunların da elektronik para kapsamında değerlendirilebileceğine ilişkin yasal bir dayanak bulunmasa da ileride bunlar hakkında da kapsamlı düzenlemeler yapılması kaçınılmaz olacaktır. Zira kripto varlıkların arz ve talebe bağlı olarak dalgalanmalar yaşaması, paradan beklenen stabil yapıyı sağlamamaktadır.[122] Stable coinlerin ise belli değerlere sabitlenmesi daha stabil ve öngörülebilir bir durum oluşturmaktadır.[123] Nitekim yapılan bazı çalışmalarda da stable coinlerin niteliğine göre elektronik para kavramı içinde değerlendirilebileceği ifade edilmektedir.[124]

---

119 BTK, Kripto Para Araştırma Raporu, 4; Pirinççi, "Yeni Dünya Düzeninde Sanal Para Bitcoin'in Değerlendirilmesi," 46.

120 Dirk Bullmann; Jonas Klemm and Andrea Pinna, In Search for Stability in Crypto-Assets: Are Stablecoins the Solution?, ECB Occasional Paper Series No: 230, 2019, 9. Stable coin kavramı yerine fiat tokens, managed coins gibi kavramların da kullanıldığına ilişkin bknz: Tobias Adrian and Tommaso Mancini-Griffoli, The Rise of Dijital Money, IMF Fintech Notes, 2019, 4.

121 Güçlütürk, "Türk Hukukunda Kripto Varlıkların Para ve Elektronik Para Niteliğinin İncelenmesi," 400.

122 Şahin, "Kripto Para Yeni Bir Vergi Sığınağı mı? Bilişim Teknolojilerindeki Gelişmeler Temelinde Bir Değerlendirme," 175.

123 Adrian and Mancini-Griffoli, The Rise of Dijital Money, 5.

124 Her Majesty's Treasury, UK Regulatory Approach to Cryptoassets and Stablecoins: Consultation and Call for Evidence, 2021, 5-6; The European Consumer Organisation (BEUC), Crypto Assets-BEUC Response to the Commission's Consultation, 2020, 8.

Emtia ve menkul kıymet görüşü bakımından bu kadar kesin bir yorum yapılamayacak olmakla birlikte, kripto varlıkların hukuki niteliğinin belirlenmesinde belli kuruluşların yapmış olduğu sınıflandırmalardan yararlanılması mümkündür. Bu kapsamda, İngiltere Finansal Yürütme Kurulu (*Financial Conduct Authority*) exchange tokens (*değişim tokenları*), utility tokens (*hizmet tokenları*), security tokens (*menkul kıymet tokenları*), e-money tokens şeklinde bir ayrım yaparken; Avrupa Bankacılık Otoritesi investment tokens (*yatırım tokenları*), exchange/payment tokens ve utility tokens şeklinde bir ayrım yapmakta, Avrupa Tüketiciler Birliği Bürosu ise bu ayrıma hibrit tokenlar şeklinde yeni bir grup daha eklemektedir.[125] Yapılan sınıflandırmalar, kripto varlıkların sahip olduğu erişim özelliklerini, sistemsel özelliklerini ve ekonomik fonksiyonlarını göz önüne alarak farklı değerlendirmeler yapılmasına imkan tanımaktadır. Kanaatimizce sınıflandırma yöntemi, sistemsel ve zamansal farklılıklara sahip olan kripto varlıkları tek bir grup altında ele almaması nedeniyle daha isabetli bir yaklaşımdır.[126] Bu yaklaşım neticesinde, niteliğine ve özelliklerine göre her varlığa farklı hukuki kimlikler vermek mümkün olacaktır. Ancak kripto varlıklar her geçen gün büyüdüğünden, farklı kategoriler oluşturulması ve sınıflandırmalar yapılması da yeterli bir çözüm değildir. Yapılan sınıflandırmalar her kripto varlığı kapsayamayacağı gibi, bir kripto varlığın birden fazla grup altında konumlandırılması da mümkün olabilecektir.[127] Bu nedenle günümüzde, hibrit tokenlar gibi farklı ayrımların yer aldığı daha kompleks ve kapsamlı çalışmalar yapılmaya başlanmıştır.[128] Kripto varlıklar nasıl sınıflandırılacak olursa olsun, yapılan düzenlemelerin uygulanma kabiliyetini kaybetmemesi için esnek bir şekilde ele alınması gerekmektedir.

B. TÜRK MEVZUATI BAKIMINDAN

Kripto varlıklara ilişkin uzun süredir tarafsızlığını koruyan Türkiye, 2021 yılında konuya ilişkin ilk düzenlemeyi yaparak bu tarafsızlığı bozmuştur. 16 Nisan 2021 tarihinde 31456 sayılı Resmî Gazete'de "*Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik*" yayımlanmıştır. Söz konusu yönetmelikte kripto varlıklar; "*dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak*

125 Financial Conduct Authority, Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3, 2019; Europe Banking Authority, Report with Advice for the European Commission on Crypto-Assets; BEUC, Crypto Assets-BEUC Response to the Commission's Consultation.

126 Apolline Blandin; Ann Sofie Cloots; Hatim Hussain; Michel Rauchs; Rasheed Saleuddin; Jason Grant Allen; Bryan Zhang and Katherine Cloud, Global Cryptoasset Regulatory Landscape Study, Cambridge Center for Alternative Finance, 2019, 12.

127 Blandin, Cloots, Hussain, Rauchs, Saleuddin, Allen, Zhang and Cloud, Global Cryptoasset Regulatory Landscape Study, 18.

128 Yapılan bu çalışmalara, Arap Birleşik Emirlikleri Menkul Kıymet ve Emtia Otoritesi'nin hazırlamış olduğu taslak çalışma örnek olarak verilebilir: Securities and Commodities Authority, The Chairman of the Authority's Board of Directors' Decision No. (23/ Chairman) of 2020 Concerning Crypto Assets Activities Regulation, 2020, Erişim Tarihi: Eylül 12, 2021, https://www.sca.gov.ae/Content/Userfiles/Assets/Documents /80041 51b.pdf.

sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıklar" olarak tanımlamıştır. Yapılan bu tanımla kripto varlıkların hangi niteliğe sahip olmadığı açıkça belirlenmiştir. Esasında yönetmelikte böyle bir düzenleme olmasaydı dahi mevcut hükümlerden hareketle aynı sonuçlara ulaşılabilirdi. Şöyle ki; Türk Parasının Kıymetinin Korunması Hakkında Kanun kapsamına girebilecek değerler kambiyo, nukut, esham, tahvilat, kıymetli madenler, kıymetli taşlarla bunlardan mamul veya bunları muhtevi her nevi eşya ve kıymet, ticari senet ve tediyeyi temine yarayan her türlü vasıta ve vesika olarak sayılmıştır.[129] Bu bakımda, Türk mevzuatına göre kripto varlıkların para olarak değerlendirilmesi mümkün olmayacaktır.[130] Bununla birlikte 2009/110 sayılı Direktif'e paralel şekilde düzenlenen 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun'un 3. maddesine göre elektronik para; belli bir fon karşılığı kabul edilen, elektronik olarak saklanan, ödeme işlemlerini gerçekleştirmek için kullanılan ve ihraç edenler dışındaki kişiler tarafından da kabul edilen parasal değeri ifade etmektedir. Bu itibarla, fon karşılığı çıkarılmayan ve ihraç eden dışındaki kişilerce kabul edilmeyen[131] kripto varlıkların Türk mevzuatına göre elektronik para olarak kabulü de mümkün görünmemektedir. Nitekim Bankacılık Düzenleme ve Denetleme Kurulu da 2013 tarihli bir basın açıklamasında: "*Herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen Bitcoin, mevcut yapısı ve işleyişi itibarıyla Kanun kapsamında elektronik para*

---

129 Kanunun 1. maddesi: *"Kambiyo, nukut, esham ve tahvilat alım ve satımının ve bunlar ile kıymetli madenler ve kıymetli taşlarla bunlardan mamul veya bunları muhtevi her nevi eşya ve kıymetlerin ve ticari senetlerle tediyeyi temine yarıyan her türlü vasıta ve vesikaların memleketten ihracı veya memlekete ithalinin tanzim ve tahdidine ve Türk parasının kıymetinin korunması zımnında kararlar ittihazına Cumhurbaşkanı salahiyetlidir."* şeklindedir. Cumhurbaşkanlığı'nın bu kapsamda yayımlamış olduğu düzenleme Türk Parası'nın Kıymetinin Korunması Hakkında 32 sayılı Karardır. Bu karar ile Türk parasının yabancı paralar karşısındaki değerinin belirlenmesine, döviz ve dövizi temsil eden belgelere (menkul değerler ve diğer sermaye piyasası araçları dahil) ilişkin tüm işlemler ile dövizlerin tasarruf ve idaresine, Türk parası ve Türk parasını temsil eden belgelerin (menkul değerler ve diğer sermaye piyasası araçları dahil) ithal ve ihracına, kıymetli maden, taş ve eşyalara ilişkin işlemlere, ihracata, ithalata, özelliği olan ihracat ve ithalata, görünmeyen işlemlere ve sermaye hareketlerine ilişkin kambiyo işlemlerine ait düzenleyici ve sınırlayıcı esaslar tayin edilmiştir.

130 Bu bakımdan kripto varlıklar, Türk Ceza Kanunu'nun 197. maddesinde düzenlenen parada sahtecilik suçuna konu olamayacaktır. Başka bir ifadeyle, eğer birisi kripto varlık birimini sahte olarak taklit eder veya çoğaltırsa parada sahtecilik suçundan dolayı sorumlu tutulamayacaktır. Ancak gelecekte, kripto varlıkların daha geniş bir kitle tarafından kabul edilerek istikrarlı bir yapıya sahip olması halinde para birimi olarak değerlendirilmesinin mümkün olduğu ileri sürülmektedir. İlgili görüş için bknz: Hamdi Furkan Günay ve Veli Kargı, "Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi," Journal of Life Economics 5, S.3 (2018): 69.

131 Aksi yönde görüş için bknz: Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış," 207; Dülger ve Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," 974.

olarak değerlendirilmemekte, bu nedenle de söz konusu Kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir." şeklindeki gerekçeyle Bitcoin'in 6493 sayılı kanun kapsamına girmeyeceğini açıkça vurgulamıştır.[132]

Kripto varlıkların menkul değer sayılabilmesi için 6362 sayılı Sermaye Piyasası Kanunu'nun 3. maddesine göre, belirli payları temsil etmesi ve kamu ya da özel sektör kuruluşlarının piyasadan borç alabilmek için kullandıkları hazine bonosu, gelir ortaklığı senetleri, devlet iç borçlanma senetleri, özel kesim tahvil ve bonoları gibi borçlanma araçlarından olması gerekmektedir. Halbuki Bitcoin gibi kripto varlıklar ne belirli payları temsil etmekte ne de kanunun aradığı anlamda borçlanma aracı olarak kullanılabilmektedir. Bu nedenle kripto varlıkların Türk mevzuatına göre menkul kıymet olarak kabul edilmesi de olanaklı değildir.[133] Emtia kavramı bakımından ise kripto varlıkların kendinden bir değere sahip bulunmaması, tamamen arz ve talebe göre değerlenmesi nedeniyle olumsuz bir yorum yapılmaktadır.[134] Kısacası, kripto varlıkların Türk hukukuna göre elektronik para, menkul kıymet ve emtia olarak sınıflandırılması zaten mümkün değildi. Dolayısıyla, ilgili düzenlemeyle mevcut hükümler kapsamında yapılan yorumlar tasdik edilmiş, yeni bir niteleme yapılmamıştır. Yönetmelikte yapılan düzenlemeler, karşılaştırmalı hukukta olduğu gibi farklı görüşlerin ileri sürülmesine ve içtihat birliğinin bozulmasına kısmen de olsa engel olabilecektir. Ancak bu düzenlemeler, konuya ilişkin soru işaretlerini yok edebilecek ve mevcut boşluğu doldurabilecek nitelikte olmayıp; aksine yeni problemler doğurabilecek niteliktedir. Zira Yönetmelik'te, kripto varlıkların ödemelerde kullanılmasını yasaklayan bir düzenlemeye yer verilmiştir. Söz konusu Yönetmeliğin çıkarılmasına dayanak olan hüküm göz önüne alındığında, MASAK'ın görüşlerinin belirleyici olduğu görülmektedir. Bundan dolayı özellikle suç gelirlerinin aklanmasına ilişkin risk nedeniyle kripto varlıkların ödemede kullanılmasının yasaklandığı izlenimi doğmaktadır. Halbuki alınan bu önlem, riski ne sona erdirebilecek ne de azaltabilecek niteliktedir. Bununla birlikte diğer birçok ülkede, piyasa değeri ve işlem hacmi nedeniyle kripto varlıkların vergilendirilmesine ve farklı alanlarda kullanılmasına yönelik çeşitli çalışmalar yürütülmektedir.[135] Bu nedenle, kripto

---

132 İlgili basın açıklaması için bknz: https://www.bddk.org.tr/ContentBddk/dokuman/duyuru_0512_01.pdf, E.T: 09.11.2020-14.18.

133 Dülger ve Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," 976. Nitekim Türkiye Sermaye Piyasası Kurulu, Sanal Paralara Dayalı İşlemler Hakkında 785 numaralı Genel Mektup'ta Sermaye Piyasası Kanunu'nda yer alan türev araçlara dayanak teşkil edebilecek unsurlar içinde sanal paraların bulunmadığını açıkça belirtmiştir. İlgili mektup için bknz: Sanal paralara ve kripto varlıklara Sermaye Piyasası Kanunu'nda yer verilmesi gerektiğini ileri süren görüş için bknz: Türkiye Bilişim Vakfı, Kripto Para ve ICO Raporu, 33.

134 Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 54; Günay ve Kargı, "Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi," 71.

135 Vergilendirme konusunda da ülkelerin izledikleri yol farklılık göstermektedir. Kripto varlıkları vergilendirme bakımından Kanada ve Endonezya emtia, İsrail sermaye kazancı, Amerika, Avusturalya ve İsviçre gibi ülkeler ise mal (property) kabul etmektedir.

varlıkların devletler için sağladığı avantajları göz önünde bulunduran ve konuyu hukukun diğer alanları bakımından da mercek altına alan daha detaylı bir çalışma yapılmalıdır.

III. KRİPTO VARLIKLAR VE CEZA HUKUKU İLİŞKİSİ

A. GENEL OLARAK

Kripto varlıkların vergilendirilmesine ilişkin bazı çalışma ve faaliyetlere başlanmış olmasına rağmen ceza hukuku alanında konuyu kapsamlı şekilde ele alan bir düzenleme henüz yapılmamıştır. Bu durum, yasal boşlukların ortaya çıkmasına ve suç işlemek isteyen kişilerin aktif olarak kripto varlıklara yönelmesine sebep olmaktadır. 2019 yılında yapılan bir çalışmada, Bitcoin işlemlerinin yarısına yakınının yasadışı faaliyetlerle ilişkili olduğu saptanmıştır.[136] Kripto varlıkların suçla olan bu çarpıcı ilişkisi, büyük oranda sistemsel avantajlardan kaynaklanmaktadır. Merkezi bir otoritenin kontrol ve denetiminin söz konusu olmaması, konuya ilişkin kapsamlı bir regülasyon bulunmaması ve işlemi gerçekleştirenlerin anonim kalabilmesi gibi faktörler, çeşitli suçların işlenmesi noktasında kripto varlıkları elverişli bir araç haline dönüştürmektedir. Suç işlemek için elverişli bir araç olması yanında, kripto varlıkların ulusal güvenliği de tehdit ettiği düşünülmektedir.[137] Gerçekten de kripto varlıklar; hukuki bir alt yapıya sahip bulunmadığından ekonomik ve mali politikalardan bağışık olup, kişilerin vergi kaçırması için önemli imkanlar sağlamaktadır. Bu niteliğinden ötürü kripto varlıkların vergi cennetlerinin karakteristik özelliklerine sahip olduğu belirtilmektedir.[138] Buna ek olarak, kripto varlıkların nükleer fırlatma kodları ve terörist saldırıları gibi devlet nezdinde tehlikeli addedilecek mesajları şifrelemek için de kullanılabileceği ileri sürülmektedir.[139]

Kripto varlıklar, doğrudan suça konu edilebileceği gibi suç işlenmesinde veya suç faillerinin kimliğinin gizlenmesinde bir araç olarak da kullanılabilmektedir. Bu varlıklar ile hırsızlık, dolandırıcılık, uyuşturucu ve uyarıcı madde ticareti, silah ticareti, çocuk pornografisi, suçtan kaynaklanan malvarlığı değerlerinin aklanması, vergi kaçakçılığı, terörizmin finansmanı gibi birçok suç işlenebilmek-

136 Sean Foley; Jonathan R. Karlsen and Talis J. Putninš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?," The Review of Financial Studies 32, S.5 (2019): 1826.

137 Engle, "Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting," 352: Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 2; Kfir, "Cryptocurrencies, National Security, Crime and Terrorism," 114; Kostenko, Strilchuk, Chernysh and Buchynska, "The Threats to National Security of Ukraine and Poland Inassisting to the Development of the Crypto-Asset Market: Legal Aspect," 232.

138 Omri Marian, "Are Cryptocurrencies 'Super' Tax Havens?," Michigan Law Review First Impressions 112, S.38 (2013): 42.

139 Engle, "Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting," 347.

tedir.[140] Kripto varlıklar sanal ortamda nakit para işlevi gördüğünden, para ile suçun kesiştiği her alanda kullanılabilmektedir. Başka bir ifadeyle, kripto varlıklar kolayca gerçek paraya dönüştürülebildiği için belli suçların işlenmesinde veya gerekli suç araçlarının elde edilmesinde finansman aracı olarak da kullanılabilmektedir.[141] Konuya ilişkin güncel bir örnek Amerika'da yaşanmıştır. 2020 yılında Adalet Bakanlığı; El Kaide, DAEŞ gibi örgütlerin terörü finanse etmek için düzenledikleri kampanyalarda kripto varlık talep ettiklerini belirterek terörizmin finansmanı bağlamında şimdiye kadar en yüksek miktar olan 2 milyonun ele geçirildiğini duyurmuştur.[142] Terörizmin finansmanı, hırsızlık, dolandırıcılık, şantaj[143] gibi temel suç tipleri yanında, kripto varlıkların veya bunların kullandığı ağların daha özel nitelikte bazı yasa dışı faaliyetlere de konu olması mümkündür. Bu kapsamda, bir başkasının bilgisayarının zararlı kod ve yazılımlarla madencilik yapmak için kullanılmasını ifade eden "*crypto jacking*" fiili örnek olarak verilebilir.[144] Bunun dışında, sahte uygulamalarla kripto varlıkların çalınması da (*cryptocurrency theft*) söz konusu olabilmektedir. Verilen bu örnekler dışında kripto varlıklar, temel suç fiillerini icra etmek için bir araç olarak kullanılmaktadır. Dolayısıyla şu an için "*kripto varlık suçu*" şeklinde bağımsız bir suç tipinden bahsedilememekte, mevcut suçlar kripto varlıklarla yeni bir işleniş şekli kazanmış bulunmaktadır.[145]

---

140 Engle, "Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting," 344; Foley, Karlsen and Putninš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?," 1799; FATF, Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, 2020, 4. Kripto varlıkların suç işlemek için kullanılmasının en çarpıcı örneklerinden biri Silk Road sitesidir. William Ulbricht tarafından kurulan bu siteden, uyuşturucu ticareti, bilişim suçları, para aklanması gibi farklı suçlardan elde edilen 33,6 milyon dolar değerinde Bitcoin ele geçirilmiştir. Bu sitelere Silk Road dışında Hansa, AlphaBay, Dream Market gibi örneklerin de verilmesi mümkündür. Konuya ilişkin ayrıntılı bilgi için bknz: Matthew Kien and Meng Ly, "Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies," Harvard Journal of Law & Technology 27, S.2 (2014): 603; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 11; U.S Department of Justice, Cryptocurrency Enforcement Framework, 19; Sesha Kethineni; Ying Cao and Cassandra Dodge, "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes," American Journal of Criminal Justice 43, S.2 (2017): 146.

141 Korver, Pelker and Poteat, "Attribution in Cryptocurrency Cases," 237; Çeker, "Kripto Paralar ve Ekonomik Etkileri," 31-32; U.S Department of Justice, Cryptocurrency Enforcement Framework, 5-6.

142 U.S Department of Justice, Cryptocurrency Enforcement Framework, 7; Cipher Trace, Cryptocurrency Crime and Anti Money Laundering Report, 2021, 26.

143 Kripto varlıkların şantaj amacıyla kullanıldığı örnekler için bknz: U.S Department of Justice, Cryptocurrency Enforcement Framework, 8; Bartusiak, "'Judicial Finding' of the Legal Nature of Cryptocurrency," 28.

144 U.S Department of Justice, Cryptocurrency Enforcement Framework, 16; Viktoriia Ivaniuk and Serhiy Banakh, "Cryptocurrency-Related Cybercrimes in Ukraine," OER Eastern Europe Law 66, S.1 (2020): 218-219; Kfir, "Cryptocurrencies, National Security, Crime and Terrorism," 118; Bu tür saldırıların en çok Monero'yu hedef aldığını belirten çalışma için bknz: Aaron Zimba; Zhaoshun Wang; Mwenge Mulenga and Nickson Herbert Odongo, "Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security," Journal of Computer Information Systems 60, S.4 (2020): 306.

145 Dülger ve Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," 978.

Görüldüğü üzere, kripto varlıkların belirsiz doğası suçluların yasadışı faaliyetlerde bulunmasını kolaylaştırmaktadır. Şüphesiz kripto varlıkların suç işlemek için cazibe merkezi haline gelmesinde, kullanıcılara sağlanan "*anonimlik*" hayati bir rol oynamaktadır. Normal şartlarda, sanal ortamda gerçekleşen para hareketlerinin takip edilmesi mümkündür. Üstelik böyle bir takibin yapılması bazı durumlarda yasal bir zorunluluk da oluşturmaktadır.[146] Ancak kripto varlıklar, gizlilik sağlanmak istenen işlemlerde ve dark web gibi platformlarda kullanıcılara bir değişim aracı olarak anonimlik vadetmektedir.[147] Blokzincir'in aleni yapısına kıyasla son zamanlarda daha çok anonimlik sözü veren Dash, Monero,[148] Zcash,[149] Grin gibi "*privacy coin*" olarak da nitelendirilen bazı kripto varlıkların ortaya çıkmasıyla alıcıyı, göndereni ve işleme konu tutarı dahi gizlemek mümkün hale gelmiştir.[150] Blokzincir yapısını kullanan kripto varlıkların kullanıcılarını belli ölçüde deşifre edebilen CipherTrace, Big Data, Titanium gibi analiz programlarının ve Chainanalysis, Elliptic gibi özelleşmiş şirketlerin varlığı nedeniyle mahremiyeti öne çıkaran kripto varlıkların sayısında ve kullanımında bir artış olacağı açıktır.[151]

Kripto varlıklar, sadece ceza hukuku bakımından değil ceza muhakemesi bakımından da özel düzenlemeler yapılmasını gerektirmektedir. Bu varlıkların kullanılması ve suça konu edilebilmesi için bilişim sistemlerinin kullanılması zorunluluk

---

146 Franziska Boehm and Paulina Pesch, "Bitcoin: A First Legal Analysis - With References to German and US-American Law," Conference Paper, 1st Workshop on Bitcoin Research in Assocation with Financial Crypto, 2014, 5.

147 Giannis Tziakouris, "Cryptocurrencies-A Forensic Challenge or Opportunity for Law Enforcement? An Interpol Perspective," IEEE Security and Privacy Magazine 16, S.4 (2018): 92; Brown, "Cryptocurrency and Criminality: The Bitcoin Opportunity," 336; Kethineni, Cao and Dodge, "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes," 142.

148 Suç işlenmesi noktasında öne çıkan Monero, transfer işlemlerinin kökenlerini, miktarlarını ve hedeflerini gizlemek için halka imzaları (ring signature) ve gizli adresleri kullanan bir kripto varlık türüdür. Monero hakkında ayrıntılı bilgi için bknz: Reddy and Minnaar, "Cryptocurrency: A Tool and Target for Cybercrime," 87; Tziakouris, "Cryptocurrencies-A Forensic Challenge or Opportunity for Law Enforcement? An Interpol Perspective," 93; Buttigieg, "Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State," 213.

149 Zcash kullanıcılarının büyük bir kısmının sistemin sunduğu anonimlik avantajından yararlanamadığı hakkında bknz: George Kappos; Haaroon Yousaf; Mary Maller and Sarah Meiklejohn, An Empirical Analysis of Anonymity in Zcash, Proceedings of the 27th USENIX Conference on Security Symposium, 2018, 475.

150 Dyson, Buchanan and Bell, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime," 1; Foley, Karlsen and Putninš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?," 1807; U.S Department of Justice, Cryptocurrency Enforcement Framework, 4.

151 Foley, Karlsen and Putninš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?," 1807; Çekin, "Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain," 332; Murphy, Murphy and Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues, 3; European Parliament, Cryptocurrencies and Blockchain, 53; Zaytoun, "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft," 431; Kfir, "Cryptocurrencies, National Security, Crime and Terrorism," 119; Daniel Dupuis and Kimberly Gleason, "Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic," Journal of Financial Crime 28, S.1 (2021): 65.

arz ettiğinden, bunlarla işlenen suçlar bilişim karakterlidir.[152] Kripto varlıkların sağladığı anonimlik yanında bilişim sistemlerinin sağladığı kolaylıktan da faydalanan suçlular, elinin altındaki tek bir tuş ile dünyanın öbür ucundaki bir olaya müdahale ederek haksız yarar sağlama imkanına sahip bulunmaktadır. Bunun sonucunda kripto varlıkların kullanıldığı suçların soruşturulması ve kovuşturulması da teknik açıdan oldukça zorlaşmaktadır. Merkezî bir yapı bulunmadığı ve yapılan işlemler geri alınamadığı için muhakeme makamlarının ihtiyaç duydukları belge ve bilgileri nasıl elde edeceği, bu varlıklara nasıl el koyacağı da oldukça problemli bir hal almaktadır.[153] Ayrıca yargı makamlarının, tamamen bilişim karakterli olan kripto varlıkların saklanması, çeşitli tedbirlere tabi tutulması noktasında cüzdan gibi uygulamalara ihtiyaç duyması da söz konusu olabilmektedir.[154]

Suçlular hem bilişim sisteminin sunduğu kolaylıktan hem de kripto varlıkların sunduğu anonimlikten faydalanırken, özel hayatın gizliliği, mülkiyet hakkı gibi temel değerler zarar görmekte ve bu durum devlete olan güvenin yitirilmesine sebep olabilmektedir. Bu nedenle, mevcut düzenlemelerin kripto varlıklarla işlenen suçları cezalandırmada yeterli olup olmadığı, yeterli değilse özel bir düzenleme yapılmasına ihtiyaç duyulup duyulmadığı tartışılmalıdır. Kapsam bakımından sınırlı olan bu çalışmada, kripto varlıkların araç olarak kullanılabileceği tüm suç tiplerinin ele alınması mümkün olmadığından konunun sınırlandırılması gerekmektedir. Söz konusu çalışma, kripto varlıklar ile en yaygın işlenen bazı suç tipleriyle sınırlandırılmıştır. FBI İnternet Şikâyet Merkezi'nin yayınlamış olduğu 2020 tarihli rapordan (*Internet Crime Report*), en çok şikâyetin dolandırıcılığa ilişkin fiiller bakımından yapıldığı, uğranılan zararın büyük bir kısmını kripto varlıkların oluşturduğu ve mağdurların nerdeyse yarısının da kripto varlıklarla ilişkili olduğu anlaşılmaktadır.[155] Yapılan başka bir çalışmaya göre, kripto varlıkları en çok hedef alan suçlar arasında hırsızlık ve dolandırıcılık suçu bulunmakta olup, bu suçlar nedeniyle sadece 2020 yılı içinde 1,9 milyar dolar değerinde zarar meydana gelmiştir.[156] Bu veriler ışığında çalışmamızda; hırsızlık, dolandırıcılık ve bu suçları tamamlayıcı nitelikte olan suçtan elde edilen malvarlığı değerlerinin aklanması suçu incelemeye tabi tutulacaktır.[157] Kripto varlıkların Türk ceza hukuku bakımından ele alındığı ilk kararın yağma suçuna ilişkin olması nedeniyle yukarıda sayılan suçlar dışında yağma suçu bakımından da bir inceleme yapılacaktır.

---

152 Dülger ve Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," 979.

153 Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 203-204.

154 Korver, Pelker and Poteat, "Attribution in Cryptocurrency Cases," 256-257.

155 Federal Bureau of Investigation, Internet Crime Report (2020), 19 vd.

156 Cipher Trace, Cryptocurrency Crime and Anti Money Laundering Report, 7.

157 Claire Nolasco Braaten and Michael S. Vaughn, "Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions," Deviant Behavior 42, S.8 (2019): 964. FATF, suçtan elde edilen malvarlığı değerlerinin aklanması ve terörizmin finansmanı suçunun işlendiğine ilişkin göstergelere yer veren 2020 tarihli bir raporunda, en sık işlenen suçlar arasında aklama suçu dışında uyuşturucu ticareti ve dolandırıcılık gibi suçların bulunduğunu belirtmiştir.

B. HIRSIZLIK SUÇU

5237 sayılı Türk Ceza Kanunu'nun (TCK) malvarlığına karşı suçlar başlığı altında düzenlenen hırsızlık suçu, zilyedinin rızası olmadan başkasına ait taşınır bir malın kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alınmasını ifade etmektedir. Suçun oluşabilmesi için "*başkasına ait taşınır bir malın*" zilyedin rızası olmadan alınması gerekmektedir. Başka bir ifadeyle, hırsızlık suçunun konusunu, başkasına ait taşınır bir mal oluşturmaktadır. Ancak mal kavramından anlaşılan ile hukuki anlamda mal/eşya kavramı her zaman örtüşmemektedir. Bu nedenle "*taşınır mal*" kavramının açıklanması ve kripto varlıkların çalınmasının bu kapsama dahil edilip edilemeyeceğinin ayrıca değerlendirilmesi gerekmektedir. Doktrindeki genel yaklaşım, "*mal*" kavramının tanımlanması noktasında medeni hukuktan yararlanılması yönündedir.[158] Medeni hukukta eşya; üzerinde hakimiyet kurulabilen, belli sınırlara sahip, ekonomik değer taşıyan ve insan dışı olan bir kavrama karşılık gelmektedir.[159] Genel kabul gören bu tanıma göre, hukuki anlamda eşyanın sahip olması gereken dört temel unsur bulunmaktadır. Bunlar; maddi bir varlığın bulunması, üzerinde hakimiyet kurulmaya elverişli olması, insan dışı olması ve ekonomik bir değere sahip olmasıdır.[160] Esasında maddi bir varlığın bulunması ile hakimiyet kurulmaya elverişli olma unsuru, birbirini tamamlayan ve biri diğerinin sonucu olarak değerlendirilebilecek unsurlardır. Bir şey üzerinde hakimiyet kurulduğundan bahsedilebilmesi için bunun sınırlandırılmış maddi bir varlığa sahip olması gerektiği açıktır.[161]

Taşınır eşya kavramının tanımı ise eşyanın yerinin fiilen değiştirilip değiştirilememesine göre yapılmaktadır. Özüne zarar vermeksizin bir yerden başka yere taşınabilen eşyalar, taşınır olarak kabul edilmektedir.[162] Böyle bir tanımın, taşınmaz kavramından hareketle menfi bir şekilde yapılması da mümkündür. Yeryüzünde sabit olması nedeniyle özüne zarar vermeden bir yerden başka yere taşınamayan ve kanun uyarınca taşınmaz niteliğine sahip olanlar dışında kalan eşyalar taşınır niteliktedir. Bu bakımdan hırsızlık suçunun konusunu "*alınabilir*" olan taşınır eşyalar

158 Mahmut Koca ve İlhan Üzülmez, Türk Ceza Hukuku Genel Hükümler (Ankara: Adalet Yayınevi, 2020), 605; M. Emin Artuk; Ahmet Gökcen, M. Emin Alşahin ve Kerim Çakır, Ceza Hukuku Özel Hükümler (Ankara: Adalet Yayınevi, 2019), 525; Durmuş Tezcan; Mustafa Ruhan Erdem ve Murat Önok, Teorik ve Pratik Ceza Özel Hukuku (Ankara: Seçkin Yayınevi, 2020), 734.

159 Turhan Esener ve Kudret Güven, Eşya Hukuku (Ankara: Yetkin Yayınevi, 2015), 41; M. Kemal Oğuzman; Özer Seliçi ve Saibe Oktay Özdemir, Eşya Hukuku (İstanbul: Filiz Kitapevi, 2014), 8.

160 Ekonomik bir değere sahip olma unsuru, üzerinde görüş birliği bulunan bir unsur değildir. Bu unsurun aranması gerektiğini düşünen yazarlar için bknz: Oğuzman, Seliçi ve Oktay Özdemir, Eşya Hukuku, 7-8. Ceza hukuku bakımından sadece ekonomik değere sahip olan şeylerin değil manevi bir değer taşıyan şeylerin de mal sayılabileceği görüşü için bknz: Nevzat Toroslu, Ceza Hukuku Özel Kısım (Ankara: Savaş Yayınevi, 2019), 135; Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 612; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 527; Tezcan, Erdem ve Önok, Teorik ve Pratik Ceza Özel Hukuku, 735.

161 Oğuzman, Seliçi ve Oktay Özdemir, Eşya Hukuku, 7.

162 Oğuzman, Seliçi ve Oktay Özdemir, Eşya Hukuku, 10.

oluşturmaktadır.[163] Dolayısıyla sadece fiziki bir varlığa sahip olması nedeniyle üzerinde hakimiyet kurularak fiilen yeri değiştirilebilen mallar hırsızlık suçuna konu olabilecektir.[164] Fakat taşınır malın illaki suçun işlendiği anda bu nitelikte olması gerekmemektedir. Taşınmaz malın çeşitli parçalarının sökülmesinde olduğu gibi, belli hallerde de taşınır malın varlığından bahsedilebilmektedir.[165]

Kripto varlıklar ise fiziki bir varlığı olmaması nedeniyle üzerinde ancak tahsis edilen anahtarlar vasıtasıyla hakimiyet kurulabilen, ekonomik değeri haiz sanal birimlerdir. Yukarıda belirtilen hususlar da dikkate alındığında, fiziki bir varlığı olmaması nedeniyle kripto varlıkların taşınır mal olarak kabulü mümkün görünmemektedir. Nitekim Adalet Divanı da vermiş olduğu bir kararda, kripto varlıkların sadece bir ödeme aracı olduğunu ve taşınır mal olarak kategorize edilemeyeceğini belirtmiştir.[166] Bu itibarla, kripto varlıkların çalınması halinde ortada taşınır bir mal söz konusu olmadığından hırsızlık suçunun oluştuğundan bahsedilemeyecektir. Ancak kripto varlıkların TCK'nın 142/2-e[167] karşısındaki durumunun ayrıca incelenmesi gerekmektedir. TCK'nın 142. maddesinin 2. fıkrasında, hırsızlık suçunun "*bilişim sistemlerinin kullanılması aracılığıyla işlenmesi*" şeklinde nitelikli bir hale yer verilmiştir. Bu nitelikli hal ile kastedilen, bilgileri otomatik olarak işleme tabi tutan manyetik sistemler kullanılarak hırsızlık fiilin icra edilmesidir.[168] Diğer bir deyişle, bu nitelikli halin uygulanabilmesi için taşınır bir malın bilişim sistemleri aracı kılınarak alınması gerekmektedir. Bu nedenle, ekonomik bir değer arz etse bile bir verinin çalınması halinde TCK'nın 142/2-e'nin uygulanması söz konusu olamayacaktır. Yargıtay Ceza Genel Kurulu da tesis etmiş olduğu bir kararda, hırsızlık suçunun konusunu oluşturacak malın yerinden alınıp götürülebilecek nitelikte olmasını ve maddi bir varlığa sahip bulunması gerektiğini vurgulamıştır. Aynı kararda, hırsızlık suçunun söz konusu olabilmesi için verinin taşınır mal niteliğine sahip olması gerektiği ancak 5237 sayılı TCK'nın hiçbir maddesinde verilerin taşınır mal olarak düzenlenmediği dolayısıyla kanunilik ilkesi gereğince cezalandırma yapılamayacağı da belirtilmiştir.[169]

---

163 Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 613; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 527; Tezcan, Erdem ve Önok, Teorik ve Pratik Ceza Özel Hukuku, 740.

164 Toroslu, Ceza Hukuku Özel Kısım, 135; Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 606; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 526; Tezcan, Erdem ve Önok, Teorik ve Pratik Ceza Özel Hukuku, 735.

165 Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 613; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 528; Toroslu, Ceza Hukuku Özel Kısım, 135; Tezcan, Erdem ve Önok, Teorik ve Pratik Ceza Özel Hukuku, 741.

166 Judgment of 22 October 2015, Skatteverket v David Hedqvist, C-264/14, EU:C:2015:718, §24.

167 TCK 142/2-e: *"Bilişim sistemlerinin kullanılması suretiyle, hırsızlık suçunun işlenmesi hâlinde, beş yıldan on yıla kadar hapis cezasına hükmolunur."*.

168 Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 649; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 551.

169 YCGK, 17.11.2009, E.2009/268, K.2009/11-193.

Verilerin hırsızlık suçuna konu olamayacağına ilişkin yerleşik içtihat, banka hesaplarında yer alan paraların internet bankacılığı hizmetinden yararlanılarak başka bir hesaba aktarıldığı durumlar için yumuşatılmıştır. Daha önceleri böyle bir fiilin icra edildiği hallerde TCK 141/2-e'nin değil, TCK 244/4'ün uygulanması gerektiği düşünülmekteydi.[170] Ancak Yargıtay, 5 yılı aşkın süredir verilerin parayı temsil ettiğini düşünmekte ve icra edilen hırsızlık eylemlerinin paraya yöneldiğini kabul ederek 142/2-e'yi uygulama yoluna gitmektedir.[171] Bu yaklaşım uygulamada istikrar kazanmasına rağmen doktrinde halen tartışılmaktadır. Sadece verilerin yer değiştirdiğinden bahisle TCK 244. maddenin 4. fıkrasının uygulanması gerektiğini savunan görüşler bulunduğu gibi,[172] Yargıtay uygulamasını destekleyen görüşler de mevcuttur.[173]

Kripto varlıklara ilişkin hukuki değerlendirmenin, söz konusu içtihat değişikliği göz önüne alınarak yapılması gerekmektedir. Zira bu içtihatla internet bankacılığı hizmetinden yararlanılarak başka bir hesaba aktarılan ve esas itibariyle veri niteliğinde olan paraların hırsızlık suçuna konu olabileceği kabul edilmiştir. Dolayısıyla kripto varlıkların çalınması halinde de aynı yorumun yapılmasının mümkün olduğu düşünülebilir. Fakat konuyla ilgili kararlar incelendiğinde, verilerin hırsızlık suçuna konu olabileceği düşüncesinden ziyade verilerin temsil ettiği somut bir değerin, paranın, korunması amacı ön plana çıkmaktadır. Daha önce de açıklandığı üzere, kripto varlıkların temsil ettiği değer kendine has ve soyut bir değerdir. Parayı temsil eden verilerin aksine kripto varlıkların temsil ettiği somut bir değer bulunmadığından, yukarıda yapılan değerlendirmelerin bunlar açısından geçerli olduğu

---

170 TCK 244/4: *"Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur."*.

171 Y15. CD, 09.06.2020, E.2020/1236, K.2020/5130 sayılı kararda konuya ilişkin şu açıklamalara yer vermiştir: *"Katılanın hesabından internetten bilgileri kullanılarak 1939 doğumlu ... adına 18800 TL para havalesi yapılmak istendiğinde bankanın katılanı arayıp işlemi onaylayıp onaylamadığını sorduğunda katılanın işlemden haberdar olmadığı anlaşılmış sonrasında yapılan araştırmada katılanın internet bankacılığında açık olan hesaptan 1920 TL ve kredi kartından 5000 TL para çekildiği ve toplamda 6920 TL paranın internet hesabına aktarıldığı anlaşıldığından aktarılan paraları çekmeye gelen kişinin polis gelene kadar oyalamaya çalışıldığı ancak sanığın durumu anlayıp kaçtığı iddia edilen olayda; bankadan parayı çekmeye çalışan kişinin bıraktığı nüfus cüzdanındaki kimlik bilgileri sanığa ait olsa da fotoğrafın sanığa ait olmadığı ve havale yapılan ...'in 1939 doğumlu olduğu anlaşıldığından sahte nüfus cüzdanı ile suça konu parayı çekmeye çalışan kişinin sanık olduğuna dair yeterli delil bulunmadığı gözetilerek sanığın beraati yerine yazılı şekilde mahkumiyetine dair hüküm kurulması, kabule göre de; Sanığın eyleminin sübutu halinde de katılanın hesabından hesaplarına paranın aktarıldığı gözetilerek eyleminin kül halinde tamamlanmış TCK'nın 142/2-e maddesindeki bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması.."*. Aynı yönde diğer bir karar için bknz: Y8.CD, 01.07.2019, E.2019/11457, K.2019/9171.

172 Tezcan, Erdem ve Önok, Teorik ve Pratik Ceza Özel Hukuku, 766.

173 Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi," İÜHFM 71, S.1 (2013): 881; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 551; Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 649; Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 101.

söylenemeyecektir. Nitekim rıza dışı telefon kontör transferinin gerçekleştiği bir olayda Yargıtay, ekonomik bir değere sahip olmasına karşın telefon kontörlerinin çalınmasını hırsızlık suçu kapsamında değil TCK'nın 244/4. maddesi kapsamında değerlendirmiştir.[174] Knight Online oyunundaki karakterin çalındığı diğer bir olayda ise verilerin ekonomik değer taşısa dahi taşınır mal haline gelmeyeceği belirtilerek hırsızlık suçundan hüküm kurulamayacağına karar verilmiştir.[175]

Konuya ilişkin içtihatlardan hareketle genel bir çıkarımda bulunulacak olursa; doğrudan parayı temsil eden veriler bakımından TCK 142/2-e uygulanabilirken, ekonomik bir değere sahip olsa bile somut bir değeri temsil etmeyen veriler bakımından hırsızlığa ilişkin hükümler uygulanamamaktadır. Ancak aksi yönde değerlendirmeler içeren bazı yargı kararlarının da bulunduğunu belirtmek gerekir. Yargıtay, konuya ilişkin önemli bir kararında şu ifadelere yer vermiştir: "*Sanığın eylemi, telefonun kullanılmasını sağlayan, ekonomik bir değer ifade eden ve bilişim sisteminde veri ile temsil edilen kontörleri, bilişim sistemini kullanıp veriyi yer değiştirmek suretiyle kendi telefon hattına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği ve ekonomik bir değeri olan, ancak bir bedel ödemek suretiyle alınabilecek olan kontörleri alarak mal edinmeye yöneliktir. Kaldı ki sanığın mağdurun telefonunda kullandığı kontörleri almak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 Sayılı TCK'nın 142/2-e maddesinde düzenlenmiş bulunan "bilişim sistemleri kullanılmak suretiyle hırsızlık" suçunun gerçekleştiği kabul edilmelidir.*"[176] Her ne kadar söz konusu karar, kripto varlıklar bakımından da uygulanabilir gibi görünse de hem doktrinin hem de Yargıtay'ın konuya ilişkin genel görüşünü yansıtmamaktadır.

Ekonomik bir değer taşıdığı şüphesiz olmakla beraber somut bir değeri temsil etmeyen kripto varlıkların doktrin ve yerleşik kararlar uyarınca TCK'nın 142/2. maddesi kapsamına dahil edilmesi mümkün değildir.[177] Bu halde, bilişim sistemlerinin araç olarak kullanıldığı birçok suç bakımından da uygulama alanı bulan TCK 244/4. madde gündeme gelecektir. Ancak ortaya çıkan bu sonuç, doktrinde haklı olarak eleştirilmektedir. Amaçsal yorum ile kripto varlıkların 142. madde içerisinde değerlendirilebileceğini düşünen bir görüş, bunların sanal alemde para olarak kabul edilmesi nedeniyle iktisadi değere sahip bir malvarlığı değerini oluşturduğunu be-

174 Y3.CD, 30.01.2013, E.2011/26435, K.2013/1955.

175 Y2.CD, 13.01.2020, E.2019/11010, K.2020/568; Y13.CD, 10.10.2017, E.2016/2155, K.2017/10403.

176 YCGK, 25.11.2014, E.2013/13-448, K.2014/524. Aynı yönde diğer bir karar için bknz: Y17.CD, 16.07.2018, E.2015/28682, K.2018/10194.

177 Benzer bir sonuca Alman hukukundaki düzenlemeler bakımından da ulaşılmaktadır. Alman hukukunda da sadece fiziksel varlığı olan taşınır mallar hırsızlık suçuna konu olabilmektedir. Konuya ilişkin ayrıntılı bilgi için bknz: Boehm and Pesch, "Bitcoin: A First Legal Analysis - With References to German and US-American Law," 7.

lirtmektedir.[178] Ayrıca TCK 142/2-e'deki düzenlemenin konusunu verilerin mi yoksa taşınır nitelikteki malların mı oluşturduğu noktasında belirsizlik bulunduğunu düşünen bu görüş, söz konusu nitelikli halin "*bilişim hırsızlığı*" şeklinde bağımsız bir suç olarak düzenlenmesi gerektiğini ifade etmektedir.[179] Doktrinde ileri sürülen diğer bir görüş ise "*taşınır mal*" kavramının aktarılabilir bir mal olarak anlaşılması gerektiğini, bu nedenle başka yere gönderilmesi veya bulunduğu yerden alınması mümkün olan kripto varlıkların da hırsızlık suçuna konu olabileceğini savunmaktadır.[180]

Kanaatimizce, sıradan veri niteliğinde olmayan kripto varlıkların çalınması halinde failin sadece TCK'nın 244/4. maddesi uyarınca cezalandırılması fiilin ağırlığı ile orantılı olmayacaktır. Kripto varlıklar sanal alemde adeta bir para gibi tedavül etmekte, her an her yerde değişim platformları veya bankamatikler aracılığıyla (sadece bazı kripto birimleri için kullanılabilmekte) para birimlerine çevrilerek kolayca maddi bir varlığa kavuşturulabilmektedir. Ayrıca fiziksel bir şeyin çalınması ile kripto varlıkların çalınması benzer hukuki sonuçlar doğurabilmektedir. Fiziki varlığı olan bir şeyin çalınmasıyla nasıl tasarruf yetkisi sona eriyorsa, Bitcoin anahtarının çalınması sonucunda da ilişkili hesap tekrar kullanılamamaktadır.[181] Bu nedenle, kripto varlıklara karşı gerçekleştiren hırsızlık fiillerinin özel olarak düzenlenmesi gerekmektedir. Ancak böyle bir düzenlemeye, bağımsız bir suç kapsamında mı yoksa hırsızlık suçuna ilişkin hükümler altında mı yer verileceği dikkatli bir şekilde değerlendirilmelidir. Kripto varlıkların, içtihat yoluyla taşınır mal kapsamına dahil edilmesi ve hırsızlık hükümleri uyarınca cezalandırılması sakıncalı sonuçlar doğurabilecek niteliktedir. Zira hem yargı kararlarında hem de doktrinde, ekonomik bir değer ifade etse de fiziki bir varlığı olmayan verilerin 142. maddede düzenlenen suça konu olamayacağı kabul edilmektedir. Bu bakımdan, kripto varlıkların çalınması halinde hırsızlık hükümlerinin uygulanabilmesi için yerleşik içtihadın değiştirilmesi gerekmektedir. Fakat bu durum kanunilik ilkesinin ihlali olarak yorumlanabilecektir. Şöyle ki; Avrupa İnsan Hakları Mahkemesi'ne (AİHM) göre kanunilik ilkesinin temelini oluşturan yasal dayanak kavramı, sadece kanunları değil yeterince öngörülebilir ve ulaşılabilir olması şartıyla mahkeme kararlarını, teamül hukuku kurallarını ve kanundan daha alt bir hiyerarşide bulunan yönetmelik gibi hukuki kaynakları da kapsamaktadır.[182] Dolayısıyla kanundaki düzenlemeler kadar

178 Dülger ve Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," 985-986.

179 Dülger ve Özkan, "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi," 987; Durdu, "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku," 101-102.

180 Ersan Şen, "Bitcoin Çalınır mı?," Erişim Tarihi: Ocak 22, 2021, https://www.haber7.com/yazarlar/prof-dr-ersan-sen/1948163-bitcoin-calinir-mi.

181 Zaytoun, "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft," 419.

182 Rohlena v. The Czech Republic, Başvuru No: 59552/08- 27.01.2015; Larionovs Tess v. Latvia, Başvuru No: 45520/04 ve 19363/05- 25.11.2014; Del Rio Prada v. Spain, Başvuru No: 2750/09- 21.10.2013; Jorgic v. Germany, Başvuru No: 74613/01-12.06.2008. Kanunilik ilkesine ilişkin ay-

bu düzenlemelerin mahkeme tarafından nasıl yorumlanıp uygulandığı meselesi de AİHM açısından önem taşımaktadır. Mahkemenin suç kapsamını sanık aleyhine genişletmemesi ve suç unsurlarını esaslı bir biçimde değiştirmemesi gerektiği kabul edilmektedir. Bununla birlikte içtihat değişikliğinin suçun özü ile uyumlu ve öngörülebilir nitelikte olması gerekmektedir.[183] Bu nitelikte olmayan içtihat değişiklikleri, AİHM tarafından kanunilik ilkesine aykırı bulunmaktadır. Kripto varlıkların hırsızlık suçu kapsamına dahil edilmesi, suçun maddi unsurlarından biri olan suç konusunun esaslı bir şekilde değiştirilmesi anlamı taşımaktadır. Üstelik daha önce TCK 244/4 kapsamında cezalandırılması kabul edilen bir kişinin, içtihat değişikliği ile TCK 142 kapsamında cezalandırılması her ne kadar suçun özü ile uyumlu bir yorum olarak değerlendirilebilirse de sanık aleyhinedir. Bu nedenle, kripto varlıkların çalınmasına ilişkin özel bir düzenleme yapılması kanunilik ilkesine daha uygun olacaktır. Ayrıca böyle bir düzenlemeye ekonomik değer taşıyan diğer verilerin de dahil edilmesiyle doktrindeki mevcut tartışmaların önüne geçilmesi mümkün olabilecektir. Yeni bir suç ihdas edilmesi yanında, kripto varlıkların hırsızlık suçu bakımından taşınır mal sayılacağına ilişkin kanuni bir düzenleme yapılması yoluna da başvurulabilecektir.

C. YAĞMA SUÇU

TCK'nın 148. maddesine göre yağma suçu, tehdit ve cebir yoluyla kişinin bir malı teslim etmeye veya malın alınmasına karşı koymamaya mecbur edilmesidir. Bu bakımdan yağma suçunun cebir veya tehditle işlenen hırsızlık suçu olduğu söylenebilir.[184] Kanun metninde sadece "*mal*" ibaresi kullanılmış ise de kanun gerekçesinde bu malın taşınır nitelikteki bir mal olduğu açıkça belirtilmiştir. Nitekim doktrinde de yağma suçunun konusunu taşınır malların oluşturduğu kabul edilmektedir.[185] Bu itibarla, taşınır mala ilişkin yapmış olduğumuz tüm açıklamalar yağma suçu bakımından da geçerlidir. Taşınır mal niteliğine sahip bulunmayan kripto varlıklar yağma suçunun da konusu olamayacaktır. Ancak Yargıtay tarafından tesis edilen bir karar, varılan bu sonuca şüpheyle yaklaşılmasına yol açmaktadır. Söz konusu karar, kripto varlıkların Türk ceza hukuku bakımından ele alındığı ilk kararlar arasında yer almaktadır. Yargıtay 6. CD tesis

rıntılı bilgi için bknz: Zeynep Esra Tarakçıoğlu, "AİHM Kararları Işığında Suçta ve Cezada Kanunilik İlkesi," (Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2020).

183 Konuya ilişkin örnek kararlar için bknz: Case of Kokkinakis v. Greece, Başvuru No: 14307/88- 25.05.1993. Benzer yöndeki diğer kararlar için bknz: Haarde v. Iceland, Başvuru No: 66847/12- 23.11.2017; Schluga v. Austria, Başvuru No: 65665/01, 71879/01 ve 72861/01- 26.09.2002; Case of Larissis and Others v. Greece, Başvuru No: 23372/94- 24.02.1998; S.W. v. United Kingdom, Başvuru No: 20166/92- 22.11.1995; N. v. Switzerland, Başvuru No: 9870/82- 13.10.1983; A.K. v. Switzerland, Başvuru No: 19189/91- 13.10.1993.

184 Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 671.

185 Toroslu, Ceza Hukuku Özel Kısım, 150; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 567; Tezcan, Erdem ve Önok, Teorik ve Pratik Ceza Özel Hukuku, 791; Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 674-675.

etmiş olduğu bir 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 götürdükleri, 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 ve sonrasında ...'la birlikte mağduru serbest bırakan diğer sanıklarla buluştuğu, olayda; Diğer sanıklarla el ve iş birliği içerisinde hareket eden sanık ...'ın, yağma ve hürriyeti tahdit eylemlerine asli fail olarak katıldığı gözetilmeden, kanıtların takdirinde yanılgıya düşülerek, yazılı şekilde, yağma suçundan TCK'nın 39. maddesi uyarınca yardım eden sıfatı ile sorumlu olduğu gerekçesi ile cezasında indirim yapılması ve hürriyeti tahdit suçundan beraatine karar verilmesi nedeniyle bozma kararı verilmiştir.*" ifadelerine yer vermiştir.[186]

Söz konusu kararda, birçok açıdan eksik değerlendirme yapılmıştır. Öncelikle, yağma suçu kapsamında değerlendirilen fiili, mağdurdan zorla bilgisayar ve cep telefonu alınmasının mı yoksa mağdurun hesabından başka bir hesaba Bitcoin transferi yapılmasının mı oluşturduğu belirsiz bırakılmıştır. Telefon ve bilgisayarın zorla alınması yanında Bitcoin işlemlerinde kullanılan şifrelerin zorla alınması ve mağdura ait Bitcoinler'in başka bir hesaba gönderilmesi de yağma suçu bakımından ayrı ayrı değerlendirmesi gereken fiillerdir. Bu kapsamda, Bitcoinler'in yağma suçuna konu olabileceği kanaatine varılırsa tek bir hareketle birden fazla yağma suçunun mu oluştuğu yoksa tek bir suçun mu oluştuğu da izaha muhtaçtır. Bitcoinler'in yağma suçuna konu olamayacağına karar verilirse de başka bir suçun söz konusu olup olamayacağının ayrıca incelenmesi gerekmektedir. Zira mağdura ait gizli anahtarın ele geçirilmesi ve Bitcoinler'in failin kontrol ettiği bir hesaba transfer edilebilmesi için bilişim sistemine girilmesi zorunluluk arz etmektedir. Bu noktada TCK'nın 243. maddesinde düzenlenen "*bilişim sistemine girme*" suçunun geçit suç niteliğinde olup olmadığı da tartışılmalıdır. Dolayısıyla somut olayda varılacak her iki sonuç bakımından da içtima meselesinin ayrıntılı bir şekilde incelenmesi gerekmektedir. Yargıtay böyle bir değerlendirmeden kaçınarak, bugün için değeri on binlerce doları geçen kripto varlıkların çalınmasını cezalandırılabilir bir fiil olarak ele almaya gerek duymamıştır.

[186] Y6.CD, 07.07.2020, E.2020/1158, K.2020/2598.

D. DOLANDIRICILIK SUÇU

Kripto varlıklar çok farklı nitelikteki dolandırıcılık fiillerine konu olabilmektedir. Özellikle saadet zincirleri (*ponzi schemes*), kripto varlıklar kullanılarak icra edilen dolandırıcılık fiillerinin başında gelmektedir.[187] Daha önce de bahsedildiği üzere, 2020 yılı içinde sadece kripto varlıklara ilişkin hırsızlık ve dolandırıcılık fiilleri nedeniyle 1,9 milyar dolar değerinde zarar meydana gelmiştir. Bu miktarın yaklaşık 1,1 milyarı Çin kaynaklı "*Wotoken*" adlı bir saadet zincirinden kaynaklanmakta olup, bu zincirlerin ne kadar ciddi sonuçlar doğurabildiğinin çarpıcı bir örneğini teşkil etmektedir.[188] Konu bakımından önem arz eden diğer bir örnek ise "*Security and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust*" davasına konu olmuştur. Karara konu olan olayda Bitcoin Savings and Trust'ın (BTCST) kurucusu olan Trendon Shavers, yatırım yapanlara günlük faiz ödeyeceği sözü vererek 700,000'den fazla Bitcoin toplamıştır. Mahkeme yapmış olduğu yargılamada, olayda emtia dolandırıcılığı suçunun işlendiği gerekçesiyle mahkûmiyet kararı vermiştir.[189] Benzer başka bir olayda ise altın ile desteklendiği, Mastercard'ın geçtiği her yerde geçerli olduğu ve birçok para birime dönüştürülebildiği iddia edilen "*My Big Coin*" isimli kripto varlıktan 6 milyar dolar değerinde haksız kazanç sağlanmıştır. Gene Linden Doları'nın kullanıldığı Second Life oyununda meydana gelen olumsuz gelişmeler karşısında, Linden Lab açıklama yaparak faiz veya herhangi bir doğrudan yatırım getirisi sunulmasını yasaklamıştır.[190] Bu noktada belirtmek gerekir ki, Bitcoin yazılımının kendisinin de bir saadet zinciri olduğunu ileri süren bazı görüşler bulunmaktadır. Bu görüşe; gerçek paranın Bitcoin'e dönüştürülmesinin kolay olmasına karşın, ancak sisteme Bitcoin alarak giren kişilerin varlığı halinde Bitcoin'in gerçek paraya dönüştürülebilmesi gerekçe olarak gösterilmektedir.[191]

Saadet zincirleri yanında genel olarak oltalama kavramı altında değerlendirilebilecek phishing, vishing, smishing, pharming[192] dolandırıcılık yöntemleriyle de kripto varlıklar haksız bir şekilde ele geçirilebilmektedir. Bu yöntemde, kullanıcıları sahte web sitelerine yönlendirmek için e-posta (*phishing*), mesaj (*smishing*) ve telefon aramaları (*vishing*) kullanılmaktadır. Normal saldırılarından farklı olarak kripto varlıklara ilişkin dolandırıcılıkta amaç, gizli anahtar bilgilerini elde etmeye

---

187 Akıllı sözleşmeler ile saadet zinciri kurulabileceği (smart ponzi schemes) ve Ethereum'da 500'den fazla saadet zinciri işletildiği hakkında bknz: Weili Chen; Zibin Zheng, Edith Ngai, Peilin Zheng and Yuren Zhou, "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum," IEEE Access 7, (2019): 37576.

188 Cipher Trace, Cryptocurrency Crime and Anti Money Laundering Report, 2020, 6-7.

189 Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, 2013.

190 "New Policy Regarding In-World Banks," Linden Lab, Erişim Tarihi: Şubat 15, 2021, https://linden-lab. wordpress.com/2008/01/08/new-policy-regarding-in-world-banks/.

191 Engle, "Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting," 352.

192 Bu dolandırıcılık fiilinde, kötü amaçlı kodların kişisel bir bilgisayara veya sunucuya yüklenmesi sonucunda kişilerin izni veya bilgisi olmadan sahte bir web sitesine yönlendirilmesi sağlanmaktadır.

yöneliktir.[193] Üstelik kripto varlıklara ilişkin gizli anahtar veya şifrelerin elde edilmesi için meşru bir değişim platformunun da taklit edilmesi mümkündür.[194] Hizmet ve malların karşılığının ödenmemesi, kripto varlıklar bakımından da sıklıkla karşılaşılan diğer bir klasik dolandırıcılık yöntemidir.[195]Ancak bu yöntem kripto varlıklar için kullanıldığında daha ağır sonuçlar doğurabilmektedir. Anonimlik nedeniyle borca aykırı davranan kişiye kullandığı hesap üzerinden ulaşılması çok mümkün olmadığı gibi yapılan işlemin geri alınması veya iptal edilmesi de söz konusu değildir.[196] Bu bakımdan dolandırıcıların kripto varlıklara yönelmesinin en önemli sebeplerinden birinin bilgi asimetrisi olduğu ifade edilmelidir.[197] Kripto varlıkların hile ile elde edilmesinde kullanılan diğer bir yöntem ise "*Business E-mail Compromise*" yöntemidir. BEC saldırıları olarak da bilinen bu yöntem, genel olarak banka havalesiyle ödeme yapan işletme ve kuruluşları hedef alan bir aldatmacadır. Bu aldatmacada dolandırıcılar, ödeme sistemleri hakkında bilgi edinmek için hackleme veya sosyal mühendislik teknikleri kullanmakta ve elde ettikleri gizli bilgilerle şirket çalışanları, yönetici gibi kişilerin yasal bir işlem yaptığını düşünmesine sebep olarak para, hediye kartı, kripto varlıklar gibi ekonomik değer taşıyan şeylerin başka bir hesaba transferinin yapılmasını sağlamaktadır. Konuya ilişkin verilebilecek son örnek ise madencilik faaliyetine ilgi duyanların, pahalı teknolojik donanımlara yatırım yapmadan madencilikten kar elde edeceği vaadiyle dolandırılması yöntemidir (*mining-investment scams*).[198]

Görüldüğü üzere, çok çeşitli dolandırıcılık yöntemleri ile kişilerin yanıltılarak kendisine ait malvarlığı değeri üzerinde normal şartlarda gerçekleştirmeyeceği bir tasarrufta bulunması söz konusu olabilmektedir. Bu fiiller neticesinde ise hem devletler hem kişiler nezdinde yıkıcı sonuçlar ortaya çıkabilmektedir. Thodex gibi platformlarla Türkiye'de de gündeme gelen benzer olaylar, bu yıkıcı sonuçlara çarpıcı örnekler oluşturmaktadır. Bu nedenle, kripto varlıkların Türk ceza hukuku bakımından dolandırıcılık suçuna konu edilip edilemeyeceğinin irdelenmesi önem arz

193 Reddy and Minnaar, "Cryptocurrency: A Tool and Target for Cybercrime," 80.

194 Reddy and Minnaar, "Cryptocurrency: A Tool and Target for Cybercrime," 80; Marie Vasek and Tyler Moore, There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scam (2015), 19th International Conference on Financial Cryptography and Data Security (FC), 9.

195 James Elliott, "Help-Somebody Robbed My Second Life Avatar!," Journal of Virtual Worlds Research 1, S.1 (2008): 6.

196 Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış," 209; Tyler Moore and Nicolas Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," in Financial Cryptography and Data Security, ed. Ahmad-Reza Sadeghi (Heidelberg: Springer-Verlag, 2013), 26.

197 Chen, Zheng, Ngai, Zheng and Zhou, "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum," 5; Vasek and Moore, There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scam, 10.

198 Vasek and Moore, There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scam, 9.

etmektedir. TCK'nın 157. maddesine göre dolandırıcılık suçu, hileli hareketle bir kişinin aldatılması suretiyle onun veya başkasının zararına olarak yarar sağlanmasıdır.[199] Bu itibarla, dolandırıcılık suçu hırsızlık suçundan önemli ölçüde ayrılmaktadır. Hırsızlık suçunda malın bir yarar sağlamak maksadıyla alınması gerekiyor olsa da fiilen bu yararın sağlanmış olması gerekmezken, dolandırıcılık suçunda hile sonucu elde edilen bir yarar bulunması gerekmektedir. Konumuz açısından önem teşkil eden diğer bir fark ise suçun konusuna ilişkindir. Hırsızlık suçunun konusunu daha önce de belirtildiği gibi sadece taşınır bir mal oluşturabilirken, dolandırıcılık suçunun konusunu haklar, alacaklar, taşınır ve taşınmaz mallar ile bir hizmet dahi oluşturabilmektedir.[200] Önemli olan, hile ile elde edilen yararın malvarlığına ilişkin olmasıdır.[201] Dolayısıyla hırsızlık ve yağma suçunda varılan sonuçtan farklı olarak, fiziksel varlığı olmayan şeylerin malvarlığına ilişkin olması şartıyla dolandırıcılık suçuna konu olması mümkündür. Nitekim Yargıtay kararları da bu yöndedir.[202]

Türk ceza hukukuna göre kripto varlıklar, örnek verilen tüm dolandırıcılık fiillerine konu olabilecek ve TCK'nın 158. maddesi kapsamında cezalandırılabilecektir.[203] Zira ekonomik bir değer taşıyan kripto varlıkların hile suretiyle elde edilmesi halinde, hileye maruz bırakılan kişinin malvarlığı bakımından bir zarara uğraması, fail veya bir başkasının da yarar sağlaması söz konusu olmaktadır. Ancak kripto varlıklar üzerinde gerçekleştirilen dolandırıcılık fiilleri, bilişim sistemleri aracılığıyla icra edilebileceği için 158. maddenin f bendinde düzenlenen nitelikli halin uygulanması gerekmektedir.[204] Kripto varlıkların hileli bir hareket ile haksız bir şekilde ele geçirilebilmesi için bilişim sistemindeki verilerin başka bir yere gönderilmesi (mesela failin Bitcoin hesabına transfer yapılması) zorunluluk arz etmektedir. Böyle bir fiil sonucunda haksız bir çıkar da elde edilmiş olacağından hem dolandırıcılık suçu hem de bilişim sistemleri aracılığıyla haksız yarar sağlama suçu

199 TCK 157. maddesi: *"Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beş bin güne kadar adlî para cezası verilir."*.

200 Tezcan, Erdem ve Önok, Teorik ve Pratik Ceza Özel Hukuku, 866; Toroslu, Ceza Hukuku Özel Kısım, 185; Koca ve Üzülmez, Türk Ceza Hukuku Genel Hükümler, 744; Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 624.

201 Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 630.

202 Yargıtay tesis etmiş olduğu bir kararda şu ifadelere yer vermiştir: "*Hırsızlık suçunun maddi konusu ekonomik değer taşıyan taşınabilir bir maldır ve bu sebeple de tek maddi konulu bir suçtur. Buna karşılık dolandırıcılık suçu iki hukuki konulu suçtur. Bunlardan birisi insan iradesinin özgürlüğü, diğeri malvarlığına dair varlık ve yararlardır. Yine dolandırıcılık suçu taşınır ve taşınmaz mallar dışında alacak hakkı gibi malvarlığı değerlerine karşı da işlenen bir suçtur*.". İlgili karar için bknz: YCGK, 04.02.2014, E.2013/15-262, K.2014/37.

203 Rusya Yüksek Mahkemesi tarafından da benzer bir sonuca varıldığına ilişkin bknz: Y. Bokovnya; T.G. Zhukova, A.A. Shutova and L.V. Ryabova, "Legal Measures for Crimes in the Field of Cryptocurrency Billing," Utopía Y Praxis Latinoamericana 25, S.7 (2020): 273.

204 Bazı ülkeler bilişim sistemleri aracılığıyla gerçekleştirilen dolandırıcılık fiilini bağımsız bir suç kapsamında (*cyber fraud*) cezalandırmaktadır. Türk hukukunda ise bu fiil dolandırıcılık suçuna ilişkin nitelikli bir hal olarak düzenlenmiştir. Böyle nitelikli bir hale yer verilmesini doğru bulmayan görüş için bknz: Toroslu, Ceza Hukuku Özel Kısım, 194.

(TCK 244/4) gündeme gelecek ve içtima bakımından bir değerlendirme yapılması gerekecektir. Bu değerlendirme ise TCK'nın 244. maddesinin niteliği göz önünde alınarak yapılmalıdır. Söz konusu maddede, "*başka bir suç oluşturmama*" şartına yer verilmiştir. Bu bakımdan ilgili madde açıkça tali norm şeklinde düzenlenmiştir. Dolayısıyla aynı eyleme iki suçun uygulanmasının mümkün olduğu hallerde, asli norm niteliğine sahip olan dolandırıcılık hükümleri tatbik edilmelidir.

E. SUÇTAN KAYNAKLANAN MALVARLIĞI DEĞERLERİNİ AKLAMA SUÇU

Hukuka uygun faaliyetlerden elde edilen gelirlerle suçtan elde edilen gelirler temel bir konuda farklılaşmaktadır. Suçtan elde edilen gelirler hukuka uygun faaliyetlerden elde edilen gelirler kadar kolay harcanamamaktadır.[205] Özellikle suç gelirlerinin büyük miktarlara ulaştığı hallerde kısa vadede harcanabilecek bir nakit söz konusu değildir. Bu nedenle, suçtan elde edilen gelirlerin yasal sisteme dahil edilmesine imkân sağlayacak bazı işlemlerin yapılması ihtiyacı ortaya çıkmaktadır. Oluşacak şüpheyi bertaraf etmek için gayri meşru yollarla elde edilen çeşitli değerlere meşruluk imajı verilmesi, suçtan kaynaklanan malvarlığı değerlerinin aklanması kavramına karşılık gelmektedir. Aklama faaliyeti çeşitli suç gruplarını besleyerek, bu grupların daha derine kök salmasına sebep olmakta ve olası failleri suç işlemeye teşvik etmektedir.[206] Bu durum, suçla mücadele edilmesini ciddi oranda zorlaştırdığı gibi vergi gelirlerini azaltarak kamu düzeninin bozulmasına da sebep olabilmektedir.[207] Ancak aklama faaliyeti sadece ülkelerin kamu düzenini ve ekonomik sistemlerini etkilememekte, küresel bazda makro ekonomik düzenin dengesinin, bütünlüğünün ve şeffaflığının da kaybolmasına yol açmaktadır.[208] Ayrıca amaçladıkları siyasi hedefe varmak için şiddeti bir yöntem olarak seçen terör örgütleri, bu amaçlarına ulaşmak için ihtiyaçları olan mali kaynağı suçtan kaynaklanan değerlerin aklanması suretiyle de elde edebilmektedir.[209] Bundan dolayı suçtan kaynaklanan malvarlığı değerlerinin aklanması bağımsız bir suç olarak düzenlenmektedir.

Suçtan kaynaklanan malvarlığı değerlerini aklama suçuna ilk olarak 4208 sayılı Karaparanın Aklanmasının Önlenmesine Dair Kanun'da "*kara para aklama suçu*"

---

205 Joras Ferwerda, The Multidisciplinary Economics of Money Laundering, (Ridderkerk: Ridderprint, 2012), 2.

206 Sacit Yılmaz, "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu," Ankara Barosu Dergisi, S.2 (2011): 75; Neslihan Coşkun, "Karaparanın Aklanması Suçu," Selçuk Üniversitesi Hukuk Fakültesi Dergisi 12, S.3-4 (2004): 245.

207 John McDowell and Gary Novis, "The Consequences of Money Laundering and Financial Crime," An Electronic Journal of the U.S. Department of State 6, S.2 (2001): 8.

208 McDowell and Novis, "The Consequences of Money Laundering and Financial Crime," 7-8; Fatih Yurtlu, "Terör Suçlarıyla Mücadelede Yeni Konsept: Önalan Suçları- BGH Kararları Işığında Almanya Örneği," Selçuk Üniversitesi Hukuk Fakültesi Dergisi 29, S.3 (2021): 2171-2172.

209 İzzet Özgenç ve Fatih Yurtlu, "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçları Bakımından Teori ve Uygulamada Ortaya Çıkabilecek Sorunlara İlişkin Bir Değerlendirme," in 5. Türk-Kore Ceza Hukuku Günleri Karşılaştırmalı Hukukta Ekonomik Suçlar Uluslararası Sempozyumu Tebliğler Cilt II, ed. İzzet Özgenç, Cumhur Şahin, Faruk Turhan (Ankara: Seçkin Yayınevi, 2020), 448.

şeklinde yer verilmiştir. Bu kanunun 2. maddesinde kara para aklama suçu tanımlanmış ve 7. maddesinde bu suça ilişkin yaptırım öngörülmüştür. Fakat TCK'nın 282. maddesinde suçtan elde edilen malvarlığı değerlerinin aklanması şeklinde bir suç düzenlenmesiyle iki kanun arasında bazı çelişkiler ortaya çıkmıştır.[210] Bu çelişkilerin ortadan kaldırılmasıyla amacıyla 18.10.2006 tarihinde yürürlüğe giren 5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkındaki Kanun ile 4208 Sayılı Kanun'un birçok hükmü yürürlükten kaldırılmış ve "*kara para*" ibaresinden "*suçtan kaynaklanan malvarlığı değerinin*" anlaşılması gerektiği açıkça düzenlenmiştir.[211] Böylece iki kanun arasında ortaya çıkan çelişki giderilmiştir.

5549 sayılı kanunda ve TCK'nın 282. maddesinde yer alan hükümler göz önüne alındığında, suçtan kaynaklanan malvarlığı değerlerini aklama suçunun işlendiğinden söz edilebilmesi için bazı şartların gerçekleşmesi gerektiği anlaşılmaktadır. Bu şartlardan ilki, öncül bir suçun varlığıdır. Suçtan kaynaklanan malvarlığı değerlerinin aklanmasından bahsedilebilmesi için öncelikle bu malvarlığı değerlerinin elde edileceği bir suç işlenmiş olmalıdır. Aklanması amaçlanan malvarlığı değerine kaynaklık eden bu suça öncül suç, ön suç, temel suç, müsnet suç, yüklem suç da denilmektedir.[212] Öncül suçun kapsamını tespit etme noktasında, kural olarak kanun koyucuların takdir yetkisi bulunmaktadır. Bu suçlar, eşik bir değer koyularak belirlenebileceği gibi tek tek sayılarak da somutlaştırılabilmektedir.[213] Birçok hükmü yürürlükten kaldırılan 4208 sayılı kanun tek tek sayma yöntemi[214] kullanması sebebiyle doktrinde yoğun bir şekilde eleştirilmiştir.[215] Bu nedenle, 5237 sayılı TCK'da sayma yönteminden vazgeçilerek eşik değer belirle-

---

210 TCK'nın 282. maddesi: *"Alt sınırı altı ay veya daha fazla hapis cezasını gerektiren bir suçtan kaynaklanan malvarlığı değerlerini, yurt dışına çıkaran veya bunların gayrimeşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla, çeşitli işlemlere tâbi tutan kişi, üç yıldan yedi yıla kadar hapis ve yirmi bin güne kadar adlî para cezası ile cezalandırılır. Birinci fıkradaki suçun işlenmesine iştirak etmeksizin, bu suçun konusunu oluşturan malvarlığı değerini, bu özelliğini bilerek satın alan, kabul eden, bulunduran veya kullanan kişi iki yıldan beş yıla kadar hapis cezası ile cezalandırılır." şeklinde düzenlenmiştir."*.

211 "Kara para aklama" kavramının "suçtan elde edilen malvarlığı değerlerinin aklanması" şeklinde değiştirilmesinin, uluslararası belgelere uyum sağlama amacı taşıdığı belirtilmektedir. Konuya ilişkin ayrıntılı bilgi için bknz: Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 1142.

212 Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 1147; Özgenç ve Yurtlu, "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçları Bakımından Teori ve Uygulamada Ortaya Çıkabilecek Sorunlara İlişkin Bir Değerlendirme," 454.

213 Ümit Kocasakal, "Karapara Aklama Suçu," (Doktora Tezi, İstanbul Üniversitesi, 2000), 178.

214 4208 sayılı kanunun 2/a maddesinde gösterilen ve öncül suç olarak nitelendirilen bu suçlar şu şekildedir: *"1918 sayılı Kaçakçılığın Men ve Takibine Dair Kanundaki suçlar, 6136 sayılı Ateşli Silahlar ve Bıçaklar Hakkında Kanundaki suçlar, 2238 sayılı Organ ve Doku Alınması, Saklanması ve Nakli Hakkında Kanundaki suçlar, 2863 sayılı Kültür ve Tabiat Varlıklarının Korunması Hakkındaki Kanundaki suçlar, 213 sayılı Vergi Usul Kanunun 359. maddesinin b fıkrasındaki suç ve 765 sayılı Türk Ceza Kanunundaki Devletin Şahsiyetine Karşı İşlenen Cürümler ve aynı Kanunun 179, 192, 264, 316, 317, 318, 319, 322, 325, 332, 333, 335, 339, 341, 342, 345, 350, 403, 404, 406, 435, 436, 495, 496, 497, 498, 499, 500, 504 ve 506. maddesinde düzenlenen suçlar."*.

215 Söz konusu eleştiriler için bknz: Kocasakal, "Karapara Aklama Suçu," 345-350; Coşkun, "Karaparanın Aklanması Suçu," 245 vd.

me yöntemi tercih edilmiştir. İlgili düzenlemeye göre, alt sınırı 6 ay ve daha fazla olan suçlar öncül suç olarak değerlendirilecektir.

Öncül suçtan kaynaklanan gelirlerin yasal bir görünüme kavuşturulması, aklama suçunun varlığı için aranan diğer bir şartı teşkil etmektedir. Malvarlığı değerlerine yasal görünüm kazandırmaya yönelik fiiller TCK'da seçimlik olarak düzenlenmiştir.[216] Seçimlik fiiller, suçtan kaynaklanan malvarlığı değerlerinin yurt dışına çıkarılması ve bunların gayri meşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla çeşitli işlemlere tâbi tutulmasıdır. Çeşitli işlemlere; sermaye piyasası araçlarına yatırım yapılması, sigorta poliçesi alınması, mali sistem vasıtasıyla yurt içinde transfer yapılması, başkası adına hesaba para yatırılması, hizmet sektörlerinden faydalanarak niteliğin, sahibin, zilyedin gizlenmesi ve farklı gösterilmesi gibi örnekler verilebilmektedir. Bunun dışındaki işlemlerle de aklama suçunun işlenmesi mümkün olup; önemli olan husus, bu işlemlerin gayrimeşru kaynağı gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak amacıyla icra edilmesidir.[217] Netice olarak, öncül bir suçtan elde edilen malvarlığı değerinin TCK 282. madde kapsamında değerlendirilebilmesi için ya yurt dışına çıkarılması ya da özel bir amaç doğrultusunda çeşitli işlemlere tabi tutulması gerekmektedir.

Öncül suçtan elde edilen hangi değerlerin TCK 282. maddede düzenlenen suça konu olabileceği, üzerinde durulması gereken bir diğer önemli meseledir. 4208 sayılı kanunun 2. maddesinde bu konuya ilişkin açık bir hükme yer verilmiştir. İlgili düzenlemeye göre; kanunun 2/a maddesinde sayılan fiillerden birinin işlenmesi suretiyle elde edilen para, para yerine geçen her türlü kıymetli evrak, mal ve gelirler ile bir para biriminden diğer bir para birimine çevrilmesi de dahil sözü edilen para, evrak, mal veya gelirlerin birbirine dönüştürülmesinden elde edilen her türlü maddi menfaat ve değer aklama suçuna konu olabilecektir. TCK'nın 282. maddesinde konuya ilişkin açık bir düzenleme yapılmamış, ancak kanun gerekçesinde yol gösterici mahiyette olan şu açıklamalara yer verilmiştir: "*Bu suçun konusunu suçtan kaynaklanan malvarlığı değerleri oluşturmaktadır. Bu malvarlığı değerlerinin elde edildiği suçun türü ve mahiyeti önemli değildir. Önemli olan bu suçun konusunu oluşturan ekonomik değerlerin başka bir suçun işlenmesi suretiyle veya dolayısıyla elde edilmiş olmasıdır.*".[218] Ayrıca Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesi Kapsamında İşlemlerin Ertelenmesine Dair Yönetmelik'te, kanun gerekçesini tamamlayıcı bir hüküm bulunmaktadır. Bu yönetmeliğin 2. maddesinde malvarlığı kavramı, para, değeri para ile temsil edilebilen taşınır veya taşınmaz, maddi veya gayri maddi her türlü mal ve haklar ile bunlar üzerindeki hakları tevsik eden her

216 Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 1144.

217 Artuk, Gökcen, Alşahin ve Çakır, Ceza Hukuku Özel Hükümler, 1145.

218 HBV Türk Ceza Hukuku Uygulama ve Araştırma Merkezi, Türk Ceza Hukuku Mevzuatı Cilt I, (Ankara: Seçkin Yayınevi, 2019), 525.

türlü yasal belge veya araç şeklinde tanımlanmıştır. Nitekim Viyana Konvensiyonu, Palermo Konvansiyonu, Strasburg Sözleşmesi gibi temel metinlerde de malvarlığı değerleri, maddi ve gayri maddi her çeşit mal ile bunlar üzerindeki bir hakkı gösteren belge ve senetler olarak sayılmıştır. Doktrinde de malvarlığı değeri ifadesinden, bir kişinin hukukî bütünlük oluşturmak üzere sahip ve yükümlü tutulacağı para ile ölçülen hak ve borçlarının tamamının, kısacası, her türlü mali değerin anlaşılması gerektiği belirtilmektedir.[219] Bu itibarla, TCK'nın 282. maddesi, ekonomik anlamda bir değeri haiz maddi ve maddi olmayan her şeyi kapsadığı gibi bu değerleri temsil veya ifade eden her türlü belge, evrak ve kaydı da muhtevasında barındırmaktadır. Dolayısıyla ekonomik bir değer taşıyan kripto varlıkların da bu suç kapsamına girmesi mümkündür. Suçla etkin bir şekilde mücadele edilebilmesi için de böyle bir sonuca varılması zorunluluk arz etmektedir.

Her yerde ve herkese anında ödeme imkânı sunan, merkezi olmayan, belirli bir seviyede gizlilik ve anonimlik sağlayan kripto varlıklar ile aklama suçunu işlemek hem daha kolay hem de daha caziptir. Şöyle ki; suçtan kaynaklanan malvarlığı değerlerinin aklanması yerleştirme, ayrıştırma ve bütünleştirme olarak nitelendirilen üç aşamada gerçekleşmektedir. Bu aşamalardan ilki, kirli değerin finansal sisteme sokulmasına ve böylece nakdi paranın kaydi paraya dönüşmesine imkân tanıyan yerleştirme aşamasıdır.[220] İkincisi ise bu değerin yasadışı kaynağından uzaklaştırılmasını sağlayan ayrıştırma aşamasıdır. Bu aşamada, suçtan elde edilen değerin izinin sürülmesi finansal işlemler çoğaltılarak engellenmeye çalışılmaktadır.[221] Son aşama olan bütünleştirme aşamasında ise aklanan değer yasal işlemlerle ülkelerin mali sistemine aktarılarak ekonomik dolaşıma dahil edilmektedir.[222] Yerleştirme, ayrıştırma ve bütünleştirme olarak sayılan bu aşamaların üçünün de ayrı ayrı gerçekleşmesi zorunlu değildir. Bazı durumlarda bu aşamaların birbiriyle örtüşmesi söz konusu olabilmektedir. Kripto varlıklarda ise bu üç aşamanın takip edilmesine çoğunlukla ihtiyaç duyulmamaktadır. Suçtan doğrudan kripto varlık kazanılması halinde, kaydi paraya çevrilmesi gereken bir değer bulunmadığı gibi merkezi yapı olmaması ve anonimlik nedeniyle bunların kaynağının izinin sürülmesi de mümkün değildir.[223] Bu avantajları kullanarak büyük miktardaki gelirleri kaynağından uzaklaştırmak da son derece hızlı ve kolay olabilmektedir.[224]

---

219 Özgenç ve Yurtlu, "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçları Bakımından Teori ve Uygulamada Ortaya Çıkabilecek Sorunlara İlişkin Bir Değerlendirme," 454; Yılmaz, "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu," 79; Kocasakal, "Karapara Aklama Suçu," 204.

220 Kocasakal, "Karapara Aklama Suçu," 71.

221 Kocasakal, "Karapara Aklama Suçu," 72; Ufuk Ünlü, "Kara Para Aklamada Yeni Yöntemler ve Kara Paranın Ekonomi Üzerindeki Etkileri," Sayıştay Dergisi, S.113 (2019): 161.

222 Kocasakal, "Karapara Aklama Suçu," 73; Türkiye Bankalar Birliği, s.17; Ünlü, "Kara Para Aklamada Yeni Yöntemler ve Kara Paranın Ekonomi Üzerindeki Etkileri," 161.

223 Reddy and Minnaar, "Cryptocurrency: A Tool and Target for Cybercrime," 76.

224 Vitalii Rysin and Mariia Rysin, "The Money Laundering Risk and Regulatory Challenges for Cryptocurrency Markets," in Restructuring Management Models-Changes-Development, ed.

Aklama sürecinde kullanılan smurfing ve parçalama yöntemlerine kripto varlıkların aklanmasında da başvurulmaktadır. Yüksek meblağlı Bitcoin'ler, aynı kişiye ait birden çok hesap açılarak bölünmekte ya da birden çok cüzdan hesabında saklanabilmektedir.[225] Yapılan bir çalışmada da Bitcoin'i yasadışı faaliyetler için kullananların, aynı taraf ile daha küçük tutarlarla ve daha fazla işlem yapma eğiliminde olduğu ortaya koyulmuştur.[226] Bununla birlikte Bitcoin ATM'lerinin de aklama faaliyetinde yoğun bir şekilde kullanıldığını belirtmek gerekir.[227] Ayrıca "*chain hopping*" olarak adlandırılan bir uygulama ile farklı kripto varlık türleri arasında geçişler yapılarak elde edilen değerin takibi de zorlaştırılabilmektedir.[228] Bu bakımdan kripto varlıklar, sağladıkları anonimlik nedeniyle suçtan elde edilen malvarlığı değerlerinin kökenini gizlemek için kullanılmaktadır. Ancak daha önce de ifade edildiği üzere, Blokzincir kullanan kripto varlıklar bakımından anonimliğin belli bir oranda yumuşatılması ve işlem yapan adresin kime ait olduğunun tespit edilmesi mümkündür. Bu nedenle, Bitcoin gibi kripto varlıkların aklanmasında tumbler ve mixer hizmetleri[229] ile off-chain kanalları[230] kullanılarak kaynak ve işlem yapan kişinin kimliği tamamen gizlenmeye çalışılmaktadır. Tumbler ve mixerler, birden fazla kullanıcının kripto varlıklarını karıştırarak işlem ile kay-

Marek Dziura, Andrzej Jaki, Tomasz Rojek (Toruń: Dom Organizatora, 2020), 194; U.S Department of Justice, Cryptocurrency Enforcement Framework, 13. Konuya ilişkin Liberty Reserve önemli bir örnek oluşturmaktadır. Kosta Rika merkezli bir kripto varlık piyasası olan Liberty Reserve para transferi için çok asgari düzeyde kişisel bilgi talep eden, bu bilgileri doğrulama ve kontrol mekanizması olmayan bir şirkettir. Bu şirket hakkında dolandırıcılık, kimlik hırsızlığı, çocuk pornosu gibi suçlardan elde edilen gelirlerin aklanması nedeniyle soruşturma başlatılmış ve yargılama sürecinin sonunda para aklandığı ve lisanssız para transferi gerçekleştirildiği gerekçesiyle kapatılma kararı verilmiştir. On yedi ülkenin dahil olduğu adli süreçte, 36 farklı karşılıklı adli yardım sözleşmesi uygulama alanı bulmuş, 15 ülkeden adli arama yapması, malvarlığı değerlerini dondurması ve müsadere tedbirine başvurması talep edilmiştir. Verilen bu örnek, kripto varlıklara ilişkin muhakeme işlemlerinin yapılmasında iş birliğinin önemini açık bir şekilde ortaya koymaktadır. Libert Reserve hakkında ayrıntılı bilgi için bknz: Kien and Ly, Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies," 595; Nolasco Braaten and Vaughn, "Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions," 965; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 10.

225 Marian, "Are Cryptocurrencies 'Super' Tax Havens?," 44.

226 Foley, Karlsen and Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?," 1801.

227 Cipher Trace, Cryptocurrency Crime and Anti Money Laundering Report, 2020, 14 vd.

228 Korver, Pelker and Poteat, "Attribution in Cryptocurrency Cases," 251; U.S Department of Justice, Cryptocurrency Enforcement Framework, 44; Buttigiegh, Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State," 213.

229 Bunların etkinliğinin sorgulanabilir ve kullanıcılar açısından daha maliyetli olduğunu düşünen görüş için bknz: Dyson, Buchanan and Bell, "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime," 3.

230 Off-chain kanalları, açılan bir ödeme kanalı aracılığıyla işlem yapılmasını ve bu işlemlerin blokzincirde yayımlanmasına gerek kalmadan sürdürülmesini sağlayan kanallardır. Bu kanallar hakkında ayrıntılı bilgi için bknz: Buttigiegh, "Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State," 213.

nağı arasındaki bağlantıyı kesmeye yarayan uygulamalardır.[231] Bu hizmetlerin kullanılmasının ne kadar çarpıcı sonuçlar doğurabileceğine Helix adlı tumbler uygulaması iyi bir örnek oluşturmaktadır. Söz konusu program, adeta bir blender işlevi görerek suç faaliyetlerinden elde edilen kripto varlıkları temiz kripto varlıklarla karıştırarak bunların birbirinden ayrılmasını ciddi oranda zorlaştırmış ve 300 milyon değerindeki Bitcoin'in aklanmasına hizmet etmiştir.[232]

Suçtan kaynaklanan malvarlığı değerlerinin aklanması ve terörizmin finansmanı suçuna ilişkin önleyici tedbirler, anonimlik perdesinin aralanmasına olanak sağladığından kripto varlıkların konu edildiği suçlarla mücadele edilmesinde de önemli bir yere sahiptir. Bu önemi somut verilerle de ortaya koymak mümkündür. Yapılan bir çalışmada, doğrudan değişim platformlarında kullanılan suç fonlarının küresel ortalamasının 2019 yılında yüzde 47% oranında azaldığı tespit edilmiştir.[233] Görüldüğü üzere, değişim hizmeti veren platformların hukuki bir düzenlemeye tabi tutulması ile suçlular üzerinde ciddi bir caydırıcılık yaratılabilmektedir. Sistemde yer alan aktörlerin hukuka boyun eğdirilmesi suretiyle en büyük engel olarak değerlendirilen anonimliğin yumuşatılması gerekmektedir. Esasında bu gereklilik, tüm devletler için yasal bir zorunluluk haline de gelmiştir. FATF, suçtan elde edilen gelirlerin aklanması ve terörizmin finansmanıyla mücadele etmek amacıyla yayınladığı 40 Tavsiye Kararı'nda sanal varlıklara (*virtual asset*) ilişkin önemli bir tavsiyeye yer vermiştir. Bahse konu metnin 15 numaralı tavsiyesinde, ülkelerin sanal varlıklardan kaynaklanan riskleri[234] kontrol edebilmek ve azaltabilmek için hizmet sağlayıcılarını aklama riskini de göz önünde bulundurarak düzenlemesi, lisans ve kayıt zorunluluğuna tabi tutması ve öngörülen diğer tedbirlerin kapsamına dahil etmesi gerektiği belirtilmiştir.[235] Benzer şekilde Mali Sistemin Karaparanın Aklanması ve Terörizmin Finansmanı Amacıyla Kullanımının Önlenmesi Hakkında 2015/849/EC sayılı Direktif'de değişiklik yapılarak aklama konusunda güncel risk taşıyan kripto varlık değişim platformları ve cüzdan sağlayıcıları yükümlüler kap-

231 Reddy and Minnaar, "Cryptocurrency: A Tool and Target for Cybercrime," 77; Tziakouris, "Cryptocurrencies-A Forensic Challenge or Opportunity for Law Enforcement? An Interpol Perspective," 93; FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 6; European Central Bank, Virtual Currency Schemes-Further Analysis, 8; U.S Department of Justice, Cryptocurrency Enforcement Framework, 41; Dupuis and Gleason, "Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic," 66.

232 Cipher Trace, Cryptocurrency Crime and Anti Money Laundering Report, 2020, 19-20; U.S Department of Justice, Cryptocurrency Enforcement Framework, 43.

233 Cipher Trace, Cryptocurrency Crime and Anti Money Laundering Report, 2020, 7.

234 Aklama ve terörizmin finansmanı suçuyla ilgili risk göstergeleri hakkında FATF'ın 2020 yılında yayımladığı önemli bir rapor bulunmaktadır. Bu raporda, klasik risk göstergelerinin sanal varlıklar bakımından da geçerli olduğu belirtilmiştir. Ayrıca transferin sıklığı ve miktarı, geçerli bir iş ilişkisi olmadan transfer yapılması, birden fazla sanal varlık arasında geçiş yapılması, privacy coin kullanılması gibi ek risk göstergeleri de belirlenmiştir. İlgili rapor için bknz: FATF, Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.

235 FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation the FATF Recommendations, 2020, 16.

samına dahil edilmiştir.[236] Avrupa Parlamentosu tarafından 2018 yılında yapılan bir çalışmada da, Avrupa Birliği standartları için kripto varlık kullanıcılarının gönüllü kayıt sisteminden ziyade zorunlu kayıt sistemine tabi tutulması gerektiği önerisine yer verilmiştir. Buna ek olarak, kullanıcıların kontrol edilmesini ve cezai yaptırıma tabi tutulmasını imkânsız hale getirmeyi amaçlayan mixer, tumbler gibi uygulamaların da yasaklanması gerektiği vurgulanmıştır.[237]

Suçtan elde edilen malvarlığı değerlerinin aklanması ve terörizmin finansmanı suçunu önlemek adına Japonya,[238] Kanada,[239] Almanya, Belarus, İsrail, Fransa, Avusturalya, İsveç, Finlandiya, İtalya, Meksika, Jersey, Malta, Estonya gibi birçok ülkede sanal para işletmelerinin lisans alması zorunlu kabul edilmiştir.[240] Amerika'da hazineye bağlı olarak faaliyet gösteren ve konuya ilişkin otorite olarak görev yapan FinCEN de değişim hizmeti sunan platformların para işletmeleri olduğunu kabul ederek bunların lisans almasını zorunlu tutmaktadır.[241] Lisans almak zorunda olan bu işletmeler, kayıt tutma, raporlama ve bu kayıtların saklanması gibi önemli yükümlülükler altına girmekte ve bu yükümlülükleri yerine getirmediği takdirde yaptırıma tabi tutulabilmektedir. Nitekim FinCEN 2015 yılında bu yükümlülüklere uymadığı gerekçesiyle Ripple hakkında cezai işlem uygulamıştır.[242] Söz konusu işlem, kripto varlıkların çıkışından itibaren bu varlıklara devlet eliyle uygulanan ilk yaptırım olarak değerlendirilmektedir.[243] Federe düzeyde de benzer düzenlemelere rastlamak mümkündür. New York, California, Alabama, Vermont, North Carolina, Connecticut, Washington gibi birçok eyalette lisans alma zorunluluğu getirilmiştir. "*BitLicense*" uygulaması gereği New York'ta faaliyet gösteren bütün sanal para işletmeleri, her işlemden önce belirtilen bilgileri yazılı olarak ifşa etmek zorundadır.[244]

---

236 AB, Directive 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, (2018), OJ L 156/43. Yapılan değişikliğin sınırlı bir kapsama sahip olması ve yasal boşlukları ortadan kaldıramaması nedeniyle eleştirildiğini görmekteyiz. Bu eleştiriler için bknz: Rysin and Rysin, "The Money Laundering Risk and Regulatory Challenges for Cryptocurrency Markets," 189.

237 European Parliament, Cryptocurrencies and Blockchain, 14.

238 Japonya'nın MT GOX platformuna ilişkin yaşanan olumsuz gelişmelerden dolayı kanunda değişikliğe gittiği hakkında bknz: FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 49.

239 Aklama suçu kapsamında sanal para işletmelerine yükümlü olarak ilk yer veren ülkenin Kanada olduğu hakkında bknz: Lee, "Decrypting Crypto: Issues Plaguing Today's Hottest Regulatory Nightmare," 575.

240 Örnek olarak verilen bu ülkelerden, Finlandiya, İsrail, Malta gibi ülkeler özel bir kanun kapsamında düzenleme yapmayı tercih ederken, Kanada, Avusturalya, Jersey ve Estonya gibi ülkeler aklama suçuna ilişkin mevcut hükümlerde değişikliğe gitmeyi tercih etmiştir.

241 Korver, Pelker and Poteat, "Attribution in Cryptocurrency Cases," 240.

242 U.S Department of Justice, Cryptocurrency Enforcement Framework, 25; Kethineni and Cao, "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity," 331.

243 BTK, Kripto Para Araştırma Raporu, 18.

244 Hughes, "Cryptocurrency Regulations and Enforcement in the U.S," 22; Murphy, Murphy and Seitzinger, Bitcoin: Questions, Answers, and Analysis of Legal Issues, 15-16; Lee, "Decrypting Crypto: Issues Plaguing Today's Hottest Regulatory Nightmare," 570.

Türk hukukunda da suçtan elde edilen malvarlığı değerlerinin aklanması ve terörizmin finansmanına ilişkin hükümlerin uygulama alanı bulabilmesi için benzer düzenlemelerin yapılması ihtiyacı ortaya çıkmıştır. Bu ihtiyacı gidermek amacıyla 1 Mayıs 2021 tarihinde 31417 sayılı Resmî Gazete'de, Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik yayımlanmıştır. Bu yönetmelikle yükümlüler kapsamına kripto varlık hizmet sağlayıcıları ve tasarruf finansman şirketleri dahil edilmiştir. Böylece suçtan kaynaklanan malvarlığı değerlerini aklama ve terörizmin finansmanı suçuyla mücadelede önemli bir adım atılmıştır. Ancak uluslararası hukuktan kaynaklanan yükümlülüklerin tam olarak yerine getirildiğini söylemek mümkün değildir. Konuya ilişkin uluslararası hukukta yapılan düzenlemeler, sadece kripto hizmet sağlayıcılarını değil sanal para hizmet sağlayıcılarını da içine alan bir kapsama sahiptir. Daha önce de belirtildiği gibi sanal paralar, kripto varlıkları da içine alan geniş kapsamlı bir kümedir. Bu bakımdan mevzuatımızda yapılan değişikliğin yetersiz olduğu ifade edilmelidir. Bu noktada, kripto varlık hizmet sağlayıcılarının tanımının ne şekilde yapılacağı da önem arz etmektedir. Bazı ülkeler ilgili kavramın tanımlanmasında, sadece sanal varlıklardan itibari paraya çevirme faaliyetini göz önünde tutmaktadır. Bu durumda alınacak önlemler, sadece kripto varlıkların itibari paraya dönüştürülmesi halinde geçerli olabilecektir. Böyle bir dönüştürmenin söz konusu olmadığı hallerde ise yasal düzenlemelerin radarından kaçılabilecektir.[245] Ayrıca yapılacak tanıma göre hizmet sağlayıcıları kapsamına madenciler gibi daha farklı fonksiyonlar icra eden aktörlerin girip girmeyeceği noktasında da tereddütler oluşabilecektir. Bu nedenle kapsamlı ve titiz bir düzenleme yapılmalı, kripto varlıklar arasındaki değişimler de yapılacak tanıma dahil edilmelidir.

SONUÇ

Teknolojinin hayatımıza getirdiği yeniliklerden bazıları günlük hayatı kolaylaştırırken, bazıları günlük hayatın yeni temeller üzerine inşa edilmesini gerektirmektedir. Hayatımıza teknolojik gelişmelerle dahil olan bu yenilikler, günlük hayatımızı kolaylaştırdığı oranda kişilerin hayatı, sağlığı veya malvarlığı bakımından tehlike de oluşturabilmektedir. Bu tehlikeye rağmen, özellikle hukuk alanında bu değişime ayak uydurulamamakta ve meydana gelen gelişmeler geriden takip edilmeye çalışılmaktadır. Devlet kontrolünde olmayan ve sadece katılımcılar aracılığıyla işleyen bir sistemin para transferi yapmak için kullanılması bu zamansal farkı daha da belirgin hale getirmiştir. Günümüzde hukuk ürünü olan

[245] KuCoin, BitFinex, StormGain gibi bazı değişim platformları sadece kripto varlıkların itibari paraya dönüştürüldüğü hallerde yükümlülüklerini yerine getirmekte, kripto varlıklar arasındaki değişimlerde anonim işlem yapılmasına olanak sağlayabilmektedir. Kimlik bilgisi gerektirmeyen değişim platformlarını listeleyen bazı internet siteleri de bulunmaktadır. Bu sitelerden biri için bknz: https://kycnot.me/. Konuya ilişkin ayrıntılı bilgi için bknz: Dupuis and Gleason, "Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic," 64.

paralar yerine sanal ortamda bu işlevi gören "veriler" kullanılmaya başlanmıştır. Kripto varlıklar olarak isimlendirilen bu veriler, merkezi bir otoriteye ihtiyaç duyulmadan dünyanın her yerine çok daha hızlı ve ucuz şekilde ekonomik bir değer transfer edilmesine olanak sağlamaktadır. Bu çarpıcı ve beklenmeyen duruma devletlerin tepkisi ise oldukça geç olmuştur. Devletlere nazaran teknolojiye daha kolay adapte olan suçlular ise kripto varlıkların sunduğu imkanları suç işlemek için kullanmaktadır.

Suçluların kripto varlıklara yönelmesiyle; hırsızlık, dolandırıcılık, uyuşturucu ve uyarıcı madde ticareti, silah ticareti, çocuk pornografisi, suçtan kaynaklanan malvarlığı değerlerinin aklanması, vergi kaçakçılığı, terörizmin finansmanı gibi birçok suç tipi yeni bir boyut kazanmıştır. Suçların kazandığı bu yeni boyut karşısında hukukun da koruma alanını genişletmesi gerekmektedir. Her ne kadar transfer işlemi yapılması için artık bankalara gerek kalmamış olsa da güvenlik ve düzen için halen hukuk kurallarına ihtiyaç duyulmaktadır. Ancak mevcut ceza hukuku kurallarının kripto varlıkların sanal, anonim ve kompleks yapısıyla mücadele etmek için yeterli olmadığı açıktır. Konuyu ele alacak ulusal nitelikteki düzenlemelerin de tek başına bu problemleri çözmesi mümkün değildir. Bu nedenle, yapılacak düzenlemenin evrensel nitelikte olması ve meydana gelecek gelişmelere uyum sağlayacak bir esneklikte ele alınması gerekmektedir. Bitcoin ile başlayan yeni dönem, suçlulara farklı imkanlar sunan binlerce kripto varlık türünü de beraberinde getirmiştir. Şüphesiz her bir kripto varlık türü için özel düzenleme yapılması mümkün değildir. Tamamen yasaklayıcı bir tutum içerisinde hareket etmek de istenilen sonuçları vermeyecektir. Yeni başlayan bu dönem artık durdurulamaz ve engellenemez bir boyuta ulaşmıştır. Ayrıca devletler için önemli fırsatlar yaratan teknolojik gelişmelerin yavaşlamasına veya durmasına da sebep olunmamalıdır.

Kripto varlıkları yasaklamak bir çözüm olamayacağından konuya ilişkin atılacak en makul adım, hepsi için ortak özellik taşıyan ve suç işleme noktasında bu varlıkları cazibe merkezi haline getiren anonimliğe odaklanmaktır. Anonimliğin yarattığı olumsuz sonuçların azaltılmasında ise kripto varlık aktörlerinden araç olarak yararlanılması düşünülmelidir. Bu çözüme temel oluşturan esas düşünce, aktörleri sistemde 3. kişi (*middle man*) olarak konumlandırabilmek ve bunlar aracılığıyla süreci daha şeffaf hale getirebilmektir. Bir kripto varlığın sadece kendi içinde sistemin devamını sağlaması çok olanaklı görünmediğinden farklı aktörlerin sürece dahil olması kaçınılmaz olmaktadır. Özellikle iki yönlü akışa sahip kripto varlıklarda bu akışı sağlayacak aktörlere ihtiyaç duyulmaktadır. Dolayısıyla bu aktörlerin düzenlenmesi yoluyla sistemin kısmen de olsa kontrol altına alınması mümkün olabilecektir. Ancak hangi aktörlerinin nasıl bir düzenlemeye tabi tutulacağı hem teknolojik gelişmeyi baltalamamak hem de insanları tamamen anonim varlıklara kaydırmamak adına titiz bir şekilde ele alınmalıdır.

KAYNAKÇA

AB, Directive 2009/110/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money İnstitutions Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 2000/46/EC, (2009), OJ L 267/7.

AB, Directive 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, (2018), OJ L 156/43.

Abramowicz, Michael. "Cryptocurrency-Based Law.", Arizona Law Review 58, S.2 (2016): 359-420.

Adrian, Tobias and Mancini-Griffoli, Tommaso. The Rise of Dijital Money. IMF Fintech Notes, 2019.

Armknecht, Frederik; Karame, Ghassan O.; Mandal, Avikarsha; Youssef, Franck and Zenner, Erik. "Ripple: Overview and Outlook, Trust and Trustworthy Computing." In Lecture Notes in Computer Science, ed. Mauro Conti, Matthias Schunter, Ioannis Askoxylaki, 163-180. Cham: Springer, 2015.

Artuk, M. Emin; Gökcen, Ahmet; Alşahin, M. Emin ve Çakır, Kerim. Ceza Hukuku Özel Hükümler. Ankara: Adalet Yayınevi, 2019.

Bartusiak, Pavlo. "'Judicial Finding' of the Legal Nature of Cryptocurrency.", Ehrlich's Journal 2, S.1 (2018): 24-36.

Bilgi Teknolojileri ve İletişim Kurumu (BTK). Kripto Para Araştırma Raporu, 2020.

Blandin, Apolline; Cloots, Ann Sofie; Hussain, Hatim; Rauchs, Michel; Saleuddin, Rasheed; Allen, Jason Grant; Zhang, Bryan and Cloud, Katherine. Global Cryptoasset Regulatory Landscape Study, Cambridge Center for Alternative Finance, 2019.

Blundell Wignall, Adrian. The Bitcoin Question: Currency versus Trust-less Transfer Technology. OECD Working Papers on Finance, Insurance and Private Pensions No: 37, 2014.

Boehm, Franziska and Pesch, Paulina. "Bitcoin: A First Legal Analysis-With References to German and US-American Law.", Conference Paper, 1st Workshop on Bitcoin Research in Assocation with Financial Crypto, 2014.

Bokovnya, Y.; Zhukova, T. G.; Shutova, A. A. and Ryabova, L.V. "Legal Measures for Crimes in the Field of Cryptocurrency Billing.", Utopía Y Praxis Latinoamericana 25, S.7 (2020): 270-275.

Bozkurt Yüksel, Armağan Ebru. "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış.", İÜHFM 73, S.2 (2015): 173-220.

Brown, Steven David. "Cryptocurrency and Criminality: The Bitcoin Opportunity.", Police Journal 89, S.4 (2016): 327-339.

Bullmann, Dirk; Klemm, Jonas and Pinna, Andrea. In Search for Stability in Crypto-Assets: Are Stablecoins the Solution?. ECB Occasional Paper Series No: 230, 2019.

Buttigieg, Christopher P. "Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State.", Law and Financial Markets Review 13, S.4 (2019): 211-227.

Calcaterra, Craig; Kaal, Wulf A. and Rao, Vadhindran. "Stable Cryptocurrencies.", Washington University Journal of Law & Policy 61, S.1 (2020): 193-228.

Chen, Weili; Zheng, Zibin; Ngai, Edith; Zheng, Peilin and Zhou, Yuren. "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum.", IEEE Access 7, (2019): 37575-37586.

Cipher Trace. Cryptocurrency Crime and Anti Money Laundering Report, 2020.

Cipher Trace. Cryptocurrency Crime and Anti Money Laundering Report, 2021.

Coinmarketcap. "Today's Cryptocurrency Prices by Market Cap." Erişim Tarihi: Kasım 15, 2021. https:// coinmarketcap.com/1/.

Coşkun, Neslihan. "Karaparanın Aklanması Suçu.", Selçuk Üniversitesi Hukuk Fakültesi Dergisi 12, S.3-4 (2004): 229-261.

Cvetkova, Irina. "The Legal Definition of Crypto Assets.", BRICS Law Journal 5, S.2 (2018): 128-153.

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

Çeker, Selman Musab. "Kripto Paralar ve Ekonomik Etkileri.", Bitirme Tezi, Yıldız Teknik Üniversitesi, 2018.

Çekin, Mesut Serdar. "Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var mı?.", İstanbul Hukuk Mecmuası 77, S.1 (2019): 315-341.

Çetinkaya, Şahin. "Kripto Paraların Gelişimi ve Para Piyasalarındaki Yerinin Swot Analizi ile İncelenmesi.", Uluslararası Ekonomi ve Siyaset Bilimleri Akademik Araştırmalar Dergisi 2, S.5 (2018): 11-21.

Dupuis, Daniel and Gleason, Kimberly. "Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic.", Journal of Financial Crime 28, S.1 (2021): 60-74.

Durdu, Erdal. "Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku.", Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2018.

Dülger, Murat Volkan ve Özkan, Onur. "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi." In Prof. Dr. Mehmet Emin Artuk'a Armağan, ed. Mahmut Koca, 963-994. Ankara: Seçkin Yayınevi, 2020.

Dyson, Simon; Buchanan, William J. and Bell, Liam. "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime.", The Journal of the British Blockchain Association 1, S.2 (2018): 1-6.

Elliott, James. "Help-Somebody Robbed My Second Life Avatar!.", Journal of Virtual Worlds Research 1, S.1 (2008): 1-11.

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

Esener, Turhan ve Güven, Kudret. Eşya Hukuku. Ankara: Yetkin Yayınevi, 2015.

Esterik Plasmeijer, Pauline W.J. van and Raaij, W. Fred van. "Banking System Trust, Bank Trust, And Bank Loyalty.", International Journal of Bank Marketing 35, S.1 (2017): 97-111.

Etherscan. "Token Tracker." Erişim Tarihi: Ocak 27, 2021. https://etherscan.io/tokens.

Europe Banking Authority. Opinion on Virtual Currencies, 2014.

Europe Banking Authority. Report with Advice for the European Commission on Crypto-assets, 2019.

European Central Bank. "Electronic Money." Erişim Tarihi: Şubat 7, 2021. https://www.ecb.europa.Eu/stats/money_credit_banking/electronic_money/html/index.en.html.

European Central Bank. Virtual Currency Schemes - A Further Analysis, 2015.

European Central Bank. Virtual Currency Schemes, 2012.

European Parliament. Cryptocurrencies and Blockchain, 2018.

FATF. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019.

FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation the FATF Recommendations, 2020.

FATF. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, 2020.

FATF. Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014.

Ferwerda, Joras. The Multidisciplinary Economics of Money Laundering. Ridderkerk: Ridderprint, 2012.

Financial Conduct Authority. Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3, 2019.

Foley, Sean; Karlsen, Jonathan R. and Putninš, Talis J. "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?.", The Review of Financial Studies 32, S.5 (2019): 1798-1853.

Greeshma, K V. "Crypto Currencies and Cybercrime.", International Journal of Engineering Research & Technology (IJERT) 3, S.30 (2015): 1-5.

Güçlütürk, Osman Gazi. "Türk Hukukunda Kripto Varlıkların Para ve Elektronik Para Niteliğinin İncelenmesi.", Regesta Ticaret Hukuku Dergisi 4, S.3 (2019): 383-408.

Günay, Hamdi Furkan ve Kargı, Veli. "Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi.", Journal of Life Economics 5, S.3 (2018): 61-76.

HBV Türk Ceza Hukuku Uygulama ve Araştırma Merkezi. Türk Ceza Hukuku Mevzuatı Cilt I. Ankara: Seçkin Yayınevi, 2019.

He, Dong; Habermeier, Karl; Leckow, Ross; Haksar, Vikram; Almeida, Yasmin; Kashima, Mikari; Kyriakos-Saad, Nadim; Oura, Hiroko; Sedik, Tahsin Saadi; Stetsenko, Natalia and Verdugo-Yepes, Concepcion. Virtual Currencies and Beyond: Initial Considerations. IMF Staff Discussion Note, 2016.

Her Majesty's Treasury (HM Treasury). UK Regulatory Approach to Cryptoassets and Stablecoins: Consultation and Call for Evidence, 2021.

Hinman, William. "Digital Asset Transactions: When Howey Met Gary (Plastic)." (SEC transcribed speech, 14 Haziran 2018). Erişim Tarihi: Ocak 20, 2021. https://www.sec.gov/news/speech/speech-hinman-061418.

Huang, Sherena Sheng. "Crypto Assets Regulation in the UK: An Assessment of the Regulatory Effectiveness and Consistency.", Journal of Financial Regulation and Compliance 29, S.3 (2021): 336-351.

Hughes, Eric. "A Cypherpunk's Manifesto." Erişim Tarihi: Ekim 25, 2020. https://www.activism.net/cypherpunk/manifesto.html.

Hughes, Scott D. "Cryptocurrency Regulations and Enforcement in the U.S.", Western State Law Review 45, S.1 (2017): 1-28.

Ivaniuk, Viktoriia and Banakh, Serhiy. "Cryptocurrency-Related Cybercrimes in Ukraine.", OER Eastern Europe Law 66, S.1 (2020): 217-224.

Jeong, Sarah. "The Bitcoin Protocol as Law, and the Politics of a Stateless Currency." Erişim Tarihi: Kasım 18, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124.

Kaplanhan, Fatih. "Kripto Paranın Türk Mevzuatı Açısından Değerlendirilmesi "Bitcoin Örneği.", Vergi Sorunları Dergisi, S.353 (2018): 105-123.

Kappos, George; Yousaf, Haaroon; Maller, Mary and Meiklejohn, Sarah. An Empirical Analysis of Anonymity in Zcash. Proceedings of the 27th USENIX Conference on Security Symposium, 2018.

Karame, Ghassan O.; Androulaki, Elli and Capkun, Srdjan. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. Cryptology ePrint Archive IACR Report No.248. 2012, 1-17.

Kethineni, Sesha and Cao, Ying. "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity.", International Criminal Justice Review 30, S.3 (2020): 325-344.

Kethineni, Sesha; Cao, Ying and Dodge, Cassandra. "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes.", American Journal of Criminal Justice 43, S.2 (2017): 141-157.

Kfir, Isaac. "Cryptocurrencies, National Security Crime and Terrorism.", Comparative Strategy 39, S.2 (2020): 113-127.

Kien, Matthew and Ly, Meng. "Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies.", Harvard Journal of Law & Technology 27, S.2 (2014): 587-608.

Koca, Mahmut ve Üzülmez, İlhan. Türk Ceza Hukuku Genel Hükümler. Ankara: Adalet Yayınevi, 2020.

Kocasakal, Ümit. "Karapara Aklama Suçu." Doktora Tezi, İstanbul Üniversitesi, 2000.

Korver, Michele R.; Pelker, C. Alden and Poteat, Elisabeth. "Attribution in Cryptocurrency Cases.", United States Attorneys' Bulletin 67, S.1 (2019): 233-262.

Kostenko, Svitlana; Strilchuk, Vitalii; Chernysh, Roman and Buchynska Anna. "The Threats to National Security of Ukraine and Poland Inassisting to the Development of the Crypto-Asset Market: Legal Aspect.", Management Theory and Studies for Rural Business and Infrastructure Development 43, S.2 (2021): 225-236.

Kounelis, Ioannis. "Secure and Trusted Mobile Commerce System Based on Virtual Currencies." Doctoral Thesis, School of Information and Communication Technology Royal Institute of Technology, 2015.

Lee, Tyler C. "Decrypting Crypto: Issues Plaguing Today's Hottest Regulatory Nightmare.", New York University Journal of Law and Business 16, S.2 (2020): 551-578.

Maese, Vivian A.; Avery, Alan W.; Naftalis, Benjamin A.; Wink, Stephen P. and Valdez, Yvette D. "Cryptocurrency: A Primer, Banking Law Journal.", 133, S.8 (2016): 468-471.

Magizov, Rustem; Kuznetsov, Sergey; Garipova, Venera; Gilmanov, Muhamat; Kasatova, Anastasia and Kuznetsov, Aleksey. Criminal, Problems of Criminal Responsibility for Illegal Circulation of Cryptocurrency. 12th International Conference on Developments in eSystems Engineering, 996-999, 2019.

Magizov, Rustem; Kuznetsov, Sergey; Garipova, Venera; Gilmanov, Muhamat; Kasatova, Anastasia and Kuznetsov, Aleksey. Problems of Legal Regulation of Cryptocurrencies. 12th International Conference on Developments in eSystems Engineering. 956-959, 2019.

Mahmutoğlu, Fatih Selami. "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi.", İÜHFM 71, S.1 (2013): 855-889.

Marian, Omri. "Are Cryptocurrencies 'Super' Tax Havens?.", Michigan Law Review First Impressions 112, S.38 (2013): 38-48.

McDowell, John and Novis, Gary. "The Consequences of Money Laundering and Financial Crime.", An Electronic Journal of the U.S. Department of State 6, S.2 (2001): 6-8.

Mcginnis, John O. and Roche, Kyle. "Bitcoin: Order without Law in the Digital Age.", Indiana Law Journal 94, S.4 (2019): 1-56.

Moore, T. and Christin, N. "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," In Financial Cryptography and Data Security, ed. Ahmad-Reza Sadeghi, 25-33. Heidelberg: Springer-Verlag, 2013.

Mowbray, Miranda. "Implementing Pseudonymity.", SCRIPT-ed 3, S.1 (2006): 34-44.

Murphy, Edward V.; Murphy, M. Maureen and Seitzinger, Michael V. Bitcoin: Questions, Answers, and Analysis of Legal Issues. Congressional Research Service Report R43339, 2015.

Mutluoğlu, Derya. "Kripto Para Birimleri ve Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu." Yüksek Lisans Tezi, Ankara Üniversitesi, 2020.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 1-9. Erişim Tarihi: Kasım 27, 2020. https://bitcoin.org/bitcoin.pdf.

Nolasco Braaten, Claire and Vaughn, Michael S. "Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions.", Deviant Behavior 42, S.8 (2019): 958-978.

Oğuzman, M. Kemal; Seliçi, Özer ve Oktay Özdemir, Saibe. Eşya Hukuku. İstanbul: Filiz Kitapevi, 2014.

Orme, David. "Is Biometrics the Answer to Crypto-Currency Crime?.", Biometric Technology Today, S.2 (2019): 8-10.

Özgenç, İzzet ve Yurtlu, Fatih. "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçları Bakımından Teori ve Uygulamada Ortaya Çıkabilecek Sorunlara İlişkin Bir Değerlendirme." In 5. Türk-Kore Ceza Hukuku Günleri Karşılaştırmalı Hukukta Ekonomik Suçlar Uluslararası Sempozyumu Tebliğler Cilt II, ed. İzzet Özgenç, Cumhur Şahin, Faruk Turhan, 447-468. Ankara: Seçkin Yayınevi, 2020.

Pirinççi, Ayşe Esra. "Yeni Dünya Düzeninde Sanal Para Bitcoin'in Değerlendirilmesi.", Uluslararası Ekonomi Siyaset İnsan ve Toplum Bilimleri Dergisi 1, S.1 (2018): 45-52.

Reddy, Eveshnie and Minnaar, Anthony. "Cryptocurrency: A Tool and Target for Cybercrime.", Southern African Journal of Criminology 31, S.3 (2018): 71-92.

Rysin, Vitalii and Rysin, Mariia. "The Money Laundering Risk and Regulatory Challenges for Cryptocurrency Markets." In Restructuring Management Models-Changes-Development, ed. Marek Dziura, Andrzej Jaki, Tomasz Rojek, 187-201. Toruń: Dom Organizatora, 2020.

Sarıkatipoğlu, Mehmet Ata; Çapkın, Timur Arif ve Karaalioğlu, Fatma. "Bitcoin: Bir Sanal Para Birimi Olarak Regülasyonu ve Kara Para Aklanması Bakımından Durumu.", GSI Dergisi, (2015): 89-102.

Securities and Commodities Authority. The Chairman of the Authority's Board of Directors' Decision No. (23/ Chairman) of 2020 Concerning Crypto Assets Activities Regulation, 2020. Erişim Tarihi: Eylül 12, 2021, https://www.sca.gov.ae/Content/Userfiles/Assets/Documents /80041 51b.pdf.

Swartz, Lana. "What Was Bitcoin, What Will It be? The Techno- Economic Imaginaries of a New Money Technology.", Cultural Studies 32, S.4 (2018): 623-650.

Şahin, Muhammet. "Kripto Para Yeni Bir Vergi Sığınağı Mı? Bilişim Teknolojilerindeki Gelişmeler Temelinde Bir Değerlendirme.", Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, S.34 (2019): 169-181.

Şen, Ersan. "Bitcoin Çalınır mı?." Erişim Tarihi: 22 Ocak, 2021. https://www.haber7.com/ yazarlar/prof-dr-ersan-sen/1948163-bitcoin-calinir-mi.

Tarakçıoğlu, Zeynep Esra. "AİHM Kararları Işığında Suçta ve Cezada Kanunilik İlkesi." Yüksek Lisans Tezi, Galatasaray Üniversitesi, 2020.

Tezcan, Durmuş; Erdem, Mustafa Ruhan ve Önok, Murat. Teorik ve Pratik Ceza Özel Hukuku. Ankara: Seçkin Yayınevi, 2020.

The European Consumer Organisation (BEUC), Crypto Assets-BEUC Response to the Commission's Consultation, 2020.

Toroslu, Nevzat. Ceza Hukuku Özel Kısım. Ankara: Savaş Yayınevi, 2019.

Türkiye Bilişim Vakfı. Kripto Para ve ICO Raporu, 2020.

Tziakouris, Giannis. "Cryptocurrencies-A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective.", IEEE Security and Privacy Magazine 16, S.4 (2018): 92-94.

U.S Department of Justice. Cryptocurrency Enforcement Framework. Report of Attorney Generals Cyber Digital Task Force, 2020.

Ünlü, Ufuk. "Kara Para Aklamada Yeni Yöntemler ve Kara Paranın Ekonomi Üzerindeki Etkileri.", Sayıştay Dergisi, S.113 (2019): 155-179.

Üzer, Betül. "Sanal Para Birimleri." Uzmanlık Yeterlik Tezi, Türkiye Cumhuriyet Merkez Bankası Ödeme Sistemleri Genel Müdürlüğü, 2017.

Vasek, Marie and Moore, Tyler. "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk.", In Financial Cryptography and Data Security, ed. Ahmad-Reza Sadeghi, 1-17. Berlin, Heidelberg: Springer-Verlag, 2013.

Velkes, Gabrielle Chasin. "International Anti-Money Laundering Regulation of Virtual Currencies and Assets.", New York University Journal of International Law and Politics 52, S.3 (2020): 875-906.

World Bank Group. Distributed Ledger Technology (DLT) and Blockchain. FinTech Note No. 1, 2017.

Wright, Aaron and De Filippi, Primavera. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia.", SSRN Electric Journal, (2015): 1-58.

Yıldırım, Murat. "Blok Zincir Teknolojisi, Kripto Paralar ve Ülkelerin Kripto Paralara Yaklaşımları.", Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 10, S.20 (2019): 265-277.

Yılmaz, Sacit. "Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu.", Ankara Barosu Dergisi, S.2 (2011): 70-97.

Yurtlu, Fatih. "Terör Suçlarıyla Mücadelede Yeni Konsept: Önalan Suçları- BGH Kararları Işığında Almanya Örneği.", Selçuk Üniversitesi Hukuk Fakültesi Dergisi 29, S.3 (2021): 2169-2208.

Zaytoun, Henry S."Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft.", North Carolina Law Review 97, S.2 (2019): 395-431.

Zimba, Aaron; Wang, Zhaoshun; Mulenga, Mwenge and Odongo, Nickson Herbert. "Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security.", Journal of Computer Information Systems 60, S.4 (2020): 297-308.