

**T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**KRİPTO PARA BİRİMİ OLARAK BITCOIN VE
CEZA HUKUKU**

YÜKSEK LİSANS TEZİ

Erdal DURDU

Tez Danışmanı: Doç. Dr. E. Eylem AKSOY RETORNAZ

AĞUSTOS 2018

**T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

**KRİPTO PARA BİRİMİ OLARAK BITCOIN VE
CEZA HUKUKU**

YÜKSEK LİSANS TEZİ

Erdal DURDU

Tez Danışmanı: Doç. Dr. E. Eylem AKSOY RETORNAZ

AĞUSTOS 2018

ÖNSÖZ

Bu çalışmada, bilişim teknolojilerinin en son yeniliklerinden biri olan kripto para birimlerinin ceza hukuku bakımından bir değerlendirmesi yapılmaya çalışılmıştır. Her gün yeni bir kripto para birimi duyurusunun yapıldığı bir ortamda – bugünkü rakam 1664-, henüz on yıllık bir geçmişi dahi olmamasına rağmen, bu teknolojik yeniliğin eriştiği işlem büyüklüğü, kullanım yaygınlığı ve çeşitliliği göz önüne alındığında, önümüzdeki dönemlerde hukuk dâhil birçok alanın gözde konusunun kripto para birimleri olacağını düşünüyorum.

Kripto para birimi, blokzinciri (blockchain) denilen teknolojik yapının sadece bir ürünü olup, çok yakın gelecekte, hukuki kişilik, hukuki sorumluluk ve bireysel temsil gibi temel hukuki kavramların yeniden gözden geçirilmesine neden olacağı öne sürülmektedir. Akıllı sözleşmeler veya akıllı mülklerle, gerçek insan ile makine veya makine ile makine arasında kurulabilecek yeni sözleşme ve mülkiyet ilişkilerinin ortaya çıkacağı, devlet tarafından yürütülen bütün kamu hizmetlerinin, blokzinciri temelinde yeniden kurgulanacağı da öne sürülenler arasında. Bunların ne kadarı gerçekleşecek veya birer iddia olarak kalacak, ileride göreceğiz. Fakat değişik alanlarda bu teknolojik yeniliği kullanmanın yollarının arandığını gözlemlemekteyiz.

Ülkemizde hukuk alanında kripto para birimleriyle ilgili yapılan ilk çalışmalardan biri sayılabilecek bu tezin ortaya çıkmasında değerli görüşleriyle çalışmama yön veren ve beni sabırla dinleme nezaketinde bulunan sevgili hocam Doç. Dr. E. Eylem Aksoy Retornaz’a en içten saygı ve teşekkürlerimi sunmak isterim.

Kendisinden ders alma onuruna eriştiğim sayın Prof. Dr. Ahmet Ulvi Türkbağ hocama en derin saygı ve şükranlarımı sunmak isterim.

Kendileriyle geçirmem gereken vakitleri, onlardan esirgeyerek bu tezi hazırlamak için aylarca bilgisayar başında gecelemelerime tahammül eden ve her zaman destekçim olan sevgili eşim Ayşe Durdu’ya ve çocuklarıma teşekkür ederim.

Bu çalışmamdan dolayı hastalığı sırasında yeteri kadar yanında olamadığım ve hâlâ iyileşme sürecinde olan sevgili anneciğim Zeynep Durdu’ya acil şifalar diliyorum. Babacığım, beni ötelere izlediğini biliyorum. Ruhun şad olsun.

Erdal Durdu
Kartal, 2018

İÇİNDEKİLER

ÖNSÖZ	ii
İÇİNDEKİLER	iii
KISALTMALAR	xii
RÉSUMÉ	xiv
ABSTRACT	xix
ÖZET	xxiii
GİRİŞ	1
BİRİNCİ BÖLÜM: KRİPTO PARA BİRİMLERİ VE BITCOIN ÖRNEĞİ	7
§1. Dijital Para Birimi Kavramı	7
I. Dijital Para	7
A. Elektronik Para	7
B. Sanal Para Birimi	9
II. Bir Dijital Para Olarak Kripto Para	10
III. Kripto Para Birimi ile Elektronik Para Arasındaki Farklar	12
IV. Kripto Para Birimi ile Diğer Sanal Para Birimleri Arasındaki Farklar	13
§2. Kripto Para Birimlerinin Ortaya Çıkışı ve Tarihsel Gelişimi	14
§3. Kripto Para Birimlerinin Ortak Özellikleri	20
A. Açık Kaynak Kod	20
B. Kriptografi	21
1. Hash Fonksiyonu	22
2. Simetrik-Anahtar Şifreleme	24
3. Açık Anahtar Şifreleme	24
4. Dijital İmza	25
C. Merkeziyetçilik	26
D. Anonimlik	27
E. Diğer Ortak Özellikler	29
§4. Kripto Para Birimleri İçin Hukuksal Düzenleme Arayışları	31
I. Hukuksal Düzenleme İhtiyacı	31
II. Tavsiyeler	33
III. Hukuksal Tanım Eksikliği	34
V. Uluslararası Arayışlar	36
A. FATF (Mali Eylem Görev Gücü)	36
B. UNODC (Birleşmiş Milletler Uyuşturucu ve Suç Ofisi)	37

C. OECD (Ekonomik İşbirliği ve Kalkınma Örgütü)	39
D. IMF (Uluslararası Para Fonu)	40
VI. Bölgesel ve Ulusal Arayışlar	42
A. Avrupa Birliği	42
1. EBA (Avrupa Bankacılık Otoritesi).....	43
2. ECB (Avrupa Merkez Bankası)	46
B. ABD.....	49
C. Almanya	49
D. Çin	49
E. Japonya	50
F. İngiltere	50
G. Rusya.....	50
H. Türkiye	51
§5. Kripto Para Birimlerinin Ceza Hukuku Bakımından Değerlendirilmesi	52
I. Kripto Para Birimlerinin Değer Olarak Sınıflandırılması	52
II. Kripto Para Birimleri Kullanımının Yasal Durumu	55
§5. Bir Kripto Para Birimi Olarak Bitcoin	57
I. Bitcoin'in ortaya çıkışı	57
II. Bitcoin Sistemine Genel Bakış.....	60
A. Bitcoin Vakfı	61
B. Bitcoin Yazılımı	61
C. Topluluk Platformları	61
D. Bitcoin Geliştirme Önerileri.....	62
III. Bitcoin Ekosistemi	62
A. Kullanıcılar.....	62
B. Takas Merkezleri	62
C. Madenciler	63
D. Yazılım Geliştiriciler.....	63
IV. Teknolojik Yapı	63
A. Bitcoin Adresi	63
B. Cüzdan.....	65
1. Deterministik Cüzdanlar	66
2. Çevrimiçi Cüzdanlar	66
3. Soğuk Cüzdanlar	67

4. Kâğıt Cüzdanlar	67
5. Cüzdan Hizmeti Veren Platformlar.....	67
6. Beyin Cüzdanı	67
C. Hareketler	68
1. Hareket yapısı.....	68
2. Hareket Ücreti	69
3. Hareket Türleri	70
4. Hareketin Onaylanması	70
5. Hareketin Doğrulanması	71
D. Madencilik.....	71
1. Blok Yapısı.....	73
2. Coinbase Hareketi	73
3. İş Kanıtı	74
4. Blokzincirinin Çatallanması.....	74
5. Madencilik Türleri	75
6. Diğer İş Kanıtı Yöntemleri.....	76
E. Blokzinciri	77
F. Bitcoin Ağı.....	78
G. Bitcoin Güvenliği	80
1. Çifte Harcama Sorunu.....	80
2. Kullanıcılar İçin Güvenlik Önerileri	81
H. Diğer Kripto Para Birimleri.....	82
1. Altcoin'ler	82
2. Metacoin'ler	83
V. Diğer Blokzinciri Uygulamaları.....	86
A. Akıllı Sözleşmeler	86
B. Dijital Varlıklar	87
C. Kitlesel Fonlama.....	87
D. Akıllı Mülkiyet.....	87
E. Mikro Ödemeler.....	87
F. Dijital Noterlik.....	88
İKİNCİ BÖLÜM: CEZA HUKUKU BAKIMINDAN KRİPTO PARA BİRİMLERİ	89
§1. Kripto Para Birimi Kullanımının Türk Ceza Kanunu'nda Düzenlenen Suçlar Bakımından İncelenmesi	89

I. Malvarlığına Karşı İşlenen Suçlar	89
A. Hırsızlık Suçu (TCK m. 141-147).....	92
1. Genel Olarak	92
2. Suçun Faili	92
3. Suçun Mağduru	93
4. Suçla Korunan Hukuki Yarar	95
5. Suçun Maddi Konusu	95
6. Suçun Unsurları.....	102
a. Maddi Unsur	102
b. Hukuka Aykırılık Unsuru	103
c. Kusurluluk.....	104
7. Suç ve Cezaya Etki Eden Nedenler.....	106
a. Suçu Ağırlaştıran Nedenler.....	106
aa. Hırsızlık suçunun, kime ait olursa olsun kamu kurum ve kuruluşlarında veya ibadete ayrılmış yerlerde bulunan ya da kamu yararına veya hizmetine tahsis edilen eşya hakkında işlenmesi.....	107
bb. Hırsızlık suçunun bir afet veya genel bir felaketin meydana getirebileceği zararları önlemek veya hafifletmek maksadıyla hazırlanan eşya hakkında işlenmesi	108
cc. Hırsızlık suçunun adet veya tahsis veya kullanımları gereği açıkta bırakılmış eşya hakkında işlenmesi.....	108
dd. Hırsızlık suçunun kişinin malını koruyamayacak durumda olmasından veya ölmesinden yararlanarak işlenmesi	108
ee. Hırsızlık suçunun doğal bir afetin veya sosyal olayların meydana getirdiği korku veya kargaşadan yararlanarak işlenmesi	109
ff. Hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi.....	109
gg. Hırsızlık suçunun tanınmamak için tedbir olarak veya yetkisi olmadığı halde resmi sıfat takınarak işlenmesi	112
hh. Hırsızlık suçunun gece işlenmesi	113
b. Suçu Hafifleten Nedenler.....	113
aa. Hırsızlık suçunun paydaş veya elbirliği ile malik olunan mal üzerinde işlenmesi.....	113
bb. Hırsızlık suçunun bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi	114
cc. Malın değerinin az olması	114

dd. Hırsızlık suçunun, malın geçici bir süre kullanılıp zilyedine iade edilmek üzere işlenmesi	115
c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep	116
d. Etkin Pişmanlık.....	116
8. Suçun Özel Görünüş Şekilleri.....	117
a. Teşebbüs.....	117
b. İçtima	118
c. İştirak	119
9. Yaptırım	119
10. Muhakemeye İlişkin Kurallar	121
B. Yağma (TCK m. 148-150)	121
1. Genel Olarak	121
2. Suçun Faili	122
3. Suçun Mağduru	122
4. Suçla Korunan Hukuki Yarar.....	123
5. Suçun Maddi Konusu.....	123
6. Suçun Unsurları.....	123
a. Maddi Unsur	123
b. Hukuka Aykırılık Unsuru	125
c. Kusurluluk.....	126
7. Suç ve Cezaya Etki Eden Nedenler.....	127
a. Suçu Ağırlaştıran Nedenler.....	127
aa. Yağma suçunun silahla işlenmesi.....	127
bb. Yağma suçunun kişinin kendisini tanınmayacak bir hale koyması suretiyle işlenmesi.....	128
cc. Yağma suçunun birden fazla kişi tarafından birlikte işlenmesi....	128
dd. Yağma suçunun yol kesmek suretiyle ya da konutta, işyerinde veya bunların eklentilerinde işlenmesi	129
ee. Yağma suçunun beden veya ruh bakımından kendisini savunamayacak durumda bulunan kişiye karşı işlenmesi.....	129
ff. Yağma suçunun var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak işlenmesi	130
gg. Yağma suçunun suç örgütüne yarar sağlamak maksadıyla işlenmesi	130
hh. Yağma suçunun gece vaktinde işlenmesi.....	131
b. Suçu Hafifleten Nedenler.....	131

aa. Kişinin bir hukuki ilişkiye dayanan alacağını tahsil amacıyla tehdit veya cebir kullanması.....	131
bb. Yağma suçunun konusunu oluşturan malın değerinin az olması .	132
c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep	132
d. Etkin Pişmanlık.....	133
8. Suçun Özel Görünüş Şekilleri.....	133
a. Teşebbüs.....	133
b. İçtima	134
c. İştirak	135
9. Yaptırım	135
10. Muhakemeye İlişkin Kurallar	136
C. Güveni Kötüye Kullanma (TCK m. 155).....	136
1. Genel Olarak	136
2. Suçun Faili	137
3. Suçun Mağduru	137
4. Suçla Korunan Hukuki Yarar.....	138
5. Suçun Maddi Konusu.....	138
6. Suçun Unsurları.....	139
a. Maddi Unsur	139
b. Hukuka Aykırılık Unsuru	140
c. Kusurluluk.....	141
7. Suç ve Cezaya Etki Eden Nedenler.....	142
a. Suçu Ağırлаştıran Nedenler.....	142
b. Suçu Hafifleten Nedenler.....	142
c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep	143
d. Etkin Pişmanlık.....	143
8. Suçun Özel Görünüş Şekilleri.....	144
a. Teşebbüs.....	144
b. İçtima	144
c. İştirak	145
9. Yaptırım	146
10. Muhakemeye İlişkin Kurallar	146
D. Dolandırıcılık (TCK m. 157-159)	147
1. Genel Olarak	147

2. Suçun Faili	147
3. Suçun Mağduru	147
4. Suçla Korunan Hukuki Yarar	148
5. Suçun Maddi Konusu	148
6. Suçun Unsurları	148
a. Maddi Unsur	148
b. Hukuka Aykırılık Unsuru	151
c. Kusurluluk	151
7. Suç ve Cezaya Etki Eden Nedenler	152
a. Suçu Ağırлаştıran Nedenler	152
aa. Dolandırıcılık suçunun dinî inanç ve duyguların istismar edilmesi suretiyle işlenmesi	153
bb. Dolandırıcılık suçunun kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan yararlanmak suretiyle işlenmesi	154
cc. Dolandırıcılık suçunun kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle işlenmesi	154
dd. Dolandırıcılık suçunun kamu kurum ve kuruluşlarının, kamu meslek kuruluşlarının, siyasi parti, vakıf veya dernek tüzel kişiliklerinin araç olarak kullanılması suretiyle işlenmesi	155
ee. Dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi	155
ff. Dolandırıcılık suçunun tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında işlenmesi	156
gg. Dolandırıcılık suçunun serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle işlenmesi	157
hh. Dolandırıcılık suçlarının, üç veya daha fazla kişi tarafından birlikte veya suç örgütü faaliyeti çerçevesinde işlenmesi	158
b. Suçu Hafifleten Nedenler	158
c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep	159
d. Etkin Pişmanlık	159
8. Suçun Özel Görünüş Şekilleri	160
a. Teşebbüs	160
b. İctima	160
c. İştirak	161
9. Yaptırım	161

10. Muhakemeye İlişkin Kurallar	162
II. Bilişim Alanında Suçlar	163
A. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244).....	164
1. Genel Olarak	164
2. Suçun Faili	165
3. Suçun Mağduru	165
4. Suçla Korunan Hukuki Yarar	165
5. Suçun Maddi Konusu	166
6. Suçun Unsurları.....	169
a. Maddi Unsur	169
b. Hukuka Aykırılık Unsuru	179
c. Kusurluluk.....	180
7. Suç ve Cezaya Etki Eden Nedenler.....	180
a. Suçu Ağırlaştıran Nedenler.....	181
b. Suçu Hafifleten Nedenler.....	182
8. Suçun Özel Görünüş Şekilleri.....	182
a. Teşebbüs.....	182
b. İhtima	183
c. İştirak	185
9. Yaptırım	185
10. Muhakemeye İlişkin Kurallar	186
III. Adliye Karşı Suçlar	187
A. Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu (TCK m. 282)	187
1. Genel Olarak	187
2. Suçun Faili	190
3. Suçun Mağduru	190
4. Suçla Korunan Hukuki Yarar	191
5. Suçun Maddi Konusu	192
6. Suçun Unsurları.....	193
a. Maddi Unsur	193
b. Hukuka Aykırılık Unsuru	194
c. Kusurluluk.....	195
7. Suç ve Cezaya Etki Eden Nedenler.....	196

a. Suçu Ağırılaştıran Nedenler.....	196
aa. Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun, kamu görevlisi tarafından veya belli bir meslek sahibi kişi tarafından bu mesleğin icrası sırasında işlenmesi	196
bb. Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun, suç işlemek için teşkil edilmiş bir örgütün faaliyeti çerçevesinde işlenmesi	197
b. Suçu Hafifleten Nedenler.....	198
c. Etkin Pişmanlık	198
8. Suçun Özel Görünüş Şekilleri	199
a. Teşebbüs.....	199
b. İhtima	200
c. İştirak	200
9. Yaptırım	200
10. Muhakemeye İlişkin Kurallar	201
§2. Kripto Para Birimlerinin Suç Konusu Olduğu Suçların Soruşturulması ve Kovuşturulmasının Zorlukları.....	203
SONUÇ	206
KAYNAKÇA.....	212
ÖZGEÇMİŞ	219

KISALTMALAR

a.g.e.	: adı geçen eser
a.g.m.	: adı geçen makale
a.g.y.	: adı geçen yazı
AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
ASIC	: Application-Specific Integrated Circuit
AY	: Anayasa
BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
BIP	: Bitcoin Improvement Proposal
bkz.	: bakınız
BTC	: bitcoin
CD	: Ceza Dairesi
CDD	: Customer Due Dilegence
CMK	: Ceza Muhakemesi Kanunu
CPU	: Central Processing Unit
DNS	: Domain Name Server
DSA	: Digital Signature Algorithm
DDoS	: Distributed Denial of Service
DoS	: denial-of-service
E.	: Esas No
EBA	: European Banking Authority
ECB	: European Central Bank
ECC	: Elliptic Curve Cryptography
ECDSA	: Elliptic Curve Digital Signature Algorithm
EİK	: Elektronik İmza Kanunu
FATF	: Financial Action Task Force
FAW	: Fork After Withholding
FinCEN	: US Financial Crimes Enforcement Network
FPoW	: Full Proof-of-Work
FSA	: Financial Services Agency
HD	: Hierarchical Deterministic
HMRC	: Her Majesty's Revenue and Customs
GB	: Gigabyte
GSM	: Global System for Mobile Communications
GUAM	: Gürcistan, Ukrayna, Azerbaycan ve Moldova
ICO	: Initial Coin Offerings
IMF	: International Monetary Fund
IP	: Internet Protocol
IT	: Information Technologies
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
İng.	: İngilizce
K.	: Karar No
KYC	: Know Your Customer
m.	: madde
md.	: madde
M.Ö.	: Milattan önce
MB	: Megabyte
OECD	: The Organisation for Economic Co-operation and Development
p2p	: Peer-to-Peer

PPoW	: Partial Proof-of-Work
QR	: Quick Response
RSA	: Rivest–Shamir–Adleman
s.	: sayfa
SGK	: Sosyal Güvenlik Kurumu
SPK	: Sermaye Piyasası Kurulu
SPK	: Sermaye Piyasası Kanunu
SPV	: Simplified Payment Verification
SSL	: Secure Sockets Layer
TBMM	: Türkiye Büyük Millet Meclisi
TLS	: Transport Layer Security
TCK	: Türk Ceza Kanunu
TCY	: Türk Ceza Yasası
TDK	: Türk Dil Kurumu
TMK	: Türk Medeni Kanunu
UNODC	: United Nations Office on Drugs and Crime
USB	: Universal Serial Bus
YCGK	: Yargıtay Ceza Genel Kurulu

RÉSUMÉ

Le sujet principal de cette thèse est de déterminer la situation juridique des cryptomonnaies qui sont considérées comme l'une des grandes innovations des technologies de l'information ces dernières années et de révéler leurs relations avec les structures et les réglementations existantes dans le système juridique, surtout en droit pénal. On constate que l'intérêt pour les cryptomonnaies augmente dans notre pays comme partout dans le monde entier. Bien que les cryptomonnaies existent depuis moins d'une dizaine d'années, elles sont utilisées dans la vie quotidienne et dans les activités commerciales comme moyen de paiement pour les achats réels et virtuels de biens et services, souvent acceptés par de nombreuses sociétés internationales. De plus, elles ont une convertibilité bidirectionnelle avec les monnaies nationales et leurs volumes de marché ont atteint jusqu'à 700 milliards de dollars américains. Tous ces résultats montrent qu'elles ont un grand potentiel et une grande importance. Les experts affirment que les systèmes des cryptomonnaies ne sont qu'un produit de la technologie « Blockchain », que cette technologie a un énorme potentiel, que, dans un avenir pas si lointain, des contrats intelligents et des propriétés intelligentes apparaîtront et de tels contacts seront signés entre les personnes physiques et les machines ou entre seulement les machines et que tous les services fournis par l'État seront reconstruits sur la base de cette nouvelle structure technologique. Il y a même des écrivains qui disent qu'un nouveau champ de droit appelé Lex Cryptographia va bientôt voir le jour.

Les technologies de l'information changent les relations individuelles et sociales et les institutions qui sont les expressions institutionnelles de celles-là ainsi que le droit. Le fait que les innovations technologiques trouvent leur place dans le système juridique nécessite parfois le changement, l'interprétation d'une manière large ou la réinterprétation des institutions et des réglementations existantes.

La position des cryptomonnaies dans le domaine du droit est aussi une incertitude. Il n'existe pas encore de pays dans le monde où les monnaies cryptographiques sont légalement définies et leurs relations avec les structures, institutions et réglementations existants sont révélées.

L'incertitude juridique concernant les cryptomonnaies est également valable pour notre pays. Il y a beaucoup à faire pour surmonter cette ambiguïté. Outre le traitement de la matière par des scientifiques spécialisés et l'organisation des réunions, il faut également la création de la jurisprudence sur les cryptomonnaies. Cette thèse vise également à contribuer à la compréhension des cryptomonnaies et à la clarification de leur situation juridique.

L'évaluation des cryptomonnaies en termes de droit pénal nécessite un travail interdisciplinaire, car il s'agit à la fois d'une question des technologies de l'information et de droit. Les technologies de l'information sont un domaine difficile à comprendre car elles s'agissent de différentes composantes techniques et de leurs relations complexes et elles se renouvellent constamment. Outre la nécessité de

comprendre que ces éléments techniques sont utilisés dans tous les domaines, le juriste doit avoir une compréhension conceptuelle des composants techniques et des concepts qui constituent leur infrastructure afin de déterminer la position des cryptomonnaies dans le système juridique. Dans le cadre de cette thèse, des explications techniques sur les cryptomonnaies ont été prises au besoin en raison de ces problèmes.

Il est certain que l'émergence des cryptomonnaies aura des conséquences juridiques, sociales, politiques, administratives, financières, économiques et même culturelles. Chaque domaine de sciences considérera différents aspects du sujet de son propre point de vue. Même dans la loi, l'intérêt et la perspective des différents domaines seront différents. Il y a également des aspects liés au droit administratif et au droit privé, en dehors du droit pénal. Cependant, la portée de cette étude se limite à un contexte général en droit pénal.

Dans l'étude, des livres, des articles scientifiques et d'autres documents écrits par des spécialistes de différents domaines ainsi que des rapports, notes d'information, symposiums et notes de conférence préparés par des organisations nationales et internationales sur les monnaies cryptographiques ont été systématiquement examinés. Les informations collectées à partir de ces sources ont été analysées, comparées et une compilation exhaustive des informations a été synthétisée pour parvenir à une conception globale visant à traiter les différents aspects du sujet.

La thèse est essentiellement composée de deux parties. Dans la première partie, des explications techniques et juridiques sont fournies pour la formation d'une compréhension conceptuelle des systèmes de cryptomonnaie et pour la compréhension de ce nouveau phénomène technologique dans son ensemble. Dans la deuxième partie, certains crimes qui sont décrites dans le code pénal turc et pour lesquelles la crypto-monnaie peut constituer la question de la criminalité sont analysées.

Le premier chapitre de la première partie est consacrée à la définition du concept de cryptomonnaie. Afin de comprendre la cryptomonnaie, les concepts de monnaie électronique, de monnaie numérique, de monnaie virtuelle et de monnaie traditionnelle sont discutés. Les similitudes, les différences et les relations entre eux et les cryptomonnaies sont étudiés. Il est possible que ces similitudes et différences, dont certaines proviennent de structures techniques et d'autres de réglementations juridiques, puissent augmenter ou diminuer à l'avenir. Pour cette raison, il n'est pas facile d'établir une définition générale des cryptomonnaies dont le processus de développement est toujours en cours. À notre avis, la cryptomonnaie peut être définie comme la monnaie numérique qui n'est sous le contrôle et la supervision d'aucune structure centrale, que la technologie de l'information, principalement les techniques cryptographiques, est utilisée pour son émission et sa circulation et qui est alternative des monnaies nationales.

Puis, les personnes, les groupes, les mouvements et les développements technologiques impliqués dans l'émergence de la cryptomonnaie sont donnés pour

l'acquisition d'une perspective historique sur le sujet. En effet, avant l'émergence de Bitcoin, la première cryptomonnaie, en 2009, les travaux sur ce sujet peuvent être remontés aux années 1980. Les techniques cryptographiques impliquées dans le fonctionnement de ces systèmes se basent sur une croyance à la confidentialité de la vie privée et à l'immunité de la liberté de communication et une conviction que cela peut être réalisé par la cryptographie.

A la fin de ce chapitre, les caractéristiques communes des cryptomonnaies sont expliquées. Avec un nombre de presque deux mille, il est difficile de trouver des caractéristiques communes qualifiant toutes les cryptomonnaies. Mais le code source ouvert, l'anonymat, la décentralisation et la cryptographie sont généralement valables pour tous. Ces caractéristiques sont expliquées clairement autant qu'un juriste doit savoir.

Le deuxième chapitre de la partie est consacré à la recherche d'une réglementation juridique des monnaies cryptographiques. Après l'identification de l'incertitude juridique, les raisons de recherches juridiques sont soulignées. Le fait que ces systèmes sont utilisés pour le financement du terrorisme, le blanchiment des monnaies, la pornographie juvénile et les crimes transfrontaliers tels que le trafic de drogue auxquels la communauté internationale est sensible ou pour faciliter l'opération de ces crimes est la cause principale de cette recherche.

Une autre raison similaire est ce que les systèmes de cryptomonnaie se transforment en paradis fiscaux pour les délits d'évasion fiscale. En outre, les systèmes monétaires cryptographiques émettent leurs propres monnaies conformément aux règles définies par leurs développeurs et en fonction de l'équilibre entre l'offre et la demande du marché. L'intérêt croissant aux cryptomonnaies pose des risques pour les politiques monétaires nationales des gouvernements. Cette situation est présentée comme une autre raison des recherches juridiques concernant le sujet.

Puis, il est montré qu'il n'est pas facile de créer des réglementations juridiques sur les cryptomonnaies et que cela entraîne des difficultés. L'une des raisons de ces difficultés est le fait que ces systèmes ont des mécanismes d'exploitation globaux. En effet, il est possible d'utiliser ces systèmes partout où l'accès à Internet est disponible. Pour cette raison, les réglementations à prendre dans la législation nationale du pays seront insuffisantes à moins d'être appuyées par d'autres pays et par des réglementations internationales. En outre, il n'est pas facile de mettre en place des règles garantissant un bon développement au lieu de règles strictes qui empêcheraient le développement du domaine de l'innovation technologique promis par les structures de blockchain et similaires utilisées par ces systèmes. Pour cette raison, les pays suivent les travaux et les études à l'échelle mondiale à cet égard et appliquent la politique «attendre et voir».

Les raisons et les difficultés des recherches juridiques concernant les cryptomonnaies et, à la suite des recommandations d'experts et des rapports produits par des organisations internationales, les conclusions des études internationales pertinentes sur cette question sont examinées. Les rapports et les notes d'information

préparés par la Groupe d'action financière (GAFI), l'Office des Nations Unies contre la drogue et le crime (ONUDC), de l'Organisation de coopération et de développement économiques (OCDE), le Fonds monétaire international (FMI), la Banque centrale européenne (BCE) et L'Autorité bancaire européenne (ABE) qui opèrent leurs activités devant L'Union Européen sont évalués de manière détaillée. Les principes de base, les risques, les menaces, les avertissements, les recommandations et les prévisions qui se présentent dans ces études fournissent un cadre pour les réglementations juridiques nationaux, régionaux et internationaux concernant les cryptomonnaies.

Ensuite, le statut juridique des cryptomonnaies dans la législation nationale de différents pays sont examinés. On peut dire que les pays réagissent aux cryptomonnaies de quatre manières différentes : l'avertissement, l'explication sur le statut juridique, la licence future, l'imposition de surveillance et l'interdiction. De plus, l'analyse faite en ce qui concerne le statut juridique de la cryptomonnaie aux Etats-Unis, en Allemagne, en Chine, au Japon, en Russie et en Turquie nous montre que dans aucun pays la situation juridique de ces monnaies n'est pas suffisamment claire, même dans certains pays les cryptomonnaies sont caractérisées de différentes manières par différentes organisations par rapport à leurs objectifs de l'entreprise.

Dans le quatrième chapitre de cette partie, la cryptomonnaie est traitée en droit pénal. Malheureusement, le nombre d'examens traitant du statut juridique de la cryptomonnaie dans notre doctrine est très faible. Dans ce chapitre, on discute d'abord de la question de savoir si les cryptomonnaies peuvent être considérées comme des monnaies, des marchandises ou des valeurs mobilières aux fins du droit pénal. Le résultat de cette analyse est ce qu'il n'est pas possible de considérer les cryptomonnaies comme des "porteurs de valeur économique" dans le cadre de la législation existante. Cependant, à la lumière des conclusions des rapports préparés par les organisations internationales telles que le GAFI et le CMB, on peut dire que les cryptomonnaies devraient être considérées comme une monnaie alternative à la monnaie réel aux fins du droit pénal.

Puis, la légalité de l'utilisation des cryptomonnaies est examinée. Il n'y a aucun obstacle juridique à l'utilisation de ces cryptomonnaies. Il est libre de commettre un acte qui n'est pas explicitement interdit par la loi en vertu de la Constitution ou du code pénal turc (TCK) et du principe de justice pénale. En conséquence, il a été conclu que l'utilisation des cryptomonnaies comme un moyen de paiement lors de l'achat et de la vente de biens et services réels et virtuels ainsi que l'échange des cryptomonnaies entre personnes en bourse ou aux centres d'échange est légale.

La cinquième et dernier chapitre de la première partie est consacrée à l'explication de Bitcoin, qui est la première cryptomonnaie et qui détient la plus grande part en termes de valeur marchande au marché. Le système Bitcoin, qui a été mis en service en 2009, détient environ 40% du marché des cryptomonnaies. D'autres systèmes des cryptomonnaies fonctionnent soit en utilisant directement les structures techniques du système Bitcoin, soit en utilisant leurs propres systèmes développés en modélisant la structure technique de ce système. Pour cette raison, l'introduction du

système Bitcoin fournira un modèle conceptuel qui facilitera la compréhension des autres cryptomonnaies.

Ce chapitre qui commence avec l'analyse de l'article de Satoshi Nakamoto expliquant la structure technique et le fonctionnement de Bitcoin, donne des explications sur les composants techniques et les opérations du système telle que l'écosystème, le mouvement, le blocage, la preuve de travail et le blockchain et l'exploration de données, le réseau et la sécurité de Bitcoin, les autres cryptomonnaies et l'utilisation de blockchain pour les raisons non-monétaires. Avec l'émergence de propriétés intelligentes et de contrats intelligents, considérés comme des applications Blockchain 2.0, on prétend qu'il y aura un nouveau tournant où des relations contractuelles entre une personne physique et une machine ou entres machines pourront être établies ou des contrats auto-réalisables pourront être créés. Les futures générations de Blockchain changeraient fondamentalement tous les services publics exécutés par l'État.

La seconde partie de la thèse est consacrée à l'évaluation des cryptomonnaies en ce qui concerne certains crimes décrites dans le Code Pénal Turc (TCK) qui peuvent concerner les cryptomonnaies. Nous traitons les actes criminels qui peuvent être considérés comme des vols (TCK a. 142) ou des délits de profits illicites en faisant du tort aux systèmes d'information ou à leurs données (TCK a. 144/4) en ce qui concerne les cryptomonnaies. la Cour de Cassation Turque a décidé que les actes illicites étaient commis contre l'argent sur le compte et non pas les données elles-mêmes. Donc, ces méfaits doivent être considérés comme des crimes de vol.

À la fin de la partie, les difficultés d'enquêter les crimes liés aux cryptomonnaies sont abordées. Ces difficultés proviennent des systèmes de cryptomonnaie ainsi que des caractéristiques uniques des preuves numériques.

ABSTRACT

This thesis's main subject is about legal statuses of cryptocurrencies, which has been emerging as one of the greatest recent innovations of information technologies. Its aim is to specify and reveal their positions and relations with the existing structures and regulations within criminal law. There is a growing interest about cryptocurrencies in Turkey as observed all around world. Although it is not more than a decade from their first existing, people started to use them as payment instruments for purchasing real and virtual goods and services in daily life and in commercial contexts; international big companies started to accept them, and there are hundreds of exchange centers special for trading them. While they have bi-directional convertibility with national currencies, their marketplace volume has reached up to 700 billion US Dollars. All of these findings show that they have a great potential and importance.

Domain specialists in this area assert that cryptocurrency is only one product of Blockchain technology, and soon we will become acquainted with its new applications like smart contract and smart property. Through agencies of these products, it will be possible to construct contracts where parties are real person and machine or both of them machines. According to them, all public services running by states will be reconstructed on this new technological innovation. In addition, some authors put forward that there will emerge a new legal area, *Lex Cryptographia*, which will change our core legal concepts.

Information technologies (IT), constantly change personal and social relations and their institutional structures, and law is not out of this scope. Sometimes it is necessary to change, stretch, or re-interpret existing institutions and regulations in order to find a proper place for these technological innovations.

Our main subject, cryptocurrency, comprises a legal uncertainty. Actually, there is no any country in the world where cryptocurrency has a precise legal certainty and defined relationships with other existing institutions and regulations. The same situation is valid for our country too. In order to resolve this legal uncertainty, there is a lot to do. There should be meetings, and domain specialists in the doctrine have to engage into the subject. While these efforts are performed, the court decisions about cryptocurrency would come up. We hope that this study should be seen as a contribution for understanding cryptocurrency and determining their legal statuses.

In order to evaluate cryptocurrencies in context of criminal law, it is a necessity to perform a multi-disciplinary study between information science and jurisprudence. IT is a relatively difficult discipline because it consists of different type of concepts, technics, components, and relations between them. It is a continually self-renewal area as well. It is obvious that every related person should have a basic understanding of IT because of its increasingly intense use in every aspect of daily life. So that, a jurist should have a good understanding of IT concepts and technological components underlying cryptocurrencies, for determining a proper place for them

and specifying their relations with the existing institutions and regulations in legal area. In the study, these considerations have been taken into account and the required technical explanations related to them are included in it.

Obviously, the emergence of cryptocurrencies has impacts on social, political, administrative, financial, economical, even cultural areas as well as on legal domain. This subject will be evaluated differently according to each discipline's purpose and perspective. Even within legal domain, the interest and perspective of different branches may differ from each other. There are also some aspects related to administrative law and private law, beside criminal law. The scope of this study is limited to a general context within criminal law.

In this study, the reports and the working notes prepared and released by certain international organizations, and notes from symposiums and conferences are reviewed. The books, articles and other writings about cryptocurrencies, which are written by different subject area specialists, are also examined systematically. The knowledge from these sources are compiled, analyzed, and compared to each other, and then synthesized to produce a whole thought with different aspects explained.

This thesis mainly has two parts. In the first part, there are technical and legal explanations about cryptocurrencies for acquiring a conceptual insight and a whole understanding of this new technological phenomenon. In the second part, there is a general evaluation of cryptocurrencies within context of criminal law. In addition, depending on this evaluation, some crimes regulated in Turkish Penal Code (TCK), which cryptocurrencies may constitute crime subject, are analyzed.

The first section of the first part is devoted to find a definition for the concept of cryptocurrency. In order to fully understand the concept of cryptocurrency, the concepts of traditional money, electronic money, digital money and virtual currency are considered and their properties, similarities and dissimilarities are investigated. While some of the similarities or dissimilarities are originated from technical structures, others come from their legal regulations, which are subject to increase or decrease in the future. Therefore, it seems that it is not so easy to come up with a generally valid definition for cryptocurrencies due to their continuing development progress. In our opinion, we can define cryptocurrency as a digital currency, in which cryptographic techniques are used to regulate the generation of its units and verify the transfer of funds, and which operates without administration and control of a central establishment.

At the continuation of the section, the people, the groups, the movements, and the technological advances underlying cryptocurrencies are mentioned in a chronological order for acquiring a historical perspective. Indeed, before the emergence of the first cryptocurrency Bitcoin in 2009, the studies in this field could be traced back to 1980s. The cryptographic technics involving in these systems are based on the belief of privacy of private life and the inviolability of freedom of communication. And cryptography would provide this privacy and freedom.

At the end of the section, the common properties of cryptocurrencies are explained. With a number of approximating to two thousand, it is difficult to find out common properties qualifying all cryptocurrencies. But open source code, anonymity, decentralization, and cryptography are generally valid for all. These properties are explained plainly, as much a jurist needs to know.

The second section of this part is dedicated to the quests for legal regulation for cryptocurrencies. After identifying legal uncertainty of them, the reasons behind these are elaborated. The main reason behind the legal quests is a growing concern at international level, that these systems are being used directly or as facilitating means, in transboundary criminal activities such as finance of terrorism, money laundering, child pornography, and drug traffic, which international community is sensitive to. A similar motive is expressed that these systems become tax havens for tax evasion. Beside these reasons, in a cryptocurrency system, issuing money is a process bonded to the rules specified by their developers freely, and its market supply and demand. With increasing interest to these currencies, it becomes risky situation for the national monetary politics of governments to fail.

At the continuation of the section, it is showed that regulating cryptocurrencies is not easy and has some difficulties. Firstly, these systems have global working mechanism. If there is internet access, it is easy to use these systems. Therefore, for a country, without support from international community and other countries, individually regulating cryptocurrencies within the national regulation is insufficient. The second concern is about taking right way: Instead of bringing bad regulations that may harm the promising blockchain technology; we should find rules that promote their healthy developments. Therefore the states follow international efforts to converge an end, so they take a wait and see approach.

After explaining the reason behind legal quests, their difficulties and the suggestion from domain specialists as well as international organizations, the results from international studies are examined. In this context, the reports prepared by The Financial Action Task Force (FATF), United Nations Office on Drugs and Crime (UNODC), The Organisation for Economic Co-operation and Development (OECD), International Monetary Fund (IMF), European Banking Authority (EBA), European Central Bank (ECB) are analyzed. The principles, risks, threats, warnings, suggestions and insight from specified in these studies can be used as a framework for bringing regulations at both national and international levels.

At the continuation of the section, the status and the legality of cryptocurrency in different countries are investigated. There are four categories about countries' responses: warnings, statements and clarifications on the legal status, (future) actions in licensing and/or supervision, and issuing bans warning. Additionally, the analysis of the statuses of these currencies in US, Germany, China, Japon, Russia and Turkey shows that there is no one country that fully specified the statuses of these currencies; even different organizations in a country, take different approaches to them.

The fourth section is devoted to understand cryptocurrency in context of criminal law. Unfortunately, in our doctrine there is no enough studies dealing with its legal status. Firstly, the possibility of considering these currencies as money, commodity, or securities is explored. The result of this analysis is that it is not possible to consider these currencies as economic value carriers, i.e., money, commodity or securities. But, as cited in the study, FATF and SPK accepts these entities as alternative currencies or alternatives to real money. So that, we may consider these economic value carriers as alternative currencies for the purpose of criminal law.

At the continuing of the section, the legality of the usages of cryptocurrencies is explored. There is no legal obstacle for using them. According to principle of legality, which is guaranteed in the Constitution and Turkish Criminal Code, it is free to commit any act that is not prohibited exclusively. So, it is not forbidden to use cryptocurrencies as payment tools in purchasing real or virtual goods and services, to exchange them between people, or to trade in the exchange centers.

The last section of the first part is dedicated to an explanation of the first and the most valuable cryptocurrency, Bitcoin. It has a 40% of cryptocurrency market share alone. The other cryptocurrencies directly use its infrastructure or build their systems according to its technical structure. Therefore, presenting Bitcoin system as a conceptual model will help us to understand other cryptocurrencies.

The section begins with Satoshi Nakamoto's famous article, "*Bitcoin: A Peer-to-Peer Electronic Cash System*", which explains the technical structure and mechanism of Bitcoin. Then it proceeds with the other concepts around the system, such as the blockchain, block, transaction, proof of work, mining, the Bitcoin network and its security, and its ecosystem as well.

The second part of the thesis is devoted to evaluate some crimes regulated in TCK, which may concern cryptocurrencies. The fundamental issue is about the criminal acts where they may fall under crime of theft (TCK m. 142) or under crime of unlawful profit by doing harmful things to information systems or their data (TCK m. 144/4). The Turkish Supreme Court decided that unlawful acts in such wrongdoings are against the money in the account, not to data itself. So these wrongdoings must be considered as crimes of theft.

The left of the second part is dedicated to the difficulties in investigation of the crimes concerning cryptocurrencies. According to findings, some difficulties originates from these systems themselves and others come from the properties of digital evidence as well.

ÖZET

Bu tezin konusu, bilişim teknolojisinin son yıllardaki en büyük yeniliklerinden biri olarak kabul edilen kripto para birimlerinin, hukuk düzeninde, özellikle ceza hukuku bağlamında hukuksal konumunun belirlenmesi ve mevcut yapı ve düzenlemelerle olan ilişkilerinin ortaya çıkarılmasıdır. Bütün dünyada olduğu gibi ülkemizde de kripto para birimlerine ilginin arttığını görülmektedir. Kripto para birimlerinin ilk ortaya çıkışlarından bu yana on yıllık bir süre geçmemesine rağmen, günlük hayatta ve ticari faaliyetlerde, gerçek ve sanal mal ve hizmet alımlarında ödeme aracı olarak kullanıldıkları, birçok uluslararası şirket tarafından kabul edildikleri, yüzlerce takas ve borsa merkezlerinde işlem gördükleri, tedavüldeki birçok ülke parasıyla çift yönlü konvertibiliteye sahip oldukları ve toplamda 700 milyar ABD dolarına kadar büyüyen pazar büyüklüğüne eriştikleri göz önüne alındığında işin mahiyeti ve önemi kendini hissettirmektedir. Konunun uzmanları, kripto para birimi sistemlerinin Blokzinciri (Blockchain) teknolojisinin sadece bir ürünü olduğunu ve bu teknolojinin çok büyük bir potansiyele sahip olduğunu iddia etmekte ve çok uzak olmayan bir gelecekte akıllı sözleşmeler ve akıllı mülklerin hayatımıza gireceğini, gerçek kişiler ile makineler veya her iki tarafın makine olduğu sözleşme ilişkilerinin kurulacağını ve Devletin yürüttüğü bütün hizmetlerin bu yeni teknolojik yapı temelinde yeniden kurgulanacağını ileri sürmektedirler. İddialar bunlarla sınırlı kalmamakta, *Lex Cryptographia* adında yeni bir hukuk alanının çok yakın bir zamanda doğumuna tanıklık edeceğimizi ifade eden yazarlar dahi bulunmaktadır.

Bilişim teknolojisi, bireysel ve toplumsal ilişkileri ve bunların kurumsal ifadesi olan yapıları sürekli değiştirmekte ve hukuk da bundan payına düşeni almaktadır. Teknolojik yeniliklerin, var olan hukuksal düzenlemeler arasından kendine bir yer bulması, bazen mevcut kurum ve düzenlemelerin az çok değiştirilmesini, esnetilmesini veya yeniden yorumlanmasını gerektirmektedir.

İnceleme konumuz olan kripto para birimlerinin hukuk alanındaki konumu da böyle bir belirsizlik arz ediyor. Bütün dünyada, kripto para birimlerinin hukuken tam olarak tanımlandığı, mevcut yapı, kurum ve düzenlemelerle ilişkilerinin ortaya konulduğu bir ülke henüz mevcut değil.

Kripto para birimlerine ilişkin hukuki belirsizlik, ülkemiz açısından da geçerli bir durumdur. Bu belirsizliğin giderilmesi için, yapılması gereken çok şey var. Doktrinde konunun uzmanı bilim adamları tarafından ele alınması, toplantılar düzenlemesinin yanında mahkeme içtihatlarının da ortaya çıkması gerekmektedir. Bu tez çalışması da, kripto para birimlerinin anlaşılmasına ve hukuki durumlarının belirginleşmesine katkıda bulunmak amacıyla hazırlanmıştır.

Kripto para birimlerinin ceza hukuku bakımından değerlendirilmesi, hem bilişim alanını hem de hukuku ilgilendiren bir konu olduğu için disiplinler arası bir çalışmayı gerektirmektedir. Bilişim teknolojileri, farklı teknik bileşenler ile bunların karmaşık ilişkilerinden oluştuğundan ve sürekli kendini yenilediğinden, anlaşılması görece zor bir alandır. Bu teknik unsurların gittikçe hayatın her alanında yoğun

kullanımının doğurduğu anlaşılma gerekliliği bir yana, bir hukukçunun kripto para birimi sistemlerinin hukuk düzenindeki konumunu belirlemesi, mevcut kurum ve yapılarla ilişkilerini ortaya koyabilmesi için bunların altyapısını oluşturan teknik bileşenlere ve kavramlara ilişkin kavramsal bir kavrayışa sahip olması şarttır. Çalışmamızda bu hususlar gözetilerek, kripto para birimlerine ilişkin teknik açıklamalar da gerektiği ölçüde yer almıştır.

Kripto para birimlerinin ortaya çıkışının hukuksal etkileri olduğu gibi sosyal, siyasal, idari, mali, ekonomik, hatta kültürel sonuçlarının da olacağı kuşkusuzdur. Her bilim dalı kendi bakışına göre konunun farklı yönlerini ele alacaklardır. Hukuk içinde dahi, farklı alanların konuya ilgisi ve bakışı farklı olacaktır. Konunun ceza hukuku yanından idare ve özel hukuk alanlarını da ilgilendiren yönleri vardır. Fakat bu çalışmanın kapsamı ceza hukukunun genel çerçevesi ile sınırlı tutulmuştur.

Çalışmada, kripto para birimleriyle ilgili ulusal ve uluslararası kuruluşlar tarafından hazırlanan raporlar, bilgi notları, sempozyum ve konferans notlarının yanında, farklı alanlardan konunun uzmanı kişiler tarafından kaleme alınan kitaplar, bilimsel makaleler ve diğer yazılar sistematik olarak incelenmiştir. Bu kaynaklardan derlenen bilgiler analiz edilmiş, karşılaştırılmış ve ortaya çıkan kapsamlı sayılabilecek bilgi dağarcığı sentezlenerek konuyu farklı yönleriyle ele almaya çalışan bütün bir düşünceye ulaşmaya çalışılmıştır.

Tez, temelde iki bölümden oluşmaktadır. İlk bölümde, kripto para birimi sistemlerine ilişkin kavramsal bir kavrayışın oluşması ve bu yeni teknolojik olgunun bir bütün olarak anlaşılabilmesi için teknik ve hukuksal açıklamalarda bulunulmuştur. İkinci bölümde kripto para birimlerinin Türk Ceza Kanunu'nda düzenlenen ve kripto para biriminin suç konusunu oluşturabileceği bazı suçların analizi yapılmıştır.

Birinci bölümün ilk ayrımı, kripto para birimi kavramı için bir tanım getirmeye tahsis edilmiştir. Kripto para biriminin anlaşılması için geleneksel para ile birlikte elektronik para, dijital para ve sanal para birimi kavramları ele alınmış, bunlar ile kripto para birimi kavramı arasındaki benzerlikler, farklılıklar ve ilişkiler ortaya konulmaya çalışılmıştır. Bazıları teknik yapılardan bazıları da yasal düzenlemelerden kaynaklanan bu benzerlik ve farklılıkların ileride çoğalıp azalmaları veya değişimleri mümkündür. Bu nedenle gelişim süreci hâlâ devam eden bir olguya işaret eden kripto para birimleri için genel geçerli bir tanım ortaya koymak çok da kolay gözükmemektedir. Kanaatimize göre, kripto para birimi, paranın ihracında ve dolaşımında başta kriptografik teknikler olmak üzere bilişim teknolojilerinin kullanıldığı, herhangi bir merkezî yapının yönetiminde ve denetiminde olmayan, ulusal paralara alternatif dijital para birimi olarak tanımlanabilir.

Bu ayrımın devamında, konuyla ilgili tarihi bakışın oluşması için kripto para biriminin ortaya çıkışında rol almış kişiler, gruplar, hareketler ve teknolojik gelişmeler kronolojik bir sırada verilmiştir. Gerçekten de ilk kripto para birimi olan Bitcoin'in 2009 yılında ortaya çıkışından önce, bu konudaki çalışmalar 1980'lere kadar geriye götürülebilir. Bu sistemlerin işleyişinde yer alan kriptografik tekniklerin temelinde özel hayatın mahremiyetine ve haberleşme özgürlüğünün

dokunulmazlığına olan inanç ve bunun kriptografi ile sağlanabileceği düşüncesi yatmaktadır.

Ayrım sonunda, kripto para birimlerinin ortak özellikleri açıklanmıştır. Günümüzde iki bine yaklaşan sayılarıyla bu para birimlerinin bütünü bir den niteleyen ortak özellikleri ortaya dökmek kolay olmasa da, ayırmda açıklanan açık kaynak kodlu olmak, anonimlik, merkezi bir yapıya sahip olmamak ve kriptografik teknikler kullanmak, genel olarak hepsi için geçerlilik arz etmektedir. Bu özellikler, konuyla ilgili bir hukukçunun gereksinimin duyacağı ölçüde, mümkün olduğunca anlaşılabilir bir sadelikte sunulmaya çalışılmıştır.

Bölümün ikinci ayrımı, kripto para birimlerine ilişkin hukuki düzenleme arayışlarına ayrılmıştır. Hukuksal belirsizliğin tespitinden sonra hukuki arayışların sebepleri üzerinde durulmuştur. Bu sistemlerin, uluslararası camianın hassas olduğu terörizmin finansmanı, suçtan kaynaklanan malvarlığı değerlerinin aklanması, çocuk pornografisi ve uyuşturucu ve uyarıcı madde ticareti gibi sınıraşan suçlarda kullanılması veya işleyişlerini kolaylaştırması, bu arayışların temel sebebi olarak gözükmemektedir. Yine benzer bir sebep, kripto para birimi sistemlerinin vergi kaçırma suçları için vergi cenneti olmaya doğru evrildiği iddialarıdır. Bunun yanında, kripto para birimi sistemleri, kendi geliştiricilerinin belirlediği kurallar çerçevesinde ve piyasanın arz ve talep dengesine göre kendi para birimi arzında bulunmaktadır. Bunlara karşı ilginin her geçen gün artması hükümetlerin ulusal para politikalarını sekteye uğratma riskleri taşımaktadır. Bu durum, konuyla ilgili hukuksal arayışların bir başka sebebi olarak gösterilmektedir.

Ayrımın devamında, kripto para birimlerine ilişkin hukuki düzenlemeler ihdas etmenin kolay olmadığı ve bazı zorluklar içerdiği gösterilmiştir. Bu zorlukların bir sebebi, bu sistemlerin küresel işleyiş mekanizmalarına sahip olmalarından kaynaklanmaktadır. Gerçekten de internet erişiminin olduğu her yerde bu sistemlerin kullanılmaları mümkündür. Bu nedenle ülkelerce ulusal mevzuatlarında yapılacak düzenlemeler, diğer ülkeler ve uluslararası düzenlemeler tarafından desteklenmedikçe yetersiz kalacaktır. Ayrıca bu sistemlerin kullandığı blokzincirini ve benzeri yapıların vadettiği teknolojik yenilik alanının gelişimini engelleyecek katı kurallar yerine, sağlıklı bir yol izlenebilmesini sağlayacak kurallar ortaya koymak pek de kolay gözükmemektedir. Bu nedenle, ülkeler bu konuda uluslararası camiada yapılan çalışmaları takip etmekte ve “bekle ve gör” politikası uygulamaktadır.

Kripto para birimlerine ilişkin hukuksal arayışların sebepleri, zorlukları ve bu konuda gerek uzmanların gerekse uluslararası kuruluşların hazırladığı raporlarda belirtilen tavsiyelerden sonra, konuyla ilgili uluslararası çalışmaların sonuçları ele alınmıştır. Bu çerçevede, Mali Eylem Gücü (FATF), Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC), Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), Uluslararası Para Fonu (IMF) ile Avrupa Birliği (AB) nezdinde faaliyet gösteren Avrupa Bankacılık Otoritesi (EBA) ve Avrupa Merkez Bankası (ECB) tarafından hazırlanan raporlar ve bilgi notlarının ayrıntılı değerlendirmesi yapılmıştır. Bu çalışmalarda ortaya çıkan temel ilkeler, riskler, tehlikeler, uyarılar, tavsiyeler ve öngörüler, kripto para birimlerine ilişkin ulusal, bölgesel ve uluslararası hukuksal düzenlenmelere ilişkin bir çerçeve sunmaktadır.

İncelemenin devamında, kripto para birimlerinin değişik ülkelerin ulusal mevzuatlarındaki hukuki konumları ile yasal durumları ele alınmıştır. Ülkelerin, kripto para birimleriyle ilgili olarak, uyarma, hukuksal durumu açıklayıcı beyanlar yapma, gelecekte lisanslama, denetleme zorunluluğu getirme ve yasaklama şeklinde dört farklı tepki verdikleri gözlemlenmektedir. Bunun dışında, ABD, Almanya, Çin, Japonya, Rusya ve Türkiye’de kripto para biriminin hukuki statüsüne ilişkin yapılan analizde, hiçbir ülkede bu para birimlerinin hukuksal konumunun yeteri kadar belirgin olmadığı, hatta bazı ülkelerde, kripto para birimlerinin farklı kuruluşlar tarafından kendi kurumsal amaçları bakımından farklı şekillerde nitelendirildikleri gözlemlenmiştir.

Bölümün dördüncü ayrımında ceza hukuku ekseninde kripto para birimi ele alınmıştır. Doktrinimizde kripto paranın hukuksal durumunu ele alan inceleme sayısı maalesef çok azdır. Bu ayrımında, önce kripto para birimlerinin ceza hukukunun amaçları doğrultusunda para, emtia veya menkul değer olarak kabulünün mümkün olup olmadığı tartışılmıştır. Bu analizden çıkan sonuç, mevcut mevzuat çerçevesinde kripto para birimlerinin bu türden “ekonomik değer taşıyıcıları” olarak kabulünün mümkün olmadığıdır. Fakat incelemede değinilen FATF gibi uluslararası kuruluşlar ile SPK’nin hazırladıkları raporlardaki tespitler ışığında, ceza hukuku amaçları doğrultusunda kripto para birimlerinin gerçek paraya alternatif para birimi olarak kabulünün doğru olacağı düşünülmüştür.

Ayrımın devamında, kripto para birimleri kullanmanın yasallığı incelenmiştir. Bu para birimlerini kullanmanın önünde yasal bir engel gözükmemektedir. Anayasada ve Türk Ceza Kanunu’nda (TCK) güvence altına alınmış olan suçta ve cezada kanunilik ilkesi gereğince kanunların açıkça yasaklamadığı bir fiili işlemek serbesttir. Bundan yola çıkılarak, kripto para birimlerinin gerçek ve sanal mal ve hizmet alım ve satımlarında ödeme aracı olarak kullanılmasının, kişiler arasında değiş tokuşa konu olmasının veya borsa ve takas merkezlerinde işlem görmesinin yasal olduğu sonucuna varılmıştır.

Birinci bölümün beşinci ve son ayrımı, ilk kripto para birimi olan ve piyasa değeri bakımından da en büyük paya sahip olan Bitcoin’in açıklanmasına ayrılmıştır. 2009 yılında faaliyete geçen Bitcoin sistemi, kripto para birimleri pazarının yaklaşık %40’ına tek başına sahiptir. Diğer kripto para birimi sistemleri, ya doğrudan Bitcoin sisteminin teknik yapılarını kullanmakta yada bu sistemin teknik yapısını model alarak, geliştirdikleri kendi sistemleriyle faaliyette bulunmaktadır. Bu nedenle Bitcoin sisteminin ortaya konulması, diğer kripto para birimlerinin de anlaşılmasını kolaylaştıracak kavramsal bir model sağlayacaktır.

Satoshi Nakamoto’nun Bitcoin’in teknik yapısını ve işleyişini açıkladığı makalesinin analiziyle başlayan bu ayrımında, sırasıyla Bitcoin etrafında oluşan ekosistem, hareket, blok, iş kanıtı, blokzinciri gibi sistemin teknik bileşenleri ve işleyişleri, madencilik, Bitcoin ağı ve güvenliği, diğer kripto para birimleri ve para birimi dışında blokzinciri uygulamalarına ilişkin açıklamalara yer verilmiştir. Blockchain 2.0 uygulamaları olarak görülen akıllı mülkler ve akıllı sözleşmelerin ortaya çıkışlarıyla, artık gerçek kişi-makine veya makine-makine arasında sözleşme

ilişkilerinin kurulabileceği veya kendi kendini ifa eden sözleşmelerin oluşturulabileceği yeni bir döneme girileceği iddia edilmektedir. Blokzincirinin gelecek nesil uygulamaları, Devletin yürüttüğü bütün kamu hizmetlerinin gerçekleşme biçimlerini kökten değiştirecek nitelikte gözükmektedir.

Tezin ikinci bölümü kripto para birimlerinin TCK’de düzenlenen bazı suçlar bakımından değerlendirmesine ayrılmıştır. Tartışma özellikle, kripto para birimlerinin suç konusu olabileceği fiillerin, TCK m. 142 vd. düzenlenen hırsızlık suçu kapsamında veya TCK m. 144/4’te düzenlenen bilişim sistemlerini engelleme ve bozma ile verileri yok etme ve değiştirme eylemleriyle haksız çıkar sağlama suçu kapsamında değerlendirilmesi gerektiği noktasında düğümlenmektedir. Yargıtay’ın bu uyuşmazlıklarda, verinin temsil edici özelliğini dikkate alarak, bilişim verisinin, hesaptaki parayı temsil ettiği görüşünden hareketle, bu para birimlerinin suç konusu olduğu fiillerin hırsızlık suçu kapsamında değerlendirilmeleri gerektiği sonucuna ulaşılmıştır.

Bölümün sonunda, kripto para birimlerine ilişkin suçların araştırılmasının zorluklarına değinilmiştir. Bu zorluklar, kripto para birimi sistemlerinden kaynaklandığı gibi, dijital delillerin kendilerine özgü niteliklerinden de kaynaklandığı belirtilmiştir.

GİRİŞ

Bilişim teknolojilerinin gelişimiyle beraber ortaya çıkan yeniliklerin amacı, yöneldiği alana hız, kolaylık, üretkenlik ve verimlilik gibi herkesin beğenisini kazanacak olumlu katkılar sağlamaktır. Bu inovasyonların, başta hukuk olmak üzere, diğer alanlara yansımaları, mevcut yapı ve düzenlemelerin bunları kabul edebilme esnekliğine bağlı olarak kolay veya zor olabilmektedir. Dünyada bütün ülkelerin ilgili hukuk düzenlerini az çok bir değişime zorlayacağı düşünülen ve son yılların teknolojik bir yeniliği olarak karşımıza çıkan kripto para birimleri, bu tezin konusunu oluşturmaktadır.

Sayıları hızla artan kripto para birimleri –bugün itibariyle ulaştığı sayı 1664* - , internet üzerinden milyonlarca kişi tarafından çevrimiçi oynanan oyunlara benzemektedir. Bu sistemlerinin, işleyiş mekanizmaları ve tabi oldukları kurallar, tıpkı birer oyunmuş gibi, geliştiricileri tarafından benimsenen amaçlara göre yine kendileri tarafından belirlenmektedir. Buna rağmen kripto para birimlerinin, günlük hayatta ve ticari faaliyetler çerçevesinde, gerçek ve sanal mal ve hizmet alımlarında ödeme aracı olarak kullanıldıkları, dünya çapında birçok büyük şirket tarafından kabul edildikleri, yüzlerce takas ve borsa merkezinde işlem gördükleri, tedavülde olan birçok ülke parasıyla çift yönlü konvertibiliteye sahip oldukları ve toplamda 700 milyar ABD dolarına kadar yükselmiş pazar büyüklüğüne eriştikleri göz önüne alındığında işin mahiyeti ve önemi kendini hissettirmektedir.

Kripto para birimi sistemlerinin, sadece geleneksel para ve onun dijital uzantısı olan elektronik paranın fonksiyonlarını, başka bir deyişle ortak hesap birimi, mübadele aracı ve sermaye birikim aracı olma işlevlerini, sanal dünyada yerine getiren alternatif para birimleri olarak görülmemeleri gerekir. Gerçekten de, bu konuyla ilgili tartışmalara bakıldığında, kripto para birimlerinin merkezi omurgasını oluşturan blokzinciri denilen teknolojik yeniliğin vadettikleri arasında akıllı sözleşmeler ve akıllı mülkler ile başlayan ve nihayetinde Devlet tarafından yürütülen, neredeyse bütün kamu hizmetlerinin merkezi bir yönetim ve denetim birimi olmadan gerçekleştirilebileceği bir süreçten bahsedilmektedir.

* <https://coinmarketcap.com>, Erişim tarihi: 24 Temmuz 2018.

Kripto para birimlerinin en önemli özellikleri merkezî birer yapı belirtmemeleri ve işleyişlerinde kriptografiyi esas almalarıdır. Bu özellikler, şüphesiz bilişim ve internet teknolojilerindeki gelişmelerinin birer yansıması olsa da bu sistemlerinin gelişimine öncülük eden *Cypherpunks* hareketinin felsefesini yansıtmaktadır. Bu hareketin bağlilarına göre kişilerin özel hayatlarında ve haberleşmelerinde mahremiyet esastır ve bu mahremiyet, hukuksal düzenlemeler yerine kriptografi kullanılarak sağlanabilir.

Mevcut ekonomik, finansal, hukuksal yapılar ve düzenlemeler açısından merkezi olmamanın veya işlemlerin şeffaflığını giderici ve işlem taraflarının kimliğini gizleyici kriptografik teknikleri kullanmanın sarsıcı etkileri olacağını tahmin etmek zor değildir. Bugünkü hukuk düzenlerinde banka ve finans kuruluşları, merkezi yapılar olarak, kendileri aracılığıyla gerçekleştirilen işlemlerin hukuka uygunlukları bakımından oldukça önemli rollere ve yükümlülöklere sahiptir. Örneğın suçtan kaynaklanan malvarlığı değerinin aklanması, vergi kaçırma veya terörün finansmanı gibi uluslararası toplumun hassas olduğı suçlar bakımından bu kuruluşların kanunla belirlenen, şüpheli işlemlerin ilgili birimlere bildirilmesi veya müşterilerinin kimliklerinin bilinmesi gibi birtakım yükümlölükleri vardır. Kripto para birimi sistemlerinde, bu yükümlölükleri üstlenebilecek veya yerine getirebilecek herhangi merkezi bir birim yoktur. Bunun yanında, işlemlerin belirsiz kimliklerle yapılabilmesinin önünde bir engel de bulunmamaktadır.

Kripto para birimlerinin sağladığı anonimlik, başka bir deyişle belirsiz kimlikle işlem yapabilme özelliğı ile arada banka gibi bir aracı olmaksızın, internet erişiminin olduğı her yerde, dünyanın bir noktasından başka bir noktasına para transferi gerçekleştirebilmektedir. Nitekim istismara açık olan bu özelliğı ilişkin olumsuzluklar gün geçtikçe artan bir şekilde yaşanmakta ve yetkililer nezdinde kripto para birimlerine karşı olumsuz bir yargının oluşumuna da neden olmaktadır.

Kripto para birimleri, suç faaliyetlerinden başka, hükümet politikalarının uygulama kapsamı dışında kaldıkları için ulusal egemenliğe de birer tehdit oluşturabilecek potansiyele sahiptirler. Bu tehditler, başta vergilendirme olmak üzere, ekonomik ve mali politikalara yöneliktir. Bunun yanında piyasada bulunan para hacmi, merkez bankaları veya benzeri kurumların belirlediğı politikalar

doğrultusunda kontrol edilirken, kripto para birimi kullanımı bu düzen için de tehdit oluşturmaktadır. Çünkü kripto para birimlerinde para ihraçları, merkezî kurumlarca belirlenen hedeflere göre değil, geliştiricilerinin belirlediği kurallar doğrultusunda, tamamen piyasanın arz ve talep dengesine göre belirlenmektedir.

Kripto para birimi sistemleri, henüz hiçbir ülkenin hukuk düzeninde belli bir konuma sahip değildir. Bu belirsizliğin temelinde, konunun yeni olması, hızla evrilmesi, gelişim aşamasında olması ve hukuki tanımı eksikliği gösterilmektedir. Bunun yanında geleneksel olarak ayrıık yapılar olan para birimi, ödeme sistemi ve emtia unsurlarının bu sistemlerde entegre olarak bir arada sunulması işleri daha da karmaşık hale getirmektedir.

Gerçekten de kripto para biriminin ne olduğu; para, emtia, menkul değer veya başka bir şey olarak kabulü konusunda tartışmalar hem ulusal hem de uluslararası düzeyde devam etmektedir. Biraz yavaş ilerleyen bu hukuksal arayış sürecinin temel kaygısı, ekonomik ve finansal alanlara olumlu katkısı olacağı düşünülen bu teknolojik yeniliğin, yersiz kısıtlamalarla önünün kesilmemesi ve yanlış yönlendirilmemesidir. Ayrıca tek bir ülke tarafından yapılacak düzenlemenin, doğası gereği küresel bir işleyişe sahip bir sistemi kontrolde yeterli olamayacağı da açıktır. Fakat kural yokluğunun neden olduğu bu belirsizlik devam ettikçe, hem bu sistemlerin sağlıklı gelişimi sekteye uğratmakta hem de yasadışı faaliyetlerde kullanılmalarına zemin hazırlanmaktadır.

Kripto para birimlerinin hukuksal konumuna ilişkin uluslararası ve ulusal düzeyde tartışmalar devam ederken, ülkemizde doktrinde bu sistemlere ilişkin yeterli sayıda çalışma bulunduğunu söyleyemeyiz. Bu konuda rastladığımız birkaç çalışma, bilimsel bir incelemeden ziyade yazarların kişisel kanaatlerini içermektedir. Bunun yanında Yargıtay'ın kripto para birimlerine ilişkin kararları da henüz oluşmamıştır.

Buna rağmen ülkemizde kripto para birimlerine ilgi her geçen gün artmakta ve kullanımları yaygınlaşmaktadır. Yakın bir zamanda, kripto para birimlerine ilişkin hukuksal uyumsuzlukların ve kriminal olayların mahkemelerimizin önüne geleceği kuşkusuzdur. Bu nedenle bu sistemlere ilişkin hukuki belirsizliğin giderilmesi önem

arz etmektedir. Bütün bunlar göz önüne alınarak, bu tezin konusu olarak kripto para birimleri seçilmiştir.

Bu incelemeyle, kripto para birimlerinin hukuksal konumları, işleyişleri ele alınmış ve ceza hukuku bağlamında bir değerlendirmesi yapılmaya çalışılmıştır. Ayrıca kripto para birimlerinin suç konusu olabileceği Türk Ceza Kanunu'nda yer alan bazı suçlar ele alınmıştır.

Çalışma, temelde iki bölümden oluşmaktadır. Birinci bölümde, kripto para birimlerinin kavramsal yapıları ve işleyiş mekanizmaları ortaya konulmaya çalışılmıştır. Bu çerçevede, uluslararası ve ulusal çalışmalarda ele alınan kripto para birimi kavramı, geleneksel para, dijital para, elektronik para, sanal para birimi ve diğer kavramlarla birlikte incelenmiş, aralarındaki benzerlikler, farklılıklar ve ilişkiler ortaya çıkarılmaya çalışılmıştır.

Kripto para birimlerinin ortaya çıkışı ve tarihsel gelişiminin ele alındığı birinci bölümün ikinci ayrımında, bilişim teknolojilerinin gelişimiyle beraber başlayan ve kripto para birimlerinin ortaya çıkışıyla sonuçlanan gelişmeler dizisi kronolojik bir çizgide ele alınmıştır. Bu gelişmeye öncülük eden kişiler, gruplar, hareketler ve diğer teknolojik yenilikler hakkında bilgi verilmiştir.

Kripto para birimlerinin ortak özelliklerinin ele alındığı üçüncü ayrımında, her geçen gün yeni bir kripto para birimi duyurusunun yapıldığı bir ortamda, bu sistemlerin paylaştıkları, açık kaynak kod, merkezi olmamak veya kriptografik teknikler kullanmak gibi ortak özellikler açıklanmaya çalışılmıştır. Bu özellikler ele alınırken, konunun anlaşılması bakımından yeteri kadar teknik bilgi birikiminin oluşması ve kripto para birimlere ilişkin kavramsal bir bakışın oluşması hedeflenmiştir.

Kripto para birimlerine ilişkin hukuksal düzenleme arayışları ayrımında, bu konudaki mevcut hukuki durum ortaya konmuş ve bu düzenleme arayışlarının nedenleri, zorlukları ve uluslararası camianın bu konudaki tavsiyelerine değinilmiştir.

Uluslararası arayışlar kısmında, FATF, IMF, OECD ve UNODC gibi uluslararası kuruluşların kripto para birimleriyle ilgili çalışmaları ele alınmış; bölgesel ve ulusal hukuksal düzenleme arayışları kısmında ise başta Avrupa Birliği olmak üzere, ABD, İngiltere, Almanya, Çin ve Rusya gibi belli başlı ülkeler ile Türkiye'nin kripto para birimine ilişkin hukuki durumları incelenmiştir.

Kripto para birimlerinin ceza hukuku bakımından değerlendirilmesini içeren ayrımda, kripto para birimlerinin para, emtia veya menkul değer olarak kabulünün mümkün olup olmadığı tartışılmıştır. Ardından, kripto para biriminin kullanımının yasallığı ele alınmıştır.

Kripto para birimleri, bilişim sistemlerine dayanan karmaşık yapı ve işleyişlere sahiptirler. Daha önce duyulmamış kavramlar, bu sistemler aracılığıyla gündeme gelmiştir. Örneğin akıllı sözleşme diye kendi kendini ifa eden sözleşmelerden bahsedilmektedir. Bunun yanında blokzinciri, iş kanıtı, hesap adresi gibi bu sistemlere ait yapısal bileşenler bilinmeden konunun tam olarak anlaşılabilmesi mümkün gözükmemektedir. Bu nedenle birinci bölümün son ayrımı, bir kripto para birimi örneği olarak Bitcoin'in detaylı incelenmesine ayrılmıştır.

Bu ayrımda, ilk kripto para birimi Bitcoin'in geliştiricisi Satoshi Nakamoto'nun Bitcoin'in teknik yapısı ve işleyişini açıkladığı makalesi ele alınmış, ardından Bitcoin ekosisteminde yer alan bileşenler tanıtılmıştır. Bitcoin sisteminin teknik yapısında yer alan Bitcoin adresi, cüzdan, hareket, blok, blokzinciri, iş kanıtı ve madencilik gibi unsurların yapılarına ilişkin açıklamalardan sonra Bitcoin ağı ve güvenliğine ilişkin hususlar ele alınmıştır. Bu kısmın sonunda, Bitcoin'e alternatif diğer kripto para birimleri tanıtılmış ve bu sistemlerin para birimi dışında diğer uygulamalarına değinilmiştir. Bu şekilde birinci bölüm tamamlanmıştır.

İncelemenin ikinci bölümünde, kripto para birimlerinin Türk Ceza Kanunu'nda düzenlenen bazı suçlar bakımından ayrıntılı bir değerlendirmesi yapılmıştır. Bu suçlar, malvarlığına karşı suçlar, bilişim alanında suçlar ile adliye karşı suçlar bölümünde yer alan suçlardan oluşmaktadır. Her bir suç için, suçların incelenmesine ilişkin klasik yöntem takip edilmiştir.

Bu bölümün ikinci ve son kısmı, kripto para birimlerinin suç konusu olduđu suçların soruşturulması ve kovuşturulmasında karşılaşılabilecek zorluklara ayrılmıştır.



BİRİNCİ BÖLÜM: KRİPTO PARA BİRİMLERİ VE BITCOIN ÖRNEĞİ

§1. Dijital Para Birimi Kavramı

İnceleme konumuz olan kripto para birimleri için dijital para, elektronik para ve sanal para birimi kavramları da kullanılmaktadır. Birbirine yakın ve bazen iç içe geçmiş özelliklere sahip para birimlerini ifade etmek için kullanılan bu kavramların bazen yanlışlıkla birbiri yerine kullanıldıkları da görülmektedir. Bu nedenle kavramsal yapıyı ortaya çıkarmak amacıyla, sırasıyla dijital para, elektronik para, sanal para birimi ve kripto para birimi kavramları incelenecektir.

I. Dijital Para

Dijital para veya dijital para birimi (ing. *digital money, digital currency*), belli bir para birimine veya para birimi türüne işaret eden bir kavram olmak yerine, geleneksel para, sanal para ve kripto para birimlerinin dijital temsil özelliğini ifade etmek için kullanılan bir çatı kavram olarak tanımlanmaktadır¹. Bu tanımdaki dijital temsil, bilgisayarlar tarafından işlenebilme özelliğini ifade etmektedir².

A. Elektronik Para

Elektronik para, bir ülkede yasal ödeme aracı olarak tedavül gören itibari paranın³ elektronik formu için kullanılan bir kavramdır.

¹ Financial Action Task Force (FATF), **Virtual Currencies - Key Definitions and Potential AML/CFT Risks**, Haziran 2014, s. 4, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, Erişim tarihi: 16 Mart 2018.

² **A.g.e.**, s. 13.

³ **İtibari para** (ing. *fiat money, fiat currency*), merkez bankaları gibi bir merkezî otorite tarafından belirlenen ve ihraç edilen yasal ödeme aracını ifade etmektedir. Günümüzde dolaşımda olan banknotlar itibari paralardır. Türkiye Cumhuriyeti için yasal ödeme aracı Türk Lirasıdır.

Avrupa Birliği (AB) Elektronik Para Direktifine (2009/110) göre, elektronik para, karşılığında gösterilen parasal değerden daha az olmayan fonun alınması üzerine ihraç edilen, ihraç edici kuruluş haricinde taahhütte bulunanlar tarafından da ödeme aracı olarak kabul edilen, ihraç edicisine karşı bir taleple temsil edilen ve elektronik olarak saklanan parasal değerdir⁴.

Elektronik para, mevzuatımızda 6493 sayılı “*Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun*”un Tanımlar başlıklı 3. maddesinin 1-f bendinde tanımlanmıştır. Buna göre, elektronik para, “*İhraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, bu Kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değeri*” ifade etmektedir.

Bu tanımda yer alan unsurlara yakından bakılırsa; elektronik paralar, elektronik ortamlarda depolanabilmelidir. Başka bir deyişle, cep telefonu, akıllı kart, bilgisayar, tablet veya çevrimiçi cüzdan gibi dijital ortamlarda depolanabilmeli ve bu araçlar arasında transfer edilebilmelidir.

Elektronik para ile ancak Kanunda belirtilen ödemeler yapılabilir. Bu ödeme işlemleri, Kanunun 12. maddesinin 1. fıkrasında düzenlenmiştir. Bunlar, ödeme hesabına para yatırma, hesaptan para çekme, para havalesi, para transferi, bilişim sistemi aracılığıyla ödeme işlemi ve fatura ödemeleridir.

Elektronik para birimleri, ihraç eden kuruluş tarafından kabul edilen bir fon karşılığı ihraç edilmelidir. Buna göre ihraç edici kuruluşa belirli bir miktar fon ödenmeli ve elektronik para ihracı bu fon karşılığında yapılmalıdır. Bu şekilde, ihraç edilen elektronik para, banknot veya madeni sikke biçiminde daha önce ihraç edilmiş geleneksel paranın yerine kullanılmaktadır.

⁴ European Central Bank (ECB), **Virtual Currency Schemes** (October 2012), s. 13.
<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, Erişim tarihi: 15 Mart 2018.

Elektronik para, yasal olarak onu ihraç etmeye yetkili kılınmış kuruluş dışında başka gerçek veya tüzel kişiler tarafından da ödeme aracı olarak kullanılabilirdir. Elektronik paranın, ihraç edici kuruluşunun dışında, başkaları tarafından da ödeme aracı olarak kabul edilmesi, onun piyasalarda tedavülünü sağlayacaktır.

B. Sanal Para Birimi

Sanal para birimi, elektronik para dışındaki diğer dijital paraları ifade etmek için kullanılan bir çatı kavramdır. Kripto para birimi de sanal para birimleri kapsamında değerlendirilmektedir.

Avrupa Merkez Bankası (*European Central Bank, ECB*), 2012 yılında yayımladığı “*Virtual Currencies Schemes / Sanal Para Birimi Şemaları*” başlıklı analizinde sanal para birimini, geliştiricileri tarafından ihraç edilip genellikle onlar tarafından kontrol edilen, belli bir sanal topluluk (*virtual community*) arasında kullanılan ve kabul edilen, yasal olarak düzenlenmemiş dijital para birimi olarak tanımlamıştır⁵.

ECB, 2015 yılında sanal para birimleriyle ilgili yayımladığı yeni analizinde 2012 yılı tanımında değişikliğe gitmiş, sanal parayı, bir merkez bankası, kredi kuruluşu veya elektronik para kuruluşu tarafından ihraç edilmeyen ve bazı durumlarda paraya alternatif olarak kullanılabilen, değer bir dijital temsili olarak tanımlamıştır⁶. Bu yeni tanımda, 2012 tanımında bulunan “*para*”, “*yasal olarak düzenlenmemiş*” ve “*belli bir sanal topluluk tarafından kullanılan ve kabul edilen*” ifadeleri çıkarılmıştır.

Avrupa Bankacılık Otoritesi (*Europe Banking Authority, EBA*), 2014 yılında yayımladığı “*EBA Opinion On ‘Virtual Currencies’ / Sanal Para Birimleri Hakkında EBA Görüşü*” raporunda⁷ sanal para birimini, bir merkez bankası veya kamu otoritesi tarafından ihraç edilmeyen, zorunlu olarak bir itibari paraya bağlanmamış olan, fakat

⁵ ECB, a.g.e., s. 5.

⁶ ECB, *Virtual Currency Schemes – A Further Analysis*, 2015, s. 33, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, Erişim tarihi: 12 Mart 2018.

⁷ Europe Banking Authority (EBA), *EBA Opinion On ‘Virtual Currencies’*, 04.07.2014, <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>, Erişim tarihi: 17 Mart 2018.

gerçek veya tüzel kişiler tarafından bir mübadele aracı olarak kabul edilen ve elektronik olarak transferi, saklanabilmesi ve ticareti mümkün, değerini dijital bir temsili olarak tanımlamıştır⁸.

Uluslararası Para Fonu (*International Monetary Fund, IMF*), 2016 yılında yayımladığı “*Virtual Currencies and Beyond / Sanal Para Birimleri ve Ötesi*” başlıklı bilgi notunda, sanal para birimlerini, özel geliştiriciler tarafından ihraç edilen ve kendine özgü birimlere sahip, değerini birer dijital temsili olarak tanımlamıştır⁹.

Mali Eylem Görev Gücü¹⁰ (*Financial Action Task Force, FATF*), tarafından 2014 yılında yayımlanan rapordaki tanıma göre, sanal para birimi, değerini dijital olarak ticaretini mümkün kılan dijital temsillerdir. Sanal para birimleri, hiçbir ülkede yasal ödeme aracı statüsüne sahip değildirler ve hiçbir hükümet tarafından ihraç edilmemiş ve teminat altına alınmamışlardır. Bu para birimleri, sahip oldukları fonksiyonları, ancak onları kullanan kişilerden oluşmuş topluluğun kabulüyle yerine getirebilmektedirler¹¹.

Amerika Birleşik Devletleri (ABD) Mali Suçlarla Mücadele Birimi (FinCEN), 2013 yılında yayımladığı *FinCEN Kurallarının Sanal Para Birimlerini Yöneten, Takas eden ve Kullananlara Uygulanması Kılavuzu*’nda¹² sanal para birimini, bazı ortamlarda para birimi gibi işlemekle birlikte gerçek paranın (*real money*) sahip olduğu bütün özelliklere sahip olmayan mübadele aracı olarak tanımlamış ve sanal para birimlerinin yasal ödeme aracı olmadığını vurgulamıştır¹³.

II. Bir Dijital Para Olarak Kripto Para

⁸ A.g.e., s. 11.

⁹ International Monetary Fund (IMF), **Virtual Currencies and Beyond**, 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, Erişim tarihi: 14 Mart 2018.

¹⁰ Mali Eylem Görev Gücü (Financial Action Task Force, FATF), kara paranın aklanması, terörizmin finansmanı ve kitle imha silahların yayılmasının finansmanı ile mücadele alanında hem ulusal hem de uluslararası alanda politikalar geliştiren ve bu politikaları destekleyen temel bir uluslararası kuruluştur. Geniş bilgi için bkz. <http://www.fatf-gafi.org>, Erişim tarihi: 16 Mart 2018.

¹¹ FATF, a.g.e., s. 4.

¹² <https://www.fincen.gov/sites/default/files/guidance/FIN-2013-G001.pdf>, Erişim tarihi: 17 Mart 2018.

¹³ A.g.e., s. 1.

Kripto para birimi kavramı, (İng. *cryptocurrency, crypto currency*) kendine özgü bazı niteliklere sahip dijital paraları ifade etmek için kullanılmaktadır. Genel olarak sanal para birimleri çatısı altında farklı kategoride ele alınan kripto para birimleri üzerinde uzlaşmış bir tanımla bulunmamaktadır. Buna sebep olarak, kripto para birimi piyasasının gelişimini hâlâ tamamlanmamış olması¹⁴ ve konuyla ilgili hukuksal düzenlemelerin ortaya çıkmamış olması¹⁵ gösterilmektedir.

Oxford sözlüğünde yer alan tanıma göre, kripto para birimi, merkez bankalarından bağımsız olarak işleyen ve paranın ihracında ve tedavülünde kriptolama tekniklerinin kullanıldığı dijital para birimidir¹⁶.

FATF'a göre kripto para birimleri, dağıtık, açık kaynak kodlu, matematiğe dayalı ve eşler arası ağ (*peer-to-peer*) üzerinde işleyen para birimlerini ifade etmektedir. Bu para birimlerinde merkezî yönetim otoritesi olmadığı gibi, merkezî bir kontrol ve gözetim de söz konusu değildir¹⁷. Kripto para birimlerinde, dağıtık ve bir merkeze bağlı olmadan işleyebilecek güvenli bir bilgi ekonomisini geliştirmek için kriptografik ilkeler kullanılmaktadır¹⁸.

Bir grup araştırmacıya göre kripto para birimi, paranın üretilmesinde ve dağıtılmasında kriptografinin kullanıldığı, eşler arası dijital bir takas sistemidir¹⁹.

Başka bir tanıma göre, kripto para birimi, kullanıcılarına, güvenilir merkezî bir otorite bulunmaksızın mal ve hizmetler için sanal bir ödeme aracı sağlayan ve standart bir para birimi gibi çalışan sanal para ihraç sistemidir. Kripto paralar, dijital bilgilerin iletilmesine dayanırlar ve kriptografik metotlar kullanarak para hareketlerinin kurallara uygun ve tekil olmalarını sağlarlar²⁰.

¹⁴ IMF, **a.g.e.**, s. 7.

¹⁵ FATF, **a.g.e.**, s. 4.

¹⁶ <https://en.oxforddictionaries.com/definition/cryptocurrency>, Erişim tarihi: 12 Mart 2018.

¹⁷ FATF, **a.g.e.**, s. 5.

¹⁸ **A.g.e.**

¹⁹ Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, Richard Brooks, "A Brief Survey of Cryptocurrency Systems," **2016 14th Annual Conference on Privacy, Security and Trust (PST)**, 2016, s. 745-752. <http://ieeexplore.ieee.org/document/7906988>, Erişim tarihi: 20 Mart 2018.

²⁰ Ryan Farrell, **An Analysis of the Cryptocurrency Industry**, 2015, s. 3. Wharton Research Scholars.130., 2015, http://repository.upenn.edu/wharton_research_scholars/130, Erişim tarihi: 6 Mayıs 2018.

Sermaye Piyasası Kurulu (SPK), Aralık 2016’da yayımladığı raporda²¹, kripto para birimlerini “*kriptografik/şifreli olarak güvenli işlem yapmaya ve ek sanal para arzına olanak sağlayan dijital değerler*” olarak tanımlamış²² ve alternatif para birimi²³ olduklarını vurgulamıştır.

Kanaatimize göre, kripto para birimi, paranın ihracında ve dolaşımında başta kriptografik teknikler olmak üzere bilişim teknolojilerinin kullanıldığı, herhangi bir merkezî yapının yönetiminde ve denetiminde olmayan, ulusal paralara alternatif dijital para birimi olarak tanımlanabilir.

Kripto para birimi ile ilgili bu tanımlarda geçen “merkezî olmama” ve “kriptografi” ve diğer ortak özellikler “Kripto Para Birimlerinin Ortak Özellikleri” bölümünde ele alınacaktır.

III. Kripto Para Birimi ile Elektronik Para Arasındaki Farklar

Elektronik para ile kripto para birimi arasında en büyük fark, elektronik paranın yasal ödeme aracı olan itibari para ile olan yasal ilişkisinin devam etmesidir²⁴.

EBA, yayımladığı raporda elektronik para ile kripto para birimi arasındaki farkı, kripto paranın zorunlu olarak itibari para birimine bağlanmamış olması, başka bir deyişle itibari para cinsinden sabit bir değere sahip olmaması ve ihraç eden tarafından zorunlu olarak nominal değeri (*par value*) üzerinden ödenmesinin sabitlenmemiş olması şeklinde açıklamıştır²⁵.

FATF’a göre, kripto para birimi, elektronik paradan farklıdır. Çünkü elektronik para, ülkede kabul edilen itibari paranın dijital temsilidir ve itibari para cinsinden ihraç edilen paranın elektronik olarak transfer edilebilmesi amacıyla

²¹ Sermaye Piyasası Kurulu (SPK), **Kripto-Para Bitcoin**, Aralık 2016, <http://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130>, Erişim tarihi: 19 Mart 2018.

²² **A.g.e.**, s. 8.

²³ Alternatif para birimi (İng. *alternative currency*), belli bir bölgede ülke parası yerine kullanılmak üzere özel olarak geliştirilmiş fakat hükümet veya bir banka tarafından düzenlenmemiş para türüdür. (SPK, **a.g.e.**, s. 5.)

²⁴ ECB, **Virtual Currencies**, s. 16.

²⁵ EBA, **a.g.e.**, s. 11.

kullanılmaktadır. Elektronik para, ülke parasıyla ilişkili olduğu için yasal ödeme aracıdır. Bu özellikler kripto para birimlerinde yoktur²⁶.

ECB'nin 2012 analizinde kripto para birimlerinin dâhil edildiği sanal para ile elektronik para karşılaştırması yapılmıştır²⁷. Bu raporda yapılan karşılaştırmaya göre, (1) Elektronik paralar, resmi olarak yetkili kuruluşlar tarafından ihraç edilmektedir. Kripto para birimleri ise, özel girişimciler tarafından geliştirilmişlerdir. (2) Elektronik paraların yasal ödeme aracı olma özelliği, kripto para birimlerinde yoktur. (3) Elektronik paralar, kendilerini ihraç eden kuruluşlar dışında, onları kabul edeceklerini taahhüt eden kuruluşlar arasında kullanılmaktadır. Buna karşın kripto para birimleri sadece onları kabul eden topluluk içinde kullanılmaktadır. (4) Elektronik paralar, yasal olarak düzenlenmişken, kripto para birimleri için herhangi bir yasal düzenleme yoktur. (5) Elektronik paraların piyasalara ihracı sabittir. Kripto para birimlerinde ise para ihracı, geliştiricilerinin isteğine bağlıdır. (6) Elektronik para fonlarının geri ödenmesi ilgili kuruluşun garantisi altındayken böyle bir garanti kripto paralar için geçerli değildir. (7) Elektronik para denetim altındayken, kripto para birimleri için öngörölmüş denetimler mevcut değildir.

IV. Kripto Para Birimi ile Diğer Sanal Para Birimleri Arasındaki Farklar

Kripto para birimleri, sanal para birimleri arasında yer almalarına rağmen, sahip oldukları bazı özellikler, onları diğer sanal para birimlerinden ayırmaktadır. Bunlardan en belirgin olanları, kripto para birimlerinin işleyişinde ve güvenliğinde kriptografik yöntemlerin kullanılması ve merkezî olmayan yapılara sahip olmalarıdır.

ECB, 2012 analizinde, sanal para birimlerini reel ekonomiyle ilişkisine göre sınıflandırarak, (1) kapalı sanal para birimi şemaları, (2) tek yönlü akışa sahip sanal para birimi şemaları ve (3) çift yönlü akışa sahip sanal para birimi şemaları şeklinde üçe ayırmıştır²⁸. Bu ayırmda kripto para birimleri, çift yönlü akışa sahip sanal para birimleri arasında yer almaktadır.

²⁶ FATF, **a.g.e.**, s. 4.

²⁷ ECB, **Virtual Currencies**, s. 18.

²⁸ ECB, **a.g.e.**, s. 13.

Kripto para birimlerinin dâhil olduğu iki yönlü akışa sahip sanal para birimleri²⁹, gerçek para ile satın alınabildikleri gibi tekrar gerçek paraya çevrilebilirler. Bu para birimleriyle hem gerçek hem de sanal mal ve hizmetler alınabilir. Bu para birimi türüne örnek, kripto para birimi olarak Bitcoin (BTC) ve merkezî sanal para birimi olarak *Second Life* isimli sanal platforma ait *Linden Dollar*³⁰ (L\$) gösterilebilir.

FATF, 2014 analizinde, sanal para birimlerini, gerçek paraya dönüştürülebilme ve merkezî bir yapıya sahip olma özelliklerine göre sınıflandırmıştır.

Kripto para birimleri veya merkezî olmayan sanal birimlerinde merkezî bir yönetim otoritesi olmadığı gibi, merkezî bir kontrol ve gözetim de söz konusu değildir. *Bitcoin*, *LiteCoin* ve *Ripple* kripto sanal para birimlerine birer örnektir³¹.

IMF'nin 2016 analizinde, dijital para, sanal para ve kripto para birimleri arasındaki ilişkiler, hiyerarşik bir düzende gösterilmiştir. Buna göre, dijital para biriminden kripto paraya doğru inildikçe, yasal ödeme aracı olarak kabul edilmek, diğer paralara çevrilebilirlik ve merkezî olma nitelikleri zayıflamaktadır³².

Kripto para birimlerini diğer sanal para birimlerinden ayıran temel özellikler, merkezî olmamaları ve işlemlerinde kriptografik yöntemler kullanılmalarıdır³³.

§2. Kripto Para Birimlerinin Ortaya Çıkışı ve Tarihsel Gelişimi

Kripto para birimlerinin ortaya çıkışı, Bitcoin sisteminin duyurulması ile başlar. Satoshi Nakamoto'nun Bitcoin sistemini açıkladığı makalesini 2008 Ekim ayında, *metzdowd.com* adlı internet sitesinde kriptografi e-posta grubunda

²⁹ A.g.e., s. 14.

³⁰ *Second Life*, (<http://secondlife.com>) Kullanıcıların kendi avatarlarını oluşturup, kendilerine ait sanal mallar ve hizmetler oluşturup alışveriş yapabildikleri bir sanal platformu ifade etmektedir. Bu platformda, bir sanal oyundaki gibi sıkı yapılar yoktur ve gevşek sınırlar söz konusudur. Mesela bir kişi kendine ait bir kafeterya açabilir, sanal yiyecekler ile içecekler sunabilir ve bunların alışverişini yapabilir. Bu alışverişlerde *Linden Dollar* (L\$) kullanılmaktadır. *Linden Dollar*, platform içi aktivitelerden kazanılabilir, gerçek para ile alınabilir ve kişiler arası transfer edilebilir ve nihayet tekrar memleket parasına çevrilebilir. (Halaburda ve Sarvary, a.g.e., s. 73.)

³¹ FATF, a.g.e., s. 5.

³² IMF, a.g.e., s. 8.

³³ A.g.e.

yayımlamıştır. Nakamoto, 3 Ocak 2009 tarihinde sistemi internet üzerinden genel kullanıcı kesimine açmış ve kendisi de ilk Bitcoin madenciliğini gerçekleştirerek, ilk bitcoin'lerin sahibi olmuştur.

Bitcoin'den önce, bu teknolojik yeniliğin ortaya çıkışını hazırlayan önemli bazı gelişmelerinden açıklanması konunun anlaşılmasına yardımcı olacaktır.

Kripto para birimlerinin ortaya çıkaran gelişmelerin başında, dijital mahremiyet taraftarı bir grup bilişim uzmanının kurduğu *Cypherpunk* hareketinin³⁴ ortaya çıkması sayılabilir. Kendilerini anonim (kimliği belirsiz) sistemler kurmaya adanmış bu kriptografi ve bilgisayar uzmanları, mahremiyetin kriptografik teknikler kullanılarak sağlanabileceğini öne sürmüşlerdir. Bitcoin'in kurucusu Satoshi Nakamoto'nun da dâhil olduğu bu grup, güçlü kriptolamanın birçok ekonomik işlemde devletin müdahalesini engelleyeceğini ve sözleşmelerin ifasını kökten değiştireceğini düşünüyorlardı. Bu düşünceler, kriptografik tekniklerin yoğun olarak kullanıldığı dijital para biriminin teorik alt yapısı olarak ilk adım kabul edilmektedir³⁵.

Kripto para biriminin prototipi sayılacak ilk sistem, *Cypherpunk* hareketi üyesi David Chaum tarafından önerilen *eCash* ödeme sistemidir³⁶. Elektronik ticarete kullanılabilecek bu ödeme sisteminde, işlem taraflarının gizliliği kriptografik tekniklerle sağlanmaktadır. Bu sistemi günümüz kripto para birimi sistemlerinden ayıran özelliği merkezi bir yönetim ve denetim birimine gereksinim duymasındır³⁷. Chaum, düşüncelerini gerçekleştirmek için 1990 yılında *eCash* markasıyla *DigiCash* şirketini kurdu. Şirket umduğu başarıyı yakalayamadı, sadece bir banka *eCash* sistemini mikro ödeme sistemi olarak hayata geçirdi. DigiCash şirketi 1998 yılında iflas etti³⁸. Fakat buna rağmen, *eCash* sistemi, kripto para birimine doğru atılan ilk somut adım olarak kabul edilmektedir.

³⁴ <https://www.cypherpunks.to>, Erişim tarihi: 21 Mart 2018.

³⁵ Eric Hughes, **A Cypherpunk's Manifesto**, <https://www.activism.net/cypherpunk/manifesto.html>, Erişim tarihi: 21 Mart 2018.

³⁶ David Chaum, **Blind Signatures For Untraceable Payments**, <https://chaum.com/publications/Chaum-blind-signatures.PDF>, Erişim tarihi: 20 Mart 2018.

³⁷ Mukhopadhyay ve dig., **a.g.e.**, s. 1.

³⁸ Halaburda ve Sarvary, **a.g.e.**, s. 113.

Kripto para birimlerinin gelişiminde ikinci önemli gelişme, ilk internet ödeme sistemi *e-gold*'un ortaya çıkmasıdır. *e-gold*, altına dayalı dijital çevrimiçi ödeme sistemidir. Sistemin amacı devletin kontrolü dışında tedavül eden özel ve uluslararası bir para birimi meydana getirmektir³⁹. *e-gold*, bir tamamlayıcı para birimi olmaktan (*complementary currency*) ziyade, alternatif bir dijital para birimidir⁴⁰. *e-gold* hareketleri, banka para işlemlerinin aksine geriye döndürülmez biçimde kesindi⁴¹. Sistemin daha sonra suçlanmasına sebep olarak gösterilen bir başka özelliği, müşterilere ait kimliklerin tespit edilmesini zorlaştıran takma adlarla kayıt olunabilmesine imkân sağlamasıydı⁴². Sistemin başarısı ve yaygınlığı, özellikle Doğu Avrupa'dan *hacker*'lerin⁴³ dikkatini çekmeye başladı ve sisteme kayıtlı hesap sahiplerinin bilgilerinin çalınmasına veya çocuk pornografisi ticareti gibi yasadışı işlemlerdeki para hareketleri için aracı olarak kullanılmasına engel olunamadı⁴⁴. Şirketin işlemleri, 2009 yılında kara para aklamak ve lisanssız para transferi işlemlerini gerçekleştirmek suçlamalarıyla ABD hükümeti tarafından askıya alındı⁴⁵.

e-gold, alternatif dijital para birimi olma, anonim işlem yapabilme ve para hareketlerinin geri döndürülemezliği (kesinliği) özellikleriyle kripto para birimlerine model olmuştur.

Kripto para birimi sistemlerinin ortaya çıkması sağlayan en önemli teknik gelişmelerden birisi de *hashcash*'tir⁴⁶. Bilişim tekniğinde *DoS* saldırısı⁴⁷ olarak bilinen zararlı aktivitelerden korunmak için geliştirilen *hashcash*, bir matematik probleminin çözümünün iş kanıtı (*work-of-proof*) olarak sunulması düşüncesine dayanmaktadır. Bitcoin sisteminde para hareketlerinden oluşan blokların, veritabanı

³⁹ P. Carl Mullan, **A History of Digital Currency in the United States**, Whitestone, Virginia: Palgrave macmillan, 2016, s. 19.

⁴⁰ **A.g.e.**, s. 24.

⁴¹ **A.g.e.**, s. 25.

⁴² **A.g.e.**, s. 24.

⁴³ **Hacker**: Teknik olarak bilgili bir bilgisayar uzmanı. Korunma altındaki kaynakları yetkisiz şekilde erişerek elde etmeyi tasarlayan teknik olarak bilgili bir bilgisayar uzmanı. (Türk standartları Enstitüsü, **TSE Bilişim Terimleri Sözlüğü İngilizce-Türkçe**, 1.b., Ankara: Onur Matbaacılık, 2006., *hacker* maddesi.)

⁴⁴ <https://dgcmagazine.com/the-e-gold-story>, Erişim tarihi: 20 Mart 2018.

⁴⁵ **A.g.y.**

⁴⁶ <http://www.hashcash.org>, Erişim tarihi: 21 Mart 2018.

⁴⁷ *DoS* saldırısı (*denial-of-service-attack*), hizmet reddi. Kaynaklara yetkili erişimin engellenmesi veya zamanın önemli olduğu etkinliklerin engellenmesi. (TSE Bilişim Terimleri Sözlüğü, *denial of service* maddesi)

(*blockchain*) eklenmesinde istenen iş kanıtı, temelde *hashcash* algoritmasıyla aynı mantığa sahiptir.

Kripto para birimlerinin oluşumu bakımından bir başka önemli gelişme, kriptografi uzmanı ve aynı zamanda *Cypherpunks* üyesi olan Wei Dai tarafından 1998 yılında önerilen *b-money* sistemidir. Dai'nin "*b-money; anonim ve dağıtık elektronik nakit sistemi*" adlı makalesinde⁴⁸ açıklanan bu sistem, izlenemez dijital takma adlara (*pseudonyms*) sahip kişilerden oluşmuş bir grubun kendi aralarındaki ödemeleri, *b-money* ile yapabilmelerini ve grup dışında herhangi bir yardım almaksızın kendi aralarındaki sözleşmelerin ifasını sağlamayı hedefliyordu⁴⁹. Dai'nin önerdiği *b-money* sisteminde yer alan temel kavramlar, daha sonra Bitcoin ve diğer kripto para birimi sistemlerinde geniş uygulama alanı bulmuşlardır. Bunlar, belli bir bilgi işlem gücünün harcanması (iş kanıtı, *work of proof*); yapılan işin ortak defterikebiri (*ledger*) güncelleyen bir topluluk tarafından doğrulanması; iş kanıtını sunan kişinin belli bir fonla ödüllendirilmesi; fon transferlerinin toplu muhasebeyle sağlanması ve kriptografik *hash*'lerle doğrulanması; sözleşmelerin yayınlanma zorunluluğu ve para hareketlerin dijital imzalarla imzalanması olarak gösterilebilir.

*Bit Gold*⁵⁰, bir başka *Cypherpunks* üyesi bilgisayar bilimcisi, hukukçu ve aynı zamanda kriptografi uzmanı olan Nick Szabo tarafından 2002 yılında önerilen bir kripto para birimi öncüsüdür. Szabo, enflasyon sorunu olmayan ve sahip olduğu değer ve işleyiş bakımından hiç veya minimal düzeyde güvenilir üçüncü bir taraf gerektiren para sistemi düşüncesini, altın gibi değerini kendinden alan ve miktarı kişilerin iradesine bağlı olarak çoğaltılamayan değerli madenleri model alarak tasarlamıştı⁵¹. Zor problemlere çözüm bulmanın altın madenciliği gibi zor bir faaliyet olduğunu düşünen Szabo'ya göre bir problemin çözümü enerji ve zaman alıyorsa, bu çözümün bir değere sahip olduğu düşünülebilir ve bu değer, onu sağlayana dijital bir mülkiyet olarak verilebilir.⁵² İş kanıtı (*proof-of-work*) gibi çalışan ve bit'lerden* oluşmuş belli bir dizinin üretilmesinin zorluğunu ispat eden bir fonksiyonun ürettiği

⁴⁸ <http://www.weidai.com/bmoney.txt>, Erişim tarihi: 21 Mart 2018.

⁴⁹ A.g.m.

⁵⁰ <http://unenumerated.blogspot.com.tr/2005/12/bit-gold.html>, Erişim tarihi: 22 Mart 2018.

⁵¹ A.g.y.

⁵² Morgen E. Peck, "Cryptoanarchists' Answer to Cash," **IEEE Spectrum**, C.49/6, Haziran 2012, s. 53.

* Bit: İkili sayı sisteminde kullanılan 0 veya 1 rakamlarının her biri. (TSE Bilişim Sözlüğü, *bit* maddesi.)

bit dizileri, *Bit Gold* ağındaki topluluk tarafından kabul edildiğinde mülkiyet zinciri veritabanına eklenecek ve iş yapana da bu işin karşılığında belli bir miktar para verilecekti⁵³. Zincirin son durumu, bir sonraki işlem için yeni bir başlangıçtır. Bu sistemde topluluk tarafından kabul edilme şartı, zaman damgası işlevi görür ve bu kabul zincir halkalarının ancak ileriye doğru büyüdüğünü garanti eder. Eğer topluluk, çözüm üzerinde uzlaşmazlarsa, bir sonraki problemin çözümüne geçilemez⁵⁴. Bu sistemde öngörülen iş kanıtı, iş kanıtını sunan kişilere ihraç edilen değer cinsinden ödeme yapılması, zaman damgası zinciri, kripto para birimlerinde uygulama alanı bulan özelliklerdir.

Bitcoin'inin doğuşunu hazırlayan gelişmelerden birisi de 2004 yılında Hal Finney tarafından geliştirilen ve Nick Szabo'nun koleksiyon teorisine dayalı dijital bir kripto para birimi için prototip olarak tasarlanan *Reusable Work of Proof (RPOW)* / *Tekrar Kullanılabilir İş Kanıtı* buluşudur⁵⁵. Szabo'nun düşündüğü bu dijital para biriminde, para ihracının zorluğu kanıtlanarak para arzının sınırlı oluşu gösterilebilecek ve bu da onun para birimi olarak kullanılabilmesine imkân sağlayacaktı. Bunun için para biriminin iş kanıtı cinsinden tanımlanması gerekiyordu. Bu dijital koleksiyon düşüncesi, Wei Dai'nin *B-money*'inde ve Szabo'nun *Bit gold*'unda birer öneriyken, Finney'in *RPOW*'uyla çalışan bir yazılım olarak ortaya konulmuş oldu⁵⁶. Bir *RPOW* kullanıcısı, gösterilen zorluk derecesini karşılayan iş kanıtını, kendi dijital imzasıyla imzalayarak sisteme sunacak ve sistem de bu iş karşılığı üretilen para birimini, imzalayan anahtar hesabına alacak kaydedecekti. Kullanıcı, hesabındaki parayı yine kendi imzasıyla başka bir genel adrese (hesap adresine) transfer edebilecekti. *RPOW* sisteminde, bütün dijital para birimlerinin çözmesi gereken çifte harcama problemi (*double spending problem*), üretilen bütün para birimlerin güvenilir bir sunucuda saklanmasıyla çözülmüyordu⁵⁷.

Bitcoin sisteminin, bu bölümde anlatılan girişimlerinin gerçekleştirmeyi hedefledikleri, reel dünyanın gerçek para birimlerine alternatif olabilecek, merkezî olmayan, paranın arzında ve kişiler arası transferinde kriptografik metotlar

⁵³ Peck, a.g.m., s. 53.

⁵⁴ A.g.m.

⁵⁵ **RPOW - Reusable Proofs of Work** <http://nakamotoinstitute.org/finney/rpow/index.html>, Erişim tarihi: 25 Mart 2018.

⁵⁶ A.g.m.

⁵⁷ A.g.m.

kullanılarak sistem güvenliğini sağlandığı, dijital para birimi düşüncesini gerçekleştirdiği söylenebilir.

Bitcoin sisteminin başarısı, başka kripto para birimi geliştiricilerini kendi düşüncelerini gerçekleştirmek yönünde teşvik etti. Bitcoin altyapısı üzerinde kurulan bu kripto para birimi sistemlerine genel olarak *alternative coin* / *altcoin* denmektedir. İlk *altcoin*, merkezî olmayan DNS sistemini gerçekleştirmek üzere *Namecoin* adıyla Nisan 2011’de duyuruldu. Bunu, aynı yılın Ekim ayında SHA-256 *hash* fonksiyonu yerine *scrypt* kullanan *Litecoin* izledi. Ardından 2012 yılında, iş kanıtı olarak *proof-of-work*’un hibrit bir modeli olan *Proof of Stake*’i kullanan *Peercoin* duyuruldu.

Metacoin olarak isimlendirilen ve bir kısmı Bitcoin *blockchain* yapısını kullanan ve bir kısmı da *ledger* (defterikebir) denilen kendi yapılarına sahip olan sistemler de ortaya çıkmıştır. Bu sistemler, birer kripto para birimi olmakla beraber dijital varlık ve dijital sözleşme gibi yeni uygulamalar sunmaktadır. Mesela 2012 yılında duyurulan *Ripple*, hem dijital para birimidir hem de finansal elektronik bir ağ olarak faaliyette bulunmaktadır. 2013 yılında önerilen ve 2015 yılında faaliyete geçen *Ethereum* kendi blokzincirine sahip ve akıllı sözleşmeler (*smart contracts*) oluşturmayı sağlayan bir sistemdir.

Bitcoin’in sağladığı gizlilik, zamanla ticari faaliyetlerini gizlemek isteyen kişilerin de dikkatini çekti. Bitcoin sisteminde para hareketlerin izlenmesi ve takma adlardan (*pseudonym*) gerçek kişilere erişilmesi çok kolay değildi. Bu özelliği suiistimal eden ilk organizasyon olan, kendisi yasadışı bir eylemde bulunmamakla birlikte, yasadışı ve yasak uyuşturucu ve ilaçların ticareti için bir platform sunan *Silk Road* adlı İnternet sitesi, para olarak bitcoin kabul ediyordu. 2013 yılında FBI tarafından kapatılıncaya kadar, *Silk Road*, bu tür faaliyetlerine devam etti. *Silk Road* olayı, merkezî bir yönetim ve denetime sahip olmayan kripto para birimlerin sunduğu hizmetlerin yasadışı işlerde kullanılabileceğini gösterdi⁵⁸.

Kripto para birimi tarihinde bir başka önemli olay, Tokyo merkezli en büyük Bitcoin borsası olan ve 2014 yılında Bitcoin para hareketlerinin % 70’ini tek başına gerçekleştirdiği tahmin edilen *Mt. Gox* adlı platformun kendisine ve müşterilerine ait

⁵⁸ Conrad Barski, Chris Wilmer, **Bitcoin For The Befuddled**, San Francisco: no starch press, 2015, s. 124.

850 bin bitcoin'in çalınmasıdır. Böyle büyük bir hırsızlık olayı üzerine şirket 2014 Şubat ayında iflasını istedi ve Nisan ayında da tasfiye edildi⁵⁹.

Bugüne kadar⁶⁰ 1583 kripto para birimi ve bunlarla ilgili 9685 market duyurusu yapılmış bulunmaktadır. Bu marketlerin toplam hacmi 326,776,640,002 ABD dolarıdır⁶¹.

§3. Kripto Para Birimlerinin Ortak Özellikleri

Kısa sürede duyurulan kripto para birimi sayısının çokluğu göz önüne alındığında, bu sistemlerin sahip olduğu özelliklerin tam bir dökümünü yapmak mümkün olmasa da onları ortak olarak niteleyen bazı temel özelliklerin varlığından bahsedilebilir. Bu bölümde bu ortak özellikler arasında en önemli olanları açıklanacaktır.

A. Açık Kaynak Kod

Kripto para birimi sistemlerinin neredeyse tamamı açık kaynak kodlu⁶² yazılımlardır. Arkasında kâr amacı güden herhangi bir ticari kuruluş olmayan Bitcoin açık kaynak kodlu bir yazılım sistemi olduğu gibi, bir şirketin desteğinde geliştirilen Zcash de açık kaynak kodlu bir yazılımdan türetilmiştir. İsteyen kişi veya gruplar bu yazılımların kaynak kodlarını kendi bilgisayarlarına indirip, istedikleri fonksiyonları yerine getiren kendi kripto para birimlerini oluşturabilirler. Kripto para birimlerinin açık kaynak kodlu bir yapıyı benimsemelerindeki temel amacın, açık kaynak kodlu yazılım olmanın avantajlarından yararlanmak olduğu söylenebilir⁶³.

Açık kaynak kodlu yazılım, en başta yazılımı oluşturan kaynak kodlarının, başkalarının incelemesine açık olmasını ifade eder. Bunun yanında kaynak kodunun

⁵⁹ Halaburda ve Sarvary, **a.g.e.**, s. 150.

⁶⁰ 25 Mart 2018 tarihi itibarıyla.

⁶¹ <https://coinmarketcap.com/coins/views/all>, Erişim tarihi: 25 Mart 2018.

⁶² **Kaynak kodu** (*İng.* Source code) yazılımın bir insan tarafından düz metin olarak (başka bir deyişle bir insan tarafından anlaşılabilen harf ve rakamlarla) yazılmış biçimidir. **The Linux Information Project**, http://www.linfo.org/source_code.html, Erişim tarihi: 26 Mart 2018.

⁶³ Peter Van Valkenburgh, **What is “open source” and why is it important for cryptocurrency and open blockchain projects?**, <https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects>, Erişim tarihi: 26 Mart 2018.

değiştirilip başka bir yazılım olarak sunulmasına veya bir yazılım bileşeni olarak kullanılmasına imkân verir. Yazılımı kullanım amacı kişisel veya ticari olabilir. Açık kaynak kodlu yazılımların paylaşımına açık olması esastır⁶⁴. Açık kaynak yazılımlar, genelde gönüllü bağışlarla varlığı sürdüren topluluklar tarafından geliştirildiği için, bu yazılımlarda, ticari kaygılar yerine, kullanıcı beklentilerini ve ihtiyaçlarını daha iyi karşılayan özelliklere öncelik verilir. Açık kaynak kodu yazılımlar, risk değerlendirmesine göre yatırım yapmak isteyen girişim sahipleri yerine, benimsenip benimsenmeyeceği belli olmayan kripto para birimi gibi sistemlere serbest katkıda bulunmayı isteyenleri cezbedeceği aşîkârdır.

Yukarıda bahsedilen *Cypherpunk* grubunun kriptografiyi bilgisayar ve internete uygulamasıyla başlatmış olduğu geniş tabanlı açık kaynaklı kriptografik araştırmaların bir sonucu olan Bitcoin'in açık kaynak kodlu yapısı, diğer kripto para birimleri için de bir model olmuştur⁶⁵. *Bitcoin Core* denilen Bitcoin temel referans yazılımı, 15.000 tekil kod yardımını ve birbiriyle herhangi bir bağı olmayan 450'nin üzerinde bağımsız programcının geliştirdiği yazılım bütününden oluşmaktadır. Birçok *altcoin*, bu referans yazılım kaynak kodunun başka geliştirici gruplar tarafından alınması ve "çatal/fork" denilen bir ayrışma ile yeni bir kripto para birimi olacak şekilde değiştirilmesiyle oluşturulmuştur⁶⁶.

B. Kriptografi

Kripto para birimi sistemlerinin en belirgin özelliği, kriptografik tekniklerin yoğun olarak kullanılmasıdır. Bu kriptografik teknikler, para birimlerinin üretilmesinde, kullanıcı hesapları arası para hareketlerinde ve bütün bu işlemlerin kaydedildiği *blockchain* veya *ledger* denilen veri yapılarının güvenliklerinin sağlanmasında kullanılmaktadır.

Kriptografi veya kriptoloji (*cryptography*, *cryptology*; *şifreleme bilimi*), hasım, rakip, muhalif başka bir deyişle istenmeyen üçüncü kişilerin veya tarafların

⁶⁴ <https://opensource.org/osd>, Erişim tarihi: 26 Mart 2018.

⁶⁵ Oliver Dale, **A History of Cryptography and the Rise of the CypherPunks**, <https://blockonomi.com/cryptography-cypherpunks/>, Erişim tarihi: 26 Mart 2018.

⁶⁶ Van Valkenburgh, **a.g.y.**

bulunduğu ortam ve kanallarda güvenli iletişim tekniklerinin uygulanmasını ve incelenmesini konu alan bilim dalıdır^{67,68}.

İncelememizde kriptografi ile ilgili açıklamalar, kripto para birimi sistemlerinde en çok kullanılan dört teknikle sınırlandırılacaktır: Bunlar, *hash* fonksiyonları, simetrik anahtar şifreleme, açık anahtar şifreleme ve onun bir uygulaması olan dijital imza teknikleridir.

1. Hash Fonksiyonu

Hash fonksiyonu, rastgele büyüklükteki bir veriyi girdi olarak alan ve sabit uzunlukta bir bit-dizisi olan *hash* (özet) değeri çıktısı üreten bir algoritmadır⁶⁹. Hash fonksiyonu deterministiktir, başka bir deyişle aynı girdi her zaman aynı *hash* değerini verir. Normal *hash* fonksiyonları farklı girdiler için aynı *hash* değeri üretebilirler fakat *hash* değerlerinin düzenli bir dağılım göstermesi beklenir. Güvenli veya kriptografik *hash* fonksiyonlarının farklı girdiler için aynı *hash* değeri üretmemeleri için, normal *hash* fonksiyonlarından daha sıkı şartlara tabidirler. Bunlar⁷⁰;

(1) Tek yönlülük (ters görüntüye dayanıklılık, *preimage resistance*): Bir *hash* değeri verildiğinde, bundan yola çıkarak girdiye erişilememelidir.

(2) Zayıf çakışmaya dayanıklılık (*weak collision resistance*): Verilen bir girdi için aynı *hash* değerine sahip farklı bir girdi bulmak, gereken işlem gücü bakımından makul ve mümkün olmamalıdır.

(3) Güçlü çakışmaya dayanıklılık (*strong collision resistance*): Aynı *hash* değerine sahip iki farklı girdi bulmak, gereken işlem gücü bakımından mümkün olmamalıdır.

⁶⁷ Franco, Pedro Franco, **Understanding Bitcoin Cryptography, engineering, and economics**, İngiltere: Wiley, 2015, s. 51.

⁶⁸ TSE Bilişim Terimleri Sözlüğünde kriptografi, “Şifreleme bilim dalı; verinin anlamsal içeriğini gizlemek, yetkisiz kullanımı önlemek veya tespit edilemeyen değişiklikleri engellemek için veri dönüşümüne ait prensipler, araçlar ve metotları kapsayan disiplin” olarak tanımlanmıştır. (TSE Bilişim Terimleri Sözlüğü, *cryptography* maddesi.)

⁶⁹ A.g.e., s. 95.

⁷⁰ A.g.e., s. 96.

MD4 (*Message Digest-4*), MD5 (*Message Digest-5*), SHA-1 (*Secure Hash Algorithm-1*) ve SHA256 (*Secure Hash Algorithm-256*) bilinen ve kullanılan kriptografik *hash* fonksiyonlarından bazılarıdır.

MD4'ün çakışmaya dayanıklı olmadığı anlaşıldığından kullanımı terkedilmiştir. Türkiye'de dijital delillerin bütünlüğünün ispatında yaygın olarak kullanılan ve MD4'ün geliştirilmiş bir sürümü olan MD5'in de çakışmaya dayanıklı olmadığı gösterilmiş ve kullanımının terk edilmesi tavsiye edilmiştir⁷¹.

SHA-1, 160 bit'lik bir *hash* fonksiyonudur ve bir girdiye uygulandığında 40 basamaklı onaltılık tabanda bir *hash* sayısı üretir. Google, SHA-1 hash fonksiyonunu kullanarak bir çakışma üretebildiğini açıklamıştır⁷². Bu nedenle SHA-1 fonksiyonu kullanan yazılımlarda, bu yapı değiştirilmekte ve SHA-256 gibi daha güvenilir ve gelişmiş *hash* fonksiyonları kullanılmaktadır.

SHA-256, SHA-2 kümesine ait 256 bit'lik bir *hash* fonksiyonudur ve SHA-1'den daha güvenlidir. SHA-256, 64 basamaklı onaltılık tabanda bir *hash* sayısı üretir. Bitcoin sisteminde, iş kanıtı (*proof-of-work*) ve Bitcoin adreslerin oluşturulmasında SHA-256 fonksiyonu kullanılmaktadır⁷³.

Bitcoin sisteminde kullanılan bir başka *hash* fonksiyonu olan RIPEMD160, açık anahtar şifreleme tekniğiyle MD4 temeli üzerine tasarlanmış ve SHA-1 *hash* fonksiyonuyla benzer bir performansa sahip RIPEMD *hash* fonksiyonunun 160 bit'lik geliştirilmiş sürümüdür. SHA-1 ve SHA-2'nin ABD Ulusal Güvenlik Ajansı (NSA) tarafından tasarlanmış olmalarına karşılık RIPEMD160 açık akademik çevrelerce tasarlanmıştır ve üzerinde başkaları tarafından kullanımını kısıtlayan bir patent hakkı bulunmamaktadır⁷⁴.

⁷¹ Bkz. Vulnerability Note VU#836068, **MD5 vulnerable to collision attacks**, <https://www.kb.cert.org/vuls/id/836068>, Erişim tarihi: 29 Mart 2018.

⁷² **The SHA1 hash function is now completely unsafe**, <https://www.computerworld.com/article/3173616/security/the-sha1-hash-function-is-now-completely-unsafe.html>, Erişim tarihi: 28 Mart 2018. (Not: Tek bir bilgisayar işlemcisi (CPU) ile 6500 yıl sürecek bu işlem için, google'un devasa bilgi işlem gücü kullanılmıştır.)

⁷³ Franco, **a.g.e.**, s. 96.

⁷⁴ Barski, Wilmer, **a.g.e.**, s. 140.

2. Simetrik-Anahtar Şifreleme

Simetrik-anahtar şifreleme (*symmetric-key encryption*), açık metinlerin şifrlenmesinde veya şifreli metinlerin deşifre edilmesinde aynı şifreleme anahtarının kullanıldığı şifreleme tekniğidir⁷⁵. Şifreleme ve deşifre etme anahtarları birbirinden biraz farklılaştırılmış da olabilirler. Simetrik anahtar, iletişimde bulunmak isteyen taraflar için ortak gizli anahtar rolünü ifa ettiği için, iletişime geçilmeden önce güvenli bir kanaldan paylaşılması gerekmektedir. Fakat bu güvenli kanal, internet üzerinden gerçekleştirilen elektronik ticarete her zaman mümkün olmayabilmektedir. *Man-In-The-Middle attack* (Araya giren kişi saldırısı veya ortadaki adam saldırısı) denilen bir saldırıyla⁷⁶, istenmeyen kişiler, taraflar arasındaki iletişim ağına sızarak şifreleme anahtarını ele geçirebilir ve bütün iletişimin içeriğini bu anahtar ile deşifre edebilirler. Bu nedenle simetrik şifreleme tekniği, güvenilir bir kanaldan ortak anahtarın paylaşılmasının mümkün olduğu durumlarda kullanılmaktadır⁷⁷.

3. Açık Anahtar Şifreleme

Açık anahtar şifreleme (*public key encryption, public key cryptography*) veya diğer adıyla asimetrik anahtar şifreleme (*asymmetric key encryption*), 1970'li yıllarda geliştirilen ve simetrik anahtar şifreleme tekniğinin zayıflığını gidermek için geliştirilmiş bir şifreleme tekniğidir⁷⁸. Açık anahtar şifrelemede, tek bir şifre yerine ortak-gizli anahtar çifti denilen mesajı şifreleyen anahtar (gizli/özel anahtar, *private key*) ile deşifre eden anahtar (ortak/açık anahtar, *public key*) farklıdır. Bu teknikte sadece gizli anahtarın (*private key*) saklanması gerekmektedir. İnternet üzerinden güvenli iletişim için kullanılan SSL ve TLS protokollerinde açık anahtar şifreleme tekniği kullanılmaktadır⁷⁹.

Açık anahtar şifreleme tekniğinde, iletişimde bulunmak isteyen A tarafı, B tarafının açık anahtarı ile şifrelenmiş rastgele bir simetrik anahtar içeren mesajı B'ye gönderir. B, kendi açık anahtarı ile şifrelenmiş mesajı gizli anahtarı ile deşifre eder

⁷⁵ Franco, **a.g.e.**, s. 125.

⁷⁶ Keith M. Martin, **Everyday Cryptography**, 2.b., İngiltere: Oxford University Press, 2017, s. 420.

⁷⁷ Franco, **a.g.e.**, s. 53.

⁷⁸ Barski, Wilmer, **a.g.e.**, s. 133.

⁷⁹ Franco, **a.g.e.**, s. 53.

ve böylece hem kendisinin hem de A'nın bildiği bu simetrik anahtarı kullanarak B ile güvenli iletişimde bulunabilir.

Açık anahtar şifreleme tekniği ile sadece simetrik anahtar üretilmektedir ve iletişimin tamamı için açık anahtar şifreleme tekniği kullanılmamaktadır. Bunun sebebi, açık anahtar şifrelemenin, simetrik anahtar şifrelemeye göre birkaç kat daha yavaş olması ve mesaj boyutunun daha büyük olmasıdır⁸⁰.

4. Dijital İmza

Açık anahtar şifrelemenin bir başka uygulaması da dijital imzalıdır. Dijital imza, el ile atılan imza gibi şu üç fonksiyonu yerine getirmektedir⁸¹: (1) İlgili mesajın imzacı tarafa ait olduğunu doğrulamak (kimlik doğrulama, *authentication*), (2) mesajın bütünlüğünü sağlamak (*integrity*), başka bir deyişle mesaja bir müdahalenin yapılmadığını garantilemek ve (3) mesajın imzacı tarafından gönderilmediği iddiasını çürütmek (inkâr edilemezlik, *non-repudiation*).

Dijital imzalama süreci şu şekilde gerçekleşir: A tarafı, B'ye göndereceği mesajın *hash*'ini bulur ve bunu gizli anahtarı (*private key*) ile şifreler. A tarafı, mesajın açık halini, dijital imzayı ve açık anahtarını (*public key*) B tarafına gönderir. B, A'nın gönderdiği dijital imzayı A'nın açık anahtarı ile deşifre eder. Mesajın *hash*'ini alır ve dijital imzanın deşifre edilmesiyle elde ettiği *hash* ile karşılaştırır. Eğer iki *hash* eşit ise, mesajın A tarafından gönderildiği ve mesaja bir müdahalenin olmadığı ispatlanmış olur. Ayrıca A, bu mesajın kendisi tarafından gönderilmediğini iddia edemez.

Bitcoin sisteminde, para transferinin gerçekleşmesi için ECDSA (*Elliptic Curve Digital Signature Algorithm*) ile oluşturulmuş dijital imza kullanılmaktadır⁸². Günümüzde en çok kullanılan dijital imza, RSA şemasıdır. *Schnorr*, *Elgamal* ve *DSA* diğer kullanılan dijital imza şemalarıdır⁸³.

⁸⁰ Martin, **a.g.e.**, s. 240.

⁸¹ Franco, **a.g.e.**, s. 57.

⁸² Barski, Wilmer, **a.g.e.**, s. 146.

⁸³ Franco, **a.g.e.**, s. 59.

C. Merkezsizlik

Geleneksel para birimleri, merkez bankaları veya aynı fonksiyonu yerine getiren finansal kuruluşlar tarafından yönetilir ve yasal olarak korunurken, güvenilir üçüncü taraf/aracı yokluğu temelinde tasarlanan kripto para birimlerinde herhangi bir merkezî yönetim ve denetim birimi yoktur. Bu nedenle bu sistemlere merkezî olmayan (*decentralized*) sistemler denilmektedir.

Kripto para birimi sistemi ağları, güvensiz bir iletişim ağı olan internet üzerinden herkesin erişilebildiği ve istediği zaman girip çıkabildiği eşler arası ağ (*peer to peer, p2p*) yapısındadırlar. Bu ağ topolojisinde, özel yetkiye sahip olmayan ve her bilgisayarın eşit olduğu eşler (*peers*) bulunur. Kripto para birimlerinin böyle bir yapıyı benimsemeleri, bir ağ topolojisi seçimi olmaktan öte, merkezî olmamanın bir gereğidir. Çünkü ancak düz, birbirinin eşiti olan düğümlerin (*node*) bulunduğu bir uzlaşma *p2p* ağı, merkezî olmayan bir sistemin işlemlerini sağlayabilir⁸⁴.

Kripto para birimi sistemlerinin *p2p* ağ yapısından kaynaklanan denetimsiz ağa giriş ve çıkıştan dolayı, ağda dürüst davranıp sistemin sağlıklı işlemlerini sağlayanlar yanında, dürüst davranmayan veya sistemi kötü amaçları için kullanmak isteyenler de bulunabilmektedir. Herkesin eşit olduğu bir sistemde, merkezî bir otorite olmadığı için, kararlar uzlaşma yoluyla alınmak zorundadır. Fakat yanlış kararlar alınması için çabalayanların da bulunduğu böyle bir toplulukta sistemin sağlıklı işlemlerini sağlayacak kararlar üzerinde uzlaşma nasıl sağlanacaktır? Bu sorun, bilgisayar bilimlerinde uzun yıllar çözüm bekleyen uzlaşmaya dayalı dağıtık bilgisayar sistemlerinin, bir veya birden fazla bileşenlerinin çalışmaması veya hatalı çalışması durumunda, sistemin güvenilirliğinin nasıl sağlanacağıyla ilgilidir. Hatalı çalışan bir bileşen, sistemin farklı birimlerine yanıltıcı mesajlar göndererek sistemi kararsızlığa düşürebilir veya kötü bir karar almaya yönlendirebilir.

⁸⁴ Andreas M. Antonopoulos, **Mastering Bitcoin Programming The Open Blockchain**, 2. b., ABD: O'Reilly, 2017, s. 171.

Bizanslı Hata Toleransı (*Byzantine Fault Tolerance Problem*) veya Bizanslı Generaller Sorunu⁸⁵ (*Byzantine Generals' Problem*) olarak bilinen bu sorun, kısaca şöyle ifade edilmektedir: Bizanslı generaller, ordularıyla farklı cephelerden kuşattıkları bir şehri, alacakları ortak bir kararla ele geçirmek istemektedirler. Generaller arasında iletişim ulaklar aracılığıyla yapılmaktadır. Şehrin bir süre gözetlenmesinin ardından ortak bir hareket planına karar verilecektir. Fakat bazı generaller hain olabilir ve dürüst generallerin ortak bir karara varmasını önleyebilirler. Dürüst generaller, şu iki durumu garanti eden bir algoritmaya sahip olmak zorundadırlar: (1) Bütün dürüst generaller aynı hareket planına karar verirler fakat hain generaller çelişkili kararlar verebilirler. Hain generaller doğru veya yanlış nasıl karar verirlerse versinler, algoritma birinci şartı garanti etmeli ve ayrıca (2) az sayıdaki hain general, dürüst generallerin kötü bir planı benimsemesine sebep olmamalıdır. Bu şekilde ortaya konulan Bizanslı Generaller Sorunu, dürüst generallerin üçte iki çoğunluğunu sağlamadığı durumlarda çözümsüzdür.

Kripto para birimi sistemleri gibi dağıtık bir bilgisayar sisteminde uzlaşma sorunu, ilk olarak Nakamoto tarafından geliştirilen *blockchain* mimarisiyle çözülmüştür. Nakamoto uzlaşması (*Nakamoto consensus*) da denilen bu çözümde, her biri tekil olarak doğrulanmış para hareketlerinden (*transaction*) oluşmuş bir kümeyi içeren bloklar, büyük bir bilgi işlem gücü harcanarak sağlanmış iş kanıtı (*work-of-proof*) ve ağda bulunan diğer düğümler tarafından bu iş kanıtının onaylaması üzerine varılan uzlaşmayla blokzincirine (*blockchain*) eklenmektedir⁸⁶.

D. Anonimlik

Kripto para birimi sistemlerinde anonimlik, kullanıcıların gerçek kimliklerini açıklamak zorunda kalmadan sisteme girebilmelerini ve para hareketlerini gerçekleştirebilmelerini ifade eder⁸⁷. Anonimlik, sistemde tutulan kayıtlardan yola çıkılarak işlemi gerçekleştiren kişilerin gerçek kimliklerine ulaşılammayı da kapsar. Kripto para birimlerinin ortaya çıkışında öncülük yapan *Cypherpunk* hareketinin mahremiyetin korunması ve kriptografinin bu amaçla kullanılması ilgili yukarıda

⁸⁵ Leslie Lamport, Robert Shostak ve Marshall Pease, "The Byzantine Generals Problem", **ACM Transactions on Programming Languages and Systems (TOPLAS)**, C. 4/3, Temmuz 1982, s. 383, <http://lamport.azurewebsites.net/pubs/byz.pdf>, Erişim tarihi: 30 Mart 2018.

⁸⁶ Antonopoulos, **a.g.e.**, s. 217.

⁸⁷ Franco, **a.g.e.**, s. 161.

açıklanan görüşleri dikkate alındığında, anonimliğin bu sistemlerin temel özellikleri arasında olması, beklenen bir durumdur.

Geleneksel para birimlerinde, nakit işlemler haricindeki para hareketlerinin çoğunluğu banka ve finansal kuruluşlar aracılığıyla gerçekleşmektedir. Bu kuruluşlar, yasal düzenlemeler gereği, müşterilerine ait kimlik bilgilerini tutmak zorundadırlar. Halbuki kripto para birimi sistemlerinde para hareketleri doğrudan taraflar arasında gerçekleşmektedir. Bu işlemler için, birer açık ve gizli anahtar (*public/private key*) çiftine sahip olmak yeterlidir. Cüzdan (*wallet*) denilen uygulamalar veya ücretsiz cüzdan hizmeti veren dijital platformlar sayesinde, kullanıcılar istediği kadar anahtar çifti edinebilirler. Hatta anonimlik ve güvenlik açısından birden fazla anahtar çiftine sahip olunması da önerilmektedir⁸⁸. Açık anahtar şifreleme teknikleriyle üretilen bu anahtarlar, karışık harf ve rakamlardan oluşurlar ve sahiplerine ait herhangi bir bilgi içermezler. Bu anahtarlarla gerçekleşen para hareketlerinde taraflarla ilgili kayıt altına alınan işlemlerde başka bilgiler yer almaz.

Kripto para birimlerinin sağladığı anonimlik görece bir mahremiyet sağlamaktadır. Bitcoin gibi sistemlerde kullanıcıların para hareketlerinde kullandığı adresler, daha çok takma ad (*pseudonym*) anonimliği sağlamaktadır⁸⁹. Kişi ile kripto para birimi ağında kullandığı adresi arasında doğrudan bir ilişki kurulamaz. Fakat kişinin hesap adresini kendisinin ifşa etmesi veya kimlik hırsızlığına maruz kalması gibi kullanıcı ile hesap adresi arasında bir bağ ortaya çıktığında, anonimlik ortadan kalkmakta ve kişinin hesap hareketleri izlenebilmektedir.

Cüzdan hizmeti platformlarından yararlanan kullanıcıların, platforma kayıt olurken verdikleri bilgiler, kişi ile hesap adresi arasında bağ kurabilmeyi mümkün kılmakta, bu da anonimliği zedelemektedir. Bunun dışında, para hareketlerinin gerçekleştiği bilgisayara ait internet trafiğinin izlenmesi yoluyla da para transferinde bulunan kişi ile kontrol ettiği anahtar çiftleri arasında ilişki kurulabilmektedir⁹⁰.

Kripto para sistemlerinin bir parçası olmamakla beraber bazı platformlar, belli bir ücret karşılığı, hesap hareketlerinin izlenmesini zorlaştırmak için karıştırma

⁸⁸ Antonopoulos, **a.g.e.**, s. 274.

⁸⁹ Farrell, **a.g.m.**, s. 4.

⁹⁰ Fergal Reid, Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System," **2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing**, Boston, ABD, 2011, s. 9.

hizmeti (*mixing service*) vermektedirler. Bu karıştırma hizmetinden yararlanan kişinin hesabından başka kişilerin hesabına ve onların hesaplarından da tekrar kişinin yeni hesabına para transferi gerçekleştirerek bir karartma yapılabilmekte ve böylece eski hesap adresiyle yenisi arasındaki ilişkiyi kopartabilmektedir⁹¹.

Mahremiyetin ön planda tutulduğu birçok kripto para birimi duyurusu yapılmıştır. Bunlardan birisi olan *Monero* kripto para birimi sisteminde hesap adresi olarak görüntüleme anahtarı⁹² (*view key*) ve harcama anahtarı (*spend key*) denilen iki anahtar bulunur. Kullanıcı isterse “view key” anahtarını başkalarıyla paylaşarak bu adrese yapılan transferleri izlenmesini sağlayabilir. Aksi takdirde işlem anında otomatik olarak üretilen gizli adrese⁹³ (*stealth address*) yapılan para transferlerini ancak işlem tarafları görebilir, üçüncü kişiler göremez.

Bitcoin sistemine gerçek kriptografik anonimliği eklemek isteyen bazı kriptografi uzmanı akademisyenler, Bitcoin topluluğundan ayrılıp geliştirdikleri *Zerocoin*’de gerçek kriptografik anonimliği sağladıklarını iddia etmektedir⁹⁴.

Son yıllarda geliştirilen kripto para birimlerinde mahremiyetin ön plana çıkarılması, kullanıcıların bu konudaki isteklerini yansıtsa da, anonimlik yukarıda açıklanan *Silk Road* olayında olduğu gibi, yasadışı hareketlerinin izlenmesini perdelemek isteyenlerce istismar edilebilmektedir. Bu durum, kripto para birimlerinin geleceğini belirsiz kılmaktadır.

E. Diğer Ortak Özellikler

Yukarıda açıklananlar dışında kripto para birimi sistemlerinin paylaştığı birçok teknik özellik daha bulunmaktadır. Kripto para birimi sistemlerinin kendi çevrelerinde oluşturduğu ekosistemler, kullanıcıların erişimine açık olan blokzinciri (*blockchain*) mimarisi, madencilik, para arzı ve hareketlerin geri alınamazlığı bunlardan bazılarıdır. Bu özelliklere dair açıklamalar, Bitcoin sisteminin detaylı olarak ele alındığı kısımda ilgili oldukları başlıklar altında yapılacaktır.

⁹¹ Franco, **a.g.e.**, s. 212.

⁹² <https://getmonero.org/resources/moneropedia/viewkey.html>, Erişim tarihi: 31 Mart 2018.

⁹³ <https://getmonero.org/resources/moneropedia/stealthaddress.html>, Erişim tarihi: 31 Mart 2018.

⁹⁴ https://anoncoin.net/Anonymity_of_cryptocurrencies/, Erişim tarihi: 31 Mart 2018.



§4. Kripto Para Birimleri İçin Hukuksal Düzenleme Arayışları

I. Hukuksal Düzenleme İhtiyacı

Günümüzde kripto para birimlerinin işleyişlerini düzenleyen ne uluslararası ne de ulusal bir hukuki düzenleme mevcuttur. Kripto para birimleri için düzenleyici kuralların olmaması, onlara varlıklarını otonom olarak sürdürebildikleri alanlar sunmakta ve hukuksal düzenlemelerden bağışık özerk yapılarımış algısı oluşturmaktadır. Fakat bu durum geçicidir, çünkü hem uluslararası kuruluşlar hem de birçok devletin ilgili kurumları, bu yapılara ilişkin hukuksal düzenleme arayışlarına devam etmektedir.

Kripto para birimlerine ilişkin hukuksal düzenleme arayışlarının temelinde, bu teknolojik yeniliğin hem ulusal hem de uluslararası boyutta yarattığı etkilerin toplumsal, siyasal, ekonomik ve finansal hayata sağlıklı yansımaları sağlama ve kötüye kullanımına engel olma düşüncesinin yattığı söylenebilir. Zira kripto para birimleri merkezî olmayan, kamu otoritesi ve kontrolü dışında yer alan kişiler veya kuruluşlar tarafından varlıkları sürdürülen ve isteyen herkesin kimliğini gizleyerek katılabildiği ve herhangi bir engel ve denetime maruz kalmadan para hareketleri gerçekleştirebildiği sistemlerdir. Bu özellikler, uluslararası toplumun hassas olduğu, suçtan kaynaklanan malvarlığı değerlerinin aklanması, uyuşturucu ve uyarıcı madde ticareti, yasadışı bahis, çocuk pornografisi, vergi kaçakçılığı ve terörizmin finansmanı gibi birçok farklı yasadışı faaliyetin gerçekleştirilebilmesi için uygun ortamlar sağlamaktadır⁹⁵.

Kripto para birimlerinin getirdiği görece anonimlik, para hareketlerinde banka gibi finansal araçların olmaması, bu paraların ne amaçla harcandığını veya nerelere ve kimlere aktarıldığını saptamayı zorlaştırmaktadır. Bunun yanında piyasada bulunan para hacmi, merkez bankaları veya benzeri kurumların belirlediği politikalar doğrultusunda kontrol edilirken, kripto para birimi kullanımı bu düzen için de tehdit oluşturmaktadır. Çünkü kripto para birimlerinde para ihraçları, merkezî

⁹⁵ Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, **Bitcoin and Cryptocurrency Technologies**, Princeton University Press, 2016, s. 204.

kurumlarca belirlenen hedeflere göre değil, tamamen piyasanın arz ve talep dengesine göre belirlenmektedir⁹⁶.

Kripto para birimlerinin yeni vergi cenneti olmaya doğru evrildiklerini belirten bir yazar, geleneksel vergi kaçırma yönelik önlemlerin Bitcoin gibi kripto para birimi sistemlerinde işe yaramayacağını öne sürmektedir⁹⁷. Yazar, kripto para birimlerinin, geleneksel vergi cennetlerinin en önemli iki özelliği olan, işlemin gerçekleştiği yerde yargılama yetkisinin olmaması ve hesap sahiplerinin anonim olması özelliklerine sahip olduğunu ifade etmekte ve ayrıca işlemlerin, finansal araçlar dışında gerçekleşmekte olduklarını belirtmektedir⁹⁸. Bu özellikler, kripto para birimlerinin vergi cenneti olmalarını destekleyecek hususlardır. Yazar, ayrıca Bitcoin hesaplarının çoğunun yatırım hesabı olduğunu ve bunun da vergi kaçırma işaret olabileceğini iddia etmektedir⁹⁹. Kripto para birimlerinin vergi kaçırma alet edilmesinin engellenmesi için hesap sahiplerinin cüzdanlarındaki gizli fonların bulunmasına imkân verecek mekanizmaların geliştirilmesi gerektiğini¹⁰⁰ belirten yazar, her ne kadar diğer geleneksel para birimleri gibi kötüye kullanılma potansiyeli olsa da beraberlerinde getirdikleri önemli yararlar dolayısıyla kripto para birimlerine karşı yasaklayıcı yöntemlerin doğru olmadığını ifade etmektedir¹⁰¹.

Kripto para birimleriyle ilgili hukuksal düzenleme arayışlarında iki önemli zorluk dikkat çekmektedir. Bu zorlukların ilki, bu sistemlerin kullandığı blokzincirini ve benzeri yapıların vadettiği teknolojik yenilik alanının gelişimini sekteye uğratacak sınırlamalar yerine, sağlıklı bir yol izlenebilmesini sağlayacak kurallar ortaya koymak kolay gözükmemektedir. İkinci olarak, hukuki uyumsuzluklar söz konusu olduğunda, küresel uygulama alanı genişliğine sahip, merkezî olmayan, bir otoriteye bağlı olmayan ve kullanıcıların anonim olarak katılabildikleri bu sistemlerde yükümlülük altına alınacak muhatap bulmak kolay değildir¹⁰².

⁹⁶ A.g.m.

⁹⁷ Omri Marian, "Kripto Para Birimi Üstün Vergi Cenneti mi?", Çeviren: Sedef Pelin Gürlek Keleş, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası (İÜHFM)**, C. LXXIV/2, 2016, s. 927.

⁹⁸ A.g.m., s. 923.

⁹⁹ A.g.m., s. 925.

¹⁰⁰ A.g.m., s. 926.

¹⁰¹ A.g.m., s. 928.

¹⁰² IMF, **a.g.e.**, s. 25.

Bununla birlikte, kripto para birimleri için hukuksal düzenlemelerin yokluğu, onların varlıklarını sürdürmelerini de tehdit etmektedir. Bu sistemlerin geniş kesimlerce kabulü, biraz daha istikrarlı yapılara kavuşmalarına ve mevcut hukuki belirsizlikten kurtulmalarına bağlı görünmektedir¹⁰³.

II. Tavsiyeler

Kripto para birimleri için hukuksal düzenlemelere ilişkin tavsiyelere bakıldığında, sert ve yasaklayıcı kuralların teknolojik gelişimi sekteye uğratacağı ve bu sistemlerin yasal kullanımını kısıtlayacağı fakat yasadışı kullanımını çok fazla engellemeyeceği belirtilmiştir¹⁰⁴.

IMF, yayımladığı bilgi notunda, yukarıda belirtilen görüşe paralel olarak, kripto para birimleriyle ilgili yapılacak düzenlemelerde, bu sistemlerin ortaya çıkardığı risk ve istismar tehlikelerini önleme ile teknolojik inovasyonu bastırarak derecede aşırı sınırlamalar arasında bir denge kurulması gerektiği tavsiyesinde bulunmaktadır¹⁰⁵.

Kripto para birimlerine ilişkin düzenlemeler, uluslararası kuruluşlardan ve ulusal düzeyde Devletlerin ilgili kurumlarından beklenmekle beraber, bu düzenlemelerin bir bölümünün, piyasanın kendi kendini düzenlemesi şeklinde özel sektör tarafından getirilmesi de önerilmektedir. Mesela Bitcoin'in kullanımını dünya çapında standarda kavuşturmak, geliştirmek ve teşvik etmek olan Bitcoin Vakfı (*Bitcoin Foundation*) gibi kuruluşlar bu tür düzenlemeler için aracı olabilir, sistemin çalışmasının dayandığı protokollerin yasal çerçevelere uyumunu gözetebilirler¹⁰⁶.

Politikacıların Bitcoin'in yasaklanması yönündeki baskılara direnmeleri gerektiğini savunan bir başka yazar, Bitcoin'in merkezî olmayan yapısı nedeniyle yasaklamasının mümkün de olmadığını iddia etmektedir¹⁰⁷. Yazar, yasaklamanın Bitcoin kullanıcılarını, yasadışı faaliyetlerden alıkoymayacağını belirtmekte ve

¹⁰³ A.g.m., s. 5; Farrell, a.g.m., s. 6.

¹⁰⁴ Jerry Brito, Andrea Castillo, **Bitcoin: A Primer for Policymakers**, Mercatus Center, 2013, s. 34.

¹⁰⁵ IMF, a.g.e., s. 7; De Filippi, a.g.m., s. 1.

¹⁰⁶ A.g.m., s. 8.

¹⁰⁷ Nikolei M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation", **Loyola Consumer Law Review**, 2012, C. 25/1, s. 167.

aslında blokzincirinin soruşturma makamlarına yasadışı faaliyetleri araştırmak için yeterli bilgi sağladığını öne sürmektedir¹⁰⁸. Yazarın, Bitcoin'in yasaklanmasına karşı öne sürdüğü bir başka gerekçe ise, Bitcoin'in temel yasalarla desteklenmiş özgür işleyişinin, yeni iş alanlarına, ekonomik büyümeye ve fırsatlara katkıda bulunacağıdır¹⁰⁹.

III. Hukuksal Tanım Eksikliği

Kripto para birimlerinin hukuk dünyasında konumunun belirlenmesi açısından belki de en önemli adım olan üzerinde uzlaşmış ortak bir hukuksal tanım henüz ortaya çıkmamıştır. Bu belirsizlik, geleneksel olarak ayrı yapılar olarak ortaya çıkan para birimi, emtia ve ödeme sistemlerinin kripto para birimi sistemlerinde birbiriyle entegreli olarak bir arada bulunmalarından kaynaklanmaktadır¹¹⁰. Bitcoin ekosisteminde, kendisiyle gerçek ve sanal mal ve hizmetler alınabilen ve belirli bir arz politikasına sahip para birimi unsuru, para hareketlerinin işlendiği ve yönetildiği teknolojik unsur (blokzinciri) ve kullanıcılar arası doğrudan veya borsalarda takas işlemlerine konu olabilen para birimi harici kullanımlar, bu duruma bir örnektir. Bunun yanında, kripto para birimleri için yapılması öngörülen düzenlemelerden, hükümete bağlı hangi merkezî veya özerk kurumun sorumlu olacağı da bu konuda atılması gereken adımları geciktirmektedir.

Kripto para birimlerinin yasal ödeme aracı (*legal tender*) olmadıkları üzerinde genel bir mutabakat bulunmakla beraber, bu olumsuz saptama kripto para birimlerine ilişkin hukuksal konumun belirlenmesi bakımından yetersiz kalmaktadır.

Bazı yazarlar, kripto para birimlerini yasaklayan yasalar olmadığı için yasadışı olmadıklarını fakat para birimi olarak kullanımının yasal olarak desteklenmediğini ve bu yüzden hukuksal olarak yasak ile serbestlik arası gri alanda konumlandığını belirtmektedirler¹¹¹.

¹⁰⁸ A.g.m.

¹⁰⁹ A.g.m., s. 171.

¹¹⁰ IMF, a.g.e., s. 24.

¹¹¹ Brito, Castillo, a.g.e., s. 22; Franco, a.g.e., s. 37.

Bir ülkede farklı kurumların kripto para birimlerini, kendi öncelikleri açısından farklı konumlandıkları da görülmektedir. Mesela ABD’de vergi otoritesi olan Milli Gelirler Dairesi (*Internal Revenue Service, IRS*) vergilendirme amaçları doğrultusunda kripto para birimlerini “mülk” olarak değerlendirirken, ABD Hazine Bakanlığına bağlı *FinCEN*, kara para aklanması ve terörizmin finansmanının engellemesi yükümlülükleri bakımından kripto para birimlerini “değer” olarak kabul etmektedir. Başka ülkeler farklı bir yaklaşımla, resmî bir sınıflama getirmek yerine gerçekleşen işlemlerin doğasına ve türüne odaklanmış bulunmaktadır. Bu durum, yapılacak düzenlemeler ve uygulamalar bakımından ülkeler arası koordinasyonu engelleyecek ve tutarsızlıklara yol açacak bir görünüm arz etmektedir¹¹².

Birçok ülke, kripto para birimlerini gelir vergisi bakımından para olmayan mülkiyet olarak kabul etmektedir. İngiltere, kripto para birimlerini yabancı döviz varlığı olarak görürken; Avusturalya, kripto para birimleri barter hareketleri olarak kabul etmekte ve ne ülke parası ne de yabancı döviz gibi bir muameleye tabi tutmaktadır. Almanya, ilk önce kripto para birimlerini vergilendirme bakımından emtia olarak görmekte iken 2014’ten bu yana yabancı döviz kuru gibi muamele edilmesi gereken bir “özel para” formu olarak değerlendirmektedir¹¹³.

Bazı yazarlar, ortaçağda ticari faaliyetlerin çoğalmasıyla tüccarlar arasında uylaşım sonucu ortaya çıkan ticaret örf ve âdet hukuku, *Lex Mercatoria* gibi kripto para birimlerinin dayandığı blokzinciri teknolojisinin, akıllı sözleşmeler, akıllı mülkler ve merkezî olmayan özerk organizasyonlar (*decentralized autonomous organizations*) aracılığıyla, mevcut hukuksal düzeni değiştireceği ve *Lex Cryptographia* adında yeni bir hukuk alanı oluşturacağını ileri sürmekte¹¹⁴.

Buna göre, blokzinciri teknolojisinin ve kurallarıyla kendi kendini ifa edebilen akıllı sözleşmelerin geniş kesimler tarafından kabul edilmesiyle birlikte, kamu kurumları veya uluslararası büyük şirketler gibi merkezî otoriteler, mevcut vasıtalarla farklı insanları kontrol etme ve biçimlendirme yeteneklerini kaybedeceklerdir. Bu

¹¹² IMF, **a.g.e.**, s. 24.

¹¹³ **A.g.e.**, s. 30.

¹¹⁴ Aaron Wright, Primavera De Filippi, **Decentralized Blockchain Technology and The Rise Of Lex Cryptographia**, 2015, s. 44. Bkz. SSRN: <https://ssrn.com/abstract=2580664> veya <http://dx.doi.org/10.2139/ssrn.2580664>, Erişim tarihi: 6 Mayıs 2018.

nedenle, ortaya çıkacak bu merkezî olmayan özerk organizasyonların mevcut yasal çerçeve içinde düzenlemeleri gereği kendini gittikçe daha çok hissettirecektir¹¹⁵.

Yazılım tabanlı olacak olan bu merkezî olmayan özerk organizasyonlar, diğer insan veya makinelerle ticaret, takas ve diğer yollarla etkileşimde bulunacak ve bu durum, geleneksel hukuki kişilik, hukuki sorumluluk ve bireysel temsil gibi temel hukuksal kavramların sorgulanmalarını ve yeniden gözden geçirilmelerini gerektirecektir¹¹⁶.

V. Uluslararası Arayışlar

Uluslararası çabalar, kripto para birimlerinin potansiyel yararları ve riskleri üzerinde oy birliğinin sağlanması üzerinde odaklanmıştır. İlgili uluslararası kuruluşlar, kendi uzmanlık alanları perspektifinden hazırlayıp paylaştıkları raporlar, el kitapları ve kılavuzlar ile kripto para birimi sistemleriyle ilgili sorunlara ilişkin tartışmalara katkıda bulunmaktadır.

A. FATF (Mali Eylem Görev Gücü)

Kripto para birimleriyle ilgili çalışmalar yapan uluslararası kuruluşlardan birisi olan Mali Eylem Görev Gücü (*Financial Action Task Force, FATF*), kara paranın aklanması, terörizmin finansmanı ve kitle imha silahların yayılmasının finansmanı ile mücadele alanında hem ulusal hem de uluslararası alanda politikalar geliştiren ve bu politikaları destekleyen temel bir uluslararası organizasyondur. FATF, internet tabanlı ödeme sistemleri olarak nitelediği sanal para birimleri ile ilgili kavramsal bir çerçeve oluşturmak ve bu sanal para birimlerinin kara paranın aklanması ve terörün finansmanının önlenmesi bakımından oluşturacağı riskleri ele almak amacıyla Haziran 2014'te bir rapor yayımlamıştır. Raporda, sanal para birimlerinin anlaşılması bakımından, ilgili kavramların tanımlarına ve sanal para birimlerin sınıflandırılmasına yer verilmiştir. Raporda, sanal para birimlerinin bir alt sınıfını oluşturan kripto para birimlerinin, sundukları anonim işlem yapabilme özelliğiyle kara paranın aklanması ve terörizmin finansmanı risklerini tırmandıklarını

¹¹⁵ A.g.m., s. 2.

¹¹⁶ A.g.m., s. 3.

belirtilmiştir¹¹⁷. Ayrıca raporda, sanal para birimlerinin kullanıldığı kara paranın aklanması ile ilgili vakalardan örnekler sunulmuştur¹¹⁸.

FATF, bir yıl sonra, Haziran 2015'te Sanal Para Birimlerine Risk Temelli Bir Yaklaşım Kılavuzu, (*Guidance For A Risk-Based Approach Virtual Currency*) yayımlamıştır. Bu kılavuz, 2013 yılında yayımlanan “*Önödemeli Kartlara, Mobil Ödemelere ve İnternet Tabanlı Ödeme Sistemlerine Risk Temelli Yaklaşım*” raporu ile yukarıda açıklanan 2014 yılı raporunu temel almaktadır. Raporda, sanal para birimine ilişkin ödeme ürünleri ve hizmetlerine FATF tavsiyelerinin risk tabanlı bir yaklaşımla uygulaması üzerinde durulmuştur¹¹⁹. Ayrıca bazı ülkelerde kripto para birimlerinin, kara paranın aklanması, terörizmin finansmanın engellenmesi ve diğer yasadışı kullanımların önlenmesi amacıyla alınan tedbirler de raporda yer almaktadır¹²⁰.

B. UNODC (Birleşmiş Milletler Uyuşturucu ve Suç Ofisi)

Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (*United Nations Office on Drugs and Crime, UNODC*), yasadışı uyuşturucu ve uluslararası suçlarla mücadele eden Birleşmiş Milletler'e yardımcı bir kuruluştur¹²¹. UNODC, “*Sanal Para Birimleri Kullanılarak Gerçekleştirilen Suç Gelirlerinin Aklanmasının Ortaya Çıkarılması ve Soruşturulması Temel El Kitabı*”nı 2014 yılında yayımlamıştır¹²². Bu yayım, GUAM ülkelerinin (Gürcistan, Ukrayna, Azerbaycan ve Moldova) kara paranın aklanması ile mücadele ve suçtan elde edilen gelirlere el koyma kapasitelerinin bölgesel ve ulusal seviyelerde güçlendirilmesi projesinde sunulan çerçeveye dayanmaktadır. Söz konusu proje, 2012 yılında GUAM Sekreteryasının talebi ve ABD Dışişleri Bakanlığı Uluslararası Kolluk ve Narkotik İşleri Bürosunun finansal olarak desteği ile gerçekleştirilmiştir.

¹¹⁷ FATF, **a.g.e.**, s. 9.

¹¹⁸ **A.g.e.**, s. 10.

¹¹⁹ FATF, **Guidance For A Risk-Based Approach Virtual Currencies**, 2015, s. 12. Rapor için bkz. <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>, Erişim tarihi: 10 Mayıs 2018.

¹²⁰ **A.g.e.**, s. 15.

¹²¹ Bkz. <http://www.unodc.org>, Erişim tarihi: 10 Mayıs 2018.

¹²² UNODC, **Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies**, 2014. Bkz. https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf, Erişim tarihi: 10 Mayıs 2018.

Hazırlanan el kitabında, sanal para birimlerine ilişkin kavramsal açıklamalar, bu sistemlerin hukuksal durumları ve bu sistemlerin geçerli mevzuat -özelikle elektronik ticaret, tüketicilerin korunması ve kara paranın aklanması mevzuatı- bakımından değerlendirilmesi yapılmıştır. Kitapta, sanal para birimlerinin ortaya çıkardığı tehditler olarak, hızlı ve geri alınamaz para transferleri¹²³, belirsiz kimlikle (anonim) işlem yapılabilmesi¹²⁴, para hareketlerine ilişkin yetersiz bilgi tutulması¹²⁵, suç gelirlerinin aklanması amacıyla kullanma durumunun saptanması zorluğu¹²⁶, karmaşık ve karartılmış para hareketleri¹²⁷, para hareketlerinde bir üst limit olmaması¹²⁸ ile ilgili açıklamalar yer almaktadır. El kitabında ayrıca, kripto para birimleri kullanılarak gerçekleştirilen suç gelirlerinin aklanması işlemlerinin ortaya çıkarılması ve soruşturulması için kullanılabilecek araçlar ve teknikler de ele alınmıştır¹²⁹.

El kitabının ilgi çekici bir bölümü de sanal para birimlerinin müsadere edilme yollarının anlatıldığı dördüncü bölümüdür. Bilindiği gibi kripto para birimleri belli fiziksel bilgisayar dosyaları olarak değil, cüzdan uygulamaları aracılığıyla gerçekleştirilebilen hareketler olarak vardır ve bu hareketler blokzincirinin birçok farklı lokasyondaki dağıtık kopyalarında tutulmaktadır. Bu nedenle para hareketlerine el koyma işlemi, ancak hareketlerin alıcı kısımlarında yer alan hesapların bağlı oldukları anahtarların bilinmesiyle mümkün olduğundan, bu para birimlerine el koyma işlemi diğer bilişim delillerine el koyma işleminden farklılık arz etmektedir. Bundan dolayı, kitapta bir bölüm sanal para birimlerine el koymanın hukuki şartları, usulleri, araçları ve tekniklerini açıklamaya ayrılmıştır¹³⁰. Kitapta ayrıca, sanal para birimlerinin kullanıldığı farklı suç tiplerinden birçok örnek vaka da yer almaktadır. El kitabında, GUAM ülkeleri mevzuatlarının kara paranın aklanması ve siber suçlar ile ilgili düzenlemeler bakımından bir değerlendirmesi de yer almaktadır¹³¹.

¹²³ A.g.e., s. 42.

¹²⁴ A.g.e., s. 44.

¹²⁵ A.g.e., s. 45.

¹²⁶ A.g.e., s. 46.

¹²⁷ A.g.e., s. 47.

¹²⁸ A.g.e.

¹²⁹ A.g.e., s. 76.

¹³⁰ A.g.e., s. 137.

¹³¹ A.g.e., s. 179.

C. OECD (Ekonomik İşbirliği ve Kalkınma Örgütü)

Ekonomik İşbirliği ve Kalkınma Örgütü (*The Organisation for Economic Co-operation and Development, OECD*), 2014 yılında hazırlattığı “*Bitcoin Sorunu: Para birimine karşı Güven-siz Transfer Teknolojisi*” adlı çalışma notunda¹³², Bitcoin örneğinde kripto para birimi konusunu ele almıştır. *OECD Finans, Sigorta ve Özel Emeklilik Üzerine Çalışma Notları* dizisinde yayımlanan ve OECD’nin resmî görüşü olarak sunulmaması istenen yayımda, yaşanan finansal krizin her türlü finansal araçlara olan güvenin kaybedilmesine yol açtığı ve bunun da güvene dayalı işlemeyi ortadan kaldıran kripto para birimlerinin de içinde yer aldığı alternatif teknolojilerinin genel bir kabulü sonucunu doğurduğu ifade edilmektedir¹³³.

Kripto para birimlerinin işleyişinin Bitcoin örneği üzerinden anlatıldığı raporda, kripto para birimlerinin hiçbir zaman alternatif yasal ödeme aracı olamayacakları öne sürülmektedir. Bunun gerekçesi ise, insanların vergilerini ödemek zorunda oldukları ve bunun da ancak hükümetlerin kontrolündeki merkez bankalarının veya benzeri kurumların kabul ettiği yasal ödeme aracı olan yasal para birimiyle mümkün olabileceği şeklinde belirtilmektedir¹³⁴.

Raporda, tüketicilerin korunması çerçevesinde kripto para birimlerinin neden olabileceği tehlikeler de yer almaktadır. Bu tehditler, piyasa uçuculuğu, oynaklığı (*volatility*), dolandırıcılık, alternatif diğer kripto para birimlerinin ortaya çıkmaları ve hukuksal düzenlemeler olarak belirtilmiştir¹³⁵.

Kripto para birimi sistemlerinde, vergi kaçırma ve kara paranın aklanması problemlerinin daha önemli olduğu belirtilen raporda¹³⁶, bu iki konuyla ilgili hukuksal düzenlemelerde, ödeme sistemleri arasında rekabeti arttıran teknolojilerin desteklenmesi; para transferlerinin söz konusu olduğu durumlarda, anonimliği

¹³² Adrian Blundell-Wignall, **The Bitcoin Question: Currency versus Trust-less Transfer Technology**, 2014, OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing. <http://dx.doi.org/10.1787/5jz2pwjd9t20-en>, Erişim tarihi: 10 Mayıs 2018.

¹³³ **A.g.e.**, s. 7.

¹³⁴ **A.g.e.**, s. 12.

¹³⁵ **A.g.e.**, s. 11.

¹³⁶ **A.g.e.**, s. 12.

engelleyici önlemlerin alınması ve tüketicilerin korunması için asgari gerekliliklerin yerine getirilmesi tavsiye edilmektedir¹³⁷.

Raporun sonuç bölümünde kripto para birimleri ile ilgili genel politika önerileri yer almaktadır¹³⁸: (1) Bankalar ve merkez bankası arası takas işlemlerinde her türlü kripto para birimi kullanımı yasaklanmalıdır. Bu şekilde para sisteminin altının oyulması engellenmiş olur. (2) Güven-siz (güvene dayanmayan) transfer ve defterikebir teknolojilerin kripto para birimi fikrinden ayrılabilceğinin farkına varmak, finansal sistemdeki gelecek rekabet açısından oldukça yararlı olabilir. (3) Tüketicilerin korunması, vergi kaçırma ve kara paranın aklanması ile ilgili otoritelerin, kripto para birimi kullanılan işlemlerde işlem tarafları kişilerin kimliklerini doğrulayabileceği bir sicil sistemi yararlı olabilir. (4) Bütün finansal aktörlerin bilanço raporu ve gelir beyanlarında bulunmaları önemlidir. (5) Takas merkezleri dolandırıcılık veya teknolojik problemlerden kaynaklanacak olumsuz durumlar için bilançolarında belirli miktarlarda ihtiyati sermaye gösterilmelidirler. (6) Kripto para birimlerinin altın gibi değerli madenlerle desteklenmesi veya onlara dayanması doğru olabilir. (7) Devlet, getirilen düzenlemelere uymayan bütün kripto para birimi ağlarını kapatmalıdır.

D. IMF (Uluslararası Para Fonu)

Uluslararası Para Fonu (*International Monetary Fund, IMF*), 2016 yılında gerçekleşen Dünya Ekonomik Forumu'nda yayımladığı “*Sanal Para Birimleri ve Ötesi: Başlangıç Değerlendirmeler*” raporunda kripto para birimlerinin de içinde yer aldığı sanal para birimleri ile ilgili kapsamlı değerlendirmelerde bulunmuştur. Raporda, sanal para birimleri ve işleyişleri hakkında genel bilgiler verilmekte ve bu şemaların parasal sistemler açısından bir değerlendirmesi sunulmaktadır. Ayrıca sanal para birimlerinin dayandığı blokzinciri gibi teknolojik yeniliklerin kara paranın aklanması, terörizmin finansmanı, tüketicilerin korunması, vergilendirme ve diğer mali ve ekonomik alanlarda potansiyel etkileri de tartışılmaktadır.

¹³⁷ A.g.e., s. 17.

¹³⁸ A.g.e.

Raporda, hem ulusal hem de uluslararası düzeyde yapılacak hukuksal düzenlemeler için çerçeve ilkeler ortaya konulmaktadır. Sanal para birimlerine ilişkin hukuksal düzenleme çabalarının uluslararası düzeyde sürdürülmesinin istenildiği raporda, bunun, farklı yargı alanları arasında uyumluluğu teşvik edecek standartları ortaya çıkaracağı öngörülmektedir. Bu standartların benimsenmesi, sınır aşan suçların ve tehditlerin araştırılması ve soruşturulması veya veri paylaşımı gibi ülkeler arası koordinasyona ve birlikte çalışmaya katkıda bulunacak düzenlemeleri de mümkün kılacaktır¹³⁹.

Raporda, sanal para birimleriyle ilgili genel açıklamalarla birlikte sanal para birimlerine ilişkin bir taksonomi de yapılmıştır¹⁴⁰. Dijital temsil özelliğinden kriptografi kullanımına göre oluşturulmuş bir spektrumda kripto para birimleri, sanal para birimlerinin en dar kümesini oluşturmaktadır¹⁴¹. Sanal para birimlerinin, para olup olmadığının tartışıldığı bölümde, sanal para birimlerinin hukuksal olarak kabul edilen para tanımını tam anlamıyla karşılamadığı belirtilmektedir¹⁴².

Raporun bir bölümü, dağıtık defterikebir teknolojisine ayrılmıştır. Bu bölümde, blokzinciri teknolojisi anlatılmakta ve bu yeniliğin, (özellikle uluslararası) para transferlerinde maliyetleri azaltacağını ve menkul değerlere ilişkin işlem sürelerini kısaltacağı ve bunun da finansal endüstride değişime yol açabileceği ifade edilmektedir¹⁴³.

Raporun sanal para birimlerine ilişkin hukuksal düzenleme ve politika zorlukları bölümünde, geleneksel olarak ayrı yapılar olan para birimi, emtia ve ödeme sistemlerinin sanal para birimlerinde bütünleşik olduğu ve bunun da üzerinde uzlaşmış ortak bir hukuksal tanım ortaya koymayı zorlaştırdığı ifade edilmektedir¹⁴⁴. Sanal para biriminin takibinin zor olduğu¹⁴⁵, sınır aşan bir teknolojiye dayandığı için ulusal düzeyde düzenlenmesinin zorluk arz ettiği¹⁴⁶ ve

¹³⁹ IMF, *a.g.e.*, s. 7.

¹⁴⁰ *A.g.e.*, s. 8.

¹⁴¹ *A.g.e.*

¹⁴² *A.g.e.*, s. 16.

¹⁴³ *A.g.e.*, s. 23.

¹⁴⁴ *A.g.e.*, s. 24.

¹⁴⁵ *A.g.e.*

¹⁴⁶ *A.g.e.*, s. 25.

merkezi olmayan yapıları nedeniyle geleneksel düzenleme modellerine kolayca uymadığı¹⁴⁷ da belirtilmektedir.

Raporda, sanal para birimlerine ilişkin ortaya çıkmakta olan düzenlemelerin, potansiyel riskleri adreslerken her yargı yetkisinin önceliğine göre şekillendiği ileri sürülmektedir¹⁴⁸. Söz konusu düzenlemelerde, sanal para birimi paydaşlar ve onlarla etkileşimde bulunan finansal kuruluşlar hedefe alınmıştır¹⁴⁹. Bu düzenlemelerin etkinliği bu piyasaların nasıl evrileceğine bağlıdır¹⁵⁰.

Raporun sanal para birimlerinden kaynaklanan risklerin incelendiği bölümde, para transferlerinin anonim şekilde yapılmasının finansal bütünlüğü tehdit ettiği belirtilmekte ve kara paranın aklanması, tüketicilerin korunması, vergilendirme, borsa (takas) kontrolleri, sermaye akışı yönetimi, finansal istikrar ve para yönetimi açısından bu sistemlerin arz ettiği riskler açıklanmaktadır¹⁵¹.

Raporda yapılacak hukuksal düzenlemelere ilişkin şu ilkeler önerilmektedir¹⁵²:

(1) Getirilecek düzenlemeler, riskleri azaltırken, teknolojik yeniliğin önünü kapatmamalıdır. (2) Düzenlemeler, sanal para birimlerinde yaşanacak değişimlerle uyumlu ve esnek yapıda olmalıdır. (3) Düzenleyiciler, sanal para birimlerine özgü yeni iş modellerini göz önüne almalıdır. (4) Düzenlemeler, suç davranışlarını (kara paranın aklanması, dolandırıcılık, vs.) içermekle kalmamalı, sanal para birimi araçlarının finansal olarak güçlü olmasını da sağlamalıdır. (5) Düzenlemeler, sanal para birimleri ile geleneksel finansal sistem arasındaki entegrasyonu da içermelidir.

VI. Bölgesel ve Ulusal Arayışlar

A. Avrupa Birliği

¹⁴⁷ A.g.e.

¹⁴⁸ A.g.e.

¹⁴⁹ A.g.e.

¹⁵⁰ A.g.e., s. 26.

¹⁵¹ A.g.e., s. 27.

¹⁵² A.g.e., s. 35.

Avrupa Birliği bünyesinde faaliyet gösteren bazı birlik kuruluşları kripto para birimleriyle ilgili kendi uzmanlık alanlarında çeşitli çalışmalarda bulunmuşlardır. Bu bölümde bu çalışmalar sonucu yayımlanan raporlar ele alınacaktır.

1. EBA (Avrupa Bankacılık Otoritesi)

Avrupa Birliği (AB) adına, finansal hareketleri izlemekle yükümlü olan Avrupa Bankacılık Otoritesi (*European Banking Authority, EBA*), piyasaların güvenli ve sağlıklı işlemelerini ve hukuksal düzenleme pratiklerinin yakınlaşmalarını destekleyen ilkeleri ve önerileri benimsemekle de görevlidir¹⁵³.

EBA, sanal para birimleriyle ilgili ilk çalışmasını, 13 Aralık 2013 tarihinde “*Tüketicilere Sanal Paralarla İlgili Uyarı*” başlıklı genel bir uyarı notu ile yayımlamıştır¹⁵⁴. Bu notta, kısaca sanal para birimleri tanımlandıktan ve işleyişleri hakkında açıklamalarda bulunduktan sonra, tüketicilere, bu para birimlerinin hukuksal olarak düzenlenmedikleri ve bu yüzden giderilmemiş riskler içerdikleri belirtilmiştir. Uyarı notunda, tüketicilerin karşılaşılabileceği riskler olarak, (1) takas platformundan veya dijital cüzdanlardan para çalınması, (2) sanal para birimlerinin ödeme aracı olarak korunmaması, (3) fiyatların oynaklığı, hızlı değişimi, (4) para hareketlerinin suç faaliyetlerinde kullanılabilmesi ve (5) vergilendirme yükümlülüklerine maruz kalma şeklinde belirtilmiştir¹⁵⁵.

Tüketiciler, sanal para alacaklarsa, (1) bu para birimlerine özgü nitelikleri tam olarak bilmeli, (2) kaybedilmesi göze alınamayacak kadar çok gerçek para kullanmamalı ve (3) normal cüzdanlarına gösterdikleri ihtiyatı dijital cüzdanları için de göstermelidirler¹⁵⁶.

EBA’nın sanal para birimleriyle ilgili ikinci çalışması, 4 Eylül 2014 tarihinde “*Sanal Para Birimleri Hakkında EBA Görüşü*” başlığıyla yayımlanmıştır. Analizde, sanal para birimlerine ilişkin genel açıklamalardan sonra, bu sistemlerden

¹⁵³ EBA, **a.g.e.**, s. 7.

¹⁵⁴ EBA, **Warning to consumers on virtual currencies**, <https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf>, Erişim tarihi: 14 Mayıs 2018.

¹⁵⁵ **A.g.e.**, s. 2-3.

¹⁵⁶ **A.g.e.**, s. 3.

sağlanabilecek potansiyel yararlarından bahsedilmiştir. Buna göre, sanal para birimlerinin finans endüstrisine muhtemel katkıları, (1) para hareketlerinde masrafların azalması, (2) işlem sürelerinin kısalması, (3) ödemelerin kesinliği, (4) ekonomik büyümeye katkı ve (5) AB dışı finansal yayılım olarak belirtilmiştir¹⁵⁷.

Bu çalışmada sanal para birimlerine ilişkin oldukça kapsamlı bir risk analizi yapılmıştır. Bu riskler, (a) kullanıcı riskleri, (b) piyasa paydaşı olmayan kullanıcı riskleri, (c) finansal bütünlük riskleri, (d) yasal para birimiyle çalışan ödeme sistemlerine yönelik riskler ve (e) hukuksal düzenleyicilere yönelik riskler olarak beş kategoriye ayrılmış ve her bir kategori altında yüksek, orta ve düşük önem derecesine göre sıralanmış toplam 70 risk sıralanmış ve her biri kısaca açıklanmıştır¹⁵⁸.

Hukuksal düzenleyicilere karşı şu riskler sıralanmıştır¹⁵⁹: (1) Hukuksal düzenleyiciler sanal para birimleri için düzenleme kararı alabilirler fakat seçtikleri yaklaşım başarısız olabilir. (2) Hukuksal düzenleyiciler, sanal para birimleri için düzenleme kararı almayabilirler fakat hukuksal olarak düzenlenmiş finansal kuruluşların sağlıklı işleyişleri, sanal para birimleriyle etkileşimlerinden dolayı zarar görebilir. (3) Geleneksel finansal faaliyetlerin hukuksal olarak düzenlenmesi ve denetimi, aynı riskleri doğuran düzenlenmemiş 'gölge' faaliyetler tarafından engellenebilir. (4) Düzenleyici, mevcut sözleşmeleri yasa dışı/ifa edilemez kılan hukuksal bir düzenleme ortaya koyduğu için davaya maruz olabilir. (5) Düzenleyici sanal para birimleri için itibari para birimlerine göre daha yumuşak düzenleme yapmaya karar vermeli mi? Bu durumda piyasalarda ödeme hizmetleri için eşit olmayan bir alan ortaya çıkacaktır. (6) Eğer eşit olmayan bir alanın varlığı korunursa, servis sağlayıcıların piyasaları terk etmesinden dolayı itibari para ödeme hizmetlerinde piyasa rekabeti zayıflayacaktır. (7) Eğer sanal para birimlerine karşı düzenleyici yaklaşım aşırı ise yeni potansiyel girişimcilerin ödeme hizmetleri piyasasına girmeleri zorlaşır. (8) Sanal para birimleri yaygın kabul görürse, itibari para ihraççısı merkez bankaları, aldıkları parasal önlemlerin etkilerini tahmin etmede zorlanacaklar ve ekonomik kontrolü kaybedeceklerdir.

¹⁵⁷ EBA, **EBA Opinion On ‘Virtual Currency’**, s. 15.

¹⁵⁸ **A.g.e.**, s. 22.

¹⁵⁹ **A.g.e.**

Bu risklerin giderilmesi için uzun vadeli hukuksal düzenlemeler öngören bir yaklaşımla bir takım öneriler tavsiye edilmiştir¹⁶⁰. Bunlardan bazıları; (1) Mevcut finansal hizmetlerle etkileşim içinde olan sanal para birimi şemalarını yönetenler, bu piyasayı düzenleyen otoriteye karşı sorumlu olmalıdır. (2) Şema yönetim otoritesi, bu sistemlerin yönetimi ve kullanımı için kurallar geliştiren kişilerden oluşan topluluktur. Tüzel kişiliğe sahip olan bu yapı, ilgili düzenlemelere ve denetimlere tabi olacaktır. (3) Anonim olarak para transferi gerçekleştirmekten kaynaklanan riskleri gidermek için itibari para birimiyle etkileşimde bulunan sanal para birimi takas merkezleri ve diğer ilgili kullanıcılar CDD (*Customer Due Diligence* / Müşteriye Özen İlkesi; bankanın müşterilerini tanıması) gereklerine ve KYC (*Know Your Customer*, Müşterilerini Tanı İlkesi) yükümlülüklerine uymalıdır. (4) Şema yöneticilerinin, takas merkezlerinin ve diğer gerekli piyasa paydaşlarının dürüstlük ilkesi doğrultusunda faaliyette bulunmaları sağlanmalıdır. (5) Takas merkezleri veya şema yöneticileri gibi piyasa paydaşları, kendi fiillerinden kaynaklanan sorumluluklarının gereğini yerine getirebilmeleri için AB sınırları içinde tüzel bir kişilik olarak kurulmuş olmalıdırlar. (6) Fiyat belirsizliği ve piyasa istismarının önlenmesi için takas merkezlerinde, iç manipülasyonlara karşı gerekli önlemler alınmalı ve para hareketleri belgeli olmalıdır. (7) İtibari para ile etkileşimli sanal para birimi hizmeti verebilmek için sicile kayıt zorunlu olmalıdır. (8) Piyasa paydaşlarının, finansal risklerin muhtemel olumsuz etkilerini giderebilecek sermayeye sahip olmaları sağlanmalıdır. (9) Piyasa paydaşları, kendi hesapları ile müşterilerine ait hesapları birbirinden ayırmalıdır. (10) Sanal para birimi şemalarının, bilgi işlem güvenliği için gerekli önlemleri almaları sağlanmalıdır. (11) Yetkisiz sanal para hareketinden sorumlu olan piyasa paydaşının bu hareketten kaynaklanan olumsuzluğu tazmin etmesi zorunlu olmalıdır. (12) Sanal para birimi şemaları, geleneksel ödeme sistemlerinden ayrı tutulmalıdır.

Bu öneriler dışında, hukuksal düzenlemelerde kavramların geniş kapsamlı tanımlanmaları; şema yönetim otoritelerinin, kendi yönetimi altındaki sanal para birimlerine özgü standartlar ortaya koyması; bu şemalara ilişkin şikâyet mekanizmalarının oluşturulması; şema yöneticileri tarafından belirli belgelerin ilgili

¹⁶⁰ A.g.e., s. 37.

düzenleyici kuruluşlara sunulması; kamuoyunun, düzenlemelerin hayata geçirilmesi süresince riskler konusunda periyodik uyarılmaları da tavsiye edilmiştir¹⁶¹.

Raporda, sanal para birimlerinin internet tabanlı sistemler oluşundan dolayı uluslararası bir düzenleme yaklaşımıyla ele alınması gerektiği belirtilmektedir. Aksi halde başarılı bir hukuksal düzenin kurulması mümkün gözükmemektedir¹⁶².

Kısa vadede yapılması tavsiye edilen önlemler olarak; sanal para birimleri ile itibari para birimleri arasındaki etkileşimden kaynaklanan kara paranın aklanması, finansal suç riskleri ile geleneksel ödeme sistemlerine yönelik risklerin bertaraf edilmesi için kredi kuruluşları, ödeme kuruluşları ve e-para kuruluşlarının sanal para birimleri alımı veya satımı gibi işlemlerden uzak durması önerilmektedir¹⁶³. AB yasakoyucularının, kara paranın aklanması ve terörizmin finansmanının engellemesi bakımından sanal para takas merkezlerini yükümlü kurumlar olarak ilan etmesi de önerilen bir başka önlemdir¹⁶⁴.

2. ECB (Avrupa Merkez Bankası)

Avrupa Merkez Bankası (*European Central Bank, ECB*), AB çatısı altında Avro'ya geçiş yapan 19 ülkenin merkez bankasıdır ve başlıca görevleri, Avro bölgesinde fiyat istikrarını sağlamak ve Avro'nun satın alma gücünü koruyucu önlemler almaktır¹⁶⁵.

ECB, sanal para birimleriyle ilgili ilk çalışmasını, 2012 yılı Ekim ayında “*Sanal Para Birimi Şemaları*” başlığıyla yayımlamıştır. Raporda, sanal para birimlerine ilişkin genel tanım, karşılaştırma ve sınıflandırma bölümünden sonra Bitcoin ve *Second Life* sanal para birimi örneklerinin ayrıntılı olarak incelendiği bölüm yer almaktadır.

Raporun son bölümünde ise sanal para birimlerinin merkez bankaları açısından risk değerlendirmesi yapılmaktadır. Buna göre, sanal para birimleri, para ihracının

¹⁶¹ A.g.e., s. 41.

¹⁶² A.g.e.

¹⁶³ A.g.e., s. 42.

¹⁶⁴ A.g.e.

¹⁶⁵ <https://www.ecb.europa.eu/ecb/tasks/html/index.en.html>, Erişim tarihi: 16 Mayıs 2018.

düşük seviyede devam etmesi şartıyla fiyat istikrarı için tehdit değildir¹⁶⁶. Bu şemalar, kararsız yapılarına rağmen, reel ekonomiyle sınırlı bağlantıları olduğu için finansal istikrar için de bir risk oluşturmamaktadırlar¹⁶⁷. Bu şemalar, ödeme sistemleri istikrarı açısından sistemik bir risk doğurmamakla beraber, kendi kullanıcılarıyla sınırlı operasyonel ve hukuksal riskler içermektedir¹⁶⁸.

Raporda, sanal para birimlerinin kullanımının artmasına paralel olarak, bu şemalarla ilgili olumsuz vakaların artması ve basının bunlarla ilgili haberleri sürekli gündeme taşımasının, merkez bankalarının görevlerini yeterince yapmadıkları algısına neden olabileceği ve bunun da merkez bankalarının saygınlığı açısından bir risk olarak değerlendirilmesi gerektiği ifade edilmektedir¹⁶⁹.

Raporda, sanal para birimlerindeki istikrarsızlığının temel sebebi olarak, bu şemalara temel oluşturacak hukuksal düzenlemelerin mevcut olmayışı belirtilmektedir¹⁷⁰. Bu sistemlerin birçok yargılama yetkisini kapsayan kullanım dağılımı göz önüne alındığında, geçerli yargılama yetkisi kurallarını saptamak veya ilgili kullanıcıların yada şema sahiplerinin konumlarını belirlemek kolay olmayacaktır. Bu nedenle hükümetler bu şemaları yasaklamak veya denetlemek istediklerinde ciddi zorluklarla karşılaşacaklardır¹⁷¹.

Raporda Bitcoin'in hukuksal durumuna da değinilmiştir¹⁷². Birliğin Elektronik Para Direktifi'ne (2009/110/EC) göre Bitcoin elektronik para değildir. Çünkü Bitcoin, direktifte elektronik para birimi olmak için belirtilen üç şarttan ikincisi olan *"karşılığında gösterilen parasal değerden daha az olmayan fonun alınması üzerine ihraç edilen"* şartını yerine getirmemektedir¹⁷³. Bundan başka, Bitcoin'i Ödeme Hizmetleri Direktifi (2007/64/EC) kapsamında bir ödeme kuruluşu olarak kabul etmek de mümkün değildir. Çünkü bu direktif, ödeme kuruluşlarının elektronik para ihracına izin vermemektedir¹⁷⁴.

¹⁶⁶ ECB, **Virtual Currency Schemes**, s. 37.

¹⁶⁷ A.g.e., s. 39.

¹⁶⁸ A.g.e., s. 42.

¹⁶⁹ A.g.e., s. 45.

¹⁷⁰ A.g.e., s. 42.

¹⁷¹ A.g.e.

¹⁷² A.g.e., s. 43.

¹⁷³ A.g.e.

¹⁷⁴ A.g.e.

ECB'nin sanal para birimleriyle ilgili ikinci çalışması “*Sanal Para Birimleri – Ek Analiz*” başlığıyla 2015 yılı Şubat ayında yayımlanmıştır. Bu çalışmada, sanal para birimleri ödemelere dönük yönleri ile ele alınmış ve merkez bankası perspektifine göre değerlendirilmiştir.

Raporda, sanal para birimlerine ilişkin hem ulusal hem de uluslararası yasal düzenleme arayışlarına da değinilmiştir¹⁷⁵. Buna göre, ülkeler sanal para birimleriyle ilgili olarak, (1) uyarma, (2) hukuksal durumu açıklayıcı beyanlar, (3) (gelecekte) lisanslama ve denetleme zorunluluğu getirme ve (4) yasaklama şeklinde dört farklı kategoride değerlendirilen yanıtlar vermektedirler.

Uyarmaya örnek olarak, Almanya Federal Finansal Denetleme Otoritesi (BaFin), Banque de France, Hollanda ve Belçika Merkez Bankalarının da aralarında bulunduğu birçok kurum sayılmaktadır¹⁷⁶. Bitcoin'in bir para birimi olmadığı, yasal ödeme aracı olarak kabul edilmediği ve finansal araç tanımını da karşılamadığını belirten açıklamalarda bulunan kurumlardan bazıları, Finlandiya, Endonezya ve Malezya Merkez Bankaları ile Almanya Maliye Bakanlığı, sayılmaktadır¹⁷⁷.

Bazı ülkeler, Bitcoin ile ilgili hizmet sunan kuruluşlar için lisanslama ve denetlenme zorunluluğu getirmeyi planlamaktadır. İsveç'te sanal para birimleri takas merkezleri için lisanslama zorunluluğu 2012 yılından beri mevcuttur¹⁷⁸. Almanya, Fransa, Hong Kong ve New York eyaleti lisanslama zorunluluğu getirmeyi düşünen ülkeler arasındadır¹⁷⁹.

Bazı ülkeler, sanal para birimleriyle ilgili birtakım faaliyetleri yasaklama yoluna gitmişlerdir. Çin, finansal kuruluşların Bitcoin ticareti yapmalarını yasaklamıştır. Rusya'da Başsavcılık, Bitcoin'in de içinde yer aldığı “ikame para birimi” kullanımının yasak olduğunu açıklamıştır¹⁸⁰.

¹⁷⁵ ECB, *Virtual Currency Schemes A Further Analysis*, s. 30.

¹⁷⁶ A.g.e.

¹⁷⁷ A.g.e., s. 31.

¹⁷⁸ A.g.e.

¹⁷⁹ A.g.e.

¹⁸⁰ A.g.e., s. 32.

B. ABD

ABD’de kripto para birimleri ile ilgili düzenlemeler, Federal hükümetin bağlayıcı bir karar almamasından dolayı eyaletler tarafından gerçekleştirilmektedir. Bu nedenle New York, Arizona, Maine, Nevada ve Vermont eyaletleri blokzinciri ve akıllı sözleşmelerle ilgili kendi yasal düzenlemelerini yapmışlardır. Milli Gelirler Dairesi (IRS), 2014 yılında yaptığı açıklamada sanal para ticaretinden kaynaklanan gelirlerin, sermaye kazançları bakımından mülk olarak değerlendireceğini belirtmiştir¹⁸¹.

C. Almanya

Alman kanunlarına göre sanal para birimleri, özel para birimi olarak finansal araçlardır ve bu nedenle vergilendirme bakımından sermaye olarak değerlendirilmektedir. Almanya Federal Finansal Denetleme Otoritesi (BaFin), Bitcoin’i, yasal ödeme aracı olan para birimiyle bağlı olmadığı için elektronik para olarak kabul etmemektedir¹⁸².

D. Çin

Çin, sanal para birimlerini sanal emtialar (*virtual commodity*) olarak kabul etmektedir. Hukuksal düzenleme eksikliğinden dolayı Bitcoin ticaretinde öncü olan Çin, sermayenin ülkeden kaçmaması için 2017 yılında kripto para birimleriyle ilgili sert düzenlemelere gitmiştir. Finansal kuruluşların ve üçüncü taraf ödeme sağlayıcıların sanal para birimleri almaları, satmaları ve bulundurmaları yasaklanmıştır. Çin Merkez Bankası, sanal para birimleri borsalarının ilgili sicillere kayıt olmalarını zorunlu kılmış ve işlemlerin sıkı denetimlere tabi tutulacağını belirtmiştir. Çin’de şirketler veya bireyler tarafından sanal para birimleriyle kitlesel sermaye toplama faaliyetleri (*Initial Coin Offerings, ICO*) yasaktır¹⁸³.

¹⁸¹ An Roinn Airgeadais (Department of Finance), **Virtual Currencies and Blockchain Technology**, Dublin: 2018, s. 13. <http://www.finance.gov.ie/wp-content/uploads/2018/03/Virtual-Currencies-and-Blockchain-Technology-March-2018.pdf>, Erişim tarihi: 17 Mayıs 2018.

¹⁸² **A.g.e.**, s. 15.

¹⁸³ **A.g.e.**, s. 17.

E. Japonya

Japonya, sanal para birimlerinin tartışmasız en büyük savunucusudur. 2014 yılında, diğer ülkeler bu sistemleri yasaklama yoluna giderken, Japonya, hukuksal düzenleme yollarını arayacağını açıklamıştır. 2016 yılında Mali Hizmetler Ajansı (*Financial Services Agency, FSA*), sanal para birimlerinin geleneksel para birimleriyle aynı statüde olmasını teklif etmiştir. Yine 2016 yılında ulusal mecliste (*Diet*) kabul edilen yasada, sanal para birimi tanımıyla birlikte takas merkezlerine ilişkin çalışma usulleri, kayıt olacakları sicil ve yükümlükleri belirlenmiştir. FSA, 2017 yılında sanal para birimlerinin birer ödeme metodu olarak kabulünü içeren bir yasayı yürürlüğe koymuştur. Japon bankalarından oluşan bir konsorsiyum, 2020 Olimpiyatlarından önce *JCoin* adında bir sanal para birimi çıkarmayı planlamaktadırlar¹⁸⁴.

F. İngiltere

İngiltere, sanal para birimlerini savunan ilk ülkeler arasındadır. 2013 yılında İngiltere Gelir ve Gümrükler İdaresi (*HMRC*), sanal para birimlerinin vergi kanunlarının uygulama alanına dâhil olduğunu açıklamıştır. HMRC, 2014 yılında yaptığı açıklamada Bitcoin'in özel para olduğunu ve bu nedenle sermaye kazançları vergisine tabi olmadığını belirtmiştir. 2015 yılında Hazine Bakanlığı, Bitcoin borsaları için kara paranın aklanmasıyla ilgili düzenlemelerin yapılacağını açıklamıştır¹⁸⁵.

G. Rusya

Rusya, sanal para birimlerine hasım olan ülkeler arasında sayılmaktadır. Rus kanunlarına göre, resmi para birimi yerini tutacak ikame para ihracı/arzu yasaktır. Rusya Merkez Bankası, yayımladığı uyarı notunda, mal veya hizmet alım satımlarında yasal para birimi (ruble) yerine sanal para birimlerinin kullanımının

¹⁸⁴ A.g.e., s. 9.

¹⁸⁵ A.g.e., s. 11.

yasak olduğunu belirtilmiş, sanal para işlemlerinin yasadışı faaliyet şüphesiyle inceleme altında olacağını açıklamıştır¹⁸⁶.

H. Türkiye

Türkiye’de sanal para birimlerinin yasal durumlarını belirleyici bir düzenleme bulunmamaktadır.

Bankacılık Düzenleme ve Denetleme Kurumu’nun (BDDK) 25 Kasım 2013 tarihinde yaptığı açıklamada¹⁸⁷, Bitcoin’in mevcut yapısı ve işleyişi itibarıyla 6493 sayılı “*Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun*” kapsamında olmadığı ve elektronik para olarak değerlendirilmediği ve bu yüzden gözetim ve denetiminin mümkün olmadığını belirtilmiştir. Açıklamada, Bitcoin sisteminde gerçekleşen işlemlerde tarafların kimliklerinin bilinmemesi sebebiyle, Bitcoin sisteminin yasadışı faaliyetler için uygun bir ortam olduğu belirtilmiştir. Ayrıca Bitcoin’in piyasa değerinin aşırı oynak olması, dijital cüzdanların çalınabilmesi, kaybolabilmesi veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi gibi risklerin yanısıra yapılan işlemlerin geri döndürülemez olmasından dolayı operasyonel hatalardan veya kötü niyetli satıcıların suiistimalinden kaynaklı risklere açık olduğu da belirtilmiştir.

Sermaye Piyasası Kurulu’nun (SPK) 27 Kasım 2017 tarihinde kurumlara gönderdiği Genel Mektup’ta¹⁸⁸ “*sanal para birimleri ile ilgili olarak Türkiye’de bir düzenleme veya tanımlama bulunmadığı ve Sermaye Piyasası Kanunu kapsamında yer alan türev araçlara dayanak teşkil edebilecek unsurlar içerisinde sanal para birimlerinin bulunmadığı dikkate alınarak, bu aşamada müşterilere yönelik sanal para birimlerine dayalı spot veya türev işlemler yapılmaması gerektiği hususunda bildirimde bulunulmasına karar verildiği bildirildi.*” ifadeleri yer almaktadır.

¹⁸⁶ FATF, **Guidance For...**, (2015), s. 19.

¹⁸⁷ BDDK, **Basın Açıklaması**,

https://www.bddk.org.tr/websitesi/turkce/duyurular/Basin_Aciklamalari/12574bitcoin_hk_basin_aciklamasi.pdf, Erişim tarihi: 17 Mayıs 2018.

¹⁸⁸ https://www.ntv.com.tr/teknoloji/spkdan-sanal-paralara-dayali-islemler-hakkinda-aciklama,4zk6GcRVf0O-pj4T_NQ-fA, Erişim tarihi: 17 Mayıs 2018.

§5. Kripto Para Birimlerinin Ceza Hukuku Bakımından Değerlendirilmesi

Üzerinde uzlaşmış ortak hukuki bir tanımı olmayan kripto para birimi kavramının, ceza hukuku uygulamaları bakımından da bir takım belirsizlikleri beraberinde getireceği açıktır.

Bu bölümde, ilk önce kripto para birimlerinin ceza hukuku bakımından hangi değer kategorisinde yer aldığı tartışılacak, ardından bu para birimlerinin doğrudan kullanımlarının suç oluşturup oluşturmadıkları konusu ele alınacaktır.

I. Kripto Para Birimlerinin Değer Olarak Sınıflandırılması

Kripto para birimleri, değer taşıyıcı niteliklerinden dolayı, elektronik para, emtia veya menkul değer kategorisinden birinde yer alabilirler. Türk mevzuatında, bu hususla ilgili bir belirlenimin olmadığı daha önce ifade edilmişti.

BDDK'nın yukarıdaki açıklamasından anlaşıldığı gibi, Bitcoin gibi bir kripto para biriminin elektronik para olarak kabul edilebilmesi için, elektronik para ihraç etme yetkisi verilmiş bir kuruluş tarafından ihraç edilmesi gerekmektedir. Fakat kripto para birimleri merkezî olmayan yapıda oldukları için bu şartı sağlamaktan uzaktırlar¹⁸⁹.

Kripto para birimlerinin elektronik para olarak kabul edilip edilmemeleri önemlidir, çünkü dijital para birimlerinin yasal para birimleriyle ilişkisi elektronik para üzerinden sağlandığından, elektronik para olarak kabul edilmek veya edilmemek, kripto para birimlerinin para olarak kabulünü etkileyecek bir sonuç doğuracaktır. Şimdiye kadar kripto para birimleri ne Türk mevzuatında ne de herhangi bir ülke mevzuatında para olarak kabul görmemiştir. Bu nedenle kripto para birimlerinin para veya yabancı döviz olarak kabulü mümkün gözükmemektedir.

Kripto para birimleri menkul değerler olarak kabul edilebilirler mi? Menkul değerlere ilişkin hukuki tanım, 6362 sayılı Sermaye Piyasası Kanunu'nun (SPK), 3.

¹⁸⁹ Ersan Şen'in Bitcoin'in elektronik para olarak kabul edilemeyeceği görüşünü paylaştığı yazısı için bkz. **Bitcoin: Elektronik Para**, <http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1120849-bitcoin-elektronik-para>, Erişim tarihi: 12 Haziran 2018.

maddesinde yer almaktadır. Bu tanıma¹⁹⁰ göre, kripto para birimlerinin menkul değer olarak kabul edilebilmeleri için belirli payları temsil etmeleri veya kamu yada özel sektör kuruluşların piyasalardan borç alabilmek için kullandıkları hazine bonosu, gelir ortaklığı senetleri, devlet iç borçlanma senetleri, özel kesim tahvil ve bonoları gibi borçlanma araçlarından olmaları gerekir. Halbuki Bitcoin gibi kripto para birimleri ne belirli payları temsil etmekte ne de borçlanma aracı olarak kullanılmaktadırlar. Bu nedenle kripto para birimlerinin menkul değerler olarak kabulü mümkün görünmemektedir. Bunun yanında Sermaye Piyasası Kurulu, yukarıda değinilen açıklamasında, *“sanal para birimleri ile ilgili olarak Türkiye’de bir düzenleme veya tanımlama bulunmadığı ve Sermaye Piyasası Kanunu kapsamında yer alan türev araçlara dayanak teşkil edebilecek unsurlar içerisinde sanal para birimlerinin bulunmadığı”*nı açıklamıştır. Türev araçlara ilişkin tanıma¹⁹¹ bakıldığında, kripto para birimlerinin, türev araç sayılabilmeleri için ya (1) SPK tarafından doğrudan türev araç olarak kabul edilmeleri veya (2) belirli varlıklara dayalı olarak ihraç edilen menkul değer olmaları veyahut (3) dayanak varlıklardaki değer değişimlerini temsil etmeleri gerekmektedir. Bu üç şartın da gerçekleşmediği göz önüne alındığında kripto para birimlerinin türev araçlar olarak kabulü mümkün gözükmemektedir.

Kripto para birimleri açısından bir başka seçenek, emtia olarak kabul edilmeleridir. Yukarıda açıklandığı üzere, birçok ülke vergilendirme bakımından kripto para birimlerini emtia olarak kabul etmektedir. Hatta Çin, bu para birimlerini sanal emtia olarak görmektedir. Bilindiği gibi, emtia, altın, gümüş, bakır, buğday, arpa, mısır, petrol, doğalgaz ve mineraller gibi kendinden bir değere sahip olup ticarete konu olabilen mallar için kullanılan genel bir kavramdır. Sanal emtia (*virtual commodity*) ise, yalnız internet üzerinde gerçekleşen sanal ekonomide ticarete konu

¹⁹⁰ **SPK Madde 3 – o) Menkul kıymetler:** Para, çek, poliçe ve bono hariç olmak üzere; (1) paylar, pay benzeri diğer kıymetler ile söz konusu paylara ilişkin depo sertifikaları, (2) borçlanma araçları veya menkul kıymetleştirilmiş varlık ve gelirlere dayalı borçlanma araçları ile söz konusu kıymetlere ilişkin depo sertifikaları

¹⁹¹ **SPK Madde 3 – u) Türev araçlar:** Aşağıda sayılan veya Kurulca bu kapsamda olduğu belirlenen diğer türev araçları: (1) Menkul kıymetleri satın alma veya satma veya birbirleri ile değiştirme hakkı veren türev araçları, (2) Değeri, bir menkul kıymet fiyatına veya getirisine; bir döviz fiyatına veya fiyat değişikliğine; faiz oranına veya orandaki değişikliğe; bir kıymetli maden veya kıymetli taş fiyatına veya fiyat değişikliğine; bir mal fiyatına veya fiyat değişikliğine; Kurulca uygun görülen kurumlarca yayınlanan istatistiklere veya bunlardaki değişikliğe; kredi riski transferi sağlayan, enerji fiyatları ve iklim değişkenleri gibi ölçüm değerleri olan ve bu sayılanlardan oluşturulan bir endeks seviyesine veya seviyedeki değişikliğe bağlı olan türev araçları, bu araçların türevlerini ve sayılan dayanak varlıkları birbirleri ile değiştirme hakkı veren türevleri,

olabilen mallar için kullanılmaktadır¹⁹². Kripto para birimlerinin, kendileri için özel olarak kurulmuş takas merkezleri ve borsalarda yasal para birimleriyle etkileşime girip alım satım işlemlerinde kullanılmaları onları emtia kavramına yaklaştırırken, kendinden bir değere (*intrinsic value*) sahip olmamaları, uzaklaştırmaktadır.

Bu analizler çerçevesinde, kripto para birimlerinin mevcut hukuksal düzenlemelere göre ne para, ne menkul değer veya türev araç ne de emtia olarak kabulü mümkün gözükmemektedir. Çin'in kabul ettiği sanal emtia kavramı ise detayları ve hukuki uygulamaları zamanla ortaya çıkacak yeni bir husustur.

Kripto para birimleriyle ilgili bu belirsizliklere rağmen, ceza hukuku bakımından soruna ışık tutacak yaklaşımın, uluslararası kuruluşların bu sistemlerle ilgili yayımladıkları raporlardan çıkarılabileceği görüşündeyiz. Bu raporlarda, kripto para birimi sistemlerinin, suçtan kaynaklanan malvarlığı değerlerinin (kara paranın) aklanması, terörün finansmanı ve vergi kaçırma suçları için elverişli imkânlar sundukları ve ortaya çıkarılan suç vakalarında, gerçek para birimi gibi işlev gördükleri belirtilmektedir.

FATF tanımında yer alan “*değerin dijital ticaretini mümkün kılan*” ifadesi ve yine ele alınan bazı raporlarda geçen “*paraya alternatif olarak kullanılabilen*” ifadesi kripto para birimlerinin gerçek para birimleri yerine alternatif olarak kullanımını teyit etmektedir. Kripto para birimlerinin “alternatif para birimi” olarak kullanımı, SPK tarafından yukarıda değinilen raporda da belirtilmektedir. Şüphesiz kripto para birimlerinin, gerçek (yasal) para birimleriyle iki yönlü etkileşim içerisinde olmaları, başka bir deyişle kolayca yasal para birimlerine dönüştürebilmeleri, onları, gerçek para birimi alternatifleri olarak kullanılabilmelerini kolaylaştırmaktadır.

Sonuç olarak, ceza hukukunu ilgilendiren olaylarda, kripto para birimlerinin, gerçek para birimlerinin alternatifi olarak kullanıldıkları varsayımının doğru bir yaklaşım olduğu kanaatindeyiz. Fakat ele alınan her olayda, ayrı ayrı değerlendirilmesi gereken, kullanılan kripto para biriminin kendine özgü nitelikleri,

¹⁹² Birinci bölümde örnek olarak verilen **Second Life** platformunda kullanıcıların sahip olduğu sanal mal ve ekipmanlar, sanal emtiaya örnektir.

kullanım amacı ve olayın diğer boyutlarının ortaya çıkarılması gerçek para birimi yerine kullanılıp kullanılmadığını belirleyecektir.

II. Kripto Para Birimleri Kullanımının Yasal Durumu

Kripto para birimlerinin kişiler arasında alım, satım, değiş tokuş ve mal veya hizmet alımlarında ödeme aracı olarak kullanılmasının yasal olduğunu belirten bir düzenleme olmadığı gibi bu işlemleri yasaklayıcı herhangi bir düzenlemenin de olmadığı görülmektedir. Başka bir ifadeyle kripto para birimi kullanımının ne lehine ne de aleyhine yasal bir düzenleme söz konusu değildir. Böyle bir durumda, hukuk devleti ilkesi ile Anayasa’da güvence altına alınmış “Suçta ve cezada kanunîlik ilkesi” gereği, yasal bir düzenlemeyle açıkça yasaklanmamış bir fiilin işlenmesi suç teşkil etmeyecektir. Bu nedenle Bitcoin gibi kripto para birimlerinin kullanımının önünde yasal engellerin olmadığı söylenebilir¹⁹³.

Kripto para birimi kullanımının TCK’de düzenlenmiş parada sahtecilik suçu bakımından değerlendirilen¹⁹⁴ Şen, bunun suç oluşturmayacağını belirtmektedir. Gerçekten de konuyla ilgili olarak TCK’de yer alan kamu güvenliğine karşı suçlar bölümünde, TCK m. 197’de düzenlenmiş parada sahtecilik suçu¹⁹⁵ bakımından, nelerin paraya eşit sayıldığı TCK m. 198’de açıklanmıştır. Buna göre, “Devlet tarafından ihraç edilip de hamiline yazılı bonolar, hisse senetleri, tahviller ve kuponlar, yetkili kurumlar tarafından çıkarılmış olup da kanunen tedavül eden senetler, tahviller ve evrak ile milli ziynet altınları, para hükmündedir”. Kripto para birimleri ne Devlet ne de yetkili kurumlar tarafından ihraç edilmedikleri için, parada sahtecilik suçu bakımından para sayılmazlar. Bu nedenle, kripto para birimi kullanımının, parada sahtecilik suçu kapsamında değerlendirilemeyeceği söylenebilir.

¹⁹³ Benzer görüş için bkz. Şen, a.g.y.

¹⁹⁴ A.g.y.

¹⁹⁵ **TCK Madde 197-** (1) Memlekette veya yabancı ülkelerde kanunen tedavülde bulunan parayı, sahte olarak üreten, ülkeye sokan, nakleden, muhafaza eden veya tedavüle koyan kişi, iki yıldan oniki yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.

(2) Sahte parayı bilerek kabul eden kişi, bir yıldan üç yıla kadar hapis ve adli para cezası ile cezalandırılır.

(3) Sahteliğini bilmeden kabul ettiği parayı bu niteliğini bilerek tedavüle koyan kişi, üç aydan bir yıla kadar hapis cezası ile cezalandırılır.

Türk Parası Kıymetini Koruma Mevzuatı bakımından da kripto para kullanımını engelleyen bir hususun olmadığı görülmektedir. Bilindiği gibi 1567 sayılı Türk Parasının Kıymetinin Korunması Hakkında Kanun, çerçeve kanun niteliğinde olup, Türk parası kıymetini koruma kapsamında öngörülen esaslar ve yaptırımlar, bu kanuna dayalı olarak çıkarılan Bakanlar Kurulu’nun 32 sayılı Türk Parası Kıymetini Koruma Hakkında Kararında düzenlenmiştir. Bakanlar Kurulunun bu kararında, Türk parası, döviz, kıymetli madenler, taşlar ve eşyalar, menkul ve gayri menkul kıymetler, krediler, gayrinakdi krediler, garantiler ile kefaletlere ilişkin düzenlemeler yer almakta olup, bunların ihracat ve ithalat rejimleri düzenlenmiştir. Kararda kripto para kullanımına uygulanacak elverişli bir hüküm yer almamaktadır¹⁹⁶.

Kripto para birimlerinin kara para aklama, vergi kaçakçılığı veya terörün finansmanı gibi devletlerin özel önlemler aldığı suçlarda kullanılması, bu sistemlerin sebep olduğu riskler bakımından uluslararası ve ulusal düzeyde tereddütlere sebep olmuşsa da, diğer çoğu ülke gibi Türkiye de bu konuda henüz yasal bir düzenleme yapmamıştır. Öyle görünmektedir ki getirilecek yasal düzenlemeler bu para birimlerinin gelişim süreçlerini nasıl tamamlayacaklarına bağlı olacaktır.

Ceza hukuku bakımından kripto para birimi sistemleriyle ilgili olarak sadece ulusal düzeyde yapılacak düzenlemelerin yeterli olmayacağı açıktır. Bu sistemlerde merkezî yönetim ve denetim birimleri olmaması ve para hareketlerinin farklı ülkelerde bulunan kimliği belirsiz kullanıcılar arasında çok kolaylıkla gerçekleştirilebilmesi, suçların önlenmesi ve suçluların ortaya çıkarılması için uluslararası yasal düzenlemelere ve işbirliğine gereksinim olduğunu göstermektedir¹⁹⁷.

Sonuç olarak, kripto para birimlerinin kullanımını yasaklayan bir hüküm Türk mevzuatında yer almamaktadır. Yukarıda ifade edildiği gibi hukuk devleti ve “suçta ve cezada kanunilik ilkesi” gereği, kanuni düzenlemelerle suç olarak düzenlenmemiş ve yaptırıma bağlanmamış fiillerin işlenmesi serbesttir.

¹⁹⁶ Aynı görüş için bkz. Şen, **a.g.y.**

¹⁹⁷ **A.g.y.**

§5. Bir Kripto Para Birimi Olarak Bitcoin

I. Bitcoin'in ortaya çıkışı

İlk kripto para birimi olan Bitcoin, 31 Ekim 2008 tarihinde Satoshi Nakamoto'nun¹⁹⁸ bir kriptografi elektronik posta grubunda “*Bitcoin: A Peer-to-Peer Electronic Cash System*” başlığıyla yayımlanan makalesiyle duyuruldu. Makalede, merkezî bir otoriteye dayanmayan, internet üzerinden erişilebilen eşler arası bir ağ (*peer-to-peer, p2p*) ortamında çalışan ve nakit paranın günlük hayatta gördüğü işlevi elektronik ticarete yerine getirmek üzere tasarlanmış, daha önce benzeri görülmemiş bir elektronik nakit para sistemi tanıtılmaktaydı.

Makalenin girişinde, elektronik ticarete finansal kuruluşların güvenilir üçüncü taraf olarak giderek artan ağırlığının maliyetleri artırdığı, bunun da günlük hayatta nakit para ile yapılan küçük meblağlı hareketlerin elektronik ortamda gerçekleşmesini zorlaştırdığı belirtilmektedir. Buna çözüm olarak, güven yerine kriptografik ispata dayanan ve iki tarafı bir aracı olmaksızın doğrudan karşı karşıya getiren bir elektronik ödeme sistemi önerilmektedir. Bu sistemde, *p2p* ağı üzerinde bulunan zaman damgalama sunucuları, bilgi işlem gücü harcayarak sağladıkları kanıtlarla, para hareketlerinin kronolojik sırasını belirleyecek ve böylece çifte harcama sorunu (*double spending problem*) çözülmüş olacaktır¹⁹⁹.

Makalenin devamında, önerilen sistemin teknolojik yapısını oluşturan bileşenler açıklanmaktadır. Elektronik para (*coin*), bir dijital imza zinciridir (*chain of digital signatures*). Böyle bir elektronik para sahibi olan kişi, daha önce gerçekleşmiş (kendisinin alıcı olduğu) bir para hareketinin *hash*'ini kendi özel anahtarı (*private key*) ile dijital olarak imzalar ve paranın bir sonraki sahibinin açık anahtarını (*public key*) ekleyerek yeni bir hareket kaydı oluşturur. Kendisine ödeme yapılan kişi,

¹⁹⁸ Satoshi Nakamoto, Japoncada “bilge” demek. Satoshi Nakamoto'nun SAMSUNG, TOSHIBA, NAKAMICHI ve MOTOROLA teknoloji şirketlerinin isimlerinden türetilme olduğu da iddia edildi. Amerika Güvenlik Ajansı'ndan (NSA) veya e-ticaret şirketinden bir grup uzmanın kod adı olduğu veya aralarında David Chaum, Hal Finney, Wei Dai, Gavin Andersen ve Finney'in komşusu Dorian Nakamoto olduğu kişilerin aslında Satoshi Nakamoto olduğu iddialar da arasında. Bu kişiler dışında farklı iddialarda adı geçenler: Vili Lehdonvirta, Michael Clear, Neal King, Vladimir Oksman, Charles Bry, Shinichi Mochizuki, Jed McCaleb ve Dustin Trammell. (Lam Pak Nian, David Lee Kuo Chuen, **Handbook of Digital Currency**, Editör: David Lee Kuo Chuen, ABD: Elsevier, 2015, s. 11 dipnot 1)

¹⁹⁹ Satoshi Nakamoto, **Bitcoin: A Peer-to-Peer Electronic Cash System**, <https://bitcoin.org/bitcoin.pdf>, Erişim tarihi: 3 Nisan 2018.

gönderilen paranın bir başkasına da gönderilmeyeceğinden nasıl emin olacaktır? Literatürde bu sorun çifte harcama problemi olarak bilinmektedir. Nakamoto'nun bu sorun için önerdiği çözüm iki adımlıdır: (1) Hareket herkese açıklanmalı ve (2) herkesin kabul edeceği hareket sırasını oluşturmak için zaman damgalayıcı sunucular kullanılmalıdır. Bu zaman damgalama sunucusu, para hareketlerinden oluşan bloğun *hash*'ini bulup ağda yayımlayacaktır. Her bir *hash*, bir önceki bloğun *hash*'ini de içerecek, böylece bir *hash*'ler zinciri oluşacaktır. Bu şekilde, zincire eklenen son *hash*, her zaman kendinden önceki bütün *hash*'lerin doğruluğunu da pekiştirecektir. Böyle *p2p* ağında konumlanmış dağıtık zaman damgası sunucusunu realize etmek için *hashcash* benzeri bir iş kanıtı (*proof-of-work*) kullanılmalıdır.

İş kanıtı, belli sayıda sıfır bit'inden oluşmuş bir *hash* değeridir ve sıfır içeren bit sayısı arttıkça, bu *hash*'i bulmak için gerekli bilgi işlem gücü üstel olarak artar. İş kanıtı, çoğunluğun kararını belirlemede de işe yarar. Her IP adresine bir oy hakkı tanımak, aynı kişinin birden fazla IP ile sisteme giriş yapabilmesinden dolayı istismara yol açabilir. Fakat iş kanıtının arkasında bulunan bilgi işlem (CPU) gücü sistemin sağlıklı çalışması için harcanan emeğin doğru bir göstergesidir. Eğer CPU gücünün çoğunluğu dürüst davranan düğümlerin (*node*) kontrolündeyse doğru zincir de sağlıklı olarak büyüyecektir. Bir saldırgan, geçmişe yönelik bir işlem yapmak için eski bir bloğu değiştirmek isterse, bu blok ile bu bloktan sonra zincire eklenmiş bütün blokların iş kanıtını tekrar hesaplamak zorunda kalacaktır. Yavaş bir saldırganın bunu başarma olasılığı, bloklar eklendikçe üstel olarak azalır²⁰⁰.

Nakamoto, sistemin oluşturduğu ağın yapacağı işleri şöyle sıralamaktadır: (1) Hareketlerin ağda bulunan bütün düğümlere iletilmesi, (2) yeni hareketlerin bir blokta toplanması, (3) blok için iş kanıtı bulmaya çalışması ve bulduğunda ağa iletilmesi, (4) yalnız geçerli ve daha önce harcanmamış hareketleri kabul etmesi ve (5) başka düğümler tarafından sunulan iş kanıtını kabul edip bu *hash*'i bir sonraki blok için kullanması. Düğümler, her zaman en uzun zincir üzerinde çalışmalıdır²⁰¹.

Nakamoto, para arzını, zincirin sağlıklı büyümesi için çalışan düğümlere belli bir miktar para ödülü verilmesi şeklinde tasarlamıştır. İş kanıtı sunan düğümler, CPU

²⁰⁰ Nakamoto, **a.g.m.**, s. 2.

²⁰¹ **A.g.m.**, s. 3.

zamanı ve elektrik enerjisi harcamaktadır. Bu emeğin karşılığı olarak verilen ödüle hareket ücreti de eklenebilir. Hareketin girdisi ile çıktısı arasındaki fark, hareket ücreti olarak kabul edilebilir²⁰².

Nakamoto, makalesinin geri kalan bölümlerini, tam düğüm yerine daha hafif bir sunucunun kullanmak isteyebileceği basitleştirilmiş ödeme doğrulama (*simplified payment verification, SPV*) sistemini, bir harekette birden fazla girdi ve birden fazla çıktıya imkân sağlayan mekanizmayı, sistemin sağladığı mahremiyeti ve bir saldırganın bir bloku değiştirebilmesinin üstel olarak azalan olasılığını açıklamaya ayırmıştır²⁰³.

Nakamoto'nun Bitcoin makalesi, referans sayfası dâhil toplam dokuz sayfaydı ve sistemin belli başlı bütün bileşenleri açıklanmıştı.

Bitcoin resmi internet sitesi olan *bitcoin.org* alan adı, 18 Ağustos 2008 tarihinde, internet alan adlarını kimliği belirsiz kişiler adına tescil etmeye imkân tanıyan *anonymousspeech.com* üzerinden Bitcoin'in ilk iki geliştiricisi Nakamoto ve Marti Malmi adlarına kaydedildi²⁰⁴.

Bitcoin projesi, 9 Kasım 2008 tarihinde açık kaynak kodlu projelere ev sahipliği yapan *SourceForge.net* sitesine kaydedildi²⁰⁵.

Nakamoto, 3 Ocak 2009 tarihinde ilk Bitcoin madenciliğini gerçekleştirdi ve *Genesis block* denilen ilk bloku oluşturarak bütün para hareketlerinin kayıtlı olduğu *blockchain* denilen blokzincirinin oluşumunu başlattı. Nakamoto, ilk blokta, hem sistemin açılış tarihini kayıtlayıcı hem de 2008 yılındaki büyük ekonomik krizi hatırlatıcı bir mesaj yerleştirmişti: “*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.*”²⁰⁶

Bitcoin yazılımı, kriptografi e-posta grubuna gönderilen e-posta ile, açık kaynak kodlu bir yazılım olarak, Nakamoto tarafından 9 Ocak'ta *SourceForge.org*

²⁰² A.g.m., s. 4.

²⁰³ A.g.m., s. 5-8.

²⁰⁴ <http://historyofbitcoin.org>, Erişim tarihi: 24 Mart 2018.

²⁰⁵ <http://historyofbitcoin.org>, Erişim tarihi: 24 Mart 2018.

²⁰⁶ İngiltere’de yayımlanan *The Times* gazetesinin 3 Ocak 2009 tarihli manşeti. Türkçe şu anlama gelmektedir: “Başbakan, bankalar için ikinci mali yardımın eşiğinde”

sitesinde yayımlandı. Dileyen yazılımı indirip sisteme dâhil olabilir ve madencilik yaparak bitcoin'ler kazanabilirdi.

Bitcoin sistemindeki ilk para transferi, 12 Ocak 2009 tarihinde, Nakamoto'nun kriptografi uzmanı Hal Finney'e 10 bitcoin (BTC) göndermesiyle gerçekleşti. Bitcoin'in ilk destekleyenler arasında, Finney ile birlikte, yukarıda bahsi geçen Wei Dai ve Nick Szabo da bulunmaktaydı²⁰⁷.

II. Bitcoin Sistemine Genel Bakış

Bitcoin sistemi, işleyişi bakımından güvenilir üçüncü bir taraf gerektirmeyen, başka bir deyişle kendi kendini yöneten ve denetleyen; para hareketlerini kriptografik yöntemlerle güvenilir kılan; ihraç edilen paraları, sistemin işleyiş güvenliğini ve devamlılığını sağlayan madencilere (*miners*) harcadıkları bilgi işlem gücü oranında dağıtma düzenine sahip ve arz olarak belli bir parasal üst limitle sınırlandırılmış (toplamda 21 milyon BTC ihraç edilecektir) bir kripto para birimi sistemidir.

Bitcoin, faaliyete geçtiği 2009 yılından bugüne pek uzun bir süre geçmemiş olsa da, öncüsü ve lideri olduğu kripto para birimlerinin bugün itibariyle toplam piyasa değeri 400 milyar ABD doları civarındadır ve kendisi de 156 milyar ABD doları ile bu pazarda %39 paya sahiptir²⁰⁸.

Bitcoin sisteminin para birimi olan bitcoin²⁰⁹ BTC veya XBT kısaltmaları ile gösterilmektedir. 1 BTC'nin 0.01 (yüzde bir) *centibitcoin* veya *bitcent*, 0.001 (binde bir) *millibitcoin* veya *millibit* (mBTC) ve 0.000001 (milyonda bir) *microbitcoin* veya *bit* (µBTC) denmektedir. Sistemde en düşük para birimi, sistemin kurucusu Satoshi Nakamoto'nun adıyla anılan ve 0.00000001 (yüz milyonda bir) BTC değerinde olan *satoshi*'dir.

Bitcoin sisteminde bugüne kadar arz edilen bitcoin sayısı yaklaşık 17 milyon BTC'dir. Sistemde 25 milyon civarında kullanıcı bulunmaktadır. 9 Şubat 2011

²⁰⁷ <http://historyofbitcoin.org>, Erişim tarihi: 24 Mart 2018.

²⁰⁸ <https://coinmarketcap.com/>, Erişim tarihi: 25 Nisan 2018.

²⁰⁹ “*Bitcoin*” deyimini sistemin bütünü için kullanılırken “*bitcoin*” sistemde kullanılan para birimi için kullanılmaktadır.

tarihinde ABD doları ile eşit parite yakalayan bitcoin, 2017 yılı sonlarında 20 bin ABD dolarına yaklaştı²¹⁰. Bugün itibariyle günlük işlem hacmi yaklaşık 1 milyon BTC'dir (10 milyar ABD doları). Bitcoin ağında gerçekleşen ortalama para hareketi (*transaction*) sayısı saniyede 2-3 arasındadır²¹¹.

A. Bitcoin Vakfı

Bitcoin sistemi etrafında bir araya gelen Bitcoin topluluğu, sistemin gelişimi ve kabulü için çaba gösteren kişilerden oluşmaktadır. Bitcoin vakfı (*Bitcoin Foundation*), kâr amacı gütmeyen ve Bitcoin topluluğu üyeleri arasında koordinasyonu sağlamayı, Bitcoin'in yararları ile ilgili farkındalık oluşturmayı ve ilgililere yol göstermeyi hedef edinen bir kuruluştur²¹².

B. Bitcoin Yazılımı

Bitcoin sistemini oluşturan ve aynı zamanda bir cüzdan uygulaması olarak da kullanılabilen *Bitcoin Core*, açık kaynak kodlu bir yazılımdır. Dileyen kişi *bitcoincore.org* adresinden indirerek, madencilik yapabilir veya para transferi gerçekleştirebilir. *Bitcoin Core* yazılımın ilk geliştiricisi de olan Satoshi Nakamoto, 2010 yılından itibaren bu yazılımın geliştirilmesi işini o tarihte artık belli bir sayısal büyüklüğe ve yetkinliğe erişen çekirdek yazılım ekibine bırakmıştır.

C. Topluluk Platformları

Bitcoin.org, Bitcoin topluluğu için ortak bir paylaşım ve kaynak platformudur. Bitcoin yazılımı ile ilgili geliştirici (*developer*) referans dokümanları bu sitede bulunmaktadır.

Bitcointalk.org sitesi, Bitcoin Forum adında topluluk için bir haberleşme ve tartışma platformu sunmaktadır. Geliştiriciler, madenciler ve diğer ilgili gruplar bu forumda Bitcoin ile ilgili paylaşımlarda bulunmaktadır.

²¹⁰ 4 Nisan 2018 itibariyle 1 BTC, 7128 ABD doları üzerinden işlem görüyor.

²¹¹ <https://coinmarketcap.com/currencies/bitcoin/>, Erişim tarihi: 26 Nisan 2018.

²¹² <https://bitcoinfoundation.org/>, Erişim tarihi: 25 Nisan 2018.

D. Bitcoin Geliştirme Önerileri

Bitcoin geliştirme önerileri, (*Bitcoin Improvement Proposals, BIP*), Bitcoin geliştiricileri tarafından, sisteme yeni özellikler katmak, mevcut eksiklikleri veya açıkları gidermek ve sistemi daha performanslı ve güvenli kılmak amacıyla Bitcoin topluluğunun görüş ve onayına sunulan önerilerden oluşmaktadır. Bu önerilerden kabul edilenler *Bitcoin Core* yazılımının yeni sürümlerinde uygulanmaktadır. Önerilerin kabulünde Bitcoin kullanıcıların rızaları aranmaktadır²¹³.

III. Bitcoin Ekosistemi

Bitcoin ekosisteminde kullanıcılar, madenciler, takas merkezleri, para transferi operatörleri ve yazılım geliştiriciler bulunmaktadır.

A. Kullanıcılar

Kullanıcılar, Bitcoin ağında sahip oldukları bitcoin'ler karşılığında gerçek ve sanal mal ve hizmetler satın almakta ve birbirlerine para transferleri gerçekleştirmektedirler. Bu kullanıcılar arasında, teknolojiyi yakından izleyenler, kriptografi veya mahremiyet savunucuları, hükümetlere güvenmeyenler, suçlular ve spekülâtörler bulunmaktadır. Kâr amacı gütmeyen *Wikileaks* gibi kuruluşlar da bitcoin bağışlarını kabul etmektedir. Sistemi yasadışı kullananların da olduğu bilinmektedir. Birçok çevrimiçi kumarhane ve yasadışı uyuşturucu satıcıları, sundukları hizmet ve ürünler karşılığında bitcoin kabul etmektedir. Son zamanlarda, bilgisayardaki verileri şifreleyip erişilmez kılan bilgisayar korsanları da şifreleri kaldırmak için bitcoin talep etmektedirler²¹⁴.

B. Takas Merkezleri

²¹³ Bitcoin geliştirme önerileri listesi için bkz. <https://github.com/bitcoin/bips>, Erişim tarihi: 25 Nisan 2018.

²¹⁴ Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency", *Hastings Science & Technology Law Journal*, C. IV, 2011, s. 165.

Gittikçe artan Bitcoin işlemlerini gerçekleştirmek için takas merkezleri veya borsalar, gerçek veya sanal para birimleri arasında değiş tokuşu sağlamakta, bu tür işlemlere birer ortam sağlamaktadırlar.

Çevrimiçi cüzdan hizmetleri sunan web siteleri, kullanıcıların bilgisayarlarına Bitcoin yazılımları kurmadan, Bitcoin adresleri oluşturma, para gönderme ve alma hizmetleri vermektedir.

C. Madenciler

Madenciler, özel olarak geliştirilmiş yazılım ve donanımlarla, kendi başlarına veya madenci havuzları oluşturarak, büyük bilgi işlem gücü gerektiren matematiksel problemler çözerek para hareket kayıtlarının, belli bir ücret karşılığı blokzincirine eklenmesini sağlamakta ve denetlemektedirler.

D. Yazılım Geliştiriciler

Yazılım geliştiricileri, Bitcoin'in açık kaynak kodlu yapısı etrafında, Bitcoin sisteminin gelişimine katkıda bulunmak veyahut yeni kripto para birimleri geliştirmek için çalışan kişilerden oluşmaktadır. Bunun yanında birçok web sitesi Bitcoin ve diğer kripto para birimleri için birer portal olarak faaliyet göstermekte ve Bitcoin ile diğer kripto para birimleriyle ilgili anlık ve istatistiksel bilgiler paylaşmaktadır.

IV. Teknolojik Yapı

Bitcoin sistemi, kendine özgü yeni teknolojik unsurlar geliştirmiştir. Bu bölümde Bitcoin sistemi oluşturan temel bileşenler ve bunların işleyişleri hakkında bilgi verilecektir.

A. Bitcoin Adresi

Bitcoin ağında kendisine para gönderilecek herkesin bir Bitcoin adresine sahip olması gerekir. Bitcoin adresi, normal bankacılık sisteminde kişilerin sahip olduğu hesap numarasına denk gelmektedir. Cüzdan uygulamalarıyla veya cüzdan hizmeti veren internet sitelerinden istenilen sayıda Bitcoin adresi oluşturulabilmektedir.

Bitcoin adresi, açık anahtar şifreleme tekniğiyle oluşturulmuş açık bir anahtarın *hash* değeridir²¹⁵. Bu açık anahtarın kendisinden türetildiği özel/gizli anahtar (*private key*), Bitcoin adresinden başka adreslere yapılan para transferlerini onaylamak için (dijital imzada) kullanılmaktadır.

Bitcoin adresi, 26-35 harf veya rakamdan oluşan bir dizidir. Güvenlik adına, her bir para transferi için farklı bir Bitcoin adresi kullanılması tavsiye edilmektedir. Günümüzde kullanılan cüzdan uygulamaları veya hizmetleri, her bir ödeme için farklı bir adres üretirler. Bu adreslerde harflerin büyüklüğü veya küçüklüğü önemlidir. Bu nedenle görüldüğü gibi kullanılmalıdır.

Bitcoin adresleri “1” veya “3” ile başlar. Geleneksel Bitcoin adresleri, açık anahtardan türetilen ve “1” ile başlayan adreslerdir ve *açık anahtar hash’ine öde* olarak (*pay-to-public-key-hash, P2PKH*) da bilinirler. Bu adreslerdeki bitcoin’leri başkalarına transfer etmek için ilgili gizli anahtar imzalarına ve açık anahtar *hash’lerine* ihtiyaç vardır. “3” ile başlayan Bitcoin adresleri, açık anahtarlardan türetilen adresler değildir ve script *hash’ine öde* (*pay-to-script hash, P2SH*) adresleri olarak bilinirler. Script adresi türüyle, para transferinde alıcı taraf, tekil adres yerine çok imzalı bir adres olarak belirtilmektedir²¹⁶.

Bitcoin adresleri karmaşık harf ve sayılardan oluştuğu için, içinde isim, marka veya başka bir tanıtıcı deyimlerin bulunduğu, (örnek: 1GSUAuXySSoYm6rH7XFZc6Hcy98zRZz) *vanity address*’ler de oluşturmak

²¹⁵ **Bitcoin adresi oluşturma:** ECC (Elliptic Curve Cryptography) tekniğiyle oluşturulmuş açık anahtar, bu tekniğin kullandığı eğri üzerindeki bir noktaya ait, 1 byte uzunluğundaki türü ve her biri 32 byte olan x ve y koordinat değerlerinden birleştirilmesinden oluşturulan 65 byte’lık bir bit dizisidir. Bu uzun sayı dizisinin SHA256 ile *hash*’i bulunur ve RIPEMD160 fonksiyonu ile tekrar *hash*’i alınır. Bu *hash* değeri, 20 byte uzunluğundadır. Bu değerin iki kere SHA256 fonksiyonu *hash*’i alınır ve bu çıktının ilk dört byte’ı alınıp, ilk *hash* işleminden elde edilen 20 byte’lık dizinin sonuna eklenir. Bu dizinin başına hangi ağda (bitcoin ağı veya test ağlarında kullanılmasını belirleyen) bir byte eklenir. Sonuçta elde edilen uzun sayısal değer, Base256 ile ve daha sonra Base58 ile kodlanır başka bir deyişle harf ve sayılara dönüştürülür. (Franco, **a.g.e.**, s. 74)

²¹⁶ Antonopoulos, **a.g.e.**, s. 81.

mümkündür. Bu tür adresler, genelde bilinen organizasyonlar veya hayır kuruluşları tarafından tercih edilmektedir. *Vanity* adresler, deneme yanılma yoluyla oluşturuldukları için çok fazla bilgi işlem gücü gerektirmektedir. Bunun için geliştirilmiş uygulamalar, hatta işlem havuzları²¹⁷ olmakla beraber, cüzdan uygulamalarından veya cüzdan hizmeti veren internet sitelerden böyle adresler temin etmek mümkün olmamaktadır. *Vanity* adres üretme hizmeti veren internet sitelerinden belli bir ücret karşılığı böyle bir adres elde etmek mümkündür²¹⁸.

B. Cüzdan

Kişilerin sahip oldukları bitcoin'ler onlara ait bilgisayarlarda veya depolama alanlarında saklı tutulmazlar. Bu bitcoin'ler *blockchain* denilen ortak defterikebirde bir hareket kaydı (*transaction*) olarak yer alırlar. Bu hareketlerde saklı tutulan bitcoin'leri harcamak veya bir başkasına transfer etmek için, yeni bir hareket kaydı oluşturup, gizli anahtar ile imzalamak gerekmektedir. Güvenlik açısından birden çok gizli anahtar kullanmak ve bunları başkalarının erişiminden korumak, hangi Bitcoin adresinde ne kadar bitcoin bulunduğunu hatırlamak, birden fazla adreste bulunan bitcoinleri tek bir hareket kaydında birleştirip başka bir hesaba göndermek gibi gittikçe artan bir karmaşayla baş edebilmek için, cüzdan (*wallet*) denilen uygulamalar kullanılmaktadır.

Cüzdan uygulamaları, genel olarak kullanıcıların Bitcoin ağıyla etkileşimde bulunduğu arayüzlerdir. Bu uygulamalar, genel kullanıcılar bakımından üç temel fonksiyonu yerine getirirler: (1) Bitcoin adresleri üretmek, (2) para hareketleri oluşturup Bitcoin sistemine gönderimi sağlamak ve (3) cüzdanın kontrolünde bulunan adreslere ait hareketleri blokzincirinden sorgulayıp ilgili hesap bakiyelerini göstermek. Bunun yanında para hareketinin gerçekleştiğinin (*confirmation*) belirlenmesi, gizli anahtarların yedeklenmesi (*backup*) veya yedeklenmiş gizli anahtarların geri yüklenmesi (*restore*) de cüzdan uygulamalarının yapabildiği işler arasındadır²¹⁹. Cüzdan uygulamaları, kontrol ettikleri gizli anahtarları simetrik-anahtar şifreleme tekniğiyle şifrelerler.

²¹⁷ Vanity adres üreten havuzlara bir örnek için bkz: <https://vanitypool.appspot.com/>, Erişim tarihi: 7 Nisan 2018.

²¹⁸ Antonopoulos, **a.g.e.**, s. 82.

²¹⁹ Barski, Wilmer, **a.g.e.**, s. 186.

1. Deterministik Cüzdanlar

Cüzdan uygulamaları, kontrol ettikleri anahtarların birbiriyle ilişkili olup olmamalarına göre ikiye ayrılmaktadırlar: Deterministik olmayan cüzdanlar (*nondeterministic wallet*) denilen cüzdanlarda, anahtarlar birbirinden bağımsızdır ve rastgele sayılardan üretilmektedir. Nakamoto tarafından geliştirilen ilk Bitcoin cüzdanı *Bitcoin Core Client* uygulaması, bu türün bir örneği olarak, kurulum aşamasında, birbirinden bağımsız yüz özel anahtar oluştuyordu²²⁰.

İkinci cüzdan türü olan deterministik cüzdanlarda (*deterministic wallet*), gizli anahtarlar, çekirdek (*seed*) denilen bir ana anahtardan (*master key*) türetildiklerinden birbiriyle ilişkilidirler ve sahipleri tarafından kaybedildiklerinde ana anahtar aracılığıyla tekrar üretilbilmeleri mümkündür. Deterministik cüzdanlar içinde en çok kullanıma sahip olan hiyerarşik deterministik cüzdanlar (*hierarchical deterministic wallet, HD wallet*), ile ağaç gibi hiyerarşik olarak ilişkili anahtarlar oluşturulabilmektedir. HD cüzdanlarıyla İngilizce belli kelimelerle kodlanabilen özel anahtarlar oluşturulabilir. Örneğin 0E7CE1A15917714D45F11E249D297E4A anahtarı, (*army claim van defense carry garbage jealous true echo media make crunch*) kelimeleriyle kodlanabilmektedir. Bu şekilde anahtarın kullanımı kolaylaşmaktadır.

2. Çevrimiçi Cüzdanlar

Cüzdanlar, internete bağlı olup olmamalarına göre çevrimiçi veya sıcak cüzdanlar (*online wallet, hot wallet*) ve çevrimdışı (*offline wallet*) olarak ikiye ayrılmaktadır²²¹. Bitcoin ağı ile etkileşimde bulunmak için internete bağlı olmak gerektiğinden, para hareketlerini gerçekleştirmek için, günlük işlemlerde çevrimiçi cüzdanlar kullanmak, başka bir deyişle, günlük işlemlerde kullanılan Bitcoin adreslerini çevrimiçi bağlantılı cüzdanlarda tutmak tavsiye edilmektedir. Bunun yanında, internete bağlı olmadığı için daha güvenilir bir ortam sağlayan çevrimdışı cüzdanlarda ise günlük işlem dışında kalan bitcoin'lere ilişkin gizli anahtarlar

²²⁰ Antonopoulos, **a.g.e.**, s. 94.

²²¹ Franco, **a.g.e.**, s. 126.

tutulmalıdır. Çevrimdışı cüzdanlar, para hareketlerini çevrimdışı olarak imzalayabilme özelliğine sahiptirler.

3. Soğuk Cüzdanlar

Soğuk cüzdanlar (*cold wallet*), gizli anahtarların internet erişimine açık olmadığı ortamlarda saklandığı cüzdanlardır. Burada saklanan özel anahtar ile bir hareketin onaylanması gerektiğinde, anahtar çevrimiçi veya çevrimdışı bir cüzdana aktarılmaktadır. Soğuk cüzdanlar, USB veya optik disk bağlantılı donanımlar olarak da geliştirilmişlerdir. Bu cihazlar dijital imzalama yeteneklerine sahiptirler ve sakladıkları gizli anahtarlar, sadece para hareketlerinin onaylanması aşamasında kullanılmaktadır.

4. Kâğıt Cüzdanlar

Kâğıt cüzdanlar (*paper wallet*), bir başka soğuk cüzdan türü olarak, özel anahtarların kâğıt üzerine yazılmaları veya QR kodu olarak basılmalarıyla oluşturulabilirler. Çevrimiçi veya çevrimdışı cüzdanlarda saklanan gizli anahtarların kâğıt üzerinde basımı yapılarak yedeklenmeleri güvenlik açısından önerilen bir önlemdir.

5. Cüzdan Hizmeti Veren Platformlar

Cüzdan hizmeti veren web siteleri de bulunmaktadır. Kullanıcıların ücretsiz kaydolabildiği bu sitelerin sağladığı hizmetlerle, Bitcoin adresi oluşturmak, para transferi gerçekleştirmek ve hesapların bakiyelerini takip etmek mümkündür. Kişilere ait gizli anahtarların güvenliğini internet sitesi sağlamaktadır. Fakat bu anahtarların, web sitesi veya bilgisayar korsanlarının saldırılarıyla ele geçirilmeleri mümkündür. Bu nedenle önemli meblağların tutulduğu adreslerin bu tür hizmetlerle sunulan cüzdanlar yerine soğuk cüzdanlarda tutulması tavsiye edilmektedir²²².

6. Beyin Cüzdanı

²²² A.g.e., s. 127.

Bu cüzdan seçenekleri dışında, beyin cüzdanı (*brain wallet*) denilen yaklaşımda, gizli anahtarlar veya onları oluşturan anahtar kelimeler bir yerlerde saklanmamakta, kullanıcıların hafızalarında tutulmaktadır²²³. Para transferi gerçekleştirileceği zaman, gizli anahtarlar gerçek cüzdanlara aktarılıp işlemler tamamlanmaktadır. Bu yaklaşımda, kişinin gizli anahtarını veya anahtarı oluşturan ana parolayı (*passphrase*) hatırlamaması tehlikesi söz konusudur.

Bitcoin sistemi için kullanılabilecek cüzdan uygulamalarının geneli açık kaynak kodlu olarak geliştirilen yazılımlardır. Masaüstü, mobil, web uygulaması veya donanım türünden önerilen Bitcoin cüzdan uygulamalarının ve cihazların listesine buradan²²⁴ ulaşılabilir.

C. Hareketler

Bitcoin sisteminde para birimi ihracı ve Bitcoin adresleri arası para transferleri, hareket (*transaction*) denilen işlem ile gerçekleştirilmektedir. Hareket, cüzdanlar veya bu hizmeti sunan web siteleri veya takas platformları aracılığıyla yapılabilmektedir. Kullanıcıların sahip olduğu bitcoin'ler, maddi birer fiziksel nesne veya kişisel bilgisayarlarının sabit disk ortamlarında saklanan fiziksel dosyalar şeklinde değil, günlük hayattaki muhasebe sistemlerinde defterikebir gibi işlev gören ve bütün hareket kayıtlarının tutulduğu ortak veri yapısında birer hareket kaydı olarak tutulmaktadır.

1. Hareket yapısı

Bir hareket kaydında, temel olarak iki bölüm vardır²²⁵: (1) Hareket girdisi; daha önce gerçekleşmiş ve harcanmamış bitcoin'lerin bulunduğu hareket kaydının referans numarası ve (2) hareket çıktısı; alıcı Bitcoin adresi ile transfer edilecek bitcoin miktarı. Hareket çıktıları, bir sonraki para transferi için hareket girdisi olarak kullanılacaktır. Alıcı, sahip olduğu bitcoin'leri harcamak veya başka birisine göndermek istediğinde yeni bir hareket kaydı oluşturacak ve hareketin girdi bölümüne bu hareketin kimlik numarasını referans olarak gösterecektir.

²²³ Barski, Wilmer, **a.g.e.**, s. 45.

²²⁴ <https://bitcoin.org/en/choose-your-wallet>, Erişim tarihi: 8 Nisan 2018.

²²⁵ Franco, **a.g.e.**, s. 78.

Yeni bir hareketin oluşturulması için, ilk önce kullanıcının bitcoin sahibi olması gerekir. Bu bitcoin, daha önce gerçekleştirilmiş bir hareketin çıktısında yer alır. Önceki hareketin çıktı kısmında alıcı Bitcoin adresi ve bitcoin miktarı yer alır.

Bir harekette birden fazla hareket girdisi seçilebilir. Örneğin 10 BTC gönderilmek istendiğinde farklı hareketlerde 4 ile 6 BTC varsa, bu iki hareketin kimlik numaraları, yeni harekette girdi referansları olarak gösterilebilir. Hareket girdisindeki toplam meblağın tamamının kullanılması gerekir. Örneğin hareket girdisinde 10 BTC varsa ve bunun 6 BTC'i başka birine gönderilmek isteniyorsa, girdide yer alan 10 BTC'nin tamamı kullanılır. Geri kalan 4 BTC, paraüstü (*change*) olarak, göndericiye ait Bitcoin adresine geri gönderilecek şekilde hareket çıktısında yer almalıdır. Aksi halde fark ne kadar büyük olursa olsun, hareket ücreti olarak kabul edilecek ve madenciye verilecektir. Bunun önüne geçmek için, bazı cüzdan uygulamaları, para transferlerinde girdi ile çıktı arasında fark olduğunda, otomatik olarak, yeni Bitcoin adresi üretilip harekette para üstünü göndericiye ait bu adrese gönderen bir çıktı oluşturmaktadırlar.

Hareket çıktısında, gönderilecek Bitcoin adresi ve bitcoin miktarı belirtilir. Birden çok hareket çıktısı oluşturmak da mümkündür. Para üstü olan hareketlerde zaten birden çok çıktı yer almaktadır.

2. Hareket Ücreti

Hareketin girdisi olarak gösterilen hareketlerdeki bitcoin miktarlarının toplamı hareketin çıktılarında gösterilen bitcoin miktarlarının toplamından fazla ise, bu fazlalık hareket ücreti veya masrafı (*transaction fee*) olarak kabul edilir²²⁶. Bu ücret, harekette yer almaz. Madenciler, bitcoin girdi toplamı ile çıktı toplamı arasındaki farkı, kendilerinin belirtecekleri bir adrese çıktı olarak gönderme hakkına sahiptirler. Madenciler blokzincirinin sağlıklı ve güvenli çalışmasını sağladıkları için, onlara bunun karşılığında teşvik amaçlı, cüz'i miktarda hareket ücreti bırakılabilmektedir. Ayrıca, sistemi gereksiz para hareketlerinden korumak için hareket ücretinin caydırıcı bir işlevi de vardır.

²²⁶ Narayanan ve diğ., **a.g.e.**, s. 78.

Hareket ücreti vermek zorunlu değildir. Fakat işlem Bitcoin ağına iletildiğinde, madenciler bunlardan bir blok oluştururken, hareket ücreti yüksek olanlara öncelik tanımaktadır. Bu nedenle hiç hareket ücreti içermeyen işlemlerin blokzincirine eklenmesi çok uzun zaman alabilmektedir. Nitekim yaptıkları işlemlerin blokzincirine hemen işlenmesini isteyen kullanıcılar, yüksek hareket ücretleri göstermelidir. Gösterilebilecek asgari hareket ücreti 1000 satoshi, başka bir deyişle 0.00001 bitcoin'dir.

3. Hareket Türleri

Hareket çıktısında, alıcı adresi olarak genellikle Bitcoin adresleri yer almaktadır. Bu tür hareketler, adrese öde (*pay-to-address*) hareketleridir ve mevcut hareketlerin %99'unu oluşturmaktadır. Bitcoin sisteminde, birden fazla kişi tarafından (*multisignature*) imzalanmak zorunda olunan veya adres yerine açık anahtara (*pay-to-public-key*, *P2PK*) veya belli bir algoritmaya sahip script'lerin kullanıldığı (*pay-to-script-hash*, *P2SH*) hareketler oluşturmak da mümkündür. Bunun dışında, Bitcoin blokzincirini farklı amaçlarla kullanmaya yarayan *OP_RETURN* hareketleri de oluşturulabilmektedir. Bir başka hareket türü olan *Coinbase transaction* veya *generation transaction* denilen, madencilerin blokzincirine ekledikleri blokta ilk hareket olarak ekledikleri para ihracı hareketi Madencilik bölümünde ele alınmaktadır.

4. Hareketin Onaylanması

Hareket, girdi ve çıktı bölümleri girildikten sonra hareketi gerçekleştiren kişi tarafından imzalanmalıdır. Kullanıcılar sahip oldukları gizli anahtar ile hareketi dijital olarak imzalarlar. Bu dijital imza, kişinin hareket girdileri üzerinde harcama yetkisine sahip olduğunu ve bu bitcoin'leri çıktıda gösterilen adreslere göndermek istediğini kanıtlamaya yaramaktadır. Dijital imzanın geçerliliği, hareketin doğrulanması aşamasında kontrol edilir. Ancak doğru dijital imzalarla sunulan hareketler geçerli olup bunun dışında sunulan hareketler veya yanlış dijital imzalı hareketler geçersizdir.

5. Hareketin Doğrulanması

Hareket, cüzdan uygulaması veya bu hizmeti veren web sitesi tarafından Bitcoin ağında yayımlanır. Her düğüm, aldığı hareketi, doğrulama işleminden geçirdikten sonra diğer düğümlere duyurur. Madenciler, bir sonraki blokta işlemek üzere, bu hareketleri doğrulayarak aday blokta (*candidate block*) toplar. Hareketin doğrulanması, her bir madenci tarafından bağımsız olarak yapılmaktadır. Bazı teknik kriterlerin dışında aşağıdaki koşulları sağlayan hareketlerin geçerli olduğu kabul edilir²²⁷:

- a) Hareketin sözdizimi (sentaks) ve veri yapısı düzgün olmalı,
- b) Hareket girdileri ve çıktıları boş olmamalı,
- c) Hareket büyüklüğü, azami blok boyutundan (1 MB) büyük olmamalı,
- d) Hareket çıktılarında belirtilen meblağlar, en az 0.0000054 BTC, en çok 21 milyon BTC arasında olmalı,
- e) Hareketteki her girdideki bitcoin daha önce harcanmamış olmalı,
- f) Hareketteki girdiler toplamı, çıktıları toplamından az olmamalı,
- g) Hareketteki her girdinin gösterdiği hareketin kilitleme script'inin (*locking script*) çıktı kilit açma script'i (*unlocking script*) ile uyduğu doğrulanmalı.

Hareketlerin blokzincirine işlenmesi için işlemden sonra belli bir sürenin geçmesinde fayda vardır. Genellikle hareketin bulunduğu bloktan sonra 6 blok daha eklendiğinde (yaklaşık bir saat), hareketin artık değiştirilemeyeceği kabul edilir²²⁸. Blokzincirine işlenmiş Bitcoin hareketleri geri alınamaz (*Irreversible transaction*). Bu sistemin temel özelliklerinden biridir. Hareketlerin geri alınamazlığı ile ilgili ayrıntılı açıklama Bitcoin güvenliği bölümde yapılacaktır.

D. Madencilik

Madencilik, Bitcoin para transferleri içeren hareketlerin (*transaction*) Bitcoin blokzincirine (*blockchain*) eklenmesidir. Hareketler, blokzincirine, blok denilen belli kümeler şeklinde eklenir. Blokzincirine blokların eklenmesi, aşırı bilgi işlem gücü

²²⁷ Antonopoulos, **a.g.e.**, s. 216.

²²⁸ Conti ve diğ., **a.g.m.**, s. 6.

gerektiren kriptografik problemlerin çözümüne bağlandığı için, bu işlem altın madenciliğine benzetilmiştir²²⁹.

Bitcoin sisteminde madenciler, her hareketin geçerli olup olmadığını, çifte harcama yapıp yapılmadığını, sistemin gereksiz yere boş hareketlerle meşgul edilip edilmediğini kontrol ederler ve uyguladıkları doğrulama yöntemleriyle sistemin omurgası niteliğindeki blokzinciri veri yapısının sağlıklı ve güvenli bir şekilde büyümesini sağlarlar²³⁰.

Altın madenciliğinde çalışan madencilere ücretlerinin altınla verilmesi gibi, blokzincirine yeni bir blok ekleyen Bitcoin madencisine de bitcoin verilmektedir. Bitcoin sisteminin erişime açıldığı 2009 yılında her bir blok ekleme için 50 BTC ödül verilirken, bugün²³¹ bu sayı 12,5 BTC'dir. Ödül miktarı her 210 bin blokta, başka bir deyişle yaklaşık olarak 4 yılda bir, yarılanmaktadır.

Bitcoin sisteminde para arzı, sadece blokzincirine blok eklendiğinde madencilere verilen ödüllerle sağlandığından, blok ödülü yarılanma algoritması doğrultusunda 2140 yılında para arzının sona ereceği ve toplam ihraç edilen para miktarının yaklaşık 21 milyon BTC'i bulacağı belirtilmektedir²³².

Blokzincirine yeni blok eklenmesi yaklaşık olarak 10 dakikada bir yapılmaktadır. 10 dakika ortalama bir süredir. Blokların 10 dakikadan daha kısa veya daha uzun bir sürede eklenmesi de mümkündür. Madencilerin hazırladıkları blokları blokzincirine eklemek için, çözmek zorunda oldukları problemin zorluk derecesi arttırabilir veya azaltılabilir olduğundan, blokların ortalama eklenme süresi 10 dakika olacak şekilde her blokzincirine 2016 blok eklenmesinin ardından otomatik olarak ayarlanmaktadır²³³. Sistemin ilk yıllarında düşük olan zorluk derecesi o kadar çok artmıştır ki, eskiden normal bir masaüstü bilgisayar ile Bitcoin madenciliği yapılabilirken, artık bu iş için geliştirilmiş özel donanımlar kullanılmaktadır.

²²⁹ Barski, Wilmer, **a.g.e.**, s. 162.

²³⁰ Franco, **a.g.e.**, s. 143.

²³¹ 9 Nisan 2018 tarihi itibarıyla.

²³² Antonopoulos, **a.g.e.**, s. 215.

²³³ **A.g.e.**, s. 260.

Bir madenci aynı anda birden fazla işlemi bir arada yürütmek durumundadır: Bir sonraki bloku, blokzincirine eklemek için o blok için kriptografik probleme çözüm bulmak; gelen yeni hareket kayıtlarını doğrulamak ve diğer düğümlere iletmek ve doğruladığı hareketleri, bir sonraki bloka dâhil edilmek üzere, bellek havuzu (*memory pool*) veya hareket havuzu (*transaction pool*) denilen geçici bir veri yapısında tutmak, bunlar arasındadır. Hareket havuzu, geçici bir bellek alanıdır ve daha önce bir bloka eklenmemiş hareketleri tutmaktadır. Hareketler yeni bloklara dâhil edildikçe bu bellek alanından silinirler²³⁴.

1. Blok Yapısı

Blokzincirine yeni blok eklendiği bilgisini alan madenciler, bu yeni eklenen blokun geçerli olduğu doğruladıktan ve hareket havuzunda tuttıkları hareketlerden bu bloka dâhil edilmiş olanları ayıkladıktan sonra, diğer madencilerle yarış içinde, hemen bir sonraki bloku oluşturmaya başlarlar. Bunun için hareket havuzundaki hareketler aday blok (*candidate block*) denilen ve henüz oluşum halinde bulunan bir blokta toplanır. Aday blokun başlığında (*block header*), bir önceki blokun kimlik numarası (*block id*), yaklaşık işlem zamanı, dâhil edilen hareketlerin kimlik numaralarını kapsayan ve hangi hareketin bu blokta yer aldığını hızlıca bulmak için kullanılabilecek Merkle ağacı (*Merkle tree*) *hash*'i, iş kanıtı (*work-of-proof*), iş kanıtını belirleyici hedef sayı ve iş kanıtının diğer madenciler tarafından kolayca doğrulanmasını sağlamak üzere kullanılan ve “*nonce*” denilen veri bulunur²³⁵. *Nonce*, iş kanıtı araştırılırken kullanılmış ve çözümü sağlayan sayıdır. Aday blokun gövdesinde para transferlerini içeren hareketler toplanır.

2. Coinbase Hareketi

Madenciler, üzerinde çalıştıkları bloklara ilk hareket olarak, *coinbase transaction* veya *generation transaction* denilen özel bir hareket ekleme hakkına sahiptirler. Bu hareket türü, para arzı olduğu için girdi kısmı (harcanacak hareket referansları) yer almaz. Hareketin çıktı kısmında ise, bloku hazırlayıp blokzincirine

²³⁴ Franco, **a.g.e.**, s. 110.

²³⁵ Narayanan ve diğ., **a.g.e.**, s. 88.

ekleyen madencinin belirlediği bir adres ile madenciliğin yapıldığı tarihte geçerli olan ödül miktarı (bugün için 12.5 BTC) vardır²³⁶.

3. İş Kanıtı

Her bir madencinin diğer madencilerden bağımsız olarak oluşturduğu aday blokunu blokzincirine eklemesi için bulduğu iş kanıtını da blok başlığına eklemesi gerektiği yukarıda belirtilmişti. Bitcoin sisteminde kullanılan iş kanıtının temelinde yukarıda anlatılan *hashcash* benzeri bir algoritma kullanılmaktadır. İş kanıtı, önceden belli olan zorluk derecesine göre belirlenmiş hedeften daha küçük bir sayının bulunması işlemine dayanır. Madenciler, işlemekte oldukları blokların başlıklarının *hash*'lerini bulur ve verilen hedeften küçük olup olmadığına bakarlar. Eğer bulunan sayı hedeften küçük değilse, "*nonce*" denilen sayıyı arttırır ve blokun *hash*'ini tekrar hesaplarlar. Bu işlem hedeften küçük bir sayı bulununcaya veya bir başka madencinin kendi geçerli blokunu Bitcoin ağına iletmesine kadar devam eder. Kendileri dışında başka bir madencinin geçerli bir blok eklemesi ve diğer madencilerin bu blokun geçerliliğini onaylaması üzerine, bütün madenciler, üzerinde çalıştıkları blok ekleme işini bırakıp yeni blok eklemeye başlarlar.

4. Blokzincirinin Çatallanması

Bitcoin sisteminde, farklı madenciler tarafından farklı blokların blokzincirine eklenmesi söz konusu olabilmektedir. Bu durum, çatal (*fork*) denilen, blokzincirinin farklı kollardan büyümesi anlamına gelmektedir. Bir madenci blokzincirine yeni bir blok eklediğinde, bunu hemen Bitcoin ağına iletir. Yeni bir blok eklendiği bilgisini alan madenciler, eklenen blokla sağlanan iş kanıtının geçerli olduğunu denetleyip doğruluğunu saptadıklarında, kendi iş kanıtı bulma işlemlerini yarıda kesip, bu blokun üzerine yeni bir blok eklemeye çalışırlar. Fakat aynı anda başka bir madenci de blokzincirine geçerli bir blok eklemiş ve bunu ağa iletmiş olabilir. Bu bilgiyi, diğer geçerli blok bilgisinden daha önce alan madenciler, bu bloku en son geçerli blok olarak kabul edip bunun üzerine yeni blok eklemeye çalışırlar. İşte bu durumda blokzincirinin çatallanması söz konusu olmaktadır. Genellikle çatallaşma çok uzun

²³⁶ A.g.e., s. 89.

sürmez, bir veya iki blok sonra çatallardan birinin uzunluğu diğerinden daha fazla olacak ve uzun blokzinciri çatalı esas blokzinciri olarak kabul edilecektir.

Blok uzunluğu, blok sayısı olarak ölçülmez bunun yerine zincirdeki toplam zorluk miktarı en uzun zinciri belirler. Aksi olsaydı, kötü niyetli bir madenci, düşük zorluk dereceli birçok blok oluşturarak en uzun zinciri oluşturabilir ve hile ile ödülü kazanan madenci olabilirdi²³⁷. Buradaki ölçüt, en çok onay alan blokzinciri çatallının esas blokzinciri olarak kabul edilmesidir. Madenciler için kazançlı olan, esas blokzincirine blok ekleyip ödül kazanmak olduğu için, blokzincirinin çatallaşması uzun sürmemektedir. Terkedilen çatalda yer alan bloklar öksüz/sahipsiz blok (*orphan block*) durumuna düşerler ve bu bloklara eklenip de blokzincirine işlenmemiş hareketler, sonradan eklenecek bloklarla blokzincirine işlenirler²³⁸.

5. Madencilik Türleri

Bitcoin madenciliği yapmak için bir yere kayıt olmak veya izin almak gerekmemektedir. Dileyen kişi açık kaynak kodlu ve ücretsiz olarak dağıtılan bir madencilik yazılımını indirerek madencilğe başlayabilir. Fakat Bitcoin sisteminde kullanılan iş kanıtı, yüksek bilgi işlem gücü gerektirmektedir. Her eklenecek blok başlığının *hash* değerini bulmak için çok büyük sayılarda *hash* fonksiyonu işlemi gerçekleştirmek gerekmektedir. Bugün bu sayı yaklaşık 30 milyon TH/s'dir. Böyle büyük bir bilgi işlem gücü ancak bu iş için özel olarak geliştirilmiş ASIC (Uygulamaya-özel bütünleşik devre / *Application-specific integrated circuit*) denilen özel donanımlardan büyük bir havuz oluşturarak sağlanabilmektedir. Sistemin ilk yıllarında mümkün olan masaüstü veya dizüstü bilgisayarlarla Bitcoin madenciliği, artık bu koşullar bakımından imkânsız görünmektedir. ASIC cihazlarına sahip olanlar da tek başlarına madencilik faaliyetinde bulunmamakta, kendi bilgi işlem güçlerini madencileri bir araya getiren havuzlara katmakta ve güçleri oranında, kazanılan bitcoin'lerden paylar almaktadırlar²³⁹.

Bitcoin madenciliği işinden kâr elde etmek için büyük bir bilgi işlem gücüne sahip olmak gerekmektedir. Bu gücü elde etmek, elektrik enerjisi ve soğutma

²³⁷ Franco, **a.g.e.**, s. 109.

²³⁸ Antonopoulos, **a.g.e.**, s. 240.

²³⁹ **A.g.e.**, s. 250.

maliyeti ortaya çıkardığından, yatırımcıların gelir ve gider hesabını iyi yapmaları gerekmektedir²⁴⁰.

6. Diğer İş Kanıtı Yöntemleri

Bitcoin sisteminde kullanılan iş kanıtından dolayı harcanan enerji, blokzincirinin güvenliğini sağlamak içindir. Bu kadar yüksek güç gerektiren bilgi işlem gücünü aşan bir hesaplama gücü kullanılmadan, blokzincirine müdahale edilemez. Bitcoin sistem güvenliğinin bu kadar pahalı sağlanması, diğer kripto para birimlerinde farklı iş kanıtı yöntemlerini kullanmaya yöneltmiştir.

Bu doğrulama algoritmalarından biri, pay kanıtı (*proof-of-stake*) yöntemidir²⁴¹. Bu yöntemde, yüksek bilgi işlem gücü gerekmez çünkü kimin hangi bloku blokzincirine ekleyeceği, ilgili para biriminden sahip olduğu sermayeye ve bu parayı elinde tutma süresine bağlıdır. Bu düzende kimin elinde sistemin desteklediği para birimi cinsinden ne kadar çok para varsa, onun blok ekleme başka bir deyişle yeni para arzına hak kazanma imkânı da o kadar artmaktadır. Pay kanıtının çevre dostu (az enerji harcanmasına neden olması), daha gevşek merkezi yapıda ve %51 saldırısına karşı caydırıcı olduğunu ileri sürenler, onun iş kanıtı yönteminden daha avantajlı olduğu iddia etmektedirler. Pay kanıtının blokzincirinin çatallanması durumunda yetersiz kalması ise yöntemin zayıflığı olarak ileri sürülmektedir. Bu yöntemi kullanan alternatif kripto para birimleri olarak *Peercoin*, *Ntx*, *Cunicula*, *Meni*, *Slasher* sayılabilir²⁴².

Bir başka doğrulama yöntemi, yakma kanıtı (*proof-of-burn*) algoritmasıdır²⁴³. Bu yöntemde, kullanıcı, sahip olduğu parayı, öyle bir adrese gönderir ki, bu para bir daha kesin olan harcanamaz, yakılmış olur. Bu yöntem, bir blokzinciri üzerinden yeni bir kripto para birimine geçişte mevcut kullanıcıların geçişlerini cazip hale getirmek amacıyla kullanılabilir. Bu yöntemde de enerji tüketimi gibi

²⁴⁰ Nirupama Devi Bhaskar, David Lee Kuo Chuen, "Bitcoin Mining Technology," **Handbook of Digital Currency**, s. 56.

²⁴¹ Narayanan ve diğ., **a.g.e.**, s. 234.

²⁴² Franco, **a.g.e.**, s. 235.

²⁴³ Narayanan ve diğ., **a.g.e.**, s. 83.

kaynakların kullanılmasına gerek yoktur. *Counterparty*, yakma kanıtı yöntemini kullanan kripto para birimi sistemleri arasındadır²⁴⁴.

E. Blokzinciri

Bitcoin sistemi ile ortaya konulan en önemli teknik yenilik, blokzinciri (*blockchain*) denilen ve para transferlerini içeren hareketlerden oluşmuş birer küme olan blokların zaman açısından kendinden önceki bloklara ardışık olarak bağlı oldukları bir veri yapısıdır. Blokzinciri mimarisi, eşler arası ağ üzerinden sağlanan dağıtık bir ortamda dijital para birimini gerçekleştirmenin en önemli bileşenidir²⁴⁵.

Blokzinciri, Bitcoin sisteminin merkezinde yer alır. Fakat belli bir merkezde tutulan ortak bir veritabanı olmak yerine, Bitcoin ağındaki tam düğüm olarak fonksiyon gören her bilgisayarın lokalinde birer kopyası tutulur. Bugün itibariyle²⁴⁶ depolama alanı olarak yaklaşık 164 GB büyüklüğünde olan Bitcoin blokzinciri, ortalama her 10 dakikada, azami büyüklüğü 1.000.000 byte boyutunda bir blokun eklendiği, tek yönlü büyüyen bir yapıdadır.

İlk blok olan *genesis block*, 0. blok olmak üzere; blok yüksekliği (*block height*), eklenen blok sayısını gösterir. Bir blokun, en son eklenen bloka göre pozisyonu da blok derinliğidir (*block depth*). Blokun referans ettiği bir önceki bloka, ana blok (*parent block*); en son eklenen bloka da blokzinciri başı (*blockchain head*) denilmektedir²⁴⁷.

Bloklar peş peşe eklendikçe, önceki blokun kimlik bilgisi (tekil *hash* değeri) de kendinden sonra eklenen blokta bulunduğundan, blokzincirinin toplam güvenliği zamanla daha da pekişmektedir. Çünkü önceki hareketleri değiştirmek için o hareketin yer aldığı bloktan başlayarak, ondan sonra eklenen bloka kadar sağlanan iş kanıtlarının toplamından daha fazla bilgi işlem gücü gerekecektir ve böyle bir saldırı,

²⁴⁴ Franco, **a.g.e.**, s. 197.

²⁴⁵ **A.g.e.**, s. 95.

²⁴⁶ <https://blockchain.info/tr/charts/blocks-size>, Erişim tarihi: 14 Nisan 2018.

²⁴⁷ Franco, **a.g.e.**, s. 140.

²⁵⁰ Antonopoulos, **a.g.e.**, s. 171.

Hareketlerin veya blokların doğrulanmasına ve ağda iletilmelerine aracı olurlar ve ağda diğer eşlerin bulunmasını ve onlarla bağlantılar kurulmasını sağlarlar.

Tam düğüm (*full node*) denilen düğümler, blokzincirinin güncel ve geçerli bir kopyasını lokallerinde tutarlar. Bu düğümler, hareket kayıtlarının doğrulanmasında, dışsal bir kaynağa ihtiyaç duymadan, kendi lokal blokzinciri kopyalarını kullanırlar. Bunun yanında bazı düğümler, blokzincirinin bir alt kümesiyle çalışırlar ve basitleştirilmiş ödeme doğrulama (*Simplified Payment Verification, SPV*) yöntemi ile hareketlerin doğrulanmasını sağlarlar²⁵¹.

Madenciler, yukarıda açıklandığı gibi, iş kanıtı sunarak blokların blokzincirine eklenmesini sağlarlar. Bazı madenciler, blokzincirinin lokal bir kopyasına da sahiptirler. Bunun yanında, blokzincirinin tamamını barındıran bir havuz sunucusuna bağlı olarak havuz madenciliğine katılan hafif düğümler (*Lightweight node*) de vardır.

Kullanıcı cüzdanları, tam veya hafif düğüm olabilirler. Bunlardan masaüstü cüzdanları genelde tam düğüm, mobil cüzdanlarda olanlar ise *SPV* düğümleridirler²⁵².

Bitcoin Core client uygulaması kullanan bazı büyük şirketler, madencilik yapmadıkları veya cüzdan hizmeti vermedikleri halde, blokzincirinin tam bir kopyasını tutarlar ve onu takas, cüzdan, blok gezgincisi ve ticari ödeme işlemcisi gibi sundukları birçok hizmette kullanırlar²⁵³.

Bitcoin ağı ile ilgili yapılan bir çalışmada²⁵⁴, Bitcoin düğümlerinin, nüfusun az olduğu veya gelişmemiş ülkeler dışında, bütün dünyada homojen biçimde dağıldığı saptanmıştır. 2014 yılına ait bu çalışmada, toplam 872.648 farklı IP adresine sahip Bitcoin düğümü saptanmış, bunlardan 6 bin civarında düğümün istikrarlı olduğu,

²⁵¹ A.g.e., s. 172.

²⁵² A.g.e., s. 173.

²⁵³ A.g.e.

²⁵⁴ Joan Antoni Donet Donet, Cristina Perez-Sola, Jordi Herrera-Joancomarti, "The Bitcoin P2P Network", **Financial Cryptography and Data Security**, FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers, Rainer Böhm, Michael Brenner, Tyler Moore, Matthew Smith (Eds.), Springer, 2014, s. 100.

sürekli biçimde ağına bağlı kaldığı belirtilmiştir. ABD ve Çin, bu ağdaki düğümlerin toplam %37'sini oluşturmakta, bu ülkeleri, Almanya, İngiltere ve Rusya takip etmektedir.

Bitcoin ağı ile ilgili istatistikler yayımlayan *bitnodes.earn.com* sitesine göre, son bir yıllık ortalamaya göre Bitcoin ağına 9852 düğüm faaliyet göstermektedir. Bu düğümlerin %24'ü ABD, %19'u Almanya, % 7'si Çin ve %6'sı Fransa'da faaliyette bulunmaktadır²⁵⁵.

G. Bitcoin Güvenliği

Bitcoin topluluğunda, sistemi genel olarak erişilmez kılacak veya blokzincirine işlenmiş ve artık bir daha değiştirilemeyeceği kabul edilen para hareketlerini değiştirebilecek çeşitli saldırılar tartışılmıştır²⁵⁶. Bitcoin sistemi, merkezî olmayan bir yapıda olduğu ve denetimsiz bir ortamda faaliyet gösterdiği için, saldırganlar için kolay bir av görünümündedir.

1. Çifte Harcama Sorunu

Bitcoin sistemini tehdit eden saldırıların başında çifte harcama sorunu (*double spending problem*) olarak nitelendirilen ve kötüniyetli birisinin sahip olduğu parayı birden fazla kez harcaması olarak özetlenebilecek sorun, sadece Bitcoin gibi kripto para birimlerine özgü olmayıp, bütün elektronik para birimleri için geçerli bir problemidir. Merkezî elektronik para birimlerinde bu sorun, kendi ekosistemlerinde gerçekleştirilen bütün para hareketlerinin tek bir elden ana hesap defterine işlenmesi zorunlu kılınarak çözülmüş olsa da merkezî olmayan kripto para birimi sistemlerinde çifte harcama sorununun çözümü daha karmaşık çözümler gerektirmiştir.

Bitcoin sisteminde çifte harcama yapılabilmesi örneği olarak: A, B'ye 5 BTC transfer eden bir hareket (H1) oluşturup blokzincirine işlenmesi için Bitcoin ağına gönderir. A, aynı zamanda, B'ye gönderdiği parayı tekrar kullanarak başka bir hareket (H2) oluşturup parayı kontrol ettiği başka bir hesaba gönderir. B, bazı

²⁵⁵ <https://bitnodes.earn.com/nodes/1523793781/#network-snapshot>, Erişim tarihi: 15 Nisan 2018.

²⁵⁶ Mauro Conti, Sandeep Kumar E, Chhagan Lal, Sushmita Ruj, **A Survey on Security and Privacy Issues of Bitcoin**, <https://arxiv.org/abs/1706.00916>, Erişim tarihi: 24 Nisan 2018.

madencilerin H1 kaydını blokzincirine işlediklerini görüp, A'ya istediği ürünleri gönderir. Bir grup başka madenci H2 hareketini içeren blokun blokzincirine eklenmesini onaylarlar. Bu şekilde H1 ve H2 hareketleri blokzincirinde farklı çatallardaki farklı bloklarda bulunurlar. Bu bloklardan H2 hareketini içeren blokun bulunduğu çatal (*fork*) esas blokzincirinin uzantısı olarak kabul edilirse, A, istediği ürünleri almış ve sözde ödemiş olduğu paraların tekrar kendisinde kalmasını sağlayarak B'yi aldatmış olur.

Çifte harcama saldırılarının başarısı, bilgi işlem kaynakları dışında, ağ iletim gecikmesi, satıcı, müşteri, Bitcoin takas hizmetleri bağlantı durumları veya Bitcoin ağındaki konumlanma ve dürüst madenci sayısı gibi farklı etkenlere bağlıdır. Kuşkusuz bir hareket kaydına ilişkin onay sayısı arttıkça, bu hareket kaydının sonraki safhalarda geçersiz olma ihtimali azalmakta ve böylelikle çifte harcama ihtimali de zayıflamaktadır²⁵⁷.

Bitcoin, çifte harcama sorununu gidermek için, blokzinciri mimarisini geliştirmiştir. Bu yapıda ancak tek yönlü para hareketi gerçekleşebilmektedir. Ekleme işlemi için iş kanıtı (*proof-of-work*) şartını yerine getirmek ve bu iş kanıtının diğer madencilerin çoğunluğu tarafından kabul edilmesi de şarttır. Bu çözüm yine de çifte harcama sorununu mutlak olarak çözmemekte, sadece ekonomik ve gerçekçi olmaktan çıkarmaktadır.

2. Kullanıcılar İçin Güvenlik Önerileri

Kullanıcılara, sahip olduğu bitcoin'leri için bazı güvenlik önlemleri almaları tavsiye edilmektedir. Bunlar arasında, gizli anahtarların fiziksel ortamlarda birden fazla yedeği olacak şekilde saklanması, donanımsal cüzdanlar kullanılması, daha sonra kendisinin dahi hatırlamayacağı çok karmaşık parolaların kullanılmaması, sahip olunan bitcoin'lerin ayrı ayrı birkaç Bitcoin adresinde tutulması, firmaların çok imzalı (*multisignature*) Bitcoin adresi kullanmaları ve beklenmedik durumlar için gizli anahtar bilgilerinin akraba veya avukat gibi diğer güvenilir birkaç kişiyle paylaşılması önerilmektedir²⁵⁸.

²⁵⁷ A.g.e., s. 11.

²⁵⁸ Antonopoulos, a.g.e., s. 273.

H. Diğer Kripto Para Birimleri

Bitcoin'in duyurulmasından sonra, özellikle 2013 yılından itibaren kripto para birimlerinin sayısı hızla artmıştır. Bu sayı günümüz itibarıyla 1591'dir²⁵⁹. Bu kadar çok sayıda kripto para biriminin piyasaya sunulmasının temel nedeni, kuşkusuz Bitcoin'in başarısıdır. Bunun yanında Bitcoin sisteminin açık kaynak kodlu bir yazılım oluşu, para birimi konusunda yeni projeler peşinde olan geliştiricilere, bu kodu alıp kendi projelerine uyarlama imkânı sağlamıştır. Yazılım geliştiriciler, Bitcoin'in ortaya koyduğu modeli izleyip, güttükleri amaçlara göre Bitcoin'e göre belli üstünlük taşıyan özellikler de ekleyerek kendi para birimlerini oluşturmuşlardır.

Bitcoin sisteminin bir çatalı konumunda olan para birimlerine, alternatif kripto para birimleri (*alternative cryptocurrency, altcoin*) denmektedir. Bunun yanında tamamen yeni bir yazılım mimarisine sahip kripto para birimlerine de *metacoin* denmektedir. Fakat her iki türdeki kripto para birimlerine *altcoin* denildiği de görülmektedir²⁶⁰.

1. Altcoin'ler

Kendisini, eşler arası internet para birimi olarak tanımlayan Litecoin²⁶¹, 2011 yılında eski bir Google çalışanı tarafından geliştirilmiştir. Bitcoin'in bir çatalı olan Litecoin'in Bitcoin'den üstünlüğü, para hareketi onaylanmasının hızlı olması (2.5 dakika) ve geliştirilmiş depolama verimliliğidir. Sistem iş kanıtı olarak daha az bellek alanına ihtiyaç duyan *scrypt* algoritmasını kullanmaktadır. Para birimi litecoin (LTC) olan sistemde toplamda 84 milyon LTC arz edilecektir²⁶². Günümüz itibarıyla 9 milyon ABD doları kripto para birimi pazar payına sahiptir²⁶³.

²⁵⁹ <https://coinmarketcap.com/all/views/all>, Erişim tarihi: 24 Nisan 2018.

²⁶⁰ Franco, **a.g.e.**, s. 171.

²⁶¹ Litecoin için bkz. <https://litecoin.org>, Erişim tarihi: 24 Nisan 2018.

²⁶² <https://litecoin.info/index.php/Litecoin>, Erişim tarihi: 24 Nisan 2018.

²⁶³ <https://coinmarketcap.com/coins/>, Erişim tarihi: 24 Nisan 2018.

Bir başka altcoin, 2012 yılında duyurulan²⁶⁴ ve blok ekleme yöntemi olarak iş kanıtı (*proof-of-work*) ve pay kanıtı (*proof-of-stake*) algoritmalarını melez olarak kullanan Peercoin'dir²⁶⁵. Bu sistemde, iş kanıtı ile eklenen bloklar, pay kanıtı ile eklenen bloklardan farklıdır. Pay kanıtı ile üretilen blokların eklenmesiyle elde edilen ödül, söz konusu para birimlerinin elde kalış süresi başka bir deyişle yaşına bağlı olarak değişmektedir²⁶⁶. %1 enflasyon farkından dolayı arz edilen paralar, pay kanıtına göre, sistemin güvenliğini sağlayan para ihraççılarına (*minter*) dağıtılmaktadır²⁶⁷. Peercoin'in para birimi PPC veya PPCoin ile gösterilmektedir. Sistemde para arzı için bir üst sınır belirlenmemiş olan Peercoin günümüz itibarıyla 68 milyon ABD doları kripto para birimi pazar payına sahiptir²⁶⁸.

Namecoin²⁶⁹, Bitcoin'in ilk çatalı olup, DNS gibi internet altyapı bileşenleri için merkezî olmayan, güvenilir, sansüre dirençli ve kişilerin mahremiyetini gözetten bir veri yapısı sunmaktadır. Aynı zamanda bir kripto para birimi olan Namecoin, Bitcoin'den farklı olarak, *merge-mining* denilen ve aynı anda birden fazla blokzincirine blok eklemeyi sağlayan bir yöntem kullanmaktadır. Para birimi NMC olan Namecoin'in diğer özellikleri (yarılanma süresi, ödül miktarı, toplam para birimi arzı, vd.) Bitcoin ile aynıdır²⁷⁰.

2. Metacoin'ler

Metacoin'ler, Bitcoin blokzinciri veya kendi blokzincirleri üzerinde dijital varlıklar, otonom ajanlar veya dışsal durum sözleşmeleri gibi yeni uygulamalar sağlayan kripto para birimi sistemleridir²⁷¹.

Colored coins (renkli paralar, jetonlar), basit bir metacoin protokol uygulaması olarak, Bitcoin para hareketlerini, harici bir varlığın oluşturulması veya devredilmesi için temsili olarak kullanabilmektedir. Burada söz konusu harici varlık, Bitcoin blokzinciri dışında var olan dijital bir varlık olabileceği gibi dış dünyaya ait herhangi

²⁶⁴ Sunny King, Scott Nadal, **PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake**, 2012, <https://peercoin.net/assets/paper/peercoin-paper.pdf>, Erişim tarihi: 24 Nisan 2018.

²⁶⁵ Peercoin için bkz. <https://peercoin.net/>, Erişim tarihi: 24 Nisan 2018.

²⁶⁶ Franco, **a.g.e.**, s. 174.

²⁶⁷ http://wiki.peercointalk.org/index.php?title=Main_Page#Peercoin, Erişim tarihi: 24 Nisan 2018.

²⁶⁸ <https://coinmarketcap.com/coins/>, Erişim tarihi: 24 Nisan 2018.

²⁶⁹ Namecoin için bkz. <https://namecoin.org/>, Erişim tarihi: 24 Nisan 2018.

²⁷⁰ Franco, **a.g.e.**, s. 75.

²⁷¹ **A.g.e.**, s. 195.

maddi bir varlık veya değer de olabilir. Dijital varlık örneği olarak, lisans, oyun, yazılım uygulaması gibi sanal mülkiyetler veya fikri mülkiyete konu her türlü nesne olabilir. Maddi varlıklar ise araba, arazi mülkiyeti, gemiler, uçaklar, vb. olabilir. Bu dijital veya maddi varlıklar, Bitcoin blokzincirinde, bitcoin hareketleri olarak temsil edilmektedir. Colored coins protokolleri, Bitcoin *script* dilinde kullanılan OP_RETURN komutu ile, dijital veya maddi varlığı blokzincirine metadata²⁷² olarak işlemektedir²⁷³.

Colored coins protokolü kullanımı için, *Open Assets* ve *Colu* gibi, Bitcoin blokzinciri üzerinde bu tür işlemler yapabilen cüzdan uygulamaları gerekmektedir²⁷⁴.

Bitcoin blokzincirini üzerine kurulu bir metacoin olan Counterparty²⁷⁵, dijital varlık oluşturmayı ve veri akışı yayınına sağlar. Bu yetenekleriyle dağıtık bir takas altyapısı oluşturur ve dijital nesnelerin ticaretini, yayımlanmış veri akışına dayalı olarak bahis ve fark sözleşmelerini mümkün kılar²⁷⁶. Counterparty ağı para birimi veya jetonu (*token*), XCP'dir. Counterparty hem bitcoin hem de XCP ile işlem yapabilmektedir. Sistemdeki mevcut 2.6 milyon XCP yakma kanıtı (*proof-of-burn*) ile 2014 Ocak ayında oluşturulmuştur ve ayrıca bir madencilik faaliyetine ihtiyaç duymamaktadır. Counterparty de, Coloured coins gibi Bitcoin *script* dili komutu OP_RETURN ile hareket kayıtları gerçekleştirir. Bugün itibariyle²⁷⁷ pazar değeri yaklaşık 55 milyon ABD doları olan Counterparty, 2 Ocak 2014 tarihinde duyurulmuştur²⁷⁸.

Ethereum²⁷⁹, 1994 doğumlu Vitalik Buterin'in 2014 yılında duyurduğu²⁸⁰, isteyen herkesin blokzinciri mimarisi üzerinde merkezî olmayan uygulamalar geliştirip kullanabileceği açık bir blokzinciri platformudur²⁸¹. "Blockchain 2.0" ve

²⁷² **Metadata:** Veri veya veri elemanları ile muhtemelen bunların tarifleri ve veri sahiplikleri hakkında bilgi veren, ayrıca erişim yolları, erişim hakları ve veri kayıp özelliği içeren veri. (TSE Bilişim Terimleri Sözlüğü, metadata md., s. 136.)

²⁷³ Antonopoulos, **a.g.e.**, s. 278.

²⁷⁴ **A.g.e.**, s. 279.

²⁷⁵ Counterparty için bkz. <https://counterparty.io/>, Erişim tarihi: 24 Nisan 2018.

²⁷⁶ Franco, **a.g.e.**, s. 197.

²⁷⁷ <https://coinmarketcap.com/currencies/counterparty/>, Erişim tarihi: 24 Nisan 2018.

²⁷⁸ <https://bitcointalk.org/index.php?topic=395761.0>, Erişim tarihi: 24 Nisan 2018.

²⁷⁹ Ethereum için bkz. <https://www.ethereum.org/>, Erişim tarihi: 24 Nisan 2018.

²⁸⁰ <https://bitcointalk.org/index.php?topic=428589.0>, Erişim tarihi: 24 Nisan 2018.

²⁸¹ Ethereum makalesi için bkz. <https://github.com/ethereum/wiki/wiki/White-Paper>, Erişim tarihi: 24 Nisan 2018.

yeni nesil blokzinciri teknolojisi iddiasıyla ortaya çıkan Ethereum sistemi, Ethereum Sanal Makinesi (*Ethereum Virtual Machine*) ile, kullanıcılara, istedikleri karmaşıklıkta kendi uygulamalarını geliştirme imkânı sağlamaktadır. Ethereum, bu özelliğiyle programlanabilir bir blokzinciridir.

Sistem, güven gerektirmeyen akıllı sözleşmelerin (*smart contracts*) kurulmasını sağlamakta ve eşler arası doğrudan etkileşimi otomatikleştirici veya bir ağda koordineli grup aksiyonlarını kolaylaştırıcı uygulamalar için uygun bir ortam oluşturmaktadır. Mesela eşler arası pazaryeri koordinasyonu veya karmaşık finansal sözleşmeler otomasyonu, Ethereum platformunda kullanılabilecek uygulamalara birer örnektir²⁸².

Ethereum sisteminde kullanılan para biriminin adı ether'dir. Kripto para birimler arasında, pazar payı olarak Bitcoin'den sonra ikinci sırada bulunan Ethereum'un bugün itibarıyla pazar değeri yaklaşık olarak 70 milyar ABD dolarıdır²⁸³.

2004 yılında duyurulan ve 33 milyar ABD doları pazar değeri²⁸⁴ ile kripto para birimleri arasında Bitcoin ve Ethereum'dan sonra üçüncü sırada yer alan Ripple²⁸⁵ aslında finansal bir ağıdır. Bu ağ, kullanıcılar arasında kredi hattı niteliğinde güven ilişkilerini oluşturmaktadır. Kullanıcılar arasında böyle bir ilişki kurulduktan sonra, Ripple protokolü, transfer edilmek istenen sermayeyi, güven zinciri boyunca dalga dalga (*ripple*) alıcıya ulaştırmaktadır. Modern Ripple ağı, sadece dijital varlıkları veya kripto para birimlerini değil, değerli madenler veya itibari paralar da dâhil olmak üzere her türlü varlığı ağ boyunca kullanıcılar arasında yönlendirebilmektedir. Ripple'ın kullandığı veritabanına *ledger* (defteri kebir) denmektedir. Bu veri yapısında bütün hesap sahiplerinin bakiyesi ve kredi limitleri bulunmaktadır. Ayrıca Bitcoin gibi bütün hareketler de tutulmaktadır²⁸⁶.

Ripple kullandığı para birimi *ripple* (XRP) veya *ripple kredisidir* ve 100 milyar üst sınırına sahiptir. Ripple ağında hesap bakiyeleri XRP, itibari para veya diğer

²⁸² <http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>, Erişim tarihi: 24 Nisan 2018.

²⁸³ <https://coinmarketcap.com/currencies/ethereum/>, Erişim tarihi: 24 Nisan 2018.

²⁸⁴ <https://coinmarketcap.com/currencies/ripple/>, Erişim tarihi: 25 Nisan 2018.

²⁸⁵ <https://ripple.com/>, Erişim tarihi: 25 Nisan 2018.

²⁸⁶ Franco, **a.g.e.**, s. 205.

dijital varlıklar halinde tutulabilmektedir. Ripple protokolü, dağıtık bir takas imkânı sunar. İsteyen kullanıcı, talimatını *ledger*'e bildirerek alış veriş işleminin otomatik olarak yapılmasını sağlayabilir. Ripple protokolü, yeni bir para birimi arzı gibi farklı dijital varlıkların oluşturulabilmesine de imkân tanımaktadır²⁸⁷.

V. Diğer Blokzinciri Uygulamaları

Bitcoin, bir kripto para birimi olmanın yanında, sahip olduğu blokzinciri teknolojisi sayesinde potansiyel farklı kullanımlara da imkân sağlamaktadır. Bu alternatif kullanımlardan bazıları yukarıda Coloured coins ve Ethereum bölümlerinde açıklandı.

Blokzincirinin, bir para birimi olarak kullanımı (örnek: Bitcoin) için “Blockchain 1.0”; akıllı sözleşmeler, kitlesel fonlama (*crowdfunding*) (Örnek: Ethereum), akıllı mülkiyetler (örnek: Coloured coins), finansal hizmetler sunan uygulamalar (Örnek: Ripple) için “Blockchain 2.0” ve para birimi, ekonomi ve piyasaların ötesinde devlet yönetimi, sağlık, bilim, edebiyat kültür ve sanat uygulamaları için “Blockchain 3.0” deyimi kullanılmaktadır²⁸⁸.

A. Akıllı Sözleşmeler

Akıllı sözleşmeler (*smart contracts*), Blockchain 2.0 uygulaması olarak, programlanabilir sözleşmeler şeklinde otonom, kendi kendine yeterli ve merkezî olmayan sözleşmelerin kurulmasına olanak tanımaktadır. Akıllı sözleşmelerin otonom yapısı, onların kurulduktan sonra artık dışarıdan müdahalelere gerek olmaksızın kendi kendilerine ifa edebilmelerini; kendi kendilerine yeterli olmaları ise kaynakları düzenleyebilmelerini ve merkezî olmamalarını başka bir deyişle, tekil bir merkezi sunucuya bağımlı olmamalarını ifade etmektedir. Akıllı sözleşmelerin tipik örneği, otomatlardır. Bu makineler, programlandıkları algoritmalara göre hareket etmektedirler²⁸⁹.

²⁸⁷ A.g.e., s. 206.

²⁸⁸ Melanie Swan, **Blockchain Blueprint for a New Economy**, ABD: O'Reilly, 2015, s. IX.

²⁸⁹ A.g.e., s. 16.

B. Dijital Varlıklar

Dijital varlık (*digital asset*), mülkiyeti dijital olarak kaydedilmiş ve doğrudan sahibi tarafından kontrol edilen bir varlık türüdür²⁹⁰. Bitcoin, böyle bir dijital varlık örneğidir. Bitcoin blokzincirinin merkezî olmayan sicil defteri yapısı, dijital varlık olarak tanımlanabilen fiziksel veya sanal varlıkların kaydedilebilmelerine ve kişiler arası transfer edilebilmelerine imkân sağlamaktadır. Yukarıda açıklanan Coloured coins, bu şekilde oluşturulmuş alternatif bir kripto para birimidir.

C. Kitlese Fonlama

Blokzinciri tabanlı kitlese fonlama (*crowdfunding*) platformları, aracı bir üçüncü taraf olmaksızın yeni proje sahiplerine kendi kripto para birimleri oluşturma imkânı sunmakta ve onların bu projelerin kriptografik hisselerini satmalarını sağlayarak fon toplayabilmelerini mümkün hale getirmektedirler²⁹¹.

D. Akıllı Mülkiyet

Akıllı mülkiyet, Bitcoin ile beraber tartışılan teknolojik yeniliklerden biridir. Akıllı mülkiyete konu olan varlıklar, Bitcoin blokzincirine erişip buradan elde ettiği bilgilere göre uygun aksiyonlar alabilme yeteneğine sahip otonom varlıklar olarak düşünülmektedir²⁹². Akıllı mülk olarak gösterilen tipik örnek, akıllı arabadır. Sahipliği blokzincirine işlenmiş olan akıllı araba, internete bağlanıp sahibinin kim olduğunu öğrenebilir ve buna göre sürüşe izin verebilir. Araba, blokzincirindeki sahibi bilgisi değiştiğinde, yeni sahibinin kontrolüne girebilir. Kiraya verilen akıllı araçlar da, blokzincirine işlemiş kiralayan, güzergâh, hız, mesafe gibi verilere dayalı olarak aksiyon alabilir.

E. Mikro Ödemeler

²⁹⁰ A.g.e., s. 15.

²⁹¹ A.g.e., s. 12.

²⁹² Franco, a.g.e., s. 185.

Bir başka blokzinciri uygulaması, mikro ödemelerdir (*micro payments*)²⁹³. Mikro ödemeler, işlem masrafı bakımından kredi kartı gibi mevcut ödeme kanallarıyla gerçekleştirilmesi ekonomik olarak uygun olmayacak kadar küçük meblağlardan oluşan ödemeleri ifade etmektedir. Bitcoin'in düşük hareket kaydı ücreti (*transaction fee*) “izlediğin kadar öde” TV yayıncılığı gibi mikro ödemeleri mümkün kılacak potansiyele sahiptir.

F. Dijital Noterlik

Dijital noterlik, blokzincirinin sağlayabileceği uygulamalardan biri olabilir. Bitcoin blokzincirine işlenmiş hareketlerin kalıcılığı ve değiştirilemezliği yanında zaman damgasına sahip oluşu, mevcut bir dokümanı, bu dokümana ait parmak izinin bir hareket olarak blokzincirine işlenmesini mümkün kılmaktadır. Böylece dokümanın blokzincirine işlendiği tarihte varlığına bir delil sağlanmış olur. Dokümandan başka, mesaj veya herhangi bir verinin bu şekilde varlığının kayıtlanması mümkündür²⁹⁴.

²⁹³ A.g.e., s. 186.

²⁹⁴ Antonopoulos, a.g.e., s. 278.

İKİNCİ BÖLÜM: CEZA HUKUKU BAKIMINDAN KRİPTO PARA BİRİMLERİ

Ş1. Kripto Para Birimi Kullanımının Türk Ceza Kanunu'nda Düzenlenen Suçlar Bakımından İncelenmesi

Bu bölümde TCK'de suç olarak düzenlenmiş suçlar bakımından kripto para biriminin kullanılması incelenecektir. Bu suçlar, Malvarlığına Karşı Suçlar, Bilişim Alanında Suçlar ve Adliye Karşı Suçlar bölümlerinde düzenlenmişlerdir. Suçların incelenmesinden önce her bölümde düzenlenen suçlarla ilgili genel kavramlar açıklanacaktır.

I. Malvarlığına Karşı İşlenen Suçlar

Malvarlığına karşı suçlar, 5237 sayılı Türk Ceza Kanunu'nda, ikinci kitabın ikinci kısmında yer alan *Malvarlığına Karşı Suçlar* başlıklı onuncu bölümde, 141 ilâ 169 maddeleri arasında düzenlenmiştir²⁹⁵.

Malvarlığına karşı suçlar, Anayasa'da *Kişi Hakları ve Ödevleri* bölümünde 35. madde'de güvence altına alınmış olan mülkiyet hakkının korunması amacıyla düzenlenmiştir. Bu bölümde düzenlenen yağma ve taşınmazdan yararlanmayı engelleme suçlarında, ayrıca kişi özgürlüğü ve güvenliği de korunmaktadır²⁹⁶.

²⁹⁵ Malvarlığına karşı suçlar bölümünde düzenlenen suçlar şunlardır: *hırsızlık suçu* (m. 141-147), *yağma* (m. 148-150), *mala zarar verme* (m. 151-152), *ibadethanelere ve mezarlıklara zarar verme* (m. 153), *hakkı olmayan yere tecavüz* (m. 154), *güveni kötüye kullanma* (m. 155), *bedelsiz senedi kullanma* (m. 156), *dolandırıcılık* (m. 157-159), *kaybolmuş veya hata sonucu ele geçmiş eşya üzerinde tasarruf* (m. 160), *hileli iflas* (m. 161), *taksirli iflas* (m. 162), *karşılıksız yararlanma* (m. 163), *şirket veya kooperatifler hakkında yanlış bilgi* (m. 164), *suç eşyasının satın alınması veya kabul edilmesi* (m. 165), *bilgi vermeme* (m. 166), (bu bölümde düzenlenen suçlar bakımından) *şahsi cezasızlık sebebi veya cezada indirim yapılmasını gerektiren şahsi sebep* (m. 167), *etkin pişmanlık* (m. 168), *tüzel kişiler hakkında güvenlik tedbiri uygulanması* (m. 169).

²⁹⁶ Doğan Soyaslan, *Ceza Hukuku Özel Hükümler*, 11. b., Ankara: Yetkin Yayınları, 2016, s. 360; Nevzat Toroslu, *Ceza Hukuku Özel Kısım*, 8. b., Ankara: Savaş Yayınları, 2015, s. 129; Mahmut

Yasal bir tanımı olmayan mülkiyet kavramı, Türk Medeni Kanunu'nda (TMK) sahibine “*hukuk düzeninin sınırları içinde o şey üzerinde dilediği gibi kullanma, yararlanma ve tasarrufta bulunma*” yetkileri veren bir hak olarak yer almaktadır²⁹⁷. Ceza hukukundaki mülkiyet kavramı, TMK'deki mülkiyet kavramı ile aynıdır²⁹⁸.

Mülkiyet kavramı, sahiplik bakımından özel hukuk kişilerinin sahip olduğu “özel mülkiyet/özel mülk” ile Devlet ve kamu kurum ve kuruluşlarının sahip olduğu “kamu mülkiyeti/kamu malı” olarak ikili bir ayrıma tabi tutulmaktadır. Bu ayrım, ceza hukuku bakımından önemlidir, çünkü kamu malına karşı işlenen suçlar için, özel mülkiyete karşı işlenen suçlara nazaran daha ağır yaptırımlar öngörülmüştür.

Özel mülkiyette, eşyanın tek kişiye ait olması durumunda kişi mülkiyeti, aynı eşya üzerinde birden fazla kişinin mülkiyetinin olması durumunda toplu mülkiyet söz konusudur. Bunun yanında toplu mülkiyet, belirli paylar şeklinde ise paylı mülkiyet²⁹⁹, herhangi bir pay olmaksızın bütünü üzerinde bir ortaklık şeklinde ise elbirliği halinde mülkiyet³⁰⁰ görünümü almaktadır. Mülkiyetin toplu veya bireysel olması, ceza hukuku açısından, ileride görüleceği gibi, -mesela hırsızlık suçu- önem arz etmektedir.

Mülkiyete göre üst bir kavram olan malvarlığında³⁰¹, mülkiyet ile beraber, zilyetlik, ayni haklar, fikri haklar ve alacak hakları yer almaktadır. Mülga 765 sayılı TCK'de “malvarlığı” yerine “mal” kavramı kullanılmaktaydı ve söz konusu suçlar

Koca, İlhan Üzülmöz, **Türk Ceza Hukuku - Özel Hükümler**, 3. b., Ankara: Adalet Yayınları, 2016, s. 509; Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, 15. b., Ankara: Seçkin Yayıncılık, 2017, s. 652; Nur Centel, Hamide Zafer, Özlem Çakmut, **Kişilere Karşı İşlenen Suçlar**, C. I, 4. b., İstanbul: Beta, 2017, s. 309.

²⁹⁷ **TMK Madde 683-** Bir şeye malik olan kimse, hukuk düzeninin sınırları içinde, o şey üzerinde dilediği gibi kullanma, yararlanma ve tasarrufta bulunma yetkisine sahiptir. Malik, malını haksız olarak elinde bulunduran kimseye karşı istihkak davası açabileceği gibi, her türlü haksız elatmanın önlenmesini de dava edebilir.

²⁹⁸ Veli Özer Özbek, M. Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Türk Ceza Hukuku Özel Hükümler**, 12. b., Ankara: Seçkin Yayıncılık, 2017, s. 593; Toroslu, **a.g.e.**, s. 125; Nurullah Aydın, **Türk Suç ve Ceza Hukuku**, 2. b., Ankara: Adalet Yayınevi, 2009, s. 262ç

²⁹⁹ **TMK Madde 668-** Paylı mülkiyette birden çok kimse, maddi olarak bölünmüş olmayan bir şeyin tamamına belli paylarla maliktir.

Başka türlü belirlenmedikçe, paylar eşit sayılır.

Paydaşlardan her biri kendi payı bakımından malik hak ve yükümlülüklerine sahip olur. Pay devredilebilir, rehnedilebilir ve alacaklılar tarafından haczettirilebilir.

³⁰⁰ **TMK Madde 701-** Kanun veya kanunda öngörülen sözleşmeler uyarınca oluşan topluluk dolayısıyla mallara birlikte malik olanların mülkiyeti, elbirliği mülkiyetidir. Elbirliği mülkiyetinde ortakların belirlenmiş payları olmayıp her birinin hakkı, ortaklığa giren malların tamamına yaygındır.

³⁰¹ Tezcan, Erdem, Önok, **a.g.e.**, s. 652; Koca, Üzülmöz, **a.g.e.**, s. 509; Aydın, **a.g.e.**, s. 262.

“*mal aleyhinde cürümler*” başlığı altında düzenlenmişti. Mal tek başına bir değer olmadığı, ancak sahiplik ile anlam kazandığı için Kanun malvarlığına karşı suçlar ifadesini benimsemiştir³⁰².

Ekonomik değeri olan ve paraya dönüştürülebilir bütün haklar ve borçlar malvarlığı olarak kabul edilmektedir³⁰³. Mülkiyetten doğan haklar ile ayni, fikri ve alacak hakları malvarlığının aktif kısmında yer alırken, kişinin borçları ve üstlendiği maddi yükümlülükler malvarlığının pasifini oluştururlar. Aktif varlıklar kişinin malvarlığı değerini arttırırken, pasif öğeler azaltırlar³⁰⁴.

Malvarlığı kavramının kapsamı, ceza hukukunda, medeni hukuktan daha geniş yorumlanmaktadır³⁰⁵. Malvarlığı ile genel olarak parasal veya ekonomik değere sahip tüm varlıklar anlaşılsa da, ceza hukuku bakımından, parasal veya ekonomik değere sahip olmayan fakat sahibi tarafından manevi değer atfedilen varlıklar da, malvarlığına dâhil kabul edilmektedir³⁰⁶. Ayrıca, medeni hukuka göre hayvan eşya veya mal olarak görülmezken, ceza hukukunda bakımından mal olarak kabul edilmektedir³⁰⁷.

Malvarlığına dâhil mallar, maddi varlığı olan mallar ile maddi varlığı olmayan mallar ayrımına tabi tutulmuştur³⁰⁸. Buna göre, kişilerin üzerinde hâkimiyet kurabildiği, ekonomik değeri olan, insan bedeni ve organı gibi kişisel olmayan, sınırlandırılabilen ve maddi varlığı olan mallar, maddi mal kavramına girer. Bunun yanında alacak hakları, doğalgaz, elektrik, enerji gibi maddi olmamakla birlikte üzerinde ayni hak kurulabilen mallar, maddi olmayan mallar olarak kabul edilmektedir³⁰⁹.

Medeni hukuktaki sahipli ve sahipsiz eşya ayrımı, ceza hukuku açısından önemlidir. Sahipsiz mallara -örneğin çöpe atılmış bir eşya- karşı, malvarlığına karşı

³⁰² Soyaslan, **a.g.e.**, s. 360.

³⁰³ Soyaslan, **a.g.e.**, s. 361; Toroslu, **a.g.e.**, s. 125.

³⁰⁴ Centel, Zafer, Çakmut, **a.g.e.**, s. 308.

³⁰⁵ Soyaslan, **a.g.e.**, s. 361; Toroslu, **a.g.e.**, s. 125.

³⁰⁶ Tezcan, Erdem, Önok, **a.g.e.**, s. 655; Soyaslan, **a.g.e.**, s. 361; Koca, Üzülmüş, **a.g.e.**, s. 523.

³⁰⁷ Tezcan, Erdem, Önok, **a.g.e.**, s. 655.

³⁰⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 308.

³⁰⁹ **A.g.e.**

suçların işlenmesi söz konusu olmaz. Çünkü bu mallar, kişilerin malvarlığına dâhil edilemezler.

İncelememizin bu bölümünde, Malvarlığına Karşı Suçlar bölümünde yer alan hırsızlık suçu (TCK m. 142-147), yağma (TCK m. 148-150), güveni kötüye kullanma (TCK m. 155), dolandırıcılık (TCK m. 157-159) suçlarının, kripto para birimlerinin suç konusu olabileceği durumlar bakımından bir değerlendirmesi yapılacaktır.

İnceleme konumuz olan kripto para birimleri, bilişim sistemleri üzerinde çalışan yapılar olduklarından, bunlara karşı işlenen mala zarar verme fiilleri, bu bölümde düzenlenen mala zarar verme suçu (TCK m. 151-152) kapsamında değil, suç konusu bilişim sistemi ve verileri olan ve ona göre daha özel bir norm olan TCK m. 244'teki "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçu kapsamında değerlendirilecektir. Bu nedenle incelememizde, mala zarar verme suçu yerine sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu ele alınmıştır.

A. Hırsızlık Suçu (TCK m. 141-147)

1. Genel Olarak

Hırsızlık suçu, 5237 sayılı Türk Ceza Kanunu'nda ikinci kitabın ikinci kısmında yer alan *Malvarlığına Karşı Suçlar* başlıklı onuncu bölümde, 141 ilâ 147. maddeleri arasında düzenlenmiştir. TCK m. 141'de hırsızlık suçunun basit hali, TCK m. 142 ve 143'te daha ağır cezayı gerektiren nitelikli haller ve TCK m. 144 ilâ 147 arasında ise cezada indirimle gidilecek haller düzenlenmiştir.

Hırsızlık suçunun temel şekli, "*zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verilir.*" olarak düzenlenmiştir.

2. Suçun Faili

Hırsızlık suçunun faili, maddede geçen “kimse” sözcüğünden de anlaşılacağı gibi, herkes olabilir³¹⁰. Bu nedenle hırsızlık, özgü suç niteliğinde değildir. Fakat malın sahibi, hırsızlık suçunun faili olamaz³¹¹. TCK m. 20’deki düzenlemeye göre, tüzel kişilere ceza yaptırımını uygulanamayacağından, bu suçun faili, tüzel kişiler de olamaz. Fakat TCK m. 169’da belirtildiği üzere, yararına haksız menfaat sağlanan tüzel kişiler hakkında tüzel kişilere özgü güvenlik tedbirlerine hükmolunur.

3. Suçun Mağduru

Hırsızlık suçunun mağduru olmak için farklı bir nitelik aranmamıştır. Bu nedenle zilyedi olduğu taşınır malı rızası dışında alınan herkes, hırsızlık suçunun mağduru olabilir³¹².

Özel hukuka ait bir kavram olan zilyetlik, TMK m. 973’te “*Bir şey üzerinde fiilî hâkimiyeti bulunan kimse onun zilyedir.*” şeklinde tanımlanmıştır. Madde metninde yer alan “şey” ifadesi hem taşınır hem de taşınmaz eşyayı kapsamaktadır. TMK m. 985’e göre, taşınır mallarda, zilyetlik mülkiyet için karine oluşturur. Bu nedenle, bir malı elinde bulunduran veya üzerinde fiilî tasarruf edebilme imkânına ve yetkisine sahip olan kişi o malın maliki sayılır. Fiilî hâkimiyet, malın kendisinin teslim edilmesi şeklinde olabileceği gibi, o mal üzerinde hâkimiyet kurmaya yarayan şeyin verilmesiyle de olabilir. Mesela otomobil üzerindeki zilyetliğin devri için anahtarının teslim edilmesi yeterlidir. Zilyetlik, mal üzerinde geçici sebeplerden dolayı tasarrufta bulunma imkânının ortadan kalkması ile kaybedilmez. Nitekim bu husus, TMK m. 976’da kayıt altına alınmıştır: “*Fiilî hâkimiyetin geçici nitelikteki sebeplerle kullanılamaması veya kullanma olanağının ortadan kalkması zilyetliği sona erdirmez.*”

Zilyetlikle ilgili olarak, medeni hukukta asli ve fer’i zilyetlik ile dolaylı ve dolaysız zilyetlik ayrımları vardır³¹³. Bir şey üzerinde sahip olunmak amacıyla fiilî

³¹⁰ Aydın, **a.g.e.**, s. 266.

³¹¹ Soyaslan, **a.g.e.**, s. 375; Koca, Üzülmüş, **a.g.e.**, s. 513.

³¹² Koca, Üzülmüş, **a.g.e.**, s. 514; Centel, Zafer, Çakmut, **a.g.e.**, s. 320.

³¹³ **TMK Madde 974-** Zilyet, bir sınırlı ayni hak veya bir kişisel hakkın kurulmasını ya da kullanılmasını sağlamak için şeyi başkasına teslim ederse, bunların ikisi de zilyet olur. Bir şeyde malik sıfatıyla zilyet olan aslî zilyet, diğeri fer’i zilyettir.

TMK Madde 975- Bir şeyde fiilî hâkimiyetini doğrudan doğruya sürdüren kimse dolaysız zilyet, başka bir kişi aracılığı ile sürdüren kimse dolaylı zilyettir.

hâkimiyet kurulmuşsa, o kişi o şeyin asli zilyedidir. Eşya üzerinde asli zilyet ile beraber bir başkasının zilyetliği de varsa, fer'i zilyetlikten bahsedilir. Örneğin, evini kiraya veren ev sahibinin, asli zilyet olarak ev üzerinde fiili hâkimiyeti devam ederken, kiracı fer'i zilyettir.

Medeni hukukta zilyetlik ile ilgili bir başka ayrım, dolaylı ve dolaysız zilyetliktir. Eşya üzerinde hâkimiyetini doğrudan sürdürebilen kişi dolaysız zilyet iken, bu hâkimiyeti kullanmak için bir başkasının aracılığına başvuran kişi dolaylı zilyettir³¹⁴. Ev sahibi - kiracı örneğinde, ev sahibi dolaylı zilyet iken, kiracı doğrudan zilyettir.

Bir kişinin bir eşya üzerinde zilyetliği, aynı veya şahsi bir hakka dayanıyorsa, hakka dayanan zilyetlik, fakat kişinin hiçbir aynı veya şahsi nitelikte bir hakkı olmamasına rağmen o eşya üzerinde fiili hâkimiyeti söz konusu ise –örneğin hırsızın çaldığı eşya üzerindeki zilyetliği-, bu durumda hakka dayanmayan (haksız) zilyetlik söz konusudur³¹⁵.

Zilyetlik ile ilgili bir başka önemli husus, zilyet yardımcılığı kavramıdır. Bir kişi, bir eşyayı zilyet olmak iradesi olmaksızın başka birisine hizmet etmek amacıyla fiilî hâkimiyeti altında bulunduruyorsa, bu kişi zilyet yardımcısıdır³¹⁶. Örneğin, patronunun otomobilini kullanan şoförün otomobil üzerinde zilyetlik iradesi yoktur ve patrona hizmet amacıyla aracı kullanmaktadır. Bu nedenle, otomobil şoförüne zilyet denilmez, zilyet yardımcısı denir.

Medeni hukuktaki zilyetlik kavramı ile ceza hukukunda zilyetlik kavramının aynı olduğunu ileri süren yazarlar olduğu gibi, ceza hukukunda zilyetliğin daha geniş anlaşılmasını gerektiğini savunan yazarlar da bulunmaktadır³¹⁷. Bu yazarların görüşüne göre, eğer medeni hukuktaki zilyet kavramı ceza hukukunda aynen benimsenirse, zilyet yardımcıları zilyet sayılmadığından, malın bu kişilerden çalınması durumunda, hırsızlık suçunun oluşmadığının kabulü gerekir ki, bu durum adaleti zedeleyecek sonuçlar doğuracaktır. Bu nedenle ceza hukukunda zilyetlik

³¹⁴ Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 66.

³¹⁵ **A.g.e.**, s. 62.

³¹⁶ **A.g.e.**, s. 66.

³¹⁷ Centel, Zafer, Çakmut, **a.g.e.**, s. 321; Soyaslan, **a.g.e.**, s. 369; Koca, Üzülmüş, **a.g.e.**, s. 536; Sulhi Dönmezer, **Kişilere ve Mala Karşı Cürümler**, 17. b., İstanbul: Beta Yayıncılık, 2004, s. 342.

kavramını, medeni hukuka göre zilyet olmamalarına rağmen, zilyet yardımcılarını da kapsayacak şekilde geniş yorumlamak gerekir.

Zilyet, malın sahibi başka bir deyişle asli zilyet olacağı gibi sadece fer'i zilyet de (mesela kiracı) olabilir. Sahiplik ve zilyetlik ayrıldığında, mağdur, zilyettir. Fakat malik ile mal arasında mülkiyet ilişkisi devam etmesi (malikin dolaylı zilyet olması) sebebiyle, malın sahibi, kamu davasında katılan olarak yer alabilmektedir.

Yukarıda belirtildiği gibi, zilyetliğin hukuka uygun olup olmaması, kişinin zilyetliğini değiştirmemektedir. Bu nedenle haksız zilyet de hırsızlık suçunun mağduru olabilir³¹⁸. Fakat taşınır malı kendisinden çalınan kişi, suçüstü veya suçun işlenmesinden hemen sonra, malını tekrar hırsızdan alırsa, bu davranış hırsızlık sayılmayacaktır³¹⁹.

Ölümle, ölenin terekesinde bulunan malvarlığı değerleri, mirasçılara geçtiğinden, bu hallerde işlenen hırsızlık suçunun mağdurunun ölenin mirasçıları olduğu kabul edilmektedir³²⁰.

4. Suçla Korunan Hukuki Yarar

Hırsızlık suçu, yukarıda belirtildiği gibi, Anayasada güvence altına alınmış mülkiyet hakkının korunması amacıyla düzenlenmiştir³²¹. Bu suçun düzenlenmesindeki hukuki yarar, sadece mülkiyetin korunması ile sınırlı tutulmamış, malın kullanma hakkını elinde bulunduranın (zilyedin) hukuki yararı da göz önüne alınmıştır³²².

5. Suçun Maddi Konusu

³¹⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 321.

³¹⁹ Ersan Şen, "Hırsızlık Suçları", **Ankara Barosu Dergisi**, 2012/3, 2012, s. 8.

³²⁰ Centel, Zafer, Çakmut, **a.g.e.**, s. 323.

³²¹ Tezcan, Ruham, Önok, **a.g.e.**, s. 653; Aydın, **a.g.e.**, s. 265.

³²² Özbek ve diğ., **a.g.e.**, s. 597; Soyaslan, **a.g.e.**, s. 373; Toroslu, **a.g.e.**, s. 30; Koca, Üzülmüş, **a.g.e.**, s. 515.

Hırsızlık suçunun konusu, başkasına ait taşınır maldır³²³. Taşınır mal, “*özüne zarar gelmeden bir yerden diğer bir yere taşınabilen*” eşyayı ifade etmektedir³²⁴. Taşınmaz mallar hırsızlık suçunun konusunu oluşturmazlar. Ceza hukukunda, bir malın taşınabilir olup olmadığı, medeni hukuktaki anlamından daha geniş yorumlanmaktadır. Buna göre, bir malın taşınabilirliğini belirleyen durum, sadece kanuni tanımı değil, onun fiilî olarak taşınabilir olup olmamasıdır³²⁵. Hareket ettirilebilen her eşya, taşınabilir maldır³²⁶. Mesela, bir binadan sökülüp götürülen pencere çerçeveleri, cami kubbesinden sökülen kurşunlar, hırsızlık suçunun konusunu oluşturabilmektedir³²⁷. Menkul değerlerler taşınır mal olarak kabul edilmektedir³²⁸.

Malın başkasına ait olması, medeni hukuka göre belirlenecek bir husustur³²⁹. Mal, mülkiyetine sahip olan kişiye aittir. Fakat malın maliki ile zilyedinin farklı olması durumunda, “başkasına ait olma”, zilyetliği elinde bulundurana ait olma şeklinde anlaşılmalıdır³³⁰.

Mülkiyete elverişsiz mallar, sahihsiz mallar, terk edilmiş mallar ve vahşi hayvanlar, hırsızlık suçunun konusunu oluşturmazlar³³¹.

Paylı veya elbirliği mülkiyeti ile birden çok maliki bulunan bir mal üzerinde, maliklerden birisi tek başına tasarrufta bulunamaz³³². Böyle bir tasarruf söz konusu olsa, fail bakımından hırsızlık suçu gerçekleşir. Fakat yasada bu tür bir hırsızlık suçu için, şikâyet şartı aranmış ve daha az bir yaptırım öngörülmüştür (TCK m. 144/1-a).

İncelememiz açısından kripto para birimlerinin de dâhil olduğu bilişim verilerinin taşınır mal sayılıp sayılmaması önem arz etmektedir. Mülga 765 sayılı

³²³ Koca, Üzülmöz, **a.g.e.**, s. 513; Dönmezer, **a.g.e.**, s. 356; Aydın, **a.g.e.**, s. 266.

³²⁴ M. Kemal Oğuzman, Özer Seliçi, Saibe Oktay-Özdemir, **Eşya Hukuku**, 19. b., İstanbul: Filiz Kitabevi, 2016, s. 10.

³²⁵ Centel, Zafer, Çakmut, **a.g.e.**, s. 327; Koca, Üzülmöz, **a.g.e.**, s. 523.

³²⁶ Özbek ve diğ., **a.g.e.**, s. 601; Soyaslan, **a.g.e.**, s. 375.

³²⁷ Centel, Zafer, Çakmut, **a.g.e.**, s. 328.

³²⁸ Zeki Hafizoğulları, Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar**, 1. b., Ankara: US-A Yayıncılık, 2017, s. 331.

³²⁹ Özbek ve diğ., **a.g.e.**, s. 601; Koca, Üzülmöz, **a.g.e.**, s. 522.

³³⁰ Centel, Zafer, Çakmut, **a.g.e.**, s. 328.

³³¹ Koca, Üzülmöz, **a.g.e.**, s. 526; Hafizoğulları, Özen, **a.g.e.**, s. 332; Centel, Zafer, Çakmut, **a.g.e.**, s. 329; Dönmezer, **a.g.e.**, 363-365.

³³² Centel, Zafer, Çakmut, **a.g.e.**, s. 330.

eski TCK'nin yürürlükte olduğu dönemde, elektrik ve doğalgaz hırsızlığında, bunların taşınır mal kavramına dâhil olup olmadıkları doktrinde çokça tartışılmaktaydı. Taşınır mal kavramının lafzi yorumu bunların taşınır mal olarak kabulüne imkân vermemekteydi. Dolayısıyla doktrinde kimi yazarlar, bunları çalma şeklinde gerçekleşen eylemlerin, hırsızlık suçu olarak nitelendirilmesini suçta ve cezada kanunîlik prensibine aykırı bulmaktaydılar. Kanunkoyucu, 1991 yılında 3756 sayılı Kanunla, hırsızlık suçu maddesine (TCK m. 491) “*Ekonomik bir değer taşıyan her türlü enerji de taşınabilir mal sayılır.*” şeklinde ek bir fıkra getirerek, bu konudaki tartışmalara son vermişti. Benzer bir tartışma bugün “bilgi verisi” konusunda yaşanmaktadır. Bu konudaki tartışmalara aşağıda yer verilmiştir.

Mevzuatımızda veri kavramı, 23.05.2007 tarihinde Resmi Gazete’de yayımlanan 5651 sayılı *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*’un tanımlar başlıklı ikinci maddesinin 1-k fıkrasında tanımlanmıştır. Bu tanıma göre veri, “*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri*” ifade etmektedir³³³.

Şen, bilgisayarda kayıtlı her türlü program, bilgi ve verilerin, sahibinin veya kullanıcısının izni olmaksızın alınması, kopyalanması veya bir başka yere gönderilmesi fiillerinin, kanunda açık olarak düzenlenmediği için, suçta ve cezada kanunilik ilkesi gereği, hırsızlık suçuna konu olamayacağını öne sürmektedir³³⁴.

Dülger, bilişim verilerinin, ne somut bir nesne ne de elektrik enerjisi olduğunu vurgulamakta³³⁵, yaşanan bilgi çağının bir gereği olarak verilerin hırsızlık suçuna konu olabileceğini ifade etmektedir³³⁶. Yazar, verilere karşı hırsızlık suçunun bağımsız bir suç tipi olarak düzenlenip suç konusu ve suç konusuna yönelik fiillerin açıkça gösterilmesinin, uygulamada ortaya çıkabilecek tereddütleri gidereceğini öne sürmektedir³³⁷.

³³³ Bilişim sistemleri, veri ve diğer ilgili kavramlarla ilgili detaylı açıklamalar *Bilişim Alanında Suçlar* başlığı altında yapılacaktır. Bkz. s. 152.

³³⁴ Şen, **a.g.m.**, s. 5.

³³⁵ Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 5. b., Ankara: Seçkin Yayıncılık, 2014, s. 549.

³³⁶ **A.g.e.**, s. 552.

³³⁷ **A.g.e.**, s. 550.

Mahmutoğlu, bilişim sistemi kullanmak yoluyla hırsızlık suçunun oluşabileceğini, burada verinin, hırsızlık suçunun konusunu oluşturmadığını fakat suçun tamamlanması bakımından araç niteliğinde olduğunu ifade etmektedir³³⁸.

Özbek, hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlendiği iddia edilen her durumda suç konusunun taşınır bir mal değil, veri olduğunu ve TCK m. 244'teki düzenlemeler karşısında hırsızlık suçunun oluşmayacağını ileri sürmektedir³³⁹.

Soyaslan, bilişim sistemlerindeki verilerin değiştirilmesi veya başka yere transfer edilmesi veyahut bu sistemlere veri eklenmesi şeklinde hırsızlık suçunun işlenebileceği görüşüne katılmamaktadır. Yazara göre bu eylemler, TCK m. 244 kapsamında değerlendirilmelidir³⁴⁰.

Yurtcan, bilişim sistemindeki verilerin, (örneğin bir CD aracılığıyla), başka bir bilgisayara aktarması durumunda hırsızlık suçunun oluşacağını, fakat bunun dışında, TCK m. 244'te sayılan fiillerle bilişim sistemine karşı işlenen fiillerin bu madde (TCK m. 244) kapsamında ele alınması gerektiğini ileri sürmektedir³⁴¹. Yazara göre, fail, verileri başka bir yere göndermiş olsa bile, bu veriler mağdurun sisteminde kayıtlı kalmakta, bu nedenle hırsızlıkta olduğu gibi taşınır malın alınması, bu mal üzerinde mağdurun tasarruf yetkisine ve zilyetliğine son vermemektedir³⁴².

Koca ve Üzülmmez, verinin hırsızlık suçuna konu olabilmesi için, dış dünyada maddi bir bünyeye sahip bir eşya ile ilgili olması, bir başka deyişle para, hisse senedi ve altın gibi cismani nitelikte taşınır bir malı temsil etmesi gerektiğini öne sürmüşlerdir³⁴³.

³³⁸ Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi," **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası (İÜHF)**, C.71/1, 2013, s. 27.

³³⁹ Veli Özer Özbek, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.9/Özel Sayı, 2007, s. 40.

³⁴⁰ Soyaslan, **a.g.e.**, s. 388.

³⁴¹ Erdener Yurtcan, **Yargıtay Kararları Işığında Malvarlığına Karşı Suçlar**, 2. b., İstanbul: Adalet Yayınevi, 2015, s. 39.

³⁴² **A.g.e.**

³⁴³ Koca, Üzülmmez, **a.g.e.**, s. 837.

Erdoğan, verinin taşınır mal olmadığını ve bu yüzden hırsızlık suçunun konusunu oluşturmayacağını belirtmektedir³⁴⁴.

YCGK, 17.11.2009 tarihinde verdiği kararda³⁴⁵ internet bankacılığı şifresinin ele geçirilip hesaptaki paranın başka bir hesaba gönderilmesinde suç konusunun veri olmadığını, verinin temsil ettiği para olduğunu belirtmiş ve bu eylemi bilişim sistemi kullanmak suretiyle hırsızlık suçu kapsamında değerlendirmiştir.

Yargıtay'ın bu kararı, şüphesiz fiziksel yapıda olmayan ve internet üzerinden erişilebilen bilişim sistemleri üzerinde sadece veri olarak bulunabilen kripto para birimleri için önemlidir. Fakat Yargıtay'ın doğrudan kripto para birimleriyle ilgili bir kararı henüz yoktur. Doktrinde ise Şen bu konuda aşağıdaki özetlenen görüşleri içeren bir çalışmada bulunmuştur.

Şen, söz konusu yazısında³⁴⁶, kripto para birimlerinden Bitcoin'e karşı hırsızlık suçunun oluşup oluşamayacağını ele almıştır. Yazar, Bitcoin'i, malvarlığına dâhil olup aktif artıran, kaybı halinde pasifi çoğaltan, banka veya reel borsa yerine internet üzerinden erişilebilen sanal ortamda tutulan para olarak tanımlamaktadır. Bitcoin, internet ortamında alınıp satılabilmekte, ürün satışlarının karşılığı olarak alıcı tarafından satıcıya ödenebilmekte ve internet ortamında bulunan borsalar aracılığıyla tedavülde olan para birimlerine çevrilebilmektedir. Yazara göre, Bitcoin hırsızlık suçuna konu olabilir, zira TCK m. 142/2-e'deki bilişim sistemi kullanarak hırsızlık suçu düzenlenmesi, hırsızlığın internet gibi sanal ortamlarda da işlenebileceğini öngörmüş ve sanal ortamda kayıtlı malvarlığı değerlerini de koruma altına almıştır.

Bununla birlikte Yargıtay, mağdurun rızasına aykırı olarak gerçekleşen telefon kontörü transferini, hırsızlık suçu kapsamında ele almayıp TCK m. 244/4'e göre değerlendirmiştir. Telefon kontörünün banka nezdindeki hesapta bulunan para gibi, elde edilmesiyle malvarlığının aktifini arttırması ve kaybıyla malvarlığının pasifini çoğaltması, başka bir deyişle ekonomik bir değere sahip olması, Yargıtay tarafından

³⁴⁴ Yavuz Erdoğan, **Türk Ceza Kanunu'nda Bilişim Suçları**, 1. b., İstanbul: Legal, 2013, s. 289.

³⁴⁵ YCGK, 17.11.2009, 2009/11-193 E., 2009/268 K. Bu karar ile ilgili tartışmalar için bkz. s. 157.

³⁴⁶ Ersan Şen, **Bitcoin Çalınır mı?**, <http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1948163-bitcoin-calindir-mi>, Erişim tarihi: 9 Temmuz 2018.

söz konusu eylemin hırsızlık suçu kapsamında değerlendirilmesi için yeterli bulunmamıştır³⁴⁷.

Yargıtay, internet üzerinden geniş kesimlerce oynanan çevrimiçi oyunlarda kullanıcılar arasında ekonomik değeri olan sanal karakter ve eşyaların bir başkasına gönderilmesi eylemini, hırsızlık suçu olarak değil, TCK m. 244/4 kapsamında değerlendirmektedir³⁴⁸.

Alman Ceza Kanunu'na göre Bitcoin gibi kripto para birimlerine karşı gerçekleştirilen çalma eylemlerinin, hırsızlık suçu kapsamında değerlendirilip değerlendirilmeyeceği hususu belirsizliğini korumaktadır. Alman Ceza Kanunu'nda 242. maddede düzenlenen hırsızlık suçuna göre, sadece fiziksel ve taşınabilir nesneler hırsızlık suçuna konu olabilir. Bu da Bitcoin gibi kripto para birimlerini hırsızlık suçu kapsamı dışında tutmaktadır. Alman Ceza Kanunu'nda veri

³⁴⁷ “Suç tarihinde sanığın Suç tarihinde sanığın internet üzerinden girdiği şifre ile müşterinin GSM numarasından başka bir GSM numarasına, oradan da yine şifre vasıtasıyla kendi numarasına müşterinin bilgisi ve rızası dışında kontör transferi yapma şeklinde gerçekleşen eyleminin TCK'nın 244/4. maddesindeki suçu oluşturduğu gözetilmeden suç vasfında yanlıya düşülerek yazılı şekilde hüküm kurulması, bozmayı gerektirmiştir(...) MUHALEFET ŞERHİ: (...) mağdura ait bulunan, ekonomik değeri ve doğrudan parasal karşılığı olan kontörü bilişim sistemini kullanmak suretiyle kendi telefon numarasına geçirmek suretiyle katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla varolan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği ve parasal değer ifade eden 70 adet kontörü alarak mal edinmeye yönelik olduğu açıktır. Yukarıda açıklanan nedenlerle somut olayda 5237 sayılı TCY'nın 142/2-e maddesinde düzenlenmiş bulunan “bilişim sistemi kullanılmak suretiyle hırsızlık” suçunun gerçekleşmesi nedeniyle yerel mahkemenin uygulamasının usul ve yasaya uygun olduğundan hükmün onanmasına karar verilmesi gerektiği görüşünde olduğumuzdan sayın çoğunluk görüşüne katılmıyoruz.” (13.CD., 30.01.2013, 2011/26435 E., 2013/1955 K., emsal.yargitay.gov.tr)

³⁴⁸ “(...) Katılanın 23.10.2011 tarihinde ... isimli oyunu oynarken bilgi ve rızası dışında e-posta adresine girilerek şifresinin ve e-posta adresinin değiştirildiğini ve **oyun karakterlerinin çalındığını**, (...) sanığın savunmasında, katılana ait e-posta adresini ... isimli oyunun hilelerinin ve kullanılmayan karakterlerinin paylaşıldığı forum sitesi olan www.onlinehile.org isimli sitede gördüğünü ve sitede bulunan şifre ile giriş yaptığını, oyun karakterlerinin ise sitede bulunmadığını ve suçlamayı kabul etmediğini söylediği (...) **Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği**, bu itibarla; suçun sübutu halinde eylemin, 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturacağı gözetilmeksizin suç vasfında yanlıya düşülerek yazılı şekilde hüküm kurulması (...)” 13.CD., 10.10.2017, 2016/2155 E., 2017/10403 K. (emsal.yargitay.gov.tr)

“(…) oyun şifresinin çalınıp oyun karakterlerinin aldığından bahisle açılan davada... şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, **çalındığı iddia edilen oyun karakterine ait sanal eşyaların** suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemin TCK.nun 244/4. maddesindeki suçu oluşturacağı da dikkate alınarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken (...)” 8.CD., 25.05.2017, 2017/897 E., 2017/6019 K. (emsal.yargitay.gov.tr)

bütünlüğünü düzenleyen madde (m. 303a), bu tür suçları kovuşturmak için alternatif bir yol sunmaktadır³⁴⁹.

ABD'de hırsızlık gibi suçlar eyaletler tarafından düzenlenmektedir. Örneğin New York Ceza Kanunu'nun 155. maddesi malvarlığına karşı işlenen hırsızlık suçunu cezalandırmaktadır. ABD'deki düzenlemelere göre, malvarlığı kavramına maddi olmayan varlıklar da dâhildir. Buna rağmen hırsızlık suçu bakımından kripto para birimleri gibi sanal mallarla ilgili tartışmalar devam etmektedir. Bazı münferit ABD mahkemeleri sanal malları fiziksel mal olarak kabul etme eğilimine sahip olsalar da Bitcoin'e karşı hırsızlık suçunun oluşabilmesi belirsizliğini korumaktadır³⁵⁰.

İnternet hukuku alanında diğer ülkelere göre daha hızlı ilerleyen Hollanda'da Temyiz Mahkemesi sanal malların, fiziksel mallar gibi malvarlığına dâhil olduğunu hüküm altına alan bir karar vermiştir³⁵¹.

Kripto para birimleri, farklı ülkelerde yaşayan geniş bir kesim tarafından, günlük ve ticari hayatta mal ve hizmet alım satımında kullanılan ve tedavüldeki paralara rahatlıkla çevrilebilen yapılarıyla, alternatif para birimleri gibi ekonomik değer taşıyıcılarıdır.

Kripto para birimleri, tıpkı elektronik paralar gibi bilişim sistemlerinde veri formunda bulunurlar. Bu veriler kendi başlarına bir değere sahip değildirler fakat temsil ettikleri paraların değer taşıyıcısıdır. Burada vurgulanması gereken husus, verilerin temsil edici özelliğidir. Bu nedenle bu verilere karşı gerçekleşen eylemlerin, temsil ettikleri paralara karşı yapıldıklarının kabul edilmesi, amaca uygun bir yorum olacaktır.

Sonuç olarak, Bitcoin gibi kripto para birimlerinin, internet üzerinden erişilen banka hesabındaki para gibi hırsızlık suçunun konusunu oluşturabileceği kanaatindeyiz. Örneğin, ele geçirdiği gizli anahtarı kullanarak, mağdurun rızası

³⁴⁹ Christoph-Nikolaus Von Unruh, **The Law of The Bitcoin**, Edt. Stuart Hoegner, ABD: iUniverse, 2015.

³⁵⁰ Franziska Boehm, Paulina Pesch, **Bitcoin: A First Legal Analysis -with reference to German and US-American law-**, s. 7. https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf, Erişim tarihi: 26 Ağustos 2018.

³⁵¹ **A.g.e.**

olmaksızın, onun Bitcoin hesabındaki bitcoin'leri kendi veya bir başkasının hesabına aktaran kişi, hırsızlık suçu işlemiştir.

6. Suçun Unsurları

a. Maddi Unsur

TCK m. 141'deki düzenlemeye göre, hırsızlık suçunun oluşması için, malın zilyedinin rızası dışında bulunduğu yerden alınması gerekmektedir³⁵². Malın bulunduğu yerden alınması ile suçun icra hareketleri başlamış, başka bir deyişle hırsızlık suçu tamamlanmış olur³⁵³. Bu nedenle hırsızlık, ani hareketli³⁵⁴ neticesi hareketle bitişik bir suçtur³⁵⁵. Alınan maldan yararlanmak şart değildir³⁵⁶.

Almaktan kastedilen anlam, hükmün gerekçesinde “*Almak fiilinden maksat, suçun konusunu oluşturan mal üzerinde mağdurun zilyetliğine son verilmesi, mağdurun suç konusu eşya üzerinde zilyetlikten doğan tasarruf haklarının kullanmasının olanaksız hale gelmesidir. Bu tasarruf olanağı ortadan kaldırılınca, suç da tamamlanır*” belirtilmiştir.

“*Bulunduğu yerden alma*” kavramıyla, failin, önceki zilyedin mal üzerindeki tasarrufuna son vererek kendi hâkimiyet alanına alması ve malın zilyetliğini ele geçirmesi kastedilmektedir³⁵⁷. Fiil almak ve sahip olmaktan oluşmaktadır³⁵⁸.

Maddede malın ne şekilde götürüldüğü ayrıca tanımlanmayıp, zilyedin tasarrufuna son verilmesi dikkate alınmıştır, bu nedenle internet bankacılığı şifresinin ele geçirilip paranın başka bir hesaba havalesi de almak olarak değerlendirilmelidir³⁵⁹.

³⁵² Hafizoğulları, Özen, **a.g.e.**, s. 331; Toroslu, **a.g.e.**, s. 137.

³⁵³ Özbek ve diğ., **a.g.e.**, s. 603; Toroslu, **a.g.e.**, s. 133; Aksi görüşte Hafizoğulları, Özen, **a.g.e.**, s. 335.

³⁵⁴ Toroslu, **a.g.e.**, s. 137; Hafizoğulları, Özen, **a.g.e.**, s. 332.

³⁵⁵ Tezcan, Erdem, Önok, **a.g.e.**, s. 697; Koca, Üzülmüş, **a.g.e.**, s. 529; Şen, **a.g.m.**, s. 327.

³⁵⁶ Özbek ve diğ., **a.g.e.**, s. 603; Centel, Zafer, Çakmut, **a.g.e.**, s. 337.

³⁵⁷ Centel, Zafer, Çakmut, **a.g.e.**, s. 331; Soyaslan, **a.g.e.**, s. 376; Dönmezer, **a.g.e.**, s. 347; Toroslu, **a.g.e.**, s. 136.

³⁵⁸ Hafizoğulları, Özen, **a.g.e.**, s. 331.

³⁵⁹ Şen, **a.g.m.**, s. 7.

Kripto para birimi örneğinde, mağdura ait gizli anahtarın hukuka aykırı olarak ele geçirilip hesapta bulunan paranın başka bir hesaba gönderilmesi, “bulunduğu yerden alma” eylemi olarak değerlendirilebilecektir.

Hukuka uygun açık veya örtülü rıza, hırsızlık suçunun oluşumunu engeller. Zilyet ile malik arasında rıza konusunda çatışma varsa, malikin rızasının üstün tutulması gerekir³⁶⁰.

b. Hukuka Aykırılık Unsuru

Hırsızlık suçunda, malın alınmasında zilyedin rızasının olması hukuka uygunluk sebebidir. Genel bir hukuka uygunluk sebebi olmasına rağmen, rızanın suç tanımında olumsuz bir unsur olarak yer alması onu hukuka uygunluk sebebi olmaktan çıkarmaz³⁶¹. Rızanın geçerli olabilmesi için özgür irade ile verilmiş olması gerekir. Malın alınmasından sonra gösterilen rıza, eylemi yasal hale getirmez³⁶². Kripto para hırsızlığı örneğinde, mağdurun rızasının olması, paranın hesaptan alınması fiilini hukuka uygun hale getirecektir.

Meşru savunmanın söz konusu olduğu durumlarda hırsızlık suçu oluşmaz³⁶³. Örneğin, kendisine bıçakla saldıran failin elinden bıçağı alan kişi meşru müdafaadan yararlanır. Kanaatimize göre kripto para birimlerinin suç konusu olduğu durumlarda, hukuka uygunluk nedeni olarak meşru savunmanın gerçekleşmesi pek mümkün gözükmemektedir.

Görevin yerine getirilmesi hırsızlık suçunun oluşumuna engel olur³⁶⁴. Haciz memurunun, görevi gereği haczedilecek mala el koyması durumunda hırsızlık suçu oluşmaz. Kripto para örneğinde, hakkında el koyma kararı verilmiş bitcoin’lerin failin hesabından alınması durumunda hırsızlık suçu oluşmayacaktır.

Öğretide zorunluluk halinin hukuki niteliği hakkında farklı görüşler öne sürülmüştür. Bir kısım yazarlar, zorunluluk halini, kusurluluğu etkileyen mazeret sebebi olarak değerlendirirken, bazı yazarlar hukuka uygunluk sebebi kabul

³⁶⁰ Tezcan, Erdem, Önok, **a.g.e.**, s. 662.

³⁶¹ Centel, Zafer, Çakmut, **a.g.e.**, s. 333.

³⁶² **A.g.e.**

³⁶³ Aydın, **a.g.e.**, s. 267.

³⁶⁴ **A.g.e.**

etmişlerdir. Zorunluluk halinin, mevcut olaya göre kusurluluğu kaldıran hal veya hukuka uygunluk sebebi olarak değerlendirilmesi gerektiği de öne sürülmüştür³⁶⁵.

TCK m. 147’de hırsızlık suçuna özel olarak düzenlenen zorunluluk hali karma niteliklidir. Hem fiilin haksızlık içeriğini azaltıcı cezayı hafifleten bir sebep hem de olayın özelliğine göre cezayı tümüyle kaldıran bir hal olarak düzenlenmiştir³⁶⁶. Buna göre, hırsızlık suçu ağır ve acil bir ihtiyacı karşılamak için işlenmişse, olayın özelliğine göre faile verilecek cezada indirimle gidilebilir veya hiç ceza verilmeyebilir. İhtiyacın acil olması, hukuki yararın tehlikeye maruz kalması veya ağır olması da failin katlanılmaya tahammül edememesidir^{367, 368}.

Zorunluluk halinin genel hukuka uygunluk sebebi olmasından dolayı bu düzenlemenin gereksiz olduğu ileri sürülmüştür³⁶⁹.

Kripto para birimi örneğinde, hasta olan çocuğuna ilaç almak zorunda olan babanın, başkasının gizli anahtarını ele geçirerek ona ait kripto parayı çalması durumunda, zorunluluk hali gündeme gelebilecektir.

c. Kusurluluk

³⁶⁵ Veli Özer Özbek, Koray Doğan, “Zorunluluk Halinin (TCK m. 25/2) Hukuki Niteliği”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. 9/2, 2007, s. 196.

³⁶⁶ Özbek ve diğ., **a.g.e.**, s. 628.

³⁶⁷ Tezcan, Erdem, Önok, **a.g.e.**, s. 693; Soyaslan, **a.g.e.**, s. 399.

³⁶⁸ "...Su hırsızlığı suçundan sanık (Y) nin yapılan yargılaması sonunda beraatine dair (Antalya)..Asliye Ceza Mahkemesinden verilen 02/12/2005 tarihli hükmün Yargıtay'ca incelenmesi katılan vekili tarafından istenmekle ve dosya C.Başsavcılığının 03/04/2007 tarihli tebliğnamesiyle dairemize gelmekle yapılan inceleme sonunda gereği düşünüldü.

1- Sanığın mühürü kırarak sayaç yerine galvaniz boru bağlamak suretiyle kaçak kullandığı iddiası ile hakkında tutanak düzenlendiği anlaşılmakla; 5237 TCK 147. maddesinin şartlarının oluşmadığı gözetilerek duruşmaya devamla suça konu olayla ilgili tüm deliller toplanarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken, sanığın günü-birlik sigortasız çalışması nedeniyle ekonomik durumunun zayıf olduğu ve insan yaşamı için hayati önem taşıyan suyu kullanarak ağır ve acil bir ihtiyacı karşılamak için bu suçu işlediği şeklindeki yasal olmayan gerekçeyle, 5237 sayılı TCK nun 147. maddesi uyarınca ceza verilmesine yer olmadığına karar verilmesi (..)

Bozmayı gerektirmiş, katılan vekilinin temyiz itirazları bu itibarla yerinde görülme; olduğundan, 1412 sayılı CMUK'nun 321. maddesi uyarınca hükmün bu sebepten dolayı bozulmasına 20/06/2007 tarihinde oybirliğiyle karar verildi." 2.CD., 20.06.2007, 2007/6126 E., 2007/9056 K. (Yurtcan, **a.g.e.**, s. 130)

³⁶⁹ Centel, Zafer, Çakmut, **a.g.e.**, s. 366; dipnot 205; Şen, **a.g.m.**, s. 353.

Hırsızlık kasten işlenebilen bir suçtur³⁷⁰. Kast, suçun kanuni tanımındaki unsurların bilerek ve isteyerek gerçekleştirilmesidir (TCK m. 21/1). Buna göre kastın varlığından bahsedebilmek için, failin, taşınabilir malın başkasına ait olduğunu ve zilyedinin rızasının olmadığını bilmesi ve buna rağmen onu almak istemesi gerekir.

Failin, malın kime ait olduğunu (mağduru) bilmesi gerekmez³⁷¹. Kripto para birimi hırsızlığı örneğinde, internet ortamından elde ettiği fakat kime ait olduğunu bilmediği gizli anahtarı kullanıp, kendisinin veya bir başkasının hesabına para transfer eden kişi, hırsızlık suçu işlemiş sayılacaktır.

Maddede geçen “*kendisine veya başkasına bir yarar sağlamak maksadı*” ifadesi, suçun oluşumu için özel kastın arandığını göstermektedir³⁷². *Yarar sağlama* ifadesini sahiplenmek anlamında anlamak gerekir. Çünkü yarar sağlama, mülkiyete dayanan haklardan sadece birisidir. Failin bu kastla hareket etmesi yeterli olup, maldan kendisinin veya başkasının faydalanmış olması gerekli değildir³⁷³.

Kripto para birimi örneğinde, gizli anahtarını ele geçirdiği Bitcoin hesabındaki bitcoin’leri, ne kendisinin ne de başkasının yararlanabileceği (sahipsiz) bir hesaba transfer edip tamamen erişilmez kılan kişi, hırsızlık suçundan sorumlu tutulmayacaktır. Çünkü failin bu eyleminde yararlanma maksadı yoktur. Söz konusu eylem, diğer şartların varlığı durumunda TCK m.244’te düzenlenen “sistemi engelleme, bozma, verileri yok etme veya değiştirme” kapsamında değerlendirilecektir.

Bilindiği gibi bir suçun taksirle işlenebilmesi ancak kanunda açıkça belirtilmiş olmasına bağlıdır. Suçun tanımında taksirle işlenebileceğine dair bir kayıt olmadığından hırsızlık suçu taksirle işlenemez. Örneğin, yanlışlıkla bir başkasının gizli anahtarını kullanıp hesapta bulunan kripto para birimini kendisinin veya başkasının hesabına aktaran kişi, hırsızlık suçu işlemiş sayılmayacaktır.

³⁷⁰ Soyaslan, **a.g.e.**, s. 379; Tezcan, Erdem, Önok, **a.g.e.**, s. 694; Toroslu, **a.g.e.**, s. 134; Koca, Üzülmüş, **a.g.e.**, s. 544; Hafizoğulları, Özen, **a.g.e.**, s. 338.

³⁷¹ Özbek ve diğ., **a.g.e.**, s. 629.

³⁷² Yurtcan, **a.g.e.**, s. 2; Dönmezer, **a.g.e.**, s. 367; Toroslu, **a.g.e.**, s. 139; Koca, Üzülmüş, **a.g.e.**, s. 545; Hafizoğulları, Özen, **a.g.e.**, s. 338; Şen, **a.g.m.**, s. 329; Aydın, **a.g.e.**, s. 266.

³⁷³ Özbek ve diğ., **a.g.e.**, s. 631.

7. Suç ve Cezaya Etki Eden Nedenler

a. Suçu Ağırılaştıran Nedenler

Hırsızlık suçunu ağırlatıcı nitelikli haller, TCK m. 142 ve 143'te düzenlenmiştir. TCK m. 142/1'de düzenlenen ağırlatıcı haller: Suçun,

- a) Kime ait olursa olsun kamu kurum ve kuruluşlarında veya ibadete ayrılmış yerlerde bulunan ya da kamu yararına veya hizmetine tahsis edilen eşya hakkında,
- c) Halkın yararlanmasına sunulmuş ulaşım aracı içinde veya bunların belli varış veya kalkış yerlerinde bulunan eşya hakkında,
- d) Bir afet veya genel bir felaketin meydana getirebileceği zararları önlemek veya hafifletmek maksadıyla hazırlanan eşya hakkında,
- e) Adet veya tahsis veya kullanımları gereği açıkta bırakılmış eşya hakkında işlenmesi durumunda cezayı ağırlatıcı nitelikli hal oluşacaktır.

Maddenin 2. fıkrasına göre suçun;

- a) Kişinin malını koruyamayacak durumda olmasından veya ölmesinden yararlanarak,
- b) Elde veya üstte taşınan eşyayı çekip almak suretiyle ya da özel beceriyle,
- c) Doğal bir afetin veya sosyal olayların meydana getirdiği korku veya kargaşadan yararlanarak,
- d) Haksız yere elde bulundurulmuş veya taklit anahtarla ya da diğer bir aletle kilit açmak veya kilitlenmesini engellemek suretiyle,
- e) Bilişim sistemlerinin kullanılması suretiyle,
- f) Tanınmamak için tedbir alarak veya yetkisi olmadığı halde resmi sıfat takınarak,
- g) Büyük veya küçükbaş hayvan hakkında,
- h) Herkesin girebileceği bir yerde bırakılmakla birlikte kilitlenmek suretiyle ya da bina veya eklentileri içinde muhafaza altına alınmış olan eşya hakkında işlenmesi halinde cezayı daha da ağırlatıcı nitelikli hal oluşacaktır.

TCK m.142/2-b bendinde düzenlenen nitelikli hırsızlığın beden veya ruh bakımından kendisini savunamayacak durumda olan kimseye karşı işlenmesi, cezayı daha da artıran başka bir nitelikli haldir. Bunlardan başka, hırsızlığın sıvı veya gaz

hâlindeki enerji hakkında ve bunların nakline, işlenmesine veya depolanmasına ait tesislerde işlenmesi (TCK m. 142/3), suçun işlenmesi sonucunda haberleşme, enerji ya da demiryolu veya havayolu ulaşımı alanında kamu hizmetinin geçici de olsa aksaması (TCK m. 142/5) veya hırsızlığın gece vakti işlenmesi (TCK m. 143) düzenlenen diğer nitelikli hallerdir.

Kripto para birimine karşı hırsızlık suçunun temel şeklinin işlenemeyeceği fakat TCK m. 142/2-e bendinde nitelikli hal olarak düzenlenen “*bilişim sistemlerinin kullanılması suretiyle*” hırsızlığın mümkün olduğu yukarıda açıklanmıştı. Bu nedenle kripto para birimlerinin suç konusunu oluşturduğu hırsızlık suçlarında diğer nitelikli haller de mevcutsa, bu durumda birden fazla nitelikli hal birlikte gerçekleşmiş olacaktır. Bu husus, hâkim tarafından suça ilişkin temel ceza tayin edilirken göz önüne alınacaktır³⁷⁴.

Bu bölümde, kripto para birimleri hırsızlığına uygulanabilir nitelikli haller açıklanacaktır.

aa. Hırsızlık suçunun, kime ait olursa olsun kamu kurum ve kuruluşlarında veya ibadete ayrılmış yerlerde bulunan ya da kamu yararına veya hizmetine tahsis edilen eşya hakkında işlenmesi

Bu nitelikli hal, kripto para birimlerinin suç konusu olduğu ve ilgili paranın kamu yararına veya hizmetine tahsis edildiği hallerde temel ceza belirlenirken göz önüne alınır. Kamu kurumu belirli bir veya birkaç kamu hizmetini ya da faaliyetini yürütmekle görevli, kamu tüzel kişiliğine sahip kuruluşlardır³⁷⁵. Örneğin, İstanbul Su İdaresi, Sosyal Güvenlik Kurumu, Devlet Su İşleri, vs.

Kripto para birimi örneğinde, failin Sosyal Güvenlik Kurumu gibi bir kamu kurumu tarafından yönetilen Bitcoin hesabına ait gizli anahtarı ele geçirip, hesaptaki bitcoin’leri kendi veya bir başkasının kontrol ettiği hesaba aktarması durumunda, bu nitelikli hal oluşacaktır.

³⁷⁴ Centel, Zafer, Çakmut, **a.g.e.**, s. 359.

³⁷⁵ Tezcan, Erdem, Önok, **a.g.e.**, s. 671.

bb. Hırsızlık suçunun bir afet veya genel bir felaketin meydana getirebileceği zararları önlemek veya hafifletmek maksadıyla hazırlanan eşya hakkında işlenmesi

Deprem, sel, yangın ve savaş gibi afet ve genel felaketlerin sebep olacağı zararları önlemek ve hafifletmek için tahsis edilmiş eşyaya karşı hırsızlık suçunun işlenmesi, nitelikli hal olarak düzenlenmiştir.

Kripto para örneğinde, hırsızlık konusu bu amaçla tahsis edilmiş kripto para ise, bu nitelikli hal, temel cezanın belirlenmesinde göz önüne alınır.

cc. Hırsızlık suçunun adet veya tahsis veya kullanımları gereği açıkta bırakılmış eşya hakkında işlenmesi

Bu nitelikli halin uygulanabilmesi için hırsızlığa konu olan eşyanın açıkta bırakılmış olması gerekmektedir. Açıkta bırakılma, koruma altına almama anlamındadır³⁷⁶. Söz konusu eşyanın, kullanım gereği veya örf ve âdet gereği açıkta bırakılmış olması gerekir³⁷⁷.

Kripto para birimleri, bilişim sistemlerinde bulunan varlıklardır. Bu nedenle bu nitelikli hal kripto para birimleri için gerçekleşmez. Bu para birimleri üzerinde tasarrufta bulunmayı sağlayan gizli anahtarların, örneğin bir kâğıt üzerine yazılı bir şekilde başkalarının erişimine açık bırakılması söz konusu olabilir. Fakat bu nitelikli halin geçerli olması için, açıkta bırakılmanın kullanım veya örf ve adet gereği olması gerekir. Yanlışlıkla açıkta bırakılmış olmanın bu nitelikli halin kapsamına girmediği kanaatindeyiz.

dd. Hırsızlık suçunun kişinin malını koruyamayacak durumda olmasından veya ölmesinden yararlanarak işlenmesi

Bu nitelikli halin oluşması için hırsızlık suçunun işlendiği sırada mağdurun malını koruyamayacak bir durumda olması ve failin bu durumdan yararlanarak suçu

³⁷⁶ Soyaslan, **a.g.e.**, s. 384.

³⁷⁷ Tezcan, Erdem, Önok, **a.g.e.**, s. 675.

işlenmesi gerekir. Mağdurun aniden fenalaşması, büyük bir üzüntü içinde olması ve bayılması gibi durumlar, bu kapsamda değerlendirilir³⁷⁸.

Kripto para örneğinde, böyle bir durumda olan mağdurun gizli anahtarını ele geçirerek, hesabındaki paranın çalınması durumunda, temel cezanın belirlenmesinde bu nitelikli halin göz önüne alınması mümkündür.

ee. Hırsızlık suçunun doğal bir afetin veya sosyal olayların meydana getirdiği korku veya kargaşadan yararlanarak işlenmesi

Doğal afet ve sosyal olaylar, toplumda kargaşa ve korkuya sebep olmakta ve kişileri telaşa ve endişeye sevk etmektedir³⁷⁹. Böyle durumlar, suç konusu eşya üzerinde denetimin azalmasına neden olarak hırsızlık suçunu kolaylaştırmaktadır. Doğal afet ve sosyal olaylar, bilişim sistemlerinin çalışmaları ve güvenliklerini olumsuz etkileyebilir hatta çalışmalarını tamamen engelleyebilir.

Bu tür olayların sebep olduğu bilişim sistemlerindeki güvenlik zafiyeti kripto para birimlerine karşı hırsızlık suçunu kolaylaştırabilir. Örneğin, güvenlik sistemlerinin devre dışı kaldığı çevrimiçi kripto para cüzdan hizmeti veren bir takas merkezinden bitcoin'lerin çalınması, normal işleyişe göre daha kolay olacaktır. Bu nedenle bu nitelikli halin kripto para birimi hırsızlık suçuna uygulanabileceği kanaatindeyiz.

ff. Hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi

Kripto para birimine karşı gerçekleşecek hukuka aykırı alma eylemlerinin hırsızlık kapsamında değerlendirilmesini sağlayacağını düşündüğümüz bu nitelikli hal, yukarıda değinildiği gibi söz konusu eylemlerin bilişim verisi üzerinde işlenmesinin hırsızlık suçu oluşturup oluşturmadığına ilişkin tartışmalarına sebep olmuştur.

³⁷⁸ A.g.e., s. 595.

³⁷⁹ Centel, Zafer, Çakmut, a.g.e., s. 352.

YCGK'nun 17.11.2009 tarihinde kararında³⁸⁰ internet bankacılığı şifresinin ele geçirilip hesaptaki paranın başka bir hesaba gönderilmesinde suç konusunun veri olmadığını, verinin temsil ettiği para olduğunu belirtmiş ve bu eylemi bilişim sistemi kullanmak suretiyle hırsızlık suçu kapsamında değerlendirmiştir. YCGK'nin bu kararı sonraki uygulamalarda istikrar kazanmıştır³⁸¹.

Doktrinde bu kararla ilgili değerlendirmelere bakıldığında çeşitli görüşlerin ortaya çıktığı görülmektedir.

Şen'e göre bilişim sisteminde bulunan verilerin izinsiz olarak başka yere gönderilmesi veya bulunduğu yerden alınması hırsızlık suçunu oluşturmaz da bu yolla başkasına ait para üzerinde zilyedinin tasarrufunun kaldırılarak paranın başka yere gönderilmesi hırsızlık suçunu oluşturur. Bu durum, suçta ve cezada kanunilik prensibine aykırılık oluşturmadığı gibi kıyas yasağının ihlaline de yol açmaz³⁸².

³⁸⁰ YCGK, 17.11.2009, 2009/11-193 E., 2009/268 K. Bu karar ile ilgili tartışmalar için bkz. s. 157.

³⁸¹ "...Şikayetçinin banka hesabına internet bankacılığı aracılığıyla girilip paranın banka hesabına transfer edilmesi şeklindeki sanığın eyleminin, TCK.nun 142/2-e madde ve fıkrasında düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, suç vasfında yanılığa düşülerek yazılı şekilde, TCK.nun 244/4. maddesi uyarınca mahkumiyet hükmü kurulması, Yasaya aykırı, Cumhuriyet Savcısı ile sanığın temyiz itirazları bu itibarla yerinde görülmesi olduğundan hükmün bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi uyarınca uygulanması gereken 1412 sayılı CMUK.nun 321. ve 326/son maddeleri gereğince BOZULMASINA, 22.11.2017 gününde oybirliğiyle karar verildi." 8.CD., 22.11.2017, 2017/16623 E., 2017/13121 K. (emsal.yargitay.gov.tr)

"...Dosya kapsamına göre, her ne kadar sanığın eyleminin 5237 sayılı Kanun'un 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturduğundan bahisle hüküm verilmiş ise de, katılan ... 'ın sorumlusu olduğu şirket hesabından 3.650,00 Türk Lirası ve katılan ...'ın hesabından ise 630,00 Türk Lirasının ...'ın hesabına aktarılmasını müteakip, yatırılan paraların bu hesaptan çekilmesi eyleminin, 5237 sayılı Kanun'un 142/2-e maddesinde düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeksizin, yazılı şekilde karar verilmesinde isabet görülmediğinden bahisle..." 8.CD., 23.11.2017, 2017/1428 E., 2017/13162 K. (emsal.yargitay.gov.tr)

"...Sanığın müşterinin banka hesabına internet bankacılığı yoluyla girip, hesabında-ki parayı kendi hesabına transfer edip bankamatik ile çekerek menfaat sağlaması karşısında eylemin TCK.nun 142/2-e maddesindeki bilişim sisteminin kullanılması suretiyle hırsızlık suçunu oluşturacağı gözetilmeden yazılı şekilde karar verilmesi, Bozmayı gerektirmiş, sanık Doğan Gürbüz'ün temyiz itirazı bu itibarla yerinde görülmesi olduğundan, hükmün açıklanan nedenle tebliğnameye kısmen aykırı olarak BOZULMASINA, 5320 sayılı Yasanın 8/1. maddesi aracılığı ile 1412 sayılı CMUK'un 326/son maddesi uyarınca kazanılmış hakkın korunmasına, 06.06.2013 gününde oybirliğiyle karar verildi..." 13.CD., 06.06.2013, 2012/8525 E., 2013/17588 K. (Yurtcan, **a.g.e.**, s. 45)

³⁸² Şen, **a.g.m.**, s. 325.

Artuk, Gökçen ve Yenidünya, TCK m. 244/4'te düzenlenen suçun tamamlayıcı norm olduğunu ve bilişim sistemi kullanmak suretiyle hırsızlık suçunun oluşabileceğini görüşüne katılmışlardır³⁸³.

Koca ve Üzülmüş, internet bankacılığı şifresinin fail tarafından ele geçirilip mağdurun hesabındaki paranın failin veya bir başkasının hesabına transfer edilmesi fiilinin “hırsızlığın bilişim sistemlerinin kullanması suretiyle işlenmesi” kapsamında değerlendirilmesi gerektiğini ileri sürmektedir³⁸⁴.

Özbek, Doğan, Bacaksız ve Tepe, Yargıtay'ın taşınır niteliğindeki parayı bilişim sistemi kullanmak suretiyle başka bir banka hesabına havale yapmasını TCK m. 244/4 anlamında bir veri transferi olarak değil, verinin temsil ettiği paranın aktarılması başka bir ifadeyle TCK m. 142/2-e'de düzenlenen “bilişim sistemi aracılığıyla nitelikli hırsızlık suçu”nu oluşturduğu kararına katılmadıklarını belirtmişlerdir³⁸⁵.

Tezcan, Durmuş ve Önok; bir başkasının internet bankacılığı şifresini ele geçirip, hesaptaki parayı kendi hesabına aktarma veya mağdurun hesabından ödeme yaparak kendine bir şey sipariş etme fiillerini ilişkin değerlendirmede, bilişim sistemlerine veya sistem içindeki verilere müdahale etmek suretiyle taşınır bir malın bulunduğu yerden alınmasını fiilen mümkün görmemektedir³⁸⁶.

Dülger, bir banka hesabında veri formunda tutulan paranın hırsızlık suçunun kapsamında taşınır mal olarak değerlendirilmesinin isabetli olduğunu ifade ederek, bilişim sistemi kullanmak suretiyle hırsızlık suçunun işlenebileceğini belirtmiştir³⁸⁷.

Başbüyük, konuyla ilgili değerlendirmesinde, banka hesabındaki paranın alacak hakkının sınırlarını belirleyen kaydi para olduğunu ve alacak hakkının hırsızlığa konu olmayacağını öne sürmüştür³⁸⁸.

³⁸³ Mehmet Emin Artuk, Ahmet Gökçen, Ahmet Caner Yenidünya, **Ceza Hukuku Özel Hükümler**, 15. b., Ankara: Adalet Yayınevi, 2015, s. 892.

³⁸⁴ Koca, üzülmüş, **a.g.e.**, s. 561.

³⁸⁵ Özbek ve diğ., **a.g.e.**, s. 967.

³⁸⁶ Tezcan, Erdem, Önok, **a.g.e.**, s. 1008.

³⁸⁷ Dülger, **a.g.e.**, s. 580.

³⁸⁸ İsa Başbüyük, “İnternet Bankacılığı Aracılığıyla Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi”, **CHD Ceza Hukuku Dergisi**, S. 21, 2013, s. 206.

Doktrinde, buradaki düzenlemenin kilit yerine geçen ve güvenliği sağlayan elektronik sistemlerin, yine bu yolla giderilerek hırsızlık yapılması ile sınırlı olduğu da ileri sürülmektedir³⁸⁹.

Kanaatimize göre, bilişim verisine ilişkin değerlendirmeler, verinin temsil ettiği nesne dikkate alınarak yapılmalıdır. Verinin parayı temsil ettiği durumlarda, bilişim sistemi kullanmak suretiyle veri üzerinde zilyetliğin hukuka aykırı bir şekilde kaldırılarak, paranın başka birinin hesabına aktarılması eylemi, hırsızlık kapsamında değerlendirilmelidir.

Kripto para birimi örneğinde, ele geçirdiği gizli anahtar ile mağdurun Bitcoin hesabına erişen ve hesaptaki paraları kendi hesabına transfer eden kişinin eylemi hırsızlık suçu kapsamında değerlendirilmelidir.

gg. Hırsızlık suçunun tanınmamak için tedbir alarak veya yetkisi olmadığı halde resmi sıfat takınarak işlenmesi

Hırsızlık suçunun faili, yakalanmasını önlemek ve böylece cezadan kurtulmak amacıyla kendisini tanınmayacak hale getirmişse veya verdiği yetki ve kolaylıklardan faydalanmak için kamu görevlisi olmadığı halde kendisini öyle göstermişse³⁹⁰, bu nitelikli hal söz konusu olur.

Tanınmamak için alınan tedbirler, fiziksel görünümü değiştirmek amacıyla yapılan şeylerle sınırlı kabul edildiğinde, bu nitelikli halin kripto para birimi hırsızlığında gerçekleşmesi mümkün gözükmemektedir. Çünkü fiziksel görünümün değiştirilmesi, kripto para hırsızlığının işlenmesini kolaylaştırmaz veya failin yakalanmasını zorlaştırmaz. Bu nedenle bu nitelikli halin, kripto para hırsızlığı suçlarında uygulanabilmesi için “tanınmamak için tedbir almak” ifadesinin geniş yorumlanması gerekir. Mesela tanınmama tedbiri, kripto paraların bulunduğu hesaba kimin eriştiğini gizlemeyi kapsayacak şekilde geniş yorumlandığında, bu nitelikli halin kripto para hırsızlığında uygulanma imkanı bulabileceği kanaatindeyiz. Fail

³⁸⁹ Hafizoğulları, Özen, **a.g.e.**, s. 354.

³⁹⁰ Tezcan, Erdem, Önok, **a.g.e.**, s. 682.

kimliğini gizleyerek veya farklı bir kimlikle kripto para birimlerinin bulunduğu bilişim sistemine girip hesaptaki paraları çalarsa veya fail, yakalanmamak için, çaldığı kripto parayı, kendisiyle ilişki kurulamayacak bir hesaba aktarırsa bu nitelikli hal oluşacaktır.

hh. Hırsızlık suçunun gece işlenmesi

Hırsızlığın gece vakti işlenmesi genel ağırlatıcı nitelikli bir hal olarak TCK m. 143'te düzenlenmiştir. Gece vakti, güneşin batmasından bir saat sonra başlayan ve doğmasından bir saat evvele kadar devam eden zaman süresini belirtmektedir (TCK m. 6/1-e). Bu düzenlemenin nedeni olarak suçun işlenmesindeki kolaylık gösterilmiştir³⁹¹.

Kripto para birimlerine karşı hırsızlık suçlarının gece işlenmesi halinde, verilecek cezada yarı oranına kadar artırımı gidilebilecektir.

b. Suçu Hafifleten Nedenler

Hırsızlık suçuna verilecek cezada indirim öngören haller, TCK m. 144 ilâ 147 arasında düzenlenmiştir. Hırsızlık suçunun, paydaş veya elbirliği ile malik olunan mal üzerinde (TCK m 144/1-a), bir hukuki ilişkiye dayanan alacağı tahsil amacıyla (TCK m.144/1-b) işlenmesi; hırsızlık konusu malın değerinin az olması (TCK m. 145), hırsızlığın malın geçici bir süre kullanılıp zilyedine iade edilmek üzere işlenmesi (TCK m. 146) ve hırsızlığın ağır ve acil bir ihtiyacı karşılamak için işlenmesi (TCK m. 147) halleri, cezayı hafifleten haller olarak düzenlenmiştir. Kripto para hırsızlığı suçlarında bu cezayı hafifletici haller, uygun düştüğü durumlarda uygulama imkânı bulacaklardır.

aa. Hırsızlık suçunun paydaş veya elbirliği ile malik olunan mal üzerinde işlenmesi

Hırsızlık, kural olarak başkasının malı üzerinde gerçekleşen bir suçtur. Bu bakımından failin kendisinin de malikleri arasında yer aldığı malı, diğer sahiplerinin

³⁹¹ Özbek ve diğ., **a.g.e.**, s. 619.

rızası olmadan çalması, suça ilişkin hükmedilecek cezada indirimine gidilmesini gerektiren bir hal olarak düzenlenmiştir.

Bu hafifletici neden, kripto para birimi hırsızlığında uygulama imkânı bulabilecek bir niteliklidir. Örneğin, ortak hesapta tutulan kripto para birimine karşı, ortak hesap sahiplerinden birisinin parayı kendi hesabına aktarması durumunda bu hafifletici nitelik oluşur.

bb. Hırsızlık suçunun bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi

Bu hafifletici nitelikte failin hukuki bir ilişkiye dayanan alacağını tahsil etmesi dikkate alınmıştır. Hukuki ilişkiye dayanan alacak, para veya mal olabilir³⁹². Fail ile mağdur arasında alacak hakkı doğuran hukuki ilişkinin geçerli olması gerekir. Hırsızlık suçuna konu olan malın, alaktan fazla olması durumunda da bu hüküm uygulanır³⁹³.

Bu hafifletici niteliğin, kripto para birimi hırsızlığında uygulama imkânı bulması mümkündür. Örneğin mağdurdan geçerli bir hukuki ilişkiye dayanan alacağını, normal yollarla alamayan fail, mağdurun hesabındaki kripto paraları kendi hesabına aktarırsa bu nitelikli hal oluşacaktır.

Bu iki cezayı hafifleten nitelik söz konusu olduğunda, hırsızlık suçunun soruşturulması şikâyet şartına bağlanmıştır. Şikâyet hakkı sahibi malın alındığı sıradaki zilyettir³⁹⁴.

cc. Malın değerinin az olması

Hırsızlık suçuna konu olan malın değerinin az olması durumunda verilecek cezada indirimine gidilebileceği gibi hiç ceza verilmeyebilir. Her olayda malın değeri, suçun işlendiği anda³⁹⁵, mağdurun zararından bağımsız³⁹⁶ objektif olarak

³⁹² Centel, Zafer, Çakmut, **a.g.e.**, s. 371; Soyaslan, **a.g.e.**, s. 395.

³⁹³ Tezcan, Erdem, Önok, **a.g.e.**, s. 688.

³⁹⁴ Centel, Zafer, Çakmut, **a.g.e.**, s. 371.

³⁹⁵ Soyaslan, **a.g.e.**, s. 400.

değerlendirilmelidir. Değerin azlığı, daha çoğunu alabilme imkânı varken, yalnız ihtiyaç kadarını alma veya değer olarak az olanı alma şeklinde de olabilir³⁹⁷. Suçun işleniş şekli göz önüne alındığında, faile hiç ceza verilmeyebilir. Bunun için olayın özelliği, mağdurun konumu, failin kişiliği ile birlikte suçun işleniş şekli göz önüne alınacaktır³⁹⁸.

Mağdur bakımından malın maddi değeri olmayıp manevi değeri olduğunda, bu hükmün uygulanması problemlidir³⁹⁹.

Kripto para hırsızlığı suçlarında, bu hafifletici nedenin uygulanabilmesi mümkündür. Örneğin, mağdurun hesabında yüklü miktarda kripto para bulunması durumunda, bütün parayı çalma imkânı varken, hepsini almayıp ihtiyaç duyduğu cüz'i kısmı alan fail, bu nitelikli halden yararlanabilecektir.

dd. Hırsızlık suçunun, malın geçici bir süre kullanılıp zilyedine iade edilmek üzere işlenmesi

TCK m. 146'da düzenlenen kullanma hırsızlığında, malın cinsi ile ilgili bir ayırım yapılmamıştır. Bu nitelikli halin oluşması için failin malı, iade etmek üzere alması gerekir⁴⁰⁰. Mal, iade edilmemiş olsa dahi, eğer iade etmek niyetiyle alındığı anlaşılıyorsa, hüküm uygulama imkânı bulur. Geçici süre ile ilgili bir sınırlama

³⁹⁶ Tezcan, Erdem, Önok, **a.g.e.**, s. 690; Aydın, **a.g.e.**, s. 272.

³⁹⁷ **A.g.e.**, s. 691.

³⁹⁸ "...TCK'nın 145. maddesine göre, faile verilen cezada indirim yapılabilmesi için malın değerinin az olması yeterli olup, hâkim indirim oranını TCK'nın 3. maddesinde öngörüldüğü üzere "işlenilen fiilin ağırlığıyla orantılı" olacak şekilde saptamalıdır.

Değer azlığı nedeniyle ceza vermekten vazgeçme kararı verilecek ise; malın değerinin azlığı yanında "suçun işleniş şekli ve özellikleri" de dikkate alınmalıdır. TCK'nın 145. maddesinin uygulanmasında hâkime takdir hakkı tanınmış olup, hâkim takdir hakkını kullanırken keyfiliğe kaçmadan, her somut olaya uygun, yasal ve yeterli gerekçe göstermek suretiyle uygulama yapmalıdır.

Somut olayda ise; 20 TL değerinde kazak çalan suça sürüklenen çocuk hakkında, hırsızlık konusunu oluşturan malın değerinin az olması nedeniyle TCK'nın 145. maddesi gereğince verilen cezadan belli oranda indirim yapılmak suretiyle hüküm kurulduğunun anlaşılması karşısında bozma talebine yönelik tebliğnamedeki düşünceye iştirak edilmemiştir.

Dosya ve duruşma tutanakları içeriğine, toplanıp karar yerinde incelenerek tartışılan hukuken geçerli ve elverişli kanıtlara, gerekçeye ve hâkimin takdirine göre; suçun sanık tarafından işlendiğini kabulde ve nitelendirmede usul ve yasaya aykırılık bulunmadığı anlaşılmış, diğer temyiz itirazları yerinde görülmemiştir..." 13.CD., 2012/17444 E., 2013/29061 K. (Yurtcan, **a.g.e.**, s. 121)

³⁹⁹ Hafizoğulları, Özen, **a.g.e.**, s. 343.

⁴⁰⁰ Özbek ve diğ., **a.g.e.**, s. 626; Soyaslan, **a.g.e.**, s. 393.

getirilmemiştir. Her somut olayda bu durum araştırılacaktır⁴⁰¹. Yargıtay, iki gün boyunca kullanılıp benzinin bitmesi üzerine bırakılan mobilet olayında iki günü “geçici süre” kapsamında değerlendirmemiştir⁴⁰².

Kripto para hırsızlığında, bu nitelikli halin uygulama imkânı bulabilmesi için, çalınan paranın aynen iade edilmesi gerektiğini düşünmekteyiz.

c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep

TCK m. 167’de belli yakınlık ilişkileri şahsi cezasızlık sebebi sayılmış, bazıları da cezayı hafifleten sebep olarak düzenlenmiştir. Buna göre; (a) haklarında ayrılık kararı verilmemiş eşlerden birinin, (b) üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın, (c) aynı konutta beraber yaşayan kardeşlerden birinin zararına işlenmesi durumunda, ilgili kişi hakkında cezaya hükmolunmaz.

Kripto para hırsızlığı örneğinde, çocuk babasının gizli anahtarını alıp, hesabında bulunan bitcoin’leri onun izni olmadan harcasa, bu eylem hırsızlık olarak değerlendirilmeyecektir.

Bu suçun haklarında ayrılık kararı verilmiş olan eşlerden birinin, aynı konutta beraber yaşamayan kardeşlerden birinin, aynı konutta beraber yaşamakta olan amca, dayı, hala, teyze, yeğen veya ikinci derecede kayın hısımlarının zararına olarak işlenmesi halinde; ilgili akraba hakkında şikâyet üzerine verilecek ceza, yarısı oranında indirilir.

d. Etkin Pişmanlık

⁴⁰¹ "Sanıkların P... ten çaldıkları kamyoneti Osmaneli ve Akyazı ilçelerine götürdükleri, yakınının araştırması sonucu aracı Akyazı’da bulup teslim aldığı anlaşılmışa göre, 765 sayılı TCK’ nin 494/1 maddesinde yazılı suçun koşulları bulunmayıp, kullanma kastının değere ilişkin yasa hükümlerinin uygulanması sırasında araç bedeli yerine, kullanma ile oluşan yağ, yakıt ve yıpranma giderinin esas alınmasını gerektireceği, 765 sayılı TCK’nın 493/1 maddesinde yazılı suçu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması, Kabule göre de, kamyonetin ücret karşılığı yük ve yolcu taşımacılığına tahsis edilip edilmediğinin araştırılmaması bozmayı gerektirmiştir." 6.CD., 2002/7519 E., 2002/10108 K. (Yurtcan, **a.g.e.**, s. 130)

⁴⁰² Tezcan, Erdem, Önok, **a.g.e.**, s. 693.

TCK m. 168’te içinde hırsızlık suçunun aralarında yer aldığı malvarlığına karşı suçlar için etkin pişmanlık düzenlenmiştir. Buna göre, hırsızlık suçu tamamlandıktan sonra fakat kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde, verilecek cezanın üçte ikisine kadar indirilir (TCK m. 168/1).

Örneğin, kripto para hırsızlığı faili, hakkında kovuşturma başlamadan önce pişmanlık duyup çaldığı bitcoin’leri aynen iade ederse, cezasında üçte ikiye kadar indirimle gidilebilecektir.

Etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi halinde, verilecek cezanın yarısına kadar indirilir (TCK m. 168/2). Yukarıda verilen örnekteki fail, hakkında kovuşturma başladıktan sonra çaldığı bitcoin’leri mağdura aynen iade eder veya karşılığı para verirse cezası yarı oranına kadar indirilecektir.

Kısmen geri verme veya tazmin halinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır (TCK m. 168/4). Yukarıdaki örnekteki failin, çaldığı bitcoin’lerin sadece bir kısmını iade etmesi durumunda, cezada indirim öngören bu düzenlemelerden yararlanabilmesi için mağdurun rızası gerekecektir.

8. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Hırsızlık suçuna teşebbüs mümkündür⁴⁰³. Failin, zilyedin mal üzerindeki zilyetliğini sona erdirip kendi hâkimiyetine geçirmesi sürecinde, elinde olmayan sebeplerle, fiilin kesintiye uğraması durumunda suç tamamlanmamış olacak,

⁴⁰³ Yurtcan, **a.g.e.**, s. 3; Dönmezer, **a.g.e.**, s. 201; Hafizoğulları, Özen, **a.g.e.**, s. 336; Dönmezer, **a.g.e.**, s. 353; Toroslu, **a.g.e.**, s. 137.

teşebbüs aşamasında kalmış olacaktır⁴⁰⁴. Bir görüşe göre, teşebbüs ancak malın alınma aşamasına kadar mümkündür⁴⁰⁵.

Kripto para örneğinde, failin mağdurun gizli anahtarını ele geçirip, hesaptaki parayı kendisinin veya başkasının hesabına geçirmeye çalışırken, hesabın bulunduğunu takas merkezine ait güvenlik sisteminin işlemi engellemesi gibi, işlemin kendi iradesi dışında kesilmesi durumunda hırsızlık suçuna teşebbüs söz konusu olacaktır.

b. İçtima

Hırsızlık suçu için, farklı bir içtima durumu öngörülmemiş olup, suçların içtimai bölümünde (TCK m. 42-44) yer alan hükümler uygulanmaktadır. Örneğin fail, bir kişiye ait birden fazla hesapta bulunan kripto parayı almışsa, tek bir hırsızlık suçu meydana gelecektir⁴⁰⁶.

⁴⁰⁴ Centel, Zafer, Çakmut, **a.g.e.**, s. 373.

⁴⁰⁵ Koca, Üzülmüş, **a.g.e.**, s. 575.

⁴⁰⁶ "1- Bir süre Finansbank Antalya Şube Müdürü olarak görev yaptıktan sonra 31.01.2009 tarihinde görevinden istifa ederek ayrıldığı anlaşılan sanığın, bankada hesapları bulunan Sencer Sarp Aral ve Ayişe Eker isimli şahısların istemleri olmaksızın, banka çalışanları ve yı yönlendirerek onlar adına sistem üzerinden banka kartları ve şifre talep ettirdikten sonra bu banka kartları ve şifreleri eline geçirmek; bilgisayar üzerinden işlem yaparak adi geçen hesap sahiplerinin sisteme tanıtılmış telefon numaraları yerine sisteme kendi telefon numarasını tanıtmak; daha sonra -müfettiş soruşturma raporunda da belirtildiği üzere- kart numarası, kartın son kullanma tarihi, cep telefonu numarası, hesap numarası bilgileri girilmeksizin talep edilmesinin mümkün olmadığı anlaşılan internet bankacılığı şifresini, sözü edilen bilgileri kullanmak suretiyle cep telefonu ile her iki hesap sahibi için ayrı ayrı talep ve temin etmek; 24.04.2007 ile 14.11.2008 tarihleri arasında toplam 35 işlemle, bankadan istifa ederek ayrıldığı 31.01.2009 tarihinden sonra 17.04.2009 ile 02.05.2009 tarihleri arasında ise toplam 3 işlemle internet bankacılığını kullanmak suretiyle Sencer Sarp Aral'a ait 5 değişik hesaptan Ayişe Ekere alt 2 değişik hesaba toplam 480.657 TL ve 275.000 EUR havale yapmak; yine internet bankacılığın' kullanmak suretiyle 28.08.2007 tarihinde Sencer Sarp Aral'a ait hesaptan 3.900 EUR ve 13.600 EUR olmak üzere toplam 17.500 EUROyu Leyla Selçuk ve Seyfi Selçuk isimli şahısların hesaplarına transfer etmek; 25.04.2007-04.05.2009 tarihleri arasında ise, toplam 829 işlemle Ayişe Ekerin hesabına hale ettiği paraları banka kartı ile Finansbank ve diğer bankalara ait ATM cihazlarından çekmek şeklindeki eylemin 24.04.2007 ile 14.11.2008 tarihleri arasındaki döneme tekabül eden kısmının "zimetin açığa çıkmamasını sağlamaya yönelik hileli davranışlarla işlenmiş olması" da dikkate alınarak 5411 sayılı Yasanın 160/2.maddesinde düzenlenen zincirleme olarak nitelikli zimet suçunu; 17.04.2009 ile 02.05.2009 tarihleri arasındaki döneme tekabül eden kısmının ise, TCK'nun 142/2- e maddesinde düzenlenen zincirleme olarak bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeksizin, isabetsiz şekilde eylemin tamamının 5411 sayılı Yasanın 160/1.maddesinde düzenlenen zincirleme olarak basit zimet suçu kapsamında kaldığı gerekçesi ile yazılı şekilde karar verilmesi, (...)

Yasaya aykırı, katılan vekilinin temyiz itirazları bu itibarla yerinde görüldüğünden, hükmün 5320 sayılı Yasanın 8/1.maddesi gereğince yürürlükte bulunan 1412 sayılı CMUK'nun 321.maddesi uyarınca BOZULMASINA, 13.12.2010 günü oybirliğiyle karar verildi." 7.CD., 13.12.2010, 2010/8140 E., 2010/16852 K. (Yurtcan, **a.g.e.**, s. 79)

YGCK'nin müşterek zilyedi bulunan bir malın çalınmasını tek bir hırsızlık suçu kapsamında değerlendiren kararı⁴⁰⁷ göz önüne alındığında, müşterek hesapta tutulan kripto paraların çalınmasında, olayda birden fazla mağdur olsa da hepsi müşterek zilyet sayıldıklarından tek bir hırsızlık suçunun söz konusu olacağı kanaatindeyiz.

Hırsızlık suçunun zincirleme suç şeklinde işlenmesi de mümkündür⁴⁰⁸. Aynı suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı eylemin birden fazla işlenmesi durumunda bir cezaya hükmedilir. Mesela, ele geçirdiği gizli anahtar ile bir başkasının hesabında bulunan kripto parayı farklı zamanlarda kendi hesabına geçiren failin eylemleri, zincirleme suç kapsamında tek bir suç olarak kabul edilecektir. Bu durumda ceza TCK m. 43 gereği artırılacaktır⁴⁰⁹.

c. İştirak

Hırsızlık suçu, iştirak bakımından bir özellik göstermemektedir ve bu nedenle müşterek faillik, azmettirme ve yardım etme şeklinde her türlü iştirak söz konusu olabilir⁴¹⁰.

Kripto para örneğinde, bir kişinin hesabındaki kripto paralara erişimi sağlayan gizli anahtarı ele geçirmek için birlikte çalışan kişiler müşterek fail veya suça yardım edenler olarak değerlendirilecektir.

9. Yaptırım

Hırsızlık suçunun temel şeklinin işlenmesi durumunda, faile bir yıldan üç yıla kadar hapis cezası verilir (TCK m. 141/1).

Hırsızlık suçunda, TCK m. 142/1'de düzenlenen nitelikli hallerden biri gerçekleşmiş ise, faile verilecek ceza üç ilâ yedi yıl arası hapis cezasıdır.

⁴⁰⁷ YCGK, 11.06.2013, 2013/13-303 E., 2013/296 K. (emsal.yargitay.gov.tr)

⁴⁰⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 374; Aydın, **a.g.e.**, s. 267.

⁴⁰⁹ Özbek ve diğ., **a.g.e.**, s. 640.

⁴¹⁰ Koca, Üzülmüş, **a.g.e.**, s. 577; Aydın, **a.g.e.**, s. 267.

Hırsızlık suçunda, TCK m. 142/2’de düzenlenen nitelikli hallerden birisinin olması durumunda, verilecek ceza, beş ilâ on yıl arası hapis cezasıdır. Hırsızlığın, TCK m. 142/2-b bendinde düzenlenen ve kamuoyunda kapkaç ve yankesicilik olarak, beden veya ruh bakımından kendisini savunamayacak durumdaki mağdura karşı işlenmesi halinde verilecek ceza üçte biri oranına kadar artırılacaktır.

TCK m. 142/3. fıkradaki düzenlemeye göre, hırsızlığın sıvı veya gaz halindeki enerji hakkında ve bunların nakline, işlenmesine veya depolanmasına ait tesislerde işlenmesi durumunda verilecek ceza, beş ilâ on iki yıl hapis cezasıdır. Bu suç, bir örgüt faaliyeti olarak işlenmişse, ceza yarı oranında artırılır ve onbin güne kadar adli para cezası verilir.

TCK m. 142/5. fıkra göre, hırsızlık suçunun işlenmesi, haberleşme, enerji ya da demiryolu veya havayolu ulaşımı alanında kamu hizmetini geçici de olsa aksatmışsa, verilecek ceza, yarısından iki katına kadar artırılacaktır.

TCK m. 143’e göre, hırsızlık suçu gece işlendiği takdirde, ceza yarı oranında artırılır.

Hırsızlık suçunda, TCK m. 144’te düzenlenen cezayı hafifletici hallerin bulunması durumunda verilecek ceza, iki aydan bir yıla kadar hapis veya adli para cezasıdır.

TCK m.145’te düzenlenen malın değerinin az olması durumunda, faile verilecek cezada indirimle gidilebilir veya hiç ceza verilmeyebilir.

Hırsızlık suçu TCK m.146’da kullanma hırsızlığı kapsamında ise, verilecek ceza yarı oranına kadar indirilir. Fakat hırsızlığın amacı suç işlenmek ise bu indirim uygulanmaz.

İşlenen hırsızlık suçunda, TCK m. 147’de düzenlenen zorunluluk hali söz konusu ise, cezada indirim yapılabilir veya hiç cezaya hükmedilmeyebilir.

10. Muhakemeye İlişkin Kurallar

Hırsızlık suçu re'sen kovuşturulan suçlardandır. Fakat TCK m. 144'te düzenlenen cezayı hafifletici haller ile TCK m. 146'te düzenlenen kullanma hırsızlığının söz konusu olduğu durumlarda kovuşturma, mağdurun veya suçtan zarar görenin şikâyetine bağlıdır.

5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddeleri uyarınca hırsızlık suçunun basit hali ve nitelikli halleri için suçu kovuşturmayla görevli mahkeme asliye ceza mahkemesidir. TCK m. 142/3. fıkradaki düzenlemeye göre, hırsızlığın sıvı veya gaz hâlindeki enerji hakkında ve bunların nakline, işlenmesine veya depolanmasına ait tesislerde işlenmesi durumunda verilecek cezanın üst sınırı on iki yıl olduğundan, bu durumda suçu kovuşturmayla görevli mahkeme ağır ceza mahkemesidir⁴¹¹.

B. Yağma (TCK m. 148-150)

1. Genel Olarak

Yağma suçu, Türk Ceza Kanunu'nda ikinci kitabın ikinci kısmında *Malvarlığına Karşı Suçlar* başlıklı onuncu bölümde 148 ilâ 150. maddeleri arasında düzenlenmiştir. TCK m. 148'de yağma suçunun temel şekli, TCK m. 149'da daha ağır cezayı gerektiren nitelikli haller ve TCK m. 150'de cezada indirime gidilecek haller düzenlenmiştir.

Yağma suçu, taşınır malın yağması (TCK m. 148/1) ve senedin yağması (TCK m. 148/2) olarak iki farklı şekilde düzenlenmiştir.

Taşınır malın yağması, *“Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden ya da malvarlığı itibarıyla büyük bir zarara uğratacağından bahisle tehdit ederek veya cebir kullanarak, bir malı teslim veya malın alınmasına karşı koymamaya mecbur*

⁴¹¹ Centel, Zafer, Çakmut, **a.g.e.**, s. 378.

kılan kişi, altı yıldan on yıla kadar hapis cezası ile cezalandırılır.” şeklinde düzenlenmiştir.

Senedin yağması ise “Cebir veya tehdit kullanılarak mağdurun, kendisini veya başkasını borç altına sokabilecek bir senedi veya var olan bir senedin hükümsüz kaldığını açıklayan bir vesikayı vermeye, böyle bir senedin alınmasına karşı koymamaya, ilerde böyle bir senet haline getirilebilecek bir kağıdı imzalamaya veya var olan bir senedi imha etmeye veya imhasına karşı koymamaya mecbur edilmesi halinde de aynı ceza verilir.” olarak düzenlenmiştir.

Yağma, öğretide cebir veya tehdit yoluyla işlenen hırsızlık suçu olarak tanımlanmaktadır⁴¹². Yağma ile hırsızlık arasındaki fark, yağma suçunda cebir ve tehdit kullanma zorunluluğudur⁴¹³.

2. Suçun Faili

Yağma suçunun faili, maddede geçen “kişi” ifadesinden de anlaşılacağı gibi, herkes olabilir⁴¹⁴. Bu nedenle suç, özgül suç niteliğinde değildir. TCK m. 167’de, fail ile mağdur arasında belli bazı akrabalık bağlarının mevcut olması, diğer malvarlığı suçları için şahsi cezasızlık sebebi veya cezada indirim gerektiren şahsi sebep sayılmışken, yağma suçu bakımından bu sebeplerin uygulanması kabul edilmemiştir.

3. Suçun Mağduru

Yağma suçunun mağduru olmak için farklı bir nitelik aranmamıştır. Suçun mağduru, malı teslim veya malın alınmasına karşı koymamaya mecbur bırakılan kişidir. Mağdurun, suçun işlenmesi sırasında yaşıyor olması gerekir, çünkü mağdur cebir veya tehdidi hissetmelidir, aksi halde fiil, hırsızlık suçuna döner⁴¹⁵.

⁴¹² Özbek ve diğ., **a.g.e.**, s. 641.

⁴¹³ Dönmezer, **a.g.e.**, s. 428; Aydın, **a.g.e.**, s. 276.

⁴¹⁴ Koca, Üzülmüş, **a.g.e.**, s. 584; Aydın, **a.g.e.**, s. 276.

⁴¹⁵ Özbek ve diğ., **a.g.e.**, s. 642.

4. Suçla Korunan Hukuki Yarar

Yağma suçunda, hırsızlık ve cebir veya tehdit suçları bir arada bulunduğu için hem malvarlığı değerleri, başka bir deyişle zilyetlik ve mülkiyet hakları, hem de kişi güvenliği ve özgürlüğü korunmaktadır⁴¹⁶. Yağma suçunda cebir veya tehdit, malvarlığına yönelen suçta araç olduğu için, düzenleme malvarlığına işlenen suçlar bölümünde yapılmıştır⁴¹⁷.

5. Suçun Maddi Konusu

Yağma suçunun konusu, hırsızlık suçunun konusu olan mal ile aynıdır. Fakat yağma suçunda mal, hırsızlıktan farklı olarak cebir veya tehdit uygulanarak mağdurdan alınmaktadır.

Mal ile ilgili açıklamalar için, özellikle kripto para birimlerinin de kategorik olarak yer aldığı bilişim verilerinin mal olarak kabul edilmesi ile ilgili doktrindeki tartışmalar için, hırsızlık suçu kısmında yapılan açıklamalara bakılmalıdır⁴¹⁸.

6. Suçun Unsurları

a. Maddi Unsur

Yağma suçu, seçimlik hareketli bir suçtur⁴¹⁹. Malın teslimi veya alınmasına karşı konulmaması için cebir veya tehdit uygulanmalıdır. Bunun yanında yağma suçu birden fazla hareketli suçtur; ilk hareket, cebir veya tehdidin uygulanması, ikinci

⁴¹⁶ Centel, Zafer, Çakmut, **a.g.e.**, s. 384; Soyaslan, **a.g.e.**, s. 402; Koca, Üzülmöz, **a.g.e.**, s. 582; Dönmezer, **a.g.e.**, s. 428.

⁴¹⁷ Tezcan, Erdem, Önok, **a.g.e.**, s. 703; Koca, Üzülmöz, **a.g.e.**, s. 583.

⁴¹⁸ Bkz. s. 96.

⁴¹⁹ Centel, Zafer, Çakmut, **a.g.e.**, s. 385.

hareket ise malın alınmasıdır⁴²⁰. İlk hareket ile ikinci hareket arasında nedensellik bağlantısı olmalıdır⁴²¹.

Yağma suçunda cebir ve tehdit, zorlama aracı olarak kullanılmaktadır. Cebir fiziksel bir zorlama iken, tehdit manevi bir zorlamadır⁴²².

Cebir, zorlayıcı etki yaratan her türlü davranıştır⁴²³. Madde hükmü gereğince, mağdurun, herhangi bir vasıta ile kendisini bilmeyecek ve savunamayacak hale getirilmesi de, yağma suçunda cebir sayılır (TCK m. 148/3). Cebir, kişiye yönelik olmalıdır fakat eşyaya yönelik cebir mağdur üzerinde zorlayıcı etki oluşturuyorsa, cebrin dolaylı olarak kişiye yönelmiş olduğu kabul edilmelidir⁴²⁴.

TCK'de tehdit, TCK m. 106'da ayrı bir suç olarak tanımlanmıştır. Buna göre, tehdit mağdurun kendisine veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğine veya malvarlığı itibarıyla büyük bir zarara uğratacağına veya sair bir kötülük edeceğine dair bir beyan olarak anlaşılmalıdır⁴²⁵. Tehdidin mağdura doğrudan veya duyabileceği şekilde yapılması gerekir. Ayrıca tehditten kaynaklanan korku ile malın teslimi veya alınmasına karşı koymama arasında sebep-sonuç ilişkisi olmalıdır⁴²⁶.

Tehditte, cebirden farklı olarak, doğrudan kişi üzerinde zorlayıcı bir etkide bulunulmamakta, mağdur saldırının gerçekleştirileceğiyle korkutulmaktadır⁴²⁷.

⁴²⁰ Koca, Üzülmmez, **a.g.e.**, s. 598.

⁴²¹ Özbek ve diğ., **a.g.e.**, s. 643.

⁴²² Koca, Üzülmmez, **a.g.e.**, s. 589.

⁴²³ Özbek ve diğ., **a.g.e.**, s. 643; Yurtcan, **a.g.e.**, s. 215.

⁴²⁴ Tezcan, Erdem, Önok, **a.g.e.**, s. 707.

⁴²⁵ "Sanığın, kendini "Murat" olarak tanıtip yakınlarından 50.000 dolar para almak amacıyla değişik zamanlarda mağdurların ev, iş ve cep telefonlarını arayarak "parayı vermedikleri takdirde çocuklarına zarar vereceğini, elinde bulunan uygunsuz fotoğrafları yakınlarına göndereceğini ve ayaklarına sıkacağı" biçiminde tehditlerde bulunduğunun ve yakının Kemal'in cep telefonuna kayıtlı "bugün ölmek için güzel bir gün", "ben ölmeden önce güldürürüm", "senin için vur emri verildi", "50 bin dolar" biçimindeki sanığın kabullendiği ses kayıtlarından anlaşılması karşısında; eyleminin bir bütün halinde yağma suçunu oluşturduğu gözetilmeden kanıtların takdir ve değerlendirilmesinde yanılgıya düşülerek yazılı biçimde uygulama yapılması, (...) Bozmayı gerektirmiş, sanık Ö. savunmasının temyiz itirazı bu bakımdan yerinde görülmesi olduğundan, hükmün açıklanan nedenle istem gibi (BOZULMASINA), sanığın kazanılmış hakkının CMUK'nun 326/son maddesi uyarınca korunmasına, 02.06.2010 gününde oybirliğiyle karar verildi." 6.CD., 02.06.2010, 2009/11754 E., 2010/7967 K. (Yurtcan, **a.g.e.**, s. 157)

⁴²⁶ Centel, Zafer, Çakmut, **a.g.e.**, s. 351.

⁴²⁷ Tezcan, Erdem, Önok, **a.g.e.**, s. 709.

Cebir veya tehdidin doğrudan mağdura yöneltilmesi şart değildir, mağdurdaki malı teslim etmeyi veya malın alınmasına karşı koyma direncini kırabilmeyi sağlayacak herhangi bir kişiye yöneltilmesi yeterlidir⁴²⁸.

Cebir veya tehdit ile malın alınması veya teslimi arasında nedensellik bağı olmalıdır⁴²⁹.

Kanaatimize göre, hırsızlık suçu ile ilgili bölümde ifade edilen internet bankacılığı şifresinin tehdit veya cebirle geçirilip paranın başka bir hesaba havalesi, yağma suçunda da “almak” olarak değerlendirilmelidir.

Kripto para örneğinde, mağdur veya bir yakını üzerinde cebir veya tehdit uygulayarak, mağdurun kripto hesabına erişimini sağlayan gizli anahtarının ele geçirilip kullanılması ile mağdurun hesabındaki paraların bir başka hesaba aktarılması, yağma suçunu oluşturmaktadır. Keza para transferi işleminin cebir ve tehdit altındaki mağdur tarafından yapılması da aynı şekilde değerlendirilmelidir.

b. Hukuka Aykırılık Unsuru

Hırsızlık suçu için düzenlenen özel zorunluluk hali, yağma için kabul edilmemiş olmakla beraber, genel nitelikli zorunluluk halinin (TCK m. 25), yağma suçuna uygulanmasının önünde bir engel yoktur⁴³⁰. Örneğin evinde çıkan yangına müdahale etmek isteyen fail, komşusunu tehdit ederek yangın tüpünü almışsa, içinde bulunduğu zorunluluk halinden yararlanabilecektir.

Kripto para birimi örneğinde, ölümcül hasta çocuğunun tedavisi için, bir başkasını tehdit edip, ondan Bitcoin temin eden kişinin durumun zorunluluk hali kapsamında değerlendirilebilir.

Yağma suçunda, tehdit veya cebir gibi zorlayıcı bir etki altında olan mağdurun rızası geçerli değildir. Mağdurun malın alınmasına izin vermesi veya malı teslim

⁴²⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 350; Toroslu, **a.g.e.**, s. 147; Aydın, **a.g.e.**, s. 277.

⁴²⁹ Koca, Üzülmüş, **a.g.e.**, s. 601.

⁴³⁰ Centel, Zafer, Çakmut, **a.g.e.**, s. 393.

etmesi durumunda rızanın varlığından bahsedilemez. Çünkü mağdur, serbest irade ile rıza göstermemekte, zorlayıcı bir etki altında bulunmaktadır.

Kripto para birimi örneğinde, ölümle tehdit edildiği için hesabındaki bitcoin'leri, failin istediği hesaba transfer eden mağdurun gösterdiği rıza geçersizdir.

Bir başka hukuka uygunluk sebebi olan meşru savunmanın yağma suçlarında uygulanması pek mümkün gözükmemektedir. Bir kişinin kendisine veya başkasına yönelmiş haksız bir saldırıyı savuşturmak için cebir veya tehdit ile saldırganın malını alması çok görülebilecek bir durum değildir. Fakat üzerine doğrultulmuş silahı zorla alan kişi için meşru savunmadan bahsedilebilir⁴³¹.

Kanun hükmünü icra, yağma suçunda gerçekleşebilecek bir hukuka uygunluk sebebidir. Örneğin haciz memurunun, haczedilecek malları zilyedinden zorla alması, kanun hükmünü icra kapsamında değerlendirilecektir.

Kripto para örneğinde, suçtan kaynaklanan malvarlığı değerinin tutulduğu Bitcoin hesabına ait gizli anahtarın failden zorla alınıp hesaptaki bitcoin'lere el konulması, kanun hükmünü icra kapsamında değerlendirilecektir.

c. Kusurluluk

Yağma suçu kasten işlenebilen bir suçtur⁴³². Yağma suçunun düzenlenişinde hırsızlıkta aranan “yarar sağlama” saiki yer almadığı için suçun oluşması için genel kast yeterlidir. Fakat öğretide, bu özel kastın aranması gerektiği de ileri sürülmektedir⁴³³. Suç olası kastla da işlenebilir⁴³⁴.

⁴³¹ Koca, Üzülmmez, **a.g.e.**, s. 607.

⁴³² Soyaslan, **a.g.e.**, s. 407; Koca, Üzülmmez, **a.g.e.**, s. 605.

⁴³³ Soyaslan, **a.g.e.**, s. 410; Centel, Zafer, Çakmut, **a.g.e.**, s. 394; Toroslu, **a.g.e.**, s. 152; Koca, Üzülmmez, **a.g.e.**, s. 605; Dönmezer, **a.g.e.**, s. 435; Aydın, **a.g.e.**, s. 277. Aksi görüşte Özbek ve diğ., **a.g.e.**, s. 655.

⁴³⁴ Koca, Üzülmmez, **a.g.e.**, s. 605.

7. Suç ve Cezaya Etki Eden Nedenler

a. Suçu Ağırlaştırıcı Nedenler

Yağma suçunu ağırlatıcı nitelikli haller, TCK m. 149'da düzenlenmiştir. Buna göre, yağma suçunun;

- a) Silahla,
 - b) Kişinin kendisini tanınmayacak hale getirmesiyle,
 - c) Birden fazla kişi birlikte,
 - d) Yol kesmek suretiyle ya da konutta, işyerinde veya bunların eklentilerinde,
 - e) Beden veya ruh bakımından kendisini savunamayacak durumda bulunan kişiye karşı,
 - f) Var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak,
 - g) Suç örgütüne yarar sağlamak maksadıyla,
 - h) Gece vakti,
- işlenmesi halinde, suç *nitelikli yağmaya* dönüştürmekte ve verilecek cezayı artmaktadır.

Maddenin 2. fıkrasında, yağma suçunun işlenmesi sırasında kasten yaralama suçunun neticesi sebebiyle ağırlaşmış hallerinin (TCK m. 87) gerçekleşmesi durumunda, yağma suçu ile birlikte ayrıca kasten yaralama suçuna ilişkin hükümler uygulanacağı belirtilmektedir.

aa. Yağma suçunun silahla işlenmesi

Yağma suçunda silah kullanılması, mağdur üzerinde korkunun etkisini arttırıcı bir özellik arz ettiğinden, suçu ağırlaştırıcı nitelikli olarak düzenlenmiştir⁴³⁵. Silah, TCK m. 6/1'de tanımlanmıştır. Buna göre, ateşli silahlar; patlayıcı maddeler; saldırı ve savunmada kullanılmak üzere yapılmış her türlü kesici, delici veya bereleyici alet; saldırı ve savunma amacıyla yapılmış olmasa bile fiilen saldırı ve savunmada kullanılmaya elverişli diğer şeyler; yakıcı, aşındırıcı, yaralayıcı, boğucu, zehirleyici,

⁴³⁵ Centel, Zafer, Çakmut, **a.g.e.**, s. 396.

"Sanığın yanında diğer sanıklar olduğu halde, müştekiye polis olduğunu söyleyip silah çekerek namlusuna mermi sürer gibi yaparak, incelemek için cep telefonunu alması biçimindeki eylemi, silahlı yağma suçunu oluşturur." 6.CD., 2004/7368 E., 2006/2642 K. (Yurtcan, **a.g.e.**, s. 207)

sürekli hastalığa yol açıcı nükleer, radyoaktif, kimyasal, biyolojik maddeler silah kabul edilmektedir. Bu nitelikli halin gerçekleşmesi için failin silahlı olması yeterli olmayıp, mağdura yöneltmesi gerekmektedir⁴³⁶.

Kripto para biriminin suç konusu olduğu yağma suçu örneğinde, silahla tehdit edilen mağdurun hesabındaki kripto paraları failin istediği hesaba transfer etmesi durumunda, nitelikli yağma oluşacaktır.

bb. Yağma suçunun kişinin kendisini tanınmayacak bir hale koyması suretiyle işlenmesi

Yağma suçunun faili, yakalanmasını önlemek ve böylece cezadan kurtulmak amacıyla kendisini tanınmayacak hale getirmişse bu nitelikli halin uygulanması söz konusu olacaktır. Failin kendisini tanınmayacak hale koyması mağdur üzerinde daha çok korkutucu etki yapar⁴³⁷. Müşterek faillik durumunda, faillerden birisinin kendisini tanınmayacak hale koyması, bunu bilen tüm fail ve suç ortakları için nitelikli halin uygulanması için yeterlidir⁴³⁸.

Kripto para örneğinde, failin kendisini tanınmayacak hale getirerek kripto para yağma suçunu işlemesi, bu nitelikli halin uygulanması gerektirir. Örneğin tanınmamak için maske takan fail, mağduru tehdit ederek ona ait kripto paraların kendi hesabına aktarılmasını sağlarsa, nitelikli yağma söz konusu olur.

cc. Yağma suçunun birden fazla kişi tarafından birlikte işlenmesi

Bu nitelikli hal, müşterek faillerin bulunduğu yağma suçlarında uygulanacaktır. Fail, en az iki kişi olmalıdır. Birden fazla kişinin birlikte suçu işlemesi arandığından suça azmettirme veya yardımcı olarak katılma durumunda bu nitelikli hal oluşmaz⁴³⁹.

Kripto para örneğinde, birden fazla failin birlikte cebir veya tehdit uygulayarak mağdurdan ele geçirdikleri gizli anahtarları kullanarak onun hesabından kendi

⁴³⁶ Tezcan, Erdem, Önok, **a.g.e.**, s. 714.

⁴³⁷ Soyaslan, **a.g.e.**, s. 420.

⁴³⁸ Tezcan, Erdem, Önok, **a.g.e.**, s. 715.

⁴³⁹ Centel, Zafer, Çakmut, **a.g.e.**, s. 398; Soyaslan, **a.g.e.**, s. 421.

hesaplarına kripto para transferi gerçekleştirmeleri durumunda bu nitelikli hal uygulanabilmelidir.

dd. Yağma suçunun yol kesmek suretiyle ya da konutta, işyerinde veya bunların eklentilerinde işlenmesi

Yağma suçunun yol keserek ya da konut veya işyerinde işlenmesi nitelikli yağma olarak düzenlenmiştir. Bu durumların, suçu ağırlatıcı hal sayılmasının sebebi, aynı zamanda seyahat özgürlüğünün kısıtlanmış ve konut veya işyeri dokunulmazlığının ihlal edilmiş olmasıdır⁴⁴⁰. Yol kesmede, başkalarından yardım isteme de zorlaştırılarak suçun işlenişi kolaylaştırılmaktadır⁴⁴¹. TCK'de konut ve işyeri dokunulmazlığının ayrı birer suç olarak düzenlenmiştir (TCK m. 116/1. ve 2. fıkralar). Bu nedenle kanun koyucunun konut ve işyeri dokunulmazlığını yağma suçunda nitelikli hal olarak düzenlemesiyle, yeni bir birleşik suç oluşturduğu anlaşılmaktadır.

Kripto para örneğinde, mağdurun yolu kesilerek ya da konutunda veya işyerinde cebir ve tehdit uygulanarak kripto para birimlerinin hesabından faillerin istediği hesaba aktarılması durumunda bu nitelikli hal uygulama alanı bulabilecektir.

ee. Yağma suçunun beden veya ruh bakımından kendisini savunamayacak durumda bulunan kişiye karşı işlenmesi

Yağma suçunun kendisini beden ve ruh bakımından savunamayacak durumda bulunan kişiye karşı işlenmesi durumunda bu nitelikli hal oluşacaktır⁴⁴². Yağma suçunun, çocuğa, yaşlıya, hastaya, malule veya ruhi ve fiziksel olarak aciz kişiye karşı işlenmesi, faildeki ahlaki kötülüğün şiddetini göstermekte, kamu vicdanını daha çok yaralamakta⁴⁴³, ayrıca fiilin icrasını da kolaylaştırmaktadır⁴⁴⁴.

⁴⁴⁰ Centel, Zafer, Çakmut, **a.g.e.**, s. 398.

⁴⁴¹ Soyaslan, **a.g.e.**, s. 421.

⁴⁴² "Hükmün gerekçesinde, 20.10.1998 doğumlu olup, suçun işlendiği 06.05.2010 tarihinde on iki yaşından küçük olan yakınının "Mahkememizce gözlemlenen haliyle beden ve ruh sağlığı bakımından kendini koruyamayacak durumda" olduğunun kabul edildiği belirtilmesine karşın, bunu gösteren somut veriler açıklanmadan TCY'nın 149.maddesinin 1.fıkrası (e) bendinin de uygulanması temel ceza belirleme gerekçesi karşısında sonuca etkili görülmemiştir." 6.CD., 2011/17375 E., 2012/1443 K. (Yurtcan, **a.g.e.**, s. 183)

⁴⁴³ **A.g.e.**, s. 422.

Bu nitelikli halin kripto para biriminin suç konusu olduğu yağma suçlarında uygulanması mümkün gözükmemektedir. Yukarıda belirtilen özelliklere sahip mağdurlara cebir ve tehdit uygulayarak kripto paralarının alındığı olaylarda nitelikli yağma söz konusu olacaktır.

ff. Yağma suçunun var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak işlenmesi

Var olan veya var olduğu zannedilen suç örgütlerinin oluşturdukları korkutucu güçten yararlanarak yağma suçunun işlenmesi durumunda bu nitelikli hal meydana gelir. Örgütün gerçekten var olması gerekmediği gibi failin örgütün üyesi olması da gerekmez⁴⁴⁵. Suçun icrasında, örgütün korkutucu gücünün tehdit olarak kullanılmış olması gerektiği anlaşılmaktadır.

Kripto para biriminin suç konusu olduğu yağma suçlarında bu nitelikli hal uygulama imkânı bulabilir. Örneğin, X mafya örgütüne mensup olduğunu söyleyen ve mağdurdan 100 bitcoin'i kendi hesabına transfer etmesini isteyen failin eyleminde bu nitelikli hal söz konusudur.

gg. Yağma suçunun suç örgütüne yarar sağlamak maksadıyla işlenmesi

Yağma suçunun suç örgütüne yarar sağlamak amacıyla işlenmesi, nitelikli yağma olarak düzenlenmiştir. Örgüt, en az üç kişinin suç işlemek maksadıyla bir araya gelerek fiili bir birliktelik oluşturmalarıyla kurulmuş olur. Örgütün üye sayısı ve araç ve gereç bakımından suçları işlemeye elverişli olması gerekir (TCK m. 220). Örgütün varlığı için devamlılık şarttır⁴⁴⁶. Örgütün yaptığı eylemlerle korku salmış olması gerekir⁴⁴⁷. Suç örgütünün var olması gerekmeyle birlikte failin bu örgüte üye olması hükümde aranmamıştır. Örgütün, suç işlemek amacıyla kurulan örgüt (TCK m. 220) veya silahlı örgütü (TCK m. 314) olması da fark etmemektedir⁴⁴⁸.

⁴⁴⁴ Özbeke ve diğ., **a.g.e.**, s. 650.

⁴⁴⁵ **A.g.e.**

⁴⁴⁶ Centel, Zafer, Çakmut, **a.g.e.**, s. 401.

⁴⁴⁷ Soyaslan, **a.g.e.**, s. 422.

⁴⁴⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 402.

Kripto para örneğinde, failin yasadışı bir örgüte yarar sağlamak amacıyla, mağdura cebir ve tehdit uygulayarak hesabındaki kripto paraları alması durumunda, nitelikli yağma suçu oluşacaktır.

hh. Yağma suçunun gece vaktinde işlenmesi

Suçun gece vakti işlenmesi genel ağırlaştırıcı nitelikli bir hal olarak TCK m. 149/1-h'de düzenlenmiştir. Gece vakti, güneşin batmasından bir saat sonra başlayan ve doğmasından bir saat evvele kadar devam eden zaman süresini belirtmektedir (TCK m. 6/1-e). Bu düzenlemenin nedeni olarak yağma suçunun işlenmesindeki kolaylık gösterilmiştir⁴⁴⁹. Suçun bir kısmının gece vakti icra edilmesi, bu nitelikli halin gerçekleşmesi yeterlidir.

Yağma suçunun gece vakti işlenmesi genel nitelikli bir hal olarak düzenlendiği için, kripto para biriminin suç konusu olduğu yağma suçlarına uygulanması mümkündür. Örneğin, saat 23.00'te mağduru tehdit ederek hesabındaki kripto paraları kendi hesabına aktartan fail, nitelikli yağmadan ceza alacaktır.

b. Suçu Hafifleten Nedenler

Yağma suçuna verilecek cezada indirim öngören haller, TCK m. 150'de düzenlenmiştir. Bunlar, kişinin bir hukuki ilişkiye dayanan alacağını tahsil amacıyla tehdit veya cebir kullanması (TCK m. 150/1) ve yağma suçunun konusunu oluşturan malın değerinin azlığıdır (TCK m. 150/2). Bu nitelikli haller, kripto paranın suçun maddi konusunu oluşturduğu yağma suçlarında uygulama imkânı bulacaklardır.

aa. Kişinin bir hukuki ilişkiye dayanan alacağını tahsil amacıyla tehdit veya cebir kullanması

Kişinin geçerli bir hukuki ilişkiye dayanan alacağını tahsil etmek için cebir veya tehdit uygulaması durumunda, yağma suçu yerine tehdit veya kasten yaralama suçuna ilişkin hükümler uygulanacaktır.

⁴⁴⁹ Soyaslan, **a.g.e.**, s. 422.

Kripto para birimi örneğinde, hukuken geçerli bir ilişkiye dayanan alacağını mağdurdan tahsil etmek için, ona cebir veya tehdit uygulayarak Bitcoin veya benzeri kripto paranın kendisine teslim edilmesini sağlayan kişi bu nitelikli halden yararlanacaktır. Bu durumda fail hakkında, yağma suçundan değil, tehdit veya kasten yaralama suçundan hüküm kurulacaktır.

bb. Yağma suçunun konusunu oluşturan malın değerinin az olması

Yağma suçuna konu olan malın değerinin az olması durumunda verilecek cezada indirimle gidilebilir⁴⁵⁰. Böyle hallerde, verilecek ceza üçte birden yarıya kadar indirilebilir. Her olayda malın değerinin azlığı, objektif olarak değerlendirilmelidir⁴⁵¹. Değerin azlığı, daha çoğunu alabilme imkânı varken, yalnız ihtiyacı kadarını alma veya değer olarak az olanı alma şeklinde olabilir⁴⁵².

Yağma suçunda korunan hukuki yarar, sadece mülkiyet ve zilyetlik olmayıp aynı zamanda kişinin beden bütünlüğü, vücut ve ruh sağlığı olduğu için, bu cezayı hafifletici halin düzenlenmiş olması doktrinde eleştirilmiştir⁴⁵³.

Kripto paranın suç konusu olduğu yağma suçlarında, bu hafifletici nedenin uygulanabilmesi mümkündür. Örneğin, silahla tehdit edilen mağdurun hesabında bulunan yüklü miktarda kripto paranın tamamını alabilecek durumdayken, sadece ihtiyaç duyduğu cüz'i kısmı alan fail, bu nitelikli halden yararlanabilecektir.

c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep

Malvarlığı bölümünde yer alan suçlar için TCK m. 167'de belli yakınlık ilişkileri şahsi cezasızlık sebebi saymış, bazıları da cezayı hafifleten sebep olarak düzenlemiştir. Fakat yağma suçu, cezasızlık hali veya cezada indirim öngörülen suçlar arasında sayılmamıştır.

⁴⁵⁰ Aydın, **a.g.e.**, s. 280.

⁴⁵¹ Tezcan, Erdem, Önok, **a.g.e.**, s. 720.

⁴⁵² Centel, Zafer, Çakmut, **a.g.e.**, s. 403.

⁴⁵³ **A.g.e.**

d. Etkin Pişmanlık

TCK m. 168/3'te yağma suçu için etkin pişmanlık düzenlenmiştir. Buna göre, yağma suçu tamamlandıktan sonra fakat kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde, verilecek cezanın yarısına kadarı indirilir.

Etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi halinde, verilecek cezanın üçte birine kadarı indirilir (TCK m. 168/3).

Kısmen geri verme veya tazmin halinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır (TCK m. 168/4).

Cezayı kaldıran ya da azaltan şahsi sebep ile etkin pişmanlık hükümlerinden kripto paranın suç konusu olduğu yağma suçlarında da uygulama alanı bulmaları mümkündür. Örneğin, yağma suçu faili, kovuşturma başlamadan önce yaptığından pişmanlık duyarak aldığı malı iade eder veya mağdurun zararını telafi ederse, cezası yarıya kadar indirilir. Eğer fail, hakkında kovuşturma açıldıktan sonra, aldığı malı iade ederse, cezasının üçte birine kadarı indirilir.

8. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Yağma suçuna teşebbüs mümkündür⁴⁵⁴. Fail, cebir veya tehditle suçun icrasına başladıktan sonra, fiilin elde olmayan sebeplerle kesintiye uğraması durumunda suç tamamlanmayıp teşebbüs aşamasında kalmış olacaktır⁴⁵⁵.

⁴⁵⁴ Toroslul, a.g.e., s. 152; Koca, Üzölmez, a.g.e., s. 624; Soyaslan, a.g.e., s. 409; Aydın, a.g.e., s. 277.

⁴⁵⁵ Tezcan, Erdem, Önok, a.g.e., s. 722.

"Sanık M.D. nin bıçağı yakınan E.B. nin boğazına dayadığı sırada adı geçen yakınının üzerini arayan sanık M. U. nün yağmalanacak bir şey bulamadığının anlaşılması karşısında; sanıkların eyleminin kalkışma aşamasında kaldığının gözetilmeden yazılı biçimde tamamlanmış suçtan hüküm kurulması bozmayı gerektirmiştir." 6.CD., 2006/19303 E., 2007/5513 K. (Yurtcan, a.g.e., s. 162)

Kripto paranın yağma suçunun konusu olduğu suçlarda, failin mağdurun gizli anahtarını cebir ve tehdit uygulayarak ele geçirdikten sonra, hesaptaki parayı kendisinin veya başkasının hesabına geçirmeye çalışırken, internetin kesilmesi gibi işlemin kendi iradesi dışında kesilmesi durumunda yağma suçuna teşebbüs söz konusu olacaktır.

b. İçtima

Yağma suçunda, TCK'de ayrı birer suç olarak düzenlenen cebir kullanma (TCK m. 108) veya tehdit (TCK m. 106), araç olarak suçun unsurunda yer alırlar ve birleşik suç meydana getirirler. Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir (TCK m. 42). Bu nedenle cebir veya tehdit için ayrı ayrı cezalandırmaya gidilmeden, yağma suçu için tek bir cezaya hükmedilir.

Yağma suçunda konut ve işyeri dokunulmazlığı suçları da, birer nitelikli unsur olarak bulunabilirler (TCK m. 149/1-d). Yine birleşik suç hükmüne göre konut veya işyeri dokunulmazlığının ihlal edilmesi ayrıca cezalandırılmayacak fakat nitelikli yağma olarak değerlendirilecektir⁴⁵⁶.

Yağma suçunda zincirleme suç hükümleri uygulanmaz⁴⁵⁷. Bu nedenle aynı suç işleme kararına bağlı olarak farklı zamanlarda aynı kişiye karşı veyahut aynı zamanda birden fazla kişiye yağma suçu işlense, fiil ve mağdur sayısınca yağma suçu oluştur ve her birisi birbirinden bağımsız olarak cezalandırılır. Örneğin fail, bir kişiye ait hesapta bulunan kripto parayı farklı zamanda cebir ve tehdit uygulayarak almışsa veya aynı anda birden fazla kişinin gizli anahtarını cebir ve tehdit kullanarak elde edip hesaplarındaki paralara el koymuşsa, her bir fiil veya mağdur için farklı bir yağma suçu meydana gelmiştir.

⁴⁵⁶ Centel, Zafer, Çakmut, **a.g.e.**, s. 407.

⁴⁵⁷ Özbek ve diğ., **a.g.e.**, s. 659; Aydın, **a.g.e.**, s. 278.

"...Sanığın 02.04.2005 tarihinde, yakınının telefonuna tehdit içerikli mesaj göndermek suretiyle 750 milyon lira para isteyip, aynı parayı almak için 04.04.2005 ve 05.04.2005 tarihinde de yine tehdit içerikli mesajlar göndererek eylemini devam ettirmesi biçimindeki oluşt, Ceza Genel Kurulunun 04.05.2010 gün ve 2010/63-102 sayılı kararı ve Dairemizin yerleşmiş uygulamasına göre, eylem bir bütün olarak 5237 satıh TCK.nun 148/1, 35/2, 62. maddelerine uyan tek yağmaya kalkışma suçunu oluşturduğu gözetilmeden yanılgıya düşülüp, üç ayrı yağmaya kalkışma Suçunun oluşturduğu kabul edilerek yazılı şekilde hüküm kurulması, Bozmayı gerektirmiştir..." 6.CD., 05.05.2010, 2009/2569 E., 2010/5495 K. (Yurtcan, **a.g.e.**, s. 156)

Müşterek hesapta tutulan kripto paranın cebir ve tehdit uygulanarak alınması durumunda, mağdur sayısı birden fazla olsa da suç konusunun tek olmasından dolayı bir yağma suçunun oluştuğu kanaatindeyiz.

Kripto para birimlerinin suç konusu olduğu yağma suçlarında, mağdura ait gizli anahtarın ele geçirilmesi veya kripto paranın failin kontrol ettiği bir hesaba transfer edilebilmesi için mağdurun bilişim sistemine zorla girilmesi durumunda, TCK m. 243'te düzenlenen "bilişim sistemine girme" suçu da işlenmiş olacaktır. Burada bilişim sistemine girme, yağma suçu için geçit suç niteliğinde olduğu için, faile ayrıca bu suçtan ceza verilemeyeceği kanaatindeyiz.

c. İştirak

Yağma suçu iştirak bakımından bir özellik göstermemektedir ve bu nedenle müşterek faillik, azmettirme ve yardım etme şeklinde her türlü iştirak söz konusu olabilir. Cebir veya tehdidin faillerden biri, malı almanın da başka bir fail tarafından gerçekleştirilmesi durumunda, nitelikli yağma suçu altında düzenlenen yağmanın birden fazla kişi tarafından işlenmesi hali uygulanacaktır⁴⁵⁸.

Kripto para örneğinde, mağdurun hesabını kontrol eden gizli anahtarı ele geçirmek için ona cebir veya tehdit uygulayan fail ile parayı kendi hesabına aktaran fail farklı ise bunlar birlikte fail olarak değerlendirilecek ve nitelikli yağmadan cezalandırılacaklardır.

9. Yaptırım

Yağma suçunun cezası, altı yıldan on yıla kadar hapis cezasıdır (TCK m. 148/1). Yağma suçunda TCK m. 149'da düzenlenen nitelikli hallerin bulunması durumunda faile verilecek ceza, on yıldan on beş yıla kadar hapis cezasıdır.

⁴⁵⁸ Koca, Üzülmüş, **a.g.e.**, s. 625.

Yağma suçunda, suç konusu olan malın değerinin azlığı suçu hafifletici bir neden olarak düzenlenmiştir. Bu durumda faile verilecek ceza, üçte birden yarıya kadar indirilir (TCK m. 150/2).

TCK m. 167’de “*Hırsızlık, güveni kötüye kullanma ve dolandırıcılık suçlarının işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*” düzenlenmesinde yağma suçu belirtilmemiştir. Buna göre, lehine yağma suçu işlenen tüzel kişi için güvenlik tedbirlerine hükmolunamayacaktır⁴⁵⁹.

10. Muhakemeye İlişkin Kurallar

Yağma suçu re’sen kovuşturulan suçlardandır. Suçun takibi herhangi bir muhakeme şartına bağlanmamıştır.

5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun’un 12. maddesindeki özel düzenleme uyarınca yağma suçunu kovuşturmayla görevli mahkeme, ağır ceza mahkemesidir⁴⁶⁰.

C. Güveni Kötüye Kullanma (TCK m. 155)

1. Genel Olarak

Güveni kötüye kullanma suçu, Türk Ceza Kanunu’nda ikinci kitabın ikinci kısmında, *Malvarlığına Karşı Suçlar* başlıklı onuncu bölümde 155. maddede

⁴⁵⁹ A.g.e., s. 628.

⁴⁶⁰ "...Vicdani kanının oluştuğu duruşma sürecini yansıtan tutanaklar belgeler ve gerekçe içeriğine göre yapılan incelemede;

Sanığın, mağdura olan alacağını istediği, mağdurun parayı bir başkasına verdiğini ve ondan almasını söylemesi üzerine "parayı bana vereceksin, vermezsen sen, dağa kaldırıyorum" dediğinin iddia edilmesi karşısında; kanıtlanması halinde eylemin 5237 Sayılı TCK.nun 148 ve 150. maddelerinde tanımlanan yağma suçun oluşturabileceği, kanıtları değerlendirme ve davaya bakma görevinin Ağır Ceza Mahkemesine ait olduğu gözetilmeden, duruşmaya devamla hüküm kurulması..." 4.CD., 12.03.2012, 2010/3736 E., 2012/5555 K. (Yurtcan, a.g.e., s. 143)

düzenlenmiştir. Maddenin 1. fıkrasında suçun temel şekli, 2. fıkrasında ise nitelikli hali düzenlenmiştir.

Güveni kötüye kullanma suçunun temel şekli, *“Başkasına ait olup da, muhafaza etmek veya belirli bir şekilde kullanmak üzere zilyedliği kendisine devredilmiş olan mal üzerinde, kendisinin veya başkasının yararına olarak, zilyedliğin devri amacı dışında tasarrufta bulunan veya bu devir olgusunu inkar eden kişi, şikayet üzerine, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.”* olarak düzenlenmiştir.

2. Suçun Faili

Güveni kötüye kullanma suçunun faili, suç konusu malın zilyetliği kendisine devredilen kişidir⁴⁶¹. Bu nedenle suç, özgü suç niteliğindedir⁴⁶². Zilyetliğin devri, malın doğrudan veya hükmen verilmesi şeklinde failin mal üzerinde hâkimiyet kurabilmesine imkân sağlanmasıyla gerçekleşir. Fail, fer’i zilyet konumundadır. Örneğin, kripto para hesabı üzerinde kontrol imkânı sağlayan gizli anahtarın belli işlemlerin yapılması için bir kişiye verilmesi halinde, bu kişi hesaptaki bitcoin’leri başka hesaplara gönderebilecek veya mal ve hizmet alabilecek imkâna kavuşmakta ve bu şekilde hesap üzerinde fer’i zilyetlik kazanmaktadır.

Güveni kötüye kullanma suçunda fail, suç konusu malın maliki olamaz⁴⁶³. Bu nedenle, paylı veya elbirliği mülkiyete konu olan mallarla ilgili olarak, müşterek veya iştirak halinde malik olanlar birbirlerine karşı güveni kötüye kullanma suçunu işleyemezler⁴⁶⁴.

3. Suçun Mağduru

⁴⁶¹ Hafizoğulları, Özen, **a.g.e.**, s. 373; Toroslu, **a.g.e.**, s. 166.

⁴⁶² Asuman Aytekin İnceoğlu, “Güveni Kötüye Kullanma Suçu”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi (GÜHFD)**, C. 2018/1, 2018, s. 46.

⁴⁶³ İnceoğlu, **a.g.m.**, s. 46.

⁴⁶⁴ **Yeni TCK Madde Gerekçeleri - Türk Ceza Kanunu**, 155. madde gerekçesi, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, Erişim tarihi: 16.08.2018; İnceoğlu, **a.g.m.**, s. 46.

Güveni kötüye kullanma suçunda mağdur, malını muhafaza etmek veya belirli bir şekilde kullanmak üzere faile malın zilyetliğini devreden kişidir⁴⁶⁵. Mağdur, mal sahibi olabileceği gibi, ondan hukuka uygun olarak malın zilyetliğinin kendisine devredildiği kişi de olabilir⁴⁶⁶.

Tüzel kişiler, bu suçun mağduru olamaz fakat suçtan zarar gören olabilirler⁴⁶⁷.

4. Suçla Korunan Hukuki Yarar

Güveni kötüye suçunda korunan hukuki yarar, maddenin gerekçesinde mülkiyet hakkı olarak belirtilmiştir⁴⁶⁸. Öğretide, bu suçun düzenlenmesiyle hem malvarlığı değerleri, başka bir ifadeyle zilyetlik ve mülkiyet hakları, hem de kişilerin sözleşmeleri nedeniyle birbirlerine duydukları güven ilişkisinin korunduğu da ifade edilmektedir⁴⁶⁹.

5. Suçun Maddi Konusu

Güveni kötüye kullanma suçunun maddi konusu, başkasına ait maldır. Malın taşınır veya taşınmaz olması arasında bir ayrım gözetilmemiştir. Misli şeyler⁴⁷⁰ ve para da bu suça konu olabilir⁴⁷¹. Madde gerekçesinde belirtildiği gibi banka hesabındaki para güveni kötüye kullanma suçunun konusu olabilir⁴⁷².

Kripto para birimi örneğinde, mağdura ait Bitcoin hesabının gizli anahtarı belirli işler yapmak için kendisine teslim edilen kişi, bu paraları kendi hesabına aktararak sahiplenirse, güveni kötüye kullanma suçunu işlemiş olacaktır.

⁴⁶⁵ Hafizoğulları, Özen, **a.g.e.**, s. 374; Toroslu, **a.g.e.**, s. 167.

⁴⁶⁶ Centel, Zafer, Çakmut, **a.g.e.**, s. 465.

⁴⁶⁷ Koca, Üzülmüş, **a.g.e.**, s. 631.

⁴⁶⁸ Aynı görüşte Aydın, **a.g.e.**, s. 286.

⁴⁶⁹ Özbek ve diğ., **a.g.e.**, s. 681; Güven ihlali için bkz. Soyaslan, **a.g.e.**, s. 441.

⁴⁷⁰ “Alışverişte prensip itibarıyla sayma veya tartma veya ölçü ile belirli hale gelen eşya *misli eşyadır*. Bu mallarda bir malın yerini aynı cinsten bir diğeri alabilir. (Oğuzman, Seliçi, Oktay-Özdemir, **a.g.e.**, s. 12.)

⁴⁷¹ Tezcan, Erdem, Önok, **a.g.e.**, s. 742; Centel, Zafer, Çakmut, **a.g.e.**, s. 468.

⁴⁷² TCK 155. madde gerekçesi.

Kripto para birimi bakımından taşınır mal ile ilgili detaylı açıklama için, hırsızlık suçu bölümünde yapılan açıklamalara bakılmalıdır⁴⁷³.

6. Suçun Unsurları

a. Maddi Unsur

Fail, mal üzerinde zilyetliğin devir amacına aykırı olarak tasarrufta bulunmakta veya malın zilyetliğinin kendisine devredildiğini inkâr etmektedir^{474,475}. Malın tasarrufu çeşitli şekilde olabilir: Malı tüketme, değerini düşürme, başkasına rehin verme, devretme, harcama, başka mala dönüştürme, vs. Bu nedenle güveni kötüye kullanma suçu serbest hareketli bir suçtur⁴⁷⁶.

⁴⁷³ Bkz. s. 96.

⁴⁷⁴ Toroslu, **a.g.e.**, s. 173.

⁴⁷⁵ "...Hizmet nedeniyle güveni kötüye kullanma ve bilişim sistemindeki verileri değiştirme suçlarından sanığın mahkûmiyetine ilişkin hükümler sanık tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü;

Sanığın, katılana ait cep telefonu satış şirketinde satış sorumlusu olarak çalıştığı sırada, kendisine verilen şifre ile şirketin bilgisayar sistemine değişik tarihlerde izinsiz girmek suretiyle, stoktaki telefonları başkasına satılmış gibi gösterdikten sonra bu telefonları stoktan alarak değişik zamanlarda başkasına sattığı, böylece sanığın hizmet nedeniyle güveni kötüye kullanma ve bilişim sistemindeki verileri değiştirme suçlarını işlediğinin iddia edildiği olayda, sanık, katılan ve tanık beyanları ile dosya kapsamına göre, suçların sanık tarafından işlendiği sabit olmakla bu gerekçelere dayanan mahkemenin kabulünde bir isabetsizlik bulunmamıştır." 15.CD., 15.01.2018, 2017/2882 E., 2018/299 K. (emsal.yargitay.gov.tr)

"Güveni kötüye kullanma suçunun oluşabilmesi için; failin bir malın zilyedi olması, malın iade edilmek veya belirli bir şekilde kullanmak üzere faile rızayla tevdi ve teslim edilmesi, failin kendisine verilen malı, verilmiş gayesinin dışında, zilyedi olduğu malda malikmiş gibi satması, rehin etmesi, tüketmesi, değiştirmesi veya bozması ve benzeri şekillerde tasarrufta bulunması ya da devir olgusunu inkâr etmesi şeklinde, kendisine veya bir başkasına yarar sağlaması gerekmektedir..." 15.CD., 2012/14766 E., 2012/5962 K. (Yurtcan, **a.g.e.**, s. 257)

⁴⁷⁶ Özbek ve diğ., **a.g.e.**, s. 684.

Güveni kötüye kullanma suçunun oluşabilmesi için, suçtan önce fail ile mağdur arasında sözleşmeye dayalı bir güven ilişkisi olmalıdır⁴⁷⁷. Bu husus, madde gerekçesinde de belirtilmiştir⁴⁷⁸.

Kripto para birimi örneğinde, belli harcamaları yapmak üzere anlaştığı mağdurun kendisine teslim ettiği Bitcoin hesabı gizli anahtarını kullanarak, farklı harcamalar yapan kişinin fiili, güveni kötü kullanma suçu kapsamına girer.

Malın zilyetliğinin devrinin inkârı, fail tarafından malın zilyetliğinin kendisine devredildiğini inkâr edip malı sahiplenmesi, başka bir deyişle kendisi ile arasındaki hukuki ilişkiyi reddederek malı iade etmemesi anlamına gelmektedir⁴⁷⁹.

Kripto para birimi örneğinde, muhafazası amacıyla kendisine verilen bitcoin'leri geri vermesi istendiğinde, failin söz konusu parayı iade etmemesi durumunda güveni kötüye kullanma suçu oluşur.

b. Hukuka Aykırılık Unsuru

⁴⁷⁷ “...Şikayetçi ile aynı hastanenin aynı bölümünde tedavi gören ve şikayetçinin önceden tanımadığı sanığın, bir yakını ile görüşüp iade etmek bahanesi ile şikayetçiden istediği cep telefonunu alıp konuşur gibi yaparak, hastanenin salon kısmına doğru gidip olay yerinden uzaklaşması şeklinde gelişen olayda, başlangıçtan itibaren hırsızlık kastıyla hareket ettiği anlaşılan sanık ile müşteki arasında yasa koyucu tarafından güveni kötüye kullanma suçunun oluşması amacıyla aranan nitelikte, zilyetliğin devrine ilişkin, tarafların aldatılmamış özgür iradeleriyle kurulan ve hukuken geçerli olan bir sözleşme, dolayısıyla hukuksal anlamda geçerli bir zilyetlik devrinin bulunduğu ve sözleşme sonucu meydana gelmiş olan güvenden söz edilemez.

Bu nedenle güveni kötüye kullanma suçunun unsurları oluşmadığından, sanığın eylemi hırsızlık suçunu oluşturmaktadır. Ayrıca, olayda dolandırıcılık suçunun oluşabileceği düşünülebilir ise de; sanığın basit bir yalandan ibaret olan sözünün hileli davranış olarak kabulü olanaklı olmadığından, dolandırıcılık suçunun da oluşmayacağı açıktır.

Bu itibarla, itirazın kabulüne, Özel Daire onama kararının kaldırılmasına, yerel mahkeme hükmünün sanığın eyleminin hırsızlık suçunu oluşturmaya karşın güveni kötüye kullanma suçunu oluşturduğunun kabulü suretiyle suç vasfının hatalı belirlenmesi isabetsizliğinden bozulmasına karar verilmelidir...” CGK, 12.06.2012, 2015/15-440 E., 2012/229 K. (Yurtcan, **a.g.e.**, s. 17-25)

⁴⁷⁸ “Suçun konusunu oluşturan mal üzerinde belirli bir şekilde kullanmak üzere fail lehine zilyetlik tesisi gerekir. Bu nedenle, güveni kötüye kullanma suçunun oluşabilmesi için hukuken geçerli bir sözleşme ilişkisinin varlığı gereklidir. Bu hukuki ilişki, örneğin kira sözleşmesi, ariyet sözleşmesi, karz sözleşmesi, vedia sözleşmesi, istisna sözleşmesi, vekalet sözleşmesi, kefalet sözleşmesi, hizmet sözleşmesi, rehin sözleşmesi ile tesis edilmiş olabilir. Bu akdi ilişki, karma veya sui generis bir sözleşme ile de tesis edilmiş olabilir. Örneğin, bir bankada açılan carî hesaba veya bir “özel finans kurumu”nda açılan “katılım ortaklığı hesabı”na ilişkin sözleşme ile de bu hukuki ilişki tesis edilmiş olabilir. Keza, örneğin bir anonim şirket yönetim kurulu üyeleri ile şirket tüzelkişiliği arasındaki hukuki ilişki, hizmet ve/veya vekalet sözleşmesine dayanmaktadır. Hatta, mülkiyeti muhafaza kaydıyla satın alınmış olan eşyanın mesela bir üçüncü kişiye satılması durumunda dahi, güveni kötüye kullanma suçunun oluştuğu kabul edilmelidir.” (TCK 155. madde gerekçesinden)

⁴⁷⁹ Centel, Zafer, Çakmut, **a.g.e.**, s. 473.

Mağdurun rızası bu suçta hukuka uygunluk sebebidir⁴⁸⁰. Muhafaza veya belli bir şekilde kullanma amacıyla bir malın zilyetliği kendine devredilmiş kişinin, devir olgusunu inkâr etmesine veya mal üzerine belirlenen kullanım biçimlerinden farklı şekilde de tasarruf etmesine mal sahibinin rızası var ise, bu durum eylemi suç olmaktan çıkarır.

Zorunluluk halinin güveni kötüye kullanma suçunda uygulanması mümkündür⁴⁸¹. Örneğin eşinin fenalaşması üzerine, kendisine muhafaza kaydıyla bırakılan bitcoin'leri harcayan kişinin içinde bulunduğu zorunluluk, eylemi hukuka uygun kılacaktır.

Meşru savunmanın bu suçta uygulanması pek mümkün gözükmemektedir. Fakat güveni kötüye kullanma suçunun failinin, zilyetliği kendisine devredilen mal üzerinde hapis hakkı⁴⁸² doğmuşsa, bu hakkın kullanılması hukuka uygunluk sebebi olacaktır⁴⁸³.

Kripto para birimi örneğinde, mağdurdan muaccel alacağı bulunan fail, gizli anahtarı kendisine rızayla teslim edilmiş hesapta bulunan bitcoin'ler üzerinde, borcu ödeninceye kadar hapis hakkını kullanırsa, bu hukuka uygunluk sebebinden yararlanacaktır.

c. Kusurluluk

Güveni kullanma suçu kasten işlenebilen bir suçtur⁴⁸⁴. Kast, suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir. Buna göre, failin malın zilyetliğini kendisine devreden kişi ile arasındaki hukuki ilişkiye aykırı olarak

⁴⁸⁰ Özbek ve diğ., **a.g.e.**, s. 688.

⁴⁸¹ İnceoğlu, **a.g.m.**, s. 69.

⁴⁸² **TMK 950** - Alacaklı, borçluya ait olup onun rızasıyla zilyedi bulunduğu taşınırı veya kıymetli evrakı, borcun muaccel olması ve niteliği itibarıyla bu eşyanın alacak ile bağlantısı bulunması hâlinde, borç ödeninceye kadar hapsedebilir.

Zilyetlik ve alacak ticarî ilişkiden doğmuşsa, tacirler arasında bu bağlantı var sayılır.

Alacaklı, borçluya ait olmayan taşınırlar üzerinde de zilyetliğin iyiniyetle kazanılmasının korunduğu ölçüde hapis hakkına sahip olur.

⁴⁸³ Koca, Üzülmüş, **a.g.e.**, s. 639; İnceoğlu, **a.g.m.**, s. 69.

⁴⁸⁴ Soyaslan, **a.g.e.**, s. 445; Centel, Zafer, Çakmut, **a.g.e.**, s. 476; Hafizoğulları, Özen, **a.g.e.**, s. 379; Aydın, **a.g.e.**, s. 288; İnceoğlu, **a.g.m.**, s. 70.

kullandığını bilmesi yeterlidir⁴⁸⁵. Suçun oluşumunda genel kast dışında başka bir saik aranmadığı için suç, olası kastla da işlenebilir⁴⁸⁶.

Kripto para birimi örneğinde, belirli şekillerde tasarruf edilmek üzere gizli anahtar kendisine teslim edilen fail, hesaptaki bitcoin'lerin kendisinin olmadığını bilmesine rağmen sahiplenmek için bu paraları kendi hesabına aktarıyorsa, suç işleme kastıyla hareket ettiği kabul edilecektir.

7. Suç ve Cezaya Etki Eden Nedenler

a. Suçu Ağırlaştırıcı Nedenler

Güveni kötüye kullanma suçunun nitelikli hali TCK m. 155/2'de düzenlenmiştir. Buna göre, *“Suçun meslek ve sanat, ticaret veya hizmet ilişkisinin ya da hangi nedenden doğmuş olursa olsun, başkasının mallarını idare etmek yetkisinin gereği olarak tevdi ve teslim edilmiş eşya hakkında işlenmesi halinde, bir yıldan yedi yıla kadar hapis ve üçbin güne kadar adli para cezasına hükmolunur.”*

Fıkarda belirtilen nitelikli hal, söz konusu hukuki ilişkilerin dayandığı yoğun güven ilişkisidir⁴⁸⁷. Kanun koyucu bu güven ilişkisinin ihlal edilmesini suçla ağırlaştırıcı bir nitelik olarak düzenlemiştir⁴⁸⁸.

Kripto para örneğinde, kripto para takas merkezinin, mağdurun muhafaza kaydı ile teslim ettiği bitcoin'leri harcaması veya devir olgusunu inkâr etmesi durumlarında güveni kötüye kullanma suçunun nitelikli hali oluşacaktır.

b. Suçu Hafifleten Nedenler

Kanunda güveni kötüye kullanma suçu için cezayı hafifleten nitelikli haller öngörülmemiştir.

⁴⁸⁵ Koca, Üzülmüş, **a.g.e.**, s. 639.

⁴⁸⁶ Özbek ve diğ., **a.g.e.**, 688; Centel, Zafer, Çakmut, **a.g.e.**, s. 476; Aydın, **a.g.e.**, s. 288; İnceoğlu, **a.g.m.**, 72.

⁴⁸⁷ İnceoğlu, **a.g.m.**, s. 73.

⁴⁸⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 478.

c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep

Malvarlığı bölümünde yer alan suçlar için TCK m. 167’de belli yakınlık ilişkileri şahsi cezasızlık sebebi sayılmış, bazıları da cezayı hafifleten sebep olarak düzenlenmiştir. Güveni kötüye kullanma, şahsi cezasızlık hali veya cezada indirim öngörülen suçlar arasındadır.

Buna göre güveni kötüye kullanma suçu, TCK m. 167/1’de belirtilen akrabalar arasında işlenmesi halinde, faile ceza verilmez.

Suç, TCK m.167/2’de sayılan akrabalar arasında işlenmesi durumunda, faile verilecek ceza, yarısı oranında indirilir.

Kripto para birimi örneğinde, babasının kendisine teslim ettiği gizli anahtarı kullanıp hesaptaki bitcoin’leri kendi hesabına aktaran kişiye ceza verilmeyecektir.

d. Etkin Pişmanlık

Malvarlığı suçları için TCK m. 168’te düzenlenmiş etkin pişmanlık hükümleri, güveni kötüye kullanma suçu için de geçerlidir. Buna göre, kendisine muhafaza kaydıyla verilmiş bitcoin’leri iade etmeyen kişi, daha sonra pişmanlık duyarak kovuşturma başlamadan önce onları aynen iade ederse cezası üçte ikisine kadar indirilecektir (TCK m. 168/1). Fail, kovuşturmadan sonra, fakat daha hüküm verilmeden bitcoin’leri aynen iade ederse veya mağdurun zararını karşılırsa, cezası yarı oranına kadar indirilecektir (TCK m. 168/2). Eğer bitcoin’leri kısmen iade eder veya mağdurun zararını kısmen giderirse, bu durumda etkin pişmanlık hükümlerinden yararlanabilmesi, mağdurun rızasına bağlı olacaktır (TCK m. 168/4).

8. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Güveni kötüye kullanma suçu, sırf hareketli bir suçtur⁴⁸⁹ ve teşebbüse elverişlidir⁴⁹⁰. Failin, malın zilyetliği devralmasından sonra, verilen amacın dışında mal üzerinde tasarrufta bulunmaya çalışırken, fiilin elde olmayan sebeplerle kesintiye uğraması durumunda suç tamamlanmamış olacak, suça teşebbüs söz konusu olacaktır. Fakat diğer seçimlik hareket olan zilyetliğin devri olgusunun inkârı şeklinde gerçekleşen suçta, teşebbüs mümkün gözükmemektedir⁴⁹¹. Suçta hareketten ayrı bir netice söz konusu olmadığı için teşebbüsün mümkün olmadığı da öne sürülmüştür⁴⁹².

Kanaatimize göre, güveni kötüye kullanma suçunda teşebbüs mümkündür. Kripto para örneğinde, mağdurun gizli anahtarının kendisine teslim edildiği fail, hesaptaki parayı kendisinin veya başkasının hesabına geçirmeye çalışırken, işlemin kendi iradesi dışında kesilmesi durumunda güveni kötüye kullanma suçuna teşebbüs söz konusu olacaktır.

b. İçtima

Güveni kötüye kullanma suçu ile zimmet suçu arasında genel norm-özel norm ilişkisi vardır⁴⁹³. Kamu görevlisi, görevi gereği kendisine teslim edilen mal üzerinde teslim amacına aykırı olarak tasarrufta bulunursa veya malın zilyetliğinin kendisine devredildiğini inkâr ederse, görevi kötüye kullanma suçu değil, özel norm niteliğindeki zimmet suçu (TCK m. 247) oluşacaktır⁴⁹⁴.

⁴⁸⁹ Koca, Üzülmüş, **a.g.e.**, s. 642; Toroslu, **a.g.e.**, s. 175; İnceoğlu, **a.g.m.**, s. 68.

⁴⁹⁰ Soyaslan, **a.g.e.**, s. 445; Centel, Zafer, Çakmut, **a.g.e.**, s. 480; Toroslu, **a.g.e.**, s. 175; İnceoğlu, **a.g.m.**, s. 77.

⁴⁹¹ Centel, Zafer, Çakmut, **a.g.e.**, s. 480.

⁴⁹² Aydın, **a.g.e.**, s. 288.

⁴⁹³ Koca, Üzülmüş, **a.g.e.**, s. 643.

⁴⁹⁴ Tezcan, Erdem, Önok, **a.g.e.**, s. 750; Aydın, **a.g.e.**, s. 287.

Kripto para birimi örneğinde, haciz memurunun, kendisine muhafaza amacıyla teslim edilen gizli anahtarı kullanarak, hesaptaki bitcoin'leri kendi hesabına geçirirse, zimmet suçu işlemiş olacaktır.

Görevi kötüye kullanma seçimlik hareketli suç olduğundan failin bu hareketlerden birisini yapmasıyla suç oluşur⁴⁹⁵. Örneğin kendisine teslim edilen bilgisayar, bir başkasına satan kişi, bilgisayar almaya gelen sahibine, böyle bir bilgisayar almadığını iddia ederse, hem zilyetliği devretme amacına aykırı olarak tasarrufta bulunmak hem de devir olgusunu inkâr etmek şeklinde iki suçtan değil, tek bir suçtan sorumlu tutulacaktır⁴⁹⁶.

Kripto para birimi örneğinde, kendisine teslim edilen Bitcoin hesabındaki paraları, farklı amaçlarla harcayan ve hesaptaki paraların iadesi istendiğinde, hesabın kendisine ait olduğunu öne sürüp gizli anahtarı geri vermeyi reddeden kişinin, tek bir güveni kötüye kullanma suçu işlediği kabul edilecektir.

Failin belirtilen amaçlarla sahte belge düzenlemesi durumunda, ayrıca resmi belgede veya özel belgede sahtecilik suçu da oluşacaktır⁴⁹⁷.

Malın devri amacına aykırı tasarrufta bulunmak, kırmak, bozmak gibi mala zarar verme şeklinde gerçekleşirse, güveni kötüye kullanma ile mala zarar verme (TCK m. 155) arasında fikri içtima uygulanmalıdır⁴⁹⁸.

Güveni kötüye kullanma suçu, aynı kişiye değişik zamanlarda bir suç işleme kararının icrası kapsamında işlenmesi mümkündür⁴⁹⁹. Kripto para birimi örneğinde, kendisine teslim edilen Bitcoin hesabındaki bitcoin'leri, değişik zamanlarda, şahsi ihtiyaçları için kullanan kişinin eylemleri, zincirleme suç kapsamındadır.

c. İştirak

⁴⁹⁵ Centel, Zafer, Çakmut, **a.g.e.**, s. 481.

⁴⁹⁶ Koca, Üzülmüş, **a.g.e.**, s. 643; Centel, Zafer, Çakmut, **a.g.e.**, s. 481; Özbek ve diğ., **a.g.e.**, s. 690; Tezcan, Erdem, Önok, **a.g.e.**, s. 751; Aydın, **a.g.e.**, s. 288; İnceoğlu, **a.g.m.**, s. 79.

⁴⁹⁷ Aydın, **a.g.e.**, s. 289; Tezcan, Erdem, Önok, **a.g.e.**, s. 751; İnceoğlu, **a.g.m.**, s. 79.

⁴⁹⁸ Özbek ve diğ., **a.g.e.**, s. 690; Tezcan, Erdem, Önok, **a.g.e.**, s. 751.

⁴⁹⁹ Özbek ve diğ., **a.g.e.**, s. 690; Centel, Zafer, Çakmut, **a.g.e.**, s. 481.

Güveni kötüye kullanma suçu, iştirak bakımından bir özellik göstermemektedir ve bu nedenle müşterek faillik, azmettirme ve yardım etme şeklinde her türlü iştirak söz konusu olabilir. Fail bakımından özgü suç niteliğinden dolayı, ancak muhafaza etmek veya belirli bir şekilde kullanmak üzere, malın zilyetliği kendisine devredilen kişiler güveni kötüye kullanma suçunun faili olabilirler. Diğer kişiler, suça azmettiren veya yardımcı olarak katılabilir⁵⁰⁰.

9. Yaptırım

Güveni kötüye kullanma suçunun temel şeklinin cezası, altı aydan iki yıla kadar hapis ve adli para cezasıdır (TCK m. 155/1).

Adli para cezasının sınırları gösterilmediğinden, verilebilecek adli para cezası, TCK m. 52 gereğince 5 ilâ 730 gün arası belirlenen bir gün üzerinden hesaplanacak meblağ olabilir⁵⁰¹.

Güveni kötüye kullanma suçunun nitelikli haline verilecek ceza, bir yıldan yedi yıla kadar hapis ve üçbin güne kadar adli para cezasıdır (TCK m. 155/2).

10. Muhakemeye İlişkin Kurallar

Güveni kötüye kullanma suçunun temel şeklinin takibi, mağdurun şikâyetine bağlıdır. Şikâyet hakkı sahibi, malın malikidir⁵⁰². Suçun TCK m. 155/2’de düzenlenen nitelikli hali için şikâyet gerekmez, soruşturma makamlarınca re’sen takip edilir.

Güveni kötüye kullanma suçunun basit ve nitelikli halinin kovuşturmasıyla görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun’un 11. maddesi uyarınca asliye ceza mahkemesidir.

⁵⁰⁰ İnceoğlu, **a.g.m.**, s. 80.

⁵⁰¹ Centel, Zafer, Çakmut, **a.g.e.**, s. 483.

⁵⁰² Tezcan, Erdem, Önok, **a.g.e.**, s. 752.

D. Dolandırıcılık (TCK m. 157-159)

1. Genel Olarak

Dolandırıcılık suçu, 5237 sayılı Türk Ceza Kanunu'nda ikinci kitabın ikinci kısmında *Malvarlığına Karşı Suçlar* başlıklı onuncu bölümde 157 ilâ 159. maddeleri arasında düzenlenmiştir. TCK m. 157'de suçun temel şekli, TCK m. 158'de daha ağır cezayı gerektiren nitelikli haller ve TCK m. 159'da cezada indirimine gidilebilecek haller düzenlenmiştir.

Dolandırıcılık suçunun basit hali, “*Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası verilir.*” olarak düzenlenmiştir.

2. Suçun Faili

Dolandırıcılık suçunun faili herkes olabilir⁵⁰³. Fakat failin belirli kişiler olması, cezayı ağırlaştırıcı neden sayılmıştır⁵⁰⁴. Suçun oluşumu bakımından hileli davranışta bulunan kişi ile haksız yarar elde eden kişinin aynı olması gerekmemektedir⁵⁰⁵.

3. Suçun Mağduru

Dolandırıcılık suçunun mağduru herkes olabilir⁵⁰⁶. Mağdur, malvarlığı bakımından zarara uğrayan kişidir⁵⁰⁷. Doktrinde mağdurun, failin “*hileli davranışlarla bir kimseyi aldatma*” davranışını algılayacak seviyede algılama

⁵⁰³ Centel, Zafer, Çakmut, **a.g.e.**, s. 499; Koca, Üzülmmez, **a.g.e.**, s. 646; Hafizoğulları, Özen, **a.g.e.**, s. 397; Ali Parlar, **Ceza Hukukunda Dolandırıcılık Suçları**, 1. b., Ankara: Bilge Basım Yayım, 2011, s. 16.

⁵⁰⁴ Toroslu, **a.g.e.**, s. 180.

⁵⁰⁵ Koca, Üzülmmez, **a.g.e.**, s. 646.

⁵⁰⁶ Hafizoğulları, Özen, **a.g.e.**, s. 396.

⁵⁰⁷ Aydın, **a.g.e.**, s. 290; Parlar, **a.g.e.**, s. 17.

yeteneğine sahip olması gerektiği ifade edilmektedir. Aksi halde dolandırıcılık suçu yerine hırsızlık suçu oluşacaktır⁵⁰⁸.

4. Suçla Korunan Hukuki Yarar

Dolandırıcılık suçunun düzenlenmesiyle korunan hukuki yarar, kişinin malvarlığı değerleridir⁵⁰⁹. Bunun yanında, kişinin iradesinin fesada uğratılıp serbest karar verme özgürlüğünün de ihlal edildiğini öne süren bazı yazarlar, irade özgürlüğünün de korunan değerler arasında olduğunu belirtmektedirler⁵¹⁰.

5. Suçun Maddi Konusu

Dolandırıcılık suçunun maddi konusu, malvarlığında yer alan ve ekonomik değeri olan taşınır veya taşınmaz mallar şeklinde maddi varlıklar olduğu gibi alacak hakları ve fikri haklar gibi maddi olmayan varlıklar da olabilir⁵¹¹.

Öğretide Şen, Bitcoin'in elde edilmesiyle aktifi artıran ve kaybedilmesiyle pasifi çoğaltan niteliğiyle malvarlığı değerlerine dâhil olduğunu belirterek, Bitcoin'in dolandırıcılık suçuna konu olabileceğini ifade etmektedir⁵¹².

6. Suçun Unsurları

a. Maddi Unsur

Dolandırıcılık suçu birden fazla hareketli suçtur⁵¹³. Suç tanımında fiil, üç hareket unsuru içermektedir. Bunlar; (1) hileli davranışlarla mağduru aldatmak, (2) mağduru veya başkasını zarara uğratmak ve (3) kendisine veya başkasına yarar sağlamaktır⁵¹⁴. Bu bakımdan dolandırıcılık suçunun oluşumu, bu üç hareketin

⁵⁰⁸ Özbek ve diğ., **a.g.e.**, s. 695; Centel, Zafer, Çakmut, **a.g.e.**, s. 500; Aydın, **a.g.e.**, s. 291; Parlar, **a.g.e.**, s. 17.

⁵⁰⁹ Yurtcan, **a.g.e.**, s. 295; Koca, Üzülmmez, **a.g.e.**, s. 646; Hafizoğulları, Özen, **a.g.e.**, s. 397.

⁵¹⁰ Centel, Zafer, Çakmut, **a.g.e.**, s. 499; Tezcan, Erdem, Önok, **a.g.e.**, s. 753; Toroslu, **a.g.e.**, s. 180, Koca, Üzülmmez, **a.g.e.**, s. 646; Soyaslan, **a.g.e.**, 425; Aydın, **a.g.e.**, s. 290; Parlar, **a.g.e.**, s. 16.

⁵¹¹ Özbek ve diğ., **a.g.e.**, s. 694; Toroslu, **a.g.e.**, s. 185; Aydın, **a.g.e.**, s. 290; Parlar, **a.g.e.**, s. 16.

⁵¹² Şen, **Bitcoin Çalınır mı?** yazısı.

⁵¹³ TCK 157. madde gerekçesi; Koca, Üzülmmez, **a.g.e.**, s. 648; Yurtcan, **a.g.e.**, s. 295.

⁵¹⁴ Özbek ve diğ., **a.g.e.**, s. 696; Tezcan, Erdem, Önok, **a.g.e.**, s. 755; Toroslu, **a.g.e.**, s. 181; Koca, Üzülmmez, **a.g.e.**, s. 648.

gerçekleşmesine bağlıdır. Aksi halde teşebbüs veya başka bir suçun gündeme gelmesi söz konusu olacaktır.

Bazı yazarlar, suç fiilinin, hileli davranışlarla bir kimseyi aldatmak (hareket) ile mağdurun veya başkasının zararına olarak kendisine veya başkasına yarar sağlamak (netice) şeklinde iki unsurdan oluştuğunu kabul etmişlerdir⁵¹⁵.

Bazı yazarlar ise, dolandırıcılık suçunda bir hareket ve iki neticenin olduğunu ileri sürmüşlerdir. Hileli davranış, suç fiilinin hareket kısmını oluştururken, mağdurun aldanması (ilk netice) ve mağdurun malvarlığında zarar meydana gelmesi (ikinci netice), fiilin netice kısmını oluşturur⁵¹⁶.

Yargıtay’a göre dolandırıcılık suçunun oluşabilmesi için failin hile ile mağdurun iradesini fesada uğratarak kendisi veya başkası yararına haksız menfaat elde etmesi gerekir⁵¹⁷.

Suç fiilinin ilk unsuru hileli davranışlarla mağduru aldatmaktır. Fail, hileli davranışla mağdurun iradesi üzerinde etki ederek, onun karar vermesini yönlendirmekte ve fiilin diğer unsurlarında yer alan mağdurun veya başkasının zararına fakat kendisinin veya başkasının yararına bir işlemin tesisini sağlamaktadır.

Hile, kandırıcı nitelikte olmalı, her olayda ayrıca değerlendirilmeli, olayın özelliği, mağdurun durumu, faille olan ilişkisi, kullanılan hilenin şekli, kullanılmışsa gizlenen ve değiştirilen belgenin nitelikleri ayrı ayrı dikkate alınmalıdır⁵¹⁸.

Failin “soyut yalan” boyutunu aşmayan davranışları hile olarak nitelendirilemez⁵¹⁹.

⁵¹⁵ Özbek ve diğ., **a.g.e.**, s. 696; Soyaslan, **a.g.e.**, s. 426; Yurtcan, **a.g.e.**, s. 295; Dönmezer, **a.g.e.**, s. 449.

⁵¹⁶ Centel, Zafer, Çakmut, **a.g.e.**, s. 501.

⁵¹⁷ 15. CD., 06.03.2014, 2012/9534 E.; 201/4151 K. (Yurtcan, **a.g.e.**, s. 296.)

⁵¹⁸ Parlar, **a.g.e.**, s. 20.

⁵¹⁹ 11. CD., 28.01.2004, 12983-219 (Parlar, **a.g.e.**, s. 22.)

"...Dolandırıcılık suçunun oluşabilmesi için; failin bir kimseyi, kandırabilecek nitelikte hileli davranışlarla hataya düşürüp, onun veya başkasının zararına, kendisine veya başkasına yarar sağlaması gerekmektedir.

Hile nitelikli bir yalandır. Fail tarafından yapılan hileli davranış belli oranda ağır, yoğun ve ustaca olmalı, sergileniş açısından mağdurun inceleme olanağını ortadan kaldıracak nitelikte bir takım

Kripto para birimi örneğinde, kendisini müteahhit olarak tanıtip, mağdura daire satacağından bahisle, ondan bitcoin temin eden kişinin eyleminde aldatmaya yönelik davranış, failin kendisini müteahhit olarak tanıtmasıdır. Fakat bu aldatmanın soyut yalan boyutunu aşması, başka bir deyişle aldatıcı davranışın, “Ben müteahhitim” demekten ibaret olmaması, örneğin sözde satacağı daireyi mağdura gezdirmesi veya müteahhitlik işlerini yürüttüğü bürosunda mağdur ile görüşmesi gibi somut aldatıcı öğelerle desteklemiş olması gerekir.

Hile, icraî olabileceği gibi, ihmali davranışlarla da gerçekleştirilebilir⁵²⁰. Hilenin ihmali olarak gerçekleştirilebilmesi için madde gerekçesinde belirtildiği gibi, failin mağduru bilgilendirmek konusunda bir yükümlülüğü olmalıdır⁵²¹.

Fiilin ikinci unsuru, mağdurun veya başkasının bir zarara uğramasıdır. Hileli davranış ile sağlanan aldatma sonucunda mağdurun veya bir başkasının malvarlığında bir zarar meydana gelmesi gerekir. Doktrinde, zararın malvarlığına ilişkin olması gerektiği bu yüzden manevi yönden uğranılan zararların bu kapsamda değerlendirilmeyeceği ifade edilmektedir⁵²².

Fiilin üçüncü unsuru, failin hileli davranışla sağladığı aldatma neticesinde kendisine veya bir başkasına yarar sağlaması gerekmektedir. Fakat doktrinde mağdur zarara uğradığı halde failin malvarlığında bir artış olmasa dahi dolandırıcılık suçunun tamamlandığı ifade edilmektedir. Yargıtay da bu görüştedir⁵²³.

hareketler olmalıdır. Kullanılan hileli davranışlarla mağdur yanılgıya düşürülmeli ve bu yanıltma sonucu yalanlara inanan mağdur tarafından sanık veya bir başkasına haksız çıkar sağlanmalıdır. Hile nitelikli bir yalandır. Fail tarafından yapılan hileli davranış belli oranda ağır, yoğun ve ustaca olmalı, sergileniş açısından mağdurun inceleme olanağını ortadan kaldıracak nitelikte bir takım hareketler olmalıdır. Kullanılan hileli davranışlarla mağdur yanılgıya düşürülmeli ve bu yanıltma sonucu yalanlara inanan mağdur tarafından sanık veya bir başkasına haksız çıkar sağlanmalıdır. Hilenin kandırıcı nitelikte olup olmadığı olaysal olarak değerlendirilmeli, olayın özelliği, fiille olan ilişkisi, mağdurun durumu, kullanılmışsa gizlenen veya değiştirilen belgenin nitelikleri ayrı ayrı nazara alınmalıdır...” 15.CD., 21.03.2013, 2011/20886 E. 2013/5262 K. (Yurtcan, **a.g.e.**, s. 43-44)

⁵²⁰ Centel, Zafer, Çakmut, **a.g.e.**, s. 507; Koca, Üzülmmez, **a.g.e.**, s. 651; Toroslu, **a.g.e.**, s. 186.

⁵²¹ “Hataya düşen kişi ile hukuki ilişkide bulunulan durumlarda, böyle bir yükümlülük vardır. Ayrıca, muhatabın belli bir husustaki hatası karşısında kişinin ihmali davranışının, örneğin susmasının, bir beyan, açıklama değerini taşıması gerekir, mağdurda oluşan hatayı engelleme yükümlülüğü altında olması gerekir.” (TCK 157. madde gerekçesi)

⁵²² Tezcan, Erdem, Önok, **a.g.e.**, s. 771; Parlar, **a.g.e.**, s. 16.

⁵²³ Tezcan, Erdem, Önok, **a.g.e.**, s. 771.

Failin elde ettiđi yarar, kumar veya bahis alacađı gibi haksız veya ahlaka aykırı olabilir⁵²⁴.

b. Hukuka Aykırılık Unsuru

Genel hukuka uygunluk sebepleri arasında yer alan ilgilinin rızası, dolandırıcılık suçunda bulunmakla beraber, mağdurun iradesinin ifsat edilmesiyle sağlandığı için geçerli değildir⁵²⁵.

Kripto para birimi örneğinde, kendisine bilgisayar alacađından bahisle mağdurun kendisine bitcoin göndermesini sağlayan failin eyleminde, mağdurun paranın gönderilmesindeki rızası geçersizdir.

Zorunluluk hali, dolandırıcılık suçunda uygulama imkânı bulabilir. Örneğin hayati tehlike içinde olan çocuğunun tedavisi için, çaresiz kalan babanın dolandırıcılık suçu işlemesi buna bir örnektir⁵²⁶.

Kripto para birimi örneğinde, acil tedavi edilmesi gereken eşi için, kripto para birimi dolandırıcılığı yapan kişi, içinde bulunduğu zorunluluk halinden yararlanacaktır.

Meşru savunma, kanun emrini icra, yetkili merciden verilen emrin yerine getirilmesinin dolandırıcılık suçunda uygulanamayacağı belirtilmektedir⁵²⁷.

c. Kusurluluk

Dolandırıcılık suçu kasten işlenebilen bir suçtur⁵²⁸. Failin kastı, fiilin bütün unsurunu da içermelidir. Fail, mağduru hile ile aldattığını, mağdurun veya başkasının bundan zarar göreceğini ve kendisinin veya başkasının bu durumdan yararlanacağını

⁵²⁴ Centel, Zafer, Çakmut, **a.g.e.**, s. 513.

⁵²⁵ Özbek ve diğ., **a.g.e.**, s. 715.

⁵²⁶ Centel, Zafer, Çakmut, **a.g.e.**, s. 514.

⁵²⁷ Hafizoğulları, Özen, **a.g.e.**, s. 405.

⁵²⁸ Soyaslan, **a.g.e.**, s. 429; Centel, Zafer, Çakmut, **a.g.e.**, s. 514; Toroslu, **a.g.e.**, s. 189; Yurtcan, **a.g.e.**, s. 295; Aydın, **a.g.e.**, s. 291.

bilmeli ve neticeyi istemelidir⁵²⁹. Netice, mağdurun zararından failin yararlanmasıdır. Bu suç, olası kast ile de işlenebilir⁵³⁰.

Öğretide, dolandırıcılık suçunda farklı kast derecelerinin olması gerektiği öne sürülmüştür. Bazı yazarlar, suçun oluşumu için genel kastı⁵³¹ yeterli görürken, bazıları suçun ancak özel kastla⁵³² işlenebileceği öne sürmüş ve bazıları da suçun basit halinin genel kastla ve bazı nitelikli hallerinin özel kastla işlenebileceği ifade edilmiştir⁵³³.

Kanaatimize göre, dolandırıcılık suçu için genel kast yeterlidir. Failin, mağduru aldattığını bilmesi ve elde edeceği haksız çıkarın mağdurun veya bir başkasının zararına olduğunu bilmesi ve istemesi yeterlidir.

7. Suç ve Cezaya Etki Eden Nedenler

a. Suçu Ağırılaştıran Nedenler

Dolandırıcılık suçunun nitelikli halleri TCK m. 158’de düzenlenmiştir. Söz konusu hallerin işlenen fiilde bulunması durumunda, nitelikli dolandırıcılık suçu oluşacak ve fail aleyhine üç yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacaktır. Nitelikli dolandırıcılık olarak düzenlenen haller şunlardır:

- a) Dinî inanç ve duyguların istismar edilmesi suretiyle,
- b) Kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan yararlanmak suretiyle,
- c) Kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle,
- d) Kamu kurum ve kuruluşlarının, kamu meslek kuruluşlarının, siyasi parti, vakıf veya dernek tüzel kişiliklerinin araç olarak kullanılması suretiyle,
- e) Kamu kurum ve kuruluşlarının zararına olarak,

⁵²⁹ Soyaslan, **a.g.e.**, s. 429; Dönmezer, **a.g.e.**, s. 473.

⁵³⁰ Koca, Üzülmüş, **a.g.e.**, s. 657; Özbek ve diğ., **a.g.e.**, s. 715; Tezcan, Erdem, Önok, **a.g.e.**, s. 788; Centel, Zafer, Çakmut, **a.g.e.**, s. 515; Aydın, **a.g.e.**, s. 291.

⁵³¹ Tezcan, Erdem, Önok, **a.g.e.**, s. 787; Koca, Üzülmüş, **a.g.e.**, s. 657; Hafızogulları, Özen, **a.g.e.**, s. 405; Centel, Zafer, Çakmut, **a.g.e.**, s. 515; Parlar, **a.g.e.**, s. 23.

⁵³² Soyaslan, **a.g.e.**, s. 429.

⁵³³ Koca, Üzülmüş, **a.g.e.**, s. 657;

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,

g) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle,

h) Tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında,

i) Serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle,

j) Banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla,

k) Sigorta bedelini almak maksadıyla,

l) Kişinin, kendisini kamu görevlisi veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtması veya bu kurum ve kuruluşlarla ilişkili olduğunu söylemesi suretiyle.

Kripto para birimine karşı dolandırıcılık suçunun temel şekli olmasa da, Şen'in de yukarıda belirtilen görüşleri doğrultusunda, TCK m. 158/1-f'de nitelikli hal olarak düzenlenen "*Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle*" şeklinde işlenmesi mümkündür. Kripto para birimlerinin suç konusu olduğu dolandırıcılık suçlarında, maddede düzenlenen diğer nitelikli haller de varsa, hâkim temel cezayı tayin ederken bu durumu göz önüne alacaktır⁵³⁴.

Aşağıda kripto para birimlerinin suç konusu olduğu dolandırıcılık suçlarına uygulanabilecek nitelikli haller ele alınacaktır.

aa. Dolandırıcılık suçunun dinî inanç ve duyguların istismar edilmesi suretiyle işlenmesi

Dolandırıcılık suçunun kişilerde bulunan dinî inanç ve duyguların kötüye kullanılması suretiyle işlenmesi nitelikli dolandırıcılık kapsamına alınmıştır. Burada din, bir aldatmaca unsuru olarak kullanılmaktadır⁵³⁵. Bu düzenlemeyle, kişilerin sahip olduğu dinî duyguların kötüye kullanımının kolaylığı göz önüne alındığı ve

⁵³⁴ Centel, Zafer, Çakmut, **a.g.e.**, s. 515.

⁵³⁵ TCK 158. madde gerekçesi. Aynı görüşte Soyaslan, **a.g.e.**, s. 432.

dinî inançların kötüye kullanımının önlenmek istendiği söylenebilir. Muskacılık, üfürükçülük, sözde cami yaptırmak için para toplanması durumunda bu suç oluşur⁵³⁶.

Kripto para örneğinde, “Cami yapacağız” diyerek mağduru aldatan ve Bitcoin bağışı yapmasını sağlayan fail için bu nitelikli hal oluşacaktır.

bb. Dolandırıcılık suçunun kişinin içinde bulunduğu tehlikeli durum veya zor şartlardan yararlanmak suretiyle işlenmesi

Eğer mağdur tehlikeli veya zor durumda bulunuyor ve fail de bunun farkında olarak, bu halden yararlanıyorsa nitelikli dolandırıcılık suçu söz konusu olacaktır. Örneğin ölümcül bir hastalığa yakalanmış bir hastayı tedavi edeceğini söyleyerek aldatan ve ondan yarar sağlayan faile bu nitelikli hal uygulanır.

Tehlikede olduğunu, doğal bir felakete maruz kaldığını veya acil ameliyat olması gerektiğini beyan edip başkalarının acıma ve dayanışma duygularını istismar ederek onları aldatan faile de bu nitelikli hal uygulanacaktır⁵³⁷.

Kripto para birimi örneğinde, kendisini kanser hastası diye tanıtarak başkalarını aldatan ve onlardan Bitcoin temin eden kişinin eylemi, bu nitelikli hal kapsamındadır.

cc. Dolandırıcılık suçunun kişinin algılama yeteneğinin zayıflığından yararlanmak suretiyle işlenmesi

Algılama yeteneği zayıf olan; başka bir deyişle anlaması, kavraması, iyiyi kötünden, doğruyu yanlıştan, yararına olanı olmayandan ayırt etmede güçlük çeken mağdura karşı dolandırıcılık suçunun işlenmesi durumunda suçu ağırlaştırıcı nitelikli hal oluşacaktır. Algılama zayıflığının sebebi, yaş küçüklüğü, ileri yaş, sarhoşluk veya akıl zayıflığı olması fark etmez⁵³⁸.

⁵³⁶ Tezcan, Erdem, Önok, **a.g.e.**, s. 773.

⁵³⁷ Soyaslan, **a.g.e.**, s. 432; Dönmezer, **a.g.e.**, s. 271.

⁵³⁸ Özbek ve diğ., **a.g.e.**, s. 702.

Kripto para örneğinde, sarhoş ettiđi mağdurun algılama yeteneğinin zayıflamasından yararlanıp aldatarak ona ait bitcoin'leri kendi hesabına transfer eden faile bu nitelikli hal uygulanır.

dd. Dolandırıcılık suçunun kamu kurum ve kuruluşlarının, kamu meslek kuruluşlarının, siyasi parti, vakıf veya dernek tüzel kişiliklerinin araç olarak kullanılması suretiyle işlenmesi

Bu ağırlaştırıcı hal için söz konusu kurum ve kuruluşların aracı olarak kullanılması gerekir. Yargıtay'a göre, dolandırıcılık suçunda bu nitelikli halin oluşabilmesi için bu kurum ve kuruluşların adlarının kullanımı yeterli olmayıp, maddi varlıklarının da kullanılması gerekir^{539,540}.

Kripto para örneğinde, dernek başkanı olan failin, dernek merkezinde derneđi ziyarete gelmiş kişiyi, derneđe yardım bahanesiyle aldatıp mağdurdan kendi hesabına bitcoin transfer etmesini sağladığı durumunda bu nitelikli hal oluşacaktır.

ee. Dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi

Bilişim sistemlerinin sağladığı kolaylık veya banka ve kredi kurumlarının sahip oldukları güvenilirlik ve kolaylıklardan yararlanarak dolandırıcılık suçunun işlenmesi nitelikli bir hal olarak düzenlenmiştir^{541,542}.

⁵³⁹ Tezcan, Erdem, Önok, **a.g.e.**, s. 776.

⁵⁴⁰ "Sanığın belli bir isimden bahsetmeden Genelkurmay'da tanıdıklarının olduğundan bahisle askerlikten muaf tutulmayı sağlayacağı söylemesi, 5237 sayılı TCK.nun 158/2. maddesinde düzenlenen nitelikli dolandırıcılık suçunu değil, 157/1. maddede düzenlenen dolandırıcılık suçu oluşturur." 11.CD., 2006/6755 E., 2006/10432 K. (Yurtcan, **a.g.e.**, s. 349)

⁵⁴¹ Koca, Üzülmöz, **a.g.e.**, s. 661.

⁵⁴² "... Bilişim sisteminin aldatılmasından söz edilemeyeceđi için, ancak bu sistemin araç olarak kullanılarak bir insanın aldatılması yani dolandırılması halinde bu bendin uygulanması mümkündür. Aksi halde yani sisteme girilerek bir kişi aldatılmayıp sistemden yararlanılarak çıkar sağlanmışsa bilişim suçu veya bilişim sistemi kullanılmak suretiyle hırsızlık suçunun oluşması söz konusu olacaktır. (...) Bilişim sisteminden maksat, verileri toplayıp, yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir. Günümüzde bilişim sistemleri ile sesli-görüntülü haberleşme, elektronik imzanın kabulü, yeni ticari ilişkiler, internet bankacılığı hizmeti ile para transferleri ve bunlar gibi pek çok yenilik toplumsal hayata girmiş, bilişim gerek iş gerekse günlük hayatta vazgeçilemeyecek kadar önemli bir noktaya ulaşmış, bilişim teknolojileri daha hızlı ve ucuz bir nitelik arz etmesi nedeniyle, klasik yöntemlere nazaran daha fazla tercih edilir duruma gelmiştir. Bu sistemlerin güvenle kullanılması, aynı anda hızlı ve kolayca birçok kişi tarafından

Bu nitelikli halin, dolandırıcılık suçuyla, suç mağdurunun olmaması sebebiyle bağdaşmadığı da ileri sürülmüştür⁵⁴³. Bilişim sistemlerinin dolandırıcılık suçlarında kullanılmasının hilenin kandırıcı özelliğini artırmadığı, bu yüzden bilişim sistemlerinin dolandırıcılık suçlarında araç olarak kullanılmasının ağırlaştırıcı bir neden olarak sayılmasının doğru olmadığı belirtilmiştir⁵⁴⁴.

Kripto para birimlerinin suç konusu olduğu dolandırıcılık suçu da bu cezayı ağırlaştırıcı hal kapsamına girecek ve nitelikli dolandırıcılık olarak cezalandırılacaktır.

Şen'in, kripto para birimlerinden Bitcoin'e karşı dolandırıcılık suçunun işlenebileceğini belirten görüşü yukarıda⁵⁴⁵ belirtilmişti.

ff. Dolandırıcılık suçunun tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında işlenmesi

Madde gerekçesinde ticari faaliyetleri meslek olarak icra eden kişilerin güvenilirliğini sağlamak amacıyla dolandırıcılık suçunun tacir veya şirket yöneticisi olan ya da şirket adına hareket eden kişilerin ticari faaliyetleri sırasında; kooperatif yöneticilerinin kooperatifin faaliyeti kapsamında işlenmesi, bu suçun temel şekline

ulaşılması ve diğer taraftaki failin kontrol imkânını azaltması nedeniyle nitelikli hal sayılmıştır."

15.CD., 05.11.2015, 2015/14190 E., 2015/30942 K., (emsal.yargitay.gov.tr)

"... Bilişim sisteminden maksat, verileri toplayıp, yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir. Günümüzde bilişim sistemleri ile sesli-görüntülü haberleşme, elektronik imzanın kabulü, yeni ticari ilişkiler, internet bankacılığı hizmeti ile para transferleri ve bunlar gibi pek çok yenilik toplumsal hayata girmiş, bilişim gerek iş gerekse günlük hayatta vazgeçilemeyecek kadar önemli bir noktaya ulaşmış, bilişim teknolojileri daha hızlı ve ucuz bir nitelik arz etmesi nedeniyle, klasik yöntemlere nazaran daha fazla tercih edilir duruma gelmiştir. Bu sistemlerin güvenle kullanılması, aynı anda hızlı ve kolayca bir çok kişi tarafından ulaşılması ve diğer taraftaki failin kontrol imkânını azaltması nedeniyle nitelikli hal sayılmıştır..." CGK, 08.03.2016, 2014/288 E., 2016/255 K. (emsal.yargitay.gov.tr)

"1- Somut olayda, müştekinin daha önce çalınan aracı ile ilgili olarak sanığın müştekiyi telefonla arayarak vereceği hesap numarasına 2.000 TL yatırması halinde aracının yerini söyleyeceği, müştekinin bunun üzerine temin edebildiği 300 TL'yi sanığın verdiği hesap numarasına yatırdığı, sanığın da hesaba yatan parayı bankamatikten çektiği şeklindeki eylemin bankanın ödeme aracı olarak kullanılması karşısında 5237 sayılı TCKnun 157.maddesinde düzenlenen basit dolandırıcılık suçunu oluşturduğu gözetilmeksizin suç vasfında yanılığa düşülerek TCKnun 158/1-f maddesinde düzenlenen banka ve kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçundan hüküm kurulması..." 15.CD., 2011/11810 E., 2012/32275 K. (Yurtcan, **a.g.e.**, s. 341)

⁵⁴³ Soyaslan, **a.g.e.**, s. 434.

⁵⁴⁴ Toroslu, **a.g.e.**, s. 194.

⁵⁴⁵ Bkz. s. 151.

nazaran daha ağır cezayı gerektiren bir nitelikli unsur olarak kabul edildiği ifade edilmektedir. Bu durumda, suç, özgü suç haline dönüşmektedir⁵⁴⁶.

Kripto para örneğinde, mal alım ve satımında kripto para kabul eden şirketin yöneticisinin, şirketin ticari güvenilirliği kullanarak müşteriyi aldatıp onlardan bitcoin alması, bu nitelikli hali oluşturacaktır.

gg. Dolandırıcılık suçunun serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle işlenmesi

Serbest meslek sahiplerinin, kendi mesleklerine duyulan güveni istismar ederek dolandırıcılık suçunu işlemeleri nitelikli bir hal olarak düzenlenmiştir. Avukat, muhasebeci ve müteahhit gibi meslek sahiplerinin mesleklerinin toplumda sahip olduğunu saygınlığı ve güveni kullanarak kişileri hataya düşürüp aldatmaları, diğer kişilere göre daha kolaydır⁵⁴⁷.

Kripto para örneğinde, kripto para birimi takas merkezi yöneticilerinin dolandırıcılık fiillerini işlemeleri durumunda, nitelikli dolandırıcılık söz konusu olabilecektir.

⁵⁴⁶ Özbek ve diğ., **a.g.e.**, s. 710.

⁵⁴⁷ "5237 sayılı TCK.nun 158/1-i bendinde "... serbest meslek sahibi kişiler tarafından, mesleklerinden dolayı kendilerine duyulan güvenin kötüye kullanılması suretiyle işlenmesi" hali nitelikli dolandırıcılık olarak kabul edilmiştir. 193 Sayılı Gelir Vergisi Kanunun 65/2. maddesinde serbest meslek faaliyeti "Sermayeden ziyade şahsi mesaiye ilmi veya mesleki bilgiye veya ihtisasa dayanan ve ticari mahiyette olmayan işlerin işverene tabi olmaksızın şahsi sorumluluk altında kendi nam ve hesabına yapılmasıdır" şeklinde tanımlanmış, aynı kanunun 66.maddesinde ise "serbest meslek faaliyetini mutat meslek halinde ifa edenler, serbest meslek erbabıdır" denilmiştir. Böylece kendi nam ve hesabına mesleğin gerektirdiği etik kurallara uygun olarak çalışması gereken kişilerin toplumda kendilerine duyulan güveni kötüye kullanmak suretiyle dolandırıcılık suçunu işlemeleri hali nitelikli dolandırıcılık olarak düzenlenmiştir. Bu bendin uygulanabilmesi için failin "serbest meslek mensubu" olması ve dolandırıcılık suçunu da mesleği gereği kendilerine duyulan güveni kötüye kullanmak suretiyle işlemesi gerekir. Somut olayda ise; sanığın, araba alım-satımı işi karşılığında aldığı bedeller için Vergi Usul Kanunu gereğince serbest meslek makbuzu düzenlemeyip fatura düzenlemek zorunda bulunduğundan, araba alım-satım işinin (galericilik) sıfatının yukarıdaki açıklamalar ışığı altında serbest meslek kavramı içinde değerlendirilemeyeceği, eylemin dolandırıcılık suçunun basit halini oluşturacağından tebliğnamedeki bozma düşüncesine iştirak edilmemiştir..." 11.CD., 2006/5396 E., 2009/563 K. (Yurtcan, **a.g.e.**, s. 321.)

hh. Dolandırıcılık suçlarının, üç veya daha fazla kişi tarafından birlikte veya suç örgütü faaliyeti çerçevesinde işlenmesi

TCK m. 157 ve 158’de düzenlenen dolandırıcılık suçunun temel şekli ve nitelikli halleri, üç veya daha fazla fail tarafından birlikte işlenmesi durumunda, verilecek ceza yarı oranında arttırılır⁵⁴⁸. Eğer bu suçlar, suç işlemek amacıyla kurulan örgüt (TCK m. 220) veya silahlı örgütü (TCK m. 314) faaliyeti çerçevesinde işlenirse verilecek ceza bir kat arttırılır.

Kripto para birimi örneğinde, kendilerine yardıma muhtaç bir aile görüntüsü vererek mağdurdan kripto para birimi alan kişiler, bu nitelikli hal kapsamındadır.

b. Suçu Hafifleten Nedenler

Dolandırıcılık suçunda cezayı hafifletici nitelikli hal TCK m. 159’da düzenlenmiştir. Buna göre *“Dolandırıcılığın, bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi halinde, şikâyet üzerine, altı aydan bir yıla kadar hapis veya adli para cezasına hükmolunur.”*

Hırsızlık suçu bölümünde, hukuki ilişkiye dayanan alacağın tahsil amacıyla suçun işlenmesi ile ilgili yapılan açıklamalar, dolandırıcılık suçu bakımından da geçerlidir⁵⁴⁹. Başka bir ifadeyle alacak, para veya mal olabilir. Fail ile mağdur arasında alacak hakkı doğuran hukuki ilişkinin geçerli olması gerekir. Dolandırıcılık suçuna konu olan malın, alacaktan fazla olması durumunda da bu hüküm uygulanır.

Suçta verilecek cezada indirim öngören bu hüküm, kripto para birimi dolandırıcılığında uygulama imkânı bulabilir. Örneğin mağdurdan geçerli bir hukuki ilişkiye dayanan alacağını, hukuki yollardan alamayan fail, mağdurun hesabındaki kripto paraları, onu aldatarak kendi hesabına transfer ettirirse bu nitelikli hal oluşacaktır.

⁵⁴⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 530.

⁵⁴⁹ Bkz. s. 111.

Bu cezayı hafifleten nitelik söz konusu olduğunda, suçunun soruşturulması şikâyet şartına bağlanmıştır.

c. Cezayı Kaldıran ya da Azaltan Şahsi Sebep

Malvarlığı bölümünde, aralarında dolandırıcılık suçunu da bulunduğu suçlar için, TCK m. 167’de belli yakınlık ilişkileri şahsi cezasızlık sebebi sayılmış, bazıları da cezayı hafifleten sebep olarak düzenlenmiştir. Hırsızlık suçu ile ilgili olarak bu konuda yapılan açıklamalar dolandırıcılık suçu için de geçerlidir⁵⁵⁰.

Cezayı kaldıran ya da azaltan şahsi sebep hükümlerinden kripto para dolandırıcılık suçu faili de, durumu uygun düşükçe yararlanması mümkündür. Örneğin babasını acil ihtiyacı olduğunu konusunda aldatan ve ondan kripto para birimi alan çocuğun eylemi TCK m. 167/1-b gereğince şahsi cezasızlık sebebidir.

d. Etkin Pişmanlık

TCK m. 168’te ise aralarında dolandırıcılık suçunun da bulunduğu bazı malvarlığı suçları için etkin pişmanlık düzenlenmiştir. Hırsızlık suçu ile ilgili olarak etkin pişmanlık için yapılan açıklamalar dolandırıcılık suçu için de geçerlidir⁵⁵¹.

Kripto para birimi örneğinde, hasta olduğunu beyan ederek mağdurdan bitcoin alan fail, kovuşturma başlamadan önce pişmanlık duyarak, mağdurdan aldığı bitcoin’leri geri verirse veya onun zararını tazmin ederse, hakkında verilecek ceza üçte ikisine kadar indirilir (TCK m. 168/1). Eğer kovuşturma başladıktan fakat daha hüküm verilmeden pişmanlık duyup aldığını iade eder veya mağdurun zararını tazmin ederse, failin cezası yarıya kadar indirilir (TCK m. 168/2). Fail, mağdurdan aldığı bitcoin’lerin tamamını iade etmez veya zararını tamamen tazmin etmezse, bu durumda failin etkin pişmanlık hükümlerinden yararlanabilmesi, mağdurun rızasına bağlıdır (TCK m. 168/4).

⁵⁵⁰ Bkz. s. 112.

⁵⁵¹ Bkz. s. 113.

8. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Dolandırıcılık suçunda hareket ile netice birbirinden ayrılabilirdiği için suça teşebbüs mümkündür⁵⁵². Suçun icrası kapsamında hileli davranış icraya başlanmış fakat aldanma gerçekleşmemişse veya aldatma gerçekleştirmiş fakat yararlanma gerçekleşmemişse, suç teşebbüs aşamasında kalmıştır⁵⁵³.

Kripto para örneğinde, failin mağduru aldattıktan sonra, onun hesabındaki parayı kendisinin veya başkasının hesabına geçirmeye çalışırken, işlemin kendi iradesi dışında kesilmesi, (örneğin internet bağlantısının kopması) durumunda dolandırıcılık suçuna teşebbüs söz konusu olacaktır.

b. İctima

Dolandırıcılık suçu için, farklı bir ictima durumu öngörülmemiş olup, suçların ictimayı bölümünde (TCK m. 42-44) yer alan hükümler uygulanacaktır⁵⁵⁴. Örneğin fail, bir kişiye ait birden fazla hesapta bulunan kripto parayı almışsa, tek bir dolandırıcılık suçu meydana gelmiştir. Yine, müşterek hesapta tutulan kripto paranın alınması durumunda, mağdurlar birden fazla da olsa müşterek zilyet sayıldıklarından tek bir dolandırıcılık suçu söz konusu olacaktır.

Hilenin, sahte belge kullanarak gerçekleştirilmesi durumunda, TCK m. 212 uyarınca fail hem dolandırıcılıktan hem de sahtecilikten cezalandırılır⁵⁵⁵.

⁵⁵² Soyaslan, **a.g.e.**, s. 429; Centel, Zafer, Çakmut, **a.g.e.**, s. 532; Koca, Üzülmez, **a.g.e.**, s. 667; Toroslu, **a.g.e.**, s. 189; Aydın, **a.g.e.**, s. 292; Parlar, **a.g.e.**, s. 24.

⁵⁵³ Tezcan, Erdem, Önok, **a.g.e.**, s. 788.

⁵⁵⁴ Özbek ve diğ., **a.g.e.**, s. 716.

⁵⁵⁵ Parlar, **a.g.e.**, s. 25.

Dolandırıcılık suçunun zincirleme suç şeklinde işlenmesi de mümkündür⁵⁵⁶. Aynı suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı birden fazla işlenmesi durumunda bir cezaya hükmedilir (TCK m. 43). Mesela, aldatmayı becerdiği mağdurun hesabında bulunan kripto parayı farklı zamanlarda kendi hesabına geçiren failin eylemi, zincirleme suç kapsamında tek bir suç olarak kabul edilecek ve TCK m. 43 gereği arttırılacaktır⁵⁵⁷.

c. İştirak

Dolandırıcılık suçu, iştirak bakımından bir özellik göstermemektedir ve bu nedenle müsterek faillik, azmettirme ve yardım etme şeklinde her türlü iştirak söz konusu olabilir⁵⁵⁸. Suçun işlenişine katkısı fiile hâkimiyet şeklinde olanlar fail, olmayanlar ise şerik kabul edilir⁵⁵⁹. Dolandırıcılık suçu neticesinde sadece haksız yarar sağlayan kişi, suçun hareket kısmına katılmamışsa cezalandırılmayacaktır⁵⁶⁰.

9. Yaptırım

Dolandırıcılık suçunun temel şeklinin cezası, bir yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezasıdır (TCK m. 157). Suçta nitelikli hallerin varlığı durumunda verilecek ceza, üç yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezasıdır (TCK m. 158). Fakat nitelikli dolandırıcılık, kamu kurum ve kuruluşlarının zararına olarak veya bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle veya banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla veya Sigorta bedelini almak maksadıyla veya kişinin, kendisini kamu görevlisi veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtması veya bu kurum ve kuruluşlarla ilişkili olduğunu söylemesi suretiyle işlenmesi durumunda hapis cezasının alt sınırı dört yıldan, adli para cezasının miktarı suçtan elde edilen menfaatin iki katından az olamaz (TCK m. 158 son cümle.)

⁵⁵⁶ Koca, Üzülmüş, **a.g.e.**, s. 668.

⁵⁵⁷ Özbek ve diğ., **a.g.e.** s. 716.

⁵⁵⁸ Tezcan, Erdem, Önok, **a.g.e.**, s. 789; Centel, Zafer, Çakmut, **a.g.e.**, s. 535.

⁵⁵⁹ Parlar, **a.g.e.**, s. 25.

⁵⁶⁰ Özbek ve diğ., **a.g.e.**, s. 716; Koca, Üzülmüş, **a.g.e.**, s. 668.

10. Muhakemeye İlişkin Kurallar

Dolandırıcılık suçu re'sen kovuşturulan suçlardandır. Fakat TCK m. 159'da düzenlenen cezayı hafifletici halin söz konusu olduğu durumlarda kovuşturma, mağdurun veya suçtan zarar görenin şikâyetine bağlıdır.

5235 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. maddesi uyarınca dolandırıcılık suçunun basit hali için suçu kovuşturmayla görevli mahkeme, asliye ceza mahkemesidir. TCK m. 158'de düzenlenen nitelikli dolandırıcılık suçunda görevli mahkeme ise 5235 sayılı Kanunun 12. maddesindeki özel düzenleme uyarınca, ağır ceza mahkemesidir.



II. Bilişim Alanında Suçlar

Bilişim sistemlerine karşı suçlar, 5237 sayılı Türk Ceza Kanunu’nda ikinci kitabın üçüncü kısmında *Bilişim Alanında Suçlar* başlıklı onuncu bölümde, 243 ilâ 246. maddeleri arasında düzenlenmiştir⁵⁶¹.

Bu bölümde düzenlenen suçlar, bilişim sistemlerine karşı doğrudan işlenen suçları kapsamaktadır. Bunun yanında bilişim sistemlerinin araç olarak kullanıldığı “dolaylı bilişim suçları”na, ilgili suç maddelerinde yer verilmiştir. Örneğin hırsızlık veya dolandırıcılık suçlarında “bilişim sistemi kullanılmak suretiyle” gerçekleştirilen nitelikli haller, ilgili suçun altında düzenlenmiştir.

Bilişim ifadesinin bilgisayarla işlenen suçlar dışında, toplumsal hayatta ses, görüntü, veri alan ve nakleden, bunları işleyen tüm elektronik araçlarla işlenen suçları da kapsamı bakımından, bilişim alanında suçlar başlığı isabetli bulunmuştur⁵⁶².

Teknolojinin gelişmesiyle, bilişim sistemlerinin toplumsal ve bireysel hayatta ve Devlet işlerinde gittikçe güçlenen konumu ve üstlendiği fonksiyonların çokluğu, bu sistemleri vazgeçilmez kılmaktadır. Bu gelişmeye paralel olarak, doğrudan bilişim sistemlerine karşı veya bilişim sistemleri kullanarak işlenen suçlar da her geçen gün artmakta ve bu sistemlerin korunması için özel önlemlerin alınmasını gerektirmektedir.

Mülga 765 sayılı TCK döneminde 1991 yılında mevzuatımıza dâhil edilen bilişim suçları, benzer yaklaşımla fakat daha ayrıntılı olarak 5237 sayılı TCK’de de yer almıştır⁵⁶³. Bilişim alanında suçlar bölümüne, en son 24.03.2016 tarihinde kabul edilen 6698 sayılı kanunun 30. maddesiyle “*yasak cihazlar ve programlar*” başlıklı 245/A maddesi eklenmiştir.

⁵⁶¹ Bu bölümde şu suçlar düzenlenmiştir: *bilişim sistemine girme suçu* (m. 243), *sistemi engelleme, bozma, verileri yok etme veya değiştirme* (m. 244), *banka veya kredi kartlarının kötüye kullanılması* (m. 245), *yasak cihaz veya programlar* (m. 245/A).

⁵⁶² Soyaslan, **a.g.e.**, s. 634.

⁵⁶³ Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 5. b., Ankara: Seçkin Yayıncılık, 2014, s. 196.

İnceleme konumuz olan kripto para birimleri açısından bilişim sistemlerini korumaya yönelik düzenlemeler oldukça önemlidir. Zira kripto para birimi şemaları, tamamen bilişim sistemleri üzerinde sanal ortamda gerçekleşen yapılara sahiptirler. Bu sistemlerin sanal piyasalara arz ettiği kripto para birimlerine ilişkin bütün hareketler bilişim sistemleri üstünde ve bu sistemler arasında gerçekleşmektedir.

İncelememizin bu bölümünde, Bilişim Alanında Suçlar bölümünde TCK m. 244'te düzenlenen “*sistemi engelleme, bozma, verileri yok etme veya değiştirme*” suçunun kripto para birimleri açısından bir değerlendirmesi yapılacaktır.

A. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)

1. Genel Olarak

Bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçu, Türk Ceza Kanunu'nda ikinci kitabın dördüncü kısmında *Bilişim Alanında Suçlar* başlıklı onuncu bölümde 244. maddede düzenlenmiştir.

Maddenin 1. fıkrasında bilişim sisteminin işleyişine karşı engelleme ve bozma fiilleri yaptırım altına alınmıştır: “*Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*”

2. fıkra, bilişim sisteminde yer alan verileri bozma ve yok etme suçu düzenlenmiştir: “*Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.*”

3. fıkra, 1. ve 2. fıkralarda belirtilen fiiller için nitelikli bir hal düzenlenmiş, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi daha ağır bir yaptırıma bağlanmıştır.

Maddenin 4. fıkrasında, 1. ve 2. fıkra, belirtilen fiillerin işlenmesiyle haksız yarar sağlama suçu düzenlenmiştir: “*Yukarıdaki fıkralarda tanımlanan fiillerin*

işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.”

2. Suçun Faili

Bilişim sisteminin işleyişinin engellenmesi ve bozulması ile verilerin yok edilmesi veya değiştirilmesi suçunda herkes bu suçun faili olabilir⁵⁶⁴.

3. Suçun Mağduru

Bilişim sistemi veya içinde barındırdığı veriler üzerinde hak sahibi olan kişi bu suçun mağduru olabilir⁵⁶⁵.

4. Suçla Korunan Hukuki Yarar

Doktrinde, bu suçun düzenlenmesiyle korunan hukuki yarar tartışmalıdır. Düzenlenmenin mala zarar verme suçunun özel halini olduğunu öne süren bazı yazarlar, maddenin 1. ve 2. fıkralarındaki düzenlemelerle mülkiyet hakkının korunduğunu, 4. fıkradaki düzenlemeyle ise bir bütün olarak malvarlığının korunduğunu ileri sürmektedir⁵⁶⁶.

Özbek, Doğan, Bacaksız ve Tepe; bu düzenlemeyle bir bütün olarak bilişim sisteminin ve verilerinin güvenliği ile mülkiyet hakkının korunduğunu belirtmektedir⁵⁶⁷.

Dülger, bilişim sistemlerinin yalnızca veri ve yazılımlardan oluşan soyut unsurları koruma altına almadığını, aynı zamanda bilişim sistemlerinin somut unsuru olan donanım kısmını da koruma altına aldığını belirterek, düzenlemeyle korunan değer karma nitelikte olduğunu öne sürmüştür⁵⁶⁸.

⁵⁶⁴ Soyaslan, **a.g.e.**, s. 642; Ali Parlar, **Türk Ceza Hukukunda Bilişim Suçları**, 1. b., Ankara: Bilge Yayınevi, 2011, s. 25.

⁵⁶⁵ Soyaslan, **a.g.e.**, s. 642; Parlar, **a.g.e.**, s. 25.

⁵⁶⁶ Tezcan, Erdem, Önok, **a.g.e.**, s. 1004.

⁵⁶⁷ Özbek ve diğ., **a.g.e.**, s. 953.

⁵⁶⁸ Dülger, **a.g.e.**, s. 407; aynı görüşte Karagülmez, **a.g.e.**, s. 237.

Erdoğan'a göre, 1. fıkarda bilişim sistemlerinin güvenilirliği⁵⁶⁹, 2. fıkarda tasarrufta bulunan verinin içeriğine göre o veriye özgü farklı değerler⁵⁷⁰, 4. fıkarda ise bunlara ek olarak, çıkar sağlanabilecek her türlü değerın korunması⁵⁷¹ amaçlanmaktadır.

Artuk, Gökçen ve Yenidünya, 1. ve 2. fıkralarda, bilişim sisteminin güvenliği ve haberleşme özgürlüğü⁵⁷² ve 4. fıkarda ise özel hayatın gizliliğinden başlayan ve malvarlığı haklarına kadar uzanan çeşitli haklar⁵⁷³ korunmaktadır.

Kanaatimize göre bilişim alanında düzenlenen suçların amacı, bu sistemlere karşı gerçekleştirilecek hukuka aykırı eylemleri yaptırıma bağlayarak onları koruma altına almak, sağlıklı çalışmalarına yardımcı olmak ve bu şekilde birey ve toplum nezdinde onlara duyulan güvenin zedelenmesini önlemektir.

5. Suçun Maddi Konusu

Düzenlemenin birinci fıkrasında yer alan bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunda, suç konusu bilişim sisteminin kendisidir. 2. fıkarda düzenlenen verilerin yok edilmesi veya değiştirilmesi suçunda ise konu bilişim sistemindeki verilerdir⁵⁷⁴.

Bilişim sistemleri, madde gerekçesinde, “*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler*” olarak tanımlanmıştır.

Bazı yazarlar, bilişim sistemlerini, veri ile olan ilişkileri çerçevesinde, verileri işleyen ve aktaran araçlardan oluşmuş bütüncül sistem olarak tanımlamışlardır⁵⁷⁵.

⁵⁶⁹ Erdoğan, **a.g.e.**, s. 184.

⁵⁷⁰ **A.g.e.**, s. 214.

⁵⁷¹ **A.g.e.**, s. 251.

⁵⁷² Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 880, 886.

⁵⁷³ **A.g.e.**, s. 891.

⁵⁷⁴ Dülger, **a.g.e.**, s. 410; Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 888, 855; Özbek ve diğ. **a.g.e.**, s. 913;

Tezcan, Erdem, Önok, **a.g.e.**, s. 1004; Soyaslan, **a.g.e.**, s. 643.

⁵⁷⁵ Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 870.

Bazı yazarlar da bilişim sistemlerini, verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması gibi fonksiyonları otomatik olarak gerçekleştiren sistemler şeklinde açıklamışlardır⁵⁷⁶.

Türkiye'nin 0.11.2010 tarihinde imzaladığı ve TBMM tarafından 22.04.2014 tarihinde 6533 no'lu kanunla onaylanan ve 02.05.2014 tarihli ve 28988 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi'nin 1. maddesinde yapılan tanıma göre bilgisayar sistemi, *“bir program çerçevesinde, otomatik veri işlemi yapan bir veya birden fazla birbirine bağlı veya ilgili cihaz ve cihaz grupları anlamına gel”*mektedir.

Bilişim sistemi kavramı, bilgisayarlar dışında veri işleme, saklama ve iletme yeteneklerine sahip diğer elektronik, manyetik veya dijital aletler (örneğin cep telefonu, akıllı saat, tablet, akıllı ev aletleri, vs.) ile bunların birbirleriyle iletişimini sağlayan ağ yapılarını (modem, switch, router, fiber optik hatlar, vs.) da içerir.

Kanaatimize göre, bilişim sistemi için daha uygun bir tanım, 06.08.2015 tarihinde 29437 sayılı Resmi Gazete'de yayımlanan *“Bölge adliye ve adli yargı ilk derece mahkemeleri ile cumhuriyet başsavcılıkları idarî ve yazı işleri hizmetlerinin yürütülmesine dair yönetmelik”*te yapılmıştır. Buna göre bilişim sistemi, *“bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi”* ifade etmektedir.

Bilişim verisi için doktrinde farklı tanımlamalar yapılmıştır. Dülger, veriyi, bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi olarak açıklamıştır⁵⁷⁷.

Karagülmez, veriyi, bilişim sistemi içerisindeki bir unsurun ya da programın ilişkilendirildiği bir bilgi veya programın işletilmesinden sonraki çıktı veya sistemdeki bilgi, kısaca bilişim sistemindeki bilgi unsuru olarak tanımlamıştır⁵⁷⁸.

⁵⁷⁶ Özbek ve diğ., **a.g.e.**, s. 941.

⁵⁷⁷ Dülger, **a.g.e.**, s. 79.

⁵⁷⁸ Karagülmez, **a.g.e.**, s. 147.

Değirmenci, veriyi, “*bilişim sistemlerinde işlenen her türlü bilgi*” olarak tanımladıktan sonra, onu durağan veri, akış verisi ve işlem verisi şeklinde üçlü bir ayrıma tabi tutmaktadır. Durağan haldeki veri bilişim sistemi aracının sabit diskinde duran veriyi; akış halinde veri, bir cihazdan diğer cihaza ağ vasıtasıyla iletilen veriyi; işlem halindeki veri ise, hafızaya alınan ve üzerinde işlem yapılan veriyi ifade etmektedir⁵⁷⁹.

Soyaslan’a göre veriler bilginin sayısal koda dönüştürülmüş halidir⁵⁸⁰.

Avrupa Konseyi Siber Suç Sözleşmesi’nin 1. maddesinde yapılan tanıma göre bilgisayar verisi, “*bir bilgisayar sisteminin belli bir fonksiyonu yerine getirmesini sağlayan uygun programları içeren, bir bilgisayar sistemi içinde işlem yapmaya uygun bir formda bilgi veya konsept ve bilgilerin sunumu anlamına gelir*”mektedir.

Mevzuatımızda veri kavramı, 23.05.2007 tarihinde Resmi Gazete’de yayımlanan 5651 sayılı *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*’un tanımlar başlıklı ikinci maddesinin 1-k fıkrasında tanımlanmıştır. Bu tanıma göre veri, “*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri*” ifade etmektedir. Benzer bir kavram olan “elektronik veri” ise 23.01.2004 tarihinde Resmi Gazete’de yayımlanan 5070 sayılı *Elektronik İmza Kanunu* (EİK) m. 3’te tanımlanmıştır. Bu tanıma göre, “*elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar*” elektronik veridir. Birinci tanımda, bilgisayar tarafından işlenebilme özelliği tanımın esasını oluşturmaktayken, ikincisinde, belli hareketlerin gerçekleşme formlarına ve ortamlarına vurgu yapılmıştır. Bilgisayar tarafından işlenebilmek için verilerin ikili sayı düzeninde (0 ve 1) olması ve elektronik, elektromanyetik, optik veya ağ ortamlarında tutulmaları gerekmektedir.

Yargıtay’ın verdiği çeşitli kararlarda, Avrupa Konseyi Siber Suç Sözleşmesi ile 5651 sayılı kanunda düzenlenen yukarıda verilen bilişim verisi tanımlarını benimsediği anlaşılmaktadır⁵⁸¹.

⁵⁷⁹ Olgun Değirmenci, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, 1. b., Ankara: Seçkin Yayıncılık, 2014, s. 50.

⁵⁸⁰ Soyaslan, **a.g.e.**, s. 644.

Kanaatimize göre bilişim verisi, bilişim sistemleri aracılığıyla, elektronik, optik veya manyetik ortamlarla, saklanmaları, işlenmeleri ve transferleri mümkün olan ve bilişim sistemlerini oluşturan bileşen ve nesnelerin yapılarını oluşturan temel kavramsal birimleri ifade etmektedir.

6. Suçun Unsurları

a. Maddi Unsur

Maddenin 1. fıkrasında yaptırıma bağlanan fiiller, bilişim sisteminin işleyişini engellemek veya bozmaktır. Suçun meydana gelmesi için bilişim işleyişini engellemek veya bozmak şeklinde iki hareketten birisinin yapılması gerekir. Bu nedenle suç, seçimlik hareketli bir suçtur.

Sistemin işleyişini engellemek, geçici olarak sistemin hizmet dışı kalmasına veya hizmetlerde aksaklıklar yaşanmasına neden olurken; sistemin bozulması, engellemeye nazaran daha kalıcı olarak hizmet dışı kalmayı ifade etmektedir⁵⁸².

Sistemin engellenmesi durumunda, sistem bozulmamakta fakat veri işleme hızının düşmesi gibi, fonksiyonlarının normal şekilde ifası engellenmektedir⁵⁸³. Örneğin, internet üzerinden yayın yapan haber portalını sürekli meşgul tutacak gereksiz e-postalar göndererek, kullanıcıların siteye erişimini engellemek, bu kapsamdadır⁵⁸⁴.

⁵⁸¹ YCGK, 17.11.2009, 2009/11-193 E., 2009/268 K.; 25.11.2014, YCGK, 2013/448 E., 2014/524 K.; 26.09.2017, 2017/956 E., 2017/370 K. (emsal.yargitay.gov.tr)

⁵⁸² Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 881-882.

⁵⁸³ Erdoğan, **a.g.e.**, s. 189; Soyaslan, **a.g.e.**, s. 643.

⁵⁸⁴ "...2-Kabule göre de; dosya kapsamına göre sanığın, şikayetçinin elektronik posta adresinin ve facebook hesabının şifresini kırarak, hesaba giriş şifresini değiştirerek erişimini engellemesi şeklinde gerçekleşen eyleminin TCK'nın 244/2. maddesi kapsamında kaldığı halde aynı yasanın 244/1. maddesinden mahkumiyet hükmü kurulması,(...) 27/02/2018 tarihinde oybirliğiyle karar verildi." 15. CD., 27.02.2018, 2017/35938 E., 2018/1367 K. (emsal.yargitay.gov.tr)

"...1- Sanığın katılana ait elektronik posta adresi ve Facebook sayfasının şifresini değiştirerek katılanın erişimine engel olması şeklindeki eyleminin TCK.nun 244/2. maddesine uygun bulunduğu gözetilmeden, yazılı şekilde uygulama yeri bulunma- yan TCK.nun 244/1. maddesi gereğince hüküm kurulması..." 8. CD., 17.09.2014, 2014/14716 E., 2014/20052 K. (emsal.yargitay.gov.tr)

Sistemi bozmaktan anlaşılması gereken, bilişim sisteminin ondan beklenen işi yapamaması, düzeninin karıştırılması, zarar verilmesi ve kötü duruma getirilmesidir⁵⁸⁵.

Bilişim sisteminin işleyişini engellemek veya bozmak için gerçekleştirilen eylem önemli değildir. Bunun için başka bir bilişim sistemi kullanılabileceği gibi, doğrudan fiziksel hasar vermek, virüs göndermek, sistemin elektriğini kesmek gibi çok çeşitli yollar kullanılabilir.

Sistemin verilerine müdahale şeklinde gerçekleşen eylem, sistemin işleyişini engellemediği veya bozmadığı takdirde 2. fıkra da yaptırıma bağlanan verileri yok etme ve değiştirme suçu oluşacaktır⁵⁸⁶.

Kripto para birimi örneğinde, madencilik faaliyet gerçekleştiren bilişim sisteminin çalışma düzenine müdahale ederek, kişilerin yeni kripto para birimi üretmelerinin engellenmesi bu suçu oluşturacağı gibi, kullanıcının sanal cüzdanının yer aldığı bilgisayara virüs göndererek bilgisayarın işleyişini engellemek veya bozulmasına neden olmak fiilleri de bu kapsamında değerlendirilecektir.

Maddenin 2. fıkrasında bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek, erişilmez kılmak, başka yere göndermek ile sisteme veri yerleştirmek şeklinde gerçekleşebilecek verilerinin yok edilmesi ve değiştirilmesi fiilleri yaptırıma bağlanmıştır.

Verilere karşı işlenen bu fiiller, 1. fıkra da düzenlenen sistemin işleyişini engelleme veya bozma seviyesine ulaşmaması gerekir. Aksi halde 1. fıkradaki suç oluşacaktır^{587,588}.

⁵⁸⁵ Dülger, **a.g.e.**, s. 414; Soyaslan, **a.g.e.**, s. 644.

⁵⁸⁶ Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 882.

⁵⁸⁷ Karagülmez, **a.g.e.**, s. 239.

⁵⁸⁸ "...1- Katılana ait ... ve ... adresine sanıklar tarafından şifresinin kırılması yoluyla girildiği ve şifrelerinin değiştirilmesi suretiyle erişilemez hale getirildiği iddiasıyla açılan davada, sanıkların tüm aşamalarındaki savunmasında şifreyi kendilerinin değiştirmediklerini savunmaları karşısında, sanıklara ait bilgisayarlardan katılanın ... adresine giriş yapıldığı tespit edilmişse de, katılanın ... ve ... adreslerine girişinin engellendiğine dair bir tespitin bulunmaması karşısında; şikayet tarihinden önce ... ve ... adresinin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı araştırılarak ve şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarasından sağlanan erişim sonucu değiştirildiği ilgili internet sağlayıcısından ve ...

Verileri bozmak, verilerin tutarlılığını ve bütünlüğünü zedeleyecek şekilde onlara zarar vermeyi ifade etmektedir⁵⁸⁹. Bu fıkra kapsamında verileri bozmak isteyen fail, sistemin işleyişine etki etmeyen bir veriyi bozmaktadır⁵⁹⁰. Örneğin, kişisel bilgisayarda kişinin sahip olduğu kripto para hesap bilgilerinin yer aldığı sanal cüzdan dosyasına, artık bir daha açamamak şeklinde müdahale edildiğinde, verinin bozulmasından bahsedilir.

Verileri yok etmek, bu verilere artık bir daha ulaşamayacak şekilde imha etmeyi ifade etmektedir. Fakat doktrinde, yasa koyucunun verinin somut olarak yok edilmesini değil, bilişim alanında geçerli olan mantıksal yok etmeyi kast ettiği de ileri sürülmektedir⁵⁹¹. Yukarıdaki örnekte sanal cüzdan dosyasının geri dönüşsüz silinmesi durumunda, verilerin yok edildiği kabul edilmelidir.

Verileri değiştirme, mevcut bir veri yerine başka bir verinin yerleştirilmesi anlamına gelmektedir⁵⁹². Sistemde bulunan bir resim yerine bir başka resmin konulması veya bir yazıda, içeriğin değiştirilmesi veyahut sisteme girişlerin kaydedildiği izleme kayıt dosyasındaki verilerin değiştirilmesi bu duruma birer örnektir. Bilgisayardaki sanal cüzdanda tutulan kripto para hesabına ait gizli anahtarın değiştirilmesi durumunda, verilerin değiştirilmesi söz konusu olacaktır.

Verilerin erişilmez kılınması, veri sahibinin istediği zaman verilerine ulaşamaması, onlar üzerinde istediği işlemleri gerçekleştirememesidir⁵⁹³. Örneğin bilişim sistemindeki sanal cüzdanını oluşturan dosyaları, sadece okunabilir duruma getirilen kişi, bu cüzdandaki verilerle işlem yapamayacaktır. Verinin şifrelenerek erişilmez kılınması da mümkündür. Bu durumda veri yok edilmemekte, sadece erişimi engellenmektedir⁵⁹⁴.

şirketten sorulup erişilmez kılındığı takdirde TCK.nun 244/2., aksi takdirde aynı yasanın 243/1. maddesi kapsamındaki suçu oluşturacağı gözetilerek sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmayla yazılı şekilde hüküm kurulması”, 8. CD., 25.04.2016, 2015/12431 E., 2016/5507 K. (emsal.yargitay.gov.tr)

⁵⁸⁹ Dülger, **a.g.e.**, s. 415.

⁵⁹⁰ Soyaslan, **a.g.e.**, s. 645.

⁵⁹¹ Erdoğan, **a.g.e.**, s. 222; Soyaslan, **a.g.e.**, s. 645; Parlar, **a.g.e.**, s. 26.

⁵⁹² Dülger, **a.g.e.**, s. 417; Soyaslan, **a.g.e.**, s. 646; Parlar, **a.g.e.**, s. 26.

⁵⁹³ Soyaslan, **a.g.e.**, s. 646.

⁵⁹⁴ Erdoğan, **a.g.e.**, s. 225.

Sisteme veri yerleřtirmek, sistemde mevcut verilere zarar vermeden ve onlara ulařma imkânını ortadan kaldırmadan ek veriler yerleřtirmektedir⁵⁹⁵. Bu durumda veri güvenliđi zarar görmektedir⁵⁹⁶.

Sistemde mevcut verilerin bařka yerlere gönderilmesiyle, verilerin kaydedilmesi, kopyalanması ve aktarılmasını anlařılmalıdır⁵⁹⁷. Verilerin bulunduđu ortamdan farklı bir biliřim sistemine veya aynı sistem içinde farklı bir konuma gönderilebilir^{598,599}. Bu iřlem internet aracılıđıyla yapılabileceđi gibi, veri taşıma aygıtlarıyla da gerekleřtirilebilir⁶⁰⁰. Örneđin kiřinin kiřisel bilgisayarında sakladığı sanal cüzdan bilgilerinin veya bu cüzdanda bulunan gizli anahtarının bir bařka bilgisayara gönderilmesini durumunda verilerin bařka bir yere gönderilmesi söz konusu olacaktır.

Kripto para birimi örneğinde, kiřinin kripto para hesabı üzerinde iřlem yapabilmesini sađlayan sanal cüzdanına erişimini engelleyen, cüzdanda bulunan gizli

⁵⁹⁵ “...Sanıklardan ...'un, e-bildirge ile bilgisayar ortamında sahte iře giriř bildirgesi düzenleyerek, müřteki ...'e ait iřyerinde alıřmayan diđer sanıkları bu iřyerinde alıřıyormuř gibi sigortalı olarak gösterdiđi, böylece sanıkların iřtirak halinde özel belgede sahtecilik suçunu iřledikleri iddiasıyla açılan kamu davasında; imza ve řifre ile bilgisayar ortamında iře giriř bildirelerinin verilmesi eyleminin, TCK'nın 244/2. maddesinde yazılı "sisteme veri yerleřtirme" suçunu oluřturup oluřturmadığı tartiřılmadan, "...oluřturulmuř sahte belge olmadığı, internet üzerinden bildirimde bulunulduđu.." gerekesiyle özel belgede sahtecilik suçundan yazılı řekilde beraat kararları verilmesi, Yasaya aykırı, katılan vekilinin temyiz itirazları bu itibarla yerinde görölmüř olduđundan hükmölerin bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi geređince uygulanması gereken 1412 sayılı CMUK'nın 321. maddesi uyarınca BOZULMASINA, 16.04.2018 tarihinde oybirliđi ile karar verildi.” 11. CD., 16.04.2018, 2016/900 E., 2018/3528 K. (emsal.yargitay.gov.tr)

⁵⁹⁶ Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 887.

⁵⁹⁷ Dölger, **a.g.e.**, s. 420.

⁵⁹⁸ Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 887.

⁵⁹⁹ “...Oluřa, katılanların beyanlarına, sanık savunmalarına ve tüm dosya kapsamına göre; sanık ...'ın tüm ařamalarındaki savunmalarında katılanlar ile ...Ticaret A.ř arasında yapılan mail yaziřmalarını hazırladıđı casus yazılım programı aracılıđı ile ele geirdiđini beyan etmesi ve katılanlar ile ... Ticaret A.ř arasında yapılan mail yaziřmalarının içeriđinin 30.10.2009 tarihli řikayet dilekesinin ekinde ... Cumhuriyet Bařsavcılıđına sunmuř olması karřısında, sanığın eyleminin TCK.nun 244/2. madde ve fıkrasında tanımlı suçu oluřturup oluřturmadığı tartiřılmadan yazılı řekilde TCK.nun 243/1. madde ve fıkrasında tanımlı suçtan beraat hükmü kurulması, Yasaya aykırı, katılanlar vekilinin temyiz itirazları bu itibarla yerinde görölmüř olduđundan hükmün bu sebeplerden dolayı 5320 sayılı Yasanın 8/1. maddesi geređince uygulanması gereken CMUK.nun 321. maddesi uyarınca BOZULMASINA, 09.01.2017 gününde oybirliđiyle karar verildi.” 8.CD.,09.01.2017, 2016/7100 E., 2017/12 K. (emsal.yargitay.gov.tr)

“...1- Biliřim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme ile biliřim sistemindeki verileri bozma yok etme, erişilmez kılma, var olan verileri bařka bir yere gönderme suçlarına iliřkin olarak, sanığın, yetkisi olmadığı halde katılan řirkete ait biliřim sistemine girerek orada bulunan verileri alıp kendi kullandıđı bilgisayara ve CD'ye aktarması řeklinde gerekleřen eyleminin bir bütün olarak TCK.nun 244/2. maddesinde düzenlenen suçu oluřturacağı gözetilmeden yazılı řekilde karar verilmesi, (...) 14.07.2014 gününde oybirliđiyle karar verildi.” 8. CD., 14.07.2014, 2013/3173 E., 2014/18506 K. (emsal.yargitay.gov.tr)

⁶⁰⁰ Erdoğan, **a.g.e.**, s. 227.

anahtarı değiştiren veya yok eden failin eylemi bu suç kapsamında değerlendirilecektir.

Maddenin 4. fıkrasında, 1. fıkra düzenlenilen bilişim sisteminin işleyişinin engellenmesi veya bozulması ile 2. fıkra düzenlenilen bu sistemlerdeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi veya var olan verilerin başka bir yere gönderilmesi sonucunda failin kendisine veya bir başkasına haksız çıkar sağlaması düzenlenmiştir⁶⁰¹.

Maddenin 1. ve 2. fıkralarında yer alan eylemlerin gerçekleştirilmesi ile birlikte haksız çıkar da sağlanmışsa, “sistemi engelleme, bozma, verileri yok etme veya değiştirme yoluyla haksız çıkar sağlama” suçu tamamlanmış olur. Fakat bu eylemin başka bir suç kapsamında olması durumunda bu suça ilişkin hükümler değil, diğer suç hükümleri uygulanır.

Doktrinde bu fıkradaki düzenlemeyi, bağımsız bir suç olarak ele alanlar⁶⁰² olduğu gibi, 1. ve 2. fıkralarda tanımlanan suçun temel biçimine yapılan atıftan dolayı nitelikli hal olarak kabul eden yazarlar da vardır⁶⁰³.

4. fıkradaki düzenlenmenin, nitelikli hal olarak kabul edilmesi durumunda, 1. ve 2. fıkralarda belirtilen suçun temel şekli gerçekleşmediği takdirde, nitelikli halin uygulanması mümkün olmayacaktır. Ayrıca nitelikli hal oluşmadığı zaman teşebbüsten söz edilemeyeceği, ancak suçun basit halinin cezalandırılabilmesi öne sürülmüştür⁶⁰⁴.

⁶⁰¹ “...Somut olayda suç tarihinde ... Emniyet Müdürlüğünde Asayiş Şube Müdürü olarak görev yapan sanığın kendisine bağlı olan Aranan Şahıslar Büro Amirliğine gelerek atış eğitimine gitmek için bürodan ayrılmak üzere olan tanık ...'in kullandığı şahıs sorgulama sistemi açık olan bilgisayardan, tanık anlatımları ve bir bilişim sistemi olan ... kayıtlarına göre ... isimli şahsa ait silah ruhsatı almasına engel sicil kaydını saat 15:24'te iptal ettiği, ... bilişim sistemine girilerek kaydın silinmesi sonucu ... isimli kişiye ... Kaymakamlığının 18.05.2009 tarihli olurları ile silah taşıma ruhsatı verilerek başkasına haksız bir çıkar sağlanması şeklindeki eylemin TCK.nun 244/2-son maddesindeki "bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme" suçunu oluşturduğu gözetilmeden, yazılı biçimde hüküm kurulması 12.04.2016 gününde oybirliğiyle karar verildi.” 8. CD., 12.04.2016, 2015/14782 E., 2016/4928 K. (emsal.yargitay.gov.tr)

⁶⁰² Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 891; Dülger, **a.g.e.**, s. 431, Tezcan, Erdem, Önok, **a.g.e.**, s. 1007; Erdoğan, **a.g.e.**, s. 247; Soyaslan, **a.g.e.**, s. 651; Koca, Üzülmüş, **a.g.e.**, s. 834.

⁶⁰³ Özbek ve diğ., **a.g.e.**, s. 921.

⁶⁰⁴ Özbek ve diğ., **a.g.e.**, s. 962.

Yargıtay buradaki düzenlemenin bağımsız bir suç olduğu görüşündedir⁶⁰⁵.

Kanaatimize göre, 4. fıkradaki düzenleme bağımsız bir suç kabul edilmelidir. Kanunkoyucu, 1. ve 2. fıkradaki fiilleri tekrarlamaksızın atıf yoluyla belirterek, bilişim sistemi yoluyla haksız çıkar sağlama şeklinde bileşik bir suç düzenlemiştir. 1. ve 2. fıkradaki eylemler, suçun seçimlik hareketlerini, haksız çıkar sağlama ise neticesini oluşturmaktadır.

Fıkra da suçun tanımında bulunan “*başka bir suç oluşturmaması halinde*” ile madde gerekçesinde geçen “*fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması*” ifadeleri çelişkili bulunmuştur. Gerekçenin bağlayıcılık özelliği olmadığı için, gerekçeye itibar edilmemesi gerektiği belirtilmiştir⁶⁰⁶.

4. Fıkra da tanımlanan fiillerin işlenmesiyle, bilişim sistemi kullanmak suretiyle hırsızlık suçu (TCK m. 142/2-e) veya bilişim sistemi kullanmak suretiyle dolandırıcılık suçu (TCK m. 158/1-f) söz konusu olabilir⁶⁰⁷. Bu durumda,

⁶⁰⁵ Erdoğan, a.g.e., s. 246.

⁶⁰⁶ Karagülmez, a.g.e., s. 243; Dülger, a.g.e., s. 432; Özbek ve diğ., a.g.e., s. 963, dipnot: 530.

⁶⁰⁷ “...Nitelikli dolandırıcılık ve bilişim sistemindeki verileri bozma, yoketme, erişilmez kılma, sisteme veri yerleştirme suçlarından sanığın mahkûmiyetine ilişkin hükümler, sanık tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü:

Sanığın, olay tarihinde katılan ...'ın email ve buna bağlı oluşturduğu facebook hesabının şifresini kırmak suretiyle katılanın izni ve bilgisi olmaksızın erişim sağladığı ve katılanın erişimini şifresini değiştirerek engellediği, ardından da arkadaş listesinde bulunan katılan ...'tan annesinin rahatsız olduğunu, paraya ihtiyacı olduğunu belirterek 1.500 Euro para istediği, katılan ...'un da kardeşi olan katılan ... vasıtasıyla sanığın kendi T.C. kimlik numarası ve kendi adına kayıtlı cep telefonu bilgileri ile PTT aracılığı ile parayı gönderdiği, bu suretle sanığın bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık ve bilişim sistemindeki verileri bozma yoketme, erişilmez kılma, sisteme veri yerleştirme suçlarını işlediğinin iddia olunduğu olayda;

1- Sanık hakkında bilişim sistemindeki verileri bozma yoketme, erişilmez kılma, sisteme veri yerleştirme suçundan kurulan hükme yönelik temyiz talebinin incelenmesinde;

Tüm dosya kapsamından sanığın atılı suçu işlediği anlaşıldığından mahkemenin kabul ve uygulamasında bir isabetsizlik görülmemiştir.

Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre; sanığın temyiz itirazlarının reddi ile hükmün ONANMASINA,

2- Sanık hakkında nitelikli dolandırıcılık suçundan kurulan hükme yönelik temyiz talebinin incelenmesinde;

Tüm dosya kapsamından sanığın atılı suçu işlediği anlaşıldığından mahkemenin kabulünde bir isabetsizlik görülmemiştir.” 15.CD., 27.03.2018, 2017/2896 E., 2018/2111 K. (emsal.yargitay.gov.tr)

“...Şikayetçinin banka hesabına internet bankacılığı aracılığıyla girilip paranın banka hesabına transfer edilmesi şeklindeki sanığın eyleminin, TCK.nun 142/2-e madde ve fıkrasında düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, suç vasfında yanılığa düşülerek yazılı şekilde, TCK.nun 244/4. maddesi uyarınca mahkûmiyet hükmü kurulması, Yasaya aykırı, Cumhuriyet Savcısı ile sanığın temyiz itirazları bu itibarla yerinde görülmesi olduğundan hükmün bu sebepten dolayı 5320 sayılı Yasanın 8/1. maddesi uyarınca uygulanması gereken 1412 sayılı CMUK.nun 321. ve 326/son maddeleri gereğince BOZULMASINA, 22.11.2017

düzenlemenin tali norm olmasından dolayı diğer suçun oluştuğu kabul edilerek, buradaki hükmün uygulanmayacağı ileri sürülmüştür⁶⁰⁸.

YCGK'nun 17.11.2009 tarihinde verdiği kararla⁶⁰⁹ internet bankacılığı şifresinin ele geçirilip hesaptaki paranın başka bir hesaba transfer edilmesi olayında suç konusunun doğrudan bilişim verisi olmadığını, verinin temsil ettiği para olduğunu vurgulamaktadır. YCGK'nun çoğunluk görüşü şöyledir: “(...)Bu bilgiler ışığında somut olay değerlendirildiğinde; Sanık V.; firari S. ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, katılanın ...bank Ankara K... Şubesindeki hesabından 10.750 YTL'yi ...bank-İstanbul Z... Şubesinde sanık V. adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; **başka bir anlatımla varolan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir.** Kaldı ki sanığın katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCY'nin 142/2-e maddesinde düzenlenmiş bulunan “bilişim sistemi kullanılmak suretiyle hırsızlık” suçunun gerçekleştiği kabul edilmelidir. Şu halde, sanığın eyleminin 5237 sayılı TCY'nin 142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır.”

Çoğunluk görüşüne katılmayan üye ise, sahibinin rızası olmaksızın verinin başka bir bilişim sistemine gönderilmesinde hırsızlık suçunun oluşmayacağını çünkü bunun için verinin taşınır bir mal olarak düzenlenmesi gerektiğini belirtmiştir.

Şen, YCGK'nun çoğunluk görüşüne katılarak, karara konu olan olayda suç konusunun bilgisayarda mevcut bilgi, veri veya programın izinsiz alınması

gününde oybirliğiyle karar verildi.” 8.CD., 22.11.2017, 2017/16623 E., 2017/13121 K. (emsal.yargitay.gov.tr)

⁶⁰⁸ Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 892; Aynı görüşte bkz. Koca, üzülmez, **a.g.e.**, s. 561.

⁶⁰⁹ YCGK, 17.11.2009, 2009/11-193 E., 2009/268 K. (emsal.yargitay.gov.tr)

olmadığını, bilişim sistemleri kullanmak suretiyle taşınır mal niteliğinde olan paranın, sahibinin rızası olmadan bir başkasının hesabına aktarılması olduğunu belirtmektedir⁶¹⁰. Burada fiil, TCK m. 244'ün koruduğu veri odaklı haksız çıkar sağlamak ile ilgili değildir. Burada mağdura ilişkin hukuki yarar, bilişim sistemi ve verinin değil, bizzat taşınır bir malın zilyedin rızası dışında bulunduğu yerden alınması sonucunda zedelenmektedir⁶¹¹. Verinin bir başka yere gönderilmesi, hırsızlık suçu olmamakla beraber, bu yolla başkasına ait paranın zilyedinin tasarrufundan çıkarılması, hırsızlık suçu olarak kabul edilmelidir. Bu şekilde bir değerlendirme kanunilik prensibine aykırı olmadığı gibi, kıyas yasağını da ihlal etmez⁶¹².

Dülger, yukarıdaki YCGK kararına ilişkin değerlendirmesinde⁶¹³, paranın veri formunda olabileceğini ve veri formundaki bu paranın borçların ifası, mal alımı veya borç verilmesi gibi işlemlerde kullanıldığını ve bu işlemlerin borçlar hukuku ve ticaret hukuku açısından geçerli olduğunu belirtmekte ve veri formundaki paranın suça konu olabileceğinin de kabul edilmesi gerektiğini ileri sürmektedir. Yazar, bir banka veya finans kurumu nezdindeki hesapta bulunan paranın veri şeklinde temsil eden halinin başka bir deyişle veri formunda da aynen kâğıt para gibi kabul edilmesi gerektiğini ifade etmektedir⁶¹⁴. Burada amaca uygun yorum ilkesi ışığında, şeklen veri değil bunun temsil ettiği para suç tipi olarak dikkate alınmalıdır. Mağdur, böyle bir eylemde verilerini değil, parasını kaybetmektedir⁶¹⁵.

Karagülmez, benzer bir yorum yaparak, TCK m. 244/4'te düzenlenen haksız çıkar sağlama suçunun tali norm hükmünde olduğunu, eylemin ancak başka bir suç oluşturmaması durumunda uygulanabileceğini belirtmektedir⁶¹⁶.

Özbek, Doğan, Bacaksız ve Tepe, Yargıtay'ın taşınır niteliğindeki parayı bilişim sistemi kullanmak suretiyle başka bir banka hesabına havale yapmasını TCK m. 244/4 anlamında bir veri transferi olarak değil, verinin temsil ettiği paranın

⁶¹⁰ Şen, **a.g.m.**, s. 7.

⁶¹¹ **A.g.m.**

⁶¹² **A.g.m.**

⁶¹³ Dülger, **a.g.e.**, s. 579.

⁶¹⁴ **A.g.e.**, s. 580.

⁶¹⁵ **A.g.e.**

⁶¹⁶ Karagülmez, **a.g.e.**, s. 243.

aktarılması başka bir ifadeyle TCK m. 142/2-e’de düzenlenen “bilşim sistemi aracılığıyla nitelikli hırsızlık suçu”nu oluşturduğu kararına katılmadıklarını belirtmişlerdir⁶¹⁷.

Erdoğan, bu karar ile değerlendirmesinde, verinin taşınır mal olmadığını ve bu yüzden hırsızlık suçunun konusunu oluşturmayacağını belirtmektedir. Bilşim sistemi aracılığıyla hırsızlık suçunun, hırsızlık tanımına uygun malın (mesela bilşim sistemiyle kilit altında tutulan bir depodaki taşınır mallar gibi) bilşim sistemi aracılığıyla çalınması durumunda oluşabileceğini iddia etmektedir⁶¹⁸. Yazar, TCK m. 244/4’te düzenlenen “sistemi engelleme, bozma, verileri yok etme veya değiştirme” fiilleriyle haksız çıkar sağlama suçunda korunan hukuki değerin veri içeriğine göre belirlenmesi gerektiğini belirtmektedir. Buna göre, korunan hukuki değerin tespitinde verinin temsil edici özelliği göz önünde tutulacaktır. Örneğin verilere özel hayata ilişkin ise özel hayatın gizliliği, haberleşmeye ilişkin ise haberleşme özgürlüğü ihlal edilmiş olmaktadır⁶¹⁹.

Yargıtay’ın mağdurun rızasına aykırı olarak gerçekleşen telefon kontörü transferi eylemini⁶²⁰ hırsızlık suçu kapsamında değerlendirmeyip TCK m. 244/4’te düzenlenen “Sistemi engelleme, bozma, verileri yok etme veya değiştirme” fiilleriyle haksız çıkar sağlama suçunun oluşturduğuna karar vermiştir. Dülger bu kararı, muhalefet şerhinde ortaya konan görüşe paralel olarak, eleştirmiştir. Yazara göre, rızaya aykırı kontör transferi, tıpkı paranın bir başka kişinin hesabına havale edilmesinde olduğu gibi malvarlığında azalmaya neden olarak verinin temsil ettiği

⁶¹⁷ Özbek ve diğ., **a.g.e.**, s. 967.

⁶¹⁸ Erdoğan, **a.g.e.**, s. 289.

⁶¹⁹ **A.g.e.**, s. 214.

⁶²⁰ “Suç tarihinde sanığın Suç tarihinde sanığın internet üzerinden girdiği şifre ile müşterinin GSM numarasından başka bir GSM numarasına, oradan da yine şifre vasıtasıyla kendi numarasına müşterinin bilgisi ve rızası dışında kontör transferi yapma şeklinde gerçekleşen eyleminin TCK’nın 244/4. maddesindeki suçu oluşturduğu gözetilmeden suç vasfında yanılgiya düşölerek yazılı şekilde hüküm kurulması, bozmayı gerektirmiş(...) MUHALEFET ŞERHİ: (...) mağdura ait bulunan, ekonomik değeri ve doğrudan parasal karşılığı olan kontörü bilşim sistemini kullanmak suretiyle kendi telefon numarasına geçirmek suretiyle katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla varolan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği ve parasal değer ifade eden 70 adet kontörü alarak mal edinmeye yönelik olduğu açıktır. Yukarıda açıklanan nedenlerle somut olayda 5237 sayılı TCY’nın 142/2-e maddesinde düzenlenmiş bulunan “bilşim sistemi kullanılmak suretiyle hırsızlık” suçunun gerçekleşmesi nedeniyle yerel mahkemenin uygulamasının usul ve yasaya uygun olduğundan hükmün onanmasına karar verilmesi gerektiği görüşünde olduğumuzdan sayın çoğunluk görüşüne katılmıyoruz.” 13.CD., 30.01.2013, 2011/26435 E., 2013/1955 K., (emsa.yargitay.gov.tr)

paranın alınarak mal edinilmesidir. Bu nedenle bu eylem, hırsızlık suçu kapsamında değerlendirilmelidir⁶²¹.

Koca ve Üzülmaz, Yargıtay'ın rızaya aykırı telefon kontörü transferine ilişkin kararını katılmaktadır. Yazarlara göre telefon kontörü, ekonomik bir değere sahip olmakla birlikte para, hisse senedi veya altın gibi dış dünyada maddi bünyeye varlık değildir. Bu nedenle kontörün, mağdurun rızası olmaksızın bilişim sistemi kullanmak suretiyle başka bir telefona transfer edilmesi hırsızlık veya dolandırıcılık suçu olarak değerlendirilemez. Bu eylem, “sistemi engelleme, bozma, verileri yok etme veya değiştirme” fiilleriyle haksız çıkar sağlama suçu kapsamına girmektedir⁶²².

Yargıtay'ın, ekonomik değeri olan bazı verilerin, zilyedinin rızası olmaksızın alınması fiillerini hırsızlık suçu kapsamında değerlendirmedeği başka kararları da mevcuttur⁶²³.

İnternet üzerinden oynanan çevrimiçi oyunlarda kullanılan sanal oyun karakterleri ve eşyalarının çalınması ile ilgili bu kararlar, YCGK'nun yukarıda verilen kararını dar yorumlandığını göstermektedir. Verinin doğrudan parayı temsil ettiği olaylarda, eylemler TCK m. 142/2-e “bilişim sistemi kullanılmak suretiyle hırsızlık” suçu kapsamında değerlendirilmektedir. Bunun dışında, eğer veri, para dışında ekonomik değere sahip başka bir nesneyi temsil ediyorsa, söz konusu

⁶²¹ Dülger, **a.g.e.**, s. 582.

⁶²² Koca, Üzülmaz, **a.g.e.**, s. 837.

⁶²³ “(...) Katılanın 23.10.2011 tarihinde ... isimli oyunu oynarken bilgi ve rızası dışında e-posta adresine girilerek şifresinin ve e-posta adresinin değiştirildiğini ve **oyun karakterlerinin çalındığını**, (...) sanığın savunmasında, katılana ait e-posta adresini ... isimli oyunun hilelerinin ve kullanılmayan karakterlerinin paylaşıldığı forum sitesi olan www.onlinehile.org isimli sitede gördüğünü ve sitede bulunan şifre ile giriş yaptığını, oyun karakterlerinin ise sitede bulunmadığını ve suçlamayı kabul etmediğini söylediği (...) **Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği**, bu itibarla; suçun sübutu halinde eylemin, 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturacağı gözetilmeksizin suç vasfında yanılığa düşülerek yazılı şekilde hüküm kurulması (...)” 13.CD., 10.10.2017, 2016/2155 E., 2017/10403 K. (emsal.yargitay.gov.tr)

“(…) oyun şifresinin çalınıp oyun karakterlerinin aldığından bahisle açılan davada... şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, **çalındığı iddia edilen oyun karakterine ait sanal eşyaların** suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemin TCK.nun 244/4. maddesindeki suçu oluşturacağı da dikkate alınarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken (...)” 8.CD., 25.05.2017, 2017/897 E., 2017/6019 K. (emsal.yargitay.gov.tr)

eylemler, TCK m. 244/4'te düzenlenen "Sistemi engelleme, bozma, verileri yok etme veya deęiřtirme" fiilleriyle haksız ıkar saęlama suu kapsamına alınmaktadır.

Kanaatimize gre, veriye karřı gerekleřtirilen hukuka aykırı eylemlerin hangi su kapsamında deęerlendirileceęine karar verilirken, sz konusu verinin temsil ettięi deęerler dikkate alınmalıdır. Eęer veri, parayı veya ekonomik bir deęeri temsil ediyorsa, dięer řartların oluřması durumunda sz konusu hukuka aykırı eylem, hırsızlık (TCK m. 142/2-e) veya dolandırıcılık (158/1-f) suu kapsamında ele alınmalıdır. Bunun dıřında veriler, kiřisel veriler (TCK m. 135- 140), ticarî sır, bankacılık sırrı veya mřteri sırrı (TCK m. 239) veya Devlet Sırlarına Karřı Sular ve Casusluk blmnde (TCK m. 326 – 339) düzenlenen sulara iliřkin olduęunda, bu suların iřlendięi kabul edilmelidir. Aksi halde m. 244'te düzenlenen sular gndeme gelecektir.

b. Hukuka Aykırılık Unsuru

Biliřim sisteminin iřleyiřinin engellenmesi veya bozulması ile verilerin yok edilmesi veya deęiřtirilmesi sularında ilgilinin rızası uygunluk sebebidir⁶²⁴.

Kripto para birimi rneęinde, bilgisayarındaki sorunu gidermek iin onu bilgisayar tamircisine gtren kiři, tamircinin sabit diski formatlamasına rıza gstermiřse, tamirci bilgisayardaki sanal czdanın silinmesinden sorumlu tutulmayacaktır.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İřlenen Sularla Mcadele Edilmesi Hakkında Kanun'un 8. maddesi, maddede sayılı belli suların iřlenmesi halinde, hâkimin sz konusu internet sitelerine eriřimin engellemesine karar verebileceęini belirtmektedir. Bu durumda, kanunun hkmn yerine getirmek (TCK m. 24/1), hukuka uygunluk sebebidir. Bunun dıřında Ceza Muhakemesi Kanunu (CMK) m. 134'e gre kolluęun gerekleřtirdięi, bilgisayarlarda, bilgisayar programlarında ve ktklerinde arama, kopyalama ve el koyma iřlemleri de kanun hkmnn icrası kapsamındadır.

⁶²⁴ Parlar, **a.g.e.**, s. 27.

Kripto para birimi örneğinde, kamu görevlisinin, suçtan kaynaklanan malvarlığı değerine el koymak için, kişisel bilgisayardaki sanal cüzdanı kopyalaması bu kapsamda değerlendirilecektir.

c. Kusurluluk

Bu maddede düzenlenen bütün suçlar kasten işlenebilen suçlardır. 1. fıkradaki düzenlenen “sistemi engelleme ve bozma” suçunda failin kastı, sistemin işleyişini engellemeye veya bozmaya; 2. fıkra da düzenlenen suç “verileri yok etme veya değiştirme” suçunda failin kast verileri yok etmeye veya değiştirmeye yönelik olmalıdır. Genel kastla işlenebilen bu suçlar, tanımlarında başkaca bir manevi unsur aranmadığı için olası kastla da işlenebilirler⁶²⁵.

4. fıkra da düzenlenen “sistemi engelleme, bozma, verileri yok etme veya değiştirme yoluyla haksız çıkar sağlama” suçunda failin kastı, bilişim sistemini engellemeye veya bozmaya; sistemdeki verileri değiştirmeye veya yok etmeye ve bu fiillerin işlenmesi sonucunda haksız yarar elde etmeye yönelik olmalıdır.

Öğretide, “sistemi engelleme, bozma, verileri yok etme veya değiştirme yoluyla haksız çıkar sağlama” suçunun olası kastla işlenebilmesi tartışmalıdır. Failde özel kastın olması gerektiğini savunan yazarlar⁶²⁶, suçun olası kastla işlenemeyeceğini ileri sürerken, genel kastın varlığını yeterli görenler⁶²⁷, suçun olası kastla da işlenebileceğini ifade etmişlerdir.

Kanaatimize göre “sistemi engelleme, bozma, verileri yok etme veya değiştirme yoluyla haksız çıkar sağlama” suçunun tanımında haksız çıkar sağlama amacı arandığından, bu suç olası kastla işlenemez.

7. Suç ve Cezaya Etki Eden Nedenler

⁶²⁵ Koca, Üzülmüş, **a.g.e.**, s. 831; Soyaslan, **a.g.e.**, s. 649; Parlar, **a.g.e.**, s. 27; Tezcan, Erdem, Önok, **a.g.e.**, s. 1007.

⁶²⁶ Koca, Üzülmüş, **a.g.e.**, s. 841; Parlar, **a.g.e.**, s. 27.

⁶²⁷ Özbek ve diğ., **a.g.e.**, s. 969.

a. Suçu Ağırlaştırıcı Nedenler

Bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sisteminin işleyişinin engellenmesi veya bozulması ile bu sistemler üzerindeki verileri bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi

Maddenin 3. fıkrasında 1. ve 2. fıkarda tanımlanan sistemi engelleme ve bozma ile verilerin yok edilmesi veya değiştirilmesi eylemlerinin banka, kredi veya kamu kurum ve kuruluşuna ait bilişim sistemi üzerinde gerçekleştirilmesi, suçu ağırlaştırıcı nitelikli bir hal olarak düzenlenmiştir. Bu durumda verilecek ceza yarı oranında artırılacaktır⁶²⁸.

Bu düzenlemenin amacı, gerek banka veya kredi kurumlarından gerçekleştirilen finansal hizmetlerde gerekse kamu kurum ve kuruluşları tarafından yürütülen kamu hizmetlerinde yoğun bilişim sistemleri kullanımınıdır. Bu nedenle bu sistemlerin işleyişlerinin engellenmesi veya bozulması veya mevcut verilerinin güvenirliliğine zarar verecek eylemlerin gerçekleştirilmesiyle doğacak ağır sonuçların engellenmesi istenmiştir⁶²⁹.

Kanaatimize göre, kripto para biriminin yer aldığı bilişim sistemleri, özel girişimciler tarafından yönetilen sistemler oldukları ve banka veya finans kurumu sayılmadıkları için bunlara karşı gerçekleştirilecek söz konusu hukuka aykırı fiiller, bu nitelikli hal kapsamında değerlendirilemez.

⁶²⁸ "...SGK İl Müdürlüğü Tescil Servisinde veri hazırlama memuru olarak görev yapan sanığın, eşi... adına gerçeğe aykırı olarak Tarım Bağ-Kur tescil işlemi yapıp, tescil tarihini 01.04.1997 olarak geriye çekerek sigortalı işe giriş bildirgesi hazırlaması ve hakkında yapılan ihbar üzerine yakalanmamak amacıyla sigortalı terk işlemi yapıp, eşinin T.C. kimlik numarasını sistemden silmesi, isteğe bağlı Bağ-Kur sigortalısı olup, üç ay üst üste pirim ödememesi nedeniyle sistem tarafından otomatik olarak sanal terki yapılan gelini ...'ın terk tarihini değiştirerek sigortalıya 1 ay 20 gün hizmet kazandırması şeklinde gerçekleşen olayda; sanık tarafından sistem üzerinden usule ve yasal mevzuata aykırı olarak yapılan tüm işlemlerin idari soruşturma aşamasında iptal edilmesi ve haksız menfaatin temin edilememesi karşısında, sanığın eylemlerinin zincirleme şekilde TCK'nın 244/2-3. maddesinde düzenlenen "kamu kurum veya kuruluşuna ait bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme" suçu oluşturduğu gözetilmeden, TCK'nın 244/4. maddesi uyarınca hüküm kurulması..." 11.CD., 09.09.2017, 2017/2370 E., 2017/5756 K. (emsal.yargitay.gov.tr)

⁶²⁹ Özbek ve diğ., a.g.e., s. 962.

b. Suçu Hafifleten Nedenler

TCK m. 244'te düzenlenen suçlar için cezayı hafifletici nitelikli haller öngörülmemiştir.

8. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

1. fıkra düzenleneni sistemi engelleme ve bozma suçunda, bilişim sisteminin engellenmesi veya bozulmasıyla suç tamamlanır. Failin bu amaçla hareket etmesine rağmen, sistemin çalışması bundan etkilenmeyebilir. Keza 2. fıkra düzenleneni sistemdeki verileri yok etme ve değiştirme suçunda, verileri yok etmek veya değiştirmek için hareket eden fail amacına ulaşmayabilir. Bu durumda suç teşebbüs aşamasında kalmış olacaktır⁶³⁰.

Kripto para birimi örneğinde, madencilik yapan bilişim sistemini bozmaya yönelik olarak gönderilen bilgisayar virüsünü, sistemi koruyan antivirüs programı engellerse, suç teşebbüs aşamasında kalacaktır.

4. fıkra düzenleneni “sistemi engelleme, bozma, verileri yok etme veya değiştirme yoluyla haksız çıkar sağlama” suçunun icrası kapsamında, haksız çıkar sağlamak için bilişim sistemlerine ve verilerine karşı gerçekleştirilen fiillerin neticesinde haksız çıkar elde edilmeyebilir. Bu durumda suç teşebbüs aşamasında kalacaktır⁶³¹. Fakat teşebbüsün hangi suça ilişkin olduğunu, failin kastı belirleyecektir. Örneğin, haksız çıkar elde etmek için sisteme veri yerleştiren fail, haksız çıkar elde edememişse, kastı haksız çıkar elde etmek olduğundan TCK m. 244/4'te düzenlenen suça teşebbüs etmiştir. Aksi halde, 2. fıkradaki suç tamamlanmış sayılacaktır⁶³².

Kripto para birimi örneğinde, kişinin bilgisayarında sakladığı sanal cüzdanındaki gizli anahtar, sisteme gönderilen bir bilgisayar virüsüyle ele geçirilip

⁶³⁰ Koca, Üzülmöz, **a.g.e.**, s. 832; Erdoğan, **a.g.e.**, s. 202; Soyaslan, **a.g.e.**, s. 649; Parlar, **a.g.e.**, s. 27.

⁶³¹ Soyaslan, **a.g.e.**, s. 653; Koca, Üzülmöz, **a.g.e.**, s. 841.

⁶³² Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 893.

başka bir yere gönderilmek istendiğinde, işlem güvenlik duvarı engeline takılıp tamamlanamazsa, suç teşebbüs aşamasında kalmış olacaktır.

TCK m. 244/4'deki suçu işleyen failin kastı haksız çıkar sağlamak olsa da, bu düzenleme tali norm olduğundan, eğer bilişim sistemi kullanmak suretiyle hırsızlık veya dolandırıcılık suçu gerçekleşmişse, bu suçlara teşebbüs söz konusu olacaktır. Örneğin, mağdurun gizli anahtarını ele geçiren fail, hesaptaki paraları kendi hesabına aktarmayı başaramadığı durumda, failin kastı bilişim sistemi kullanma suretiyle hırsızlık olduğundan, hırsızlığa teşebbüsten cezalandırılacaktır.

b. İçtima

Öğretide, 1. ve 2. fıkralarda düzenlenen suçlar bakımından TCK m. 243'de düzenlenen "bilişim sistemine girme" suçunun, "geçit suç" olduğunu, bu nedenle, failin, sadece bu fıkralarda düzenlenen suçlardan cezalandırılması gerektiği öne sürenler⁶³³ olduğu gibi, fikri içtima uygulanması gerektiğini öne süren yazarlar⁶³⁴ bulunmaktadır.

Geçit suç ilişkisi TCK m. 243 ile 4. fıkra da düzenlenen haksız yarar sağlama suçu arasında da vardır⁶³⁵.

Kanaatimize göre, bilişim sistemine veya sistemdeki verilere zarar verme suçları ile bilişim sistemlere girme suçu (TCK m. 243) arasında araç - amaç ilişkisi söz konusu olabilir. Bu tür bir ilişkinin olduğu olaylarda, failin kastı doğrultusunda suç fiili tek bir bütün olarak kabul edilmeli ve olayın özelliğine göre amaç suçun işlendiği kabul edilmelidir.

2. fıkra da düzenlenen bilişim verilerine zarar verme suçunun işlenmesi ile TCK m. 151'de düzenlenen mala zarar verme suçu da oluşmaktadır. Bu durumda fikri içtima hükümleri uygulanmalıdır⁶³⁶.

⁶³³ Dülger, **a.g.e.**, s. 430; Özbek ve diğ., **a.g.e.**, s. 950; Soyaslan, **a.g.e.**, s. 650; Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 884; Erdoğan, **a.g.e.**, s. 202; Parlar, **a.g.e.**, s. 28.

⁶³⁴ Koca, Üzülmüş, **a.g.e.**, s. 819.

⁶³⁵ Soyaslan, **a.g.e.**, s. 652; Parlar, **a.g.e.**, s. 28.

⁶³⁶ Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 889.

Kanaatimize göre, 1. ve 2. fıkra düzenlenen suçlar ile TCK m. 151’de düzenlenen mala zarar verme suçları arasında genel norm - özel norm ilişkisi olduğundan, bilişim sistemlerine ilişkin sistemi engelleme ve bozma ile verileri yok etme ve değiştirme eylemleri 1. ve 2. fıkra kapsamında değerlendirilmelidir.

Kripto para birimi örneğinde, Bitcoin madenciliği yapmasını engellemek için mağdurun bilişim sistemine giren ve sistemi bozan kişi, sadece “sistemi engelle ve bozma” suçundan sorumlu tutulmalıdır.

Bilişim verilerinin başka bir yere gönderilmesi, TCK m. 136’da düzenlenen “kişisel verileri hukuka aykırı olarak verme veya ele geçirme” suçuna da neden olabilir⁶³⁷. Bu durumda olayın özelliğine göre fıkri içtima uygulanabileceği gibi her iki suçtan da cezalandırma yoluna gidilebilir.

Bilişim sistemine veri eklenmesi ve verilerin değiştirilmesi, bir belgenin düzenlenmesine esas oluşturuyorsa, TCK m. 212’de düzenlenen belgede sahtecilik suçu da gündeme gelecektir. Bu durumda fail ayrıca bu suçtan da cezalandırılmalıdır⁶³⁸.

4. fıkra düzenlenen 1. ve 2. fıkradaki fiillerin işlenmesi neticesinde haksız çıkar elde etme suçu tali norm olduğundan, işlenen fiille hırsızlık veya dolandırıcılık gibi başka bir suç gerçekleşmişse, bu fıkradaki hüküm uygulanmayacak, diğer suçun olduğu kabul edilecektir⁶³⁹.

⁶³⁷ “...Dosya kapsamına göre; sanığın, katılanın cep telefonunu katılandan habersiz kendi kullandığı bilgisayara bağlayarak içerisinde bulunan rehber ve media dosyalarının tamamını ele geçirdiği ve cep telefonundaki kayıtları sildiği iddia ve kabul edilen olayda, sanığın sübut bulan eylemleri nedeniyle TCK’nın 244/2. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme, aynı Kanunun 134/1 maddesinde düzenlenen özel hayatın gizliliğini ihlal ve 136/1 maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçlarını oluşturduğu gözetilmeden sadece TCK’nın 136/1. maddesinde düzenlen verileri hukuka aykırı olarak verme veya ele geçirme suçundan sanığın mahkumiyete karar verilmesi aleyhe temyiz olmadığından bozma nedeni yapılmamıştır.

Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre, sanık müdafinin atılı suçun yasal unsurlarının oluşmadığına ilişkin temyiz itirazlarının reddiyle, eleştirilen husus dışında, sair yönleri usul ve kanuna uygun bulunan hükmün isteme aykırı olarak ONANMASINA, 18.10.2017 tarihinde oybirliğiyle karar verildi.” 12.CD., 18.10.2017, 2016/10576 E., 2017/7642 K. (emsal.yargitay.gov.tr)

⁶³⁸ A.g.e.

⁶³⁹ Artuk, Gökçen, Yenidünya, a.g.e., s. 892.

1. ve 2. fıkradaki düzenlenen “sistemi engelleme, bozma, verileri yok etme veya değiştirme” fiilleri, 4. fıkra düzenleneni haksız çıkar sağlama suçunun birer unsuru haline dönüştüklerinden, bu suçun işlenmesi durumunda, fail sadece 4. fıkraya göre cezalandırılacaktır⁶⁴⁰.

Bu suçların zincirleme suç olarak, başka bir deyişle aynı suç işleme kararının icrası kapsamında değişik zamanlarda aynı kişiye karşı birden fazla işlenmesi mümkündür⁶⁴¹.

c. İştirak

TCK m. 244’te düzenlenen, bilişim sistemi engelleme ve bozma; sistemdeki verileri yok etme ve değiştirme ile bu fiilleri işleyerek haksız yarar sağlama suçları, iştirak bakımından bir özellik göstermemektedir ve bu nedenle müşterek faillik, azmettirme ve yardım etme şeklinde her türlü iştirak söz konusu olabilir⁶⁴².

9. Yaptırım

1. fıkra düzenleneni sistemi engelleme ve bozma suçunun cezası, bir yıldan beş yıla kadar hapis cezasıdır (TCK m. 244/1).

2. fıkra düzenleneni verileri yok etme ve değiştirme suçunun cezası, altı aydan üç yıla kadar hapis cezasıdır (TCK m. 244/2).

1. ve 2. fıkradaki fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza yarı oranında artırılır (TCK m. 244/3).

4. fıkra düzenleneni haksız yarar sağlama suçunun cezası, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasıdır. Fakat bu suça ilişkin fiiller, başka bir suçun oluşumuna da neden oluyorsa, fail o suçtan da cezalandırılacaktır (TCK m. 244/4).

⁶⁴⁰ Özbek ve diğ., **a.g.e.**, s. 970.

⁶⁴¹ Artuk, Gökçen, Yenidünya, **a.g.e.**, s. 884; Dülger, **a.g.e.**, s. 428; Özbek ve diğ., **a.g.e.**, s. 969.

⁶⁴² Soyaslan, **a.g.e.**, s. 650; Özbek ve diğ., **a.g.e.**, s. 969; Tezcan, Erdem, Önok, **a.g.e.**, s. 1010.

10. Muhakemeye İlişkin Kurallar

TCK m. 244'te düzenlenen suçlar şikâyeteye tabi olmayıp re'sen takip edilen suçlardır.

5235 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. maddesi uyarınca sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu kovuşturmayla görevli mahkeme, asliye ceza mahkemesidir.



III. Adliye Karşı Suçlar

Adliye karşı suçlar, 5237 sayılı Türk Ceza Kanunu'nda ikinci kitabın dördüncü kısmında *Adliye Karşı Suçlar* başlıklı ikinci bölümde, 267 ilâ 298. maddeleri arasında düzenlenmiştir⁶⁴³.

İncelememizin başında detaylı olarak gösterildiği üzere FATF, IMF, OECD, ECB gibi uluslararası ve bölgesel kuruluşlar, kripto para birimlerinin terörün finansmanı, vergi kaçırma ve kara para aklama suçlarında kullanılmaları üzerinde önemle durmuşlar ve bu konudaki risklerin giderilmesi veya azaltılması için ulusal ve uluslararası düzeyde önemler alınmasını önermişlerdir.

İncelememizin bu kısmında, kripto para birimlerinin suç konusu olabileceği Adliye Karşı Suçlar bölümünde TCK m. 282'de düzenlenmiş olan “suçtan kaynaklanan malvarlığı değerlerini aklama” suçu ele alınacaktır.

A. Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu (TCK m. 282)

1. Genel Olarak

Suçtan kaynaklanan malvarlığı değerlerini aklama suçu, 5237 sayılı Türk Ceza Kanunu'nda ikinci kitabın dördüncü kısmında *Adliye Karşı Suçlar* başlıklı ikinci bölümde bölümünde 282. maddede düzenlenmiştir.

⁶⁴³ Bu bölümde şu suçlar düzenlenmiştir: *İftira* (m.267), *Başkasına ait kimlik veya kimlik bilgilerinin kullanılması* (m. 268), *Suç üstlenme* (m. 270), *Suç uydurma* (m. 271), *Yalan tanıklık* (m. 272), *Yalan yere yemin* (m. 275), *Gerçeğe aykırı bilirkişilik veya tercümanlık* (m. 276), *Yargı görevi yapma, bilirkişiyi veya tanığı etkilemeye teşebbüs* (m. 277), *Suç uydurma* (m. 278), *Kamu görevlisinin suçu bildirmemesi* (m. 279), *Sağlık mesleği mensuplarının suçu bildirmemesi* (m. 280), *Suç delillerini yok etme, gizleme veya değiştirme* (m. 281), *Suçtan kaynaklanan malvarlığı değerlerini aklama* (m. 282), *Suçluyu kayırma* (m. 283), *Tutuklu, hükümlü veya suç delillerini bildirmeme* (m. 284), *Gizliliğin ihlali* (m. 285), *Ses veya görüntülerin kayda alınması* (m. 286), *Genital muayene* (m. 287), *Adil yargılamayı etkilemeye teşebbüs* (m. 288), *Muhafaza görevini kötüye kullanma* (m. 289), *Resmen teslim olunan mala elkonulması ve bozulması* (m. 290), *Başkası yerine ceza infaz kurumuna veya tutukevine girme* (m. 291), *Hükümlü veya tutuklunun kaçması* (m. 292), *Kaçmaya imkân sağlama* (m. 294), *Muhafızın görevini kötüye kullanması* (m. 295), *Hükümlü veya tutukluların ayaklanması* (m. 296), *İnfaz kurumuna veya tutukevine yasak eşya sokmak* (m. 297), *Hak kullanımını ve beslenmeyi engelleme* (m. 298).

Suçun temel şekli “*Alt sınırı altı ay veya daha fazla hapis cezasını gerektiren bir suçtan kaynaklanan malvarlığı değerlerini, yurt dışına çıkaran veya bunların gayrimeşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla, çeşitli işlemlere tâbi tutan kişi, üç yıldan yedi yıla kadar hapis ve yirmibin güne kadar adli para cezası ile cezalandırılır.*” olarak düzenlenmiştir.

Maddenin 2. fıkrasında, suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçu düzenlenmiştir: “*Birinci fıkradaki suçun işlenmesine iştirak etmeksizin, bu suçun konusunu oluşturan malvarlığı değerini, bu özelliğini bilerek satın alan, kabul eden, bulunduran veya kullanan kişi iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.*”

Maddenin 3. ve 4. fıkrasında ilk iki fıkroda düzenlenen suçların nitelikli halleri düzenlenmiştir. 5. fıkroda, bu suçların lehine işlendiği tüzel kişiye, tüzel kişilere özgü güvenlik tedbiri uygulanacağı hüküm altına alınmıştır. Son fıkroda ise bu suçlar için etkin pişmanlık hükmü düzenlenmiştir.

1. fıkroda düzenlenen suçtan kaynaklanan malvarlığı değerlerini aklama suçunun tamamlanması için daha önce işlenmiş bir suçtan elde edilmiş malvarlığı değerinin yurt dışına çıkarılması, kaynağının gizlenmesi veya meşru yollarla elde edildiği kanaatini uyandırmak amacıyla çeşitli işlemlere tabi tutulması gerekmektedir⁶⁴⁴.

2. fıkroda düzenlenen, suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçunun oluşabilmesi için bu suçun failinin iştirak etmeksizin aklama suçunun gerçekleşmiş olması gerekmektedir. Bu suçun düzenlenmesiyle TCK m. 165’te tanımlanan “*suç eşyasını satın almak veya kabul etmek*” suçu⁶⁴⁵ arasında genel norm - özel norm ilişkisi oluşturulmuştur⁶⁴⁶.

⁶⁴⁴ Yener Ünver, **Adliye Karşı Suçlar**, 2. b., Ankara: Seçkin Yayıncılık, 2010, s. 297.

⁶⁴⁵ **TCK Madde 165-** (1) Bir suçun işlenmesiyle elde edilen eşyayı veya diğer malvarlığı değerini, bu suçun işlenmesine iştirak etmeksizin, satan, devreden, satın alan veya kabul eden kişi, altı aydan üç yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.

⁶⁴⁶ Dülger, **a.g.e.**, s. 385.

Fakat bu suç ancak doğrudan kastla işlenebilir olmakla suç eşyasını satın almak veya kabul etmekten ayrılmaktadır⁶⁴⁷.

Suçtan kaynaklanan malvarlığı değerlerini aklama suçu, yerleştirme, ayrıştırma ve bütünleştirme şeklinde üç aşamada gerçekleşmektedir. Yerleştirme aşamasında, suçtan elde edilen gelir, nakit formundan finans sisteme aktarılmaktadır. Ayırma veya ayrıştırma aşamasında, çok sayıda karmaşık mali işlem yapılarak, suç gelirinin kaynağıyla olan bağı koparılmaya, izi takip edilemez hale getirilmeye çalışılmaktadır. Bütünleşme aşamasında ise, suç geliri, yasal yollarla finans sistemine sokulmaktadır⁶⁴⁸.

Kripto para birimleri için uluslararası hukuksal düzenleme arayışları bölümünde, bu sistemlerin suçtan kaynaklanan malvarlığı değerlerinin aklanmasında kullanılmasının çeşitli kuruluşlar tarafından öngörüldüğünü açıklanmıştı⁶⁴⁹.

Kripto para birimleri, aklama suçunun üç aşamasında da kullanılabilir. Yerleştirme aşamasında, suç geliri, nakit veya diğer finansal araçlar yerine kripto para birimi olarak tutulduğunda, bankacılık ve finans sistemlerinin tabi olduğu sıkı denetim şartlarından korunmuş olmaktadır.

Kripto para birimleri ayrıştırma aşamasında aklama suçuna kolaylık sağlayacak imkânlar sunmaktadır. Yukarıda açıklanan karıştırma (*mixing*) hizmetleriyle⁶⁵⁰ karmaşık para hareketleri gerçekleştirilerek, suç gelirinin kaynağı ile ilişkisi kopartılabilir ve bu şekilde izi kaybettirilebilir.

Aklama suçunun bütünleştirme aşamasında da kripto para birimlerinin kullanılması mümkündür. Suçtan elde edilen malvarlığı değerleri kripto para olarak tutulduğunda, bu paralar ile gerçek ve sanal mal ve hizmetleri alınabilir, takas

⁶⁴⁷ Kerim Çakır, **Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu**, Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul, 2016, s. 209.

⁶⁴⁸ Dülger, **a.g.e.**, s. 53-57; Çakır, **a.g.e.**, s. 24-28; Mali Suçları Araştırma Kurulu (MASAK), **Aklamının Aşamaları**, <http://www.masak.gov.tr/tr/content/aklamenin-asamalari/58>, Erişim tarihi: 19 Ağustos 2018.

⁶⁴⁹ Bkz. s. 36.

⁶⁵⁰ Bkz. s. 27.

merkezlerinde ulusal paralara çevrilebilir. Bu şekilde suçtan elde edilen malvarlığı değerlerinin finans sistemine yasal işlemlerle sokulması mümkündür.

2. Suçun Faili

Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun faili herkes olabilir⁶⁵¹. Buna göre suçtan kaynaklanan malvarlığı değerini “yurt dışına çıkaran” veya bunların yasadışı kaynağını veya elde ediliş yolunu gizlemek için “çeşitli işlemlere tabi tutan” herkes bu suçun faili olabilir.

İkinci fıkrada tanımlanan suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçunu, fail, azmettiren veya yardımcı olarak herkes işleyebilir veya katılabilir; fakat söz konusu kişinin, 1. fıkrada tanımlanan aklama suçuna iştirak etmemesi gerekir. Aksi halde bu kişi, aklama suçundan sorumlu tutulacaktır⁶⁵².

Ünver, suça ilişkin hükmün gerçek ve tüzel kişilerin bu suça faili olabilecek şekilde özgü suç olarak düzenlendiğini belirtmektedir⁶⁵³.

Doktrinde, suçun düzenleniş biçimine göre tüzel kişilerin bu suçun faili olabileceği hususu tartışmalıdır⁶⁵⁴.

3. Suçun Mağduru

Suçun mağduru, toplumu oluşturan herkestir⁶⁵⁵. Suçun Adliye Karşı Suçlar bölümünde düzenlenmesi, mağdurun Devlet olabileceğini düşündürse de⁶⁵⁶, tüzel

⁶⁵¹ Dülger, **a.g.e.**, s. 192.

⁶⁵² Çakır, **a.g.e.**, s. 360.

⁶⁵³ Ünver, **a.g.e.**, s. 299. Yazar, incelemesinin devamında, s. 312’de bu suç tipinin özgü suç olmadığını belirtmektedir.

⁶⁵⁴ Ünver, **a.g.e.**, s. 299; Sacit Yılmaz, “Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu”, **Ankara Barosu Dergisi**, C. 2011/2, 2011, s. 78. Yazar, tüzel kişilerin bu suçun faili olarak düzenlenmesini eleştirmektedir. Tüzel kişilerin bu suçun faili olamayacağına savunan görüş için bkz. Dülger, **a.g.e.**, s. 200.

⁶⁵⁵ Çakır, **a.g.e.**, s. 246.

⁶⁵⁶ Yılmaz, **a.g.m.**, s. 78.

kişiler, suçun mağduru olamayıp suçtan zarar gören olabileceklerinden Devlet bu suçun mağduru olamaz. Yargıtay da bu görüştedir⁶⁵⁷.

Suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçu da topluma karşı işlendiğinden bu suçun mağduru toplumu oluşturan herkeştir⁶⁵⁸.

4. Suçla Korunan Hukuki Yarar

Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun Adliye Karşı Suçlar bölümünde düzenlenmesine dikkat çeken Dülger, bu düzenlemeyle korunan temel hukuki yararın kamu düzenini sağlamak olduğunu, fakat bunun yanında adaletin düzgün işlenmesi, suç gelirlerine sahip olunmasının ve kullanılmasının engellenmesi ve yeni suçlara finansman desteğinin kesilmesinin de korunan değerler arasında olduğunu belirtmektedir⁶⁵⁹.

Kocasakal, mülga 765 sayılı TCK'de yer alan "Karapara aklama suçu"nda, yasadışı faaliyetlerin finansmanının önlenmesi, kamu düzeni ile finansal ve ekonomik düzenin korunmasının amaçlandığını belirtmektedir⁶⁶⁰.

2. fıkrada düzenlenen suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçunda korunan hukuki yarar, suçtan kaynaklanan malvarlığı değerlerini aklama suçu ile aynıdır⁶⁶¹.

⁶⁵⁷ "Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun niteliği itibariyle somut olayda suçtan doğrudan zarar görmesi söz konusu olmayan Hazine'nin davaya katılmasına karar verilmesi, hukuki değerden yoksun olup hükmü temyize hak vermeyeceğinden, hazine vekilinin temyiz isteminin CMUK'nın 317. maddesi uyarınca REDDİNE, 31.05.2016 tarihinde oybirliğiyle karar verildi."

(16.CD., 2016/2422 E. , 2016/3835 K.)

⁶⁵⁸ Dülger, **a.g.e.**, s. 360.

⁶⁵⁹ Murat Volkan Dülger, **Suçtan Kaynaklanan Malvarlığı Değerlerinin Aklanmasına İlişkin Suçlar ve Yaptırımlar**, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul, 2010, s. 187.

⁶⁶⁰ Ümit Kocasakal, **Karapara Aklama Suçu**, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul, 2000, s. 174.

⁶⁶¹ Dülger, **a.g.e.**, s. 359.

5. Suçun Maddi Konusu

Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun konusu, suçtan kaynaklanan malvarlığı değeridir⁶⁶². Bu malvarlığı değerinin, daha önce işlenmiş ve alt sınırı bir yıl veya daha fazla hapis cezasını gerektiren bir suçtan elde edilmiş olması gerekmektedir. Bu suç, doktrinde öncül suç olarak nitelendirilmektedir. Söz konusu malvarlığı değerleri, ya bir suçun işlenmesi neticesinde elde edilmiş olmalı veya bir suçun işlenmesi dolayısıyla elde edilmiş olmalıdır⁶⁶³.

Aklama suçundan hüküm kurulması için öncül suçtan mahkûmiyet kararı gerekmemekte, fakat suçun işlendiğinin belirlenmiş olması gerekmektedir⁶⁶⁴. Suçun yurt dışında işlenmesi durumunda da, ilgili suç öncül suç kapsamında değerlendirilecektir⁶⁶⁵.

2. fıkarda düzenlenen suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçunun konusu da aklama suçu ile aynıdır⁶⁶⁶.

Mülkiyete göre üst bir kavram olan malvarlığında mülkiyet ile beraber, zilyetlik, ayni haklar, fikri haklar ve alacak hakları yer almaktadır⁶⁶⁷. Mülkiyetten doğan haklar ile ayni, fikri ve alacak hakları malvarlığının aktif kısmında yer alırken, kişinin borçları ve üstlendiği maddi yükümlülükler malvarlığının pasifini oluştururlar. Aktif varlıklar kişinin malvarlığını arttırırken, pasif öğeler azaltırlar⁶⁶⁸. Malvarlığı ile ilgili detaylı açıklamalar için *Malvarlığı Karşı Suçlar* bölümünde yapılan açıklamalara bakılabilir⁶⁶⁹.

⁶⁶² Ünver, **a.g.e.**, s. 303; Dülger, **a.g.e.**, s. 205; Kocasakal, **a.g.e.**, s. 203.

⁶⁶³ Çakır, **a.g.e.**, s. 257.

⁶⁶⁴ Kocasakal, **a.g.e.**, s. 201; Yılmaz, **a.g.m.**, s. 80; Dülger, **a.g.e.**, s. 209; Çakır, **a.g.e.**, s. 278.

⁶⁶⁵ Dülger, **a.g.e.**, s. 215; Çakır, **a.g.e.**, s. 273.

⁶⁶⁶ Dülger, **a.g.e.**, s. 361.

⁶⁶⁷ Tezcan, Erdem, Önok, **a.g.e.**, s. 652; Koca, Üzülmüş, **a.g.e.**, s. 509.

⁶⁶⁸ Centel, Zafer, Çakmut, **a.g.e.**, s. 308.

⁶⁶⁹ Bkz. s. 89.

6. Suçun Unsurları

a. Maddi Unsur

Suçtan kaynaklanan malvarlığı değerlerini aklama suçu, seçimlik hareketli bir suçtur⁶⁷⁰. Bu seçimlik hareketlerden birisinin veya her ikisinin işlenmesiyle suç tamamlanmış olur.

İlk seçimlik hareket, suçtan kaynaklanan malvarlığı değerinin yurt dışına çıkarılması şeklinde düzenlenmiştir. Bu nedenle suç bağlı hareketlidir. Malvarlığı değerinin yurt dışına nasıl transfer edildiğinin bir önemi yoktur. Bu işlem, elektronik fon transferi gibi banka veya finansal bir kuruluş aracılığıyla olabileceği gibi, nakit olarak üstte taşınmak suretiyle de gerçekleştirilebilir.

İnceleme konumuz kripto para örneğinde, bu suç bakımından öncül suç olarak kabul edilecek bir suçun işlenmesiyle elde edilmiş kripto para türünden kara paranın, yurt dışında bulunan birisinin hesabına transfer edilmesi, bu hareketi oluşturacaktır. Bu seçimlik hareketin gerçekleştirilişi sırasında, yurt dışına transfer edilen malvarlığı değerlerinin suçtan elde edilmiş olduğunun bilinmesi başka bir deyişle failde bu kastın varlığı yeterlidir⁶⁷¹.

İkinci seçimlik hareket, suçtan kaynaklanan malvarlığı değerlerinin gayrimeşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak amacıyla çeşitli işlemlere tabi tutmak şeklinde düzenlenmiştir. Suçtan elde edilen malvarlığı değerinin yasadışı kaynağını gizlemek ve meşru bir yolla elde edildiği konusundan ilgililer nezdinde kanaat uyandırmak için malvarlığı değerini, “değerlendirme”, “kullanma”, “bulundurma”, “kaynak, nitelik, zilyet veya malikinin değiştirilmesi veya gizlenmesi” gibi çeşitli işlemlerden geçirmek, bu hareketin gerçekleşmesini sağlayacaktır. Bu işlemler değişik şekilde gerçekleştirilebilir. Bu nedenle bu seçimlik hareket, serbest hareketlidir. Doktrinde, “çeşitli işlemler”

⁶⁷⁰ Ünver, **a.g.e.**, s. 300.

⁶⁷¹ TCK 282. madde gerekçesi.

ifadesiyle, kanunilik ilkesi gereği, birden fazla işlemin yapılması gerektiği ileri sürülmektedir⁶⁷².

Kripto para örneğinde, para hareketlerinin kimler arasında gerçekleştirildiğini gizlemek amacıyla kullanılan karıştırma hizmetinden (*mixing service*) yararlanmak⁶⁷³, bu hareket kapsamında değerlendirilecektir.

2. fıkra düzenlenen suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçu, seçimlik hareketli bir suçtur. Tanımda yer alan “satın alma”, “kabul etme”, “bulundurma”, ve “kullanma” eylemlerinin aklama suçundan elde edilen malvarlığı değerlerine karşı gerçekleştirilmesiyle suç oluşur. Failin, suçun tanımında belirtilen eylemler dışında başka bir eylemi işlemesi durumunda, bu suç oluşmaz. Bu nedenle suç, bağlı hareketli bir suçtur⁶⁷⁴.

Kripto para örneğinde, suçtan kaynaklanan malvarlığı değeri olarak kripto para birimini kabul eden failin eylemi bu suç kapsamında değerlendirilecektir.

b. Hukuka Aykırılık Unsuru

Hukuka uygunluk sebepleri arasında sadece kanun hükmünü yerine getirmenin suçtan kaynaklanan malvarlığı değerlerini aklama suçunda uygulanabileceği belirtilmektedir⁶⁷⁵. 2006 yılında yürürlükten kaldırılmış olan 4208 sayılı Kanunun 10 ve 11. maddeleri halen yürürlükte. Söz konusu maddelerde düzenlenen “kontrollü teslimat” olarak gerçekleştirilen işlemler, kanun hükmünü icra kapsamında değerlendirilecektir. Buna göre, yetkili makamların bilgisi ve denetimi altında, suç faillerinin belirlenmesi, her türlü delilin tespiti, toplanması, kaçak veya kaçak olmasından şüphe edilen mal veya fonların müsaderesi amacıyla, yurt içinde dağıtılacak veya yurt dışından Türkiye'ye getirilerek dağıtılacak veya Türkiye'de hazırlanarak yurtdışına götürülecek veya Türkiye'den transit geçecek, uyuşturucu ve psikotrop maddeler, 1988 tarihli Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına

⁶⁷² Ünver, **a.g.e.**, s. 302; karşıt görüş için bkz. Dülger, **a.g.e.**, s. 258.

⁶⁷³ *Mixing Service* (karıştırma hizmeti) için “Kripto Para Birimlerinin Ortak Özellikleri” altında *Anonimlik* kısmına bakınız.

⁶⁷⁴ Dülger, **a.g.e.**, s. 364.

⁶⁷⁵ Dülger, **a.g.e.**, s. 303.; Çakır, **a.g.e.**, s. 307.

Karşı Birleşmiş Milletler Sözleşmesinin⁶⁷⁶ eki I ve II numaralı tablolar ile bu tablo değişikliklerinde yer alan maddelerin ve bunlara bağlı fonlar veya karapara veya karaparaya kaynaklık edecek diğer her türlü kaçak veya kaçak olmasından şüphe edilen eşyanın nakilleri, bu kapsamda değerlendirilecektir.

Kripto para birimi örneğinde, yetkili makamların bilgisi ve denetimi altında, suç faillerin belirlenmesi veya delillerin toplanması amacıyla uyuşturucu ticareti yapan kişilere kripto para cinsinden fon transferinin yapılması, kanun hükmünü icra kapsamında değerlendirilecektir.

c. Kusurluluk

Suçtan kaynaklanan malvarlığı değerlerini aklama suçu, kasten işlenebilir. Suç, seçimlik hareketli bir suç olması nedeniyle her bir seçimlik hareket için manevi unsurunun ayrı olarak değerlendirilmesi gerekir. Buna göre, suç, ilk seçimlik hareket olan suç konusunu yurt dışına çıkarmak şeklinde işlendiği takdirde, suçun oluşumu için genel kast yeterli görülmektedir⁶⁷⁷. Bu durumda fail, suç konusunun daha önceden işlenmiş bir suçtan elde edildiğini ve yurt dışına çıkartarak bu malvarlığı değerini akladığını bilmeli ve istemelidir.

İkinci seçimlik hareket, yasadışı elde edilen malvarlığı değerinin kaynağını gizlemek veya meşru yollardan edinildiği kanaatini uyandırmak amacıyla çeşitli işlemler gerçekleştirmektedir. Bu düzenlemede geçen “amacıyla” ifadesi harekette özel kastın arandığını göstermektedir⁶⁷⁸. Buna göre, fail tarafından icra edilen işlemler, suçtan elde edilmiş malvarlığı değerinin kaynağını gizleme veya meşru yollardan edinildiği amacıyla gerçekleştirilmemişse, bu seçimlik hareket bakımından suç oluşmayacaktır.

Kasten işlenebilen suçlar, kural olarak olası kastla da işlenebilir. Fakat suçun düzenlenişinde, “bilerek”, “bildiği halde”, “bilmesine rağmen” gibi ifadeler varsa bu

⁶⁷⁶ Türkiye’nin 20.12.1988 tarihinde imzaladığı bu sözleşme, TBMM tarafından 22.11.1995 tarihinde 4136 sayılı Kanunla kabul edilmiş ve 25.11.1995 tarihinde 22474 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

⁶⁷⁷ Ünver, **a.g.e.**, s. 304.

⁶⁷⁸ Yılmaz, **a.g.m.**, s. 86.

suçun olası kastla işlenmesi mümkün değildir⁶⁷⁹. Buna göre, suç tanımında buna ilişkin ifadeler yer almadığından, suçtan kaynaklanan malvarlığı değerlerini aklama suçu olası kastla işlenebilen bir suçtur.

2. fıkarda düzenlenen suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçu için tanımda geçen “bilerek” ifadesi, suçun ancak doğrudan kastla işlenebileceğini göstermektedir. Bu nedenle bu suç olası kastla işlenemez⁶⁸⁰.

7. Suç ve Cezaya Etki Eden Nedenler

a. Suçu Ağıraltıran Nedenler

1. fıkarda düzenlenen suçtan kaynaklanan malvarlığı değerlerini aklama suçu ile 2. fıkarda düzenlenen suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçunun nitelikli halleri, aynı maddenin 3. ve 4. fıkalarında düzenlenmiştir.

aa. Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun, kamu görevlisi tarafından veya belli bir meslek sahibi kişi tarafından bu mesleğin icrası sırasında işlenmesi

Maddenin 3. fıkrasında bu suçların kamu görevlisi tarafından işlenmesi veya avukat, muhasebeci veya noter gibi belli bir meslek sahibi kişi tarafından mesleğinin icrası sırasında işlenmesi, verilecek cezayı yarı oranında arttıran suçu ağırlatıcı bir nitelik olarak düzenlenmiştir. Kamu görevlisinin suçun işlenme anında kamu görevliliği statüsünün devam etmesi dışında ek bir koşul getirilmemiştir. Burada failin görevinin sağladığı suçu işleme kolaylığı göz önüne alınmıştır⁶⁸¹.

Kripto para birimi örneğinde, kamu görevlisinin, yasadışı uyuşturucu ticaretinden elde edilen bitcoin’leri, yurtdışından kontrol edilen bir hesaba

⁶⁷⁹ Dülger, **a.g.e.**, s. 275.

⁶⁸⁰ Çakır, **a.g.e.**, s. 364.

⁶⁸¹ Ünver, **a.g.e.**, s. 307.

göndermesi veya kaynağını gizleyecek işlemlere tabi tutması durumunda bu nitelikli hal oluşacaktır.

Belli bir meslek sahibinin mesleğini icra ederken bu suçları işlemesinin ağır nitelikli bir hal olarak düzenlenmesinin nedeni, mesleğin suçların işlenmesine sağladığı kolaylıktır. Doktrinde, bütün mesleklerin değil, sadece bu suçları işleme bakımından kolaylık sağlayan mesleklerin bu kapsamda ele alınması gerektiği ifade edilmiştir⁶⁸².

Kripto para birimi örneğinde, avukatın suçtan kaynaklanan bitcoin'lerin kaynağını gizlemek için çeşitli işlemlere (başkasına göndermesi, müvekkilinden elde etmiş gibi makbuz düzenlemesi, vb.) tabi tutması durumunda bu nitelikli hal oluşacaktır.

bb. Suçtan kaynaklanan malvarlığı değerlerini aklama suçunun, suç işlemek için teşkil edilmiş bir örgütün faaliyeti çerçevesinde işlenmesi

Bu suçlar, bir örgüt kapsamında işlendiği takdirde nitelikli hal oluşacak ve verilecek ceza bir kat arttırılacaktır. Örgüt, en az üç kişinin suç işlemek maksadıyla bir araya gelerek fiili bir birliktelik oluşturmalarıyla kurulmuş olur. Örgütün üye sayısı ve araç ve gereç bakımından suçları işlemeye elverişli olması gerekir (TCK m. 220). Örgütün varlığı için devamlılık şarttır. Suç örgütünün var olması gerekmektedir. Örgütün, suç işlemek amacıyla kurulan örgüt (TCK m. 220) veya silahlı örgütü (TCK m. 314) olması da fark etmemektedir⁶⁸³. Öğretide, suç örgütü faaliyet çerçevesinde aklama suçu işlendiğinde, bu hususun suçun nitelikli hali olarak düzenlenmesinden dolayı, faile madde gerekçesinde belirtildiği gibi hem bu suçtan hem de TCK m. 220'den ceza verilmesi tartışmalıdır. Bazı yazarlar, birleşik suç hükümlerine göre tek bir suçtan cezalandırma yoluna gidilmesi gerektiği öne sürerken⁶⁸⁴ bazı yazarlar da gerçek içtima hükümlerine göre her iki suçtan da ceza verilmesi gerektiğini ifade etmektedir⁶⁸⁵.

⁶⁸² Yılmaz, **a.g.m.**, s. 53.

⁶⁸³ Ünver, **a.g.e.**, s. 308.

⁶⁸⁴ Yılmaz, **a.g.m.**, s. 89.

⁶⁸⁵ Çakır, **a.g.e.**, s. 328; Ünver, **a.g.e.**, s. 308; Dülger, **a.g.e.**, s. 313.

Kanaatimize göre, aklama suçu bir örgüt faaliyeti olarak işlendiğinde faile gerçek içtima hükümlerine göre her iki suçtan ceza verilmelidir. Aksi halde TCK m. 220/4’de düzenlenen “*örgütün faaliyeti çerçevesinde suç işlenmesi halinde, ayrıca bu suçlardan dolayı da cezaya hükmolunur*” hükmü anlamsız kalacaktır.

Kripto para birimi örneğinde, daha önce işlenmiş bir suçtan elde edilen bitcoin’lerin X suç örgütü faaliyeti çerçevesinde işlenmesi durumunda bu nitelikli hal oluşacak, faille her iki suçtan ceza verilecektir.

b. Suçu Hafifleten Nedenler

Suçtan kaynaklanan malvarlığı değerlerinin aklanması suçunda cezayı hafifleten herhangi bir nitelikli hal öngörülmemiştir.

c. Etkin Pişmanlık

Maddenin 6. fıkrasında suçtan kaynaklanan malvarlığı değerlerini aklama suçu ile suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçu için etkin pişmanlık düzenlenmiştir. Buna göre, bu suçlar tamamlandıktan sonra fakat kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek suç konusu malvarlığı değerlerinin ele geçirilmesini sağlamaları veya bulunduğu yeri yetkili makamlara haber vererek ele geçirilmesini kolaylaştırmaları durumunda, haklarında suçtan kaynaklanan malvarlığı değerlerini aklama suçundan cezaya hükmolunmaz.

Aklanan malvarlığı değerinin Bitcoin gibi bir kripto para birimi olduğu suçun faili de, durumu uygun düşükçe etkin pişmanlık hükmünden yararlanabilecektir. Örneğin, uyuşturucu ticareti yaparak elde ettiği bitcoin’leri, kovuşturma başlamadan önce, pişmanlık duyarak, yetkililere teslim eden veya bu paranın bulunduğu hesabı kontrol eden gizli anahtar kodunu yetkililere veren fail, etkin pişmanlıktan yararlanabilecek ve bu suçtan ceza almayacaktır.

8. Suçun Özel Görünüş Şekilleri

a. Teşebbüs

Suçtan kaynaklanan malvarlığı değerlerini aklama suçuna teşebbüs mümkündür⁶⁸⁶. Birinci seçimlik hareket bakımından, suçun faili, malvarlığı değerini yurt dışına aktarırken, elinde olmayan sebeplerle aktarma gerçekleşmezse, suç tamamlanmış olmayacak, teşebbüs hali söz konusu olacaktır. İkinci seçimlik harekette, fail malvarlığı kaynağını gizlemek veya yetkililer üzerinde malvarlığı değerinin meşru bir yoldan elde edildiği kanaatini uyandırmak için çeşitli işlemler gerçekleştirdiği halde, malvarlığı değerinin kaynağının öncül suç olduğu ortaya çıkabilir veya yetkililer bu malvarlığı değerinin meşru olmayan yollardan elde edildiğinin farkına varabilir. Bu durumda da teşebbüs söz konusu olacaktır.

Kripto para örneğinde, suçtan kaynaklanan bitcoin'lerin, yurt dışından kontrol edilen bir hesap aracılığıyla yurt dışına çıkarılmaya çalışırken, paranın başka birisi tarafından transfer edilmesi gibi işlemin failin iradesi dışında kesintiye uğraması durumunda, suç teşebbüs aşamasında kalmış olacaktır.

2. fıkrada düzenlenen suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçu da teşebbüse elverişlidir. Belirli bir neticenin aranmadığı bu suçta satın alma, kabul etme, bulundurma ve kullanma, failin elinde olmadan belli bir aşamada kesilmiş olabilir. Bu durumda teşebbüs söz konusu olacaktır⁶⁸⁷.

Kripto para örneğinde, failin suçtan kaynaklandığını bildiği kripto para birimini hesabına geçirmeye çalışırken, internet bağlantısının kesilmesi gibi işlemin kendi iradesi dışında kesintiye uğraması durumunda, suç teşebbüs aşamasında kalmış olacaktır.

⁶⁸⁶ Dülger, **a.g.e.**, s. 307.

⁶⁸⁷ Çakır, **a.g.e.**, s. 368.

b. İçtima

Suçtan kaynaklanan malvarlığı değerlerini aklama suçu için farklı bir içtima durumu öngörülmemiş olup, suçların içtima bölümünde (TCK m. 42-44) yer alan hükümler uygulanacaktır. Örneğin fail, suç fiilini oluşturan seçimlik hareketlerin ikisini birden işlese de tek bir suç oluşacaktır. Aklama suçu ile malvarlığı değerinin elde edildiği öncül suçun faili aynı olduğunda, her iki suç bağımsız suç olarak düzenlendiğinden ayrı ayrı cezalandırılmaları gerekir⁶⁸⁸.

Bu suçun zincirleme suç olarak işlenmesi mümkündür. Bir suç işleme icrası kapsamında, suçtan elde edilen malvarlığı değerini aklamak amacıyla, suç tanımında yer alan seçimlik hareketleri değişik zamanlarda ayrı ayrı gerçekleştiren fail hakkında zincirleme suç hükümleri uygulanacaktır⁶⁸⁹. Örneğin suçtan elde edilen bitcoin'lerin, dikkat çekmemek için değişik zamanlarda yurtdışından kontrol edilen hesaba transfer edilmesi durumunda, zincirleme suça ilişkin hükümler uygulanacaktır.

İkinci fıkrada düzenlenen suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçu ile aklama suçunun faili aynı olamayacaklardır. Aksi halde fail, aklama suçundan sorumlu tutulacaktır. Bunun dışında, malvarlığı değerini kabul etmek ve kullanmak şeklinde, suç tanımında belirtilen iki veya daha fazla hareket birlikte işlendiği takdirde tek bir suç oluşacaktır.

c. İştirak

Maddede düzenlenen her iki suç iştirak bakımından bir özellik göstermemektedir ve bu nedenle müşterek faillik, azmettirme ve yardım etme şeklinde bu suçlara her türlü iştirak söz konusu olabilir.

9. Yaptırım

⁶⁸⁸ Yılmaz, **a.g.m.**, s. 88.

⁶⁸⁹ Çakır, **a.g.e.**, s. 325.

Maddenin 1. fıkrasında düzenlenen daha önce işlenmiş bir suçtan kaynaklanan malvarlığı değerini yurtdışına çıkaran veya bunların gayrimeşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla, çeşitli işlemlere tâbi tutan failin cezası, üç yıldan yedi yıla kadar hapis ve yirmibin güne kadar adli para cezasıdır (TCK m. 282/1).

2. fıkroda düzenlenen, suçtan kaynaklanan malvarlığı değerini suçunun işlenmesine iştirak etmeksizin, bu suçun konusunu oluşturan malvarlığı değerini, bu özelliğini bilerek satın alan, kabul eden, bulunduran veya kullanan kişinin cezası, iki yıldan beş yıla kadar hapis cezasıdır (TCK m. 282/2).

3. fıkraya göre düzenlenen nitelikli hale göre, 1. ve 2. fıkralarda düzenlenen suçların kamu görevlisi tarafından veya belli bir meslek sahibi kişi tarafından bu mesleğin icrası sırasında işlenmesi halinde, verilecek hapis cezası yarı oranında artırılacaktır (TCK m. 282/3).

Suçtan kaynaklanan malvarlığı değerini aklama suçu, bir suç örgütü faaliyeti olarak işlendiğinden faillere verilecek ceza bir kat artırılır (TCK m. 282/4).

Suçtan kaynaklanan malvarlığı değerini aklama suçu, tüzel kişi yararına işlenmişse, bu tüzel kişi hakkında, tüzel kişilere özgü güvenlik tedbirlerine (izin iptali, eşya veya kazanç müsaderesi) hükmolunur (TCK m. 282/5).

10. Muhakemeye İlişkin Kurallar

Suçtan kaynaklanan malvarlığı değerlerini aklama ile suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçları, soruşturma makamlarınca re'sen takip edilir.

Suçtan kaynaklanan malvarlığı değerlerini aklama ile suçtan kaynaklanan malvarlığı değerini bilerek satın alma, kabul etme, bulundurma ve kullanma suçlarını kovuşturmakla görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. maddesi uyarınca, asliye ceza mahkemesidir.



§2. Kripto Para Birimlerinin Suç Konusu Olduğu Suçların Soruşturulması ve Kovuşturulmasının Zorlukları

Kripto para birimleri, bilişim sistemleri üzerinde veri olarak bulunur ve işlem görürler. Bu sistem ve verilerin hukuka aykırı eylemlere maruz kalmaları yukarıda açıklanan suçların oluşumuna sebep olur. Bu suçların soruşturmaları ve kovuşturmaları, diğer suçlara göre daha zordur. Bunun iki nedeni olduğu söylenebilir; ilki, verilerin dijital delil olarak ortaya koyduğu zorluklardır. İkinci neden ise kripto para birimi sistemlerinin kendine özgü yapılarından kaynaklanmaktadır.

Dijital deliller, fiziksel yapıda olmalarından dolayı maddi yapıdaki nesnelerin özelliklerine sahip olmakla birlikte, kendine özgü niteliklere de sahiptirler⁶⁹⁰:

Dijital deliller hassastır, başka bir deyişle kolayca değiştirilebilir, bozulabilir veya yok edilebilirler. Dijital verilerin elde edilmesi, toplanması, korunması adli bilişim tekniklerini kullanmayı gerektirir.

Dijital deliller kolayca kopyalanabilir veya çoğaltılabilir. Bundan dolayı orijinalliklerinin ve aidiyetlerinin tespiti uzmanlık gerektirir. Sahte dijital delillerin kolayca oluşturulabilmeleri, bunların dikkatli incelemelere ve doğrulamalara tabi tutulmalarını gerektirir.

Dijital deliller, doğrudan anlaşılamayan ve tespit edilmeleri için uygun araç ve uzmanlık gerektiren gizli yapılara sahiptirler. Dijital delilleri, tabii halleriyle görmemiz mümkün değildir. Bunun için uygun donanımlara ve yazılımlara ihtiyaç vardır.

Dijital delillere tek başına el konulamaz ve elde edilebilmeleri bulundukları cihazlara erişimin sağlanmasıyla mümkündür. Dijital delilin bulunduğu araç veya ortam, her zaman el koyma işlemine uygun olmayabilir. Örneğin yurt dışında bulunan bir bilişim sistemindeki delile el koymak için ilgili bilişim cihazına el koymak veya bu sisteme erişim sağlamak her zaman mümkün olmayabilir.

⁶⁹⁰ Değirmenci, **a.g.e.**, s. 132-136.

Dijital deliller, farklı hukuk ve yargılama yetkisine sahip ülkelere kolayca yayılabilme niteliğine sahiptirler. Örneğin Ukrayna’da bir grup bilgisayar korsanı, Kanada’da bulunan bir bilgisayar sunucusunu kullanarak Türkiye’deki bir bankaya siber saldırı düzenleyebilir ve bu suça ait veriler, bu ülkelerle beraber başka yerlere de dağılmış olabilir.

Dijital deliller, uçucu/geçici nitelikte olabilirler. Dijital aletin geçici bellek alanında tutulan bilgiler, bir ortama kaydedilmiş olmadıkça kaybolabilirler. Mesela kaydedilmemiş bir doküman, bilgisayarın elektriği kesilirse, bir daha ele geçmeyebilir. Bu nedenle açık veya kapalı bilgisayarlarda delil incelemesi ancak bilişim uzmanlarınca yapılmalıdır.

Dijital delillerin bütünlüğü de karmaşıklık arz eder. Uçucu/geçici niteliklerinden dolayı sürekli değişim gösterebilir, farkında olmadan değiştirilmiş olabilir ve inceleme esnasında bütünlüklerine istenmeden zarar verilebilir. Bunun için de ancak adli bilişim konusunda uzman olan kişilerce bu deliller incelenmelidir.

Kripto para birimlerinin işleyişleri göz önüne alındığında bu paraların suç konusunu oluşturduğu suçların araştırılmasında, birtakım yeni zorlukların ortaya çıkması mümkündür.

Bu suçlar, bilişim sistemleri kullanılarak işlenen suçlar oldukları için soruşturulmaları, klasik soruşturma teknikleri yerine daha uzmanlık gerektiren adli bilişim tekniklerinin yoğun kullanımını gerektirecektir.

Kripto para birimleri, merkezî olmayan yapılar olduğu için, soruşturma ve kovuşturma makamları, ihtiyaç duydukları belge ve bilgileri talep edebilecekleri bir muhatap bulmakta zorlanacaklardır. Örneğin, Bitcoin, isteyen herkesin belirsiz (anonim) kimliklerle işlem yapabildiği, merkezî bir yönetim ve denetim biriminin olmadığı bir sistemdir. Yasadışı bir işlem söz konusu olduğunda, olayda kullanılan Bitcoin adresinin kime ait olduğunu tespiti için işbirliği talep edilecek bir yetkili bulunamaz.

Kripto para birimlerinin merkezî olmayan yapıları, bilişim sistemlerinin kolaylaştırdığı sınıraşan suç olgusunu daha da içinden çıkılmaz bir duruma dönüştürme kapasitesine sahiptir. Mesela Bitcoin, dünyanın internete erişilebilen her yerinde işlem gören bir kripto para birimidir. Böyle bir durum, farklı yargılama yetkisine tabi birden fazla alanı işin içine katmaktadır. Bu tür uluslararası işbirliğini gerektiren olayların hızlı bir şekilde soruşturulmaları ve kovuşturulmaları pek mümkün gözükmemektedir.

Bankalar ve finansal kuruluşlar, tabi oldukları yasal zorunluluklardan dolayı, şüpheli işlemleri yetkili mercilere (MASAK gibi) bildirmek zorundadırlar. Böyle bir zorunluluk, kripto para birimi sistemleri için, ilgili merkezî yapının yokluğundan dolayı mümkün gözükmemektedir. Ayrıca bu sistemlerde para hareketleri, aracı kuruluşlar olmaksızın doğrudan taraflar arasında gerçekleştiğinden, yasadışı işlemlerin ortaya çıkarılması zorlaşmaktadır.

Kripto para birimi sistemleri, para hareketi işlemlerinin geri alınması, müsadere veya el koyma bakımından da zorluk arz ederler. Bütün para hareketleri, işlemin taraflarınca bilinen ve kontrol edilen gizli anahtarla gerçekleştirildiğinden, bir hesaptaki paraya el konulması, ancak ilgili gizli anahtarın bilinmesiyle mümkündür. Bu nedenle işbirliği yapmayan veya bulunamayan failin söz konusu olduğu durumlarda, el koyma veya işlemin geri alınması mümkün değildir.

Kripto para birimleri sağladıkları belirsiz kimlikle işlem yapabilme özelliği (anonimlik), suç şüphelilerinin ortaya çıkarılmasını zorlaştıran bir faktördür. Bir kişinin sisteme kaydolması için herhangi bir kimlik ibraz etmesine gerek yoktur. Kişilerin hesap numaraları, ilgili kişiyle ilgili herhangi bir belirlenim içermeyen, harf ve rakamlardan oluşan uzun bir diziden oluşmaktadır. Bütün para hareketleri bu hesaplar arasında gerçekleşmektedir. Bunun yanında bazı kripto para birimi sistemleri (zCash, Monero gibi), tam anonimlik sağladıklarını iddia etmektedir. Bu sistemlerde işlemi sadece taraflar görebilmekte, üçüncü kişiler yapılan işlemi dışarıdan inceleyememektedir. Yine şüpheli işlemleri gizlemek için üçüncü kişiler tarafından sunulan karıştırıcı (*mixer*) hizmeti kullanılarak, para hareketlerinin izlenmesi daha da zorlaştırılabilmektedir.

SONUÇ

Bu çalışmada, bilişim teknolojisinin en son yeniliklerinden biri olan kripto para birimleri incelenmiştir. Para birimi, ödeme sistemi ve emtia olarak bütünleşik bir yapı sunan bu sistemler, hukuk, ekonomi, finans ve diğer alanlardaki yapı ve düzenlemelerde değişimi zorlayan özellikler göstermektedir.

Kripto para birimlerinin, günlük hayatta ve ticari faaliyetler çerçevesinde, gerçek ve sanal mal ve hizmet alımlarında ödeme aracı olarak kullanıldıkları, dünya çapında birçok şirket tarafından kabul edildikleri, yüzlerce takas ve borsa merkezlerinde işlem gördükleri, tedavülde olan ülke paralarıyla çift yönlü konvertibiliteye sahip oldukları ve toplamda 700 milyar ABD dolarına kadar büyüyen pazar büyüklüğüne eriştikleri göz önüne alındığında işin mahiyeti ve önemi kendini hissettirmektedir.

Kripto para birimi sistemlerinin, Blokzinciri (Blockchain) teknolojisinin sadece bir ürünü olduğunu ve bu teknolojinin çok büyük bir potansiyele sahip olduğu iddia eden uzmanlar, çok uzak olmayan bir gelecekte hukuki kişilik, hukuki sorumluluk ve bireysel temsil gibi mevcut hukuki kavramları da gözden geçirmeye neden olacak, kendi kendini ifa edebilen akıllı sözleşmeler ve akıllı mülklerin gündeme geleceğini öne sürmektedirler. Değişim bunlarla sınırlı kalmayacak, merkezi bir idare olmaksızın herkesin erişimine ve denetimine açık ortak siciller oluşacak ve Devletin yürüttüğü bütün hizmetler, bu teknolojiye dayanan yeni kurumlara geçecektir.

Günümüzde neredeyse her gün yeni bir kripto para birimi duyurusunun yapılmasına rağmen bu sistemlerin mevcut kurum ve yapılarla ilişkisini ve konumu belirleyecek hukuksal düzenlemeler henüz ortaya çıkmamıştır. Bu nedenle çalışmamızda bu hususlar göz önüne alınarak, kripto para birimlerinin hukuk dünyasında, özellikle ceza hukuku boyutu açısından, belirsizliğinin giderilmesi, mahiyetinin anlaşılması ve mevcut düzenlemelere ilişkilerinin ortaya çıkarılmasına gayret edilmiştir.

Kripto para birimleri, bilişim sistemlerine dayanan karmaşık yapı ve işleyişlere sahiptirler. Daha önce bilinmeyen kavramlar, bu sistemler aracılığıyla gündeme

gelmiştir. Hukuki belirsizliğin giderilmesine katkısı olacağı düşünüldüğünden, ilk kripto para birimi olan ve kripto para birimlerine ilişkin pazarın yaklaşık %40'ına hâkim olan Bitcoin sistemi ele alınmış ve onun üzerinden konunun teknik boyutuyla incelenmesi yapılmıştır.

Çalışmada, kripto para birimleri ile ilgili ulusal, bölgesel ve uluslararası kurum ve kuruluşlar ile bireysel yazarlar tarafından hazırlanan kaynaklardan oluşan kitaplar, bilimsel makaleler, çalışma raporları, bilgi notları, konferans ve sempozyum notları incelenmiş ve konunun hukuki ve teknik yönden anlaşılması için farklı görüşlere yer vermeye özen gösterilmiştir.

Çalışma, temelde iki bölümden oluşmuştur. İlk bölümde, kripto para birimi kavramının anlaşılması ile hukuki ve teknik yönlerinin ortaya çıkarılması amaçlanmıştır. İkinci bölümde ise ceza hukuk bağlamında bu para birimlerinin hukuksal durumu ele alınmıştır. Bunun yanında Türk Ceza Kanunu'nda düzenlenen bazı suçlar bakımından kripto para birimlerin değerlendirmesi ile bunların suç konusu olduğu suçlara ilişkin soruşturma ve kovuşturmalarda karşılaşılabilecek zorluklar ele alınmıştır.

Çalışmanın ilk bölümü, kripto para birimi kavramı için bir tanım arayışı ile başlamaktadır. Bu amaçla konuyla ilgili yayımlanan ulusal ve uluslararası çalışmalara ait rapor ve bilgi notları, değişik yazarların kitapları ve bilimsel makaleleri incelenmiştir. Kripto para birimleri, geleneksel para birimi ve onun dijital uzantısı elektronik para ile yakın bir ilişki içinde olduklarından, kavramların bazen yersiz olarak birbirini yerine kullandığı görülmektedir. Bunun yanında, kripto para birimleri sanal para birimi olarak farklı sanal para birimleriyle aynı kategoride değerlendirilmektedir. Konunun iyi anlaşılması amacıyla bu kavramlar arasında ilişkiler ile benzerlik ve farklılıklar ortaya konmaya çalışılmıştır.

Kripto para birimi için üzerinde herkesin uzlaşabileceği ortak bir tanımın ortaya konması zor gözükmektedir. İncelemede de görüldüğü gibi, bu para birimine ilişkin çeşitli tanım önerileri bulunmaktadır. Kanaatimize göre, kripto para birimi, paranın ihracında ve dolaşımında başta kriptografik teknikler olmak üzere bilişim teknolojilerinin kullanıldığı, herhangi bir merkezî yapının yönetiminde ve

denetiminde olmayan, ulusal paralara alternatif dijital para birimi olarak tanımlanabilir.

Bu para birimlerinin, diğer benzer kavramlardan farkı kısaca şöyle özetlenebilir: Kripto para birimi, elektronik para değildir, çünkü yasal ödeme aracı olan itibari para ile ilişkili değildir; kripto para birimi, diğer sanal para birimlerinden de ayrılır, çünkü, hem sanal hem de reel ekonomiyle ilişkilidir.

Kripto para birimleri, bilişim teknolojisindeki gelişimler dizisinin sonucudur. Birinci bölümün ikinci ayrımında, bu sistemlerin ortaya çıkmalarına öncülük eden kişiler, gruplar, teknolojik gelişmeler ele alınmış, konuyla ilgili tarihi bir perspektif oluşturulmaya çalışılmıştır. Gerçekten de kripto para birimleri, temeli 1980’lerde atılan bir yenilik olarak anlaşılmalıdır.

Kripto para birimi sistemleri, hâlâ gelişim evrelerinde olmalarından dolayı, hepsini birden niteleyebilecek özellikleri ortaya çıkarmak kolay değildir. Birinci bölümün üçüncü ayrımı, bu ortak özelliklerin araştırılmasına ayrılmıştır. Mevcut duruma göre, açık kaynak kodlu olmak, anonimlik, merkezsizlik ve kriptografik tekniklerden yararlanmak, bütün bu para birimleri için geçerli ortak özellikleri ifade etmektedir. Bunlarla ilgili olarak, bir hukukçunun bilmesinin faydalı olacağı düşünülen hususlar açıklanmıştır.

Kripto para birimine ilişkin kavramsal açıklamalardan sonra konuyla ilgili hukuksal düzenleme arayışları ele alınmıştır. Bu arayışlarının temelinde, bu teknolojik yeniliğin hem ulusal hem de uluslararası boyutta yarattığı etkilerin toplumsal, siyasal, ekonomik ve finansal hayata sağlıklı yansımaları sağlama ve kötüye kullanımına engel olma düşüncesi yatmaktadır. Bunun yanında, kripto para birimleri, suç faaliyetlerinden başka, başta vergilendirme olmak üzere, ekonomik ve mali politikalara yönelik hükümet politikalarının uygulama kapsamı dışında kaldıkları için ulusal egemenliğe birer tehdit oluşturabilecek potansiyele sahiptirler. Gerçekten de bazı yazarlar, kripto para birimlerinin vergi cenneti olmaya doğru evrildiklerini öne sürmüşlerdir.

Kripto para birimleriyle ilgili hukuksal düzenleme arayışlarında iki önemli zorluk dikkati çekmektedir. Bunların ilki, bu sistemlerin kullandığı blokzincirini ve

benzeri yapıların vadettiği teknolojik yenilik alanının gelişimini sekteye uğratacak sınırlamalar yerine, sağlıklı bir yol izlenebilmesini sağlayacak kurallar ortaya koymak çok da kolay gözükmemektedir. İkinci olarak, uygulama alanı olarak küresel genişliğine sahip, merkezî olmayan, herhangi bir otoriteye bağlı olmayan ve kullanıcıların anonim olarak katılabildikleri bu sistemlerin birçok yargılama yetkisine dağılmış olmaları dolayısıyla yükümlülük altına alınacak muhatap bulmak çok da kolay gözükmemektedir. Fakat bu belirsizlik, bu sistemlerin gelişimini de olumsuz etkilemektedir.

Kripto para birimleri için sert ve yasaklayıcı kuralların teknolojik gelişimi sekteye uğratacağı ve bu sistemlerin yasal kullanımını kısıtlayacağı fakat yasadışı kullanımı çok fazla engellemeyeceği belirtilmiştir.

Kripto para birimlerinin hukuk dünyasında konumunun belirlenmesi açısından belki de en önemli adım olan üzerinde uzlaşmış ortak bir hukuksal tanım henüz ortaya çıkmamıştır. Bu belirsizlik, geleneksel olarak ayrı yapılar olarak ortaya çıkan para birimi, emtia ve ödeme sistemlerinin kripto para birimi sistemlerinde birbiriyle entegreli olarak bir arada bulunmalarından kaynaklanmaktadır.

Bazı yazarlar, ortaçağda ticari faaliyetlerin çoğalmasıyla tüccarlar arasında uylaşım sonucu ortaya çıkan ticaret örf ve âdet hukuku, *Lex Mercatoria* gibi kripto para birimlerinin dayandığı blokzinciri teknolojisinin, akıllı sözleşmeler, akıllı mülkler ve merkezî olmayan özerk organizasyonlar aracılığıyla, mevcut hukuksal düzeni değiştireceği ve *Lex Cryptographia* adında yeni bir hukuk alanı oluşturacağını ileri sürmektedirler.

Çalışmanın bu kısmında, FATF, UNODC, IMF ve OECD, EBA ve ECB gibi uluslararası ve bölgesel kuruluşların çalışmalarına yer verilmiş ve ABD, Almanya, Çin, Japonya, İngiltere, Rusya ve Türkiye’de kripto para ile ilgili hukuksal durum ve düzenlemelere değinilmiştir. Kripto para birimlerine ilişkin hukuksal belirsizliğin neredeyse bütün ülkelerde sürdüğünü anlaşılmaktadır.

Birinci bölümün beşinci ayrımında, kripto para birimleri, ceza hukuku bakımından incelenmiştir. Bu doğrultuda, bu paraların elektronik para, emtia veya

menkul değer olup olmadıkları araştırılmış ve her üç değer kategorisine tam anlamıyla uymadıkları belirlenmiştir. Uluslararası ve ulusal kurum ve kuruluşların tanımlamalarına göre, kripto para birimlerinin alternatif para birimi olarak ekonomik değer taşıyıcı işlevi gördükleri ve ceza hukuku bağlamında gerçek paraya alternatif para birimi olarak ele alınmaları önerilmiştir.

Kripto para birimlerinin, mevcut mevzuata göre kullanımlarının yasallığı ile ilgili olarak, doktrinde az da olsa açıklanan görüşler değerlendirilmiş ve bu para birimlerinin kullanımlarının ne yasaklayan ne de yasal olduğu belirleyen düzenlemelerin olmadığını saptanmıştır. Buna göre, suçta ve cezada kanunilik ilkesi gereğince kanunla açıkça yasaklanmamış kripto para birimi kullanımının serbest olduğu görüşü belirtilmiştir.

Bölümün son ayrımında, kripto para birimlerine ilişkin teknik kavrayışın pekişmesi amacıyla, Bitcoin örneği üzerinden bu sistemlerin teknik yapısı ve işleyiş mekanizmaları ele alınmıştır. Bitcoin etrafında oluşan ekosistem ile bu sistem aracılığıyla gerçekleşen para arzı, para transferleri, madencilik faaliyetleri, cüzdan, blokzinciri ve daha birçok teknik yapı ve kavram, anlaşılır bir düzeyde açıklanmaya çalışılmıştır. Bunun yanında, diğer kripto para birimleri ile ileride gerçekleştirebileceği öngörülen uygulamalardan örnekler verilerek, konuyla ilgili bir gelecek perspektifi oluşturulmaya çalışılmıştır.

İkinci bölüm iki ayrımdan oluşmaktadır. İlk ayrımda, kripto para biriminin suç konusu olabileceği Türk Ceza Kanunu'nda düzenlenen bazı suçlar bakımından değerlendirmeler yer almaktadır. Malvarlığına karşı suçlar, bilişim alanında suçlar ve adliyeye karşı suçlar bölümlerinde yer alan bu suçlar, klasik suç incelemesi usulüne uygun olarak kripto para birimi odaklı incelenmiştir. Buna göre, bilişim sistemlerinde kripto para birimini temsil eden verilere karşı malvarlığına karşı işlenen hırsızlık, yağma, dolandırıcılık ve güveni kötüye kullanma suçlarının işlenmesi mümkündür. Yargıtay'ın da aynı doğrultuda içtihadta bulunduğu bir husus olarak, bu suç fiillerinde suç konusu bilişim verisi değil, bu verilerin temsil ettiği hesaptaki paralardır.

Bu ayırmda biliřim sistemleri ve verilerine karřı iřlenen suçlar ile suçtan kaynaklanan malvarlıęı deęerlerini aklama suçları da ele alınmıřtır.

İkinci bölümün son ayırımında, kripto para birimleriyle ilgili suçların arařtırılmasının zorluklarına deęinilmiř ve bunların sebepleri gösterilmiřtir. Bu zorlukların bir kısmı bu para birimlerinin yapı ve iřleyiřlerinden kaynaklanmaktadır. Dijital delillere özgü nitelikler de bu suçların soruřturulmaları ve kovuřturulmalarını zorlařtıracak faktörler içermektedir.

Bu çalıřmayla kripto para birimleriyle ilgili olarak belli bir bilgi daęarcıęı ortaya konulmaya çalıřılmıřtır. Fakat kripto para birimleriyle ilgili henüz içtihatlar oluřmamıřtır. Doktrinde de yeteri kadar tartıřılmamıřtır. Bu yüzden konu hukuki açıdan sınırlı olarak incelenebilmiřtir.

Kripto para birimleri, hayatın deęiřik alanlarına nüfuz ettikçe, bu iliřkilerin hukuk dünyasına yansıması da söz konusu olacaktır. Konuyla ilgili ortaya çıkacak içtihat ve tartıřmalar, kripto para birimlerinin hukuksal konumunu belirlemeye yardım edeceęi gibi gerekli hukuksal düzenlemelerin oluřumu için de bir birikim saęlayacaktır.

KAYNAKÇA

ABD Hazine Bakanlığı Mali Suçlarla Mücadele Birimi (Department of Treasury Financial Crimes Enforcement Network, FinCEN), **Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies**, 2013, <https://www.fincen.gov/sites/default/files/guidance/FIN-2013-G001.pdf>, Erişim tarihi: Erişim tarihi: 17 Mart 2018.

An Roinn Airgeadais (Department of Finance), **Virtual Currencies and Blockchain Technology**, Dublin: 2018, <http://www.finance.gov.ie/wp-content/uploads/2018/03/Virtual-Currencies-and-Blockchain-Technology-March-2018.pdf>, Erişim tarihi: 17 Mayıs 2018.

Antonopoulos, Andreas M., **Mastering Bitcoin Programming The Open Blockchain**, 2. b., ABD: O'Reilly, 2017.

Artuk, Mehmet Emin, Gökçen, Ahmet, Yenidünya, Ahmet Caner, **Ceza Hukuku Özel Hükümler**, 15. b., Ankara: Adalet Yayınevi, 2015.

Aydın, Nurullah, **Türk Suç ve Ceza Hukuku**, 2. b., Ankara: Adalet Yayınevi, 2009.

Back, Adam, **Hashcash - A Denial of Service Counter-Measure**, 2002, <http://www.hashcash.org/papers/hashcash.pdf>, Erişim tarihi: 23 Mayıs 2018.

Barski, Conrad, Wilmer, Chris, **Bitcoin For The Befuddled**, San Francisco: no starch press, 2015.

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), **Basın Açıklaması**, https://www.bddk.org.tr/websitesi/turkce/duyurular/Basin_Aciklamalari/12574bitcoin_hk_basin_aciklamasi.pdf, Erişim tarihi: 17 Mayıs 2018.

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

Blundell-Wignall, Adrian, **The Bitcoin Question: Currency versus Trust-less Transfer Technology**, 2014, OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing, <http://dx.doi.org/10.1787/5jz2pwjd9t20-en>, Erişim tarihi: 10 Mayıs 2018.

Boehm Franziska, Pecschi, Paulina, **Bitcoin: A First Legal Analysis -with reference to German and US-American law-** https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf, Erişim tarihi: 26 Ağustos 2018.

Brito, Jerry, Castillo, Andrea **Bitcoin: A Primer for Policymakers**, ABD: Mercatus Center, 2013.

Buterin, Vitalik, **A Next-Generation Smart Contract and Decentralized Application Platform**, <https://github.com/ethereum/wiki/wiki/White-Paper>, Erişim tarihi: 24 Nisan 2018.

Centel, Nur, Zafer, Hamide, Çakmut, Özlem, **Kişilere Karşı İşlenen Suçlar**, C. I, 4. b., İstanbul: Beta, 2017.

Conti, Mauro, Kumar E, Sandeep, Lal, Chhagan, Ruj, Sushmita, **A Survey on Security and Privacy Issues of Bitcoin**, <https://arxiv.org/abs/1706.00916>, Eriřim tarihi: 24 Nisan 2018.

Chaum, David, **Blind Signatures For Untraceable Payments**, <https://chaum.com/publications/Chaum-blind-signatures.PDF>, Eriřim tarihi: 20 Mart 2018.

Chuen, David Lee Kuo (Editör), **Handbook of Digital Currency**, ABD: Elsevier, 2015.

Çakır, Kerim, **Suçtan Kaynaklanan Malvarlığı Deęerlerini Aklama Suçu**, Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul, 2016.

Dai, Wei, **B-Money, An Anonymous, Distributed Electronic Cash System**, <http://www.weidai.com/bmoney.txt>, Eriřim tarihi: 21 Mart 2018.

Dale, Oliver, **A History of Cryptography and the Rise of the CypherPunks**, <https://blockonomi.com/cryptography-cypherpunks/>, Eriřim tarihi: 26 Mart 2018.

De Filippi, Primavera, "Bitcoin: a regulatory nightmare to a libertarian dream", **Internet Policy Review**, C. 3/2, 2014.

Deęirmenci, Olgun, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, 1.b., Ankara: Seçkin Yayıncılık, 2014.

Donet Donet, Joan Antoni, Perez-Sola, Cristina, Herrera-Joancomarti Jordi, “**The Bitcoin P2P Network**”, Financial Cryptography and Data Security, FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers, Editörler: Rainer Böhme, Michael Brenner, Tyler Moore, Matthew Smith, Springer, 2014.

Dönmezer, Sulhi, **Kişilere ve Mala Karşı Cürümler**, 17. b., İstanbul: Beta Yayıncılık, 2004.

Dölger, Murat Volkan, **Biliřim Suçları ve İnternet İletişim Hukuku**, 5. b., Ankara: Seçkin Yayıncılık, 2014.

Dölger, Murat Volkan, **Suçtan Kaynaklanan Malvarlığı Deęerlerinin Aklanmasına İliřkin Suçlar ve Yaptırımlar**, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul, 2010.

Erdoğan, Yavuz, **Türk Ceza Kanunu’nda Biliřim Suçları**, 1. b., İstanbul: Legal, 2013.

Europe Banking Authority (EBA), **EBA Opinion On ‘Virtual Currencies’**, 04.07.2014, <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>, Eriřim tarihi: 17 Mart 2018.

Europe Banking Authority (EBA), **Warning to consumers on virtual currencies**, <https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf>, Eriřim tarihi: 14 Mayıs 2018.

European Central Bank (ECB), **Virtual Currency Schemes**, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, Eriřim tarihi: 15 Mart 2018.

European Central Bank (ECB), **Virtual Currency Schemes – A Further Analysis**, 2015, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, Erişim tarihi: 12 Mart 2018.

Farell, Ryan, An Analysis of the Cryptocurrency Industry, **Wharton Research Scholars.130.**, 2015, http://repository.upenn.edu/wharton_research_scholars/130, Erişim tarihi: 6 Mayıs 2018.

Finney, Hal, **RPOW - Reusable Proofs of Work** <http://nakamotoinstitute.org/finney/rpow/index.html>, Erişim tarihi: 25 Mart 2018.

Franco, Pedro, **Understanding Bitcoin Cryptograpy, engineering, and economics**, İngiltere: Wiley, 2015.

Financial Action Task Force (FATF), **Virtual Currencies - Key Definitions and Potential AML/CFT Risks**, Haziran 2014, s. 4, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, Erişim tarihi: 16 Mart 2018.

Financial Action Task Force (FATF), **Guidance For A Risk-Based Approach Virtual Currencies**, 2015, <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>, Erişim tarihi: 10 Mayıs 2018.

Grinberg, Reuben, "Bitcoin: An Innovative Alternative Digital Currency", **Hastings Science & Technology Law Journal**, C. IV, 2011, s. 160-208.

Halaburda, Hanna, Sarvary, Miklos, **Beyond Bitcoin, The Economics of Digital Currencies**, Palgrave Macmillan, 2016.

Hughes, Eric, **A Cypherpunk's Manifesto**, <https://www.activism.net/cypherpunk/manifesto.html>, Erişim tarihi: 21 Mart 2018.

International Monetary Fund (IMF), **Virtual Currencies and Beyond**, 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, Erişim tarihi: 14 Mart 2018.

İnceoğlu, Asuman Aytekin, "Güveni Kötüye Kullanma Suçu", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi (GÜHFD)**, C. 2018/1, 2018, s. 41-85.

Kaplanov, Nikolei M., "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation", **Loyola Consumer Law Review**, 2012, C.25/1, s. 111-174.

Karagülmez, Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 5. b., Ankara: Seçkin Yayıncılık, 2014.

King, Sunny, Nadal, Scott, **PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake**, 2012, <https://peercoin.net/assets/paper/peercoin-paper.pdf>, Erişim tarihi: 24 Nisan 2018.

Koca, Mahmut, Üzülmüş İlhan, **Türk Ceza Hukuku - Özel Hükümler**, 3. b., Ankara: Adalet Yayınları, 2016.

Kocasakal, Ümit, **Karapara Aklama Suçu**, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul, 2000.

Lamport, Leslie, Shostak, Robert, Pease, Marshall, “The Byzantine Generals Problem”, **ACM Transactions on Programming Languages and Systems (TOPLAS)**, C.4/3, Temmuz 1982, s. 382-401, <http://lamport.azurewebsites.net/pubs/byz.pdf>, Erişim tarihi: 30 Mart 2018.

Lipkis, Sarah, Roth, Amanda, “Anatomy: What is Alternative Currency”, **World Policy Journal**, Yaz 2014, C.XXXI, 2014, s. 12-13, https://worldpolicy.org/wp-content/uploads/2014/06/Summer14_12-13_Anatomy_0.pdf, Erişim tarihi: 19 Mart 2018.

Mahmutoğlu, Fatih Selami, “Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası (İÜHF)**, C.LXXI(1), 2013, s. 855-889.

Marian, Omri, "Kripto Para Birimi Üstün Vergi Cenneti Mi?", Çeviren: Sedef Pelin Gürlek Keleş, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası (İÜHF)**, C. LXXIV/2, 2016, s.919-930.

Martin, Keith M., **Everyday Cryptography**, 2. b., İngiltere: Oxford University Press, 2017.

Mukhopadhyay, Ujan, Skjellum, Anthony, Hambolu, Oluwakemi, Oakley, Jon, Yu, Lu, Brooks, Richard, “A Brief Survey of Cryptocurrency Systems” **2016 14th Annual Conference on Privacy, Security and Trust (PST)**, 2016, s. 745-752. <http://ieeexplore.ieee.org/document/7906988>, Erişim tarihi: 20 Mart 2018.

Mullan, P. Carl, **A History of Digital Currency in the United States**, Whitestone, Virginia: Palgrave Macmillan, 2016.

Nakamoto, Satoshi, **Bitcoin: A Peer-to-Peer Electronic Cash System**, <https://bitcoin.org/bitcoin.pdf>, Erişim tarihi: 3 Nisan 2018.

Narayanan, Arvind, Bonneau, Joseph, Felten, Edward, Miller, Andrew, Goldfeder, Steven, **Bitcoin and Cryptocurrency Technologies**, Princeton University Press, 2016.

Oğuzman, M. Kemal, Seliçi, Özer, Oktay-Özdemir, Saibe, **Eşya Hukuku**, 19. b., İstanbul: Filiz Kitabevi, 2016.

Özbek, Veli Özer, “Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. 9/Özel Sayı, 2007, s. 1019-1063.

Özbek, Veli Özer, Koray Doğan, “Zorunluluk Halinin (TCK m. 25/2) Hukuki Niteliği”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. 9/2, 2007, s. 195-222.

Özbek, Veli Özer, Kanbur, M. Nihat, Doğan, Koray, Bacaksız, Pınar, Tepe, İlker, **Türk Ceza Hukuku Özel Hükümler**, 12. b., Ankara: Seçkin Yayıncılık, 2017.

Oxford Sözlüğü, <https://en.oxforddictionaries.com/definition/cryptocurrency>, Erişim tarihi: 12 Mart 2018.

Parlar, Ali, **Türk Ceza Hukukunda Bilişim Suçları**, 1. b., Ankara: Bilge Basım Yayın, 2011.

Parlar, Ali, **Türk Ceza Hukukunda Dolandırıcılık Suçları**, 1. b., Ankara: Bilge Basım Yayım, 2011.

Peck, Morgen E., “Cryptoanarchists’ Answer to Cash”, **IEEE Spectrum**, C.49/6, s. 51-56, Haziran 2012.

Pisa, Michael, Juden, Matt, **Blockchain and Economic Development: Hype vs. Reality**, https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf, Erişim tarihi: 14 Nisan 2018.

Popper, Nathaniel, “**Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin**”, New York Times. <http://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html>, Erişim tarihi: 23 Mayıs 2018.

Reid, Fergal, Harrigan, Martin, "An Analysis of Anonymity in the Bitcoin System", **2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing**, Boston, MA, 2011, s. 1318-1326.

Szabo, Nick, **Bit Gold**, <http://unenumerated.blogspot.com.tr/2005/12/bit-gold.html>, Erişim tarihi: 22 Mart 2018.

Sermaye Piyasası Kurulu (SPK), **Kripto-Para Bitcoin**, Aralık 2016, <http://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130>, Erişim tarihi: 19 Mart 2018.

Soyaslan, Doğan, **Ceza Hukuku Özel Hükümler**, 11. b., Ankara: Yetkin Yayınları, 2016.

Swan, Melanie, **Blockchain Blueprint for a New Economy**, ABD: O'Reilly, 2015.

Şen, Ersan, “Hırsızlık Suçları”, **Ankara Barosu Dergisi**, 2012/3, 2012, s. 321-357.

Şen, Ersan, **Bitcoin: Elektronik Para**, <http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1120849-bitcoin-elektronik-para>, Erişim tarihi: 12 Haziran 2018.

Şen, Ersan, **Bitcoin Çalınır mı?**, <http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1948163-bitcoin-calindir-mi>, Erişim tarihi: 9 Temmuz 2018.

Tezcan, Durmuş, Erdem, Mustafa Ruhan, Önok, R. Murat, **Teorik ve Pratik Ceza Özel Hukuku**, 15.b., Ankara: Seçkin Yayıncılık, 2017.

Türk standartları Enstitüsü (TSE), **TSE Bilişim Terimleri Sözlüğü İngilizce-Türkçe**, 1.b., Ankara: Onur Matbaacılık, 2006.

Toroslul, Nevzat, **Ceza Hukuku Özel Kısım**, 8. b., Ankara: Savaş Yayınları, 2015.

UNODC, **Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies**, 2014, https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf, Erişim tarihi: 10 Mayıs 2018.

Ünver, Yener, **Adliye Karşı Suçlar**, 2. b., Ankara: Seçkin Yayıncılık, 2010.

Van Valkenburgh, Peter, **What is “open source” and why is it important for cryptocurrency and open blockchain projects?**, <https://coincenter.org/entry/what->

is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects, Eriřim tarihi: 26 Mart 2018.

Von Unruh, Christoph-Nikolaus, **The Law of The Bitcoin**, Edt. Stuart Hoegner, ABD: iUniverse, 2015.

Wright, Aaron, De Filippi, Primavera, **Decentralized Blockchain Technology and The Rise Of Lex Cryptographia**, 2015, <http://dx.doi.org/10.2139/ssrn.2580664>, Eriřim tarihi: 6 Mayıs 2018.

Yeni TCK Madde Gerekçeleri - Türk Ceza Kanunu, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, Eriřim tarihi: 16.08.2018.

Yılmaz, Sacit, “Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu”, **Ankara Barosu Dergisi**, C. 2011/2, 2011, s. 70-97.

Yurtcan, Erdener, **Yargıtay Kararları Işığında Malvarlığına Karşı Suçlar**, 2. b., İstanbul: Adalet Yayınevi, 2015.

İnternet siteleri

https://anoncoin.net/Anonymity_of_cryptocurrencies/, Eriřim tarihi: 31 Mart 2018.

<https://bitcoinfoundation.org/>, Eriřim tarihi: 25 Nisan 2018.

<https://bitcoin.org/en/choose-your-wallet>, Eriřim tarihi: 8 Nisan 2018.

<https://bitcointalk.org/index.php?topic=395761.0>, Eriřim tarihi: 24 Nisan 2018.

<https://blockchain.info/charts/hash-rate?timespan=all>, Eriřim tarihi: 25 Nisan 2018.

<https://bitnodes.earn.com/nodes/1523793781/#network-snapshot>, Eriřim tarihi: 15 Nisan 2018.

<https://coinmarketcap.com/all/views/all>, Eriřim tarihi: 24 Nisan 2018.

<https://counterparty.io/>, Eriřim tarihi: 24 Nisan 2018.

<https://www.cypherpunks.to>, Eriřim tarihi: 21 Mart 2018.

<https://www.computerworld.com/article/3173616/security/the-sha1-hash-function-is-now-completely-unsafe.html>, Eriřim tarihi: 28 Mart 2018
www.kb.cert.org/vuls/id/836068, Eriřim tarihi: 29 Mart 2018.

<https://dgc magazine.com/the-e-gold-story>, Eriřim tarihi: 20 Mart 2018.

<https://emsal.yargitay.gov.tr>

<https://www.ethereum.org/>, Eriřim tarihi: 24 Nisan 2018.

<http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>, Eriřim tarihi: 24 Nisan 2018.

<https://www.ecb.europa.eu/ecb/tasks/html/index.en.html>, Eriřim tarihi: 16 Mayıs 2018.

<http://www.hashcash.org>, Eriřim tarihi: 21 Mart 2018.

<http://historyofbitcoin.org>, Eriřim tarihi: 24 Mart 2018.

<https://getmonero.org>, Eriřim tarihi: 31 Mart 2018.

<http://www.knowyourmobile.com/mobile-phones/bitcoin/21526/bitcoin-how-get-it-action-your-mobile>, Eriřim tarihi: 14 Nisan 2018.

<https://litecoin.org>, Eriřim tarihi: 24 Nisan 2018.

<http://www.masak.gov.tr/tr/content/aklamanin-asamalari/58>, Eriřim tarihi: 19 Aęustos 2018.

<http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>, Eriřim tarihi: 21 Mart 2018.

<https://namecoin.org/>, Eriřim tarihi: 24 Nisan 2018.

https://www.ntv.com.tr/teknoloji/spkdan-sanal-paralara-dayali-islemler-hakkinda-aciklama,4zk6GcRVf0O-pj4T_NQ-fA, Eriřim tarihi: 17 Mayıs 2018.

http://www.linio.org/source_code.html, Eriřim tarihi: 26 Mart 2018.

<https://opensource.org/osd>, Eriřim tarihi: 26 Mart 2018.

<https://peercoin.net/>, Eriřim tarihi: 24 Nisan 2018.

http://wiki.peercointalk.org/index.php?title=Main_Page#Peercoin, Eriřim tarihi: 24 Nisan 2018.

<https://ripple.com/>, Eriřim tarihi: 25 Nisan 2018.

<http://www.tdk.gov.tr>, Eriřim tarihi: 18 Haziran 2018.

<http://www.unodc.org>, Eriřim tarihi: 10 Mayıs 2018.

<https://vanitypool.appspot.com/>, Eriřim tarihi: 7 Nisan 2018.

ÖZGEÇMİŞ

Erdal Durdu, 1970 yılında İslâhiye-Gaziantep'te doğmuştur. İslâhiye Lisesi'nde başladığı lise eğitimini 1987 yılında Adana Erkek Lisesi'nde tamamlanmıştır. 1992 yılında Ege Üniversitesi Bilgisayar Mühendisliği'ni, 2015 yılında Fakülte Birinciliği derecesiyle Doğuş Üniversitesi Hukuk Fakültesi'ni ve 2016 yılında Doğuş Üniversitesi Fen Edebiyat Fakültesi Psikoloji bölümünü çift anadal olarak tamamlamıştır. Evli ve 3 çocuk babası olan Durdu, çalışma hayatına bir kamu kurumunda bilgisayar mühendisi olarak devam etmektedir.



TEZ ONAY SAYFASI

Üniversite : T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü : SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı : Erdal DURDU
Tez Başlığı : KRİPTO PARA BİRİMİ OLARAK BITCOIN VE CEZA HUKUKU
Savunma Tarihi : 07 / 09 / 2018
Danışmanı : Doç. Dr. E. Eylem AKSOY RETORNAZ

JÜRİ ÜYELERİ

Unvanı, Adı Soyadı

İmza

Doç. Dr. E. Eylem AKSOY RETORNAZ



Doç. Dr. Pınar MEMİŞ KARTAL



Doç. Dr. Güçlü AKYÜREK



Enstitü Müdürü

Prof. Dr. M. Yaman ÖZTEK

