BLOKZİNCİR-KRİPTO VARLIK BAĞLANTILI YAYGIN SAHTEKARLIK TÜRLERİNİN DOLANDIRICILIK VE İLİŞKİLİ SUÇLAR YÖNÜNDEN ANALİZİ

(Araştırma Makalesi)

DOI: https://doi.org/10.33717/deuhfd.1375575

Arş. Gör. Dr. İsa BAŞBÜYÜK [*]

Öz

Blokzincir, akıllı sözleşme ve kripto varlıklar gibi teknolojik gelişmeler, bir taraftan kullanıcıların elektronik ortamda anonim ve aracısız işlem yapabilmesini mümkün kılarken, diğer taraftan malvarlığını hedef alan sahtekarlıkların işlenme yöntemine yeni bir boyut kazandırmıştır. En yaygın şekliyle "sözde kripto para borsaları, sahte kripto varlıklar, likidite boşaltma, fiyat manipülasyonu girişimleri, sözde yatırım ve madencilik uygulamaları" formunda karşılaşılan bu tarz sahtekarlıklar genelde dolandırıcılık suçuyla birlikte anılmaktadır. Ancak kripto varlık alanındaki yenilikçi vakıalar, yanlış beyan veya asılsız vaatlerle mağduru kandırarak menfaat sağlamaya ikna etmeyi yasaklayan Türk Ceza Kanunu m. 157'de tanımlanan dolandırıcılık suçunun kapsamını tartışmaya açmakta ve yeni düzenleme ihtiyacını gündeme getirmektedir. Bu çalışmanın konusu, öncelikle kripto varlık bağlantılı sahtekarlık olaylarını analiz edip, ortaya çıkış şekillerine göre sınıflandırmak; sonrasında ise sahtekarlık türü özelinde TCK m. 157'de düzenlenen dolandırıcılık suçunun uygulanabilirliğini test etmektir. Böylece dolandırıcılık suçunu tanımlayan düzenlemenin kripto varlık bağlantılı sahtekarlıklarla mücadelede yetersiz kaldığı noktaları ortaya çıkarmak ve yeni düzenlemede bulunması gereken özelliklere dikkat çekmek amaçlanmaktadır.

Anahtar Kelimeler

Kripto varlık, Dolandırıcılık, Manipülasyon, Sahtecilik, Bitcoin madenciliği, Kripto para borsası, Likidite havuzu, Metaverse dolandırıcılığı

[*] Dokuz Eylül Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, İzmir (isa.basbuyuk@gmail.com) ORCID: 0000-0002-6432-1909 (Geliş Tarihi: 15.08.2023-Kabul Tarihi: 25.09.2023) *Yazar, eserinin Derginize ait bilimsel etik ilkelere uygun olduğunu taahhüt eder.*

ANALYZING COMMON BLOCKCHAIN AND CRYPTOCURRENCY-RELATED SCAMS UNDER THE FRAUD AND RELATED OFFENCES

(Research Article)

Abstract

Technological developments such as blockchain, smart contracts, and crypto assets, on the one hand, enable internet users to transact anonymously and decentralized on the other hand they added a new dimension to the method of scams against the property. Such scams, which are most commonly known as "fake cryptocurrency exchange, scam coins, rug pull, pump-and-dump, investment and mining scam" are often associated with the crime of fraud. However, innovative cases in the cryptocurrency space bring the scope of the fraud offense under the Turkish Criminal Code (Art. 157), which prohibits deceiving a person and persuading him/her to benefit through misrepresentations or false promises, into question and reminds about the needs for new regulation. For these reasons, the subject matter of this study is primarily to analyze and classify cryptocurrency-related scams, and then to test the adeptness of fraud definition in the Turkish Criminal Code to these cases. Thus, it is aimed to reveal the inability of traditional fraud definition in fighting crypto-related scams and to draw attention to the features that should be found in the new regulation.

Keywords

Cryptocurrency, Fraud, Scams, Market manipulating, Bitcoin mining, Cryptocurrency exchange, Liquiditiy pool, Metaverse fraud

I. HUKUKİ SORUN, KONU VE KAPSAM

A. Sorunun Tespiti ve Başlık Tercihi

Literatürümüzde çeşitli yönleriyle ele alınan kripto varlıkların, malvarlığına yönelik saldırılarda araç olarak kullanılabileceği ve dolandırıcılık suçuna *konu* edilebileceği yeni bir mesele değildir[1]. Ancak kripto varlık bağlantılı haksızlıkların, *gerçekleşme şekli itibariyle* dolandırıcılık suçunun *fiil unsurunu* karşılayıp karşılamayacağı ise haricen ele alınması gereken güncel ve önemli bir meseledir.

Açmak gerekirse, doğrudan eşler arasında işlem yapabilme ve otonom kayıt tutabilme imkânı sunan blokzincir teknolojisi, elektronik kayıtların işlenmesinde yöntemsel değişikliğe yol açarken, aynı zamanda bu kayıtların temsil ettiği değerin muhafazası, işletilmesi ve transferinde "yeni durumlar" yaratmıştır. Elektronik ortamda işlem yapma alışkanlıklarını değiştiren blokzincir teknolojisindeki yenilikçi tarz, kripto varlık bağlantılı haksızlıkların işleniş şekillerine de yansımaktadır. Özellikle, dolandırıcılık suçuyla birlikte anılan bazı kripto varlık bağlantılı sahtekarlıklarda; i) haksızlığın tamamen elektronik ortam üzerinden aracısız gerçekleştirilebilmesi, ii) belirsiz sayıdaki kullanıcı kitlesinin farklı yöntemlerle hedef alınabilmesi ve ikna sürecinin basitleşmesi, iii) ekonomik değerin temsil eden özel anahtarlara yönelmesi, iv) yararın ne şekilde faile geçtiğinin önemini yitirmesi dikkat çekicidir.

Oysa, bir ekonomik değerin muhafazası, sahipliği ve kaybına dair sürecin kendisi, *mağdurun durumunu* ve *yarar geçişini* unsur olarak düzenleyen dolandırıcılık suçuna ilişkin tipe uygunluk değerlendirmesinde belirleyici rol oynamaktadır. Dolayısıyla malvarlığını hedef alan kripto varlık bağlantılı haksızlıkların, ***hangi biçimlerde ortaya çıktığı*** ayrıntısıyla ortaya konularak; bunların ***a) fiil unsuru itibariyle*** mevcut dolandırıcılık suçuna uyup

---

[1] **Aktolga Öztürk**, Ayça: "Kripto Paralara İlişkin Dolandırıcılık Yöntemleri", Finans Hukuku ve Gündemi Dergisi, Sayı 3, Şubat 2020, (https://www.kanunum.com/file/cid9721408_vid18006506_fid1042080); **Aksoy Retornaz**, E. Eylem: "Ceza Hukuku Perspektifinden Blokzincir", Gelişen Teknolojiler ve Hukuk I - Blokzincir ve Hukuk, 2. Baskı, İstanbul 2021, s. 302; **Tahan**, Özge: "Kripto Paraların Türk ve Alman Ceza Hukuku Düzenlemeleri Yönünden Değerlendirilmesi" Suç ve Ceza Dergisi, C: 14, S: 1, 2021, s. 136. **Balcı**, Murat/**Çakır**, Kerim: "Kripto Para Dolandırıcılığı", Terazi Hukuk Dergisi, 16(181), s. 1684; **Tarakçıoğlu**, Esra: "Kripto Varlıklar ve Ceza Hukuku Sorumluluğu", Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, Cilt 11, Sayı 2, Aralık 2021, s. 334; **Sarıkaya**, Samet, "Kripto Varlık Dolandırıcılığı", Anadolu Üniversitesi Hukuk Fakültesi Dergisi, Cilt 9, Sayı 2, Temmuz 2023, s. 567.

uymadığı; uymadığı hallerde ***b) bağlantılı suçların*** boşluğu ne ölçüde doldurabileceği incelenmeli; böylece bu tür haksızlıklarla etkili mücadelede ***c) ihtiyaç duyulan düzenlemenin temelde hangi özellikleri barındırması*** gerektiği güncel bir mesele olarak tartışılmak durumundadır.

Tanımını TCK m. 157'den alan dolandırıcılık suçu, unsurları itibariyle malvarlığına yönelen aldatıcı girişimler içerisinde daha dar bir alanı işaret ettiğinden, başlıkta "*kripto varlık dolandırıcılığı"* ifadesi tercih edilmemiştir. Bunun yerine "*kripto varlık bağlantılı sahtekarlık*" ifadesi kullanılarak, hem kripto varlık piyasasındaki aldatma temelli haksızlıkların tipiklik sınırına takılmadan bütün halinde ele alınması hem de dolandırıcılık suçunun hangi tür sahtekarlıklarda niçin yetersiz kaldığının ortaya konulması amaçlanmıştır.

B. Konu ve Kapsam Sınırlaması

Blokzincir teknolojisinin aracılık faaliyetlerini azaltması ve işlem ücretlerini düşürmesi sebebiyle farklı sektörlere entegrasyonu yüksek ihtimaldir[2]. Bu çerçevede, günümüzde öne çıkan blokzincir ve kripto varlık bağlantılı sahtekarlıkların icra yöntemlerinin çalışma konusu yapılması, hem mevcut düzenlemelerin ne ölçüde etkili koruma sağlayacağını ortaya koymak hem de tipiklik sorunlarını çözmeye yönelik düzenlemenin kıstaslarını belirlemek adına önem arz etmektedir. Çalışma kapsamında i) blokzincir ve kripto varlıklarla bağlantılı yaygın sahtekarlıklar, ortaya çıkış şekillerine göre ayrı başlıklar halinde sınıflandırılacak, ii) her bir sahtekarlık türü özelinde, dolandırıcılık ile bağlantılı suçların çözümsüz bıraktığı noktalara değinilecek ve iii) tamamen elektronik ortamda icra edilen bu haksızlıklar karşısında nasıl bir düzenlemeye ihtiyaç duyulduğuna dikkat çekilecektir. Konu ve makale kapsamını aşmamak adına, blokzincirle bağlantılı genel hususların açıklanması[3] ve değinilen olaylardaki nitelikli hal, iştirak, içtima, teşebbüse ilişkin meseleler inceleme dışı bırakılmıştır.

Aslında, TCK bakımından elektronik ortamda işlenen dolandırıcılık fiillerinin bağımsız bir suç olarak düzenlemesi meselesi, kripto varlıklarla

---

[2] Pratikte birtakım güçlükler olmakla birlikte, blokzincirin enerji, tıp, finans alanı dışında, üretim endüstrisinde de kullanılabileceğini gösteren inceleme için **Zhang**, Qiang/**Liao**, Baoyu/**Yang**, Shanlin: "Application of blockchain in the field of intelligent manufacturing", Frontiers of Engineering Management, Volume 7, 2020, 578-591, s. 582 vd.

[3] Örnek ayrıntılı inceleme için bkz. **Balcı**, Umut: "Kripto Paraların Ceza Hukuku Boyutu ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri", TBBD, 2021 (155), s. 206 vd.

sınırlı değildir[4]. Ancak, bu ihtiyaç kripto varlık piyasasında daha da hissedilir hale gelmiştir. Bu nedenle, aşağıda kripto varlık bağlantılı sahtekarlıkların ortaya koyduğu koşulları TCK m. 157 etrafında inceleyerek, dile getirdiğimiz sorunu *olgusal boyutuyla* analiz etmeye gayret edeceğiz. Konunun *normatif boyutuna* ilişkin olarak, elektronik ortamda işlenen (=bilgisayar) dolandırıcılığının kapsamını ise karşılaştırmalı hukuktaki düzenlemeler ışığında, ayrı bir tamamlayıcı çalışmada ele alacağız.

C. İçerik ve Plan

Çalışmamız üç kısım ve sonuçtan oluşmaktadır: İlk kısım, iki numaralı ***(II)*** başlıkta, kripto varlık, dağıtık defter ve blokzincir teknolojileri arasındaki temel bağlantı ile dolandırıcılık suçunu hangi yönleriyle ilgilendirdiği hususlarında açıklama yapılacaktır.

İkinci kısım, üç numaralı ***(III)*** başlıkta, "***kripto varlıklarla ilişkili sahtekarlık yöntemleri"*** Türkiye dahil tüm dünyadan örnekler üzerinden alt başlıklarda sınıflandırılmıştır. Bu kapsamda, ***(A)*** kripto para borsası sahtekarlıkları kapsamında hayali borsacılık ve cüzdan boşaltma fiilleri; ***(B)*** kripto para birimleri özelinde sahtecilik fiilleri; ***(C)*** akıllı kontratlar aracılığıyla işletilen likidite havuzlarını boşaltma (rug pull) fiilleri; ***(D)*** yanlış ve yanıltıcı bilgilerle kripto varlık arzı (ICO dolandırıcılığı); ***(E)*** fiyat manipülasyonu (pump-and-dump); ***(F)*** sahte madencilik ve sözde kazanç uygulamaları; ***(G)*** sanal ortama ilişkin sahtekarlıklar (metaverse dolandırıcılığı) icra yöntemleri açıklanarak, dolandırıcılık ve bağlantılı suçlar kapsamında incelenmiştir.

Üçüncü kısım, dört numaralı **(IV)** başlıkta, genel olarak "**özellik arz eden meseleler"** irdelenmiştir. Bunlar arasında, ***(A)*** amaçsız ve faydasız kripto varlıkların (Shitcoin/memecoin) durumu; ***(B)*** kripto varlık piyasasındaki riskin bilinirliğinin mağduriyete etkisi; ***(C)*** hileyle kripto varlık cüzdan anahtarının ele geçirilmesinin tipikliğe etkisi; ***(D)*** ponzi ve piramit satış usullerinin bu tarz sahtekarlıklar içerisindeki yeri üzerinde durulmuştur. Nihayet beş numaralı **(V)** başlıkta ise ele alınan sorunla ilgili ihtiyaç duyulan düzenleme hakkındaki görüşümüze yer verilerek çalışma sonlandırılmıştır.

---

[4] Türk Ceza Kanunu'nda, yetkisi olmadığı halde, başkasına ait internet bankacılığı uygulamasını kullanmaya ve bu suretle haksız yarar elde etmeye yönelik fiilleri karşılayan bir hüküm olmadığı hususundaki inceleme için bkz. **Başbüyük**, İsa: "İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi", Ceza Hukuku Dergisi, Sayı:21 - Nisan 2013.

II. KAVRAM VE İLİŞKİLENDİRME

A. İlgili Kavramlar ve Hukuki Nitelik

Kripto varlık bağlantılı sahtekarlıklar, dağıtık kayıt tutan blokzincir ağının inşasından, akıllı sözleşmelerin yazımı ve her türlü kripto varlığın üretim ile piyasa sürülmesi aşamasına kadarki süreçte kendini gösterebilmektedir. Kripto varlık, blokzincir ve dağıtık defter teknolojileri elektronik bir sistemin (=elektronik ağ) bütününü izaha yarayan, birbirlerini tamamlayan yakın bağlantılı kavramlardır. Bu bakımdan, her üç kavramın bir bütün halinde kısaca izah edilmesinde fayda bulunmaktadır.

Dağıtık defter/ağ teknolojisi, birden çok bilgisayarın merkezi sunucuya gerek kalmaksızın bir araya gelip, eşler arasında (peer-to-peer, P2P) doğrudan işlem yapabilmesine imkân tanıyan bir elektronik ağdır[5]. İşlem kayıtları doğrudan ağ üzerinde tutulmakta ve ağdaki işlem güvenliği katılımcı bilgisayarların "uzlaşmaları" üzerinden sağlanmaktadır[6]. ***Blokzincir (=Blockchain)*** ise dağıtık ağda gerçekleştirilen işlemeleri, kriptografi ve algoritma yöntemlerini kullanarak güvenli ve eşzamanlı bir şekilde kayıt altına alabilen veri tabanı teknolojisidir[7]. Geleneksel veri tabanlarından tamamen farklı sistemle çalışan Blokzincir, işlem kayıtlarını satır, sütun, tablo ve dosya usulü depolamak yerine, dijital olarak birbirine şifrelenerek (hash fonksi-yonu), -değiştirilmeyi ve mükerrer harcamayı engellemek üzere-, zincirlenmiş bloklara kaydeder[8].

Kripto varlık blokzincir ağındaki işlemlerde kullanılmak üzere, şifreleme teknolojisiyle oluşturulan ve ölçü bildiren sanal belirteçlerdir. Sanal belirteçlerin ilki olan Bitcoin, bağlı bulunduğu Bitcoin Blokzinciri'nde elektronik-nakit ödeme aracı olarak kullanılmak üzere tasarlandığından, başlarda *kripto para* ifadesi tercih edilmiş; ancak, işleyişin zamanla çeşitlenmesiyle piyasadaki bütün belirteçleri tanımlamak adına kripto varlık ifadesi ağırlık kazanmıştır. Günümüzde kripto varlıklar, bağlı bulundukları blokzincir

---

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

6 Word Bank Group, DTL, s. 6.

7 Word Bank Group, DTL, s. 6.

8 Saldırganın, örneğin harcadığı parayı haksız şekilde geri alabilmesi için hem değiştirilecek bloğu tespit edilebilmesi hem sıradaki bloğun bulabilmesi hem de piyasadaki işlemlere bağlı gittikçe artan zincir hızını yakalayarak alternatif zincir oluşturabilmesi gerekmektedir. Sayılan üç olasılığın gerçekleşme ihtimalinin imkansıza yakın olduğu iddia edilmektedir (bkz. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, s. 6).

ağında *ödeme fonksiyonunu yerine getirenler -örneğin Bitcoin, Ether-* ***kripto para birimi (coin)****;* bir blokzincir ağına inşa edilen platformlar tarafından kendi amaçları doğrultusunda üretilmiş olanlar ise *-örneğin DAI, SAND-* ***kripto jeton (token)*** olarak alınmakta; bunlar da üretilme amaçlarına göre varlığa dayalı jetonlar, hizmet ve menkul kıymet jetonları şeklinde ayrıma tabi tutulmaktadır[9]. İnternet bağlantısına sahip kullanıcılar tarafından kolaylıkla alım-satıma konu edilebilen kripto varlıklar, türüne ve fonksiyonuna bakılmaksızın, spekülatif yatırım aracı olarak piyasalardaki varlığını sürdürmeye devam etmektedir.

Kripto varlıkların ihtilaf konusu olması halinde, hukuken "eşya" gibi mi yoksa "salt ekonomik değer" olarak mı korunması gerektiği hususunda uzlaşı sağlanabilmiş değildir[10]. Ancak, kripto varlıkların taşıdıkları ekonomik değer itibariyle malvarlığına dahil olduğu noktasında önemli bir itiraz bulunmamaktadır. Bu nedenle, kripto varlıkların hukuki niteliğine ilişkin tartışma dolandırıcılık gibi, malvarlığını konu edinen suçlar yönünden etki doğurmamaktadır[11]. Kaldı ki, hâkim yaklaşıma göre, hukuk korumasının dışında kalmayan ve ekonomik kıymeti bulunan değerlerin bütünü malvarlığı kapsamında ceza hukuku korumasına dahildir[12]. Kripto varlıkların üretilmesi ve ticareti yasak olmadığı gibi, piyasadaki arz-talep ölçüsünde fiyatlandığı açıktır. Eylemin gerçekleştiği sırada ekonomik değer taşıyan kripto varlıkların sanal niteliği "malvarlığı değerlerini" konu edinen dolandırıcılık ve bağlantılı suçların tatbikine engel değildir. Bizce asıl sorun, sahtekarlığın

---

9 Kripto varlıkların sınıflandırılmasına dair inceleme için bkz. **Oliveira**, Luis/**Zavolokina**, Liudmila/**Bauer**, Ingrid/**Schwabe**, Gerhard: "To Token or not to Token: Tools for Understanding Blockchain Tokens", In: International Conference of Information Systems (ICIS 2018), San Francisco, USA, 12-16/12/2018, ICIS, s. 5.

10 Bu konudaki mahkeme kararları ve görüşlere ayrıntılı yer veren çalışma için bkz. **Sarel**, Roee. "Property Rights in Cryptocurrencies: A Law and Economics Perspective." North Carolina Journal of Law & Technology, vol. 22, no. 3, April 2021, s. 417 vd. Türk hukukuna yönelik inceleme için bkz. **Bilgili**, Fatih/**Cengil**, M. Fatih: "Bitcoin Özelinde Kripto Paraların Eşya Niteliği Sorunu", SSRN, 2019, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432713), s. 12 vd.; **Özdemir**, Gençer: "Kripto Paraların Eşya Niteliği", SDÜHFD, Cilt 11, Sayı 1, 2021, s. 297 vd.

11 Kıyas için bkz. **Aksoy Retornaz**, s. 302; **Tarakçıoğlu**, s. 336; **Kapancı**, Kadir Berk: "Özel Hukuk Penceresinden Blokzincir: Sanal Para Değerleri ve Akıllı Sözleşmeler Üzerine Değerlendirmeler", Gelişen Teknolojiler ve Hukuk 1- Blokzincir, On İki Levha Yayıncılık, İstanbul 2020, s. 120.

12 Ceza hukuku tarafından korunması gereken malvarlığın kapsamına ilişkin benimsenen yaklaşım hakkında bkz. **Wessels,** Johannes/**Hillenkamp**, Thomas: Strafrecht BT 2, 39. Aufl. 2016, kn: 532; **Cramer**, Peter/**Perron**, Walter: S/S-StGB § 263, 29. Auflage, München, 2014, Kn: 84; **Ekici Şahin**, Meral: Dolandırıcılık Suçu, Ankara 2019, s. 115.

icra şekli itibariyle suçun eylem unsuruna uygunluğunda ortaya çıkmaktadır. Dolayısıyla, dolandırıcılık suçunun eylem unsurunun yarattığı kısıtlamaya kısaca değindikten sonra, bu sahtekarlıkların işleyişine ve özelliklerine yakından bakma ihtiyacı duyulmaktadır.

Kripto varlık bağlantılı sahtekarlıklar gerek kripto para birimleri gerekse de kripto jetonları konu edilebilir. Kripto para birimi ile kripto jetonların üretimi, kullanım alanı ve kullanıcıya ulaştırılma şeklindeki farklılık, bunlarla bağlantılı sahtekarlık vakıalarının işleyişine de yansımaktadır. Bu nedenle, *kripto para birimi sahteciliğine* ayrı başlıkta yer verilmiştir. Nihayet, sahtekarlığın diğer türlerinde adından söz ettiren kripto para borsası, likidite havuzu, kripto varlık arzı, kripto varlık cüzdanı, metaverse, shitcoin/memecoin gibi önem az eden diğer kavramlar ise ilgili başlık altında ve lüzumlu olduğu ölçüde açıklanacaktır.

B. Konunun Dolandırıcılık Suçunun "Fiil Unsuruyla" İlişkisi

Kripto varlık bağlantılı sahtekarlık girişimlerinin temel motivasyonu sahte uygulama, sözde girişim ve gerçeğe aykırı açıklamalarla yatırımcıları hataya düşürerek, haksız kazanç elde etmektir. Bu sebeple, kripto varlık bağlantılı sahtekarlık olaylarının çeşitli içerik ve yayınlarda dolandırıcılık suçuyla (=*fraud, scam* gibi)[13] birlikte anılması oldukça olağandır. Ayrıca, yabancı basın ve kurumlar, kripto varlıklarla ilgili gündeme gelen her türlü aldatıcı girişimi "kendi mevzuatlarına uygun olarak" dolandırıcılık suçuyla ilişkilendirebilmektedir. Bu alanda yoğun mücadele yürüten Amerikan uygulaması, niteliği fark etmeksizin her türdeki kripto varlık bağlantılı sahtekarlıkları kablolu veya kablosuz iletişim ortamında işlenen *dolandırıcılık*[14] *(=18. U.S.C. §§ 1343, wire fraud)* kapsamında görmektedir[15]. Söz konusu

---

13 Karşılaştırınız "Common cryptocurrency scams and how to avoid them", Kaspersky, (https://www.kaspersky.com/resource-center/definitions/cryptocurrency-scams); "Yaygın olarak görülen kripto para birimi dolandırıcılıkları ve bunlardan kaçınma", Kaspersky, (https://www.kaspersky.com.tr/resource-center/definitions/cryptocurrency-scams); Benzer şekilde bkz. **Altınöz**, Utku/**Altınöz**, Hasip: Hile Ekonomisi, Piyasalarda Yatırımcı Psikolojisi ve Finansal Skandallar, 2. Baskı, Ankara 2020, s. 152.

14 Suçun unsurları hakkında açıklama için bkz. **Doyle**, Charles: "Mail and Wire Fraud: A Brief Overview of Federal Criminal Law", Congressional Research Service, CRS REPORT, 11.02.2019, s. 3.

15 Bu konudaki en güncel haber için bkz. **McGinley**, Ian: "Wire fraud: the most powerful law in crypto right now", Routers, 23.08.2022, (www.reuters.com/legal/legalindustry/wire-fraud-most-powerful-law-crypto-right-now-2022-08-23/). Ayrıca, aşağıda değineceğimiz Amerika Birleşik Devletler menşeili sahtekarlık örneklerinde de, gerekli yasal sürecin "wire fraud" üzerinden işletildiği görülmektedir.

dolandırıcılık türünde, aldatıcı planı icra eden failin suça konu yararı mağdurun tasarrufuyla ele etmek zorunda olmaması[16] ve suçun tamamlanması için mağdurda aktüel bir zarar meydana gelmesinin aranmaması[17] suç tipini daha esnek hale getirmektedir. Bu durum, iletişim dolandırıcılığı düzenlemesinin kripto varlık bağlantılı sahtecilikleri kapsama ihtimalini -en azından Yüksek Mahkeme bu hususdaki görüşünü ortaya koyana kadar- oldukça yükseltmektedir. Yine, haksız yarar elde etmek amacıyla bilgisayar ortamında gerçeğe aykırı program oluşturmak; gerçeğe aykırı, eksik veya izinsiz veri kullanmak; veri işleme sürecine müdahalede bulunmak suretiyle malvarlığı zararına yol açan girişimlerini cezalandıran Alman Ceza Kanunu (StGB) § 263a'daki bilgisayar dolandırıcılığı düzenlemesi, hataya dayalı tasarruf unsurunu aramadığı için, temel dolandırıcılık suçuna (StGB 263) kıyasen daha geniş bir hareket alanı sunmaktadır[18].

Oysa Türk hukukunda dolandırıcılık suçu, temel şekli itibariyle sıkı şartlara bağlandığından, mal varlığını hedef alan kripto varlık bağlantılı aldatıcı girişimlerin çeşitliliği karşısında kapsam sorunu yaratmaya açıktır. Nitekim, *"Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişi*"den söz eden TCK m. 157'deki aldatıcılık (=hile), dolandırıcılık suçunun tek belirleyici unsuru değildir[19]. Buna göre dolandırıcılık suçunun oluşması, hileli hareketle ***i)*** muhatabın hataya düşürülmesi, ***ii)*** hataya düşen mağdurun tasarrufta bulunması, ***iii)*** tasarruf sonucunda zarar meydana gelmesi, ***iv)*** oluşan bu zararın fail açısından yarar teşkil etmesi şeklinde birbirine neden-sonuç ilişkisiyle bağlı unsurların gerçekleşmesine bağlıdır[20].

Haliyle hukukumuz açısından, blokzincir ve kripto varlık bağlantılı sahtekarlıklar, yatırımcısını hataya düşürdüğü ve zarara yol açacak bir tasar-

---

16 **Doyle**, s. 6. Ayrıca bkz. *Ciminelli v. United States*, S. Ct. No. 21-1170 (U.S. May. 11, 2023), s. 16.

17 **Doyle**, s. 5, dn: 34.

18 **Wessels/Hillenkamp**, BT, § 13, Kn: 602.

19 Bu hususta suç tipiyle ilgili açıklamalar için bkz. **Ekici Şahin**, s. 185 vd.; **Özbek**, Veli Özer/**Doğan**, Koray/**Bacaksız**, Pınar: Türk Ceza Hukuku Özel Hükümler, 17. Baskı, Ankara 2022, s. 727 vd.; **Tezcan**, Durmuş/**Erdem**, Mustafa Ruhan/**Önok**, Rıfat Murat: Teorik ve Pratik Ceza Özel Hukuku, 20. Baskı, Ankara 2020, s. 891; **Eker Kazancı**, Behiye/**Zeyrek**, İlker: "TCK'da Dolandırıcılık Suçu", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, Cilt 21, Özel Sayı, 2019, s. 525.

20 **Kangal**, Zeynel: "Dolandırıcılık Suçu, Özel Ceza Hukuku Cilt IV, Malvarlığına Karşı Suçlar, On İki Levha Yayıncılık, İstanbul, 2018, s. 263; **Ekici Şahin**, s. 201; **Başbüyük**, İsa: Dolandırıcılık Suçunda Hile Unsuru, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Doktora Tezi, 2019, s. 101.

rufa sevk ettiği ölçüde dolandırıcılık suçu başlığı altında incelenebilecek; bu kalıba uymayan vakıaların cezalandırılabilirliği ise tartışmaya yol açacaktır. Tipiklik tartışmasının, süreç itibariyle nereden kaynaklanabileceği, aşağıda her bir sahtekarlık türü özelinde gösterilmeye çalışılmıştır.

III. KRİPTO VARLIK İLİŞKİLİ YAYGIN SAHTEKARLIK TÜRLERİNİN DEĞERLENDİRİLMESİ

A. Kripto Varlık Platformları Aracılığıyla İşlenen Sahtekarlıklar: Hayali Borsa Uygulamaları ve Cüzdan Boşaltma

1. Ortaya Çıkış Şekli

Kripto varlıkların alım-satımına aracılık etmek üzere hizmet veren çevrim içi platformlar, hukuki nitelikleri tartışmaya açık olsa da, günümüzde halen en yaygın ifadesiyle "***kripto para borsası***"[21] olarak anılmaktadır. Bunlar çalışma usulüne göre, temelde *merkezi yapıdaki* ve *merkeziyetsiz kripto para borsaları* olmak üzere temelde ikili ayrıma tabi tutulmaktadır[22]. Bu başlık altındaki sahtekarlık vakıaları, kullanıcıların bakiyelerini kendi bünyesinde tutan merkezi yapıdaki borsalarda ortaya çıkmaktadır. Merkezi yapıdaki borsalar, en kısa tanımıyla, internet bağlantısına sahip herkesin blokzincir ağına bağlanma zahmetine girmeden, kolay ve güvenli yoldan kripto varlık ticareti yapabilmesi için gerekli alt yapıyı sunan -Binance, FTX, Coinbase gibi[23]- *aracı* kuruluşlardır[24]. Ancak bu tür borsalarda kullanıcı açısından bazı riskler bulunmaktadır: *İlk olarak,* kullanıcılar hesap açtıkları borsa platformuna tek taraflı güvenmek durumundadır. *İkincisi*, sermaye ve lisans koşulunun aranmaması, bu platformların kurulmasını

---

21 Bu tabir, doğrudan kripto varlık alım satımına aracılık eden teşebbüsleri işaret eden ticari tabir haline geldiğinden, biz de çalışmamızda "kripto para borsası" ifadesini kullanmayı tercih ediyoruz.

22 Her iki borsanın özelliğini barındıranlar hibrit borsa şeklinde anılmakta olup, kripto para borsaların tür ve çalışma prensipleri hakkında bilgi için bkz. **Danial**, Kiana: "3 Different Types Of Cryptocurrency Exchanges: CEX, DEX, And Hybrid", Nasdaq, 12.07.2018, (www.nasdaq.com/articles/3-different-types-cryptocurrency-exchanges-cex-dex-and-hybrid-2018-07-12,); **Satsuk**, Pavel: "Types of Cryptocurrency Exchanges", soft-fX, (www.soft-fx.com/blog/types-of-cryptocurrency-exchanges/).

23 Piyasanın önde gelen kripto para borsaları için bkz. https://coinmarketcap.com/rankings/exchanges/.

24 **Reiff**, Nathan: "What Are Centralized Cryptocurrency Exchanges?", Investopedia, 27.08.2021, (https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/).

kolaylaştırmaktadır[25]. Lisans alma zorunluluğu kabul edilse de[26], *üçüncüsü*, çevrim içi olma özekleri dolayısıyla, kripto para borsaları, kötü niyetli işletmecilerin suiistimaline her zaman açıktır. Bu riskler, gündemden düşmeyen kripto para borsası sahtecilikleri için uygun zemin hazırlamıştır[27].

Kendisini **BitKRX** olarak adlandıran sözde kripto varlık platformu, güya Güney Kore'nin en büyük Bitcoin borsası KRX'in şubesi olduğu reklamıyla çok sayıda kişinin üye olmasını sağlar. Ancak, bir süre sonra BitKRX hesaplarındaki yatırımcılara ait varlıkların yok olmasıyla gerçek ortaya çıkar[28]. Benzer sahtekarlık ülkemizde, **Thodex skandalıyla** adını duyurur. Kripto varlık alım satımına aracılık etmek üzere 2017 yılında kurulan Koineks adlı şirket, 2020 yılında Türkiye merkezli global pazara açılan ilk kripto para borsası olarak ismini Thodex şeklinde değiştirir[29]. Şirket 2021 yılının başından itibaren çeşitli kampanya ve yüksek miktarlardaki promosyon vaatleriyle ilgi toplar. Aynı yıl 15 Mart ve 15 Nisan tarihleri arasında her yeni kullanıcıya hediye Dogecoin vaadi, kampanyaların en dikkat çekicisidir. Ancak, 19 Nisan'da kullanıcılardan, hesaplarındaki varlıklara erişememe şikayetleri yükselirken; cevaben borsa cüzdanlarının saldırıya uğradığını ve ödeme güçlüğüne düştüklerini açıklayan şirket yetkilileri, 20 Nisan 2021 tarihinde uygulamayı tamamen kapatır[30]. Durumdan şüphelenen kulla-

---

25 BDDK tarafından, 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamında gözetim ve denetiminin mümkün olmayacağı açıklanmıştır (bkz. BDKK'nın 2013/32 sayı, 25.11.2013 tarihli Basın Acıkması, www.bddk.org).

26 Konu tartışmalı olmakla birlikte, Amerika Birleşik Devletleri'nde kripto varlık platformlarının Amerikan Menkul Kıymetler Komisyonu'ndan (=SEC) lisans alarak faaliyette bulunmasını aramaktadır. Güncel durumu yansıtan açıklama için **Gensler**, Chair Gary: "Prepared Remarks of Gary Gensler On Crypto Markets Penn Law Capital Markets Association Annual Conference", U.S. SECURITIES AND EXCHANGE COMMISSION, Speech, 04.04.2022, (https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422).

27 Sahte kripto para platformlarının listesi için bkz. "A List of Fake Crypto Websites & Trading Platforms 2022", Trend Micro, https://news.trendmicro.com/2022/01/31/a-list-of-fake-crypto-websites-trading-platforms-2022/.

28 **"Rising Scams in Cryptocurrency and DeFi Projects You Should Know"**, Blockchain Magazine, (https://blockchainmagazine.net/rising-scams-in-cryptocurrency-and-defi-projects-you-should-know/).

29 **"Cryptocurrency Exchange THODEX Starts Worldwide User Recruitment"**, 24.12.2020, Yahoo Finance, (https://finance.yahoo.com/news/cryptocurrency-exchange-thodex-starts-worldwide-155200636.html).

30 Thodex yatırımcılarının mağduriyetiyle sonuçlanan sürecin işleyişi hakkında bkz. **Özen**, Ercan/**Vurur**, N. Sertap: "Digital Era Digital Risks: The Case Study of Turkish Crypto

nıcılar, platform yöneticileri hakkında suç duyurusunda bulunur. 2 milyar dolarlık "**kripto para dolandırıcılığı"** iddiasıyla başlatılan soruşturmada, Thodex üzerinden binlerce kişiyi dolandırdığı gerekçesiyle kırmızı bültenle aranan şirket kurucusu, Arnavutluk'ta yakalanır. Yine, kripto varlık platformu **Vebitcoin** teknoloji şirketi tarafından yapılan *"finansal güçlük nedeniyle faaliyetlerine son verdikleri"* açıklamasının ardından, şirketin Türkiye'deki finansal kuruluşlardaki hesapları bloke edilmiş ve şirket yöneticisi ve bazı çalışanlar göz altına alınmıştır. Gözaltına kadar geçen süreçte, faillerin yatırımcı hesaplarındaki kripto paraları çeşitli borsalar üzerinden yurt dışına aktardıkları belirtilmektedir[31].

2. Ara Değerlendirme

Dolandırıcılık suçu için öncelikle kullanıcıların borsa hesaplarında tuttuğu kripto varlıkların sahiplik durumu tespit edilmelidir: Kullanıcıların bakiyelerine yansıyan kripto varlıklar, borsanın kontrolündeki blokzincir cüzdanlarında tutulmakta; yine kullanıcının talimatı doğrultusunda işleme sokulmaktadır[32]. Günümüzde merkezi borsaların ekseriyeti, kullanıcılarla yaptıkları sözleşme uyarınca, kripto varlıkları torba niteliğindeki ortak/paylaşımlı cüzdanlarda muhafaza etmekteyken (*örn: Binance*), bazıları ise kripto varlıkları kullanıcıya özel bağımsız cüzdanlarda tutma seçeneği (*örn: Gemini*) sunabilmektedir[33]. Paylaşımlı cüzdan sisteminde, kullanıcılar tarafından aktarılan varlıkların sahipliği borsaya geçmektedir. Buna karşılık, özel cüzdan seçeneğinde hukuken bir devirin gerçekleşip gerçekleşmediği duraksama yaratmaktadır[34]. Ancak her halde, cüzdan özel anahtarı kullanıcıyla paylaşılmadığı müddetçe, kripto varlıkların hakimiyeti bizce de borsada kal-

---

Currencies Market", 15'th International Scientific Practical Conference, Volume 2, Moldova 2021, s. 12, (https://ibn.idsi.md/sites/default/files/imag_file/p-10-13.pdf).

31 **"Vebitcoin'in CEO'su gözaltına alındı, Türkiye'deki banka hesaplarına bloke konuldu"**, 24.04.2021, BBC Türkçe, (https://www.bbc.com/turkce/haberler-turkiye-56867733).

32 Merkezi yapıdaki borsaların, kullanıcıların varlıklarını elinde tutan "aracı" olarak, işlem emirlerini yerine getirdiği ve bankalar gibi fonksiyon üstlendiği hususunda bkz. **Reiff**, *yuk. dipnot* 24; Ayrıca **Johnson**, Kristin N.: "Decentralized Finance: Regulating Cryptocurrency Exchanges", Wm. & Mary Law Review, Volume 62, 2021, s. 1953.

33 Borsalarla ilgili olarak, kripto varlıkların farklı muhafaza şekillerine dikkat çeken çalışma için bkz. **Haentjens**, Matthias/**Graff**, Tycho De/**Kokorin**, Ilya: "The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them", Singapore Journal of Legal Studies, No 2, 2020, s. 534.

34 **Haentjens**/**Graff**/**Kokorin**, s. 537.

maya devam ettiğinden[35], hukukumuz açısından kullanıcılara ait varlıkları kendi sahipliğinde tutan borsanın dolaylı temsilci gibi hareket ettiği ve böylece borsa hesabına yapılan varlık transferlerinin, kullanıcı yönünden tasarruf unsurunu karşıladığı sonucuna ulaşılmalıdır. Elbette, karşılaşması olası farklı muhafaza yöntemleri aksi yönde düşünmeyi gerektirebilir.

Tasarruf meselesi çözümlendikten sonra, kullanıcıların borsadaki kripto varlıklarına kısmen veya tamamen ulaşamadığı durumlar hilenin konumuna göre üç farklı ihtimal üzerinden incelenmelidir:

(a) ***İlk ihtimalde,*** en başından beri meşru bir iş faaliyeti yürütüldüğü izlenimi veren failin, gerçek niyetini gizleyerek, maddi davranışlarla muhataplarını hataya düşürüp tasarrufa sevk etmesi temel bir dolandırıcılık örneğidir. Şirketin kurulma ve işletilme süreci, hesap hareketlilikleri, agresif reklamlar ve abartılı vaatler, ilgililerin gerçekle bağdaşmayan açıklamaları, uygulamanın şüpheli şekilde kapatılması, kullanıcıları oyalamaya yönelik tutumlar, paravan hesap kullanma şeklindeki detaylar dolandırıcılığın tespitinde yardımcıdır. Dolandırıcılık suçunun açıkça tespit edilebildiği bu ihtimalde, aile veya arkadaş gibi yakınların suça katılımını ortaya çıkarmak güçtür.

(b) Cüzdan boşaltmanın gündeme geldiği ***ikinci ihtimalde***, fail tamamen meşru ticari amaçla işlettiği kripto para borsasında biriken varlıkları kendine mal edinirken; aynı zamanda bakiyelerde rakamsal değişiklikler yapmak ya da sözde "siber saldırıya" uğradıklarını öne sürmek gibi gerçeğin açığa çıkmasını engelleyici tedbirlere başvurabilir. Buradaki hileli hareket, dolandırıcılık suçundaki "muhatabı hataya düşürme" ve "tasarrufa sevk etme" bağlantısına sahip değildir. Borsa uygulamasının sermaye şirketi olarak faaliyet gösterdiği böylesi durumlarda, şirket yetkili veya yöneticisinin, kullanıcılardan gelen, ancak şirket malvarlığında yönetilen varlıkları elde etmeye yönelik davranışı ilk olarak TCK m. 155/2'deki güveni kötüye kullanma suçunu akla getirmektedir. Suçun konusunun "mal" ile ifade edilmesinin yarattığı sorun ayrı bir inceleme konusu olmakla birlikte[36]; her halde temel amacı "hak sahiplerinin malvarlığı değerlerini korumak" olan nitelikli güveni kötüye kullanma suçunun cezasının alt sınır (1 yıl) itibariyle azlığı

---

35 Kıyaslayınız **Haentjens/Graff/Kokorin**, s. 540 ile s. 561.

36 Kripto varlıkların güveni kötüye kullanma suçunun konusu olabileceği görüşü için bkz. **Balcı**, Murat/**Çakır**, Kerim: "Kripto Para Borsaları ve Güveni Kötüye Kullanma Suçu", Prof. Dr. Selçuk Öztek'e Armağan, Ankara 2022, s. 460. Hırsızlık suçu özelindeki açıklamalarından kıyasen, kripto varlıkların mal olarak kabul edilemeyeceği görüşü için **Aksoy Retornaz**, s. 300.

suçlulukla mücadeleye engeldir. Nitekim cüzdan boşaltma fiili, piyasadaki güven ve ekonomik istikrarı olumsuz etkileyebilecek potansiyele sahip bir haksızlıktır. Bu nedenle, kripto varlık alım-satımına aracılık eden platformlarındaki varlıkları mal edinen ilgililerinin cezalandırılması için tıpkı Bankacılık zimmetindeki gibi[37] özel düzenlemeye ihtiyaç bulunduğu kanaatindeyiz.

(c) Sayısız müşterinin varlıklarını kontrol eden kripto para borsaları, siber tehlikeler için açık hedef konumundadır[38]. Diğer taraftan, bankalara kıyasen gelişmiş bir alt yapı, denetim ve yasal çerçeveden yoksunluk da bu borsalar için önemli bir risk kaynağıdır[39]. Bunlarla bağlantılı olarak, ***üçüncü ihtimalde***, siber saldırı, kötü yönetim, alt yapı yetersizliğinden kaynaklı şirketi zora sokan durumları gizlemek için hileli hareketlere başvurulması mümkündür. Durumu gizleyerek düzetmeyi amaçlayan ilgililerin, hesap ve kayıtlara müdahale etmesi dolandırıcılık suç tanımına uygun değildir. Örneğin, olay tarihi itibariyle müşterilere ait 450 milyon dolar değerinde Bitcoin'in kaybolduğu **MtGox vakası**nda[40], hesaplardaki eksilmenin hırsızlık, dolandırıcılık veya kötü yönetim sonucu mu oluştuğu başta anlaşılamazken; sonrasında, siber saldırı sonucu kısım kısım gerçekleştiği ve zamanla azalan varlıklar dolayısıyla ödeme aczine düşen şirketin iflas ettiği tespit edilir[41]. MtGox'un sahibi Mark Karpeles aleyhine açılan davaya bakan Tokyo Bölge Mahkemesi, sanığın durumu gizlemek için elektronik kayıtlarda oynama yaptığını kabul etmekle birlikte; kripto varlıkları kendi zimmetine geçirdiğine yönelik herhangi bir delile rastlanmadığı gerekçesiyle güveni kötüye kullanma suçundan beraatına karar vermiştir[42]. Bir kripto

---

37 **5411 sayılı Bankacılık Kanunu, Zimmet, Madde 160**: (1) Görevi nedeniyle zilyetliği kendisine devredilmiş olan veya koruma ve gözetimiyle yükümlü olduğu para veya para yerine geçen evrak veya senetleri veya diğer malları kendisinin ya da başkasının zimmetine geçiren banka yönetim kurulu başkan ve üyeleri ile diğer mensupları, altı yıldan oniki yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılacakları gibi bankanın uğradığı zararı tazmine mahkûm edilirler. (2) Suçun, zimmetin açığa çıkmamasını sağlamaya yönelik hileli davranışlarla işlenmesi hâlinde faile on iki yıldan az olmamak üzere hapis ve yirmibin güne kadar adli para cezası verilir; (…)"

38 **Johnson**, s. 1954.

39 **Johnson**, s. 1971.

40 Ayrıntılı inceleme için bkz. https://research.bitexen.com/post/inceleme-mt-gox-davasi.

41 **Nilsson**, Kim: "The missing MtGox bitcoins", 19.04.2015, WIZSEC Bitcoin Security Specialist, (https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html).

42 "**Mt Gox CEO Mark Karpeles Found Not Guilty of Embezzlement**", Bitcoin.com News, 15.03.2019, (https://news.bitcoin.com/mtgox-ceo-mark-karpeles-not-guilty-embezzlement/).

varlık borsası işletmecisinin, yatırımcılara ait varlıkları riske sokan durumları gizleyerek, şirketin olağan işleyişini sürdürmesi malvarlığına karşı suçlara kıyasen farklı bir hukuki yararı ihlal etmektedir. Bu nedenle, "*önlem alınması gereken hallerde lüzumlu tedbirleri almayan"* kripto borsası yetkililerinin cezalandırılması için Bankacılık Kanunu m. 152'dekine benzer bir düzenlemeye ihtiyaç olduğunu vurgulamak isteriz.

B. Kripto "Para Birimlerinde" Sahtecilik

Kripto varlık türleri olarak, kripto para birimleri (=coin) ile kripto jetonların (=token) teknolojik özellikleri itibariyle birinden ayrıştığını ifade etmiştik. Blokzincir tabanlı bir uygulama bünyesinde ve geliştirici kontrolünde çıkarılan kripto jetonların aksine; *kripto para birimleri,* ait oldukları ağda kişi ve uygulamaların hakimiyetinden bağımsız varlık göstermektedir. Haliyle, kripto jetonlarla bağlantılı sahtekarlıklar ağırlıkla temsil etikleri plan/projelerin aldatıcılığıyla ortaya çıkarken; kripto para birimlerinde sahtecilik sanal ürünün kendisini ve değerini konu almaktadır. Bugüne kadar genellikle Bitcoin'i referans alan bu sahtekarlıklar, *kripto para biriminin varlığına* veya *vaat edilen vasıflarına* ilişkin olmak üzere iki farklı şekilde ortaya çıkabilir. Dolandırıcılık suçundan yapılan incelememizi etkileyeceği için, her iki ihtimali ayrı başlıkta ele almayı tercih ediyoruz.

i. Kripto Para Biriminin Varlığına Yönelik Sahtekarlık (*Uydurma Kripto Para, Fake Coin*):

Gerçekte web tabanlı inşa edilmiş elektronik belirteçlerin, tıpkı Bitcoin gibi, sözde ödeme fonksiyonunu yerine getirmek üzere merkeziyetsiz ve takası mümkün bir kripto para birimi olduğundan bahisle satışa sunulması yaygın sahtekarlıklardandır. Konuyla ilgili olarak, 4 milyar dolarlık dolandırıcılıkla anılan Londra merkezli "**OneCoin**" olayı dikkat çekicidir. Gerçekte kripto özelliği bulunmayan OneCoin, Bitcoin'e rakip bir ödeme aracı olarak üretildiği, madencilik yapılabileceği ve aktüel bir değer taşıdığı yalanıyla internet sitesi üzerinden satışa çıkarılır. Ustaca yapılan toplantılar, tanıtımlar ve kazanma hırsını tetikleyen açıklamalar çok sayıda kişinin OneCoin almasını ve katmanlı şekilde pazarlanmasını sağlar[43]. Ancak, yetkililerin müdahalesiyle dolandırıcılık şebekesi açığa çıkar[44]. Benzer olay

---

[43] Haberlere konu olayın ayrıntısı için bkz. **"Cryptoqueen: How this woman scammed the world, then vanished"**, BBC News, 24.11.2019, (www.bbc.com/news/stories-50435014).

[44] Dolandırıcılıkta kilit role sahip olduğu düşünülen Ruja Ignatova, FBI tarafından halen aranmaktadır. **"Missing Cryptoqueen: FBI adds Ruja Ignatova to top ten most wanted"**, BBC News, 01.07.2022, (www.bbc.com/news/world-us-canada-62005066).

Anadolu Cumhuriyet Başsavcılığı tarafından hazırlanan iddianameye de konu olmuştur. Basına yansıyan iddiaya göre, şüpheliler "**Coinspace**" isimli şirket üzerinden "S-Coin", "First Coin" isimli ve gerçekte hiçbir borsada işlem göremeyen hayali kripto paraları, tıpkı Bitcoin gibi gelecekte yüksek getiri sağlayacağı yönündeki tanıtımlarla piyasaya sürüp, katmanlı şekilde pazarlamasını sağlayarak önemli miktarda yatırım toplar[45].

Bu tür sahtekarlıkta, tertipçilerin gerek satışa sundukları sanal belirtecin kendisi gerek başvurdukları pazarlama stratejileri, tipe uygun dolandırıcılık girişimini belirgin bir şekilde ortaya koymaktadır. Şöyle ki, "sanal" mekanizmalar, onları işler hale getiren donanım ve yazılımın varlığıyla birlikte bütün olarak "maddi gerçekliğin" parçasıdır. Buna paralel, blokzincir ağına sahip olmayan bir elektronik belirteci, sözde kripto para birimi olarak pazarlamak, gerçeği olduğundan farklı göstermeye yönelik hileli davranıştır. Ayrıca bu belirteçler serbest piyasa koşulları altında değerlenme olanağından yoksun kaldığından, söz konusu hileli davranış zarar unsuru yönünden de dolandırıcılık suçuna uymaktadır.

ii. Kripto Para Biriminin Vasıflarına Yönelik Sahtekarlık:

Kripto para biriminin, -Ethereum örneğinde olduğu gibi- geliştirilmesi planlanan ödeme ağı henüz fiilen etkin hale getirilmeden üretilmesi ve satışa çıkarılması mümkündür. Bu yöntemi işleten kimi geliştiriciler, ağın teknik özellikleri, kripto para biriminin değeri ve dayandığı varlıklar, uzman kadrosu, iş ortaklıkları gibi konularda gerçeğe aykırı tanıtımlar yaparak sahtekarlığa zemin hazırlayabilir. Görünüşte sanal belirtecin mevcut olduğu böylesi durumlar hakkında sahtecilik iddiasında bulunmak, daha karmaşık bir incelemeyi gerektirmektedir.

Örnek sayılabilecek bir olayda, Randall Crater, eşler arası ödeme sistemi kurma projesiyle piyasaya sürdüğü "**My Big Coins" (=MBC)** adlı sanal varlığı, Bitcoin gibi işlevsel bir kripto para birimi olduğu; kredi kartları ve ATM'lerde işlem göreceği; madencilik yapılabileceği; mal, nakit veya diğer sanal para birimleriyle kolayca değiştirebileceği; altın gibi değerli varlıklarla desteklendiği yönündeki tanıtımlar eşliğinde 2014-2017 yılları arasında satışa arz eder. Ancak, zamanla bazı işlerin ters gitmesi üzerine dolandırıcılık

---

[45] Olay hakkında ayrıntılı bilgilendirme için bkz. **Akçakaya**, Yusuf: **"Saadet zinciri ile Bitcoin vurgunu"**, Gazete Oksijen, 07.05.2021, (www.gazeteoksijen.com/turkiye/saadet-zinciri-ile-bitcoin-vurgunu-26804; "Bitcoin Benzeri Dijital Para Üzerinden Milyonluk Vurgun Yapanlar Kaçtı", (https://gercekbandirma.com/bitcoin-benzeri-dijital-para-uzerinden-milyonluk-vurgun-yapanlar-kacti).

suçunun işlendiği şüphesiyle yürütülen soruşturma sonucunda[46]; herhangi bir değerli varlıkla desteklenmediği ve kolayca transfer edilebilir olmadığı anlaşılan MBC'lerin, gerçeğe aykırı açıklamalarla pazarlandığı açığa çıkar[47]. Ayrıca Randall Creater'in, yatırımcılardan gelen 6 milyon dolar civarındaki parayı şahsi banka hesaplarına gönderdiği; bu yatırımları kişisel harcamalar ve lüks mallar satın almak için kullandığı tespit edilerek, dolandırıcılık suçundan (=wire fraud)[48] cezalandırılmasına hükmedilir[49]. Ponzi ve piramit satış özelliklerine rastlanmayan MBC'nin en başından beri dolandırıcılık girişimi olduğu, geliştiricinin süreç içerisindeki davranışları ile sistemin işleyişi üzerinden gözlemlenebilmektedir[50].

Ödeme ağında kullanılmak üzere piyasaya sürülen kripto para biriminin teknolojik özellikleri, değeri, teminatları, ortaklıkları hakkında gerçeğe aykırı açıklamalarla piyasaya sürülmesi ilk bakışta dolandırıcılık suçuna uyan hileli davranıştır. Geliştiricilerin satıştan elde ettiği yatırımları şahsi harcamalar için kullanması ve/veya paravan borsalar üzerinden farklı yerlere transfer etmesi, yatırımcıların geçiştirilmesi, şaibeli iş birlikleri dolandırma kastını tespite yardımcı ayrıntılardır. Ancak doğrudan sahte kripto para birimlerinin kullanıldığı ***Onecoin*** gibi örneklerin aksine, kurulması vaat edilen sistemin vasıflarını konu alan bu tarz somut olaylarda dolandırıcılığı tespit etmek çok daha zor ve hassas bir meseledir. Nitekim sistemin planlandığı gibi işletilememesi ya da vaat edilen ortaklık, geliştirme ve güncellemelerin bir türlü tamamlanamaması veya transfer sorunlarının aşılamaması gibi

---

46 Suçlama hakkında resmî açıklama için bkz. "**New York Man Charged with Cryptocurrency Scheme**", The United States Department of Justice, Office of Public Affairs, 27.02.2019, (https://www.justice.gov/opa/pr/new-york-man-charged-cryptocurrency-scheme).

47 MBC hakkında ilk incelemeyi başlatan ABD Vadeli Emtia Ticareti Komisyonu'nun (CFTC), 2018 tarihli şikayetine dayanak gösterdiği bulgular için bkz. *Commodity Futures Trading Commission v. My Bıg Coın Pay, Inc*., Case 1:18-cv-10077-RWZ, Document 1, 01/16/18, (www.cftc.govsites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfmybigcoinpaycomplt011618.pdf).

48 "Wire Fraud" için (II-B) başlığı altındaki açıklamalara bakınız.

49 Basın açıklaması için bkz. "**Founder of Purported Cryptocurrency Company Sentenced to More Than Eight Years in Prison for Multi-Million-Dollar Fraud Scheme**", U.S. Attorney's Office, District of Massachusetts, 31.01.2023, (https://www.justice.gov/usao-ma/pr/founder-purported-cryptocurrency-company-sentenced-more-eight-years-prison-multi-million).

50 Süreç hakkında detaylı inceleme için bkz. **O'Connor**, Fergal/**Lucey**, Michael: "The Incomplete History of My Big Coin", in Batten-Corbet-Lucey Handbooks in Alternative Investments. Editors J. Batten, B. Lucey and S. Corbett, SSRN, (https://ssrn.com/abstract=3905960).

başarıızlığa bağlı sebeplerle de yatırımcıların zarara uğraması olasıdır. Bizce, yoğun rekabet altındaki ve neredeyse tamamen beklentiler etrafında şekillenen proje aşamasındaki bu tarz girişimlerin abartı çıtasını alışılandan fazla yükseltebileceği göz önünde bulundurulmalı; eşler arası ödeme sistemi kurmaya yönelik gerçek girişimler dolandırıcılık suçuyla ilişkilendirilmeden önce sürecin bütünü hassasiyetle incelenmelidir. Aksi yaklaşım, teknolojik gelişmenin önünün kesilmesiyle sonuçlanabilir.

Öte yandan, ***bir diğer önemli ihtimalde***, dışa yansıtılan gerçeğe aykırı tanıtımlar/vaatler, şahsi hesaplara para aktarımı ile lüks harcamalar gerçekte uyuşturucu, pornografi ve bahis oyunlarından elde edilen geliri aklamak ve yasa dışı para akışını sağlamak üzere hayata geçirilmiş olabilir. Özellikle, ponzi görüntüsü altında, suçtan elde edilen geliri aklama sürecinin işletilmesi kuvvetle muhtemeldir. Tam bu noktada, iştirake ilişkin hükümlerin yetersiz kalabileceği de göz önünde bulundurularak, ***suç işlemek veya işlenmesini kolaylaştırmak üzere elektronik ortamda platform işletenlerin cezalandırılmasını*** sağlamaya yönelik torba düzenleme yapılması aciliyet arz etmektedir.

C. Likidite Havuzunu Boşaltma: Halı Çekme (Rug Pull)

1. İşleyiş Yöntemi

Likidite havuzu (=luquidity pool), merkeziyetsiz finans projeleri için ihtiyaç duyulan likiditeyi sağlamak üzere oluşturulmuş, akıllı sözleşme hakimiyetindeki kripto varlık havuzlarıdır[51]. Likidite havuzlarının başarısı, bağlı olduğu protokollerin etkin çalışması dışında, geliştiricinin güvenilirliğine de ihtiyaç duyar. Bu güveni suiistimal eden ***Rug Pull,*** geliştiricinin, görünürde kendi blokzincir tabanlı uygulamasına kaynak sağlamak üzere likidite havuzu oluşturduğu ve sonrasında biriken likiditeyi alıp ortadan kaybolduğu sahtekarlık türü olup; dilimize "halı çekme" veya "havuz boşaltma" ifadeleriyle çevrilmektedir.

Süreç şu şekilde işlemektedir: Geliştirici proje kapsamında ürettiği kripto jetonu -örn: **Yc**oin-, piyasada işlem gören bir kripto para birimiyle -örn: Ether- eşleyerek "**YCN**/ETH" işlem çiftine sahip likidite havuzu

---

[51] Kripto likidite havuzları ve işleyiş hakkında teknik bilgi için bkz. **Heimbach**, Lioba/ **Wnag**, Ye/**Wattenhoffer**, Roger: "Behavior of Liquidity Providers in Decentralized Exchanges", Cornell University, arXiv.org, 11.10.2021, (https://arxiv.org/pdf/2105.13822.pdf). Genel bilgi için ise bkz. "**What Are Liquidity Pools**?", Cryptopedia, 01.12.2021, (https://www.gemini.com/cryptopedia/what-is-a-liquidity-pool-crypto-market-liquidity).

oluşturur. Böylece, yatırımcıların ETH karşılığında YCN alması mümkün hale gelir. Bu sistem aynı zamanda yatırımcılara, satın aldıkları YCN'leri, belirli vadeyle havuza kilitleyip likidite sağlamasına (=luquidity provider) ve karşılığında gelir elde etmesine (***likidite madenciliği****/= yield farming*) olanak sağlamaktadır. Amaç, havuzda mümkün olduğunca büyük miktarda likidite birikmesidir. Havuzdaki takas, ödünç, fiyatlandırmaya yönelik işlemleri kapsayan süreç tamamen akıllı sözleşmeler tarafından yürütülür.

Ancak kötü niyetli geliştiriciler, likiditeye erişim ayrıcalığı elde edebilmek için akıllı sözleşme üzerinde bir takım gizli tedbirler alabilir[52]. Bu alandaki sahtekarlık, üç farklı şekilde karşımıza çıkmaktadır: ***Birinci ihtimalde***, geliştiriciler, yönetici anahtarı veya sözleşmeye ekledikleri kod yardımıyla erişim sağladığı havuzdaki fonları (yani örneğimizde EHT'leri), istediği anda boşaltabilir. ***İkinci ihtimalde***, geliştiriciler satışa arz ettikleri kripto jetonlara "takası sınırlayan" kod yerleştirir ve böylece kendi ellerindeki ayrıcalıklı jetonlarla havuzda biriken fonları (EHT) istedikleri gibi takas ederek havuzu boşaltabilir. Havuzdaki likiditenin bir anda sıfırlandığı her iki ihtimalde de, yatırımcılar sahtekarlık amacıyla üretildiği anlaşılan değersiz bir kripto jetonla baş başa kalır. Basına yansıyan **Squid Game** sahtekarlığında, geliştiriciler, üzerine çalıştıklarını iddia ettikleri oyun projesine ait *Squid Token* adlı kripto jetonları, SQUID/BNB işlem çiftiyle Binance blokzincir ağında oluşturdukları likidite havuzu üzerinden piyasaya arz ederler. Squid Token'ların başlangıçta 0,01 dolar olan fiyatı, Pakcakeswap isimli merkeziyetsiz borsada işlem görmeye başlamasıyla kısa sürede 3.000 dolar seviyelerine ulaşır. Pazarlama sırasında, talep düşüşlerine dirençli tasarlandığı *(=anti-dump teknolojisi)* yalanıyla tanıtılan bu kripto jetonların, gerçekte takası engelleme amacıyla hazırlandığı anlaşılır. Bu nedenle, yatırımcılar havuzdan aldıkları Squid Token'larla yükselen fiyattan işlem yapamazken, geliştiriciler kendilerindeki takası mümkün Squid Token'lar sayesinde havuzdaki bütün likiditeyi (=BNB) boşaltarak ortadan kaybolur. Sahtekarlık, Squid Token fiyatının 0.002 dolara düşmesiyle son bulur[53].

Üçüncü ihtimalde ise görünürde herhangi bir sahteciliğe başvurmayan geliştirici, en değerli olduğu anda bütün jetonlarını havuzda takas etmek

---

[52] Ayrıntılı inceleme için bkz. **Rossow**, Andrew: "What Are Rug Pulls? Are They a Crime?", NFT NOW, 28.11.2022, (https://nftnow.com/guides/scams-explained-what-are-rug-pulls-and-are-they-a-crime/); Kıyaslamak için bkz. **"What is a Rug Pull? DeFi and Exit Scams Explained"**, Solidus Labs, (https://www.soliduslabs.com/post/rug-pull-crypto-scams).

[53] **Stokel-Walker**, Chris: "How a Squid Game Crypto Scam Got Away With Millions"**,** WIRED, Security, 02.12.2021, (https://www.wired.com/story/squid-game-coin-crypto-scam/).

suretiyle kendi projesinden karlı biçimde ayrılmakta ve yatırımcıların zarar görmesine yol açmaktadır. Havuz boşaltmanın yumuşak şekli *(=soft rug pull)* olarak ifade edilen bu yöntemde[54], projeden el çeken geliştiriciler, yatırımcıların beklentilerini boşa çıkarmaktadır. Likidite madenciliği projesi olan **Polywhale Finans** olayında, geliştiriciler sosyal medya hesabı üzerinden, özetle sistemin planladıkları gibi işlememesini ve sağlık sorunlarını gerekçe göstererek, platform üzerindeki faaliyetleri durdurup, projeyi topluma bıraktıklarını açıklarlar. Piyasaya sürüldükten sonra 180 dolar seviyesine ulaşan proje jetonu KRILL ise yüzde 99,9 değer kaybeder[55]. Sosyal medya ve basında, Polywhale kurucuları, kasadaki bütün jetonları kripto varlık piyasasının düşüşe geçtiği sırada atarak, yumuşak geçişli bir havuz boşaltma dolandırıcılığı yapmakla itham edilmektedir[56].

2. Ara Değerlendirme

Akıllı sözleşmenin idaresindeki likiditenin geliştirici tarafından boşaltıldığı ilk iki ihtimalde, fiyatlamanın ve takas işleminin otonom gerçekleştirileceği inancıyla işlem yapan mağdurların en başından beri hileli hareketle hataya düşürüldüğü açıktır. Ancak akıllı sözleşmenin idaresindeki kripto değerlerin ele geçirilme yöntemi, dolandırıcılık suçunda tipiklik tartışması yaratacak niteliktedir: Şöyle ki, geliştiriciler suça konu yararı akıllı sözleşmenin kontrolündeki likiditeye erişerek ***kendi davranışlarıyla*** elde ederken, mağdurların bu yararı faile sağlamaya yönelik bir davranışı bulunmamaktadır. Oysa hileye rağmen, yararın bizzat fail tarafından elde edildiği durumlar, TCK m. 157'deki suç tanımının dışında kalmaktadır[57]. Ayrıca akıllı sözleşmelerin otonom çalışma prensibi ve kripto varlıkların "mal" niteliği konusundaki soru işaretleri, bu sorunun ***güveni kötüye kullanma*** ve ***hırsızlık suçları*** etrafında çözümlenmesini de zorlaştırmaktadır. Nihayet, bahse konu haksızlıkta akıllı sözleşmeye herhangi bir müdahalede bulunulmadığı; bila-

---

54 **Puggioni**, Valerio: "Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it", Cointelegraph, 06. 02.2022, (https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it).

55 01.08.2022 tarihi itibariyle Coinmarketcap fiyatı 0.004017 Amerikan Doları'dır (www.coinmarkercap.com).

56 **Young**, Martin: "Polywhale Team Jumps Ship Amid DeFi Rug Pull Accusations", Yahoo Finance, 22.06.2021, (https://finance.yahoo.com/news/); "Polywhale Team Abandon $100 Million Project Amid Scam Allegations", Crypto News, 21.06.2021, (https://cryptonews.net/news/security/845997/).

57 Suç tipinde açıkça kaleme alınmasa da, dolandırıcılık suçunun oluşabilmesi için hataya düşürülen kişinin zarara neden olacak bir tasarrufta bulunması gerektiği hususunda bkz. **Ekici Şahin**, s. 270.

kis sözleşme kodları en başında failin haksız yarar elde etmesine imkân verecek şekilde yazıldığı için TCK m. 244/4 anlamında bilişim sistemine müdahale etme unsuru da gerçekleşmemektedir.

Neticede, yapısal özelliği itibariyle finansal işlemleri otonom yürütmesi gereken akıllı sözleşme protokol ve bileşenlerinin, haksız yarar elde etmek ve bu suretle ilgililerin malvarlığında zarara yol açmak üzere tasarlanması, esasen dolandırıcılık merkezli bir haksızlıktır. Kullanıcıların zararına menfaat elde etmek üzere gerçekleştirilen elektronik ortamdaki aldatıcı girişimler karşısında, mevcut duruma kıyasen daha etkili bir koruma sağlanabilmesi için yararın mağdur eliyle sağlanmasını aramayan dolandırıcılık suçu düzenlemesine ihtiyaç duyulacağını düşünmekteyiz. Nihayet, beklentilerin karşılıksız bırakılmasıyla sonuçlanan havuz boşaltmanın yumuşak şeklinde (=Soft Rug Pull), hilenin varlığı ve ispatı sorun teşkil edeceğinden, cezai tedbirler etkisiz kalacaktır.

D. Yanlış ve Yanıltıcı Bilgilerle İlk Kripto Arzı (ICO Dolandırıcılığı)

ICO (İlk Kripto Varlık/Token Arzı[58]-Initial Coin Offerring), blokzincir tabanlı proje geliştiricilerinin, proje kapsamında ürettiği kripto jetonları elektronik ortamda piyasaya arz etmek suretiyle sermaye piyasası ve halka arz formalitelerinden bağımsız, hızlı ve kolayca kaynak toplamak için başvurduğu yöntemin adıdır[59]. Piyasaya arz edilen kripto jetonları satın alanlar, borsada listelenmeye başlamasıyla birlikte ikincil piyasalarda bunların ticaretini yapabileceği gibi; projenin başarıya ulaştığı ölçüde kendilerine tanınan hak, hizmet veya temettüden yararlanabilir[60].

Geliştirici, bir yandan teknik dokümanda şirket ve insan kaynağı, projenin konusu, ihtiyaç duyulan kaynak miktarı hakkında bilgi sunarken, diğer yandan çeşitli tanıtım ve reklam faaliyetleriyle yatırımcıların ilgisini çekmeye çalışır[61]. Arza katılan yatırımcılar için en yaygın risk olan sahte proje-

---

58 **Telvetoğlu**, Mete: Hukuki Yönleriyle Kripto Varlıklar ve Kripto Varlıkların İlk Arzı (Initial Coin Offering), 2. Baskı, İstanbul 2021, s. 262.

59 Ayrıntılı açıklama için bkz. **Frankenfield**, Jake: "Initial Coin Offering (ICO)", Investopedia, 03.11.2020, (www.investopedia.com/terms/i/initial-coin-offering-ico.asp).

60 Bkz. **Sherry**, Benjamin: "What Is an ICO?", Investopedia, 25.08.2021, (www.investopedia.com/news/what-ico/); Süreç hakkında ayrıntı için bkz. **Telvetoğlu**, s. 266 vd.

61 ICO yönteminin temel karakteristiği hususunda inceleme için bkz. **Zetzsche**, Dirk A./**Buckley**, Ross P./**Arner**, Douglas W./**Linus**, Föhr: "The ICO gold rush: it's a scam, it's a bubble, it's a super challenge for regulators" University of Luxembourg Law Working Paper, No. 11, 2017, UNSW Law Research Paper, No. 83, s. 6 vd.

lerdir. ICO'lara duyulan güvenin azalmasıyla, varlık arzları merkezi yapıdaki borsalar denetiminde (**IDO**=Initial Exchange Offering) veya merkeziyetsiz borsalar üzerinden (**IEO**=Initial DEX Offering) yapılmaya başlanmıştır[62]. Süreç ve isimlendirmedeki farklılıklara rağmen, temelde kitle fonlaması mantığıyla işleyen kripto varlık arz yöntemleriyle, **a)** sahte, **b)** manipüle edilmiş veya **c)** özensiz projeler üzerinden haksız kazanç elde etmek mümkündür.

Vaatlerin pazarlandığı bu tarz fon toplama girişimlerinde dolandırıcılığın tespiti için öncelikle proje hakkındaki ***vaatlerin gerçekleşmesine yönelik riskler*** ile projenin ***gerçekliğine yönelik riskler*** birbirinden ayrılmalıdır. Başarısızlığa bağlı kazanç vaadinin -abartıya başvurulsa dahi- hileli davranış teşkil etmeyeceği açıktır. Diğer taraftan, proje sahibinin işin niteliğine, teknolojik alt yapıya, insan kaynağına vs. ilişkin gerçeğe aykırı bilgilerle kaynak topladığı ihtimalde ise ***dolandırıcılık*** ve ***manipülasyon*** olmak üzere, hileli davranışla ilişkili iki tür haksızlık karşımıza çıkmaktadır:

Birincisi, gerçeği olduğundan farklı göstermek suretiyle yürütülen kripto varlık arz projeleri, -yaygın örneklerdeki gibi sahte veya taklit projeler- dolandırıcılık suçu kapsamında ele alınabilir. Somut olayın özellikleri, hileli davranışın dolandırıcılık suçuna yönelik olup olmadığının tespitinde hayati öneme sahiptir. Geliştiriciler, en başından beri gerçekte bir proje geliştirme niyetleri olmadığı halde, sözde proje üzerinden ürettikleri kripto varlıkları piyasaya arz ederek, fonları topladıktan sonra bir anda ortadan kaybolabilir; ICO'yu bir süre işletip, ürettikleri jetonlar yüksek değerine ulaştığında ellerindekini de satıp projeden ayrılabilir; ya da tecrübesiz yatırımcıları tuzağa düşürmek için mevcut ICO'larla benzer isim ve tasarımda web sitesi hazırlayabilirler[63]. Örneğin, **Saveroid** vakıasında, Alman merkezli start-up kurucusu *Yassin Hankir*, ICO aracılığıyla yaklaşık 50 milyon dolar değerinde fon topladıktan sonra, sosyal medya hesabında "hoşça kalın" mesajını paylaşarak ortadan kaybolur. Hankir'e ofis, telefon ve sosyal medya hesaplarından ulaşılamaz[64]. Bu tarz örneklerdeki hileli davranışın TCK m. 157'deki dolandırıcılık suçuna uygun düştüğünde duraksama yoktur.

---

62 Aralarındaki farklar için bkz. **Gouda**, Namrata: "Key Differences Between IDO, ICO, IEO, and IPO", https://medium.com/geekculture/key-differences-between-ido-ico-ieo-and-ipo-10dad82b9e5d).

63 Kıyaslayınız. **Dülger**, Murat Volkan/**Özkan**, Onur: "Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi", Prof. Dr. Mehmet Emin Artuk'a Armağan, Ankara 2020, s. 988.

64 İnceleme için bkz. **Penke**, Michel: "40 Millionen verdient, Firma unerreichbar, Chef twittert Urlaubsbilder", WETL, Wirtschaft & Technik, 18.04.2018, (https://www.welt.de

İkincisi, yatırımcıların kararlarını ve proje kapsamındaki kripto varlıkların fiyatını etkilemeye yönelik gerçeğe aykırı açıklamalar ise dolandırıcılık suçunun kapsamı dışında kalmaktadır. Manipülasyon teşkil eden davranışlar, SPK m. 107/2'deki ***"bilgi bazlı piyasa dolandırıcılığı"*** suçunu akla getirmektedir. Ancak, ICO kapsamında kripto varlık arzının Sermeye Piyasası Kanunu'na tabi olup olmayacağı meselesi -Kurulun açıklamalarına rağmen- henüz netliğe kavuşmamıştır[65]. Mevcut koşullarda, işlem bazlı dolandırıcılık suçuna dair şüphenin soruşturulması Sermaye Piyasası Kurulu'nun yazılı başvurusuna bağlı olduğundan (SPK m. 105/1); belirsizlik açıklığa kavuşturulmadığı müddetçe, Kurulun blokzincir tabanlı kitle fonlamalarındaki manipülasyonların cezalandırılmasına yönelik başvuruda bulunması beklenmemektedir.

Karşılaştırmalı hukukta, Amerika Menkul Kıymetler ve Borsa Komisyonu (SEC), kripto varlık arzlarının, yatırım sözleşmesinin özelliklerini barındırdığı ölçüde, sermaye piyasalarını düzenleyen hükümlere tabi olacağını kabul etmekte ve gerçeğe aykırı bilgilerle kripto varlık arz ederek menfaat sağlamaya yönelik fiillerin, bizdeki piyasa dolandırıcılığı düzenlemesinin karşılığı olan menkul kıymet/sermaye dolandırıcılığı *(=securities fraud)* kapsamında cezalandırılması için gerekli girişimlerde bulunmaktadır[66]. Örneğin, SEC Haziran 2021 tarihli duyurusunda, Loci şirketi yöneticisi John Wise'nin, şirketin gelirleri, çalışan sayısı, faydalandıkları yazılım platformu hakkında gerçek dışı ve yanıltıcı bilgilerle piyasaya **LOCIcoin** adlı token arz ederek 2017 ile 2018 yılları arasında 7.6 milyon dolar fon topladığı ve böylece sermaye dolandırıcılığına ilişkin düzenlemeleri ihlal ettiği gerekçesiyle işlem yapıldığını açıklamıştır[67]. Ancak hukukumuz açısından, gerek TCK m. 157 gerekse de SPK m. 107'nin benzer vakılar karşısında gerekli korumayı sağlamayacağı hatırlatılmalı ve fiyatları etkileme suçunun kapsamının kripto varlıkları da içine alacak şekilde düzenlenmesi çözüm seçeneği olarak dile getirilmelidir.

/wirtschaft/webwelt/article175595788/Fintech-Start-up-Hack-oder-ICO-Betrug-Was-ist-bei-Savedroid-los.html).

65 Bu hususta ayrıntılı inceleme için bkz. **Başbüyük**, İsa: "Blokzincir Üzerinden Fon Toplama: Kripto Varlık Arzı (ICO) ve Sermaye Piyasası Kanunundaki Suçlarla İlişkisi", (Ed.) Ekici, Şahin/Solak, Ekrem/Avşar, Muhammed Emre, Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı, Adalet Yayınevi, Ankara 2021, s. 313.

66 Amerika Menkul Kıymetler Borsası'nın konu hakkındaki yaklaşımı için bkz. **Başbüyük**, Blokzincir Üzerinden Fon Toplama, s. 315.

67 "**SEC Charges ICO Issuer and CEO With Fraud and Unregistered Securities Offering**", U.S. Securities and Exchange Commission, Press Release, 21.06.2021, (https://www.sec.gov/news/press-release/2021-108).

E. Fiyat Manipülasyonu: Şişir-Boşalt (Pump-and-Dump) Tertibi

1. İşleyiş

Kaynak dildeki yaygın ifadesiyle *Pump-and-Dump*, planlı alım emirleri oluşturmak ve/veya gerçeğe aykırı tavsiyelerde bulunmak suretiyle, belli bir hisse veya emtianın fiyatını arttırmaya **(=şişir)** ve böylece düşük fiyattan alınan pozisyonları yükselen fiyattan kapatarak **(=boşalt)** kazanç elde etmeye yönelik bir tertiptir[68]. Satış baskısı sonucu düşen fiyatlar, yüksek fiyattan pozisyon alan yatırımcıları zarara uğratmaktadır. Geleneksel borsalarda önemli bir geçmişe sahip olan haksız kazanç yöntemi, kripto varlık piyasasında da kendini yaygın bir şekilde göstermektedir.

Yükseliş beklentisi yaratmak, geleneksel borsada şirketin mevcut durumu hakkında yanlış veya yanıltıcı bilgi kullanılmasını gerektirebilirken; kripto varlık piyasalarında koordineli emir girişleri çoğu zaman yeterli gelmektedir[69]. ***İlk aşamada*** belirli kripto varlık için toplu talep yaratılır. Bu durum, piyasadaki yatırımcıları ilgili varlığı satın almaya teşvik ederek, varlığın değerinin daha da yükselmesini sağlar[70]. ***İkinci aşamada*** ise tertipçiler, düşük fiyattan oluşturdukları pozisyonlarını yükselen fiyattan kapatır ve gelen satışlar nedeniyle varlığın değeri hızlıca düşer. Tertipten habersiz şekilde varlığı yüksek fiyattan satın alan yatırımcılar (=***bag holder***) ekonomik kayba uğrar. Pump-and-dump, gerçek dışı-yanıltıcı haber, yayın, tanıtımlarla da desteklenebilir. Öte yandan, piyasa algısına tesir edebilecek büyüklükte fona sahip kimseler (=balina), algoritmik alım-satım emirleriyle veya sınırlı hallerde takipçi sayısı fazla olan sosyal medya fenomenleri ise yanıltıcı tavsiyelerle herhangi bir organizasyona ihtiyaç duymaksızın benzer fiyat oynaklığını yaratabilmektedir.

Alım emirleri ve gerçeğe aykırı açıklamalarla fiyat hareketliliği yaratmak, temelde Sermaye Piyasası Kanunu m. 107 uyarınca cezalandırılan bir

---

68 **Dhir**, Rajeev: "Pump and Dump", Investopedia, Laws & Regulatıons - Crıme & Fraud, 02.06.2021, (https://www.investopedia.com/terms/p/pumpanddump.asp9).

69 Amerika Menkul Kıymetler Borsası'nda yer alan küçük çaplı şirketlere ilişkin standartlarının daha esnek olduğu; bu durumun küçük şirketler hakkında gerçeğe aykırı bilgilerle hisse senedi piyasasını manipüle etmeyi kolaylaştırdığı hususunda bkz. **Kleinberg**, Bennet/**Kamps**, Josh: "To The Moon: Defining And Detecting Cryptocurrency Pump-And-Dumps", Crime Science, 7, No: 18, 2018, s. 3, (https://crimesciencejournal.biomedcentral.com/track/pdf/10.1186/s40163-018-0093-5.pdf).

70 Teknik inceleme için bkz. **Xu**, Jiahua/**Livshits**, Benjamin: "The Anatomy of a Cryptocurrency Pump-and-Dump Scheme", 28th USENIX Security Symposium (USENIX Security 19), 2019, Santa Clara, CA, USA, s. 1610-1611, (bkz. https://www.usenix.org/system/files/sec19-xu-jiahua_0.pdf).

girişimdir. Ancak, kripto varlıkların sermaye piyasası aracı olma niteliği belirgin bir şekilde sonuca bağlanmadığından, kripto varlık ilişkili manipülasyonların SPK kapsamında cezalandırılabileceğini söylemek mümkün olmamaktadır[71]. Ayrıca, sadece belli özellikteki kripto varlıklar *(=security token)* sermaye piyasası aracı olabileceğinden, farklı türdeki kripto varlıklar için devam edecek olan kapsam sorunu, bir bütün olarak dolandırıcılık suçu yönünden incelenmelidir.

2. Ara Değerlendirme

Planlı alım emirlerinin ana hedefi, "fırsat algısı" yaratmak suretiyle beklenti içerisine sokulan yatırımcıyı varlık satın almaya sevk etmektir. Kural olarak, niteliği gereği kesinlik içermeyen belirsiz durumlar hakkında muhatapta beklentiye sebebiyet vermek hile teşkil etmez[72]. Oysa, planlı emir girişleriyle beklentinin yönetilmeye kalkışıldığı ihtimalde ise sorun farklı bir boyut kazanmaktadır. Şöyle ki, planlı alım-satım emirleriyle piyasada algı oluşturmaya yönelik girişimler, muhataplarını yanıltma gücüne sahip olmasına rağmen, "maddi gerçeği olduğundan farklı tasvir etmeye yönelik" açık bir davranış içermemektedir.

TCK m. 157'deki "hileli davranış" ifadesi geniş yorumlanarak kapsam sorunu aşılabilirse de, somut olaydaki planlı emir girişleri ile dolandırıcılık suçunun diğer unsurları arasındaki bağlantıyı ortaya koymak mümkün olmamaktadır. Nitekim, dolandırıcılık suçunda elde edilen yarar, hileli hareket sonucu iradesi sakatlanan ve tasarrufa sevk edilen mağdurun malvarlığında oluşan zararın karşılığıdır. Volatilitesi yüksek bir piyasanın genel yatırımcı kitlesini hedef alan bu tarz girişimlerde, sayılan unsurların ne şekilde gerçekleştiği ve bunlar arasındaki kesintisiz neden-sonuç ilişkisinin nasıl ortaya konulacağı tamamen belirsiz bir hal almaktadır. Haliyle, bu tarz fiyat manipülasyonlarında, -gerçek dışı haber, bilgilendirme ve sair yönlendirici paylaşımlar kullanılmış olsa dahi- TCK m. 157'deki dolandırıcılık suçuna uyan bir mağduriyetin bulunmadığı sonucuna ulaşmaktayız[73].

Konuyu yoğun şekilde ele alan ABD uygulamasında, Amerika Adalet Bakanlığı'nın çözümü, kripto varlık piyasasını ilgilendiren fiyat manipülasyonu ile ilgili girişimlerin, elektronik iletişim aracılığıyla işlenen dolan-

---

71 Bkz. **Başbüyük**, Blokzincir Üzerinden Fon Toplama, s. 313.

72 Bu hususta bkz. **Kurşat**, Zekeriya: Borçlar Hukuku Alanında Hile Kavramı, İstanbul 2003, s. 13.

73 Dikkat çekmek gerekirse, gerçekte şişir-boşalt için hazırlanmış bir kripto varlığın, uydurma proje kapsamında piyasaya arz edilmesi (bkz. ICO sahtekarlığı), arza katılanlar yönünden dolandırıcılık suçuna meydan verecektir.

dırıcılık düzenlemesi (=wire fraud) uyarınca soruşturulabileceği yönündedir[74]. Nitekim, John McAfee'nin SEC tarafından suçlandığı iddianamede, McAfee'nin yaklaşık 1 milyon takipçisi olan Twitter hesabından "günün jetonu" içerikli paylaşımlarla elindeki kripto jetonun fiyatının yüzde 40 yükselmesini sağladığı, kendi kripto jetonlarını yüksek fiyattan sattığı, sonrasında da yüzde 90 düşüşe sebebiyet verdiği; böylece menkul kıymet dışında elektronik iletişime dair dolandırıcılık hükümlerini ihlal ettiği belirtilmiştir[75]. Bu düzenleme maddi yarar elde etmek üzere hileli davranışlarda bulunmayı yeterli gördüğünden, ilk bakışta makul bir çözüm gibi gözükmektedir[76]. Ancak, taktiksel alım-satım emirlerinin, suç tipindeki gerçeği olduğundan farklı gösterme şartını karşılayıp karşılamadığı konusundaki son kararı Yüksek Mahkeme verecektir.

Bizce, bireysel yatırımcıların da manipülasyondan yararlanmaya çalıştığı, hatta bunun için ticaret robotlarının geliştirildiği dikkate alınırsa, piyasa istikrarını doğrudan tehdit eden bu tarz haksızlıkların, dolandırıcılıktan ziyade fiyatları etkileme boyutuyla ele alınması korunan hukuki değer itibariyle[77] daha elverişlidir. Ancak TCK m. 237'deki fiyatları etkileme suçu incelendiğinde; metindeki "mal" ifadesinin belirli bir ihtiyaca yönelik besin dışındaki maddeleri işaret ettiği[78]; buna paralel olarak, sadece belli bir ekonomik değer veya hakkı temsil eden elektronik kayıtlardan oluşan kripto/ sanal varlıkların "mal" kapsamına girmediği sonucuna varmaktayız. Kripto varlık ticaretinin gelecekte çeşitlenerek yaygınlaşması imkân dahilindedir. Bu nedenle, çözüm için kripto varlık fiyatlarını etkilemeye yönelik planlı alım emirlerini yönetenlerin -yani organizatörlerin- kovuşturulmasına imkân veren; ayrıca ticaret robotu (=*trading bot*) gibi suçun işlenmesinde kullanılan araçları ceza miktarında dikkate alan düzenlemeye ihtiyaç bulunduğu kanaatindeyiz.

---

74 **McGinley**, Ian: "Wire fraud: the most powerful law in crypto right now", Routers, 23.08.2022, (www.reuters.com/legal/legalindustry/wire-fraud-most-powerful-law-crypto-right-now-2022-08-23/).

75 McAfee olayı hakkında ayrıntı için bkz. **Santos**, Michael: "Crypto Pump & Dump Fraud", Cryptocurrency Securıtıes Fraud (McAfee Pump & Dump Case), PRISON PROFESSORS, (https://prisonprofessors.com/crypto-pump-dump-fraud/).

76 "Wire Fraud" için (II-B) başlığı altındaki açıklamalara bakınız.

77 Fiyatları etkilemeye yönelik fiillerin etki ettiği hukuki değerler hakkında bkz. **Tepe**, İlker: Fiyatları Etkileme Suçu (TCK m. 237), Ceza Hukuku Dergisi, Cilt: 5, Sayı: 14, Aralık 2010, s. 94.

78 Madeni veya kâğıt formdaki paralar dahil, taşınır veya taşınmaz nitelikteki, ekonomik değeri olan her türlü nesnenin bu suçta mal kapsamına girdiği hususunda bkz. **Akbulut**, Berrin: "Fiyatları Etkileme Suçu", TAAD, Yıl:6, Sayı:20 (Ocak 2015), s. 38-39.

F. Sahte "Bitcoin Madencilik" Oluşumları ve Sözde Kazanç Uygulamaları

Madencilik, en özet şekliyle, iş kanıtı (proof of work-*PoW*) konsensüs mekanizmasına sahip bir blokzincir ağındaki işlem bloklarının, ödül kripto varlık karşılığında onaylanması ve kaydedilmesi sürecini ifade eder[79]. Madencilik faaliyeti, gelişmiş donanım ve yüksek elektrik gücü gerektirmektedir. Bu sebeple bazı platformlar, belli bir bedel karşılığında kullanıcılarına çevrim içi-bulut madencilik yapabilme veya madencilik girişimlerinden kâr payı alabilme imkânı sunmaktadır. Haliyle, bu alanda da çeşitli sahtekarlıklar kendini göstermektedir.

Bir dönem Türkiye'de de oldukça yoğun faaliyet gösteren **BitClub Network (BCN)** oluşumu, ilk başta yasal Bitcoin Madencilik Şirketi olarak tanıtılır. Katılımcılardan yatırım talep şirket, karşılığında madencilik gelirinden pay vermeyi ve sisteme yeni katılımcı dahil edenleri de ödüllendirmeyi vaat eder. Ancak 2014 ile 2019 yılları arasında varlık gösteren şirket, yatırımcılara vaat ettikleri kazançları vermediği gibi, onlardan daha fazla ödeme talep eder. Sonunda BitClup Network'un, gerçeğe aykırı ve yanıltıcı rakamlarla yatırımcılarını ikna etmeye çalışan sahte oluşum olduğu anlaşılır[80].

Madencilik ve kazanç sahtekarlıkları, farklı ve güncel şekillerde ortaya çıkabilir. Temelde uydurma yatırım ve hizmet karşılığında yatırım çeken bu tarz sahtekarlıklar, mağdurları hataya düşürüp tasarrufa sevk etme özelliğiyle TCK m. 157'de tanımlı dolandırıcılık suçuna uymaktadır. Madencilik dışında, yatırımcılara ellerindeki kripto varlıkları değerlendirerek kazanç sağlamayı teklif eden sözde uygulamaların genel olarak dolandırıcılık kapsamında değerlendirilmesi mümkündür. Ancak, merkeziyetsiz finans protokollerinin sunduğu sınırsız seçenek, sahtekarlık girişimlerinin icra şeklini karmaşıklaştırmaya; böylece aldatma ve tasarruf unsuru yönünden dolandırıcılığın sınırlarını zorlamaya açıktır. Örneğin, kripto varlık alım-satım

---

79 Bu hususta genel bilgiler için bkz. **Hong**, Euny: "How Does Bitcoin Mining Work?", Invostepedia, 05.05.2022, (https://www.investopedia.com/tech/how-does-bitcoin-mining-work/).

80 Bu yöntemle BitClup üyelerinden en az 722 milyon USD tutarında yatırım elde edildiği iddia edilmiştir. "**BitClup**", The United States Department of Justice, Updated District of New Jersey, 29.07.2021, (https://www.justice.gov/usao-nj/bitclub). Benzer şekilde, "Two Estonian Citizens Arrested in $575 Million Cryptocurrency Fraud and Money Laundering Scheme", The United States Department of Justice, Office of Public Affairs, Press Release 21.11.2022, (https://www.justice.gov/opa/pr/two-estonian-citizens-arrested-575-million-cryptocurrency-fraud-and-money-laundering-scheme).

işlemlerini karlı biçimde yürütme hizmeti vermek adına yatırımcının fonlarına erişim sağlayan uygulamaların, hileli işletilerek yatırımcıyı zarara uğrattığı ihtimalde tipiklik sorunları da beraberinde gelecektir. Dolayısıyla, bu tür haksızlıklarla mücadelede, elektronik ortamda yarar elde etmek için mağdurları zarara uğratmaya yönelik aldatıcı girişimleri dolandırıcılık suçu kapsamında cezalandıran bağımsız bir düzenlemenin faydalı olacağını vurgulamak isteriz.

G. Sanal Ortam Bağlantılı Sahtekarlıklar: Metaverse Dolandırıcılığı

Metaverse, kullanıcıların üç boyutlu bir sanal alanda birbirleriyle ve dijital varlıklarla etkileşime girebileceği sanal bir evreni ifade eder[81]. Blokzincir tabanlı uygulamalar olan metaverse platformları ise kullanıcılarına sanal mal veya hizmet satın alabilecekleri dijital ortamlar sunarken, sahip olunan sanal varlıklar *kripto jetonlar* aracılığıyla temsil ve idare edilmektedir. Kullanıcılar, çoğunlukla misli olmayan (*nun-fungible token, NFT)* jetonlardan oluşan metaverse varlıklarını, yine metaverse platformlarına özgü çevrim-içi cüzdanlarda tutarlar. Bu cüzdanlar ayrıca, bağlı olduğu ağın kripto para birimi ve diğer jetonların yönetilmesine de olanak tanır. Böylece, kullanıcılar cüzdanlarındaki diğer kripto varlıklarla istedikleri metaverse kripto jetonunu kolaylıkla satın alabilir. Metaverse dolandırıcılığı olarak anılan sahtekarlık vakıalarının hedefi bahsi geçen cüzdanlardaki varlıklar olup; ya ***i)*** kullanıcılara gerçekte değersiz/işlevsiz kripto jetonlar satın aldırmak, ya ***ii)*** kullanıcıların metaverse cüzdanlarıyla etkileşime geçip, cüzdandaki kripto jetonları ele geçirmek (=cüzdan boşaltma) şeklinde icra edilmektedir.

Birinci tür sahtekarlık ekseriyetle yatırım dolandırıcılığı modeline benzetilebilir: Sözde metaverse işletmesini temsil eden ikna edici internet siteleri, e-postalar, reklamlar aracılığıyla yanıltılan kullanıcılar, değersiz/ sahte NFT satın almaya veya içi boş projeler için ödeme yapmaya sevk edilebilir[82]. ***İkinci tür*** sahtekarlık ise sosyal mühendislik modeliyle karşımıza

---

81 Metaverse hakkında temel açıklamalar için bkz. **Folger**, Jean: "What Does Metaverse Mean and How Does This Virtual World Work?", Investopedia, 05.08.2022, (https://www.investopedia.com/metaverse-definition-5206578). Metaverse ve ceza hukuku ilişkisi hakkında detaylı inceleme için bkz. **Bacaksız**, Pınar: "Metaverse ve Sanal Gerçeklik Ortamları Karşısında Ceza Hukuku", İnÜHFD, 14(1), 2023, s. 291 vd.

82 "Las Vegas resident charged in $45 million metaverse scam that touted trillion-dollar returns", CNBC, TECH 19.05.2023, (https://www.cnbc.com/2023/05/19/nevada-man-added-to-45-million-metaverse-crypto-fraud-indictment.html).

çıkar: Hileyle güveni kazanılan kullanıcının bazı site veya platformlarla bağlantı kurması sağlanır, ardından ustaca hazırlanmış akıllı sözleşmeler kullanıcıya ait dijital cüzdanla etkileşime girer ve cüzdandaki sanal varlıklar boşaltılır. Alternatif yöntemde, kullanıcı satın almamış olmasına rağmen cüzdanına gönderilen tuzak NFT ile etkileşime girmek suretiyle de varlıklarını yitirebilir[83]. Nihayet ***üçüncü tür*** sahtekarlıkta, cüzdan uygulamasının şifresi hileyle ele geçirilerek, içerisindeki varlıklar kullanıcıdan habersiz boşaltılabilir.

Kullanıcının hile etkisiyle değersiz varlık için ödeme yaptığı ya da cüzdandaki jetonları boşaltacak bağlantıya bizzat sebep olduğu ihtimallerde, yarar mağdur eliyle sağlandığı için dolandırıcılık suçunun tasarruf ve zarar unsurları oluşmaktadır. Buna karşılık, geleneksel yöntem olan sahte web sayfaları aracılığıyla metaverse cüzdan giriş bilgilerinin öğrenildiği ve bu suretle erişim sağlanan cüzdanların fail tarafından boşaltıldığı örneklerde, mağduru tasarrufa sevk unsuru gerçekleşmemektedir. Ayrıca, cüzdana erişim ve varlıkları ele geçirme noktasında farklı metotların geliştirilmesi, ilk başta dolandırıcılık suçunu sabit gördüğümüz sahtekarlık yöntemlerini de tartışmaya açabilir. Bu sebeple, elektronik ortamdaki fiillerde yararın faile doğrudan mağdur eliyle geçmesi kıstasını yumuşatan bir dolandırıcılık düzenlemesine olan ihtiyacı yinelemek isteriz.

Söz konusu ihtiyacın TCK m. 244/4'teki düzenlemeyle karşılanabilir olup olmadığı sorulabilir[84]. Ancak, kanaatimizce, metaverse cüzdan uygulamasına rıza dışı erişim bilişim sistemine hukuka aykırı girme suçunu oluştursa da; platformun işleyişine yönelik müdahale olmaksızın varlıkların başka cüzdanlara aktarılması TCK m. 244'te korunan hukuki değeri ihlal etmemektedir[85]. Burada *kullanıcıların hedef alındığı* ancak *bilişim sistemlerinin araç olarak kullanıldığı* yarar sağlama faaliyeti bulunduğundan, sorunun dolandırıcılık kapsamında yapılacak yasal düzenlemeyle çözümlenmesinin yerinde olacağını düşünüyoruz.

---

83 "Cybercriminals target metaverse investors with phishing scams", CNBC, TECH 26.05.2022, (https://www.cnbc.com/2022/05/26/cybercriminals-target-metaverse-investors-with-phishing-scams.html).

84 Hesapların ele geçirilmek suretiyle maddi yarar sağlanması halinde TCK m. 244/4'teki suçun uygulanması gerektiği konusunda bkz. **Bacaksız**, s. 298.

85 Benzer konuda aynı görüş hakkında detaylı açıklama için **Başbüyük**, İsa: "Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi", *Ceza Hukuku Dergisi*, 5(14), Aralık 2010, s. 171.

IV. ÖZELLİK ARZ EDEN MESELELER

A. Amaçsız ve Faydasız Kripto Varlıkların Durumu: Shitcoin/ Memecoin

Piyasada **"shitcoin"** ve **"memecoin"** ifadeleriyle bir tür sahtekarlığı çağrıştıran (=*scamcoin*) kripto varlıkların dolandırıcılık suçuyla ilişkisine değinilmelidir. *Shitcoin*, mevcut kripto varlık protokolleri üzerine inşa edilmiş, amacı ve projesi bulunmayan, kısa ömürlü, genellikle manipülasyon amacıyla üretildiği düşünülen kripto varlıkları işaret etmektedir[86]. *Memecoin* ise, viral haline gelmiş güncel olaylar, resim ve hikayelerden ilham alan; eğlence amacıyla hazırlanmış kripto varlıklar (örn: Dogecoin ve Shiba) için kullanılmaktadır[87]. Elbette, sınıflandırmanın referans alınabilir belirlilikte olmadığı belirtilmelidir[88]. Asıl mesele, sürekli yeni kripto varlığın borsalarda alıcı bulmak üzere listelendiği bir piyasada, belli bir ihtiyacı giderme amacından yoksun, "öylesine" üretilen kripto varlıklar dolayısıyla uğranılan zararların dolandırıcılığa konu sahtekarlık olup olmadığıdır.

Gerçek niyeti gizlemeye yönelik ve hukuken anlamsal değere sahip davranışlar da hilenin konusunu oluşturabilir[89]. Ancak, kripto varlık üretmek ve piyasa sürmek şeklindeki davranış, bizce günümüz şartlarında bu kripto varlığın teknolojik kullanım alanı ve amacının bulunduğu yönünde anlam taşımamaktadır. Bu nedenle, doğrudan muhatabını hataya düşürmeye yönelik tipe uygun bir hileli tasarım olmadığı müddetçe, amaçsız üretilen kripto varlıkları piyasaya arz edip, bunlardan kazanç sağlamanın, yatırımcılar için zarar riski içerse de, dolandırıcılık suçunu karşılamadığı düşüncesindeyiz.

B. Kripto Varlık Alanındaki Risklerin Bilinmesi ve Mağduriyete Etkisi

Yasal denetim bulunmaması, blokzincir tabanlı girişimlerin güvenilirliği konusundaki riski en üst düzeye çıkarmakta ve bu riskin yükünü tama-

---

86 **Frankenfield**, Jake: "Shitcoin", Investopedia, 24.06.2021, (www.investopedia.com/terms/s/shitcoin.asp).

87 **"What Are Meme Coins and How Do They Work?"**, Crypto.com, 11.03.2022, (crypto.com/university/what-are-meme-coins).

88 Nitekim bu hususa dikkat çeken bir yazı için bkz. **Lanz**, Jose Antonio: "What Makes a Shitcoin 'Shit'? Major Figures in Crypto Disagree", Dcrypto, News 13.11.2022, (https://decrypt.co/114305/what-makes-a-shitcoin-shit-major-figures-in-crypto-disagree).

89 **Wessels/Hillenkamp**, BT, § 13, Kn: 496; **Cramer/Perron**, S/S-StGB, § 263, Kn: 14/15. Ayrıca Başbüyük, Hile Unsuru, s. 68 vd.

men yatırımcıya bırakmaktadır. Ancak, herhangi bir sahtekarlık olmasa da, proje aşamasındaki bu girişimlerin teknik sebeple başarıya ulaşamaması; başarıya rağmen bunun, anlık ve sert tepkilere sahne olan kripto varlık piyasasındaki fiyatlanmaya yansımaması yatırımcı için işin doğasından kaynaklanan bir diğer yüksek risk kaynağıdır. Herkesçe bilinen (veya bilinmesi beklenen) böylesine yüksek malvarlığı riskine rağmen, yatırımcının sırf kazanç gayesiyle kripto varlıklara yatırım yapmış olmasının, dolandırıcılık iddialarına etkisi gündeme gelmektedir[90].

Öncelikle, malvarlığı zararına yol açan *"ağ protokollerinin planlandığı gibi çalışmaması, kod yazımından kaynaklı aksaklıklar, sponsor ve ortaklıkların bozulması, siber saldırı vb."* şeklindeki ***işin yürütümüne dair riskler*** ile ***güvene dair riskin*** kaynakları birbirinden farklıdır. Bu nedenle, yatırımları kaybetme ihtimalinin yüksekliği ve kazancın şansa bağlı olması, teorik anlamda kripto varlık ilişkili hileli hareketin, zarara yol açan süreçteki nedenselliğini ortadan kaldırmaz. Ancak bu yaklaşımı, pratikte amaca elverişli şekilde uygulayabilmek her zaman mümkün değildir. Şöyle ki;

(i) **İspat Engelleri:** *Bazı durumlarda*, maddi kayba yol açan riskin nedenini tespit etmek güçleşebilir; sebepler iç içe geçebilir. Örneğin, Terra blokzincir ağının para birimi Luna'nın tarihi çöküşünün, kötü yönetim mi yoksa dolandırıcılık kaynaklı mı olduğu halen netleştirilememiştir[91]. *Öte yandan*, blokzincir tabanlı iş modellerinin henüz fikir aşamasında yatırımcı çekebilme özelliği, bunlarla ilgili abartı/övgü ile sahtekarlığının birbirinden ayırt edilmesini zorlaşmaktadır. Sıklıkla karşılaşıldığı üzere, geliştiricilerin vaat ettikleri geliştirme ve güncellemeleri zamanında veya hiç yapmaması, projeden el çekmeleri veya projeyi pasife almaları, sıfırdan benzer başka proje geliştirmeye yönelmeleri dolandırıcılığa elverişi, ***fakat*** hile ve kastı mahkumiyete yeter ölçüde ispattan yoksundur. Kaldı ki, spekülatif araçların fiyatları herhangi bir nedenle değişkenlik gösterebileceğinden, varlık fiyatının düşmesiyle oluşan zararın, dolandırıcılık suçundaki nedensel sürece uygunluğu da ayrıca problem yaratacaktır.

---

90 Nitekim, My Big Coins yargılamasında, savunma makamının dolandırıcılık suçlamasına karşı ***"kripto varlık dünyasında bir girişimin başarıyla sonuçlanmama riskinin işin doğasından kaynaklandığı ve herkesçe bilindiğini; başarısızlığın mahkumiyete kanıt olamayacağını"*** yönündeki savunması dikkat çekicidir. Kaynak için bkz. **Raymond**, Nate: "My Big Coin virtual currency firm founder convicted of fraud", ROUTERS, 21.07.2022, (https://www.reuters.com/legal/government/my-big-coin-virtual-currency-firm-founder-convicted-fraud-2022-07-21/).

91 Terra blokzincirinin gelişim ve çöküş süreci hakkında ayrıntı için bkz. Wikipedia, **"Terra (blockchain)"**, (https://en.wikipedia.org/wiki/Terra_(blockchain).

(ii)* Unsur Eksikliği:** Doktrindeki hâkim yaklaşım, bir iddianın gerçekliğiyle ilgilenmeyen ve bu konuda beklentisi olmayan mağdurun, farklı motivasyonla tasarrufta bulunduğu hallerde, dolandırıcılık suçunda tipe uygun hatanın oluşmayacağı yönündedir[92]. Bu yaklaşım, kamu otoritelerinden bağımsız işleyen ve yüksek risk iştahının egemen olduğu kripto varlık piyasalarındaki yatırımcı profili açısından anlam ifade etmektedir. Nitekim, birçok yatırımcının, kripto varlıkla ilişkili projenin mevcudiyeti, türü, geleceği, hatta gerçekliğiyle ilgilenmeksizin, yatırım kararı aldığı bilinmektedir. Haliyle, kimi kripto varlık bağlantılı sahtekarlıklarda yatırımcıların kaynağı ne olursa olsun "her türlü riski umursamayarak"*** tamamen kazanç motivasyonuyla şansını denediği, böylece dolandırıcılık suçunun mağduru olamayacakları savunması ileri sürülebilir. Kaldı ki, elektronik ortamdaki sahtekarlıklarda sayısız mağdurun hangi motivasyonla hareket ettiğini ayırt etmek de imkansızdır. Dolayısıyla, çalışmanın birden fazla yerinde vurguladığımız gibi, elektronik ortamdaki dolandırıcılık girişimlerinin cezalandırılmasında mağdurun tipiklikteki rolünü azaltan; aldatıcı hareketlerin hataya düşürmeye ve zarara uğratmaya yönelik olmasını yeterli gören düzenlemenin bu başlık altındaki sorunları da çözebileceği kanaatindeyiz.

C. Hileyle Kripto Varlık Cüzdan-Özel Anahtarını Ele Geçirmek

Kripto varlık cüzdanları, sahip olunan kripto varlıkları gösteren ve bunları yönetmek için kullanılan özel anahtarların saklandıkları çevrim içi (sıcak cüzdan) veya çevrim dışı (soğuk cüzdan) ara yüzlerdir[93]. Çevrim içi cüzdanlarda saklanan özel anahtarları öğrenen üçüncü kişiler, bu anahtarın temsil ettiği kripto varlıklar üzerinde tasarruf imkanına erişmektedir. Haliyle, kimi sahtekarlık vakıaları söz konusu özel anahtarları ele geçirmek üzerine kurgulanmaktadır.

Örneğin, meşru kripto para birimi "Bitcoin Gold" için sözde cüzdan hizmeti sağlayacakları iddiasıyla tuzak web sitesi (mybtgwallet.com) oluşturan failler, kampanya kapsamında, özel anahtarlarını kendileriyle paylaşan yeni kullanıcılardan ömür boyu ücret almamayı vaat eder. Birçok kullanıcı, şüphe doğuracak bu teklife rağmen, siteyi ikna edici bulur ve cüzdan anahtarlarını paylaşırlar. Failler, özel anahtarını öğrendikleri cüzdanlardaki 3

---

92 **Cramer/Perron**, S/S-StGB, § 263, kn: 40. Ayrıca bkz. **Tröndle**, Herbert/**Fischer**, Thomas: S**trafgesetzbuch und Nebengesetze**, 52. Auflage, München, 2004, § 263, kn:33a-33b.

93 Kripto varlık cüzdanlarının türleri ve işleyişi hakkında ayrıntılı inceleme için bkz. **Frankenfield**, Jake: "Cryptocurrency Wallet: What It Is, How It Works, Types, Security", Investopedia, 27.05.2022, (https://www.investopedia.com/terms/b/bitcoin-wallet.asp).

milyon dolarlık kripto varlığı başka cüzdanlara aktararak, haksız yarar elde ederler[94].

Bu tarz sahtekarlıklar, -örneğin bankacılık bilgi ve şifrelerini hedef alan- klasik kimlik avcılığı vakıalarından ayrılmaktadır. Özel anahtarın ele geçirilmesi, aynı zamanda özel anahtarın temsil ettiği değerin hakimiyetinin de faile geçmesini sonuçlar. Ancak, özel anahtarın hileli hareketle ele geçirilmesi, tasarruf unsuru içermediğinden TCK m. 157 anlamında dolandırıcılık suçuna konu bir fiil değildir. Öte yandan, maddi varlığı bulunmadığı için özel anahtar ve temsil ettiği değerlerin çalınmasının hırsızlık suçunu oluşturmayacağı haklı olarak ifade edilmektedir[95]. Nihayet, özel anahtarın kullanılması, bizce TCK m. 244 anlamında bilişim sistemine tipe uygun müdahale de içermemektedir. Özel anahtarlar ve bunların temsil ettiği kripto varlıklara, eşya benzeri bir koruma sağlamanın hukuken etkili bir çözüm olup olmayacağı meselesini, makalemizin kapsamını aşması sebebiyle farklı bir çalışmada ele almayı planlıyoruz. Her halde, hileyle özel anahtarın ele geçirildiği bu tarz örneklerde de "yarar elde etmek/yarara erişmek üzere elektronik ortamda gerçekleştirilen aldatıcı bir girişim" söz konusudur. Dolayısıyla, mağdurun tasarrufta bulunmasını zorunlu kılmaktan ziyade, failin mağdurları aldatma motivasyonunu öne çıkaran bir dolandırıcılık düzenlemesinin bu konudaki ihtiyaca da cevap verebileceğini düşünüyoruz.

D. Ponzi Şeması ve Piramit Satış Yöntemlerinin Tipikliğe Etkisi

Ponzi şeması ve piramit satış, kripto varlık bağlantılı sahtekarlıklar içinde özel bir türü ifade etmemekle birlikte, geleneksel yöntem olarak adından sıkça söz ettirmektedir[96]. Bu sebeple, bağımsız bir sahtekarlık türü yerine, harici mesele olarak ele alınmıştır.

Elektronik ortama uyarlanma kabiliyeti yüksek olan ponzi şeması, kripto varlık piyasasında yatırım dolandırıcılığı formunda karşıma çıkmaktadır. Girişimciler, getiri vaat edebilecekleri bir uydurma yatırım platformu oluşturur, vadesi gelen ilk ödemeler sisteme dahil olan katılımcıların yatırımlarıyla karşılanarak kazanç görüntüsü yaratılır, yatırımcı sayısı arttıkça para çekme işi zorlaştırılır ve kolluk güçlerinin müdahalesiyle gerçek ortaya

---

94 **"Bitcoin Gold Wallet Scam Nets $3 Million in Illicit Earnings"**, CoinDesk, 22.11.2017, (https://www.coindesk.com/markets/2017/11/22/bitcoin-gold-wallet-scam-nets-3-million-in-illicit-earnings).

95 **Aksoy Retornaz**, s. 299-300.

96 **Bulut**, Esra: "Klasik Ponzi Girişimcilikten Dijital Ponzi Girişimciliğe: Benzer Taktikler, Farklı Platformlar", Finansal Araştırmalar ve Çalışmalar Dergisi, Cilt 14, Sayı 26, Ocak 2022, s. 34.

çıkar[97]. Kazanç görüntüsü, aldatıcı ve oyalayıcı davranışlara başvurmak suretiyle, yatırımcılara herhangi bir ödeme yapmadan da sağlanabilir. Gerçekte var olmayan ticari faaliyet ve gelir üzerinden, kâr payı vaadiyle yatırım çeken ponzi şeması, dolandırıcılık suçuna uygundur. Ancak, geleneksel aldatıcı metotların dışında, akıllı sözleşmeler ve algoritmalar aracılığıyla yürütülen merkeziyetsiz finans şemalarının ponzi mantığıyla işletilmesi -tespiti güç olsa da- mümkündür. Ayrıca ponzi niteliğini öngörerek sisteme dahil olanların TCK m. 157 kapsamındaki mağdur sıfatı tartışmalı hal alabilir. Elektronik ortamdaki aldatıcı girişimleri dolandırıcılık kapsamında cezalandıran fail merkezli harici düzenlemenin, bu hususlarda da fayda sağlayabileceği belirtilmelidir.

Piramit satış ise, sözde bir kripto varlığın doğrudan satışla piyasaya sürüldüğü, pazarlama aşamasına katılımcıların da kademe itibariyle dahil edildiği, satıcı kademesi arttıkça üst kademedekilerin daha fazla komisyona hak kazandığı (=çok katmanlı pazarlama ağı) olaylarda kendini göstermektedir[98]. Kartopu sözleşmesi şeklinde de anılan bu satış yönteminde, çok fazla yatırımcının, gösterişli ve umut verici temaslarla sisteme dahil edilmesi hedeflenir. Her ne kadar piramit satışları yasaklayan Tüketicinin Korunması Hakkında Kanun m. 80/2 dolandırıcılık suçuna atıfta bulunsa da; bu yöntemin bire bir dolandırıcılık suçuna uygunluğu tartışmalıdır[99]. Şüphesiz, tamamen sahte kripto varlığın pazarlandığı OneCoin gibi olaylarda, dolandırıcılık suçunun oluştuğu açıktır[100]. Ancak, somut olay özelinde dolandırıcılık suçunun tipiklik unsurlarını ihlal etmeden de piramit satış sistemi işletilebilir[101]. Kaldı ki, piramit satışlarda blokzincirden yararlanılması halinde, tipiklik sorunu daha karmaşık bir hal alacaktır. Dolayısıyla, piramit satışları

---

97 **Singletary**, Michelle: "Six signs crypto investment is a classic Ponzi scheme", The Washington Post, 18.05.2022, (https://www.washingtonpost.com/business/2022/05/18/fbi-eminifx-crypto-pyramid-scam/).

98 Nitekim "OneCoin" vakasında, çok seviyeli bir satış ağı kurulduğu için piramit satışa örnek gösterilmektedir: **Jeager**, Jaclyn: "Anatomy of a cryptocurrency pyramid scheme", Compliance Week, 01.04.2019, (www.complianceweek.com/risk-management/anatomy-of-a-cryptocurrency-pyramid-scheme/26820.article). Ayrıca, **Aksoy Retornaz**, s. 304.

99 Bu hususstaki görüşler için bkz. **Başbüyük**, Hile Unsuru, s.293; **Aksoy Retornaz**, s. 304.

100 **Aksoy Retornaz**, s. 304.

101 **Hakeri**, Hakan: "Zincirleme-Piramitsel Oyunlar Düzenleme Suçu", YD, Ocak-Nisan 2001, Sayı: 1-2, s. 167. Özellikle katılımcıların bilgilendirildiği durumlarda dolandırıcılık suçunun oluşmayacağı hususunda **Kangal**, s. 260. Buna ek olarak, sürecin işeyişinin hileli hareketle gizlenmediği ve katılımcıların bilgilendirilmesinin beklenmediği durumlarda da hileden bahsetmek mümkün olmamalıdır (bkz. **Başbüyük,** Hile Unsuru, s. 295).

dolandırıcılık suçundan bağımsız cezalandırmaya yönelik ihtiyaç[102], bu alanda da kendini göstermektedir.

V. DEĞERLENDİRME VE GÖRÜŞÜMÜZ

TCK m.157'deki düzenleme, hileye başvuran fail ile aldatılan kişi arasındaki ilişkinin özelliklerini bütün olarak suç tanımına dâhil etmekte; böylece ***mağdur,*** hem hataya düşürülen hem de tasarrufta bulunmak suretiyle yarar geçişini sağlayan *belli/belirlenebilir kimse* olarak tipikliğin önemli şartı haline gelmektedir. Oysa bu durumun, kripto varlık bağlantılı sahtekarlıklarla mücadelede tıkanıklığa yol açması kaçınılmazdır. Şöyle ki;

-i-

Kripto varlık bağlantılı sahtekarlıklar yöntem itibariyle, ya ***(i) doğrudan blokzincir-kripto varlıklardan yararlanmak*** *(örn: likidite havuzu boşaltma, metaverse dolandırıcılığı);* ya ***(ii) blokzincir-kripto varlıkları araç olarak kullanmak*** *(örn: yatırım dolandırıcılığı)* ya da ***(iii) blokzincir-kripto varlıkların bahsi geçirilmek*** *(örn: uydurma kripto para birimi satmak)* suretiyle icra edilmektedir. Doğrudan blokzincir üzerinde inşa edilen ilk tür sahtekarlıklar, TCK m. 157'deki tanımın dışında yeni durumlar oluşturmaya açıktır. İkinci tür sahtekarlıklar ise çoğunlukla dolandırıcılık suçuna denk düşmekle birlikte, ispat konusunda gri alanlar oluşturmaktadır. Elbette, bu durum da dolandırıcılık suçunun karmaşık yapısıyla ilgilidir. Nihayet, üçüncü tür sahtekarlıklar dolandırıcılık suçuna uyum ve ispat konularında özellikli bir hal yaratmamaktadır.

-ii-

Hilenin diğer unsurlarla olan ilişkisi, bugüne kadar dolandırıcılık suçunu hırsızlık ve güveni kötüye kullanma yahut piyasa dolandırıcılığı gibi bağlantılı suçlardan ayırt etmeye yarayan önemli bir sınır çizgisi olmuştur. Ancak, bu sınırın gözetilmesindeki hukuki fayda, "ekonomik değer" hakimiyetine farklı-sanal bir boyut getiren blokzincir ortamında iyice önemini yitirmeye adaydır.

-iii-

Her halde, blokzincir ve kripto varlık bağlantılı sahtekarlıklarda öne çıkan, "*i) çoğunlukla anonim olan genel kullanıcı kitlesinin hedef alınması ve mağdur kimliğinin önemsizleşmesi, ii) mağdurları doğrudan hedef alma ihtiyacı duymaması, iii) kullanıcıların gerçekten kandırılıp kandırılmadığını*

---

[102] Bu hususstaki ihtiyacı dile getiren görüşler için **Kangal**, s. 260; **Ekici Şahin**, s. 504; **Aydın**, Murat: "Piramit Satış Sistemlerinin Ceza Hukuku Açısından Değerlendirilmesi", Terazi Hukuk Dergisi, Cilt 9, Sayı 100, Aralık 2014, s. 466.

denetlemenin imkansızlığı, iv) cüzdan hizmetleri veya akıllı sözleşmelerin dahiliyle yarara erişme şeklinin değişmesi" gibi özellikler, dolandırıcılık suçunun geleneksel tanımıyla çatışma içerisindedir. Buna rağmen söz konusu sahtekarlıkları mevcut dolandırıcılık suçu kapsamında cezalandırmaya çalışmak, hukuk ve ispat kaidelerinin esnetilmesine yol açacaktır. Cezalandırmama yoluna gidilmesi ise blokzincir ve kripto varlık bağlantılı sahtekarlıklarla mücadeleyi zayıflatacaktır.

Bizce, elektronik ortamda işlenen fiiller bakımından mağdurun rolünün azaltıldığı "fail merkezli" bir dolandırıcılık düzenlemesine olan ihtiyaç gözden geçirilmeli; maddi yarar elde etmek üzere, -yetkisiz erişim dahil- kişilerin zararına yol açan aldatıcı tertipleri cezalandıran bağımsız bir hükme yer verilmelidir. Bu hüküm sayesinde, yarar üzerinde kontrol ve erişim imkanı sağlayan vasıtaların (cüzdan özel anahtarı gibi) elde edilmesi de dolandırıcılık suçunun kapsamına alınabilecek; böylece tasarruf unsuruyla ilişkili elektronik ortamdaki çoğu vakıada pratik önemi bulunmayan ve uygulama engeli yaratabilecek tartışmaların önüne geçilebilecektir.

Öte yandan, dolandırıcılık suçunun kapsamı dışında kalan bağlantılı hususlarla ilgili olarak;

i. Kripto para borsacılık faaliyetlerinde, sözleşmeye aykırı tasarruflar veya varlıkları riske sokan durumları gizlemeye yönelik hileli davranışların cezalandırılması için "Bankacılık zimmeti" (BK m. 160), "Düzeltici, iyileştirici ve kısıtlayıcı önlemleri almamak" (BK m. 152) vb. şeklindeki bankacılık sektörüne dair benzer suç tiplerine yer verilmesi;

ii. Dolandırıcılık suçunun kapsamı dışında kalabilecek ve ispat engeline takılabilecek durumlar için hukuka aykırı fiilleri işlenmesini mümkün kılmak veya kolaylaştırmak üzere elektronik ortamda platform işletmeyi cezalandıran torba düzenleme çıkarılması;

iii. Fiyat manipülasyonuna yol açan girişimlerin organizatörlerini cezalandırmak amacıyla TCK m. 237'de değişiklik yapılması;

iv. Protokoller aracılığıyla hile unsuru olmadan işletilmesi olasılık dahilinde olan piramit satışların ayrıca ve açıkça suç olarak tanımlanması;

yönündeki kanaatlerimizi çalışmamızın sonucu olarak paylaşmak ve bu vesileyle kripto varlık bağlantılı sahtekarlıkların cezalandırılması sürecinde yaşanması muhtemel sorunlara dikkat çekmek isteriz.

KAYNAKÇA

Akbulut, Berrin: "Fiyatları Etkileme Suçu", TAAD, Yıl:6, Sayı:20 (Ocak 2015), s. 25-57.

Akçakaya, Yusuf: "Saadet zinciri ile Bitcoin vurgunu", Gazete Oksijen, 07.05.2021, (www.gazeteoksijen.com/turkiye/saadet-zinciri-ile-bitcoin-vurgunu-26804).

Aksoy Retornaz, E. Eylem: "Ceza Hukuku Perspektifinden Blokzincir", Gelişen Teknolojiler ve Hukuk I - Blokzincir ve Hukuk, 2. Baskı, İstanbul 2021.

Aktolga Öztürk, Ayça: "Kripto Paralara İlişkin Dolandırıcılık Yöntemleri", Finans Hukuku ve Gündemi Dergisi, Sayı 3, Şubat 2020, (https://www.kanunum.com/file/cid9721408_vid18006506_ fid1042080)

Altınöz, Utku/**Altınöz**, Hasip: Hile Ekonomisi, Piyasalarda Yatırımcı Psikolojisi ve Finansal Skandallar, Seçkin Yayıncılık, 2. Baskı, Ankara 2020.

Aydın, Murat: "Piramit Satış Sistemlerinin Ceza Hukuku Açısından Değerlendirilmesi", Terazi Hukuk Dergisi, Cilt 9, Sayı 100, Aralık 2014, s. 461-466.

Bacaksız, Pınar: "Metaverse ve Sanal Gerçeklik Ortamları Karşısında Ceza Hukuku", İnÜHFD, 14(1), 2023, s. 289-303.

Balcı, Murat/**Çakır**, Kerim: "Kripto Para Borsaları ve Güveni Kötüye Kullanma Suçu", Prof. Dr. Selçuk Öztek'e Armağan, Ankara 2022, s. 447-473.

Balcı, Murat/**Çakır**, Kerim: "Kripto Para Dolandırıcılığı", Terazi Hukuk Dergisi, 16(181), 2021, s. 1684-1689.

Balcı, Umut: "Kripto Paraların Ceza Hukuku Boyutu ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri", TBBD, 2021 (155), s. 203-259.

Başbüyük, İsa: "Blokzincir Üzerinden Fon Toplama: Kripto Varlık Arzı (ICO) ve Sermaye Piyasası Kanunundaki Suçlarla İlişkisi", (Ed.) Ekici, Şahin/Solak, Ekrem/Avşar, Muhammed Emre, Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu Tebliğler Kitabı, Adalet Yayınevi, Ankara 2021, s. 313-328, *(Anılış, "Blokzincir Üzerinden Fon Toplama").*

Başbüyük, İsa: "Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi", *Ceza Hukuku Dergisi*, 5(14), Aralık 2010, s. 151-192.

Başbüyük, İsa: "İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi", Ceza Hukuku Dergisi, Sayı:21 - Nisan 2013, s. 197-214.

Başbüyük, İsa: Dolandırıcılık Suçunda Hile Unsuru, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Doktora Tezi, 2019, *(Anılış, "Hile Unsuru").*

Bilgili, Fatih/**Cengil**, M. Fatih: "Bitcoin Özelinde Kripto Paraların Eşya Niteliği Sorunu", SSRN 2019, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432713).

Bulut, Esra: "Klasik Ponzi Girişimcilikten Dijital Ponzi Girişimciliğe: Benzer Taktikler, Farklı Platformlar", Finansal Araştırmalar ve Çalışmalar Dergisi, Cilt 14, Sayı 26, Ocak 2022, s. 18-54.

Cramer, Peter/**Perron**, Walter: S/S-StGB § 263, 29. Auflage, München, 2014.

Danial, Kiana: "3 Different Types Of Cryptocurrency Exchanges: CEX, DEX, And Hybrid", Nasdaq, 12.07.2018, (www.nasdaq.com/articles/3-different-types-cryptocurrency-exchanges-cex-dex-and-hybrid-2018-07-12).

Dhir, Rajeev: "Pump and Dump", Investopedia, Laws & Regulatıons - Crıme & Fraud, 02.06.2021, (https://www.investopedia.com/terms/p/pumpanddump.asp9).

Doyle, Charles: Mail and Wire Fraud: A Brief Overview of Federal Criminal Law, Congressional Research Service, CRS REPORT, 11.02.2019.

Dülger, Murat Volkan/**Özkan**, Onur: "Kirpto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi", Prof. Dr. Mehmet Emin Artuk'a Armağan, Ankara 2020, s. 963-994.

Eker Kazancı, Behiye/**Zeyrek**, İlker: "TCK'da Dolandırıcılık Suçu", D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, Cilt 21, Özel Sayı, 2019, s. 517-583.

Ekici Şahin, Meral: Dolandırıcılık Suçu, Adalet Yayınevi, Ankara 2019.

Frankenfield, Jake: "Cryptocurrency Wallet: What It Is, How It Works, Types, Security", Investopedia, 27.05.2022, (https://www.investopedia.com/terms/b/bitcoin-wallet.asp).

Frankenfield, Jake: "Initial Coin Offering (ICO)", Investopedia, 03.11.2020, (www.investopedia.com/terms/i/initial-coin-offering-ico.asp).

Frankenfield, Jake: "Shitcoin", Investopedia, 24.06.2021, (www.investopedia.com/terms/s/shitcoin.asp).

Gensler, Chair Gary: "Prepared Remarks of Gary Gensler On Crypto Markets Penn Law Capital Markets Association Annual Conference", U.S. SECURITIES AND EXCHANGE COMMISSION, Speech, 04.04.2022, (https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422).

Gouda, Namrata: "Key Differences Between IDO, ICO, IEO, and IPO", https://medium.com/geekculture/key-differences-between-ido-ico-ieo-and-ipo-10dad82b9e5d).

Haentjens, Matthias/**Graff**, Tycho De/**Kokorin**, Ilya: "The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them", Singapore Journal of Legal Studies, No 2, 2020, s. 526-563.

Hakeri, Hakan: "Zincirleme-Piramitsel Oyunlar Düzenleme Suçu", YD, Ocak-Nisan 2001, Sayı: 1-2, s. 137-172.

Heimbach, Lioba/**Wnag**, Ye/**Wattenhoffer**, Roger: "Behavior of Liquidity Providers in Decentralized Exchanges", Cornell University, arXiv.org, 11.10.2021, (https://arxiv.org/pdf/2105.13822.pdf).

Hong, Euny: "How Does Bitcoin Mining Work?", Invostepedia, 05.05.2022, (https://www.investopedia.com/tech/how-does-bitcoin-mining-work/).

Jeager, Jaclyn: "Anatomy of a cryptocurrency pyramid scheme", Compliance Week, 01.04.2019, (www.complianceweek.com/risk-management/anatomy-of-a-cryptocurrency-pyramid-scheme/26820.article).

Johnson, Kristin N.: "Decentralized Finance: Regulating Cryptocurrency Exchanges", Wm. & Mary Law Review, Volume 62, 2021, s. 1911-2001.

Kangal, Zeynel: Dolandırıcılık Suçu, Özel Ceza Hukuku Cilt IV, Malvarlığına Karşı Suçlar, On İki Levha Yayıncılık, İstanbul 2018.

Kapancı, Kadir Berk: "Özel Hukuk Penceresinden Blokzincir: Sanal Para Değerleri ve Akıllı Sözleşmeler Üzerine Değerlendirmeler", Gelişen Teknolojiler ve Hukuk 1- Blokzincir, On İki Levha Yayıncılık, İstanbul 2020, s. 111-154.

Kleinberg, Bennet/**Kamps**, Josh: "To The Moon: Defining And Detecting Cryptocurrency Pump-And-Dumps", Crime Science, 7, No: 18, 2018, s. 3, (https://crimesciencejournal.biomedcentral.com/track/pdf/10.1186/s40163-018-0093-5.pdf).

Kurşat, Zekeriya: Borçlar Hukuku Alanında Hile Kavramı, Seçkin Yayıncılık, İstanbul 2003.

Lanz, Jose Antonio: "What Makes a Shitcoin 'Shit'? Major Figures in Crypto Disagree", Dcrypto, News 13.11.2022, (https://decrypt.co/114305/what-makes-a-shitcoin-shit-major-figures-in-crypto-disagree).

McGinley, Ian: "Wire fraud: the most powerful law in crypto right now", Routers, 23.08.2022, (www.reuters.com/legal/legalindustry/wire-fraud-most-powerful-law-crypto-right-now-2022-08-23/).

Nilsson, Kim: "The missing MtGox bitcoins", 19.04.2015, WIZSEC Bitcoin Security Specialist, (https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html).

O'Connor, Fergal/**Lucey**, Michael: "The Incomplete History of My Big Coin", Handbooks in Alternative Investments, (Editors J. Batten, B. Lucey and S. Corbett), (internet kopyası için https://ssrn.com/abstract=3905960).

Oliveira, Luis/**Zavolokina**, Liudmila/**Bauer**, Ingrid/**Schwabe**, Gerhard: "To Token or not to Token: Tools for Understanding Blockchain Tokens", In: International Conference of Information Systems (ICIS 2018), San Francisco, USA, 12-16/12/2018, ICIS, s. 1-18.

Özbek, Veli Özer/**Doğan**, Koray/**Bacaksız**, Pınar: Türk Ceza Hukuku Özel Hükümler, 17. Baskı, Seçkin Yayıncılık, Ankara 2022.

Özdemir, Gençer: "Kripto Paraların Eşya Niteliği", SDÜHFD, Cilt 11, Sayı 1, 2021, s. 289-306.

Özen, Ercan/**Vurur**, N. Sertap: "Digital Era Digital Risks: The Case Study of Turkish Crypto Currencies Market", 15'th International Scientific Practical Conference, Volume 2, Moldova 2021, s. 10-13, (https://ibn.idsi.md/sites/default/files/imag_file/p-10-13.pdf).

Penke, Michel: "40 Millionen verdient, Firma unerreichbar, Chef twittert Urlaubsbilder", WETL, Wirtschaft & Technik, 18.04.2018, (https://www.welt.de/wirtschaft/webwelt/article175595788/Fintech-Start-up-Hack-oder-ICO-Betrug-Was-ist-bei-Savedroid-los.html).

Puggioni, Valerio: "Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it", Cointelegraph, 06. 02.2022, (https://cointelegraph.com

/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it).

Raymond, Nate: "My Big Coin virtual currency firm founder convicted of fraud", ROUTERS, 21.07.2022, (https://www.reuters.com/legal/government/my-big-coin-virtual-currency-firm-founder-convicted-fraud-2022-07-21/).

Reiff, Nathan: "What Are Centralized Cryptocurrency Exchanges?", Investopedia, 27.08.2021, (https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-ex changes/).

Rossow, Andrew: "What Are Rug Pulls? Are They a Crime?", NFT NOW, 28.11.2022, (https://nftnow.com/guides/scams-explained-what-are-rug-pulls-and-are-they-a-crime/).

Santos, Michael: "Crypto Pump & Dump Fraud", Cryptocurrency Securıtıes Fraud (McAfee Pump & Dump Case), PRISON PROFESSORS, (https://prisonprofessors.com/crypto-pump-dump-fraud/).

Sarel, Roee: "Property Rights in Cryptocurrencies: A Law and Economics Perspective." North Carolina Journal of Law & Technology, vol. 22, no. 3, April 2021, s. 389-446.

Sarıkaya, Samet: "Kripto Varlık Dolandırıcılığı", Anadolu Üniversitesi Hukuk Fakültesi Dergisi, Cilt 9, Sayı 2, Temmuz 2023, s. 555-581.

Satsuk, Pavel: "Types of Cryptocurrency Exchanges", soft-fX, (www.soft-fx.com/blog/types-of-cryptocurrency-exchanges/).

Sherry, Benjamin: "What Is an ICO?", Investopedia, 25.08.2021, (www.investopedia.com/news/what-ico/).

Singletary, Michelle: "Six signs crypto investment is a classic Ponzi scheme", The Washington Post, 18.05.2022, (https://www.washingtonpost.com/business/2022/05/18/fbi-eminifx-crypto-pyramid-scam/).

Stokel-Walker, Chris: "How a Squid Game Crypto Scam Got Away With Millions", WIRED, Security, 02.12.2021, (https://www.wired.com/story/squid-game-coin-crypto-scam/).

Tahan, Özge: "Kripto Paraların Türk ve Alman Ceza Hukuku Düzenlemeleri Yönünden Değerlendirilmesi" Suç ve Ceza Dergisi, C: 14, S:1, 2021, s. 99-159.

Tarakçıoğlu, Esra: "Kripto Varlıklar ve Ceza Hukuku Sorumluluğu", Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, Cilt 11, Sayı 2, Aralık 2021, s. 295-352.

Telvetoğlu, Mete: Hukuki Yönleriyle Kripto Varlıklar ve Kripto Varlıkların İlk Arzı (Initial Coin Offering), 2. Baskı, İstanbul 2021.

Tepe, İlker: "Fiyatları Etkileme Suçu (TCK m. 237)", Ceza Hukuku Dergisi, Cilt: 5, Sayı: 14, Aralık 2010, s. 89-102.

Tezcan, Durmuş/**Erdem**, Mustafa Ruhan/**Önok**, Rıfat Murat: Teorik ve Pratik Ceza Özel Hukuku, 20. Bası, Seçkin Yayıncılık, Ankara 2020.

Tröndle, Herbert/**Fischer**, Thomas: S**trafgesetzbuch und Nebengesetze**, 52. Auflage, München, 2004.

Uçkun, Nurullah/**Dal**, Lokman: "Kripto Para Yatırımcılarında Finansal Risk Toleransı", Muhasebe ve Finansman Dergisi, Sayı 89, Ocak 2021, s.155-170.

Wessels, Johannes/**Hillenkamp**, Thomas: Strafrecht BT 2, 39. Aufl. 2016.

Xu, Jiahua/**Livshits**, Benjamin: "The Anatomy of a Cryptocurrency Pump-and-Dump Scheme", 28th USENIX Security Symposium (USENIX Security 19), 2019, Santa Clara, CA, USA, (https://www.usenix.org/system/files/sec19-xu-jiahua_0.pdf).

Young, Martin: "Polywhale Team Jumps Ship Amid DeFi Rug Pull Accusations", Yahoo Finance, 22.06.2021, (https://finance.yahoo.com/news/).

Zetzsche, Dirk A./**Buckley**, Ross P./**Arner**, Douglas W./**Linus**, Föhr: "The ICO gold rush: it's a scam, it's a bubble, it's a super challenge for regulators" University of Luxembourg Law Working Paper, No. 11, 2017, UNSW Law Research Paper, No. 83.

Zhang, Qiang/**Liao**, Baoyu/**Yang**, Shanlin: "Application of blockchain in the field of intelligent manufacturing", Frontiers of Engineering Management, Volume 7, 2020, s. 578-591.