

T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



**TERÖRİZMİN FİNANSMANI ARACI
OLARAK KRİPTO PARALAR**

YÜKSEK LİSANS TEZİ

Danışman

Hazırlayan

Doç. Dr. Metin CEYLAN Yunus Emre ÇAMURŞEN

MALATYA 2022

T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

YÜKSEK LİSANS TEZİ

**TERÖRİZMİN FİNANSMANI ARACI OLARAK KRİPTO
PARALAR**

Yunus Emre ÇAMURŞEN

Tez Danışmanı

Doç. Dr. Metin CEYLAN

MALATYA 2022

ONUR SÖZÜ

Doç. Dr. Metin CEYLAN danışmanlığında hazırladığım “Terörizmin Finansmanı Aracı Olarak Kripto Paralar” adlı yüksek lisans tezimin akademik kurallara ve etik davranış ilkelerine uygun olarak bütünüyle tarafımdan yazıldığını; çalışmada yararlanmış olduğum tüm kaynakların, metinde ve kaynakçada yöntemine uygun bir şekilde gösterilenlerden oluştuğunu belirtir, bunu onurumla doğrularım.

Yunus Emre ÇAMURŞEN

Malatya, 2022.

ÖNSÖZ

Teknolojik gelişmeler katlanarak ilerlerken, hukuk kademeli olarak ilerler. Aradaki fark açıldıkça, kişiler artık kendi kurallarını koymaya başlarlar. “Collingridge Çıkmazı” doğrultusunda, bir teknoloji ilk aşamasındayken yapılacak hukuki düzenlemeler kolay olmakla birlikte; teknolojinin ortaya çıkaracağı etkiler, ancak bu teknolojinin ilerlemesi ve geniş çapta kullanılması ile ortaya çıkacağından, bu teknoloji çoğunlukla göz ardı edilir ve düzenleme yapılmaz. Teknoloji ilerleyip, geniş çapta kullanılmaya başlandığı durumda düzenleme yapma ihtiyacı hasıl olur; ancak bu aşamada da yapılacak düzenleme artık zaman alıcı, karmaşık ve oldukça zor bir hale gelmiş olacaktır.

İlk kripto para ve blok zincir olan Bitcoin’in ortaya çıkması üzerinden on dört sene geçmiş olmasına rağmen hukuki düzenleme yapılma isteğinin yeni ortaya çıkmış olması, yukarıda anlatılanları doğrulamaktadır. Hukuki düzenlemelerin ancak yürürlüğe konulmaya başlandığı bu ekosistemde, söz konusu teknolojileri mevcut boşluktan faydalanarak hukukun yasakladığı eylemleri gerçekleştirmek için kullanan azımsanmayacak bir kitle bulunmaktadır. Bu çalışmanın konusunu da, anonimlik, gizlilik, izlenemezlik gibi işlevleri olan kripto paraların hukukun yasakladığı bir eylem olan terörizmin finansmanını gerçekleştirmek amacıyla kullanılması oluşturmaktadır. Kripto paralar merkeziyetsiz yapıları gereği, üzerinde düzenleme yapılması zor ya da kısmen imkânsız bir teknolojidir. Bu çalışma, kripto paraların bu tür özellikleri dikkate alınarak; kripto paraları yapılarına aykırı biçimde dar bir kapsama indirgemeye çalışmaksızın, farklı yönleri ile hukuk dışı öğretilerden de yararlanarak ele almıştır. Bu kapsamda çalışmanın başta hukuk olmak üzere birçok alana katkı sağlayacak bir eser olduğu düşünülmektedir.

Gerek bu çalışmanın hazırlanmasında gerekse uzun süren yüksek lisans dönemimin başarıyla tamamlanmasında emeklerini esirgemeyen çok kıymetli danışman hocam Doç. Dr. Metin CEYLAN’a, çalışmanın ortaya çıkışında emeği geçen hocam Dr. Mete ERDEM’e; artık aramızda olmayan annem Asiye ÇAMURŞEN’e, babam Kenan ÇAMURŞEN’e ve ablam Esra AYANOĞLU’na, beni her koşulda destekledikleri için teşekkürü borç bilirim.

ÖZET

Merkezi bir otoriteye dayanmayan, dağıtık bir veri tabanı olan blok zincirler ve kripto paralar, sağladıkları anonimlik, gizlilik, izlenemezlik gibi özellikleri doğrultusunda hukukun yasakladığı birtakım eylemlerin gerçekleştirilmesinde araç olarak kullanılabilirler. Bu çalışmada, bu tür bir kullanımın en tehlikeli görünülerinden biri olan, kripto paraların terörizmin finansmanının gerçekleştirilmesi amacıyla kullanılması üzerinde durulmuştur. Bu kapsamda çalışmada blok zincir ve kripto paraların ihtiva ettiği temel özellikler, gerektiğinde detaylarından ödün verilmeksizin, tarihsel boyutu ile aktarılmıştır. Ayrıca çalışmada kripto paraların terörizmin finansmanı eylemini gerçekleştirme aracı olarak kullanım biçimleri açıklanmış ve ardından ulusal ve uluslararası düzenlemeler kapsamında terörizmin finansmanı ele alınmıştır. Son olarak finansman konusu fonun kripto para olması halinde mevcut tedbirlerin uygulanmasındaki birtakım sorunlar irdelenmiştir.

Anahtar Kelimeler : Terörizmin finansmanı, malvarlığının dondurulması, müsadere, blok zincir, kripto para, merkeziyetsizlik, gizlilik, izlenemezlik, anonimlik, Bitcoin, Ethereum, sıfır bilgi kanıtı, stabil kripto para

ABSTRACT

Blockchains which are a distributed databases that are not based on a central authority and cryptocurrencies which are type of a blockchain can be used as a tool to perform some actions prohibited by law, in line with the anonymity, privacy, and untraceability they provide. In this study, the use of cryptocurrencies, which is one of the most dangerous aspects of such use, for the financing of terrorism is emphasized. In this context, in the study, the basic features of the blockchain and cryptocurrencies are conveyed with their historical dimension, without compromising the details when necessary. In addition, the use of cryptocurrencies as a means of carrying out the act of financing terrorism is explained in the study, and then the financing of terrorism is discussed within the scope of national and international regulations. Finally, some problems in the implementation of existing measures in case the fund subject to financing is cryptocurrency are examined.

Keywords : Financing of terrorism, asset freezing, confiscation, blockchain, cryptocurrency, decentralization, privacy, untraceability, anonymity, Bitcoin, Ethereum, zero-knowledge proof, stablecoin

İÇİNDEKİLER

ONUR SÖZÜ	iii
ÖNSÖZ.....	iv
ÖZET	v
ABSTRACT	vi
İÇİNDEKİLER	vii
KISALTMALAR	xi
ŞEKİLLER	xv
GİRİŞ	1
PARA VE PARANIN TARİHSEL GELİŞİM SÜRECİ İÇERİSİNDE İNCELENMESİ ...	3
1.1. Takas	3
1.2. Para	6
1.2.1. Paranın Tanımı ve Etimolojisi	6
1.2.2. Paranın Değeri ve Para Olma Gücü Yaklaşımları.....	7
1.2.3. Paranın İşlevleri	10
1.2.4. Paranın Klasik Anlamda Nitelikleri.....	11
1.2.4.1. Yarar ve Değer	11
1.2.4.3 Dayanıklılık.....	12
1.2.4.4. Homojenlik.....	12
1.2.4.5. Bölünebilirlik	12
1.2.4.6. Değerini Koruyabilmesi.....	13
1.2.4.7. Ayırt Edilebilirlik	13
1.2.5. Para Türleri	14
1.2.5.1. Emtia Para	14
1.2.5.1.1. Uluslararası Para Sistemleri	16
1.2.5.1.1.1. Gümüş Standardı	16
1.2.5.1.1.2. Çift Metal Sistemi.....	17
1.2.5.1.1.3. Altın Standardı	19
1.2.5.1.1.4. Altın Değişimi Standardı	21
1.2.5.1.1.5. Bretton Woods Sistemi.....	22
1.2.5.1.1.6. Dalgalı Kur Sistemi	25
1.2.5.2. Temsili Para.....	25
1.2.5.3. İtibari Para	25

1.2.5.4. Dijital Para.....	27
1.2.5.4.1. Merkez Bankası Dijital Para Birimi (CBDC).....	30
1.2.5.5. Elektronik Para	35
1.2.5.6. Sanal Para.....	37
1.2.5.7. Kripto Para.....	40
BLOK ZİNCİR.....	41
2.1. Giriş.....	41
2.2. Blok Zincir Fikri ve Teknolojisine Ulaştıran Çalışmalar.....	43
2.2.1. SDD-1	43
2.2.2. Kriptografik Bulmacalar, Merkle Ağacı ve Kriptografik Hash	44
2.2.3. Chaum Kasa Modeli, DigiCash ve eCash.....	49
2.2.4. Bizans Generalleri Problemi	53
2.2.5. Kripto Anarşist Manifesto.....	60
2.2.6. Paxos Protokolü.....	60
2.2.7. Dijital Belgelerin Zaman Damgası İle Doğrulanması.....	63
2.2.8. b-Money	64
2.2.9. Proof-of-Work (PoW) ve Hashcash.....	68
2.2.10. Bit Gold	69
2.2.11. Reusable Proofs of Work (RPoW).....	70
KRİPTO PARA.....	72
3.1. Giriş.....	72
3.2. Terimin Kökenleri ve Tanımlanması	73
3.3. Kripto Paraların Terörizmin Finansmanı Aracı Olarak Kullanılabilmesini Sağlayan Özellikleri Dikkate Alınarak, Kripto Paralar İle İlgili Bazı Kavram Ve Uygulamalar	80
3.3.1. Yaygın Olarak Kullanılan Bazı Kripto Paralar Hakkında Genel Bilgiler	86
3.3.1.1. Bitcoin (BTC).....	87
3.3.1.2. Ethereum (ETH).....	89
3.3.1.3. Monero (XMR)	92
3.3.1.4. BNB	93
3.3.1.5. Polkadot (DOT)	93
3.3.2. Satoshi Nakamoto.....	94
3.3.3. PoW ve PoS.....	96
3.3.4. Genel Olarak Anonimlik, İzlenemezlik ve Gizlilik (Privacy) Odaklı Kripto Paralar.....	97

3.3.5. İkinci Katman (Layer 2) Çözümleri ve Zincirler Arası Köprüler.....	106
3.3.6. Stabil Kripto Paralar	110
3.3.7. İlk Para Arzı [Initial Coin Offering (ICO)] ve Türevleri.....	114
3.3.8. Kripto Para Borsaları (CEX/DEX)	120
3.3.9. FATF'nin 10, 15 ve 16 Numaralı Tavsiyeleri Kapsamında Kripto Paralar	126
3.3.10. Türkiye'deki Kripto Para Düzenlemesi.....	128
TERÖRİZMİN FİNANSMANI VE FİNANSMANIN ÖNLENMESİ	129
4.1. Giriş.....	129
4.2. Terörizmin Finansmanı İle İlgili Kavramlar.....	129
4.2.1. Terör ve Terörizm Kavramları.....	129
4.2.2. Finansman ve Terörizmin Finansmanı Kavramları	133
4.3. Terörizmin Finansmanının Önlemeye Yönelik Uluslararası Düzenlemeler.....	134
4.3.1. Birleşmiş Milletler Nezdinde Yapılan Düzenlemeler	134
4.3.1.1. Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme	134
4.3.1.2. Güvenlik Konseyi Akıllı Yaptırım Kararları	136
4.3.2. Avrupa Birliği Nezdinde Yapılan Düzenlemeler	138
4.3.3. Avrupa Konseyi Nezdinde Yapılan Düzenlemeler	139
4.3.4. FATF'nin 9 Özel Tavsiyesi.....	140
4.4. Türk Hukukunda Terörizmin Finansmanı Suçu Ve Önlenmesi	142
4.4.1. Terörizmin Finansmanı Suçu.....	143
4.4.1.1. Suçun Konusu.....	143
4.4.1.1.1. Suçun Hukuki Konusu.....	144
4.4.1.1.2. Suçun Maddi Konusu	146
4.4.1.2. Fiil.....	148
4.4.1.3. Fail	149
4.4.1.4. Mağdur.....	150
4.4.1.5. Manevi Unsur	152
4.4.1.6. Hukuka Aykırılık Unsuru	152
4.4.1.7. Kusurluluk	153
4.4.1.8. Nitelikli Hal.....	155
4.4.1.9. Suçun Özel Görünüş Biçimleri.....	155
4.4.1.10. Muhakeme	159
4.4.1.11. Yaptırım.....	159
4.4.1.12. Terörizmin Finansmanının Önlenmesine Dair Bir Tedbir Olarak, Malvarlığının Dondurulması Tedbiri.....	160

4.4.1.12.1. Malvarlığının Dondurulması Tedbirinin Kripto Paralar Çerçevesinde Ele Alınması.....	163
4.4.1.13. Terörizmin Finansmanı Suçu Bakımından Elkoyma ve Müsaderenin Kripto Paralar Çerçevesinde Ele Alınması.....	166
SONUÇ.....	176
KAYNAKÇA	183



KISALTMALAR

AEC	: Anonymity-Enhanced Cryptocurrency
AML	: Anti Money Laundering
AVAX	: Avalanche
BCDU	: Banco Central de Uruguay
BCN	: Bytecoin
BIS	: Bank for International Settlements
BOC	: Bank of Canada
BTC	: Bitcoin
CBCC	: Central Bank Cryptocurrencies
CBDC	: Central Bank Digital Currency
CBOB	: Central Bank of the Bahamas
CEX	: Centralized Exchange
CLOB	: Central Limit Order Book
CMK	: Ceza Muhakemesi Kanunu
CPMI	: Committee on Payments and Market Infrastructures
DAO	: Decentralized Autonomous Organization
DeFi	: Decentralized Finance
DEX	: Decentralized Exchange
DLT	: Distributed Ledger Technology
DOT	: Polkadot
E.	: Esas

ECASH	: Electronic Currency And Secure Hardware
ECB	: European Central Bank
ECCB	: Eastern Caribbean Central Bank
ETH	: Ethereum
EVM	: Ethereum Virtual Machine
FATF	: Financial Action Task Force
FED	: The Federal Reserve System
FINRA	: Finansal Endüstri Düzenleme Kurumu
IBRD	: International Bank for Reconstruction and Development
ICO	: Initial Coin Offering
ICU	: International Clearing Union
IMF	: International Monetary Fund
IOCTA	: Internet Organised Crime Threat Assessment
ISF	: International Stabilization Fund
K.	: Karar
KYC	: Know Your Customer
MiCA	: Markets in Crypto-assets
NFT	: Non-Fungible Tokens
NSBT	: Neutrino System Base Token
PAXG	: PAX Gold
PBFT	: Practical Byzantine Fault Tolerance
PBOC	: People's Bank of China
PoS	: Proof of Stake

POS	: Point of Sale
PoW	: Proof of Work
R.G.	: Resmi Gazete
ROI	: Return of Investment
RPoW	: Reusable Proofs of Work
S.	: Sayı
SCBDC	: Synthetic CBDC
SCRT	: Secret
SOL	: Solana
SPV	: Simplified Payment Verification
T	: Tarih
TCMB	: Türkiye Cumhuriyeti Merkez Bankası
USDN	: Neutrino USD
USDT	: Tether
UST	: Terra USD
UTXO	: Unspent Transaction Output
VA	: Virtual Asset
VASP	: Virtual Asset Service Provider
vd.	: ve diğerleri / ve devamı
WOW	: World of Warcraft
XMR	: Monero
XVG	: Verge
ZEC	: Zcash

ZEN : Horizen

zk : zero-knowledge



ŞEKİLLER

- Şekil 3. 1:** İbn Teymiyye Basın Merkezi tarafından düzenlenen kampanya. 82
- Şekil 3. 2:** Captcha kodunu geçtikten sonra her seferinde farklı bir adres üreten üçüncü aşama..... 84
- Şekil 3. 3:** El-Kaide kampanyası için paylaşılan Bitcoin cüzdan adresi..... 85
- Şekil 3. 4:** Gerçekleştirilen ilk Ethereum transferi..... 98
- Şekil 3. 5:** Aztec ağına gerçekleştirilen bir yatırma işlemi..... 109
- Şekil 3. 6:** UST'nin 9 Mayıs 2022'de başlayan denklik bozulmasının mum grafiği. 1 Amerikan doları yerine 0,032 Amerikan doları üzerinden işlem görmektedir. (Coinbase, UST/USD paritesi)..... 113
- Şekil 3. 7:** USDN değeri üzerindeki dalgalanmaların mum grafiği. (Kucoin, USDN/USDT paritesi)..... 114
- Şekil 3. 8:** Bir DEX üzerinde sığ bir emir defterine sahip bir parite. (DEXE/USDT) . 122
- Şekil 3. 9:** Bir CEX üzerinde sığ bir emir defterine sahip bir parite. (AVAX/USDT.e) 123
- Şekil 3. 10:** DEX üzerinde konulan bir emrin ağdaki görüntüsü. 124

GİRİŞ

Para, tarih boyunca sınırsız ihtiyaçları karşılamak ve sınırsız amaçları gerçekleştirmek için kullanılagelmiştir. İki ya da birden fazla tarafın aralarında; devletler, kurumlar ya da organizasyonlar tarafından tanınmış bir para ile değişim yapmasında bir sorun bulunmamakla beraber bu değişimi hangi amaçla yerine getirdikleri, tarafların ötesinde olumsuz bir etki doğurabilir. Bu çalışmayı ilgilendiren etki, bu etkinin bir suçun oluşmasına yani terörizmin finansmanına sebebiyet veren boyutu ile ilgilidir.

Blok zincir (blockchain) kısaca kriptografik işlemlerin gruplaşarak meydana getirdiği bloklardan oluşan dağıtık dijital defterlerdir. Bu teknoloji, 1980'li yılların sonundan itibaren yapılagelmiş birtakım çalışmaların da etkisiyle ilk kez 2008 yılında Satoshi Nakamoto takma ismini kullanan kişi ya da grubun yayınladığı "Bitcoin: A Peer-to-Peer Electronic Cash System" makalesi ile tanıtılmıştır¹. Bitcoin, ilk blok zincir uygulaması ve ödeme aracıdır. Blok zincirin bu ödeme aracı görünümüne "kripto para"² adı verilmektedir. Kripto para, Bretton Woods Konferansı ile 1944 yılında kurulan uluslararası para hukuku rejiminden devletlerin kontrolünün dışında ortaya çıkan bir sapmadır. Kripto paralar; blok zincir teknolojisinin sunduğu merkeziyetsizlik, işlemlerin şeffaf olması ve aynı zamanda gizlenebilirlik ve anonimlik sunması, işlemlerin geri döndürülemez olması gibi özellikleri sayesinde klasik ödeme araçlarına büyük bir alternatif olarak karşımıza çıkmaktadır. Mevcut kripto paraların neredeyse tamamına yakını blok zincir tabanlı olup, blok zincirin dışında diğer dağıtık defter teknolojilerine dayanan birtakım kripto paralar da bulunmaktadır.

¹ Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, <https://bitcoin.org/bitcoin.pdf> (Son erişim:08.04.2022)

² Çalışmanın giriş kısmında belirtmek gerekir ki, terimin İngilizcesi "cryptocurrency" olup bitişik yazılmaktadır. Fakat terimin Türkçe kullanımı çoğunlukla "kripto para" olarak kelimeler ayrılarak gerçekleştirilmektedir. Bu doğrultuda Türk Dil Kurumu'nun güncel sözlüklerini (terim sözlükleri dahil) tarayıp bu terim hakkında hiçbir sonuca ulaşamayınca, bilgi edinme hakkı çerçevesinde "Atatürk Kültür, Dil Ve Tarih Yüksek Kurumu Başkanlığı"na 27.04.2022 tarihinde başvuruda bulunmuş ve 29.04.2022 tarihinde başvurum cevaplanmıştır. Türk Dil Kurumu tarafından incelenen başvurum "Sormuş olduğunuz kelime grubunun yazımı, değerlendirilmek üzere ilgili komisyona gönderilmiştir." şeklinde cevaplanmıştır. Bu sebeple şu an terimin doğru yazımı hakkında, hatta terimin kendisi hakkında, Türk Dil Kurumu bünyesinde kabul edilen bir düzenleme bulunmamaktadır. Her ne kadar kendim bu aşamada terimin orijinal halinin de bitişik yazıldığını varsayarak "elektroşok" ya da "astrofizik" gibi terimlerde de olduğu gibi "kriptopara" olarak yazılmasını daha doğru buluyor olsam da; hukuk alanında az da olsa yayınlanan güncel eserlerde terimin yazımı "kripto para" olarak tercih edildiğinden, bu çalışmada da şimdilik bu kullanımı takip ederek "kripto para" şeklinde ayrı yazmanın daha uygun olacağını düşünmüş bulunmaktayım. Çalışmada ayrıca benzer bir şekilde "blok zincir" şeklinde bir yazım tercih edilmiştir.

İlk kripto para transferinin üzerinden on üç yıl geçtiği göze alındığında kripto paraların diğer ödeme araçlarına göre hala yeni bir kavram olduğu kabul edilebilir. Kripto paraların gerek finans sisteminde gerekse ekonomi ve hukuk sistemi içerisindeki yeri henüz belirlenebilmiş değildir. Kripto paralara olan ilgi, gittikçe ilerlemekte ve bu durum biraz önce sayılan alanlarda yapılan çalışmalarda artışa da yansımakta ise de henüz yeterli çalışmanın bulunmadığını söylemek mümkündür. Bu durum blok zincirin sunduğu imkanlar olan merkeziyetsizlik, anonimlik ve gizlilik ile beraber düşünüldüğünde kullanıcılara oldukça geniş bir hareket alanı sunmaktadır. Bu doğrultuda bahsedilen özelliklerin kanun koyucular, uluslararası sözleşmeler ve yasalar tarafından yasaklanmış faaliyetlerin yürütülmesinde faydalanılacağını beklemek yanlış olmaz. Kripto paralar bu sebeple uluslararası toplumun kabul edilemez görerek yasakladığı ve suç olarak tanımladığı faaliyetlerin hukuk dışı mali kaynağını teşkil edebilir. Bununla birlikte terör faaliyetlerini kendisine bir yöntem benimsemiş olan yasa dışı gruplar ve örgütlerin bu faaliyetlerini kripto para kaynakları ile desteklediği de bilinen bir gerçektir.

Bu doğrultuda çalışmada kripto paraların ortaya çıkışları, protokol düzeyinde özellikleri belirtilip ekonomideki, finans sektöründeki ve uluslararası para hukukundaki yeri incelendikten sonra mevcut hukuki düzenlemeler ışığında ve somut olaylar çerçevesinde terörizmin finansmanı aracı olarak kullanılması ele alınacaktır.

BİRİNCİ BÖLÜM

PARA VE PARANIN TARİHSEL GELİŞİM SÜRECİ İÇERİSİNDE İNCELENMESİ

Kripto paranın ne olduğu ile ilgili tartışmalara girmeden önce, paranın ne olduğu hususunun ortaya konması gerekmektedir. İnsanların bir şeyi para olarak kullanmaları, oldukça farklı sebeplere bağlı olsa da birtakım ortak amaçların varlığı da söz konusu olabilir. Çalışmanın bu bölümünde, geçmişten günümüze toplumsal ilişkilerin vazgeçilmezi olan paranın ne olduğu, ortaya çıkış süreci kapsamında tarihsel bir çerçeve ile ortaya konacaktır.

1.1.Takas

Takas, kelime anlamı olarak malların para dışındaki şeyler ile mübadelesi³ ya da tarafların tatmin oluncaya kadar sürdürdükleri karşılıklı, tamamlayıcı mübadele⁴ olarak tanımlanabilir.

Takas sıkça tarihsel süreçte paradan önce ortaya çıkmış, paranın öncüsü; ilkel toplulukların kullandığı bir yöntem olarak değerlendirilmektedir. Modern ekonominin babası kabul edilen Adam Smith'ten yirminci yüzyılın sonlarına kadar paranın kökeninin takas olduğu kabul edilmekteydi. Adam Smith'in ortaya attığı bu görüş, kendinden sonra gelen Carl Menger, William Stanley Jevons ve Rober Clower gibi ekonomistler tarafından da takip edilmiştir. Bu görüşe göre ekonomi evrimsel bir gelişim içindedir; bu gelişimin en ilkel halini insan doğasının kendisinden ortaya çıkan takas oluşturmaktadır;

³ <https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/barter> (Erişim: 24.01.2022)

⁴ Humphrey, Caroline, "Barter and Economic Disintegration", *New Series*, 1985/20 (1), s. 49.
<https://voidnetwork.gr/wp-content/uploads/2016/09/Barter-and-economic-disintegration-by-Caroline-Humphrey.pdf> (Erişim: 11.04.2022)

para, takastan ortaya çıkmıştır⁵. Clower ve Jevons'a göre takasın terk edilmesinin sebebi ise yüksek işlem ücreti (takas edilecek emtianın taşınması nedeniyle) gerektirmesidir⁶.

Takas sisteminin para sistemine göre birtakım zorlukları bulunmaktadır. Takasta karşılaşılan ilk zorluk, birbirlerinin sahipliklerini karşılıklı olarak isteyen iki kişiyi bulmaktır. Ortada birçok insan ve birçok sahipliği istenilen şey olabilir; takasın gerçekleşmesi için sınırsız ihtimaller havuzunda çifte rastlantıların olması gerekir ki bu oldukça güçtür⁷. Örneğin kil çömlek üreten bir kişinin patatese ihtiyacı olduğunu ve çömlleklerini patates ile takas etmek istediği varsayımında bu kişinin takası ancak elinde patates olan ve bu patatesleri çömlek karşılığında takas etmek isteyen biri ile sağlaması gerekmektedir. Elinde patates olan ama çömlek isteyen ya da çömlek isteyen ama elinde tavuk bulunan kimselerin olduğu varsayımında bu takas gerçekleşmeyecektir⁸. Ya da modern toplumdaki örneklemek gerekirse, bulunduğu evin kullanımını kendisine yetmeyen bir kişi, evi kendisine fazlasıyla yetecek bir eve sahip ve takas isteyen başka bir kişiyi bulsa bile, ikinci evin sahibinin ilk ev ile takas isteyeceğini beklemek güçtür. Birtakım emtialar kullanmak bu karşılıklı orantısızlığı giderilmesini ve isteklerin uyuşabilmesini sağlayabilir. Bu emtialar birer "mübadele aracı" olarak tıkalı iki yönlü bir işleme üçüncü bir çıkış yolu sunabilir⁹.

Takasta karşılıklı isteklerin tam anlamıyla uyuşması gerekliliği dışında ortaya çıkan bir diğer sorun, bu istekler uyuşsa bile mübadelenin hangi oranda yapılacağı sorunudur. Bir emtianın başka bir emtia ile değişimi yapılırken ikisi arasında belirli bir oranın bulunması gerekmektedir. Aksi takdirde takası gerçekleştiren taraflardan biri emtiayı birinden alıp diğerinden satarak kazanç elde edecektir¹⁰.

Takasın bahsedilen zorluklarının yanında parasal sisteme göre birtakım kolaylıkları da olabilir. Örneğin takasta tarafların sadece karşılıklı sunulan malları incelemeleri yeterliyken; parasallaştırılmış ekonomide, sunulan malların miktarı ve

⁵ Humphrey, 1985, s. 49.

⁶ Humphrey, 1985, s.50.

⁷ Jevons, William, Money and the Mechanism of Exchange. New York: D. Appleton and Company, 1875. <https://oll.libertyfund.org/title/jevons-money-and-the-mechanism-of-exchange> ss. 3-4. ; Taskinsoy, John, "From Primitive Barter to Inflationary Dollar: A Warless Economic Weapon of Mass Destruction", 2020, s. 7 <http://dx.doi.org/10.2139/ssrn.3542145> (Erişim: 11.04.2022)

⁸ Dalton, George. "Barter." *Journal of Economic Issues - Association for Evolutionary Economics*, 1982/16 (1), ss. 182-183. <http://www.jstor.org/stable/4225147> (Erişim: 11.04.2022)

⁹ Jevons, 1875, s. 4.

¹⁰ Jevons, 1875, s. 5.

özelliklerinin yanında kullanılan paranın sürekli dalgalanan değeri de göz önünde tutulmaktadır¹¹. Yine takasta talep, takasın gerçekleştiği anda karşılanmasına rağmen para ile ödemede ancak ödemeyi takip eden bir işlemin varlığı değerini realize edilmesini sağlayacaktır¹².

Yukarıda belirtilen, paranın takastan ortaya çıktığı düşüncesi çeşitli dayanaklar öne sürülerek günümüzde terk edilmeye başlanmıştır¹³. Adam Smith ve takip edenler tarafından düşünülen para modeli, takasın ilk olarak ilkel topluluklar içinde ortaya çıkmış olduğundan hareket etmektedir. Fakat takasın ilk olarak topluluk içinde değil, topluluklar arasında ortaya çıkmış olması¹⁴ bu modelin geçersizliğine ilk dayanaktır. Bununla birlikte bu modelde takasın ilkel topluluklarda kullanıldığı, terk edildiği ve paraya geçildiği¹⁵ söylene de takas, paranın bilindiği ve kullanıldığı topluluklarda hala devam etmektedir¹⁶. Takas yolunu seçen kişiler alternatif ve daha uygun yolların (çoğunlukla para) olduğunu bilmesine rağmen bazı özel sebepler nedeniyle takas yolunu seçebilirler¹⁷. Basit bir örnek ile bir dişçi evi için yapacağı harcamalar karşılığında bir marangozun dişlerini tedavi edebilir. Her iki taraf da sundukları hizmet karşılığında para ödemeyerek vergiden kaçınabilmektedir¹⁸. Takasın terk edilip paraya geçildiği düşüncesine rağmen takas ve para kavramları iç içe geçmiştir. Takas bazı durumlarda paranın değer ölçüsü işlevini de yerine getirebilir¹⁹. Örneğin Selk'nam²⁰ yerlilerinde karşılaşılan takasta:

“3-4 ok = 1 iyi yay

2 ok = 1 ok kılıfı”

¹¹ Humphrey, 1985, s.60.

¹² Humphrey, 1985, s. 48.

¹³ Chapman, Anne, “Barter as a Universal Mode of Exchange”, *L'Homme*, 1980, s. 54.

https://www.persee.fr/doc/hom_0439-4216_1980_num_20_3_368100 (Erişim: 10.04.2022); Graeber, David, *Debt: The First 5000 Years*, Melville House, 2011, s. 28.

https://warwick.ac.uk/fac/arts/english/currentstudents/undergraduate/modules/fulllist/special/statesofdamage/syllabus201516/graeber-debt_the_first_5000_years.pdf (Erişim: 11.04.2022); Hart, Keith, “Notes Towards An Anthropology Of Money”, *Kritikos*, 2005/2.

https://intertheory.org/hart.htm?fbclid=IwAR30etRsErMO-39RaHQFkTC2msAwX5BJcE1Wy8xCs5_sQJOtpAJf8k9wtNU

(Erişim: 12.04.2022); Humphrey, 1985, s. 48.

¹⁴ Chapman, 1980, s. 47.; Graeber, 2011, s. 28.

¹⁵ Humphrey, 1985, s. 50.

¹⁶ Dalton, 1982, s. 188.; Humphrey, 1985, s. 48.

¹⁷ Dalton, 1982, s. 188.

¹⁸ Dalton, 1982, ss. 186-187.

¹⁹ Chapman, 1980, s. 54.

²⁰ Güney Amerika'nın Patagonya bölgesinde yaşamış bir halk.

şeklinde oranlar kararlaştırılmaktaydı²¹. Bununla birlikte para arzının kısıtlaştığı durumlarda paranın kendisi de takasın konusunu oluşturabilir²².

Parasız değişim aracı anlamıyla takas hiçbir zaman niceliksel olarak önemli ve baskın bir değişim modeli olmamıştır. Yine de geçmişten günümüze ve her türlü ekonomik modelde takas ile hala karşılaşmak mümkündür²³. Uzunca bir süre takasın paranın ortaya çıkışındaki ilk adım olduğu düşünülse de, yukarıda açıklanan nedenler uyarınca bu düşünce terk edilmiştir. Günümüzde paranın hediye mübadelesi ya da kredi ve borçlanmadan ortaya çıktığı kabul edilmektedir²⁴.

1.2. Para

1.2.1. Paranın Tanımı ve Etimolojisi

Para, birçok dilde etimolojik olarak “Juno Moneta”dan gelmektedir²⁵. Bu duruma orta İngilizcede “moneie” ve “moneye”; İngilizcede “money”; eski Fransızcada “moneie”; Latince “monēta”; Azerice, Türkmençe veya Rusçada “manat (монета)” gibi örnekler verilebilir. Moneta, Roma mitolojisinde bir tanrıçadır. Antik Roma’da para basımı Juno Moneta tapınağında yapılmaktaydı²⁶; bu nedenle birçok dilde para kelimesinin, özellikle İngilizcede para basmak anlamındaki “mint” kelimesinin moneta kelimesinden geldiği söylenmektedir. Türkçedeki “para” kelimesi ise Farsçadaki “pāre” kelimesinden gelmektedir²⁷.

Para için; “devletin ya da devletin yetkili kıldığı kurumların belli bir hesap birimine dayalı olarak, basılmak suretiyle dolaşıma çıkarılan, yapılan işlemlerde kabulü zorunlu olan menkul eşya”, “mal ve hizmetlerin satın alınmasında kullanılan genel kabul görmüş her şey²⁸” şeklinde tanımlamalar yapmak mümkündür.

²¹ Chapman, 1980, s.51.

²² Humphrey, 1985, s. 48.

²³ Dalton, 1982, s. 185.

²⁴ Araujo vd., On the Origin of Money, 2016, ss. 1-2.

https://extranet.sioe.org/uploads/sioe2017/araujo_bignon_breton_camargo.pdf (Erişim:01.06.2022)

²⁵ Hart, 2005.

²⁶ Wikipedia, “Temple of Juno Moneta”, https://en.wikipedia.org/wiki/Temple_of_Juno_Moneta (Erişim: 12.04.2022)

²⁷ <https://sozluk.gov.tr>

²⁸ Yalta, A. Yasemin, Para Teorisi ve Politikası Ders Notları, s.1

https://acikders.tuba.gov.tr/pluginfile.php/4391/mod_resource/content/3/ders-notlari-kitap-%28s1%2C1%29.pdf (Erişim: 12.04.2022)

1.2.2. Paranın Değeri ve Para Olma Gücü Yaklaşımları

Paranın, ortak bir değer ölçüsüne olan ihtiyacın sonucu olarak ortaya çıktığı söylenebilir. Değer ölçüsü toplumdaki topluma değişkenlik gösterebilir. Genellikle miktar olarak kıt ve toplumun büyük kısmının ona sahip olma isteği olan şey değerlidir. Bununla birlikte değer üç farklı biçimde ele alınabilir. Sosyolojik anlamda değer, insan yaşamında nihai olarak iyi, uygun ve arzu edilen şeydir. Ekonomik anlamda değer, hangi şeylerin ne kadar arzu edildiğinin derecesidir. Bu derece, insanların o şeyi elde etmek için vazgeçmeyi göze aldığı miktar ile ölçülebilir. Dilsel olarak değer ise kısaca “anamlı fark”tır²⁹. Adam Smith ise “The Wealth of Nations” eserinde değeri iki formun bütünü olarak ele almıştır. Bunlar “kullanım değeri” ve “değişim değeri”dir. Smith’e göre kullanım değeri yüksek olan bir şeyin değişim değeri olmayabilir; ya da değişim değeri çok yüksek olan bir şeyin kullanım değeri olmayabilir³⁰. Bununla birlikte değer, “emek değeri” ya da “kullanım değeri” olarak da açıklanabilmektedir. Biri üretim ile, diğeri tüketim ile gelen değerdir³¹.

Paranın neden bir değere sahip olduğu hakkında çeşitli teoriler ortaya atılmıştır³². Peşin ödeme kısıtı modelinde³³ para çeşitli işlemleri gerçekleştirmek için gereklidir; bu işlemler para olmadan gerçekleştirilemez³⁴; para değerlidir çünkü mal alımı için kullanılır³⁵. Truman Bewley’nin sonsuz ufuklar modelinde³⁶ ve Neil Wallace’ın örtüşen

²⁹ Graeber, David, *Towards an Anthropological Theory of Value*, Palgrave, 2001, ss. 1-2.
https://monoskop.org/images/3/36/Graeber_David_Toward_an_Anthropological_Theory_of_Value.pdf (Erişim: 12.04.2022)

³⁰ Akt. Fayazmanesh, Sasan, *Money and Exchange: Folktales and reality*, Routledge, 2006, s. 51.
<https://library.oapen.org/bitstream/id/ba173030-dbe5-4ecd-a8b3-6ae249a39407/1005953.pdf> (Erişim: 13.04.2022)

³¹ Ross, Edward Alsworth. “The Standard of Deferred Payments.”, *The Annals of the American Academy of Political and Social Science*, 1892/3, s.42. <http://www.jstor.org/stable/1008596> (Erişim: 14.04.2022)

³² Hayashi, Fumio, Akihiko Matsui, “A Model of Fiat Money and Barter”, *Journal of Economic Theory*, 1996/68 (1), s. 111. <https://doi.org/10.1006/jeth.1996.0006> (Erişim: 09.04.2022)

³³ Clower, Robert W.. “A Reconsideration Of The Microfoundations Of Monetary Theory.” *Economic Inquiry*, 1967/6. <https://www.semanticscholar.org/paper/A-RECONSIDERATION-OF-THE-MICROFOUNDATIONS-OF-THEORY-Clower/416792d58f668aafc6cb0b9a56aef70daeb1c7b2> (Erişim: 09.04.2022)

³⁴ Spencer, Adam Hal, Lecture 6: Cash in Advance, lecture notes, *Advanced Monetary Economics 2020*, The University of Nottingham, 2020.
https://static1.squarespace.com/static/6109a70ff6be433c1a1339fe/t/6112c69da1c3e55c3df1b735/1628620447733/L6_CIA_2020_Mar16.pdf (Erişim: 09.04.2022)

³⁵ Ellison, M., *Monetary Economics*, Chapter 4 – Cash in Advance Model, lecture notes, s. 28.
<https://users.ox.ac.uk/~exet2581/msc/ec924cia.pdf> (Erişim: 09.04.2022)

³⁶ Bewley, Truman, “The Optimum Quantity of Money, 1979”,
<https://www.kellogg.northwestern.edu/research/math/papers/383.pdf> (Erişim: 09.04.2022)

nesiller teorisinde³⁷ paranın bir değere sahip olmasının nedeni başka bir değer saklama aracı olmamasındandır. Örtüşen nesiller teorisinde paranın tamamen değer saklama aracı olduğu üzerinde durulmuş, mübadele aracı olma özelliği dikkate alınmamıştır³⁸. Robert Townsend’in Turnpike modelinde ise para sadece ödeme anlamındadır³⁹.

Bununla birlikte paranın para olma gücünü nereden aldığı konusunda da çeşitli görüşler bulunmaktadır:

Bunlardan ilki “realist” görüştür. Realist para, para olma gücünü kendinden alır. Bu görüş odağına değer kendiliğinden geldiği para tipi olan “emtia para”yı almaktadır. Kıymetli madenler (altın, gümüş vs.) kendiliğinden bir değere sahip olduklarından değerlidir. Fakat banknotların ortaya çıkması, kıymetli madenler ile banknotlar arasındaki bağın kopması, paranın üzerinde yazılan değer olan nominal değer üzerinden işlem görmesi gibi sonuçlar yüzünden bu görüş geçerliliğini yitirmiştir.

İkinci görüş ise Georg Friedrich Knapp tarafından ortaya konan “devletçi” görüşüdür. Bu görüşe göre para, para olma gücünü devletten alır. Bu görüşe göre para, ekonominin yarattığı bir varlık değil; hukukun yarattığı bir varlıktır⁴⁰. Devlet, ekonomik alanda sahip olduğu egemenlik yetkisine dayalı olarak değişim aracı, değer ölçüsü ve tasarruf aracını belirlemektedir. Paranın diğer nesnelere farkı, devlet tarafından basılmasıdır⁴¹. Bu doğrultuda Herschel Grossman, çağdaş kağıt paranın, devletin yaptırım gücü nedeniyle yasal bir ödeme aracı olarak kabul edildiğini ileri sürer⁴².

³⁷ Wallace, Neil, “The Overlapping Generations Model of Fiat Money”, *Models of Monetary Economies*, Federal Reserve Bank of Minneapolis, <https://www.minneapolisfed.org/~media/files/pubs/books/models/cp49.pdf?la=en> (Erişim: 09.04.2022)

³⁸ Kiyotaki, Nobuhiro, Randall Wright. “On Money as a Medium of Exchange.” *Journal of Political Economy* 97, 1989/4: s. 928. <http://www.jstor.org/stable/1832197> (Erişim: 13.04.2022)

³⁹ Townsend, Robert M. “Models of money with spatially separated agents.” *Models of monetary economies*, 1980, ss. 265-303. <http://m.robertmtownsend.net/sites/default/files/files/papers/published/ModelsofMoney1980.pdf> (Erişim: 09.04.2022)

⁴⁰ Georg Friedrich Knapp’ten akt. Davies, Glyn, *A History of Money*, University of Wales Press, 2002, s. 26. https://books.google.com.tr/books?hl=tr&lr=&id=cU2uBwAAQBAJ&oi=fnd&pg=PR3&dq=money+definition&ots=UjkXIZ5BH&sig=YRtg5IQ3x22RW2ec7dktDXsbwVM&redir_esc=y#v=onepage&q=money%20definition&f=false (Erişim: 14.04.2022)

⁴¹ Korkmaz Sürer, Mukaddes. “Uluslararası Para Hukuku”, *Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni*, 2005/25, s. 215. <https://dergipark.org.tr/tr/pub/iuhmhohb/issue/9365/117182> (Erişim: 13.04.2022)

⁴² Demir Abaan, Ernur, “Para: Teorik Bir Tarama ve Tartışma”, Türkiye Cumhuriyeti Merkez Bankası, 1997, s. 12. <https://www.tcmb.gov.tr/wps/wcm/connect/c0f93298-5bb3-40bb-8d38-f8555426ab64/1997-3.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-c0f93298-5bb3-40bb-8d38-f8555426ab64-m3fw5z-> (Erişim:20.05.2022)

Ağırlıklı olarak ekonomistlerin savunduğu üçüncü görüş ise “toplumcu” görüştür. Bu görüşe göre; bir nesnenin ticari hayatta para olarak kullanılması insanın güveniyle olur. Devlet ne kadar düzenleme yaparsa yapsın, bir nesne ticari hayatta toplum tarafından değer ölçüsü, değişim aracı ve tasarruf aracı olarak kabul edilmiyorsa o şey para değildir. Para niteliğinin kazanılabilmesi için toplumun zorunlu ödeme aracı olduğu yönündeki inancı söz konusu olmalıdır⁴³. Kültürel bağlamdan ayrılamayacak şekilde paranın değer barındırabilmesi için insanların o parayı istemesi ve nasıl kullanılacağını bilmesi gerekmektedir⁴⁴. Toplumcu görüş paranın oluşmasında toplumun genel kabulünü yeterli görmektedir. Buradaki genel kabulün yasalardan ötürü gelen genel kabulden⁴⁵ ayrı değerlendirilmesi gerekmektedir. Bu görüş devletin para konusundaki yetkisini göz ardı etmektedir.

Para olma gücü konusunda dördüncü görüş ise Avrupa Birliği'nin oluşturulduğu dönemde ortaya çıkmış “kurumsalci” görüştür. Bu görüşe göre ekonominin şekillendirilmesinde kurumların önemli bir rolü vardır. Bu kapsamda paraya para olma değerini veren ülkedeki kurumsal yapıdır. Devletler tek başlarına para olarak işlev görecektir nesneyi belirleyemezler. Çağdaş ekonomide devletin belirlediği şey para birimidir. Dolaşıma para çıkarılması ve dolaşıma çıkan paranın değerinin belirlenmesi kurumsal yapı içerisinde olmaktadır. Çağdaş ülkelerde devlet para birimini belirledikten sonra para dolaşıma çıkartmak konusunda merkez bankasına yetki verir. Merkez bankası da dolaşıma para çıkarır ve paranın değerini korumak için bir para politikası belirler.

⁴³ Korkmaz Süre, 2005, ss. 215-216.

⁴⁴ Weatherford, Jack, The History of Money, 2009, https://books.google.com.tr/books?hl=tr&lr=&id=v8oxCs1eWgsC&oi=fnd&pg=PR11&dq=history+of+money&ots=sHobjRSPX0&sig=bB55zxJSKg3BCLArhGus9gCVH_A&redir_esc=y#v=onepage&q=history%20of%20money&f=false 2009, s. 20. (Erişim: 08.04.2022)

⁴⁵ Fisher, Irving, The Purchasing Power of Money, its Determination and Relation to Credit, Interest and Crises, 1922, Macmillan, s. 16. <https://eet.pixel-online.org/files/etranslation/original/Fisher%20The%20Purchasing%20Power%20of%20Money.pdf> (Erişim:20.04.2022)

1.2.3. Paranın İşlevleri

Paranın belirli işlevleri yerine getirdiği dolayısıyla para olduğu düşünülmektedir. Bir şeyi para olarak tutma ve kullanma dürtüsü, bu işlevlerin varlığına bağlıdır⁴⁶.

Paranın işlevleri hakkında ilk ayrıntılı sınıflandırma Jevons tarafından yapılmıştır. Jevons paranın dört işlevi olduğundan bahstemekle birlikte bunların ikisinin temel işlevler olduğunu belirtmektedir. Jevons'a göre paranın en temel işlevleri mübadele aracı olması ve hesap birimi ölçüsü olmasıdır⁴⁷. Jevons'a göre paranın diğer iki işlevi ise değer standardı olması ve değer saklama aracı olmasıdır⁴⁸.

John Maynard Keynes ise paranın iki temel fonksiyonundan bahsetmektedir. Bunlar mübadeleyi sağlamak ve servet değeri saklama aracı olmaktır⁴⁹.

Günümüzde paranın klasik işlevleri, çoğunlukla Jevons'un saymış olduğu dört işlevden üçü kullanılarak tanımlanmaktadır. Bunlar paranın mübadele aracı olması, hesap birimi ölçüsü olması ve değer saklama aracı olmasıdır⁵⁰.

Paranın mübadele aracı olması, mal ve hizmetlerin satın alınmasında aracı olarak davranması anlamına gelir. Paranın bu özelliği sayesinde isteklerin çakışmasının beklenmesine gerek duyulmaz.

Paranın hesap birimi olması, piyasadaki mal, hizmet ya da herhangi bir işlem için ortak bir değer ölçüsü işlevi görmesi anlamına gelir.

Paranın değer saklama aracı olması ise, paranın istendiğinde daha sonra kullanılmak için saklanabilmesi ile ilişkilidir. Paranın saklama durumunda değerini koruyor olması önemlidir. Bununla birlikte paranın, saklama amacından vazgeçilerek mübadele için kullanılmasına ya da tam tersine geçişin kolay ve bedelsiz olması gerekmektedir⁵¹.

Bu üç işlevin yanında literatürde farklı işlev tanımlamaları da getirilebilmektedir. Bu tanımlamalardan en çok başvurulanı paranın “vadeli ödeme standardı⁵²” olması

⁴⁶ Brunner, Karl, Allan H. Meltzer. “The Uses of Money: Money in the Theory of an Exchange Economy.” *The American Economic Review*, 1971/61 (5), s. 784. <http://www.jstor.org/stable/1813142> (Erişim: 13.04.2022)

⁴⁷ Jevons, 1875, s. 13.

⁴⁸ Jevons, 1875, ss. 14-15.

⁴⁹ Akt. Davidson, Paul. “Money and the Real World.” *The Economic Journal*, 1972/82 (325), s. 102. <https://doi.org/10.2307/2230209> (Erişim: 12.04.2022)

⁵⁰ Brunner ve Meltzer, 1971, s. 784.; Davidson, 1972, s. 104.

⁵¹ Davidson, 1972, s. 104

⁵² Davies, 2022, s. 77.; Ross, 1892.

işlevidir. Bu işlev Jevons'un saydığı dört işlevden biri olmak ile birlikte Jevons tarafından "değer standardı"⁵³ olarak anılmıştı⁵⁴. Paranın vadeli ödeme standardı olması işlevi, borçlanma ve krediler gibi işlemlerde kullanılabilmesidir. Paranın genellikle yaşadığı alım gücündeki değişiklik, enflasyon gibi sebepler nedeniyle bu özelliği eleştirilmek ile birlikte; oldukça farklı biçimlerde kurulabilen vadeli ödemelerde, vade sonunda paranın alım gücünün düşmüş ya da artmış olmasının taraflardan birine yarara ya da diğerine zarara neden olan tek etmen olmadığı hesaba katılmalıdır⁵⁵.

1.2.4. Paranın Klasik Anlamda Nitelikleri

Paranın para olabilmesi için bazı niteliklere sahip olması gerektiği literatürde birçok kez dile getirilmiştir⁵⁶. Bu kısımda Jevons tarafından Michel Chavalier'in sınıflandırması izlenerek yapılan klasik sıralama takip edilip, Jevons'un bu konudaki görüşleri açıklanmıştır⁵⁷. Belirtmek gerekir ki bu niteliklere yenilerinin eklenmeleri mümkün olmakla birlikte, paranın üzerinde çoğunlukla uzlaşmış olunan aşağıda niteliklerinin ortaya konması tercih edilmiştir.

1.2.4.1. Yarar ve Değer

Paranın değer ihtiva eden şeyler ile değiş tokuşunun yapılması, paranın kendiliğinden de bir değerinin olmasını gerektirdiği düşüncesine itebilir. İnsanların öncelikle para olarak belirlenen şeyi kabul etme motivasyonuna sahip olmaları gerekmektedir. Bu motivasyonu çeşitli etkenler tetikleyebilir, alışkanlık, gelenek ya da yasal düzenlemeler olabilir. Paranın geniş kesimlerce benzer miktarlarda atfedilmiş bir saygınlığının olması gerekir. Bunun yanı sıra paranın kullanımının bir yarar sağlaması beklenir⁵⁸.

⁵³ Newcomb, Simon. "The Standard of Value." *The North American Review*, 1879/129 (274), ss. 223–37, <http://www.jstor.org/stable/25100790> (Erişim: 14.04.2022)

⁵⁴ Jevons, 1875, s. 14.

⁵⁵ Newcomb, 1879, s. 229.; Ross, 1892, s.300.

⁵⁶ Jevons, 1875, s. 30.

⁵⁷ Jevons, 1875, ss. 30-40.

⁵⁸ Jevons, 1875, ss. 32-34.

1.2.4.2. Taşınabilirlik

Paranın kendiliğinden bir değere sahip olması yeterli değildir; ayrıca bu değer in ağırlık ve hacimle orantılı olması gerekmektedir; yani birim değer in değerli ya da değersiz şeylerin karşılığında kullanırken orantılı olması gerekir. Jevons'a göre paranın aynı anda hem ağırlık yapacak kadar değersiz ya da değerinden ötürü çok küçük olacak şekilde değerli olmaması gerekir. Paranın taşınabilir olması bir kişinin kayda değer miktarda parayı yanında taşıyabilme özelliğinin dışında yüksek miktarda parayı yakın ya da uzak mesafeye küçük ücretlerle transfer edebilme olanağı da sağlar⁵⁹.

1.2.4.3 Dayanıklılık

Sürekli sirkülasyon halinde olan ve uzun süre saklanabilen paranın bu durumları karşılayacak biçimde dayanıklı olması gerekmektedir. Jevons'a göre para tahrip edilemeyecek ölçüde dayanıklı olmalıdır⁶⁰.

1.2.4.4. Homojenlik

Parayı oluşturan materyalin homojen olması gerekmektedir, bunun sonucunda aynı birimde para her zaman aynı değeri taşıyacaktır. Bu nitelik, paranın hesap birimi olma işlevi ile yakından ilişkilidir⁶¹.

1.2.4.5. Bölünebilirlik

Homojenlik ile bağlantılı olarak bir paranın bölünebilir olması gerekmektedir. Paranın bölünebilir olması tek başına yeterli olmayıp, bölündükten sonra önceki durumuna göre değer kaybetmiyor olması da gerekmektedir. Paranın bu niteliğ i de homojenlik gibi hesap birimi olma işlevinin yerine getirilmesini sağlamaktadır.

⁵⁹ Jevons, 1875, ss. 34-36.

⁶⁰ Jevons, 1875, ss. 36-37.

⁶¹ Jevons, 1875, s. 37.

1.2.4.6. Deęerini Koruyabilmesi

Bir para kullanılırken deęerinde dalgalanmalar olabilir ve bu dalgalanmaların gerekleşmesi çoęunlukla istenmez. Bu durum Jevons'a göre özellikle bor sözleşmelerinde karřımıza çıkmaktadır. Paranın deęer kazanması ya da deęer kaybetmesi sonucu borlanan ya da bor verenin ilk duruma göre gereęinden fazla kazanç elde etmesi ya da zarar etmesi mümkün olabilir. Jevons'a göre "kazanan kaybedenin kaybettięi kadar kazanır" söylemi hatalıdır. Şöyle ki, bir paranın deęer kaybetmesi veya kazanması her zaman aynı etkiyi yaratmamaktadır. Örneęin birim deęeri 10 olan bir paranın %20 deęer kaybetmesi sonucu deęerinin 8'e düşmesi sonrası, tekrar 10 birim deęere ulaşması için bu sefer %25'lik bir artışın gerekeceęini söylemek mümkündür. %20'lik bir düşüş, kaybın önlenmesi için %25'lik bir yükseliş gerektirmektedir⁶².

1.2.4.7. Ayırt Edilebilirlik

Bir paranın dięer para ve eşyalardan kolaylıkla ayırt edilebilir olması gerekmektedir. Buradaki kolaylık, makul derecede bilgiye sahip bir kişinin parayı ayırt edebilmesi ölçüsündedir. Örneęin bir elmasın günlük kullanımda para olarak kullanılması bu sebepten ötürü çok zordur; çünkü sadece bu konuda belirli derecede uzman kişiler elmasın orijinallięini kavrayabilir. Ayırt edilebilirlik özellięi paranın üzerine konan bir damga ya da mühür ile sağlanabilmektedir⁶³.

⁶² Jevons, 1875, s. 38-39.

⁶³ Jevons, 1875, s. 40.

1.2.5. Para Türleri

1.2.5.1. Emtia Para

Emtia para (commodity money), paranın ilk ve temel görünümü kabul edilebilir⁶⁴. Bir emtia, tüketilmek ya da üretimde kullanılmak yerine ticaret için kullanılırsa yani mübadele aracı olarak kullanılırsa emtia para haline gelir⁶⁵. Emtia paralarda paranın değeri kendiliğinden, var olduğu maddeden gelir, mübadele aracı olmalarının yanında başka amaçlarla kullanılabilirler⁶⁶. Emtia paralar genellikle toplumlarda kıt olan şeylerin bir değer ölçüsü haline getirilmesidir.

Tarih boyunca çeşitli uygarlıklar çeşitli emtiaları para olarak kullanmıştır. Hayvan derisi, avcılık döneminde kullanılmaya başlanmış olup en eski emtia paralardandır⁶⁷. Pastoral göçebe dönemde ise değer ölçüsü için hayvanların (özellikle koyun ve sığırların) kullanıldığı bilinmektedir. Bu hayvanlar nakledilebilmelerindeki kolaylık, nakledilirken kendilerini taşıyabilmeleri, yıllarca saklanabilmeleri gibi birçok özelliğe sahip olmalarından ötürü kısmen paranın işlevlerini görmekteydiler. Özellikle Homeros'un birçok şiirinde öküzün bir değer ölçüsü işlevini yerine getirdiği görülmektedir⁶⁸. Latince para anlamına gelebilen "pecunia" kelimesinin sığır anlamına gelen "pecus" kelimesinden türemiş olması⁶⁹ bir diğer örnek olarak gösterilebilir⁷⁰. Bu dönemde köleliğin görüldüğü toplumlarda kölelerin de mübadele aracı olarak kullanıldığı bilinmektedir⁷¹. Antik İrlanda'da köle kızlar gemi, arazi, konut, hayvan gibi eşyalara karşılık bir ölçü olarak kullanılmıştır⁷².

⁶⁴ Lapavitsas, Costas. "Money and the Analysis of Capitalism: The Significance of Commodity Money." *Review of Radical Political Economics*, 2000/32 (4), s. 654. [https://doi.org/10.1016/S0486-6134\(00\)90004-4](https://doi.org/10.1016/S0486-6134(00)90004-4) (Erişim: 14.04.2022)

⁶⁵ Kiyotaki ve Wright, 1989, s. 929.

⁶⁶ Selgin, George. "Synthetic commodity money." *Journal of Financial Stability*, 2005/17, s. 92. <https://doi.org/10.1016/j.jfs.2014.07.002> (Erişim: 14.04.2022)

⁶⁷ Jevons, 1875, s. 20.

⁶⁸ Jevons, 1875, s. 21.

⁶⁹ <https://en.wiktionary.org/wiki/pecunia> (Erişim: 14.04.2022)

⁷⁰ Geva, Benjamin. "From Commodity to Currency in Ancient History--On Commerce, Tyranny, and the Modern Law of Money." *Osgoode Hall Law Journal*, 1987/25, s. 125. <https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1847&context=ohlj> (Erişim: 15.04.2022); Jevons, 1875, s. 22.

⁷¹ Jevons, 1875, s. 23; Weatherford, 2009, s.22.

⁷² Weatherford, 2009, s. 22.

İnsanlığın kişisel ss eřyalarına olan ilgisi belki de en ilkel tutkularдан biridir. Bu doęrultuda genellikle kk, saęlam materyallerden yapılmıř ve tařınması kolay bu eřyaların para iřlevini grmř olması kaınılmaz bir sonutur. Kuzey Amerika yerlilerin "wampum" adını verdikleri, beyaz ve siyah deniz kabuklarının birleřtirilmesiyle oluřturulan sslerin sıklıkla renklerine ve boyutlarına gre mbadele aracı olarak kullanıldıkları bilinmektedir. Hatta bu nesnelere bir para birimi olarak o kadar dzgn kullanılmaktaydı ki 1649 yılında Massachusetts Mahkemesi tarafından 40 řiline bedel olarak kullanılması kararlařtırılmıřtır⁷³

İnsanlığın yerleřik hayata gemesi ile tarım dneminde birok tarım rnnn dolařıma uygun yapısı sebebiyle mbadele aracı olarak kullanıldıęı grlmektedir. rneęin mısır, antik Yunanlardan bu yana Avrupa'nın birok kısmında para iřlevi grmektedir; hatta Norve'te mısırın bankalara yatırıldıęı, bor alırken ve verirken kullanıldıęı uygulamalara rastlanmaktadır. Bununla birlikte Akdeniz uygarlıklarının nemli bir kısmında (İyon adaları, Akdeniz'e kıyısı olan Anadolu ve Ortadoęu řehirleri), kalitesinin grecelięi, belirli bir sre bozulmadan durabilmesi ve blnebilir olması zelliklerine sahip zeytinyaęının para birimi olarak kullanıldıęı bilinmektedir⁷⁴.

Bununla birlikte Hindistan'da badem, Guetemala'da mısır, Babil ve Asurlular arpa, Moęollar ay tuęlalarını para olarak kullanmıřtır⁷⁵. Aztek uygarlıęında kakao ekirdekleri para olarak kullanılmaktaydı⁷⁶. Emtia paraların kendilięinden gelen deęerleri sayesinde Aztekler para olarak kullandıkları kakao ekirdeklerini isterlerse ezip kakao presi haline getirip yiyecek ve iecek haline getirip kazan elde edebilirlerdi⁷⁷.

Tarih boyunca yukarıda belirtildięi zere birok emtia para olarak kullanılsa da bunlar arasında en ok kullanılanı řphesiz deęerli madenlerdir (altın ve gmř). Metallerin saęlam olması, iřlenebilir olması grece kıtlıkları para olarak tercih edilmelerine yol amıřtır. zellikle kendilięinden gelen deęeri sayesinde altın, tarih boyunca deęeri korumakta bir istikrar kaynaęı haline gelmiřtir⁷⁸.

İlk madeni para basılmadan nce, deęerli metaller kleler halinde kullanılmaktaydı. zellikle ilk olarak Kapadokya blgesinde karřılařılan, klelerin

⁷³ Jevons, 1875, ss. 24-25.

⁷⁴ Jevons, 1875, ss. 25-26.

⁷⁵ Weatherford, 2009, s. 20.

⁷⁶ Weatherford, 2009, s. 17.

⁷⁷ Weatherford, 2009, s. 20.

⁷⁸ Taskinsoy, 2020, s. 11.

ağırlığına ve kullanılan metalin kalitesine güvence veren resmi mühürlerin basılması, madeni para modelinin öncüsü sayılabilir⁷⁹. Bununla birlikte basılan ilk madeni paraların, milattan önce 7. yüzyıla kadar ulaştığı düşünülen, Lidyalılar tarafından basılan elektron⁸⁰ alaşımı paralar olduğu kabul edilebilmektedir. İlk paranın Lidyalılar tarafından basıldığı kabulüne zaman zaman karşı argümanlar getirilse de paranın Lidyalılar tarafından kullanılmaya ve yayılmaya başlandığı konusunda bilim insanları neredeyse hemfikirdir⁸¹.

1.2.5.1.1. Uluslararası Para Sistemleri

Emtia paraların tarih boyunca yakın zamana kadar en baskın para türü olduğunu söylemek yanlış olmaz. Uluslararası para sistemlerinin değerli metaller çevresinde şekillenmiş olması bu duruma dayanaktır. Bu nedenler uluslararası para sistemleri emtia para başlığı altında incelenecektir. Uluslararası para sisteminin evreleri beş döneme ayrılabilir. Bunlar çift metal sistemi (bimetalizm), altın standardı, altın değişimi standardı, Bretton Woods sistemi ve dalgalı kur sistemidir⁸². Bunun yanında ilk olarak genellikle sınıflandırmaya katılmayan “gümüş standardı” incelenecektir.

1.2.5.1.1.1. Gümüş Standardı

Her ne kadar kabul edilen uluslararası para sistemi sınıflandırmasında altın standardı dönemi öncesi genellikle çift metal dönemi olarak varsayılsa da, gümüş standardı evresinin de var olduğu kabul edilebilmektedir⁸³. Gümüş standardı sisteminin başlangıcı, Sümerlere ya da antik Yunanlara⁸⁴ atfedilse de özellikle 16. yüzyılda Bolivya’da bulunan Cerro Rico dağı gümüş rezervlerinin İspanyol Krallığı tarafından

⁷⁹ Geva, 1987, s. 130.

⁸⁰ Altın-gümüş alaşımı.

⁸¹ Geva, 1987, s. 131.

⁸² Akdoğan, Ece Ceylan, “Uluslararası Para Sisteminin Geçmişi, Bugünü ve Geleceği”, *Çankaya Üniversitesi Hukuk Fakültesi Dergisi*, 2020/5 (1), s. 93
<http://earsiv.cankaya.edu.tr:8080/xmlui/bitstream/handle/20.500.12416/4711/Akdoğan%2C%20Ece%20C..pdf?sequence=1&isAllowed=y> (Erişim: 15.04.2022)

⁸³ Officer, Lawrence H., “Silver Standard”, In: Durlauf, S.N., Blume, L.E. (eds) *Monetary Economics*. The New Palgrave Economics Collection. Palgrave Macmillan, London., s. 357
https://doi.org/10.1057/9780230280854_38 (Erişim: 15.04.2022); Taskinsoy, 2020, ss. 13-15.; Friedman, Milton, “Bimetallism Revisited.” *The Journal of Economic Perspectives*, 1990/4 (4), s. 85
<http://www.jstor.org/stable/1942723> (Erişim: 16.04.2022)

⁸⁴ Officer, 2010, s. 358.

kazılmaya başlanmasıyla gündeme gelmiştir⁸⁵. Öyle ki, 16. Yüzyıl ile 18. Yüzyıl arasında Dünya'daki gümüş rezervlerinin %80'i bu dağdan çıkan gümüş ile karşılanmaktaydı⁸⁶. Gümüş standardının en bilinen kullanımı İspanyol Krallığı tarafından basılan İspanyol doları ile gerçekleşmiştir. Gümüş İspanyol doları, oldukça fazla kullanımı nedeniyle ilk uluslararası para olarak kabul edilebilmektedir. İspanyol doları, Birleşik Devletler tarafından çıkarılan para basma kanunu olan "The Coinage Act of 1792" ile birlikte ortaya çıkarılan Amerikan dolarının da kökenini oluşturmaktadır. Kanuna göre Amerikan doları İspanyol dolarına eşitlenerek basılmaya başlanmıştır. İspanyol doları 1857 yılına kadar⁸⁷ Birleşik Devletler'de yasal para olarak kullanılmıştır.

1.2.5.1.1.2. Çift Metal Sistemi

Yukarıda açıklandığı üzere, uluslararası para sistemi sınıflandırmasında altın standardı dönemi öncesi çoğunlukla çift metal sistemi olarak kabul edilmektedir. Çift metal sisteminde iki metalin (çoğunlukla altın ve gümüş) aynı anda para olarak dolaşımda olması söz konusudur. Çift metal sisteminde uluslararası ödemelerde altın ve gümüşün kullanılmakta, kurlar da söz konusu altın ve gümüş paraların içerdiği altın ve gümüş miktarlarıyla belirlenmekteydi⁸⁸. Bununla birlikte zamanla paralardaki değerli maden miktarlarında oynamalar söz konusu olmuştur. Bu tür gelişmeler "Gresham yasası" olarak bilinen bir duruma yol açmıştır. Gresham yasası 1858 yılında Henry Dunning Macloed tarafından, I. Elizabeth'in mali danışmanı Sir Thomas Gresham'a atfedilerek ortaya atılmıştır. Macloed'un Gresham yasasına göre iyi para ve kötü para aynı anda dolaşımda olamazlar⁸⁹; kötü para, iyi parayı kovar⁹⁰; fakat iyi para kötü parayı kovamaz⁹¹. Ayrı düşürülen paralar kullanılmak için tercih edilirken ayarı yüksek paralar saklanma eğilimine maruz kalır.

⁸⁵ Taskinsoy, 2020, s. 13.

⁸⁶ https://en.wikipedia.org/wiki/Cerro_Rico (Erişim: 15.04.2022)

⁸⁷ Bkz. The Coinage Act of 1857.

⁸⁸ Akdoğan, 2020, s. 93.

⁸⁹ Macleod, Henry Dunning, The Elements of Political Economy, 1858, ss. 475-476, https://books.google.com.tr/books?hl=tr&lr=&id=sA8ZAAAAYAAJ&oi=fnd&pg=PA1&dq=Henry+Dunning+Macleod&ots=THnYsyvQo8&sig=1s61jFp_K7wwgxbH1Z1fz9jJWq4&redir_esc=y#v=onepage&q=gresham&f=false (Erişim: 16.04.2022)

⁹⁰ Giffen, Robert. "The Gresham Law." *The Economic Journal*, 1891/1 (2), s.304, <https://doi.org/10.2307/2956251> (Erişim: 16.04.2022)

⁹¹ Jevons, 1875, s. 81.

Çift metal sistemi ile ilgili olarak açıklanması gereken bir diğer kavram “paraşüt teorisi”dir. Paraşüt teorisine göre iki metalin birlikte kullanıldığı sistemlerde, metallere birinin arzındaki artış, azalma ya da arz şoku gibi durumlarda diğer metal fiyat ya da piyasa istikrarını sağlamak için bir “paraşüt” görevi görecek⁹². Paraşüt teorisi Türkçe literatürde hatalı bir şekilde sıklıkla Leon Walras’a atfedilse de, bu yaygın kanının aksine teoriyi ilk kez ortaya koyan Michel Chevalier’dir⁹³. Paraşüt teorisi Chevalier’den sonra Louis Wolowski tarafından da açıklanmıştır⁹⁴. Teori daha sonra, kendisini sıkı bir monometalist olarak tanımlayan⁹⁵ (literatürde hatalı bir şekilde “bimetalizm savunucusu” olarak bahsedilebilse de) Leon Walras tarafından kullanılmıştır. Walras’a göre altın standardı geçerli olmalıdır; bununla beraber altının fiyatında gerçekleşebilecek istikrarsızlıkları dengelemek için gümüşten faydalanılacaktır⁹⁶. Walras’a göre altının

⁹² Asadov, Alam, Mansur Masih, “Reversal of monetary history: Is return to trimetalism a viable alternative?”, 2016, ss. 8-9.

https://www.researchgate.net/publication/319814437_Reversal_of_monetary_history_Is_return_to_trimetalism_a_viable_alternative (Erişim: 17.04.2022); Laidler, David, *The Golden Age of the Quantity Theory*, Princeton University Press, 1991, ss. 30-31.

https://books.google.com.tr/books?id=tLgABAAAQBAJ&printsec=frontcover&dq=The+Golden+Age+of+the+Quantity+Theory&hl=tr&sa=X&redir_esc=y#v=onepage&q&f=false (Erişim: 17.04.2022); Laidler, David, “Rules, Discretion and Financial Crises in Classical and Neoclassical Monetary Economics”, *Economic Issues*, 2002/7 (part 2), s. 20.

https://www.researchgate.net/publication/237137945_Rules_Discretion_and_Financial_Crises_in_Classical_and_Neoclassical_Monetary_Economics (Erişim: 17.04.2022); Ljungberg, Jonas, Anders Ögren, “Discipline or international balance: the choice of monetary systems in Europe”, *The European Journal of the History of Economic Thought*, 2021, s.6 <https://doi.org/10.1080/09672567.2021.1946121> (Erişim: 17.04.2022); Pender, Michael, Andreas Resch, *Schumpeter's Venture Money*, Oxford University Press, 2021, s. 76

https://books.google.com.tr/books?id=qrwcEAAAQBAJ&pg=PA76&dq=michel+chevalier+parachute+effect&hl=tr&sa=X&ved=2ahUKEwi02cXM9Jr3AhWER_EDHTEuBi8Q6AF6BAgHEAI#v=onepage&q=michel%20chevalier%20parachute%20effect&f=false (Erişim: 17.04.2022)

⁹³ Chevalier, Michel, *On the Probable Fall in the Value of Gold*. D. Appleton and Company, 1859, ss. 5, 74, 162. <https://oll.libertyfund.org/title/cobden-on-the-probable-fall-in-the-value-of-gold> (Erişim: 17.04.2022); Flandreau, Marc, *The Glitter of Gold: France Bimetallism and the Emergence of the International Gold Standard 1848-1873*, Oxford University Press, 2003, s. 158.

<https://books.google.com.tr/books?id=Uw5REAAAQBAJ&pg=PA158&dq=chevalier+parachute+theory&hl=tr&sa=X&ved=2ahUKEwiMofzm3pr3AhUgRvEDHU7oB4sQ6AF6BAgKEAI#v=onepage&q=chevalier%20parachute%20theory&f=false> (Erişim: 17.04.2022); Jevons, William Stanley, *A Serious Fall in the Value of Gold Ascertained: And Its Social Effects Set Forth*, 1863, s. 37.

https://books.google.com.tr/books?id=4IcBAAAQAQAJ&printsec=frontcover&dq=A+serious+fall+in+the+Value+of+Gold+ascertained,+and+its+social+effects+set&hl=tr&sa=X&redir_esc=y#v=onepage&q&f=false (Erişim: 17.04.2022); Laidler, 2002, s. 30.; Laidler, David. “British Monetary Orthodoxy in the 1870.” *Oxford Economic Papers*, 1988/40 (1), s.96, <http://www.jstor.org/stable/2663255> (Erişim: 17.04.2022); Pender ve Resch, 2021, s. 76.

⁹⁴ Ljuberg ve Ögren, 2021, s.6.

⁹⁵ Cirillo, Renato, “Leon Walras’ Theory of Money.” *The American Journal of Economics and Sociology*, 1986/45 (2), s. 216. <http://www.jstor.org/stable/3486926> (Erişim: 17.04.2022)

⁹⁶ Friedman, 1990, s. 95.

arzında yükseliş ya da düşüş olduğunda gümüş miktarı düşürülüp arttırılarak fiyatlar stabil tutulabilecektir⁹⁷. Walras'ın ortaya attığı bu sistem “gümüşle düzenlenmiş altın standardı” olarak adlandırılabilir⁹⁸.

Paraşüt teorisi, çift metal sistemini tek metal sistemine (çoğunlukla altın standardı) karşı avantajlı bir konuma sokar. Özellikle 19. yüzyılın ortalarında keşfedilen altın rezervlerinin (özellikle Avustralya altın madenleri) altın fiyatlarını düşürme eğilimine götürmesine⁹⁹ rağmen, çift metal sistemini benimseyen Fransa tarafından fiyatların başarıyla stabil tutulabilmesi bu teorinin en iyi örneklerindedir¹⁰⁰.

19. yüzyılın özellikle ikinci yarısında çift metal sisteminden vazgeçilerek altın standardına geçiş söz konusu olmuştur.

1.2.5.1.1.3. Altın Standardı

Altın standardı, ülkelerin kendi para birimlerinin belirli bir miktar altına eşitlenmesi ile söz konusu olmaktadır; para belirlenmiş oranlarda altına dönüştürülebilmektedir¹⁰¹. Altın standardı sisteminin ilk uygulamaları Büyük Britanya tarafından gerçekleştirilmiş olup 18. yüzyılın başına denk gelmektedir. 1704 yılında Kraliçe Anne tarafından yayınlanan bildiri ile Batı İngiliz Adaları'nda altın standardı sistemine geçilmeye çalışılmış olursa da sistem, o dönemde oldukça baskın bir şekilde kullanılan gümüş İspanyol doları karşısında başarısız kalmıştır¹⁰². Ardından 1717 yılında Kraliyet Darphanesi'nin (Royal Mint) başında¹⁰³ olan Sir Isaac Newton tarafından gümüşten altına geçiş oranının güncellenmesiyle ile Büyük Britanya “istenmeden” de olsa fiili olarak (de facto) altın standardı sistemine geçmiştir¹⁰⁴. Newton, altın paranın gümüş değerini 21 şiline eşit olacak şekilde uyarlamıştı. Bu durumda Büyük

⁹⁷ Leon Walras'tan akt. Cirillo, 1986, s. 216.

⁹⁸ Fisher, 1922, s. 183.

⁹⁹ Jevons, 1875, s. 135.

¹⁰⁰ Asadov ve Masih, 2016, s.9.; Flandreau, 2003, s. 158.; Jevons, 1875, s. 139.; Laidler, 1988, s. 96; Ljunberg ve Ögren, 2021, s. 7.

¹⁰¹ Bordo, Michael D., Gold Standard, <https://www.econlib.org/library/Enc/GoldStandard.html> (Erişim: 16.04.2022)

¹⁰² Taskinsoy, 2020, s. 15.; https://en.wikipedia.org/wiki/British_West_Indies_dollar (Erişim: 16.04.2022)

¹⁰³ İng. Master of the Mint.

¹⁰⁴ Cooper, Richard N. vd., “The Gold Standard: Historical Facts and Future Prospects.” *Brookings Papers on Economic Activity*, 1982/1, s. 3, <https://doi.org/10.2307/2534316> (Erişim: 16.04.2022); Fay, C. R. “Newton and the Gold Standard.” *Cambridge Historical Journal*, 1935/5 (1), s. 110, <http://www.jstor.org/stable/3020836> (Erişim:16.04.2022)

Britanya'daki altının fiyatı, diğer ülkelere göre olması gerekenden daha pahalı hale gelmiştir. Bunun sonucunda Britanyalı tüccarlar ithalatta ödemeleri gümüş ile yaparken, ihracatta ücreti altın olarak almaya başladılar. Bu durumu Adam Smith kısaca şu şekilde özetlemiştir:

...Dışarıda gümüş ile ülkemize göre daha çok altın alınabileceği için dışarıya gümüş gönderip, karşılığında altın getirilip, getirilen altınlar ile dışarıya göre ülkemizde daha çok gümüş alınması sağlanmıştır. Bu döngü devam ettikçe dolaşımdaki gümüş para miktarı giderek azalır altın para miktarı giderek artmıştır.¹⁰⁵

Sonuç olarak dolaşımda neredeyse sadece altın paranın kalması ile Büyük Britanya fiili olarak altın standardı sistemine geçen ilk ülke olmuştur. Bununla birlikte altın standardına yasal olarak (de jure) geçen ilk ülke de Büyük Britanya'dır. Doktrinde Büyük Britanya'nın altın standardına geçişinin başlangıcı hakkında farklı kabuller bulunmaktadır. İlk olarak altın standardına geçişin 1816 tarihinde çıkarılan "The Coinage Act 1816" ile, gümüş paranın artık temsili para olarak kabul edilmesi, yasal para olarak kullanımının çok düşük limitler ile sınırlandırılması¹⁰⁶ ve İngiliz pound'u değerinin altın karşılığının ifade edilmeye başlanması reformları altın standardının başlangıcı olarak kabul edilebilmektedir¹⁰⁷. Ardından 1819 yılında Avam Kamarası'nda onaylanarak yasalanan "1819 Act for the Resumption of Cash Payments" ile Bank of England'a nakit paranın belirli bir oranda altın ile dönüşümü yetkisini vermesi de altın standardının başlangıcı olarak kabul edilebilmektedir¹⁰⁸. Son olarak 1819 tarihli kanunun Bank of England'a verdiği yetki fiili olarak 1821 tarihinde kullanılmaya başlandığından¹⁰⁹, 1821 tarihi de bir kısım yazarlar tarafından Büyük Britanya'da altın standardının başlangıcı olarak kabul edilmektedir¹¹⁰.

¹⁰⁵ Adam Smith'ten akt. Fay, 1935, s. 112.

¹⁰⁶ Redish, Angela. "The Evolution of the Gold Standard in England.", *The Journal of Economic History*, 1990/50 (4), ss. 801-802, <http://www.jstor.org/stable/2122455> (Erişim: 17.04.2022)

¹⁰⁷ Cooper, 1982, s. 3.; Redish, 1990, s.789.

¹⁰⁸ Bordo; Crosby, Mark, "Currency Unions, Currency Boards and Other Fixed Exchange Rate Arrangements", *The Australian Economic Review*, 2001/34 (3), s. 367. <http://neyapti.bilkent.edu.tr/Readings/CU-CB.pdf> (Erişim: 17.04.2022)

¹⁰⁹ World Gold Council, Key documents in the history of gold, s. 130 <https://www.gold.org/sites/default/files/documents/1819may21.pdf> (Erişim: 17.04.2022)

¹¹⁰ Akdoğan, 2020, s. 94.; Bordo, Michael D., Anna J. Schwartz, A Retrospective on the Classical Gold Standard, 1821-1931, University of Chicago Press, 1984, s.1 <http://www.nber.org/books/bord84-1> (Erişim: 17.04.2022); Royal Mint, What was the Gold Standard?, <https://www.royalmint.com/invest/discover/gold-news/what-was-the-gold-standard/> (Erişim: 17.04.2022)

Her ne kadar altın standardına geçen ilk ülke Büyük Britanya olsa da, uluslararası para sistemi olarak altın standardı döneminin başlangıcı genellikle birçok ülkenin art arda bu sisteme geçmeye başladığı 1870'ler kabul edilmektedir¹¹¹. 1871'de Almanya, 1873'te Birleşik Devletler, 1878'de Fransa, 1895'te Japonya altın standardına geçiş yapan ülkelerdir¹¹². 1870'lerden I. Dünya Savaşı'nın başına kadar süren bu evre "klasik altın standardı dönemi" olarak adlandırılmaktadır.

1.2.5.1.1.4. Altın Değişimi Standardı

1925 ile 1931 yılları arasındaki bu dönem "iki savaş arası dönem" olarak da adlandırılabilir¹¹³. Bu dönem Büyük Britanya'nın altın standardına tekrar geçtiği 1925 yılından, altın standardından ayrıldığı 1931 senesine kadar sürdüğü kabul edilmektedir¹¹⁴.

I. Dünya Savaşı'nın ardından rezerv sorunlarıyla karşılaşmışlardır. Ülkeler tekrar altın standardına geçmek isteseler de altın stoku kıtlığı çekmekteydiler, altın değişim oranları sabitliğini yitirmiş bulunmaktaydı¹¹⁵. Bunun sonucunda 1922 yılında yapılan Cenova Konferansı'nda en çok tartışılan konu altın standardına tekrar dönmektir. Konferansta altın değişim standardına geçiş önerilmiştir¹¹⁶. Bu doğrultuda ülkeler altın standardına dönebilmek için rezervlerini tamamen altın ile doldurmaya çalışmak yerine, altın standardını sağlamış ülkeler olan Büyük Britanya ve Birleşik Devletler'in para birimleri olan ve altın ile dönüşümü mümkün sterlin ve doları altın ile beraber tutmaya başlamışlardır¹¹⁷. Fakat bu sahte¹¹⁸ altın standardı sistemi kısa sürmüştür; 1929 Buhran'ı ve sterlin üzerindeki spekülasyon hareketleri¹¹⁹ nedeniyle 1931 yılında önce Britanya'nın

¹¹¹ Akdoğan, 2020, s. 94.

¹¹² Taskinsoy, 2020, s. 15.

¹¹³ Cooper, 1982, s. 19; Akdoğan, 2020, s. 95.

¹¹⁴ Wandschneider, Kirsten. "The Stability of the Interwar Gold Exchange Standard: Did Politics Matter?", *The Journal of Economic History*, 2008/68 (1), s. 151., <http://www.jstor.org/stable/40056779> (Erişim: 17.04.2022); 1982, ss. 19-20; Taskinsoy, 2020, s. 16.

¹¹⁵ Wandschneider, 2008, s. 152.

¹¹⁶ Igwe, Isaac O.C., "History of the International Economy: The Bretton Woods System and its Impact on the Economic Development of Developing Countries", *Athens Journal of Law*, 2018/4 (2), s. 109. <https://www.athensjournals.gr/law/2018-4-2-1-Igwe.pdf> (Erişim: 18.04.2022)

¹¹⁷ Cooper, 1982, s.19.; Taskinsoy, 2020, s. 16.

¹¹⁸ Akdoğan, 2020, s. 96.

¹¹⁹ Taskinsoy, 2020, s. 16.

ardından 1933 yılında Birleşik Devletler’in altın standardı sisteminden vazgeçmesi nedeniyle altın değişim standardı da sona ermiştir¹²⁰.

1.2.5.1.1.5. Bretton Woods Sistemi

I. Dünya Savaşı sonrası kurulmaya çalışılan uluslararası para sisteminin başarısız olması, ardından II. Dünya Savaşı’nın gerçekleşmesi Büyük Britanya ve Birleşik Devletler’i bir savaş sonrası para sistemi oluşturmaya itmiştir¹²¹. Bu doğrultuda 1944 yılında Bretton Woods kasabasında toplanan 44 ülke temsilcisi Bretton Woods Anlaşması’nı imzalamıştır. Konferansa katılan ülkelerin paylaştığı ortak görüş, iki Dünya Savaşı arasında yaşanan uluslararası ekonomik istikrarsızlığın tekrar yaşanmamasıydı¹²².

Konferans kapsamında yeni bir para sistemi için iki farklı model teklif edilmiştir. Bunlar Büyük Britanya’yı temsilen John Maynard Keynes tarafından ve Birleşik Devletler’i temsilen Harry Dexter White tarafından önerilen plandır.

Keynes planı “Uluslararası Takas Birliği [International Clearing Union (ICU)]” kurulmasını öngörmekteydi. ICU, merkez bankalarının ticari bankalar için tuttuğu hesaplara benzer bir şekilde merkez bankaları için hesap tutmaktaydı¹²³. Bu hesaplar uluslarüstü bir para birimi olacak “bancor” ile işleyecekti. Bancor’un değeri altın ile tanımlanacaktı fakat Birlik isterse bunu sonradan değiştirebilecekti¹²⁴. Üye ülkeler altın karşılığında bancor elde edebilecek fakat bancor’u altına dönüştüremeyecekti¹²⁵. Her ülke belirlenen limitler dâhilinde borçlanabilecekti; tutulan hesaplar özel borçlanmalardan ziyade kredili mevduat hesabı şeklinde işleyecekti¹²⁶. Keynes planında White planının

¹²⁰ Cooper, 1982, s. 20.

¹²¹ Igwe, 2018, s. 111.

¹²² Erdem, Mete, “BRICS Koşullu İhtiyat-Fonu Düzenlemesi: Hukuksal ve Kurumsal İnceleme”, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 2016/7 (1), s. 300. <https://doi.org/10.21492/inuhfd.387923> (Erişim: 02.07.2022)

¹²³ de Vries, Margaret Garritsen, *The IMF in a Changing World, 1945-85*, International Monetary Fund, 1986, s. 7. <https://www.elibrary.imf.org/view/books/071/07050-9780939934652-en/07050-9780939934652-en-book.xml> (Erişim: 02.06.2022)

¹²⁴ de Vegh, I. “The International Clearing Union.”, *The American Economic Review*, 1943/33 (3), s. 536. <http://www.jstor.org/stable/1812989> (Erişim: 18.04.2022)

¹²⁵ de Vries, 1986, s. 7.

¹²⁶ Iwamoto, Takekazu. “The Keynes Plan for an International Clearing Union Reconsidered.”, *Kyoto University Economic Review*, 1995/65 (2), s. 31, <http://www.jstor.org/stable/43217486> (Erişim: 18.04.2022); de Vries, 1986, s. 7.

aksine hesaplara para yatırma söz konusu değildi; bunun yerine ödeyen ve ödeme alan ülkenin hesapları borçlandırılır ya da kredilendirilirdi¹²⁷.

White planı ise bir “Uluslararası İstikrar Fonu [International Stabilization Fund (ISF)]” öngörmekteydi¹²⁸. Fon’un değişim oranlarında istikrar sağlama, üretken sermayenin ülkeler arasında akışını sağlama gibi amaçları bulunmaktaydı¹²⁹. White planında Fon’un para birimi olarak “unitas” adı verilen ve $137\frac{1}{7}$ grain saf altına (\$10) eşit değerinde bir para birimi önerilmekteydi¹³⁰.

Her iki planın da bazı benzerlikleri ve farklılıkları bulunmaktaydı. İlk olarak White modelinin tamamıyla Keynesyen bir model olduğunu söylemek mümkün değilse de White’ın Keynesyen olduğu bilinmekle¹³¹ birlikte iki planın da Keynesyen yaklaşımdan etkilendiği söylenebilir.

Her iki plan da yeni bir para birimi oluşturulmasını öngörmekteyken; Keynes’in bancor’u bağımsız değerinde, uluslarüstü, yeni bir para birimiyken White’ın unitas’ı sadece 10 doları söylemenin farklı bir yolu¹³². Bancor hem mübadele aracı hem de rezerv para birimi olma özelliği gösterirken unitas sadece bir hesap birimiydi¹³³.

White planında ülkelerin ücretli üyeliğe benzer bir şekilde¹³⁴ Fon’a para yatırması gerekiyorken Keynes planında böyle bir gereklilik yoktu; sistem kredi temelli çalışmaktaydı¹³⁵. Planlardaki bu farklılığın Amerikan bankalarındaki mevduat hesabı prensibi ile Britanya bankalarındaki kredi prensibine benzerlik göstermesi tesadüf değildir¹³⁶.

¹²⁷ De Vries, 1986, s. 7.; Iwamoto, 1995, s. 31.; Williams, John H., “Currency Stabilization: The Keynes and White Plans.”, *Foreign Affairs*, 1943/21 (4), s. 648. <https://doi.org/10.2307/20029784> (Erişim: 18.04.2022)

¹²⁸ Iwamoto, 1995, s. 23.

¹²⁹ de Vegh, 1943, s. 554.; de Vries, 1986, ss 7-8.

¹³⁰ de Vegh, 1943, s. 556.; . IMF History Volume 3 (1945-1965). USA: International Monetary Fund, 1996., s. 87. <https://doi.org/10.5089/9781451972511.071> (Erişim: 18.04.2022)

¹³¹ Boughtan, James M., Why White, Not Keynes? Inventing the Post-War International Monetary System, International Monetary Fund, 2002, ss. 5-6. <https://www.imf.org/external/pubs/ft/wp/2002/wp0252.pdf> (Erişim:19.04.2022)

¹³² Amato, Massimo, Luca Fantacci, “Back to which Bretton Woods? Liquidity and clearing as alternative principles for reforming international money”, *Cambridge Journal of Economics*, 2014/38 (6), ss. 5-6. https://www.researchgate.net/publication/228461779_Back_to_which_Bretton_Woods_Liquidity_and_clearing_as_alternative_principles_for_reforming_international_money (Erişim: 19.04.2022); Iwamoto, 1995, s. 31.

¹³³ Iwamoto, 1995, s. 33.

¹³⁴ de Vries, 1986, s. 8.

¹³⁵ Williams, 1943, s. 648.

¹³⁶ Williams, 1943, s. 648.

Yine her iki planın da altın standardının farklı bir varyantı olduğu söylenebilir¹³⁷.

44 ülkenin katılımıyla sonuçlanan konferansta White'ın planı daha baskın çıkararak anlaşmaya varılmıştır. Konferans yeni bir uluslararası para sisteminin doğmasına sebep olmuştur. Konferansın sonucunda “Uluslararası Para Fonu [International Monetary Fund (IMF)]” ve “Uluslararası İmar ve Kalkınma Bankası [International Bank for Reconstruction and Development (IBRD)]” kurulmuştur.

Bretton Woods sistemi, üye devletlerinin para birimlerini değiştirebilmesini garanti eden, Amerikan dolarına bağlı ayarlanabilir bir kambiyo rejimi görünümündedir¹³⁸. Bretton Woods sisteminin ortaya koyduğu kurallar; döviz kurlarının istikrarının sağlanması, döviz denetimi ve ithal kısıtlamalarının kaldırılması, yeterli uluslararası likiditenin sağlanması olarak belirtilebilir¹³⁹. Sistem ayarlanabilir sabit kur üzerinden işlemektedir. Sisteme göre Birleşik Devletler dışındaki bütün ülkeler para birimlerini dolara endekslemiş, Amerikan doları da altına sabitlemiştir. Sistemin bu nedenle “dolara dayalı altın standardı” olarak adlandırılabilmesi mümkündür¹⁴⁰. Sistem, altın standardı ve altın değişim standartlarının bir sentezi¹⁴¹, altın değişim standardının seyreltilmiş hali¹⁴² ya da altın standardının zayıf bir varyantı¹⁴³ olarak değerlendirilebilmektedir.

Bretton Woods sisteminin sağladığı altına ve dolara dönüşülebilirlik efektif olarak sadece 1959'dan 1968'e kadar işleyebilmiştir¹⁴⁴. Ardından 1971 yılında Birleşik Devletler tarafından uluslararası işlemlerde belirlenen kur üzerinden altın alım satımının desteklenmesine son verilmesi, altına dönüşülebilirliği kaldırmasıyla Bretton Woods sistemi fiilen çökmüştür¹⁴⁵.

¹³⁷ Akdoğan, 2020, s. 97.; Williams, 1943, ss. 649,651.

¹³⁸ Erdem, 2016, ss. 301-302.

¹³⁹ Öztürk, Nazım, "İMF'nin Değişen Rolü ve Gelişmekte Olan Ülke Ekonomilerine Etkileri", *Ankara Üniversitesi SBF Dergisi*, 2002/57, ss. 100-101 <https://dergipark.org.tr/tr/pub/ausbf/issue/3098/42876> (Erişim: 19.04.2022)

¹⁴⁰ Akdoğan, 2020, s. 97.

¹⁴¹ Taskınoy, 2020, s. 18.

¹⁴² Igwe, 2018, s. 118.

¹⁴³ Bordo vd., "Gold, Fiat Money, and Price Stability." *B.E. Journal of Macroeconomics: Topics in Macroeconomics* 7, 2007, s. 5. <https://www.nber.org/papers/w10171> (Erişim: 20.04.2022)

¹⁴⁴ Taskınoy, 2020,

¹⁴⁵ Akdoğan, 2020, s. 100.; Erdem, 2016, s. 304.

1.2.5.1.1.6. Dalgalı Kur Sistemi

Altın döviz standardına son verildikten sonra dolar serbest piyasada dalgalanmaya bırakılmıştır¹⁴⁶. 1973 yılında bazı Avrupa ülkelerinin ulusal paralarını dolara karşı dalgalanmaya bıraktıklarını beyan etmeleri ile Dalgalı Kur Sistemi'ne geçilmiştir¹⁴⁷. Dalgalı kur sisteminde kurlar piyasa güçlerince serbest piyasa tarafından belirlenir.

Uluslararası para sistemleri incelenirken görüldüğü üzere para sistemleri değerli metaller çevresinde şekillenmiştir. Bu durum yukarıda belirtildiği üzere en çok bilinen emtia paralar olan değerli metaller (özellikle altın) üzerinden şekillenmiştir. Emtia paraların kullanımı azalsa da hiçbir zaman tamamen kaybolmamış; ticari ve ekonomik hayatın normal akışının kesintiye uğradığı zamanlarda tekrar ortaya çıkmıştır.

1.2.5.2. Temsili Para

Temsili para (representative money) kavramı Jevons tarafından ortaya atılmıştır¹⁴⁸. Temsili para kısaca kendi değeri neredeyse hiç olmayan, başka bir değeri temsil eden paradır. Temsili paranın en iyi örnekleri üzerinde ne kadar altın ya da gümüşü temsil ettiğini belirten banknotlardır. Banknotlar istenildiği zaman üzerinde yazan altın ya da gümüş ile değiştirilebiliyordu.

Temsili paraların kullanım sebebi genellikle değerli madenleri taşıma riski ya da külfeti altında kalmamak kabul edilebilir. Bununla birlikte özellikle Avrupa'da temsili paranın ortaya çıkması; tüccarların ödemelerde her seferinde farklı şekil, ağırlık, saflıkta olabilen ya da kısmen zarar görmüş paraları kontrol etme zahmetine katlanması sorununa çözüm olarak gerçekleşmiştir¹⁴⁹.

1.2.5.3. İtibari Para

İtibari para (fiat money) günümüzde en çok kullanılan para türüdür. Günlük hayatta para kelimesi telaffuz edildiğinde kastedilen itibari paradır.

¹⁴⁶ Öztürk, 2002, s. 108.

¹⁴⁷ Akdoğan, 2020, s. 104.

¹⁴⁸ Jevons, 1875, s. 194.

¹⁴⁹ Jevons, 1875, ss. 199-200.

İtibari paraların kendiliğinden bir değeri yoktur ve başka bir emtiaya dönüştürülemezdir¹⁵⁰. İtibari paraların bu anlamlarıyla 1971 yılında Birleşik Devletler başkanı Nixon'ın kendi deyimiyle “altın penceresini kapatma¹⁵¹”sıyla tam olarak geçerli hale geldiğini söylemek mümkündür.

İtibari paraların tarihteki ilk görünümünün ne olduğu konusunda farklı görüşler bulunmaktadır. Bu görüşler arasında belki de en ilginç, Pasifik Okyanusu'nun güneyinde bulunan Yap Adası'nda kullanılan, “Rai” adı verilen ortası delik, yerinden oynatılamayacak kadar büyük ve ağır yuvarlak taşların ilk itibari para olduğudur. Keynes, Friedman, Tobin ve Mankiw gibi birçok ekonomist açık bir şekilde ya da ima ederek bu taşların ilk itibari para örneği olduğunu söylemektedirler¹⁵². Her ne kadar bu taşların itibari para gibi çevrilemez olmaları ve kullanım değerlerinin olmamaları söz konusuysa da itibari para olarak değerlendirilmekten ziyade itibari para ile emtia para arasında bir görünüm arz ettiklerini kabul etmek daha doğru olacaktır. Bu doğrultuda itibari paraların ilk kez, geçtiğimiz milenyumun başında Çin tarafından kullanılmaya başlandığı söylenebilir¹⁵³. Kullanılan bu kağıt paralar başlangıçta altın, gümüş gibi emtialara çevrilebilir özellik taşıyorsa da uygulamada çoğunlukla çevrilmemekteydi. Bu durum başlangıçta bir tercih iken sonraları gereğinden fazla kağıt para basılması nedeniyle çevrilebilirlik mümkün olmamaya başlaması ile birlikte¹⁵⁴ belirli bir sürenin ardından Hanedanlık tarafından da yasaklanmıştı. Bu nedenle Çin kağıt paraları itibari para olarak değerlendirilebilir.

İtibari paralar, altına ya da değerli metale “çevrilememeleri” özellikleri nedeniyle, literatürde ilk olarak “çevrilemez kağıt para (inconvertible paper money)” olarak ifade edilebilmekteydi¹⁵⁵. Çevrilemez kağıt para, itibari parayı ve çevrilebilir olup belirli bir süreliğine bu özelliğini kaybetmiş paraları kapsayacak şekilde kullanılmaktaydı¹⁵⁶. Örneğin Jevons tarafından Bank of England tarafından basılan banknotlar 1797 yılında

¹⁵⁰ Goldberg, Dror, “Famous Myths of ‘Fiat Money.’”, *Journal of Money, Credit and Banking*, 2005/37 (5), s. 957. <http://www.jstor.org/stable/3839155> (Erişim: 20.04.2022)

¹⁵¹ Bordo vd., 2007, s. 5.

¹⁵² Akt. Goldberg, 2005, s. 959.

¹⁵³ Jevons, 1875, ss. 197-198.

¹⁵⁴ Hozumi, Fumio. “The Characteristics Of The History Of Chinese Money.” *Kyoto University Economic Review*, 1954/24 (2), ss. 20,29. <http://www.jstor.org/stable/43217017> (Erişim: 20.04.2022)

¹⁵⁵ Jevons, 1875, s. 234.

¹⁵⁶ Jevons, 1875, ss. 234-235.; Brinton, Crane. “The History of Paper Money to the War.”, *The Journal of Modern History*, 1934/6 (3), s. 308. <http://www.jstor.org/stable/1871279> (Erişim: 21.04.2022)

çevrilebilirliğine yasaklanmasından tekrar açılmasına kadar geçen sürede çevrilemez kağıt para olarak değerlendirilmiştir¹⁵⁷. 1826 yılından 1881 yılına kadar Arjantin’de kullanılan çevrilebilirliği olmayan “peso moneda corriente”, itibari paranın en bilinen erken örneklerindendir¹⁵⁸.

İtibari paraların yukarıda değinildiği üzere kendiliğinden değerleri bulunmamaktadır. Bu nedenle kimi zaman “değersiz para” olarak adlandırılabilmektedir¹⁵⁹. İtibari paranın bunun yerine “yasal” değerleri bulunmaktadır. Bu değer hükümetler ve/veya yasalar ile tanınır¹⁶⁰.

1.2.5.4. Dijital Para

Gerek literatürde gerek sosyal yaşamda “dijital para”, “sanal para”, “elektronik para” ve “kripto para” kavramları birbirleri yerine kullanılmaktadır. Terminolojik ve taksonomik bir kargaşanın henüz tam olarak çözülemediği görülmektedir. Bu doğrultuda çalışmanın bu başlığında her ne kadar dijital para, para türleri içerisinde konumlanırsa da bu durumun öncelikli olarak dijital parayı bir para türü olarak konumlandırmaktan ziyade kavram kargaşasının ortaya konması gerekliliğinden ötürü olduğunu belirtmekte yarar vardır. Yine de bu çalışmada dijital paranın kapsayıcı bir kavramdan ziyade elektronik para, sanal para ve kripto para gibi farklı bir para türü olarak ele alınabileceği literatürdeki bir kısım çalışmalar ile desteklenerek kabul edilmektedir.

Dijital paranın literatürde çoğunlukla kapsayıcı bir kavram olarak kullanıldığı görülmektedir. Kısaca dijital olarak değer temsil eden her şey dijital para olarak adlandırılabilmektedir. Bununla birlikte dijital paranın kripto para ve sanal parayı kapsayacak fakat elektronik parayı dışlayacak şekilde tanımlandığı da görülmektedir. Bu durum çeşitlendirilebilmekle birlikte aşağıda bazı ulusal/uluslararası kuruluşların dijital parayı nasıl tanımladığı incelenecektir.

¹⁵⁷ Jevons, 1875, ss. 234-235.

¹⁵⁸ Irigoin, Maria Alejandra. “Inconvertible Paper Money, Inflation and Economic Performance in Early Nineteenth Century Argentina.”, *Journal of Latin American Studies*, 2000/32 (2), <http://www.jstor.org/stable/158568> (Erişim: 21.04.2022); Jevons, 1875, s. 234.

¹⁵⁹ Lapavitsas, 2000, s. 631.

¹⁶⁰ Brinton, 1934, s. 308.; Jevons, 1875, s. 234.

Avrupa Merkez Bankası [European Central Bank (ECB)] tarafından 2012 yılında yayınlanan sanal para bülteninde¹⁶¹ dijital para kapsayıcı bir şekilde kullanılmıştır. Bültende sanal paralardan bir dijital para “türü” olarak bahsedilmektedir¹⁶². Bununla birlikte her ne kadar bültende bahsedilen şekilde bir “dijital para” kavramı geçse de, “dijital” kelimesi ayrıca paranın formunu açıklamak için kullanıldığı gözükmektedir. Bültende para formlar “fiziksel” ve “dijital” olarak ayrılıp, para türleri bu formatlar altında kategorize edilmiştir¹⁶³. Hem elektronik paranın hem de sanal paranın “dijital” formda olduğu vurgulanmıştır¹⁶⁴. Sonuç olarak bültende “dijital para” kavramı geçiyorsa da bu kavram sanal paraları ve elektronik paraları kapsayıcı bir şekilde kullanılmış, bir para türünden ziyade paranın bir “formu” olduğu üzerinde durulmuştur.

İngiltere Merkez Bankası (Bank of England) tarafından 2014 yılında yayınlanan bültende dijital paraların dağıtık defter¹⁶⁵ teknolojisini [distributed ledger technology (DLT)] kullanıyor olması vurgulanmakla birlikte dijital para, kripto paraları karşılayan bir kavram olarak kullanılmıştır¹⁶⁶.

ECB, 2015 yılında sanal paralar hakkında yayınladığı ileri analiz çalışmasında, 2012 bültenine benzer bir şekilde sanal paraların “dijital” bir değeri temsil ettiğini ve dijital para türü olduğunu tekrarlamıştır¹⁶⁷. Bununla birlikte çalışmada kesin bir ayrım gözetilmeden para formları basılı, elektronik, dijital ve sanal olarak genişletilerek anılmıştır¹⁶⁸.

Mali Eylem Görev Gücü [Financial Action Task Force (FATF)] tarafından 2014 yılında sanal paralar hakkında sunulan raporda dijital paraların sanal para ve elektronik

¹⁶¹ European Central Bank (ECB), Virtual Currency Schemes, 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> (Erişim: 23.04.2022)

¹⁶² ECB, 2012, ss. 5, 11.

¹⁶³ ECB, 2012, ss. 5, 11.

¹⁶⁴ ECB, 2012, s. 16.

¹⁶⁵ Distributed Ledger Technology: Verilerin ağda birden fazla yerde saklanabilir, erişilebilir, onaylanabilir olmasını kılan teknoloji.

¹⁶⁶ Ali vd., “Innovations in Payment Technologies and the Emergence of Digital Currencies”, Bank of England Quarterly Bulletin, 2014/54 (3), s. 262. <https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/innovations-in-payment-technologies-and-the-emergence-of-digital-currencies.pdf> (Erişim: 24.04.2022)

¹⁶⁷ European Central Bank (ECB), Virtual Currency Schemes – a further analysis, 2015, s. 25. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> (Erişim: 24.04.2022)

¹⁶⁸ ECB, 2015, s. 24.

parayı kapsayacak şekilde tanımlanabileceği; fakat kavram karmaşasına mahal vermemek adına raporda kullanılmayacağına değinilmiştir¹⁶⁹.

Uluslararası Ödemeler Bankası [Bank for International Settlements (BIS)] Ödemeler ve Piyasa Altyapıları Komitesi [Committee on Payments and Market Infrastructures (CPMI)] tarafından 2015 yılında yayınlanan raporda dijital para, çoğunlukla dağıtık defter teknolojisi vurgulanarak, kripto paraları karşılayacak şekilde kullanılmıştır¹⁷⁰. Bununla birlikte “kripto para” terimini kullanmaktan kaçınılmıştır. Raporda yer alan para taksonomisinde elektronik para, hem yasal elektronik parayı hem de dijital parayı kapsayacak şekilde geniş kullanılmış olup; dijital paralar -sonradan merkezi kurumların da dolaşıma sürebileceği düşünülüp- merkezi ve merkeziyetsiz olarak ayrılmıştır¹⁷¹.

Yukarıda BIS, ECB ve FATF gibi kuruluşların tarafından erken dönem dijital para yaklaşımları belirtilmiştir. Bununla birlikte whitepaper’larında¹⁷² dijital para kavramının anıldığı çeşitli kripto para ve blok zincir platform/protokollerinin de belirtilmesine yarar vardır¹⁷³.

Öncelikle ilk kripto para ve blok zincir örneği olan Bitcoin’in Satoshi Nakamoto ismindeki kişi ya da grup tarafından 2008 yılında yayınlanan makalesine¹⁷⁴ bakılmasında yarar vardır. Bitcoin, Nakamoto tarafından makale başlığında eşlerarası “elektronik” para sistemi olarak tanımlanmıştır¹⁷⁵. Makalenin ilerleyen kısmında da elektronik para kavramı tercih edilip¹⁷⁶, dijital para kavramı kullanılmamıştır.

¹⁶⁹ Financial Action Task Force, FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014, s. 4. <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (Erişim:22.04.2022)

¹⁷⁰ Committee on Payments and Market Infrastructures (CPMI), Digital Currencies, 2015, Bank For International Settlements, ss. 1, 3, 5. <https://www.bis.org/cpmi/publ/d137.pdf> (Erişim: 22.04.2022)

¹⁷¹ CPMI, 2015, s. 6.

¹⁷² Türkçeye “teknik doküman” olarak çevrilebilir. Whitepaper, projelerin çıkarılmadan önce detaylarının ve amaçlarının ortaya konulduğu belgelerdir. Aynı kavramlar olmasa da amaçları doğrultusunda “izahname”lere de benzemektedirler.

¹⁷³ Bu örneklerde sıkça karşılaşılan “cash” ve “coin” terimleri karışıklık yaratmamak için bu çalışmada “para” olarak çevrilmiştir.

¹⁷⁴ Satoshi Nakamoto isminin takma olduğu konusunda büyük ölçüde uzlaşmış olursa da bu kişinin kim ya da kimler olduğu hakkındaki teoriler üzerinde tezin ilerleyen kısmında kısaca durulacaktır.

¹⁷⁵ Nakamoto, 2008, s. 1.

¹⁷⁶ Nakamoto, 2008, s. 2.

2014 yılında Vitalik Buterin tarafından yayınlanan Ethereum whitepaper'ına bakıldığında “kripto para” kavramı tercih edilmekle birlikte “dijital para” kavramı az da olsa kripto para kavramını kapsayacak şekilde anılmıştır¹⁷⁷.

2019 yılında yayınlanan Luna whitepaper'ında dijital para kavramı anılan yerlerde kripto parayı karşılayacak şekilde kullanılmıştır¹⁷⁸.

2020 yılında yayınlanan Avalanche whitepaper'ında ise Avalanche'ın hedefinin “dijital” varlıkları üretme, transfer etme ve ticaretini gerçekleştirme olduğu belirtilmiştir¹⁷⁹. Çalışmada para birimleri kabaca itibari ve dijital olarak ayrılmıştır¹⁸⁰.

Belirtmekte yarar vardır ki, yukarıda uygulamadan seçilen örneklerdeki dijital para kavramı kullanımları, terminolojik ya da taksonomik farklılıkları belirtme kaygısı ile konmamıştır. Uygulamadaki örneklerde dijital para kavramının kabaca kripto paraları karşılayacak şekilde kullanıldığı gözükmektedir.

Yukarıda bazı uluslararası kurumların erken dönem dijital para kavramı kullanımı incelenmişti. Dijital paranın erken dönem kullanımlarının kapsayıcı özellik ihtiva ettiği gözükmektedir. Bununla birlikte son yıllarda dijital parayı kapsayıcı bir kavramdan ziyade ayrı bir para türü olarak konumlandırabilecek bir kullanımdan bahsetmekte yarar vardır.

1.2.5.4.1. Merkez Bankası Dijital Para Birimi (CBDC)

“Merkez Bankası Dijital Para Birimi [Central Bank Digital Currency (CBDC)]” kavramı, son yıllarda çoğu uluslararası kuruluş ve organizasyonun gündeminde olan bir kavramdır. CBDC kısaca merkez bankaları tarafından ihraç edilen dijital para olarak tanımlanabilir. CBDC görece yeni bir kavram olup literatürde özellikle 2016 yılından

¹⁷⁷ Buterin, Vitalik, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform”, 2014, ss. 4, 10, 30.

[https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum White Paper - Buterin 2014.pdf](https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum%20White%20Paper%20-%20Buterin%202014.pdf) (Erişim: 05.04.2022)

¹⁷⁸ Kereiakes vd., “Terra Money: Stability and Adoption”, 2019, ss. 1, 13. https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf (Erişim: 24.04.2022)

¹⁷⁹ Sekniqi vd., “Avalanche Platform”, 2020, s. 2. https://assets.website-files.com/5d80307810123f5ffbb34d6e/6008d7bbf8b10d1eb01e7e16_Avalanche%20Platform%20Whitepaper.pdf (Erişim: 24.04.2022)

¹⁸⁰ Sekniqi vd., 2020, s. 10.

itibaren çalışmaların yoğunlaştığı görülmektedir. Yine de fikrin ilk olarak 1987 yılında James Tobin tarafından öne sürüldüğü kabul edilmektedir¹⁸¹.

2015 yılında İngiliz Merkez Bankası tarafından yayınlanan araştırma gündeminde, merkez bankalarının kendi dijital paralarını çıkarmaları ve bunun mevcut ödeme sistemleri üzerindeki etkisinin ne olacağı konusuna dikkat çekilmiştir¹⁸². Ardından aynı yıl bu gündemden etkilenecek çalışmayı yaptığını belirten¹⁸³ George Danezis ve Sarah Meiklejohn tarafından, kısmen ilk CBDC çalışması kabul edilebilecek “Merkez Bankalı Kripto Para (Centrally Banked Cryptocurrencies)” yayınlanmıştır. Bu çalışma, Ben Laurie tarafından 2011 yılında yayınlanan çalışmada yer alan “dağıtık merkezi otorite (distributed central authority)” modelini takip etmektedir¹⁸⁴. Danezis ve Meiklejohn’un “RSCoin” olarak adlandırdığı bu modelde para arzının kontrolü tamamen merkez bankalara aitken, işlemlerin kontrolünü ve devamlılığını sağlayan ise merkez bankalarının yetki verdiği kurumların oluşturduğu dağıtık bir yapıdır¹⁸⁵.

2016 yılında İngiltere Merkez Bankası tarafından yayınlanan çalışma tebliğinin¹⁸⁶ her ne kadar teknolojik adaptasyondan ziyade makroekonomik perspektiften yaklaşılsa da¹⁸⁷, CBDC ile ilgili detaylı ilk çalışmalardan biri olduğu söylenebilir. Çalışmada “dijital para” kavramından “dağıtık defter teknolojisini ve merkeziyetsiz ödeme sistemlerini haiz paranın her türlü elektronik formu” anlaşılması gerektiği belirtilmiştir¹⁸⁸. Çalışmada mevcut elektronik ödeme sistemleri, merkezi oldukları vurgulanarak dijital para

¹⁸¹ Tobin, James. “A Case for Preserving Regulatory Distinctions.”, *Challenge*, vol. 30, no. 5, 1987/30 (5), ss. 12–13, <http://www.jstor.org/stable/40720529> (Erişim: 27.04.2022)

¹⁸² Bank of England, One Bank Research Agenda, 2015, s. 6. <https://www.bankofengland.co.uk/-/media/boe/files/research/one-bank-research-agenda---summary.pdf?la=en&hash=B2C820FBF6A960C4A625C2DAB5B5B6CE4FEDF120> (Erişim: 25.04.2022)

¹⁸³ Danezis, George, Sarah Meiklejohn, “Centrally Banked Cryptocurrencies”, 2015, s. 1. <https://eprint.iacr.org/2015/502.pdf> (Erişim: 25.04.2022)

¹⁸⁴ Ben Laurie, “An Efficient Distributed Currency”, 2011, s. 1. <https://www.links.org/files/distributed-currency.pdf> (Erişim: 26.04.2022)

¹⁸⁵ Danezis ve Meiklejohn, 2015, ss. 1, 3.

¹⁸⁶ Barrdear, John, Michael Kumhof, “The Macroeconomics Of Central Bank Issued Digital Currencies”, Staff Working Paper No. 605, 2016. <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1> (Erişim: 26.04.2022)

¹⁸⁷ Barrdear ve Kumhof, 2016, s. 8.

¹⁸⁸ Barrdear ve Kumhof, 2016, s. 5.

kavramından ayrı tutulmuştur¹⁸⁹. Bu doğrultuda söz konusu tebliğde dijital paraların CBDC ve kripto paraları kapsayacak şekilde kullanıldığı anlaşılmaktadır¹⁹⁰.

CBDC'ler BIS'in de gündeminde olan bir konudur. Bununla birlikte 2017 yılında BIS tarafından yayınlanan çeyreklik bültende CBDC kavramı yerine CBCC (Central Bank Cryptocurrencies) kavramı ele alınmıştır¹⁹¹. Bununla birlikte çalışmada oluşturulan para taksonomisinde "elektronik" bir para formu olarak kapsayıcı nitelikte ele alınmışken dijital para kavramına yer verilmemiştir¹⁹². Ardından BIS bünyesinde yapılan ilk ayrıntılı CBDC çalışması, CPMI tarafından 2018 yılında yapılmıştır¹⁹³. Çalışmada sunulan para taksonomisinde 2017 çalışmasının getirdiği paranın "elektronik" formunun yerini paranın "dijital" formu almıştır¹⁹⁴. Yine 2020 yılında BIS tarafından ayrıntılı bir CBDC raporu hazırlanmıştır¹⁹⁵. Raporda merkez bankalarının %80'inin aktif bir şekilde CBDC ile ilgilendiği belirtilmektedir¹⁹⁶. Çalışmada CBDC işlem defteri yapısının üç şekilde oluşturulabileceğinden bahsedilmektedir. İlk olarak CBDC'ler merkezi bir defter sisteminde işleyebilir. İkinci olarak CBDC'ler blok zincirdekine benzer şekilde dağıtık defter teknolojisine dayanabilir. Son olarak CBDC'ler bu iki sistemin karışımı bir defter teknolojisi ile işleyebilir; bu da merkezi defterin sadece ihraç edilen CBDC'lerin kaydını tuttuğu dağıtık defterli bir işleyiştir¹⁹⁷.

IMF bünyesinde 2019 yılında hazırlanan raporda, CBDC'lerin merkez bankaları tarafından elektronik para sağlayıcıları ile birlikte çıkarılabilecekleri önerisi getirilmiş, bu tür paralar da "Sentetik Merkez Bankası Dijital Para Birimi [synthetic CBDC (sCBDC)] olarak adlandırılmıştır¹⁹⁸. Bu yöntemin CBDC'lere göre merkez bankaları için daha ucuz ve risksiz olduğu belirtilmiştir¹⁹⁹. Bununla birlikte 2020 tarihli BIS raporunda

¹⁸⁹ Barrdear ve Kumhof, 2016, s. 5.

¹⁹⁰ Barrdear ve Kumhof, 2016, ss. 3-6.

¹⁹¹ Bech, Morten, Rodney Garratt, Central Bank Cryptocurrencies, BIS Quarterly Review, 2017. https://www.bis.org/publ/qtrpdf/r_qt1709f.html (Erişim: 27.04.2022)

¹⁹² Bech ve Garratt, 2017, s. 60.

¹⁹³ Committee on Payments and Market Infrastructures (CPMI), Central bank digital currencies, Bank for International Settlements, 2018. <https://www.bis.org/cpmi/publ/d174.pdf> (Erişim: 27.04.2022)

¹⁹⁴ CPMI, 2018, s. 5.

¹⁹⁵ Bank for International Settlements, Central bank digital currencies: foundational principles and core features, 2020. <https://www.bis.org/publ/othp33.pdf> (Erişim: 27.04.2022)

¹⁹⁶ BIS, 2020, s. 2.

¹⁹⁷ BIS, 2020, s. 12.

¹⁹⁸ Adrian, Tobias, Tommaso Mancini-Griffoli, "The Rise Of Digital Money", International Monetary Fund, 2019, s. 1. <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097> (Erişim: 28.04.2022)

¹⁹⁹ Adrian ve Mancini-Griffoli, 2019, ss. 14-15.

sCBDC'lerin tam olarak CBDC niteliği taşıyamadıklarından CBDC olarak kabul edilemeyeceği belirtilmiştir²⁰⁰.

IMF bünyesinde 2022 yılında yayınlanan çalışmada CBDC'ler çeşitli ülke örnekleri üzerinden incelenmiştir²⁰¹. Bunlar çıkardığı CBDC kullanılmakta olan Bahamalar Merkez Bankası [Central Bank of the Bahamas (CBOB)]; pilot CBDC uygulamalarına başlayan Çin Halk Bankası [People's Bank of China (PBOC)], Doğu Karayipler Merkez Bankası [Eastern Caribbean Central Bank (ECCB)] ve Uruguay Merkez Bankası [Banco Central de Uruguay (BCDU)]; mevcut bir CBDC projesi olan ve parlamentosu tarafından tartışılmakta olan İsveç Merkez Bankası (Sveriges Riksbank); CBDC'yi uygulamış fakat vazgeçmiş olan Kanada Bankası [Bank of Canada (BOC)]'dir²⁰². Çalışmada ayrıca CBDC'ler için üç ayrı işleyiş modeli öngörülmüştür²⁰³. Bunlardan ilki tek taraflı (unilateral) CBDC olup, bu modelde merkez bankaları CBDC'lerin çıkarılması, dağıtımı ve son kullanıcıya erişimi gibi bütün konuları üstlenmektedir. İkinci model aracılı (intermediated) CBDC olup merkez bankaları bu modelde CBDC'lerin çıkarılmasını üstlenip, son kullanıcıya erişimi konusunu özel firmalara bırakmaktadır. Son model ise 2019 çalışmasında da ortaya konulduğu gibi sentetik CBDC (sCBDC) olup CBDC'lerin üretimi merkez bankalarında hesabı olan özel firmalara bırakılmıştır. sCBDC modelinin bu çalışmada 2019 yılı raporunun aksine CBDC olarak sayılmayacağı belirtilmiştir.

CBDC'ler ECB tarafından da yakından takip edilmekte olup, CBDC'lerin açık ekonomi çerçevesinde incelendiği 2020 tarihli çalışmada CBDC'lerin merkez bankası rezervlerini toplumun erişimine açma fonksiyonu göreceğinden bahsedilmektedir²⁰⁴.

CBDC'ler hiç şüphesiz Federal Rezerv Sistemi²⁰⁵ [The Federal Reserve System (FED)] tarafından doların dijitalleşmesi süreci içinde incelenmektedir. Governörler Kurulu (Board of Governors) tarafından 2022 yılında yayınlanan araştırma ve analiz raporunda CBDC, "kamuoyunun geniş bir şekilde erişimine açılan merkez bankası dijital

²⁰⁰ BIS, 2020, s. 4.

²⁰¹ Soderberg, Gabriel, "Behind the Scenes of Central Bank Digital Currency", International Money Fund, 2022, s. 1. <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174> (Erişim: 28.04.2022)

²⁰² Soderberg, 2022, s. 1.

²⁰³ Soderberg, 2022, ss. 8-9.

²⁰⁴ Ferrari vd., "Central bank digital currency in an open economy", European Central Bank, 2020, s. 5. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2488~fede33ca65.en.pdf> (Erişim: 28.04.2022)

²⁰⁵ Birleşik Devletler'in merkez bankası.

öz kaynağı” olarak tanımlanmaktadır²⁰⁶. Raporunda FED’in CBDC çıkarmanın yollarını ve etkilerini araştırdığı belirtilmektedir²⁰⁷. Çalışmada dijital paralar, ticari banka hesaplarında bulunan bakiyeleri ve finansal servis sağlayıcılarının bakiyelerini kapsayacak şekilde kullanılmıştır²⁰⁸. Raporunda kripto paralar dijital para olarak kabul edilmeyip, “dijital varlık” statüsü atfedilmiştir²⁰⁹.

Türkiye Cumhuriyeti Merkez Bankasının (TCMB) da CBDC tedavülü için çalışmalarda bulunduğu bilinmektedir. Bu doğrultuda 2021 yılında ASELSAN, HAVELSAN ve TÜBİTAK-BİLGEM ile birlikte “Dijital Türk Lirası İşbirliği Platformu” oluşturulup AR-GE projesi hayata geçirilmiştir. TCMB, dijital Türk lirasını “mevcut ödemeler altyapısını tamamlayıcı nitelikte” ele almaktadır²¹⁰. Bununla birlikte Türkiye Cumhuriyeti Cumhurbaşkanlığı 11. Kalkınma Planı²¹¹’nda da “Blokzincir tabanlı dijital merkez bankası parası uygulamaya konulacaktır.” İfadesi yer almaktadır.

Yukarıda da görüldüğü üzere çoğu ülke ve kuruluşun CBDC ile yakından ilgilendiği, ulusal paralarını dijitalleştirmeye hevesli olduğu görülmektedir. Bu doğrultuda çalışmalarda CBDC’ler için teknolojinin nimetlerinden sayılabilecek DLT’lerin kullanılabilmesinden sürekli bahsedilmiştir. BIS’in 2020 raporunda da değinildiği gibi, CBDC’lerin dağıtık defter teknolojisini kullanması mümkün iken merkezi kayıt sistemi ile de işleyebilmesi mümkündür²¹². CBDC’lerin dağıtık defter teknolojisini kullanıyor olması, blok zincir olduğu anlamına gelmez. Zira blok zincir olmayan DLT’ler de mümkündür. Bununla birlikte CBDC’lerde baskın bir şekilde DLT’nin tercih edildiği söylenemez²¹³. IMF’nin 2022 yılı çalışmasında belirtilen merkez bankalarından sadece Bahamalar ve Doğu Karayipler’in DLT tercih ettiği görülmektedir.

²⁰⁶ Board Of Governors Of The Federal Reserve System, Money and Payments: The U.S.Dollar in the Age of Digital Transformation, The Federal Reserve System, 2022, s.1. <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf> (Erişim: 28.04.2022)

²⁰⁷ Board of Governors of the Federal Reserve System, 2022, s. 3.

²⁰⁸ Board of Governors of the Federal Reserve System, 2022, s. 5.

²⁰⁹ Boards of Governors of the Federal Reserve System, 2022, s. 11.

²¹⁰ Türkiye Cumhuriyeti Merkez Bankası (TCMB), Merkez Bankası Dijital Türk Lirası Ar-Ge Projesi Hakkında Basın Duyurusu, 2021, <https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Duyurular/Basin/2021/DUY2021-40> (Erişim: 28.04.2022)

²¹¹ Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji Ve Bütçe Başkanlığı, On Birinci Kalkınma Planı (2019-2023), Temmuz 2019, <https://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf> (Erişim: 22.05.2022)

²¹² BIS, 2020, s. 12.

²¹³ Soderberg, 2022, s. 51.

Çin ise DLT'yi e-CNY²¹⁴ üzerinde denemiş ve işlem kapasitesi ve veri depolama kapasitesi yeterli bulunmadığından merkezi sistem ile devam etmektedir. Bununla birlikte daha efektif görünen bölgelerde DLT ile işleyen e-CNY'ler de kullanılmaktadır²¹⁵.

CBDC'ler ile ilgili tartışılması gereken bir husus da anonimlikdir. Dijital çağda devletler birçok ödeme sistemi üzerinde takip edilebilirlik açısından hakimiyet sağlayabiliyorken fiziki para üzerinde sağlayamamaktadır. Fiziki paralar insanların elindeki en büyük, belki de kalan en son, anonim ödeme aracıdır²¹⁶. Bu nedenle devletlerin fiziki para yerine takip edebildikleri ve merkez bankaları tarafından üretilmiş dijital paraları tercih etmeye yöneliyor olması tesadüf değildir. Uygulamada olan CBDC'lere bakıldığında anonimliğin sadece düşük miktarda transferlerde mümkün olduğu görülmektedir²¹⁷.

Dijital para ile ilgili açıklamaları bitirmeden önce, dijital para başlığının ilk paragrafında belirtilen dijital para kavramı üzerindeki kargaşa sorununa çözüm önerisi sunulabilir. Dijital para kavramı literatürde çoğunlukla diğer para birimlerini kapsayıcı olarak kullanılabilir. Fakat özellikle son yıllarda yapılan dijital para çalışmalarının CBDC üzerinde yoğunlaştığı ve dijital paranın CBDC'yi kastedecek şekilde kullanıldığı görülmektedir. Bu sebeple bu çalışmada “dijital para”nın; elektronik, sanal ya da kripto para gibi para türlerini kapsayıcı anlamından ziyade, kendi başına ayrı bir para türü (CBDC) olarak kabul edilebileceği önerilmektedir. Gerçekten de CBDC'ler birçok açıdan elektronik para, sanal para ya da kripto paralardan ayrılmaktadır.

1.2.5.5. Elektronik Para

Elektronik para geniş anlamda parasal değerın elektronik formu olarak tanımlanabilir²¹⁸. Basel Bankacılık Gözetim ve Denetim Komitesi'nin 1998 yılında yaptığı tanıma göre elektronik para, ödeme noktası terminalleri yolu ile (POS-point of

²¹⁴ Dijital Yuan.

²¹⁵ Soderberg, 2022, ss. 16-17.

²¹⁶ Kripto paralar bu deyimın dışında bırakılmıştır.

²¹⁷ People's Bank of China, Working Group on E-CNY Research and Development of the People's Bank of China, Progress of Research & Development of E-CNY in China, People's Bank of China, 2021, s. 7. <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf> (Erişim: 29.04.2022); Soderberg, 2022, s. 15

²¹⁸ European Central Bank (ECB), Electronic Money, https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html (Erişim: 30.04.2022)

sale) veya iki araç arasında doğrudan veya İnternet’te açık bilgisayar ağları üzerinden borçların ödenmesi için depolanmış değer veya önceden ödeme mekanizmasıdır²¹⁹. Avrupa Birliği’nin 2009/110 sayılı Elektronik Para Kuruluşlarının Kurulması, Faaliyetlerinin Sürdürülmesi, Denetimi Direktifi’nin 62.maddesine göre ise elektronik para, “*ödeme işlemlerinin yerine getirilmesi için fon sağlanması amacı ile çıkarılmış ve onu çıkaran haricinde gerçek ve tüzel kişi tarafından kabul edilen, manyetik olanlar da dâhil elektronik olarak onu ihraç edene karşı bir taleple temsil edilmek üzere depolanmış parasal değer*” şeklinde tanımlanmaktadır²²⁰.

Türk hukukunda da elektronik para 6493 sayılı Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun²²¹’da tanımlanmıştır. Kanunun 3. Maddesinin 1. Fıkrasının (ç) bendine 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 değer*”dir.

FATF ise 2014 raporunda elektronik paraları, itibari paranın dijital temsili olarak tanımlamaktadır²²².

Bir para türü olarak elektronik para; günlük hayatta kullanılan paranın, ticari banka ya da elektronik para kuruluşu gibi gerekli izinleri almış bir kuruluşa yatırılması suretiyle, elektronik ortamda kullanıma hazır hale gelmiş karşılığı olarak özetlenebilir²²³.

Klasik anlamda elektronik paralar ile CBDC’ler arasındaki temel fark; elektronik paralar ticari banka ya da izin verilen kuruluşlar tarafından ihraç edilirken, CBDC’ler sadece merkez bankası tarafından ihraç edilir.

Bir önceki paragrafta “klasik” kelimesinin kullanılmasının sebebi oldukça yeni bir kanun teklifinin bu güne kadarki elektronik para anlamını değiştirebileceğinden hareketlidir. 28 Mart 2022 tarihinde kongre üyesi Stephen Lynch tarafından Amerika

²¹⁹ Bozkurt Yüksel, A. Ebru, “Elektronik Para, Sanal Para, Bitcoin Ve Linden Doları’na Hukuki Bir Bakış”, *İÜHFİM*, 2015 (2), ss. 183-184. <https://dergipark.org.tr/tr/download/article-file/230763> (Erişim: 30.04.2022)

²²⁰ Bozkurt Yüksel, 2015, s. 184.

²²¹ R.G., T: 27/6/2013, S: 28690.

²²² FATF, 2014, s. 4.

²²³ Perçin, Önder vd., Sorularla Fintek: Elektronik Para Kuruluşları Ve Ödeme Kuruluşları - Açık Bankacılık - Kriptopara Ve Kriptopara Alım Satım Platformları, On İki Levha Yayıncılık, 2021, s. 2.

Birleşik Devletleri Kongresi'ne sunulan, "Elektronik Para Birimi ve Güvenli Donanım Kanunu [Electronic Currency And Secure Hardware (ECASH) Act] teklifi (bill)²²⁴ mevcut elektronik para ya da CBDC tanımlamalarından ayrılan bir yapıya sahiptir. Kanun teklifinde sunulan ödeme modelinde klasik anlamda elektronik paraların ya da CBDC'lerin kayıt defteri temelli yapısının aksine ECASH²²⁵ modeli donanım temellidir. Para transferleri çevrimdışı, güvenilir donanım aygıtları ile yapılmaktadır²²⁶. Modelin para birimi "elektronik dolar" ya da "e-cash" olarak adlandırılmıştır²²⁷. Bununla birlikte modeldeki önemli bir farklılık, paranın Federal Reserve (merkez bankası) yerine Treasury (hazine) tarafından üretilmesidir²²⁸.

Söz konusu teklif çerçevesinde modelin anonimlik düzeyinde elektronik para ve CBDC'lerin aksine fiziki paraya yaklaşan bir şekilde avantaj sağladığı gözükmektedir. İşlemlerin çevrimdışı yapılabilmesi bu hususta önemlidir. Kanun teklifinin kabul edilip modelin uygulamaya konulması durumunda elektronik paranın diğer para türlerinden sınırları daha çok çizilmiş bir şekilde ayrılabilceğini söylemek mümkündür.

1.2.5.6. Sanal Para

Sanal paralar kavramı da literatürde elektronik para, dijital para veya kripto para ile ya da yerine kullanılabilir. Sanal parayı bir para türü olarak sayılan türlerden ayırmadan önce bazı kuruluşlar tarafından sanal para için getirilmiş tanımlamalara bakmakta yarar vardır.

ECB'nin 2012 tarihli sanal para bülteninde sanal paralar; geliştiricileri tarafından üretilmiş ve kontrol edilmekte olan, spesifik bir sanal topluluğun üyeleri tarafından kabul edilip kullanılan, yasal olarak düzenlenmemiş bir dijital para türü olarak tanımlanmıştır²²⁹. Bültende sanal paraların bir elektronik para türü olarak da konumlandırılabilceğini fakat özellikle Avrupa Birliği'nin 2009/110 sayılı elektronik para direktifi göz önünde bulundurulduğunda aralarında önemli farklılıklar olduğundan

²²⁴ H.R. 7231 - Electronic Currency And Secure Hardware (ECASH) Act, 2022, <https://lynch.house.gov/cache/files/1/7/17e47e5a-2bff-42c1-b509-eb8a50931fa6/BDDFF183213326821B5C88B7F326EABB.ecashact-lynch.pdf> (Erişim: 30.04.2022)

²²⁵ Elektronik para anlamında kullanılmamış "e-cash" ile karıştırılmaması gerekir.

²²⁶ H.R. 7231 - Electronic Currency And Secure Hardware (ECASH) Act, 2022, s. 3.

²²⁷ H.R. 7231 - Electronic Currency And Secure Hardware (ECASH) Act, 2022, s. 2.

²²⁸ H.R. 7231 - Electronic Currency And Secure Hardware (ECASH) Act, 2022, s. 1.

²²⁹ ECB, 2012, s. 5.

bahsedilmektedir. Bunlardan ilki, elektronik paralarda elektronik para ile geleneksel para arasındaki bağ yasal bir temelde olmakla birlikte hesap birimi geleneksel paralar ile aynıdır. Buna karşın sanal paranın dayandığı yasal bir temel olmamakla birlikte hesap birimi de geleneksel para (euro, dolar, lira vb.) olmayıp kendi hesap birimidir. Bununla birlikte elektronik paradan geleneksel paraya geçişte güvence olmasına karşın sanal paralarda bu geçiş sanal para üreticisinin ya da geliştiricisinin takdirine bırakılmıştır²³⁰.

ECB, 2012 bülteninde (2015 tarihli ileri analiz çalışmasında da kabul takip edildiği şekilde) sanal para sistemlerini üçe ayırmıştır. Bunlardan ilki “kapalı” sanal para sistemleri olup, bu sistemde sanal paranın gerçek ekonomi ile bir bağı olmayıp genellikle “oyun içi” olarak adlandırılmaktadır²³¹. Bu sistemde sanal para sadece oyun içi eşyalar ya da servisler için kullanılabilir. Kapalı sanal para sistemlerinde sanal para vasıtasıyla gerçek ekonomide herhangi bir ürün alınıp satılamaz. Bu tür sistemlere örnek olarak “World of Warcraft (WoW)” oyunundaki “WoW gold” verilebilir. Oyuncular WoW gold’u gerçek paraları²³² ile alamamakta, öncelikle “WoW Token” satın alıp bu Token’ları oyun içi müzayede evinde satarak gold’a dönüştürebilmektedirler²³³. Gold ya da diğer oyun içi eşya ya da servislerin gerçek para için satılması oyun geliştiricisi Blizzard Entertainment tarafından yasaklanmıştır²³⁴.

ECB’nin belirttiği ikinci sistem ise “tek yön akışlı” sanal para sistemleridir. Bu sistemlerde sanal paralar gerçek paralar kullanılarak belirli bir değişim oranında satın alınabilir; fakat sanal paradan gerçek paraya dönüş mümkün değildir²³⁵. Bu sistemlere örnek olarak “Pokémon GO” mobil oyunundaki “PokéCoin”²³⁶ ya da “subreddit” denilen belirli ilgi alanlarının topluluğunun oluşturduğu “reddit” sitesindeki “reddit coins”²³⁷ örnek verilebilir. Bununla birlikte reddit tarafından 2020 yılında “vault”²³⁸ sistemi

²³⁰ ECB, 2012, s. 16.

²³¹ ECB, 2012, s. 13.

²³² Bu deyim sanal paranın zıttı bir anlamda, geleneksel paraları da kastedecek şekilde kullanılmış olup; ayrı bir para türü olarak anlaşılmalıdır.

²³³ Blizzard, “Using a WoW Token”, <https://eu.battle.net/support/en/article/000031218> (Erişim: 01.05.2022)

²³⁴ Blizzard, “Trading Items and Services for Real Money”, <https://us.battle.net/support/en/article/269874#:~:text=You%20are%20not%20allowed%20to,or%20services%20for%20real%20money>. (Erişim: 01.05.2022)

²³⁵ ECB, 2012, s. 14.

²³⁶ Niantic, <https://niantic.helpshift.com/hc/en/6-pokemon-go/faq/94-using-pokecoins-to-make-purchases-in-the-shop-1582065532/>, (Erişim: 01.05.2022)

²³⁷ Reddit, “reddit coins”, <https://www.reddit.com/coins> (Erişim: 01.05.2022)

²³⁸ Reddit, “vault”, <https://www.reddit.com/vault/> (Erişim: 01.05.2022)

içerisinde tanıtılan, kullanıcıların katıldıkları subreddit'lere özel olarak ödüllendirildiği ve subreddit topluluğunun subreddit sahipliğini kazanmasını sağlayan "Reddit Community Points"ler (ilk örneği "Moons") sanal para olmayıp, kripto paradırlar²³⁹.

ECB'nin belirttiği üçüncü ve son sistem ise "çift yön akışlı" sanal para sistemleridir. Bu sistemde kullanıcılar gerçek para ile sanal paraları alıp satabilirler. Bu sistemin ilk, belki de en çok bilinen örneği "sanal para" kavramının yer edinmesini sağlamış bir rol yapma oyunu olan Second Life'ta kullanılan "Linden doları"dır²⁴⁰. Bununla birlikte ECB, 2012 bülteninde kripto paraları da sanal para kapsamına almıştır .

ECB, 2015 tarihli ileri analiz çalışmasında da sanal paraları kripto paralar ve sanal paraları kapsayacak şekilde kullanmıştır²⁴¹.

FATF, 2014 tarihli raporunda sanal paraları; dijital olarak ticareti yapılabilen, paranın klasik işlevlerini yerine getirebilecek özellikte, resmi statüsü olmayan, değerini dijital temsili olarak tanımlamıştır²⁴². FATF de ECB'ye benzer şekilde sanal paraları açık (dönüştürülebilir) ve kapalı (dönüştürülemez) olarak sınıflandırmıştır²⁴³. FATF, söz konusu raporda kripto paraları, "merkeziyetsiz sanal para" olarak adlandırarak sanal para içerisine dahil etmiştir²⁴⁴.

Sanal paraların çoğunlukla yanlış bir şekilde kripto paraları da kapsayacak şekilde kullanıldığı görülmektedir. Sanal paralar, FATF'nin 2014 raporunda –her ne kadar raporda kripto paralar sanal para statüsüne alınsa da- belirtildiği üzere merkezi yapıdadır. Sanal para, sanal parayı üreten ya da işleten yapıdan bağımsız değildir. Sanal paralar kriptografinin nimetlerinden yararlanmazlar; blok zincir üzerinde işlemezler. Bununla birlikte sanal parayı elektronik para ya da dijital paradan (CBDC) ayıran husus da sanal paranın resmi statüye sahip olmamasıdır. Bu doğrultuda sanal paralar resmi bir statüye sahip olmayan, merkezi paralar olarak; kripto para, elektronik para ya da dijital paradan ayrı bir para türü olarak değerlendirilebilir.

²³⁹ Kraken, "What is Reddit MOON?", <https://www.kraken.com/learn/what-is-reddit-moon> (Erişim: 01.05.2022)

²⁴⁰ Second Life, "Buying & Selling Linden Dollars", <https://lindenlab.freshdesk.com/support/solutions/articles/31000138105-buying-selling-linden-dollars> (Erişim: 01.05.2022)

²⁴¹ ECB, 2015, s. 4.

²⁴² FATF, 2014, s. 4.

²⁴³ FATF, 2014, s. 4.

²⁴⁴ FATF, 2014, s. 5.

1.2.5.7. Kripto Para

Bu çalışmanın da omurgasını oluşturan; eşler arası, merkeziyetsiz, kriptografik işleme dayalı ödeme sistemi olan kripto paralar, para türleri başlığı altında elektronik para, dijital para ve sanal paradan ayrı bir para türü olarak yerini almakla birlikte; çalışmanın devamında detaylı bir şekilde inceleneceğinden, tekröre düşmemek adına, bu başlıkta sadece ismi zikredilmekle yetinilmiştir.



İKİNCİ BÖLÜM

BLOK ZİNCİR

2.1. Giriş

Blok zincir (blockchain), kriptografik işlemlerin gruplaşarak meydana getirdiği bloklardan oluşan, kurcalamayı belli eden (tamper evident) ve kurcalamaya dayanıklı (tamper resistant) dağıtık dijital defterler ya da dağıtık veri tabanlarıdır. Blok zincir bloklardan oluşur; her blok kendinden bir önceki bloğa doğrulama ve konsensüs kararından geçerek kriptografik olarak bağlanır (kurcalamayı belli etme). Yeni bloklar eklendikçe eski bloklar üzerinde değişiklik yapmak zor hale gelir (kurcalamaya dayanıklılık)²⁴⁵.

Blok zincir teknolojisi bir kişinin, bir kurumun, bir merkezi otoritenin, bir aracının tahakkümü altında değildir²⁴⁶. Blok zincir, güvenilir üçüncü tarafın, merkezi bir otoritenin sağlayabildiği kısmı güveni, dağıtık yapıyı mimarisiyle tek bir lidere bağımlı olmaksızın mutlak güvene dönüştüren bir teknolojidir²⁴⁷. Güven kavramını biraz daha açmak mümkündür.

Ticarette, mal alım satımında ya da genel olarak bir değer transferinde ezelden beri bir “güven bunalımı” sorunu bulunmaktadır²⁴⁸. Bu güven bunalımı sorunu genellikle “karşı taraf riski” üzerinden tezahür etmektedir. Karşı taraf riski önceden tanınmayan, tanınsa bile tam olarak güvenilemeyen bir kişi ile ürün-para alış verişi yapma çerçevesinde ortaya çıkar. Örneğin bir ürünü satan ürünü alanın ödemeyi yapıp yapmayacağından endişelenir. Ürünü alan da ürünü satanın ürünü kendisine zamanında teslim edip edemeyeceğinden, ürünle ilgili verilen taahhütlerin yerine getirilip getirilmeyeceğinden endişelenir. Bu durumun aşılabilmesi için güvenilir üçüncü taraf

²⁴⁵ Yaga vd., “Blockchain Technology Overview”, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, s. 1. <https://doi.org/10.6028/NIST.IR.8202> (Erişim: 30.03.2022)

²⁴⁶ Güven V. ve E. Şahinöz, BLOKZİNCİR – KRIPTO PARALAR – BITCOIN, Satoshi Dünyayı Değiştiriyor, (2. Baskı), Kronik Kitap, İstanbul 2018, s. 156.

²⁴⁷ Güven ve Şahinöz, 2018, s. 184.

²⁴⁸ Güven ve Şahinöz, 2018, s. 161.

olarak nitelendirilebilen “kurum” olgusu oluşturulmuştur²⁴⁹. Kurumlar, içinde yer aldıkları toplumun nesnel koşullarını daha da sağlamlaştırmak ve belirgin kılmak üzere toplum tarafından oluşturulurlar²⁵⁰. Bu çerçevede toplumsal kurum bir toplumun temel kaygıları ve faaliyetlerini düzenleyen ve toplumsal ihtiyaçlarını karşılayan tüm yapısal bileşenlerini karşılamaktadır²⁵¹. Söz konusu güven bunalımında bu bunalımı “kısmi” olarak çözen kurumlar, yasalar, bankalar, noter vs. olabilir²⁵². İşte blok zincir, kurumlar ile çözülmeye çalışılan bu güven sorununu, kurumlara ihtiyaç olmadan, dağıtık bir yapı ile mutlak güven sağlayarak çözmeyi vadeder. Burada belirtmek gerekir ki, yukarıda verilen örneğin ekonomi ya da ticaret çerçevesinde olmasından, blok zincirin sadece bu alanda faaliyet gösterebilmesi anlamı çıkarılmamalıdır. Dağıtık bir veri tabanı olan blok zincirin, alışlagelmiş yöntemlerden daha efektif ve güvenilir olduğu sürece her türlü veri ve her türlü alan için kullanılabilmesi unutulmamalıdır. Örneğin blok zincir, bireylerin ve toplumun hukuki güvenliğini sağlamaya dayalı bir faaliyet sürdüren²⁵³ noterlerin yerini alabilir²⁵⁴; ya da ulusal düzeyde olsun ya da olmasın herhangi bir seçim blok zincir üzerinden gerçekleştirilebilir²⁵⁵.

Blok zincir teknolojisi gerçek anlamıyla ve tam şekilde ilk kez Satoshi Nakamoto ismindeki kişi ya da grubun 2008 yılında yayınladıkları makale ile ortaya çıkmış ve geniş kitlelere yayılma fırsatı bulmuş olsa da, teknolojinin altındaki fikir ve çalışmalar 1980’li yılların sonu ve 1990’lı yılların başına tekabül etmektedir²⁵⁶.

²⁴⁹ Güven ve Şahinöz, 2018, s. 171.

²⁵⁰ Okan, Oya, Kurumlar Sosyolojisi Ders Notları, İstanbul, 2021.

²⁵¹ Okan, 2021.

²⁵² Güven ve Şahinöz, 2018, s. 171.

²⁵³ Tekben, Tuğçe, “Noterin Hukuki Statüsü Ve Noterlik Kanunu’nun 162. Maddesi Uyarınca Sorumluluğu Üzerine Bir İnceleme”, *İzmir Barosu Dergisi*, Eylül 2021, s. 71.
<https://www.izmirbarosu.org.tr/pdfdosya/noterin-hukuki202214145432429.pdf> (Erişim:21.05.2021)

²⁵⁴ Kara, Kübra, “Geliştirdiği uygulamayla noter işlemlerini "sanal" ortama taşıdı”, Anadolu Ajansı, 10.05.2022. <https://www.haberler.com/guncel/gelistirdigi-uygulamayla-noter-islemlerini-sanal-14929714-haberi/> (Erişim:21.05.2021)

²⁵⁵ İnanç Sönmez, Bade, “Blok zinciri tabanlı ilk seçim Sierra Leone’de gerçekleştirildi”, Dünya Halleri, 13.03.2018. <https://www.dunyahalleri.com/blok-zinciri-tabanlı-ilk-secim-sierra-leonede-gerceklestirildi/> (Erişim:21.05.2022)

²⁵⁶ Yaga vd., 2018, s. 2.; <https://academy.binance.com/en/articles/history-of-blockchain> (Son erişim: 30.03.2022)

2.2. Blok Zincir Fikri ve Teknolojisine Ulařtırın alıřmalar

İlk blok zincir ve kripto para Bitcoin olsa da blok zincir teknolojisinin sahip olduđu bazı elementler yıllar süren bazı alıřmaların ürünüdür. Blok zincir ve kripto paraların tarihesini kriptografi alıřmalarına dayanarak oldukça eskilere götürebilmek mümkündür. Hatta bu tarih sistematik bir şekilde kayıt tutmanın görüldüğü milattan önce 4000’li yıllara, antik Mezopotamya’ya kadar götürülebilir²⁵⁷. Fakat bu alıřmada sırasıyla ideolojik ve teknolojik olarak Bitcoin örneğine ulařmanın amaç edinildiği düşünölen “Kripto Anarřist Manifesto” ve “Paxos Protokolü” blok zinciri ve kripto paranın etkilendiği örnekler arasında ilk sırada yer edinmiřtir²⁵⁸. Yine de kriptografi ve dođal olarak kriptoloji öđretisinin daha erken birtakım teknolojik ürünlerinin blok zincirin oluşumuna etki ettiđi de açıktır. Bu dođrultuda yukarıda sayılan iki alıřma ile bařlangı yapmadan önce, daha derinlere inerek 1970’li yılların ortasından itibaren yapılmıř, blok zincir teknolojisinde de benzerlerine bařvurulan bazı alıřmalar ele alınacaktır. alıřmalar ele alınırken blok zincir ve kripto paraların yapısını oluřturan bazı temel kavram ve özelliklere de deđinilmiř olunacaktır. Bu sayede blok zincirin genel özelliklerinden bazıları ortaya ıkıř süreci ile birlikte deđerlendirilebilecek, alıřmanın devam eden kısmında tekrar edilmesine gerek duyulmayacaktır.

2.2.1. SDD-1

Blok zinciri kaba tabir ile dađıtık bir veri tabanı olarak tanımlarsak, bu fikir 1976 yılında geliřtirilmeye bařlanan ve 1977 yılında Eugene Wong tarafından prototipi ortaya konan SDD-1’e kadar götürülebilir²⁵⁹. SDD-1 dađıtık bir veri tabanı yönetim sistemidir²⁶⁰. SDD-1 sistemi ile veri tabanı yönetiminde depolama bilgisayarlardan

²⁵⁷ Orville R. Keister, “Commercial Record-Keeping in Ancient Mesopotamia”, *The Accounting Review* 1963/38 (2), s. 372. <https://www.jstor.org/stable/242928> (Eriřim:02.05.2022)

²⁵⁸ Güven ve řahinöz, 2018, s. 141.

²⁵⁹ Sherman vd., “On the Origins and Variations of Blockchain Technologies”, University of Maryland, 2018, s. 2. <https://arxiv.org/ftp/arxiv/papers/1810/1810.06130.pdf> (Eriřim: 30.04.2022); Wong, Eugene, “Retrieving dispersed data from SDD-1: A system for distributed databases,” 1977 Berkeley Workshop on Distributed Data Management and Computer Networks, University of California, Berkeley, CA

²⁶⁰ Rothnie vd., “Introduction to a System for Distributed Databases (SDD-1)”, *ACM Transactions on Database Systems*, 1980/5 (1), s. 1. <https://dl.acm.org/doi/pdf/10.1145/320128.320129> (Eriřim: 02.05.2022)

oluşan bir ağa yayılmıştır²⁶¹. Dağıtık veri tabanlarının merkezi veri tabanlarına göre birtakım avantajları bulunmaktadır. Dağıtık veri tabanlarının veri fazlalığı oluşturarak merkezi veri tabanlarına kıyasla daha güvenilir ve erişilebilir olduğu kabul edilir²⁶². Çünkü SDD-1 veri tabanı sitelerinden her biri, bütün veri tabanının bir kısmını bulundurur. Veri tabanının bazı kısımları birden fazla sitede aynı anda bulunuyor olabilir; veri fazlalığını bu durum yaratmaktadır²⁶³.

SDD-1'in geliştirilmiş ilk genel amaçlı dağıtık veri tabanı²⁶⁴ olması nedeniyle blok zincir teknolojisinin oluşumuna dolaylı yoldan katkı sağladığı söylenebilir.

2.2.2. Kriptografik Bulmacalar, Merkle Ağacı ve Kriptografik Hash

“Kriptografik Bulmacalar”, “Merkle Ağacı” ve “Kriptografik hash” blok zincirin temel yapısının oluşmasına direkt olarak etki eden çalışmalardır. Aynı başlıkta incelenmelerinin nedeni her üçünün de doğrudan ya da dolaylı bir şekilde Ralph Merkle tarafından ortaya konmasından dolayıdır.

“Kriptografik bulmacalar” ya da diğer ismi ile “Merkle’in bulmacaları”, Merkle tarafından 1974 yılında geliştirilip, 1978 yılında ilk kez makale olarak yayınlanan²⁶⁵, açık anahtarlı (asimetrik) şifrelemenin ortaya çıkmasını sağlamış bir açık anahtarlı anlaşma tekniğidir. Bu teknik, iki kişi arasındaki mesajlaşma vasıtasıyla, aralarında daha önceden bir sır mevcut olmasa bile, paylaşılmış bir sırrın (shared secret) üzerinde anlaşma sağlanmasına imkan tanır²⁶⁶.

Güvenli iletişim, iki kişi arasında gizli bir şekilde gerçekleşen, üçüncü bir kişinin kurulan iletişimin ne olduğunu bulma çabasını sonuçsuz çıkaracak derecede kurulmuş bir iletişim biçimidir²⁶⁷. Merkle tarafından ortaya konan kriptografik bulmacalar sistemi,

²⁶¹ Rothnie vd., 1980, s. 1.

²⁶² Zhou vd., “The Semi-join Query Optimization in Distributed Database System”, National Conference on Information Technology and Computer Science (CITCS 2012), 2012, s. 606. <https://doi.org/10.2991/citcs.2012.232> (Erişim: 03.05.2022)

²⁶³ Bernstein vd., "The Concurrency Control Mechanism of SDD-1: A System for Distributed Databases (The Fully Redundant Case)," *IEEE Transactions on Software Engineering*, 1978/4 (3), s. 154. <https://ieeexplore.ieee.org/document/1702517> (Erişim: 03.05.2022)

²⁶⁴ Rothnie vd., 1980, s. 15.

²⁶⁵ Merkle, Ralph C., “Secure Communications Over Insecure Channels”, *Communications of the ACM*, 1978/21 (4). <https://doi.org/10.1145/359460.359473> (Erişim: 03.05.2022)

²⁶⁶ Wikipedia, Merkle’s Puzzles, https://en.wikipedia.org/wiki/Merkle%27s_Puzzles (Erişim: 03.05.2022)

²⁶⁷ Merkle, 1978, s. 295.

gizliliğin sağlanması oldukça zor olduğu durumlarda bile güvenli iletişim kurulmasına imkan tanır²⁶⁸. Merkle'in söz konusu çalışmasının ismi de bu amacı ortaya koymaktadır: "Güvenilir Olmayan Kanallarda Güvenli İletişim (Secure Communications Over Insecure Channels)".

Kriptografik bulmacalar basite indirgenerek bir örnek üzerinden açıklanabilir. X ve Y açık bir iletişim kanalında güvenli bir iletişim kurmak istemektedirler. Fakat bu kanalda iletilen bütün mesajları Z de görmektedir. Güvenli bir iletişim için şifreli bir mesajlaşma ve şifreyi çözecek bir şifre anahtarı gerekmektedir. X, Y'ye şifreli mesaj yollarsa bile Y anahtarın ne olduğunu bilmeden bu mesajları çözemeyecektir. X anahtarı kanalı kullanarak Y'ye yollarsa, bu anahtar kanalı takip eden Z tarafından da görülebileceğinden şifreli mesajlaşma Z tarafından da çözülebilecek ve iletişim güvenli olmayacaktır. Elimizdeki bu durumda X, öncelikle Y'ye çok sayıda bulmaca yollayacaktır. Bu bulmacalardan her biri sadece çözüldüğünde okunabilen bir bulmaca numarası ve anahtarını ihtiva etmektedir. Her bulmacanın numarası ve içerdiği anahtar birbirinden farklıdır. Y, X'in yolladığı birçok bulmacadan bir tanesini seçerek çözer. Y bulmacayı çözdüğünde o bulmacaya ait numarayı ve anahtarı elde etmiş olur. Elde ettiği bu anahtar X ile aralarında yapılacak şifreli mesajlaşmayı deşifre edecek anahtardır. Y bulmacayı çözdükten sonra bulmacanın numarasını X'e kanaldan geri yollar. X, bulmacaların hangisinin hangi numarayı ve anahtarı ihtiva ettiğini bildiğinden Y'nin hangi bulmacayı çözdüğünü ve dolayısıyla aralarındaki mesajlaşmada hangi anahtarı kullanacağını da bilir.

Bu doğrultuda X ve Y, iletilen bütün mesajların Z tarafından da okunabildiği güvenilir olmayan bir kanalda, aralarında bir şifre anahtarı oluşturarak şifreli mesajlaşmayı gerçekleştirebileceklerdir. Bu iletişimde gönderilen bütün bulmacaları ve Y'nin X'e geri gönderdiği bulmaca numarasını Z de görecektir; fakat Z bu numarayı bilse de numaranın hangi bulmacaya ait olduğunu bilemediğinden anahtara da erişemeyecektir. Z'nin anahtara erişebilmesi için Y'nin çözdüğü bulmacayı bulana dek bulmacaları çözmesi gerekmektedir, bu da büyük bir emek ve zamana bedel olacaktır²⁶⁹.

Merkle'in ilk kez 1974 yılında ortaya koyduğu bu çalışmasından hareketle Whitfield Diffie ve Martin E. Hellman, 1976 yılında ilk açık anahtar protokolünü ortaya

²⁶⁸ Merkle, 1978, s. 295.

²⁶⁹ Merkle, 1978, ss. 295-296.

çıkarmıştır²⁷⁰. Diffie ve Hellman'ın çalışmasında da Merkle'in çalışmasına benzer şekilde, daha önceden hiç iletişim kurmamış iki kişinin genel bir kanaldan şifreli bir iletişim kurabilmesi sorunu ele alınmıştır²⁷¹. Diffie ve Hellman anahtar değişimi sisteminde iletişim kuran taraflarda açık ve özel olmak üzere ikişer tane anahtar bulunmaktadır. Açık anahtarlar herkes tarafından görülebilirken, özel anahtarlar sadece sahibi tarafından görülebilir. Diffie ve Hellman anahtar değişimi sistemi kabaca izah edilecek olursa, güvenli iletişim kurmak isteyen her iki taraf da birbirine açık anahtarını yollar. Örneğin X ve Y birbirine açık anahtarını yollar. X, Y'nin açık anahtarı ile kendi gizli anahtarını; Y ise X'in açık anahtarı ile kendi gizli anahtarını birleştirdiğinde paylaşılmış ortak bir sır ortaya çıkar. X ve Y ortak bu sır ile güvenli bir şifreli iletişim kurabilirler. Dışarıdan bir kişi her iki açık anahtarı da görebilse de, X veya Y'nin gizli anahtarlarını bilemediğinden iletişim güvenli kalır.

Genel olarak açık anahtarlı şifrelemede yukarıda da belirtildiği gibi açık ve özel olmak üzere iki anahtar bulunur. Asimetrik anahtar şifreleme algoritmasını kullanan bu şifrelemede X kişisi Y kişisine mesaj yollarken, mesajı Y kişinin açık cüzdanı ile şifreler. Şifrelenen bu mesaj sadece Y kişinin özel cüzdanı ile yani Y tarafından deşifre edilebilir.

Yukarıda izinsiz bir blok zincirde yapılan bütün işlemlerin herkese açık, herkes tarafından görülebilir olduğundan bahsedilmişti. Bu durum yapılan her işlemin herkes tarafından görülebildiği bir ağın nasıl olur da gizli ve güvenli bir işlem gerçekleştirmek için kullanıldığı sorusunu akla getirebilir. Bu başlıkta bahsedilen açık anahtarlı şifreleme gibi blok zincir tarafından kullanılan kriptoloji ürünleri sayesinde, ağ güvenli bir hale gelmektedir. İlk blok zincir olan Bitcoin'de de açık anahtarlı şifrelemenin nasıl kullanıldığı Nakamoto tarafından açıklanmıştı²⁷².

Belirtmek gerekir ki, Merkle tarafından ortaya atılan kriptografik bulmaca modelinin her ne kadar öncelikli olarak açık anahtarlı şifrelemenin ortaya çıkmasını sağlamış olduğu bilinse de; modelin ayrıca çalışmanın ilerleyen kısımlarında incelenecek

²⁷⁰ Diffie, Whitfield, Martin E. Hellman, "New Directions in Cryptography", *IEEE Transactions On Information Theory*, 1976/22 (6), s. 644. <https://ee.stanford.edu/~hellman/publications/24.pdf> (Erişim: 03.05.2022)

²⁷¹ Diffie ve Hellman, 1976, s. 644.

²⁷² Nakamoto, 2008, s. 2.

olan ve Bitcoin tarafından da kullanılan “Proof-of-Work (PoW)²⁷³” modelinin de ilkel bir görünümünü teşkil ettiği söylenebilir²⁷⁴.

Merkle Ağacı’ndan (Merkle Tree) bahsetmeden önce, blok zincir ve genel olarak kriptolojide oldukça karşımıza çıkan “hash”, “hash fonksiyonu” ya da “kriptografik hash fonksiyonu” kavramlarının kısaca belirtilmesi gerekebilir. Hash, blok zincirin temelini oluşturan kavramlardan biridir. Hash, Türkçeye tam olarak çevrilemese ve bu çalışmada da orijinal ismi ile anılacaksa da; işlevini açıklamak için “parmak izi” ya da “özet”e benzetilebilir²⁷⁵. Hash fonksiyonu, herhangi uzunluktaki bir veriyi sabit uzunluktaki bir veriye dönüştüren fonksiyondur²⁷⁶. Hash, bir verinin, mesajın ya da belgenin özgünlüğünü kanıtlamak için kullanılır. Bir belgedeki en ufak bir değişiklik farklı bir hash değerine sebep olacaktır. Dolayısıyla özgün belgenin özeti ve ulaşan belgenin özeti mukayese edildiğinde belgenin özgünlüğü öğrenilir²⁷⁷. Kriptografik hash fonksiyonlarının öncüsü Ralph Merkle 1979 tarihli doktora tezinde, özgünlüğünün doğrulanması gereken çok büyük veri alanlarının olabileceğini fakat sadece küçük veri alanlarının doğrulanabilir ve depolanabilir olduğundan bahsetmektedir²⁷⁸. Oldukça büyük bir verinin doğrulanması için gereken emek ve zaman bu verinin doğrulanmasını imkansız hale bile getirebilir. Bunun yerine verinin tek yönlü bir fonksiyon ile yani hash fonksiyonu ile özetlenerek daha kolay bir şekilde doğrulanması gerekecektir.

İlk kez Diffie ve Hellman, 1976 tarihli çalışmalarında dijital imza sistemi kurarken tek yönlü bir doğrulama fonksiyonuna ihtiyaç duyulduğundan bahsetmiştir²⁷⁹. 1979 tarihinde Merkle tarafından açıklanan hash fonksiyonları ve ardından Merkle ve Ivan Damgård tarafından tasarlanan “Merkle-Damgård yapısı” ya da “Merkle-Damgård hash fonksiyonu”, kriptografik hash fonksiyonun öncüsü olup, MD5 ve SHA-1 gibi programlamada oldukça fazla kullanılmış algoritmaların da oluşmalarını sağlamıştır.

²⁷³ Türkçeye “iş kanıtı”, “iş ispatı”, “emeğin kanıtı” olarak çevrilebilmekle birlikte, terim haline geldiğinden orijinal ismi ile anılacaktır.

²⁷⁴ Sherman vd., 2018, s. 3.

²⁷⁵ Güven ve Şahinöz, 2018, ss. 45, 50.

²⁷⁶ Güven ve Şahinöz, 2018, s. 50.

²⁷⁷ Güven ve Şahinöz, 2018, s. 45.

²⁷⁸ Merkle, Ralph, Secrecy, Authentication, And Public Key Systems, Department Of Electrical Engineering Stanford University, 1979, s. 11. <https://www.merkle.com/papers/Thesis1979.pdf> (Erişim: 04.05.2022)

²⁷⁹ Diffie ve Hellman, 1976, ss. 648-650.; Preneel, Bart, The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition, Katholieke Universiteit Leuven, 2010, s. 1. <https://www.esat.kuleuven.be/cosic/publications/article-1532.pdf> (Erişim: 03.05.2022)

Şöyle ki, MD5 ve SHA-1, kriptografide “İsviçre çakısı” olarak adlandırılmaktadır²⁸⁰. Yukarıda bahsedildiği üzere blok zincir de hash üzerine kurulmuştur. Bitcoin gibi bir çok kripto para işlemlerin doğrulanması ya da PoW hesaplaması için Merkle-Damgård yapısı ile oluşturulmuş SHA-256 (SHA-2) hash algoritmasını kullanmaktadır.

Bilgilerden oluşan blokların değiştirilemez bir şekilde kriptografik hash fonksiyonları ile zincirlenmesi fikri ilk kez Merkle’in 1979 tarihli çalışmasında karşımıza çıkmaktadır²⁸¹. Merkle bu fikrini “ağaç” metaforu üzerinden “Ağaç Doğrulaması”²⁸² şeklinde açıklamakta bu nedenle “Merkle Ağacı” olarak adlandırılmaktadır. Blok içerisine kaydedilen işlemler ikişerli olarak gruplanır ve hash’leri alınır. Bu hesaplanan hash’ler yine ikişerli olarak gruplanır ve yine hash’ler alınır. En sonunda iki tane hash kalıp onlar da hash’lenince “Merkle Kökü” hesaplanmış olur. İşlemler ikişerli olarak işlendiğinde tek kayıt kalırsa bu kayıt kendisi ile hashlenir²⁸³.

Bahsedilen bu yapı bir ağaca benzemektedir. İşlemler ağacın yapraklarını oluşturur; işlemlerin hash’leri alınıp ikişerli gruplanıp hesaplandıkça ağacın dalları oluşur ve en sonunda köke yani Merkle Kökü’ne ulaşmış olunur.

Merkle Ağacı blok zincirin en önemli unsurlarındandır. Merkle Ağacı sistemi, kullanıldığı alanda hız, verim ve güvenlik açısından yüksek avantaj sağlar²⁸⁴. Merkle Ağacı ile işlem teyitleri daha kolay yapılır. Merkle Ağacı sayesinde bir işlemin doğrulanması için tüm işlemlerin kontrolüne gerek kalmaz²⁸⁵.

Blok zincirin yapı taşlarından Merkle Ağacı kullanımı ilk blok zincir olan Bitcoin’de de karşımıza çıkmaktadır. Nakamoto Bitcoin makalesinde ilk olarak disk boyutunda tasarruf yapılabilmesi için Merkle Ağacı modelinin kullanılabileceğinden bahsetmiştir (Reclaiming Disk Space). Nakamoto’ya göre harcanmış bir işlem yeterli sayıda blok geçirdikten sonra silinerek disk tasarrufu sağlanabilirdi. Bu da Merkle Ağacı ile hashlenerek mümkün olacaktır. Yani block hash’ine sadece kök eklenir, eski işlemler ağacın budanmasına benzer şekilde budanır, disk boyutundan tasarruf edilir²⁸⁶. Belirtmek

²⁸⁰ Preneel, 2010, s.1.

²⁸¹ Sherman vd., 2018, s. 2.

²⁸² Merkle, 1979, ss. 40-45.

²⁸³ Güven ve Şahinöz, 2018, ss. 56-57.

²⁸⁴ Paribu, “Merkle Tree”, 2021, <https://www.paribu.com/blog/sozluk/merkle-tree-nedir/> (Erişim: 04.05.2022)

²⁸⁵ Güven ve Şahinöz, 2018, s. 58.

²⁸⁶ Nakamoto, 2018, s. 4.

gerekir ki Nakamoto tarafından açıklanan disk boyutundan tasarruf edilmesini sağlayan bu model, Nakamoto'nun anlattığı haliyle Bitcoin'de kullanılmamaktadır. Bunun yerine “pruning²⁸⁷” denilen yöntem kullanılarak bütün blok zincir depolanmadan blok zincire katılım sağlanır. Nisan 2022 itibariyle Bitcoin'i full node²⁸⁸ (tam düğüm) çalıştırmak isteyen bir kişinin yaklaşık 400 GB²⁸⁹ veri indirmesi ve bu veriyi bilgisayarında tutması gerekmektedir. Bununla birlikte pruning modu kullanılırsa, yine tüm verilerin indirilmesi gerekse de sadece 6 GB kadar²⁹⁰ bir depolama alanı kullanılır²⁹¹.

Nakamoto tarafından yayınlanan makalede Merkle Ağacı'nın sağladığı bir başka avantaj Basitleştirilmiş Ödeme Teyidi [Simplified Payment Verification (SPV)] olarak belirtilmiştir. Nakamoto tarafından öne sürülen bu model, ödemelerin full node çalıştırmadan onaylanabilmesini sağlar²⁹². SPV'de Merkle Ağacı sistemi kullanılarak sadece blok başlıkları indirilir. SPV'nin sağladığı bu tasarruf sayesinde mobil cihazlar gibi kapasitesi bilgisayarlara göre daha küçük cihazlarda ödemelerin onaylanabilmesi amaçlanmıştır.

2.2.3. Chaum Kasa Modeli, DigiCash ve eCash

David Chaum, Amerikan bir bilgisayar mühendisi ve kriptografıdır. Chaum tarafından yapılan çalışmalar elektronik paranın ve dijital paranın ilk örneklerini ortaya çıkarmıştır. Bununla birlikte bazı çalışmalarda ilk blok zincir modelinin de Chaum tarafından ortaya konduğu da savunulmaktadır²⁹³.

Chaum Kasa Modeli, David Chaum tarafından 1979 yılında ortaya konup, 1982 yılında doktora tezinde detaylı bir şekilde açıklanmıştır²⁹⁴. Chaum'a göre birbirine karşı güven duymayan örgüt ya da kuruluşlar kendi aralarında güven duyabildikleri yüksek

²⁸⁷ Nakamoto modeline benzer şekilde Türkçede “budama” anlamına gelebilmektedir.

²⁸⁸ Kaba tabirle blok zinciri içerdiği tüm kayıtlarıyla, bütün olarak çalıştırma.

²⁸⁹ <https://bitcoincore.org/en/download/>

²⁹⁰ Pruning oranını kullanıcılar değiştirebilmektedir.

²⁹¹ Bitcoincore, “*Bitcoin Core requires a one-time download of about 400GB...if you enable pruning, you can store as little as 6GB total without sacrificing any security...*”, <https://bitcoincore.org/en/download/> (Erişim:05.05.2022); Statista, “*Size of the Bitcoin blockchain from January 2009 to April 4, 2022*”, <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/> (Erişim: 05.05.2022)

²⁹² Nakamoto, 2018, s. 5.

²⁹³ Sherman vd., 2018, s.1.

²⁹⁴ Chaum, David L., Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups, University of California, Berkeley, 1982. https://chaum.com/wp-content/uploads/2022/02/chaum_dissertation.pdf (Erişim: 01.05.2022)

güvenlikli bir bilgisayar sistemi kurabilirler²⁹⁵. Chaum'un tezinin konusunu oluşturan bu fikir, blok zincir, kripto para ve akıllı sözleşmenin temel ideolojisine oldukça benzemektedir. Blok zincirler yapısı gereği "güven gerektirmeyen (trustless)" oluşumlardır. Yani ağı kullanan kişilerin birbirlerini, bir kuruluşu ya da üçüncü bir kişiyi tanıması ya da bunlara güvenmesi gerekmez. Nakamoto da bu durumu 2008 yılında "Güven yerine kriptografik kanıta dayalı bir elektronik ödeme sistemine ihtiyaç vardır; böyle bir sistem iki tarafın aralarında üçüncü bir aracıya ihtiyaç duymadan direkt olarak işlem yapabilmesini sağlar." şeklinde özetlemiştir²⁹⁶.

Sherman vd., Chaum Kasa Modeli'nin blok zincirin birçok özelliğini taşıdığını savunmaktadır²⁹⁷. Modelde işlemlerin imzalandığı, kaydedildiği ve yayınlandığı fiziki kasalar bulunmaktadır²⁹⁸. Kasalar bütün katılımcılar tarafından doğrulanabilir olacaktır²⁹⁹. Bu özellikleriyle sistemin blok zinciri andırdığı söylenebilir.

Kasa Modeli'nin ardında Chaum, çoğunlukla ödeme modelleri hakkında yaptığı çalışmalar ile tanınmaktadır. Bu noktada Chaum'un kör imza (blind signature) ile izlenemez ödeme modeli sunduğu 1983 tarihi çalışması oldukça önemlidir³⁰⁰. Kör imza, Chaum tarafından ortaya atılmış dijital imzanın özelleşmiş bir halidir. Bu sistemde gönderici ve alıcı arasında, gönderilen şeyin içeriğini bilmeden kör imza atan üçüncü bir kişi bulunmaktadır. Chaum, kör imza sistemi kullanılarak izlenemez bir ödeme modeli oluşturulabileceğinden bahsetmektedir³⁰¹. Bununla birlikte mevcut anonim ödeme araçlarının (kağıt para, madeni para) kontrol ve güvenlik konusunda ödeme kanıtının zor olması, hırsızlığın mümkün olması ya da yasadışı faaliyetler için kullanılabilmesi gibi sıkıntıları olduğunu belirtmektedir³⁰². Buna karşın Chaum sunduğu izlenemez ödeme sistemi sayesinde hem denetlenebilirliğin hem de bireysel mahremiyetin sağlanacağını düşünmektedir³⁰³. Chaum'un bu düşüncesi, denetlenebilirlik amaçlandığı için kripto paralardan çok dijital para sistemlerine yaklaşmaktadır.

²⁹⁵ Chaum, 1982, s. iv.

²⁹⁶ Nakamoto, 2008, s. 1.

²⁹⁷ Sherman vd., 2018, s. 1.

²⁹⁸ Sherman vd., 2018, s. 3.

²⁹⁹ Chaum, 1982, s. 3.

³⁰⁰ Chaum, David, "Blind Signatures for Untraceable Payments", *Advances in Cryptology*. Springer, Boston, MA, 1983. https://doi.org/10.1007/978-1-4757-0602-4_18 (Erişim: 05.05.2022)

³⁰¹ Chaum, 1983, s. 202.

³⁰² Chaum, 1983, s. 199.

³⁰³ Chaum, 1983, s. 203.

Chaum tarafından öne sürülen bir başka model, ilk kez 1985 yılında yayınlanan “Kimlik Tanılama Olmadan Güvenlik: Büyük Biraderi³⁰⁴ Hükümsüz Kılacak Ödeme Sistemleri³⁰⁵” adlı makalesinde bahsedilen “kart bilgisayar”dır. Kart bilgisayar modeli, Chaum tarafından 1987 yılında önceki makale revize edilerek “Kimlik Tanılama Olmadan Güvenlik: Büyük Biraderin Hükümsüz Kılacak Kart Bilgisayarlar³⁰⁶” makalesinde tekrar açıklanmıştır. Bu modelde bireyler kart şeklinde küçük bilgisayarlar para transferi yapabileceklerdi. Modelde bireyler kart bilgisayarını kullanmak için kendilerine özel, en az 40 basamaklı, gizli bir anahtara sahiptirler³⁰⁷. Kart bilgisayarların kaybolması ya da bozulması durumunda bireyler yeni kart bilgisayarlarına bu özel anahtarlarını girerek bilgilerine tekrar erişebileceklerdir. Bu model kripto para sahiplerinin varlıklarına erişebilmek için kullandıkları özel anahtarlara oldukça benzemektedir.

Modelin önemi, bu çalışmanın birinci bölümünde, elektronik para başlığında incelenen 28 Mart 2022 tarihli “Elektronik Para Birimi ve Güvenli Donanım Kanunu [Electronic Currency And Secure Hardware (ECASH) Act] teklifine (bill) benzemesidir. Söz konusu teklifte getirilmek istenen modelde de Chaum’un 1985 yılında önerdiği modele benzer bir şekilde para transferleri çevrimdışı, güvenilir donanım aygıtları ile yapılmaktadır.

Chaum ardından 1989 yılında “DigiCash” adı altında bir elektronik para şirketi kurmuştur. DigiCash bünyesinde markalaşan “eCash” ilk elektronik para uygulamalarından biridir. Bununla birlikte eCash İsviçre’nin Cenevre kentinde bulunan CERN’de 1994 yılında gerçekleştirilen ilk “Uluslararası Dünya Çapında Ağ³⁰⁸ Konferansı (International World Wide Web Conference)”nda tanıtılmış ve denenmiş olup, bu kullanım tarihteki ilk bilgisayar ağları arası elektronik para transferi olarak

³⁰⁴ “Büyük birader (big brother)”, George Orwell’in, “Bin Dokuz Yüz Seksen Dört (Nineteen Eighty-Four)” ya da “1984” olarak bilinen romanında yer alan ve sürekli insanları izleyen bir diktatördür. Chaum burada bireylerin mahremiyetine atıf yapmak amacıyla bu tabiri kullanmıştır.

³⁰⁵ Chaum, David, “Security Without Identification: Transaction Systems To Make Big Brother Obsolete”, *Communications of the ACM*, 1985/28 (10), s. 1030.
<https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf> (Erişim: 05.05.2022)

³⁰⁶ Chaum, David, “Security Without Identification: Card Computers To Make Big Brother Obsolete”, 1987. <https://ir.cwi.nl/pub/5519/5519D.pdf> (Erişim: 10.05.2022)

³⁰⁷ Chaum, 1987, s. 14.

³⁰⁸ “www”, Tim Berners-Lee tarafından 1989 yılında CERN’de geliştirilen, ilk kez 1991 yılında kamuya açık hale getirilen günümüzde baskın bir şekilde kullanılan internet servisi.

nitelendirilmektedir³⁰⁹. eCash'in bu önemi dışında diğer elektronik paralardan ayrılan yanı, açık anahtarlı şifrelemeden ve kör imzalamadan yararlanarak kullanıcılara gizlilik ve izlenemezlik sağlamasıydı. Sağladığı bu gizlilik ile günümüzdeki kripto paraları andırmaktadır.

1995 yılında Amerika Birleşik Devletleri'nin Boston şehrinde MIT³¹⁰ bünyesinde dördüncüsü düzenlenen Konferans çerçevesinde Michael Peirce ve Donal O'Mahony tarafından yayınlanan makalede³¹¹ de eCash'in web üzerinde yer alan ilk elektronik para olduğu belirtilip, "tamamen anonim elektronik para sistemi" olarak adlandırılmıştır.

eCash sistemindeki paralar banka tarafından oluşturulmakta, kişiler bankadaki hesaplarına eCash yatırıp buradan eCash çekebilirlerdi. eCash ile kabul eden kuruluşlardan alış veriş ya da ödeme yapılabilirdi³¹².

eCash ihracı yapan ilk banka 1995 yılında Amerika Birleşik Devletleri'ndeki "Mark Twain Bank" olmuştur³¹³. Bunu 1996 yılında "Deutsche Bank"³¹⁴, 1997 yılında "Bank Austria" ve "Den norske Bank" gibi bankalar takip etmiştir³¹⁵.

Chaum'un çalışmaları, özellikle internet üzerinde çalışan bir nakit modeli olarak eCash, kripto paralara giden yolda oldukça önemli çalışmalar olsa da, Chaum'un ortaya koyduğu modellerin merkezi bir aracıya ihtiyaç duyması (genellikle banka) bu modelleri elektronik para modellerine ve dijital para modellerine (CBDC) daha çok yaklaştırmaktadır³¹⁶. Bu durum Nakamoto tarafından

³⁰⁹ DigiCash, "World's first electronic cash payment over computer networks.", 1994. https://chaum.com/wp-content/uploads/2022/01/05-27-94-World_s-first-electronic-cash-payment-over-computer-networks.pdf

³¹⁰ Massachusetts Institute of Technology - Massachusetts Teknoloji Enstitüsü.

³¹¹ Peirce, Michael, Donal O'Mahony, "Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set", WWW4, 1995, <https://www.w3.org/Conferences/WWW4/Papers/228/> (Erişim:14.05.2022)

³¹² Peirce ve O'Mahony, 1995.

³¹³ DigiCash, "First Bank to Launch Electronic Cash", 1995, <https://chaum.com/wp-content/uploads/2022/01/10-23-95-First-Bank-to-Launch-Electronic-Cash.pdf> (Erişim: 14.05.2022)

³¹⁴ DigiCash, "DigiCash's Ecash to be Issued by Deutsche Bank", 1996, https://chaum.com/wp-content/uploads/2022/01/05-07-96-DigiCash_s-EcashTM-to-be-Issued-by-Deutsche-Bank.pdf (Erişim: 14.05.2022)

³¹⁵ DigiCash, "Bank Austria and Den norske Bank to issue ecash the electronic cash for the Internet", 1997, <https://chaum.com/wp-content/uploads/2022/01/04-14-1997-Bank-Austria-and-Den-norske-Bank-to-issue-ecashTM-the-electronic-cash-for-the-Internet.pdf> (Erişim:14.05.2022)

³¹⁶ Narayanan, Arvind, Jeremy Clark, "Bitcoin's Academic Pedigree: The Concept Of Cryptocurrencies Is Built From Forgotten Ideas In Research Literature", *Communications of the ACM*, 2017/60 (12), s. 1. <https://doi.org/10.1145/3134434.3136559> (Erişim:16.05.2022)

Birçok insanın e-para'lar hakkında bunların ümitsiz bir vaka olduğu konusunda kesin yargıları var; çünkü 1990'lardan itibaren bu konuda uğraşan bütün firmalara başarısız oldu. Bu sistemlerin başarısız olmasının ana nedeninin merkezi kontrole dayanmalarına inanıyorum. Bence burada (Bitcoin) ilk kez merkeziyetsiz ve güvene dayalı olmayan bir sistem deniyoruz.

şeklinde izah edilmişti³¹⁷. Bu durum Buterin tarafından da 2014 yılında “1980 ve 1990’ların anonim e-cash protokolleri, çoğunlukla Chaum körleştirmesi olarak bilinen kriptografik ilkelere dayalı, yüksek derece gizlilik sağlamaktaydılar. Fakat bu protokoller merkezi bir aracıya ihtiyaç duymakta olduklarından başarısız olup, popülerliklerini kaybettiler.” şeklinde açıklanmıştır³¹⁸. Tekrar belirtmek gerekir ki blok zincir üzerinde işleyen kripto paralarda herhangi bir aracı söz konusu değildir.

2.2.4. Bizans Generalleri Problemi

“Bizans generalleri problemi” ve bu problemin yol açtığı “Bizans hatası” ve bu hatanın kısmen çözüldüğü “Bizans hata toleransı” kavramları blok zincir için oldukça önemli kavramlardır. Blok zincir gibi dağıtık deftere dayalı teknolojilerde, ağır konsensüse ulaşabilmesi için bu hataya karşı dayanıklı olması gereklidir.

Bizans generalleri problemi ilk kez 1982 yılında, bu çalışmanın aşağısında incelenecek “Paxos protokolü” çalışmasını da gerçekleştiren Leslie Lamport, Robert Shostak ve Marshall Pease tarafından ortaya konmuştur³¹⁹. Belirtmek gerekir ki Bizans generalleri, ortaya konan sorunu açıklamak için kullanılan bir algoritmadır.

Çalışmada güvenilir bir sistemin bir veya birden fazla bileşenlerinin hatası ile başa çıkabilir olması gerektiği belirtilmiştir³²⁰. Bu doğrultuda bu durum bir sorun olarak Bizans generalleri üzerinden açıklanmıştır. Bir şehri kuşatan Bizans ordusu olduğu varsayılır. Bu ordu bölükler şeklinde birbirlerinden ayrı şekilde konumlanmakta ve her birinin başında bir general bulunmaktadır. Generaller birbirleri ile iletişimi haberciler vasıtasıyla gerçekleştirmektedir. Kuşatılan şehre saldırı kararı ya da geri çekilme kararı

³¹⁷ Nakamoto, Satoshi, “Bitcoin open source implementation of P2P currency”, P2P Foundation, 15.02.2009, <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493> (Erişim:17.05.2022)

³¹⁸ Buterin, 2014, s. 4.

³¹⁹ Lamport vd., “The Byzantine Generals Problem, *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, 1982/4 (3). <https://lamport.azurewebsites.net/pubs/byz.pdf> (Erişim: 12.05.2022)

³²⁰ Lamport vd., 1982, s. 382.

verilecektir. Bu konuda generallerin bir oy hakkı bulunup, mutabakata varılarak ya saldırılacak ya da geri çekilecektir³²¹. Örneğin toplamda dokuz generalin olduğunu varsayalım. Bu generallerden dördü saldırma, dördü geri çekilme yönünde karar vermiş olsun. Kararı dokuzuncu general belirleyecektir. Fakat bu general hain olup; geri çekilmeye karar veren generallere geri çekileceğini, saldırmaya karar veren generallere saldıracağını iletebilir. Bu durumda toplu bir saldırı ya da geri çekilme mutabakatına varılmadan ordunun yarısı saldırarak, diğer yarısı geri çekilecek; hem ordu, hem şehir kaybedilebilecektir. Bununla beraber habercilerin haberi ulaştıramaması, haberin düşmanın eline geçmesi ya da mutabakata varılsa bile bu emire bazı generallerin uymaması gibi sorunların da olabileceği hesaba katılmalıdır.

Bu problemde generallerin yerini, dağıtık sistemlerde düğümler (node) almaktadır. Lamport vd. sistemlerin konsensüsü sağlayamamasına sebep olabilecek Bizans generalleri probleminin çözümü hakkında aynı çalışmada çeşitli öneriler getirmiş, fakat bu önerilerin ekonomik olmadıklarını, gereğinden fazla zaman ve uğraş gerektirdiğini belirtmiştir³²². Lamport vd.'a göre getirilen çözümler ile bu problemin $3m+1$ katılımcının olduğu bir sistemin en fazla m kadar hain ile başa çıkabileceğini belirtmiştir³²³. Yani bu durum, dağıtık bir sistemde konsensüse ulaşabilmek ve sistemin hatasız bir şekilde devam etmesi için düğümlerin en az üçte ikisinin güvenilir olmasını gerektirmektedir.

Bizans generalleri problemi aslında üç temel konuyu içinde barındırmaktadır. İlk olarak merkezi otoritesi olmayan bir topluluğun üyeleri mutabakata varabilmelidir. İkinci olarak, bu mutabakat kötü niyetli katılımcılara rağmen sağlanabilmelidir. Üçüncüsü ise sistem hata toleranslı olmalıdır, yani sistemdeki katılımcıların biri ya da birkaçında bir aksaklık/hata meydana geldiğinde sistem doğru ya da doğruya yakın sonuçlar vermelidir³²⁴.

Bizans generalleri probleminin çözümü hakkında birçok çalışma yapılmış olup, problemin “efektif” ilk çözümü 1999 yılında Miguel Castro ve Barbara Liskov tarafından Pratik Bizans Hata Toleransı³²⁵ [Practical Byzantine Fault Tolerance (PBFT)] adı verilen

³²¹ Lamport vd., 1982, ss. 382-383.

³²² Lamport vd., 1982, ss. 400-401.

³²³ Lamport vd., 1982, s. 385.

³²⁴ Güven ve Şahinöz, 2018, s. 231.

³²⁵ Castro, Miguel, Barbara Liskov, “Practical Byzantine Fault Tolerance”, Massachusetts Institute of Technology, 1999. <https://pmg.csail.mit.edu/papers/osdi99.pdf> (Erişim: 17.05.2022)

bir konsensüs algoritmasıdır. Fakat bu algoritma da Lamport vd.'nin getirmeye çalıştığı çözümlere benzer bir şekilde sistemin en az üçte ikisinin güvenilir olmasını gerektirmektedir³²⁶.

İlk blok zincir olan Bitcoin zinciri Bizans Hata Tolerans'lıdır. Bitcoin'in sahip olduğu "Nakamoto Konsensüsü" adı verilen konsensüs modelinde Bizans hatası, "Proof-of-Work³²⁷ (PoW)" algoritması ve "oyun teorisi"nden faydalanılarak olasılıksal³²⁸ olarak çözülmüştür.

Aşağıda daha ayrıntılı olarak incelenecek PoW modelinde madencilerin üst üste sürekli blok üretmesini engellemek amacıyla, belirli bir zorlukta matematiksel problemlerin çözülmesi için işlem gücü harcamasını söz konusudur. Aksi bir durum, kaba bir örnek ile, herkesin boş bir kağıdın üzerine "200 TL" yazıp bunun para olarak kullanılabilmesi gibi olacaktır. PoW sistemi, Nakamoto tarafından da "Bizans Generalleri Problemi'ne çözüm" olarak nitelendirilmiştir³²⁹.

Nakamoto konsensüsü, PoW sistemi ve en uzun zincir kuralı takip edilerek sağlanır. Her ne kadar Bitcoin'in Bizans Hata Toleransı'na sahip olduğu belirtilse de, hata toleransına "tamamen" sahip olmadığı söylenebilir. Bunun sebebi "%51 atağı" denen bir durumun varlığıdır³³⁰. %51 atağı kısaca, kötü niyetli bir saldırganın, ağdaki hash oranının çoğunluğunu ele geçirmesi anlamına gelir. Bu tür bir atak, atak yapanın bir takım eylemlerde bulunabilmesine olanak sağlar. Atak yapan isterse işlemlerin bir kısmının ya da tamamının -ağda yayınlansa bile- onaylanmamasına sebep olabilir. Ayrıca kötü niyetli grubun ağın çoğunluğunu ele geçirdiği bu saldırıda "çifte harcama (double spending)" sorunu da gündeme gelebilecektir. Fakat belirtmek gerekir ki bu tür bir atakta bile iş kanıtı gerçekleştirilmeksizin kripto para üretimi ya da üretilen kripto paraların çalınması gibi durumlar blok zincirin yapısı gereği mümkün değildir.

³²⁶ Castro ve Liskov, 1999, s. 1.

³²⁷ Türkçeye "iş kanıtı", "iş ispatı", "emeğin kanıtı" olarak çevrilebilmekle birlikte, uygulamada bir terim haline geldiğinden bu çalışmada orijinal hali ile anılacaktır.

³²⁸ Yin vd., "Scalable and Probabilistic Leaderless BFT Consensus through Metastability", Cornell University, 2020, s. 1. https://assets.website-files.com/5d80307810123f5ffbb34d6e/6009805681b416f34dcae012_Avalanche%20Consensus%20Whitepaper.pdf (Erişim: 19.05.2022)

³²⁹ Nakamoto, Satoshi, Bitcoin P2P e-cash paper, Cryptography Mailing List, 13-11-2008, <https://satoshi.nakamotoinstitute.org/emails/cryptography/11/#selection-15.0-15.10> (Erişim: 19.05.2022)

³³⁰ Buterin, Vitalik, A Guide to 99% Fault Tolerant Consensus, 2018, https://vitalik.ca/general/2018/08/07/99_fault_tolerant.html (Erişim: 19.05.2022)

Çifte (mükerrer) harcama sorunu kısaca, aynı değerın bir kez harcıandıktan sonra ikinci kez tekrar harcıanabilmesi probleimidir. Örneğın nakit ile yapılan bir alış verişte çifte harcama ile karşılaşılmaz. X kişisi Y kişisine 50 TL vermiş ise, verilen 50 TL'nin sahibi artık Y kişisidir. X kişisi söz konusu 50 TL'yi tekrar harcıayamaz. Her ne kadar fiziki ortamda çifte harcama sorunu oluşmasa da, elektronik ortamda veriler rahatlıkla taklit edilebildiğinden bu sorun mevcuttur. Bununla birlikte elektronik ortamdaki bu sorunun üzerinden, güvenilir bir üçüncü taraf sayesinde gelmektedir³³¹. Bu tür transferlerde güvenilir üçüncü taraf bankalar ya da PayPal gibi şirketler olabilir. Bununla birlikte güvenilir üçüncü tarafın ancak kısmi bir güven sağlayabildiği söylenebilir. Çünkü kayıtların, işlemlerin tek bir merkezi yapıda, bu yapının tekelinde tutulması mutlak bir güven ve garanti sağlayamaz. Çünkü kayıt defterlerini tutan tek bir merkezin olması, bu merkezi yapıda tutulan verilerin çalınabileceği ve değiştirilebileceği gerçeğini engelleyemez³³².

İlk kripto para Bitcoin'den önce hiçbir yapı, çifte harcama problemini banka gibi güvenilir bir üçüncü taraf, merkezi bir otorite olmaksızın çözememiştir³³³. Merkezi otoritenin olduğu elektronik bir ödeme sisteminde çifte harcama sorunu, harcıanan her paranın harcıandıktan sonra merkeze geri dönmesi ve tekrar üretilmesi ile çözülmektedir. Yani bu tür bir sistemde paranın çifte harcıanmamış olması demek, ilk kullanıldığında direkt olarak merkez tarafından darp edilmiş olması demektir. Bununla birlikte merkez ayrıca yapılan bütün işlemlerin bilgisine sahiptir ve dolayısıyla hangisinin önce yapıldığından haberdardır³³⁴. Fakat görüldüğü üzere bu tür bir sistem tamamen merkeze ya da güvenilir üçüncü taraf dediğimiz yapıya dayanmaktadır. Bu merkezi yapıda meydana gelebilecek bir güven sorunu ya da hata, bütün harcama sisteminin çökmesi anlamına gelebilecektir.

Blok zincirde ise yapılan işlemler zaman damgası ile işaretli olmaları ve işaretli olan bu işlemlerin herkese açık bir şekilde yayınlanarak zincirdeki yerini almaları ile çifte harcama problemi çözülmüş olur³³⁵. Bir işlem iş kanıtı ile matematiksel olarak zincirde önceki işlemlere bağlı olduğundan değiştirilemez ve geriye döndürülemez hale gelir. Bu

³³¹ Güven ve Şahinöz, 2018, s. 221

³³² Güven ve Şahinöz, 2018, s. 222.

³³³ Nakamoto, 2008, s. 1.

³³⁴ Nakamoto, 2008, s. 2.

³³⁵ Nakamoto, 2008, s. 2.

tür bir sistem merkezi bir otorite ya da güvenilir bir üçüncü tarafın çifte harcamanın gerçekleşmediği garantisine ihtiyaç duymayacaktır.

Blok zincir merkezi otorite olmadan çifte harcama sorununu çöze de, yukarıda bahsedildiği üzere %51 atağı gerçekleştiğinde, kötü niyetli saldırganlar ağıın çoğunluğunu ele geçirdiğinden çifte harcamaya da sebebiyet verebileceklerdir. Nakamoto konsensüsünde, yukarıda bahsedildiği üzere PoW sistemi ve uzun zincirin takip edilmesiyle mutabakata varılır. %51 atağı gerçekleştiğinde ana zincirin yanında saldırganların oluşturduğu ikinci bir zincir oluşacaktır. Ağıın hash gücünün çoğunu saldırganlar elinde bulundurduğundan doğal olarak bu ikinci zincir daha uzun olacak, uzun olan zincir takip edilir kuralına göre bu zincir takip edilebilecektir. Belirtmek gerekir ki, %51 atağının oluşmadığı normal şartlarda da ana zincirin yanında paralel zincirler oluşabilmektedir. İki ya da daha fazla zincirin aynı anda ağda dolaşmaya başlaması bir problem oluşturmaz, çünkü madenciler tarafından hesaplama zorluğu daha yüksek olan ve daha uzun olan zincir kabul edilecek diğer zincirlerdeki bloklar “öksüz (orphan) blok” haline gelecek ve dışlanacaktır. Öksüz blokta gerçekleştirilen işlemler ise işlem havuzuna geri bırakılacaktır. %51 atakta da aslında öksüz bloklar oluşturulup bundan faydalanılmaktadır.

Yukarıda, ilk blok zincir olan Bitcoin’de Bizans hatasının PoW ve oyun teorisi ile çözüldüğünden bahsedilmişti. Oyun teorisi bu çalışmada açıklanamayacak kadar uzun olduğundan, ilk kez Nakamoto tarafından ortaya konan blok zincirin bu teoriden nasıl faydalandığından bahsedilecektir.

Acımasız tetik/tetikçi (grim trigger), oyun teorisinde tekrarlayan oyunlarda (blok zincirin de olduğu gibi) ortaya çıkan bir kavramdır. Nash Dengesi durumuna ulaşmış ve tekrar eden oyunlarda oyuncular, dengenin etkisiyle birbiriyle işbirliği halinde olmaya meyleder. Bu kavram bir firavun örneği üzerinden açıklanacaktır³³⁶.

Örneğin bir Mısır firavunu olduğunu düşünelim. Bu firavun, ilahi bir güce sahip olduğunu, Tanrı’dan devşirilmiş bir gücü olduğunu iddia etmektedir. Bir gün yaşanan bir kaos ortamında bu firavun öldürülürse, firavunun bahsettiği gibi ilahi bir güce sahip olmadığı anlaşılacaktır. Firavunun ilahi bir güce sahip olmaması demek, firavunun yerine geçecek olan veliahtların da ilahi güce sahip olmayacakları anlamına gelir. Oluşacak bu

³³⁶ Güven ve Şahinöz, 2018, s. 308.

genel kanaat sonucu veliahtların kalabalıklar üzerinde güç tahakküm etmesi imkansız hale gelecektir. Çünkü kalabalıklar aynı şekilde veliahtları da zorlayacaktır. Sonuç olarak firavunun öldürülmesi, içinden çıkılmaz bir döngünün başlaması haline gelecektir. Ülke yönetilemez olacak, bu durum firavunun yanında kalabalıkların da cezalandırılması anlamına gelecektir. Bu tür tekrarlanan oyunları daha önce tecrübe etmiş kişiler en doğru hamlenin “acımasız tetiği” en baştan çekmemek yani firavunu öldürmemek olduğuna kanaat getirirler³³⁷.

Acımasız tetiğin blok zincir ile olan ilişkisi de %51 atağı iledir. Normal şartlarda bir grup madenci geçerli olmayan bir blok yaratarak yeni bir zincir başlatsalar bile diğer madenciler bu alternatif zinciri takip etmeyeceklerdir. Çünkü diğer madenciler geçersiz olduğu sonradan anlaşılacak bloğa eklenecek her yeni bloğun da geçersiz olacağını bilmektedirler. Fakat %51 atağının olduğu bir durumda, uzun olan zincir atağı yapan grubun oluşturduğu bloklardan ibaret olacağından kural gereği uzun olan bu zincirin takip edileceği beklenir. Fakat burada oyun teorisi ve “acımasız tetik” devreye girmektedir. Hash oranının çoğunluğunu elde eden kötü niyetli grup, firavunu yani ana zinciri öldürüp, onun yerine veliahdını yani kendi getirdikleri sahte zinciri devreye soksalar bile; artık tetik bir kez çekildiğinden, başka bir çoğunluk da bu sahte zinciri öldürüp başka bir sahte zincir oluşturabilir ve bu döngü sistemi çökertene kadar devam eder. Bu sebeple %51 atağı gerçekleştiren grup atağı gerçekleştirirse, bu atağın aslında kendi ayağına sıkması anlamına geleceğini baştan bilmektedir³³⁸. Bu nedenle blok zincirde Nash dengesinden bahsedilebilir, istikrarlı ana zincir takip edilir; ağa katılanlar kendileri için en iyi durumun ağa katılan topluluğun da en iyi durumunu oluşturduğu noktada gerçekleşeceğini bilir.

Bizans hata toleranslı blok zincirin üzerinde gerçekleşebilecek %51 atağı ile ilgili açıklamaları bitirmeden önce, yukarıda %51 ile ilgili yapılan açıklamaların PoW sistemi üzerinden yapıldığını belirtmekte fayda vardır. Kripto paralarda oldukça kullanılan bir diğer mekanizma olan Proof-of-Stake³³⁹ (PoS) sisteminde PoW’daki anlamıyla bir madencilik söz konusu değildir. PoS sisteminde her katılımcı ne kadar kripto para tutuyorsa o oranda blok oluşturulma görevinin kendisine verilmesi söz konusu olup, blok

³³⁷ Güven ve Şahinöz, 2018, ss. 308-309

³³⁸ Güven ve Şahinöz, 2018, ss. 307-316.

³³⁹ Türkçeye “hisse ispatı” şeklinde çevrilebilmekle birlikte, blok zincirler hisseleri olan şirketler olmadıklarından, çalışmada bu tabir yerine orijinal ismi ve PoS kısaltması ile anılacaktır.

içerisinde meydana gelen işlemlerden komisyon elde edilecektir³⁴⁰. Bu doğrultuda PoS sisteminde %51 atağın gerçekleştirilebilmesi için, atağı gerçekleştirenlerin ağda stake edilen kripto paraların çoğunluğunu elinde bulundurması gerekmektedir³⁴¹.

%51 atağın uygulamada gerçekleşen örneklerinden de bahsedilmesinde fayda vardır. Öncelikle belirtmek gerekir ki 2009 yılından bu yana işlemekte olan Bitcoin zincirinde şu ana kadar %51 atak gerçekleşmemiştir; bu andan sonra da gerçekleşebilmesi şimdilik pek mümkün gözükmemektedir; çünkü %51 atağı gerçekleştirebilmek için katlanılması gereken maliyet oldukça artmıştır. Fakat diğer kripto paralarda bu atak ile karşılaşmıştır. Örneğin bir Ethereum çatalı³⁴² olan “Ethereum Classic” 2020 yılının ağustos ayı içerisinde üç kez %51 atağa maruz kalmıştır³⁴³. Bir “Bitcoin Cash” çatalı ve doğal olarak Bitcoin çatalı olan “Bitcoin SV”, 3 Ağustos 2021’de %51 atağa maruz kalmış ve atak yüzlerce blok devam etmiştir³⁴⁴. Bununla birlikte atak gerçekleşmemiş olsa da oldukça güncel bir örnek olarak, 9 Mayıs 2022 tarihinde başlayan ve market değerinde yaklaşık 40 milyar dolarlık bir erimenin gerçekleştiği “Luna” ve “Ust”de değer düşüşü sebebiyle (Luna’da %99’un da üstünde) atak yapılması maliyeti de oldukça düştüğünden, bu durum engellenmek için Terra zinciri 12 Mayıs 2022’de durdurulmuştu³⁴⁵. Ayrıca belirtmek gerekir ki %51 atağa daha dayanıklı bir şekilde oluşturulan ağlar da mevcuttur. Örneğin oldukça yeni bir blok zincir ağı projesi olan Mina ağı, blok zincir büyüklüğünü yalnızca 22 kilobayt ile tutarak bütün kullanıcıların ağı full node çalıştırmasını olanak sağlayarak ağın daha merkeziyetsiz hale gelmesini, dolayısıyla %51 atağa karşı daha dayanıklı olmasını amaçlamaktadır³⁴⁶.

³⁴⁰ Güven ve Şahinöz, 2018, s. 78.

³⁴¹ Ethereum, “Proof-of-Stake (PoS)”, <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> (Erişim: 20.05.2022)

³⁴² *İng.* fork. Çatallanma.

³⁴³ Voell, Zack, “Ethereum Classic Hit by Third 51% Attack in a Month”, Coindesk, 30.08.2020, <https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/> (Erişim: 20.05.2022)

³⁴⁴ Gkritsi, Eliza, “BSV Suffers 51% Attack: Report”, Coindesk, 04.08.2021, <https://www.coindesk.com/markets/2021/08/04/bsv-suffers-51-attack-report/> (Erişim: 20.05.2022)

³⁴⁵ Terra, “The Terra blockchain was officially halted at a block height of 7603700. <https://lcd.terra.dev/blocks/latest> Terra validators have decided to halt the Terra chain to prevent governance attacks following severe \$LUNA inflation and a significantly reduced cost of attack.”, 12.05.2022

https://twitter.com/terra_money/status/1524785058296778752?s=20&t=MU8IOWUnw4ZrS4nxxCtYFA (Erişim: 20.05.2022)

³⁴⁶ <https://minaprotocol.com/> (Erişim: 08.08.2022)

Son olarak Bizans hata toleransı ile blok zincir dışındaki uygulamalarda da pekâlâ karşılaşılabileceğini belirtmek gerekir. Örneğin Boeing 777 ya da Boeing 787 gibi uçuş kontrol sistemleri Bizans hata toleranslıdır; çünkü bu sistemler gerçek zamanlı sistemler olup en küçük uyumsuzluk bile feci sonuçlara davetiye çıkarabilir.

2.2.5. Kripto Anarşist Manifesto

Blok zincir ve kripto parayla fikir temelinde ilk kez 1988 yılında Timothy C. May tarafından yayınlanan “Kripto Anarşist Manifesto (The Crypto Anarchist Manifesto)” bildirisinde karşılaşılmaktadır³⁴⁷. May tarafından ortaya atılan kripto anarşist topluluk fikrinde, iki kişi birbirinin gerçekte kim olduğunu ya da yasal kimliğini bilmeden mesajlaşabilir, iş ilişkisi kurabilir ya da elektronik sözleşmeler imzalayabilirler³⁴⁸. May’e göre gerçekleştirilen bütün bu etkileşimler şifrelenmiş ve kurcalamaya dayanıklı kriptografik verilerin dolaştığı, takip edilemez protokoller marifetiyle gerçekleştirilecektir. May’e göre kişisel bilgisayarlar ve ağlar bu fikri gerçekleştirebilecek kapasite ve hıza ancak ulaşmıştır. Yazıda ayrıca bu konseptin anonim ve dijital bir piyasa oluşturacağı; konseptin uyuşturucu ticareti yapanlar, vergi kaçırıcılar tarafından kullanılabilirliği; adam kaçırmaya veya suikast ticareti şeklinde kötü bir piyasa da oluşturabileceğini ve bu nedenlerle devlet tarafından yasaklanmak isteneceğini; fakat bunun söz konusu modelin yayılmasını durdurmayacağı düşünülmektedir³⁴⁹.

Özetle May, merkezi bürokrasinin merkezi olmayan kriptografiyle, merkezi otorite kontrolünün birey özgürlüğüyle, ulus-devlet yapısının ise sınırları olmayan çok katılımlı network/topluluk ile değiştirilmesi gerektiğinden bahsetmektedir.

2.2.6. Paxos Protokolü

May’in kripto anarşist manifestosu fikir düzeyinde kaldığından, Leslie Lamport tarafından 1989 yılında ortaya çıkarılan Paxos protokolü, blok zincirin bir model olarak

³⁴⁷ May, Timothy C., 1988, The Crypto Anarchist Manifesto, 1988.

<https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html>
(Son erişim: 03.04.2022)

³⁴⁸ May, 1988.

³⁴⁹ May, 1988.

ilk görünümü olarak kabul edilebilir³⁵⁰. Paxos, konsensüse ulaşmak için oluşturulmuş bir dağıtık algoritma protokolüdür³⁵¹. Protokol ilk kez Lamport'un 1990 tarihli "*The Part-Time Parliament*" yazısında açıklanmakla birlikte bir makale olarak 1998 yılında yayınlanmıştır³⁵².

Protokolün ismi ve dayandığı fikir, Ege Denizi'nde bulunan bir ada olan Paxos'ta uygulandığı düşünülen bir yasama sistemine dayanmaktadır. Paxos önceden teokrazi ile yönetilmekteyken bir süre sonra parlamenter sisteme geçmiştir. Parlamenter sistem birtakım sorunları beraberinde getirmiştir; parlamentodaki üyeler bütün zamanlarını burada geçirmektense adanın zenginlik kaynağı olan ticaret ile uğraşmak istemektedirler. Bu nedenle Paxos parlamentosu faaliyetleri, üyeleri farklı zamanlarda parlamentoya girip çıkmasına rağmen işleyişini sorunsuz devam ettiren bir şekilde yürümektedir. Bu doğrultuda Paxos parlamento üyelerinin her birinde parlamentoda alınan kararların yazıldığı bir defter bulunmaktadır; parlamentoda kararları yazıya geçiren ayrıca bir sekreter bulunmaz. Bu defterlere alınan kararlar sıra sayılarıyla birlikte, üyeler tarafından, üzerinde oynama yapılamayacak şekilde mürekkep ile yazılmaktadır. Örneğin üyelerden birinin defterinde karar şu şekilde yazılmış olabilir:

"155: Zeytinyağı vergisi ton başına 3 drahmidir."

Üye, parlamentonun aldığı 155. kararı deftere mürekkep ile yazmıştır. Parlamentonun "defterlerin tutarlılığı" kuralına göre 155. karar bütün defterlerde aynı şekilde yazılmış olmalıdır. Bununla birlikte bir üyenin defterinde yazılı bu kural, diğer üyenin bu kural koyulurken mecliste bulunmaması ve kararın geçtiğini henüz öğrenmemiş olması nedeniyle yazılmamış olabilir. Yine de farklı gruplar tarafından, farklı zamanlarda, birbirinden habersiz bir şekilde, aynı sıra sayılarıyla farklı kararlar geçme ihtimali bulunmaktadır. Örneğin bir grup:

"37: Tapınak duvarına resim yapmak yasaktır."

³⁵⁰ Yaga vd., 2018, s.2.

³⁵¹ Ataşen, Kerem, "Paxos Algoritması", <https://bag.org.tr/?p=508>. (Son erişim: 30.03.2022); Paxos (bilgisayar bilimi), [https://stringfixer.com/tr/Paxos_\(computer_science\)](https://stringfixer.com/tr/Paxos_(computer_science)). (Son erişim: 30.03.2022)

³⁵² Lamport, Leslie, "The Part-time Parliament.", *ACM Trans. Comput. Syst.*, 1998/16 (2), 133–169. <https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Part-Time-Parliament.pdf> (Son erişim: 30.03.2022)

şeklinde bir karar alıp meclisi terk ettikten sonra, bundan tamamen habersiz başka bir grup meclise girip aynı sıra sayısıyla:

“37: *İfade özgürlüğü garanti altına alınmıştır.*”

şeklinde apayrı bir karar almış olabilir. Bu durumun önlenmesi için Paxos parlamento sistemi, mecliste karar alınabilmesi için üyelerin çoğunluğunun aynı anda mecliste bulunması, meclise belirli bir süre hiçbir üyenin girip çıkmaması ve alınan kararın o an parlamentoda bulunan bütün üyelerce defterlere işlenmesi şartlarına dayanmıştır³⁵³.

Lamport tarafından açıklanan Paxos protokolündeki konsensüs modeli, Paxos parlamentosundaki modele benzemektedir. Paxos protokolünde parlamento üyelerinin yerini bilgisayarlar-düğüm (node) almaktadır. Paxos protokolünde düğümlerin üç rolü olabilir, bunlar önerenler, kabul edenler ve öğrenenlerdir³⁵⁴. Bir düğüm birden fazla rolü aynı anda alabilir³⁵⁵. Paxos algoritması, karara varabilmek ve ilerleme kaydedebilmek için bir lidere ihtiyaç duyar. Lider aynı zamanda seçkin bir öneren ve öğrenen rolüne sahiptir³⁵⁶. Bir teklif sırasında birden fazla lider bulunabilir. Bu liderler sürekli çelişen öneriler ileri sürerek ilerlemeyi duraksatabilir. Sonuç olarak protokol, nihai bir lider seçildiğinde ilerlemeye devam eder.

Paxos protokolünde sadece önerilen değerler için, tek bir sonuca varılır ve algoritma tarafından bir değer üzerinde nihai bir sonuca varılmadıkça düğümlere değer iletilmez³⁵⁷. Paxos algoritması ile konsensüse varmak için, sistemdeki işlemcilerin çoğunluğunun aynı sonuç üzerine uzlaşmaya varması gerekmektedir. Eğer işlemci topluluğundaki herhangi bir düğümün verdiği karar çoğunluğun verdiği karardan farklı ise söz konusu düğüm kararında ısrarcı olmaz ve çoğunluğun kararını kabul edip, bildirir ve ilerlemeyi devam ettirir³⁵⁸. Konsensüse katılan işlemciler sadece kendi önerileri için

³⁵³ Lamport, 1998, ss. 2-3.

³⁵⁴ Charapko vd., “Bridging Paxos and Blockchain Consensus.”, *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, s. 2
<https://cse.buffalo.edu/~demirbas/publications/bridging.pdf> (Erişim: 31.03.2022)

³⁵⁵ Krzyzanowski, Paul, “Understanding Paxos”, 2019.

<https://people.cs.rutgers.edu/~pxk/417/notes/paxos.html>

³⁵⁶ Lamport, Leslie, Paxos Made Simple, 2001, ss. 7-8. <https://lamport.azurewebsites.net/pubs/paxos-simple.pdf>

³⁵⁷ Lamport, 2001, s.1. ; Yalçınsoy, Hakan, “Paxos Konsensüs Protokolü”,
<https://hknycnsy.medium.com/paxos-konsensüs-protokolü-f7787e57df3c>

³⁵⁸ Ataşen, 2019.

değil, bütün öneriler için sonuca varmalıdır. Karar kılınan sonuç herkes tarafından bilinebilir olmalıdır. Paxos protokolü de tıpkı Paxos parlamentosu gibi üyeleri sürekli katılım göstermese de işleyişine devam edebilecek özelliğe sahiptir.

Paxos protokolünün çalışma prensiplerinden özellikle işlemlerin aktarılış aşamasının ve lider seçim aşamasının blok zincir ile benzerlik göstermesi, Paxos protokolünün blok zincirin öncülerinden olduğunu göstermektedir³⁵⁹. Bununla birlikte Paxos protokolü ile blok zincir arasında birçok farklılığın da olduğunu söylemek mümkündür. Paxos protokolü çok daha küçük kümeler ile işleyiş gösterirken blok zincir üzerinde binlerce katılımcı ile çalışmaktadır³⁶⁰. Bununla beraber Paxos protokolünde seçilen lider birden sonraki bloklarda da liderlik gösterebilirken blok zincirde aynı liderin ağı kontrol altında tutmasının önlenmesi için sadece birkaç mikro blok süresince liderliği korunmaktadır³⁶¹.

2.2.7. Dijital Belgelerin Zaman Damgası İle Doğrulanması

Lamport'un oluşturduğu Paxos protokolünün yanında, 1991 yılında Stuart Haber ve W. Scott Stornetta'nın zaman damgası³⁶² imzası ile kriptografik şekilde şifrelenmiş bir zincirin anlatıldığı çalışması, blok zincir için bir diğer önemli çalışmadır³⁶³. Çalışmada yazı, ses, resim, video gibi dijital dokümanların ne zaman oluşturulduğunun ya da üzerinde ne zaman değişiklik yapıldığının zaman damgası ile doğrulanması ve geriye dönük değiştirilememesi üzerinde durulmaktadır³⁶⁴. Haber ve Stornetta, dijital belgelerin üzerinde yapılan değişikliklerin fiziki materyalleri üzerinde herhangi bir iz bırakmayacağından dolayı dijital belgenin kendisi üzerinde, yani veri düzeyinde bir damgalama yapılması gerektiğini öne sürmüşlerdir³⁶⁵.

³⁵⁹ Charapko vd., 2018, s. 8.

³⁶⁰ Charapko vd., 2018, s. 7.

³⁶¹ Charapko vd., 2018, s. 4.

³⁶² Zaman damgası günümüzde dijital doğrulama alanında sıkça kullanılmakta olup Türk hukukunda da 5070 sayılı Elektronik İmza Kanunu'nda "*Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt*" şeklinde tanımlanarak kendine yer bulmuştur.

³⁶³ Haber, Stuart., Scott Stornetta, "How to Time-Stamp a Digital Document.", In: Menezes, A.J., Vanstone, S.A. (eds) Advances in Cryptology-CRYPTO' 90. CRYPTO 1990. Lecture Notes in Computer Science, vol 537. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-38424-3_32 (Son erişim: 02.04.2022)

³⁶⁴ Haber, Stornetta, 1991, s. 437.

³⁶⁵ Haber, Stornetta, 1991, s. 439.

Lamport'un oluşturduğu Paxos protokolü ile Haber ve Stornetta'nın dijital belgelerin zaman damgası ile doğrulanması modeli birlikte blok zincir tasarımının oluşmasını sağlayan erken dönem çalışmalarıdır³⁶⁶. Nakamoto tarafından Bitcoin makalesinde Haber ve Stornetta'nın 1991 tarihli makalesine atıfta bulunulması ve makalede yapılan toplam sekiz atıftan üçünün Haber ve Stornetta'nın çalışmalarına ait olması bu çıkarımı desteklemektedir. Gerçekten de Haber ve Stornetta'nın çalışmasında bahsetmiş oldukları prototip kullanılarak dijital belgelerde değişiklik yapılmadığının gözlemlenebilmesi ve geriye dönük değişikliklerin yapılmasının önlenmesini sağlayan model, blok zincirin önceki bloklar üzerinde değişiklik yapılamaması özelliğine oldukça benzemektedir. Bununla beraber bu modelde merkezileştirilmiş (centralized) bir zaman damgası servis sağlayıcısına (time-stamping service) ihtiyaç olması, blok zincirin merkeziyetsiz (decentralized) yapısından ayrılmaktadır.

2.2.8. b-Money

Blok zincir ve blok zincirin ilk uygulama alanı olan kripto paraların erken dönem görünümülerinden bir diğeri 1998 yılında Wei Dai tarafından yayınlanan, Nakamoto tarafından yayınlanan makalede de yapılan sekiz atıftan ilki³⁶⁷ olan "b-money" yazısıdır³⁶⁸. Wei Dai, Timothy C. May'in 1988 tarihli bildirisini merkeze alıp, May'in bahsettiği kripto anarşist topluluğun işleyebilmesi için bir mübadele aracına (para) ihtiyaç duyacağını belirtmektedir.

Dai, çalışmasında iki tür para protokolü önermiştir. İlk protokolde bütün katılımcılar kendi bilgisayarlarında her bir müsteara (pseudonym) ne kadar para ait olduğunu belirten bir veri tabanı bulundurlar. Bu veri tabanlarının bütünü güncellenerek paranın aidiyetini belli eder. Dai ilk protokolde beş konu üzerinde durmaktadır.

Dai'ye göre ilk konu paranın nasıl oluşturulacağıdır. Bu protokolde para, herkes tarafından oluşturulabilir; fakat parayı oluşturmak isteyen kimselerin daha önce çözülmemiş bir hesaplama problemini çözmeleri gerekmektedir. Üretilen paranın

³⁶⁶ Yaga vd., 2018, s.2.

³⁶⁷ Nakamoto, 2008, s. 1.

³⁶⁸ Dai, Wei, "b-money", 1998, <http://www.weidai.com/bmoney.txt> (Son erişim: 03.04.2022)

miktarını da hesaplamının zorluğu belirlemektedir. Örneğin bir hesaplama probleminin çözülmesi 100 saat sürüyorsa ve 100 saatlik hesaplama süresini satın almak piyasada 5 birime mal oluyorsa bu hesaplama problemini çözen kimse 5 birim değerinde para (b-money) elde edecektir.

Dai'ye göre ikinci konu paranın nasıl aktarılacağıdır. Bu durumda örneğin “abc” müstearına sahip bir kimse “dfg” müstearına sahip kimseye para göndermek istediğinde ağa “*dfg'ye 100 birim para gönderiyorum*” şeklinde kendisi tarafından imzalanmış bir mesaj gönderir. Bu mesajın yayınlanmasından sonra ağdaki herkes abc'nin hesap kaydında kesinti yapar; dfg'nin hesabına da ekleme yapar. Eğer bu işlem abc'yi eksi bakiyeye düşürecek miktarda ise abc'nin ağa yolladığı mesaj görmezden gelinir.

Dai'ye göre üçüncü konu ağdaki sözleşmelerin geçerliliğidir. Geçerli bir sözleşme taraflardan birinin temerrüde düşmesi durumunun engellenmesi için bir maksimum miktar tazminat ihtiva etmelidir. Sözleşme ayrıca anlaşmazlık olduğu durumda bunu çözebilecek bir hakem de bulundurmalıdır. Sözleşme ağda yayınlanmadan önce, tarafların tümü ve hakem ile kendi müstearları kullanılarak imzalanmak zorundadır. Sözleşme taraflar ve hakem tarafından imzalandıktan sonra yayınlanır. Yayınlanan sözleşmedeki tazminat miktarları, ağ katılımcıları tarafından sözleşmede belirlenmiş miktarda sözleşme tarafları ve hakemin bakiyesinden kesinti yapılır; yapılan kesintiler sözleşmeye özel bir sözleşme hesabı açılarak ve bu hesaba eklenerek veri tabanlarına işlenir. Sözleşme, kesintiler sonucu taraflardan birinin hesap kaydında eksi bakiye oluşması ile sonuçlanmadığı sürece aktif hale gelecektir. Eğer kesinti eksi bakiye oluşturuyorsa sözleşme görmezden gelinecek ve hesap kayıtları sözleşme önceki duruma dönecek şekilde düzeltilenecektir. Ağdaki örnek bir sözleşme şu şekilde olabilir:

“abc, P probleminin çözümünü 0:0:0 1/1/2001 tarihinden önce dfg'ye göndereceğini kabul eder. dfg, 0:0:0 1/1/2001 tarihinden önce abc'ye 100 birim para göndereceğini kabul eder. xyz, bir anlaşmazlık durumunda hakem olacaktır. abc, temerrüt durumunda maksimum 1000 birim tazminat ödemeyi kabul eder. dfg, temerrüt durumunda maksimum 500 birim tazminat ödemeyi kabul eder. xyz temerrüt durumunda maksimum 200 birim para ödemeyi kabul eder.”

Dai'ye göre dördüncü konu sözleşmenin sonuçlanmasıdır. Sözleşme temerrütlü ya da temerrütsüz sonuçlanabilir. Bu durumda iki duruma göre taraflar şu örnek mesajları imzalayarak ağda yayınlar:

“SHA-1³⁶⁹ hash H algoritmali sözleşme tazminatsız sonuçlanmıştır.”

“SHA-1 hash H algoritmali sözleşme takip eden tazminatlar ile sonuçlanmıştır: ...”

Mesajlar imzalı bir şekilde yayınlandıktan sonra ağdaki katılımcılar sözleşme öncesinde tarafların hesap kayıtlarından maksimum tazminat miktarında düşülen bakiyeleri geri ekler, sözleşme hesabı kapatılır ve temerrüt gerçekleşmişse tazminat tarifesi uyarınca bakiye kesilir ya da eklenir.

Dai'ye göre beşinci ve son konu ise sözleşmenin icra kabiliyetidir. Sözleşmenin tarafları hakemin varlığıyla bile uygun bir çözüme ulaşamıyorlarsa tazminat tarifesi yayınlarlar. Ağ katılımcıları bu tarifeye göre hesap kaydı üzerinde değişiklikleri gerçekleştirirler.

Wei Dai tarafından öne sürülen ikinci protokolda ise hesap kayıtları bütün ağ katılımcıları yerine ağ katılımcılarının oluşturduğu küme topluluklarında (sunucu) bulundurulur. Aktarım işlemleri bu sunucularda yayınlanarak doğrulanır. Sunucular, güvenilirliklerini sağlamak için özel bir hesapta belirli bir miktar para tutmak zorundadır. Bu para ayrıca kötüye kullanımları cezalandırmak ya da kanıtını ödüllendirmek için kullanılır. Ayrıca her sunucu düzenli aralıklarla, üretilen para miktarını ve para sahipliklerini belirten kendi veri tabanını sunmak zorundadır. Her katılımcı yayınlanan bu veri tabanı ile kendi bakiyesinin uyuşup uyuşmadığını ve toplam para miktarının toplam üretilen para miktarından fazla olmadığını kontrol edebilir. Bu sayede sunucuların kötü niyetli olarak ücretsiz bir şekilde para üretmelerinin önüne geçilmektedir³⁷⁰.

Dai'nin önerdiği “b-money” modeline Nakamoto tarafından atıf yapılması; market değeri en büyük ikinci³⁷¹ kripto para birimi ve zinciri olan Ethereum'un kentilyonda biri olan en küçük birimi “wei”³⁷² ve Ethereum tabanında değeri kontratlar marifetiyle 1 ABD dolarına eşit tutulan “Dai” isimlerinin Wei Dai'ye ithafen konması,

³⁶⁹ “SHA-1” yani “Secure Hash Algorithm”, Amerikan Ulusal Güvenlik Dairesi (NSA) tarafından tasarlanmış bir kriptografik hash fonksiyonudur.

³⁷⁰ Dai, 1998.

³⁷¹ <https://coinmarketcap.com/> (Son erişim: 04.04.2022)

³⁷² Buterin, 2014, s. 30.

bu çalışmanın blok zincir ve kripto paralar için ne derece önem taşıdığını göstermektedir. Gerçekten de Dai'nin 1998 yılında önerdiği iki protokol de kripto paralar ile önemli ölçüde benzerlikler taşımaktadır.

İlk olarak Dai modelinde paranın üretimi, Proof-of-Work (PoW) sistemini kullanan kripto paralardaki para üretimine oldukça benzemektedir. Dai tarafından oluşturulan model, kripto para üretimi hakkında öne sürülen ilk model olarak kabul edilmektedir³⁷³. PoW sistemi çoğu kripto paranın temelini oluşturduğundan aşağıda ayrı bir başlık altında incelenecektir.

Wei Dai'nin b-money modelinde de ağdaki para, PoW yöntemi ile bilgisayarların daha önceden çözülmemiş belirli bir zorluktaki hesaplama problemini çözmeleri ile üretilmekteydi. Üretilen paranın değeri ve miktarı problemin zorluğu ile ilişkilidir. Başta ilk kripto para olan Bitcoin ve diğer çoğu kripto para da PoW sistemi kullanılmaktadır³⁷⁴. PoW sistemi kullanılan kripto paralarda bloklar belli bir işlemci gücü kullanılarak kazılır ve bulunur; bloğu bulan kişiler üretilen para ile ödüllendirilir.

Dai'nin modeli ile blok zincirdeki bir diğer benzerlik ise işlemlerin herkes tarafından bilinebilir bir şekilde yayınlanmasıdır³⁷⁵. Gerçekleştirilen işlemler herkes tarafından bilinebilir ve kontrol edilebilir şekilde ağda yerini alır. Haber ve Stornetta'nın yukarıda değinilen zaman damgası modelinde de benzer bir özellik olsa da, Dai modeli ve blok zincir bu özelliği merkeziyetsiz bir biçimde çözebilirken zaman damgası modelinde merkezi ve güvenilir bir kuruma ihtiyaç duyulmaktaydı³⁷⁶.

Dai'nin önerdiği, hesap kayıtlarının bütün ağ katılımcıları yerine ağ katılımcılarının oluşturduğu küme topluluklarında tutulduğu ve bu sunucuların işleyiş göstermesi için belirli bir miktarda para tutması gerektiği ikinci para modeli, oldukça yaygın bir diğer kripto para algoritması olan Proof-of-Stake (PoS) sistemine oldukça benzemektedir. Çalışmanın ilerleyen kısmında da bahsedileceği üzere PoS sistemini kullanan kripto paralarda PoW sistemini karşın madencilik ile yeni para üretimi gerçekleşmez. Bunun yerine önceden basılmış kripto paralar hesaplarda tutularak zincirin devamlılığı sağlanır ve kullanıcılar hesaplarındaki miktarlara göre ödüllendirilir.

³⁷³ Buterin, 2014, s. 4.

³⁷⁴ Nakamoto, 2008, s.3.

³⁷⁵ Nakamoto, 2008, s.2.

³⁷⁶ Haber ve Stornetta, 1991, s. 440.

2.2.9. Proof-of-Work (PoW) ve Hashcash

PoW sistemi günümüzde bir çok kripto paranın temelini oluşturmakla birlikte ilk kez 1997 yılında Adam Back tarafından “hashcash” adı verilen sistem ile tanıtılmıştır³⁷⁷. Hashcash sistemi e-posta spamlerini ya da DoS³⁷⁸ ataklarını engelleyen bir sistemdir. Bu fikir ile ilk olarak 1992 yılında Cynthia Dwork ve Moni Noir tarafından spam³⁷⁹ e-postaların gönderilmesini engellemek için ortaya koyulan makalede karşılaşılmaktadır³⁸⁰. Bu sistemde spam e-posta’ları engellemek için, e-posta göndericisinin küçük bir işlem maliyetine katlanması gerekmektedir. Bu maliyet, göndericinin posta gönderirken sisteminde çözmesi gereken bir hesaplama fonksiyonu şeklindedir. Bu hesaplama fonksiyonunun e-posta işleyişi engellemeyecek kadar kolay fakat spam e-posta gönderemeyecek kadar da zor olması gerekmektedir. Bu hesaplama fonksiyonunun getirdiği maliyete katlanamayan kötü niyetli spam göndericisi eyleminden vazgeçecektir³⁸¹.

Back tarafından yayınlanan hashcash’te de benzer şekilde, istenmeyen spamleri ya da siber saldırıları engellemek için, bu eylemleri gerçekleştirirken kriptografik bir iş kanıtı (PoW) algoritması çözülmesini gerektirecek bir sistem ortaya konmuştur. Sistemin maliyet fonksiyonu aynı anda hem verimli bir şekilde onaylanabilir hem de işleme konulmasını gerektirebilecek kadar zor olmalıdır. Hashcash sisteminde herhangi bir eylemi gerçekleştirmek isteyen kişi, sistemin işlemci (CPU) gücünü kullanarak bir “token”³⁸² mint³⁸³ eder. Mint edilen bu token çözülen algoritmanın ve harcanan emeğin kanıtı olarak sunucuya sunulur. Sunucu bu tokenin değerini kontrol eder ve gereken değerde olduğunu kanaat getirirse kişinin eylemini gerçekleştirmesine izin verir³⁸⁴. E-posta üzerinden örneklemek gerekirse, e-posta yollamak isteyen bir kişinin işlemcisi

³⁷⁷ Back, Adam, “Hashcash - A Denial of Service Counter-Measure”.

https://www.researchgate.net/publication/2482110_Hashcash_-_A_Denial_of_Service_Counter-Measure (Son erişim: 05.04.2022)

³⁷⁸ *ing.* Denial-of-service-attack. Internet ağı üzerindeki sunucuları hedef alan ve kullanıcıların sunucuya erişimini engelleyen siber atak.

³⁷⁹ İstenmeyen, gereksiz, dolandırmaya dayalı çok sayıda posta.

³⁸⁰ Dwork, Cynthia, Moni Naor, “Pricing Via Processing or Combatting Junk Mail.”, *Advances in Cryptology: CRYPTO 1992*, Annual International Cryptography Conference, 1992. <https://web.cs.dal.ca/~abrodsky/7301/readings/DwNa93.pdf> (Son erişim: 05.04.2022)

³⁸¹ Dwork ve Noir, 1992, s. 1.

³⁸² Türkçeye “jeton” olarak çevrilebilmekle birlikte kendi ismi ile anılmaya devam edilecektir.

³⁸³ Türkçede “basmak” ya da “para basmak” anlamına gelmektedir.

³⁸⁴ Back, 1997, s.1.

belirli bir güç harcayarak algoritmik bir fonksiyonu çözer; bir token mint eder ve sunucuya sunar; sunucu yeterince güç harcadığını onaylarsa e-postayı karşı tarafa ulaştırır. Her e-posta gönderiminde sistemin bir güç harcayacak olması, kötü niyetli e-posta göndericilerinin buna katlanmak istememesi nedeniyle gereksiz e-posta göndermemelerini sağlayacaktır.

2.2.10. Bit Gold

Blok zincir ve kripto para teknolojisine götüren bir diğer çalışma, ilk kez 1998 yılında öne sürülen ve 2005 yılında çerçevesi genişletilerek ortaya konan “bit gold³⁸⁵”dur. Bit gold, sıkça Satoshi Nakamoto olduğu öne sürülen³⁸⁶ Nick Szabo tarafından ortaya atılmıştır³⁸⁷. Szabo, ilk kez bit gold’dan bahsettiği 1998 tarihli makalesinde daha çok mülkiyet haklarının blok zincir benzeri merkeziyetsiz bir sistem ile saklanması ya da aktarılması konusunda durmuş olsa da 2005 yılında bit gold kapsamını genişletmiştir³⁸⁸.

Szabo’ya göre günümüzde kullanılan paranın değerinin üçüncü bir taraf marifetiyle korunmaya bağlı olması bir problemdir. Bu problem ile değerli metallerde karşılaşılmaz; çünkü değerli metallerin değeri kendiliğinden gelir; bir kurumun ya da üçüncü bir tarafın sağladığı güvenceye ihtiyacı yoktur. Fakat yine de değerli metallerin para olarak kullanılmasının da sakıncaları bulunmaktadır. Değerli metaller günlük ve tekrarlayan işlemler için ayarlanabilirlik sorunu nedeniyle kullanılmaya pek müsait olmamakla birlikte bu işlemler için işlenebilmesi de oldukça maliyetlidir. Bununla beraber bu metallerin taşınması (özellikle büyük miktarlarda) güvenli de değildir. Szabo’ya göre bu sorunların çözümü; üretimi, aktarımı oldukça kolay ve üçüncü bir kurumun güvencesine ihtiyaç duymayan dijital bit gold ile olacaktır.

³⁸⁵ Türkçeye “bit altın” ya da “dijital altın” olarak çevrilebilir.

³⁸⁶ <https://www.nasdaq.com/articles/elon-musk-backs-bitcoins-creator-satoshi-nakamoto-theory> (Son erişim: 06.04.2022); <https://likeinamirror.wordpress.com/2013/12/01/satoshi-nakamoto-is-probably-nick-szabo/> (Son erişim: 06.04.2022); https://en.wikipedia.org/wiki/Satoshi_Nakamoto (Son erişim: 06.04.2022)

³⁸⁷ Szabo, Nick, “Secure Property Titles with Owner Authority”, 1998. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/securetitle.html> (Son erişim: 06.04.2022)

³⁸⁸ Szabo, Nick, “Bit Gold”, 2005, <http://unenumerated.blogspot.com/2005/12/bit-gold.html> (Son Erişim: 07.04.2022); Blog yazısı 2008 tarihli gözükse de, gerek URL üzerinden gerek de webarchive üzerinden kontrol edildiğinde üzere ilk olarak 2005 yılında yayınlandığı görülebilir.

Szabo'nun bit gold modeli de PoW'a benzer bir sisteme dayanmaktaydı. Szabo, kripto para madenciliğine benzer olarak "bit gold mining" terimini kullanmıştır³⁸⁹. Bununla birlikte Szabo, bloklarda oluşan zincir anlamına gelen blok zincire oldukça benzer bir şekilde, "bit³⁹⁰lerden oluşan ip" tabirini kullanmaktaydı. Bununla birlikte Szabo, çifte harcama sorununu Bitcoin'de olduğu gibi PoW sistemi ile değil, network katılımcılarının çoğunluğunun onayı ile aşmaya çalışmıştır. Haliyle bu sistem sybil saldırılara³⁹¹ davetiye çıkarmaktaydı³⁹².

2.2.11. Reusable Proofs of Work (RPoW)

Satoshi Nakamoto'nun 2008 yılında tanıttığı ilk blok zincir olan Bitcoin'e ulaşmadan önce oldukça önemli bir diğer çalışma, Szabo gibi sıkça Satoshi Nakamoto olduğu iddia edilen³⁹³ ve ilk bitcoin transferinin³⁹⁴ alıcısı olan Hal Finney'nin ortaya sürdüğü "RPoW" sistemidir³⁹⁵. RPoW, açılımı ile "Reusable Proofs of Work"³⁹⁶, Adam Back tarafından geliştirilen hashcash sistemindeki PoW yapısını kullanmaktadır. Hashcash sisteminde yukarıda açıklandığı üzere emeğin ispatı olarak bir token mint edilmekteydi³⁹⁷. Bu PoW token, oluşturması belirli bir zaman ve güç harcayan ama kolaylıkla doğrulanabilir bir token'dır. Hashcash'te oluşturulan bu token'lar kural olarak tekrardan kullanılamaz çünkü bu durum çifte harcama (double-spending) problemine yol açacaktır. Finney tarafından geliştirilen RPoW sistemi ise üretilen bu token'ların tekrar kullanılabilmesini sağlamaktaydı. Finney'nin "ardışık kullanım" olarak adlandırdığı bu özellikte mint edilen token'lar yenisi ile değiştirilir; bu şekilde tekrar kullanılır; ardından tekrar yenisi ile değiştirilir; tekrar kullanılır ve bu döngü devam ederdi. Bu yöntem ile

³⁸⁹ Szabo, 2005.

³⁹⁰ Veri depolama ve transferlerde en küçük birim.

³⁹¹ Bir kişi veya bir grubun birden fazla hesap, node, bilgisayar vb. ile ağı geçirmeye çalışması.

³⁹² Güven ve Şahinöz, 2018, s. 151.

³⁹³ <https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-hostwriter-who-wasnt/?sh=4b4558d74a37> (Son erişim: 07.04.2022);

https://en.wikipedia.org/wiki/Satoshi_Nakamoto#Hal_Finney (Son erişim: 07.04.2022)

³⁹⁴

<https://www.blockchain.com/btc/tx/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16> (Son erişim: 07.04.2022)

³⁹⁵ Finney, Hal, Reusable Proofs of Work, 2004.

<http://web.archive.org/web/20071222072154/http://rpow.net/> (Son erişim: 07.04.2022)

³⁹⁶ Türkçeye "Tekrar Kullanılabilir İş Kanıtı" olarak çevrilebilir.

³⁹⁷ Back, 1997, s.1.

PoW token'ların maliyet etkinliđi artarken sistem olduđu gibi alıřmaya devam eder. Finney bu sistemin e-posta'lar iin verimliliđi arttıracadıını sylemektedir. Gelen e-postalardaki token'lar gidecek e-postalar iin kullanılabilir; spam e-posta sahipleri bunu kullanamaz; ünkü spam e-posta hesaplarına gelen e-posta olmaz. Finney, ayrıca sistemin Szabo tarafından ortaya atılan bit gold iin de kullanılabilirleđini sylemektedir. RPoW sistemi ile mint edilen token'lar kiřiden kiřiye deđiř tokuřu sađlayabilecek ve bir deme aracı olarak kullanılabilirlecekti³⁹⁸.

³⁹⁸ Finney, 2004.

ÜÇÜNCÜ BÖLÜM

KRİPTO PARA

3.1. Giriş

Çalışmanın “Blok Zincir” başlığını taşıyan ikinci bölümünde, blok zincirin genel olarak tanımlaması yapıp, blok zincir teknolojisine giden yolda yer alan ve blok zincirin temel elementlerini ihtiva eden önemli erken dönem çalışmaları incelenmeye çalışılmıştır. Bu incelemeler yapılırken “hash”, “Merkle ağacı”, “PoW” veya “PoS” gibi blok zincirlerin temelini oluşturan bazı kavramlar, ortaya çıkış süreçleri ile birlikte açıklanmıştır.

Blok zincirin bir uygulaması olan kripto paralar ile ilgili bahsedilecek kavram ve konular genel olarak blok zincir ile de ilgili olacağından, tekrare düşmemek adına bir kısmı bu bölümde irdelenecektir. Tekrar belirtmekte fayda vardır ki, bu bölümün başlığı “Kripto Para” olsa da, bu durum kripto paraların blok zincirden ayrı düşünüleceği anlamına gelmemelidir. Zira kripto paralar blok zincir teknolojisinin bir uygulama alanıdır. Bu nedenle bu bölümde açıklanacak çoğu özelliğin blok zincir kapsamında da ifade edilebileceği kabul edilebilir, yani blok zincir özelliklerine kripto para örneği üzerinden de ulaşılabilir. Fakat önemle belirtmek gerekir ki, kripto paraların neredeyse tamamı bir blok zincir üzerinde çalışsa da, blok zincir üzerinde çalışmayan kripto paralar ile karşılaşmak da mümkündür. Örneğin “tangle” ağı üzerinde çalışan “IOTA” ya da “hasgraph” ağı üzerinde çalışan “Hedera” kripto paraları buna örnek gösterilebilir. Söz konusu ağlar da blok zincir gibi dağıtık defter teknolojisini kullanmaktadırlar.

Bu başlık altında “kripto para” olarak adlandırılan örneklerin ayrıca “blok zincir” ağı anlamına da gelebileceğini önemle tekrar ifade etmek gerekir. Örneğin Bitcoin (BTC) bir kripto para olarak adlandırılrsa da ayrıca “Bitcoin blok zinciri”ni ifade eder. Ya da Solana (SOL), hem Solana ağını hem de kripto parasını ifade eder.

Çalışmanın yukarısında “güven bunalımı” sorunundan, bu sorunun çözümü için ortaya çıkan “kurum” kavramından bahsedilmiştir. Blok zincir, güvenilir üçüncü tarafın sağladığı kısmi güveni, merkezi bir otoriteye bağlı olmaksızın, dağıtık bir mimari ile

mutlak güvene dönüştürmekteydi. Bu durum para üzerinden yani kripto para üzerinden de irdelenebilir.

Çalışmanın ilk bölümünde bahsedildiği üzere, toplumsalcı görüşe göre bir şeyin para niteliğini kazanılabilmesi için toplumun o şeyin zorunlu ödeme aracı olduğu yönündeki inancı söz konusu olmalıdır³⁹⁹. Bu görüşe göre bir nesnenin ticari hayatta para olarak kullanılması insanın güveniyle olur. Devlet ne kadar düzenleme yaparsa yapsın, bir nesne ticari hayatta toplum tarafından değer ölçüsü, değişim aracı ve tasarruf aracı olarak kabul edilmiyorsa o şey para değildir. Bu görüşe göre bir şeyi para yapan insandır; insanın ona verdiği değer ve gelecekte de var olacağına dair duyduğu inançtır⁴⁰⁰. Bu doğrultuda paranın da bir toplumsal sözleşme olduğu söylenebilir. Dolayısıyla geniş anlamıyla paranın devlete ihtiyacı olmadığı söylenebilir. Tarih boyunca birçok devletli para bir süre sonra yok olmuş, birçok devletsiz para yüzyıllarca varlığını sürdürebilmiştir⁴⁰¹. Bu kapsamda kripto paraların toplumsalcı görüş kapsamında merkezi otoriteleri gereksiz kılarak bir ödeme aracına dönüştüğü söylenebilir.

3.2. Terimin Kökenleri ve Tanımlanması

“Kripto para (cryptocurrency)” kavramı ilk kripto para olan Bitcoin’den eski değildir. Bununla birlikte Bitcoin’in ortaya çıkmasından çok önce, kripto paraları andıran bazı modellerin ve tanımlamaların olduğu bilinmektedir. Örneğin bu doğrultuda “takip edilemez ödeme sistemi⁴⁰²”, “takip edilemez elektronik nakit⁴⁰³”, “anonim elektronik para sistemi⁴⁰⁴” ya da “anonim elektronik nakit⁴⁰⁵” gibi para modelleri ile karşılaşılabilir. Burada “takip edilemezlik” konusunda kısaca belirtmek gerekir ki, bütün kripto paralar

³⁹⁹ Korkmaz Süner, 2005, ss. 215-216.

⁴⁰⁰ Güven ve Şahinöz, 2018, s. 184.

⁴⁰¹ Güven ve Şahinöz, 2018, s. 202.

⁴⁰² Chaum, 1982, s. 1.

⁴⁰³ Chaum vd., “Untraceable Electronic Cash”, *Advances in Cryptology - CRYPTO '88, LNCS 403*, 1990, s. 1. http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf (Erişim:21.05.2022)

⁴⁰⁴ Peirce ve O’Mahony, 1995.

⁴⁰⁵ Law vd., “How To Make A Mint: The Cryptography Of Anonymous Electronic Cash”, National Security Agency Office of Information Security Research and Technology, 1996. <https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm> (Erişim: 21.05.2022)

aynı özellikleri göstermezler; Bitcoin işlemleri takip edilebilirken⁴⁰⁶, Monero gibi bazı kripto paralar takip edilemezdir⁴⁰⁷.

Kripto para (cryptocurrency) tabirinin ilk olarak, 2009 yılında, Bitcoin e-posta listesinde, anonim bir kullanıcı tarafından, Bitcoin'in kriptografik fonksiyonlara dayanmasından hareketle kullanıldığı bilinmektedir. Nakamoto ile ilk Bitcoin destekleyicilerinden Martti Malmi arasında yapılan e-postalaşma sırasında Nakamoto tarafından: “Belki de Bitcoin’i tanımlarken kullanmamız gereken kelime budur, sen ne düşünüyorsun?” sorusu Malmi tarafından: “Kulağa iyi geliyor. Eşlerarası kriptopara, slogan olabilir.” olarak cevaplanmıştır⁴⁰⁸. Daha sonraları Malmi'nin belirttiği şekilde, Bitcoin “eşlerarası elektronik nakit” yerine “eşlerarası kripto para” olarak tanımlanmaya başlanmıştır⁴⁰⁹.

Kripto paralar kısaca “dağıttık bir yapıya sahip, merkezi bir otoriteye dayanmayan, herkese açık, şifrelemeye dayalı para” olarak tanımlanabilir. Kripto paraların üzerinde anlaşılmış bir tanımla bulunmamaktadır. Kripto parayı tanımlama girişimleri kripto para uygulamalarından ziyade daha çok ulusal ve uluslararası kuruluşlar bünyesinde gerçekleşmektedir. Bu girişimlerin kripto paraları legalize etme kaygısından kaynaklandığı söylenebilir. Bu kapsamda her kuruluşun kripto paraları konumlandırmak istediği yer doğrultusunda, ya da farklı bir anlatımla, daha kolay müdahale edebileceğini düşündüğü bir şekilde tanımlama girişiminde buldukları görülmektedir. Bu girişimlerin çoğu zaman kripto paraların yapısı ile bağdaşmayan bazı tanımlamalara da sebebiyet verdiği söylenebilir. Bununla birlikte yeri gelmişken, “müdahale edebilme çerçevesinde bir tanımlama girişimi” konusunda belirtmek gerekir ki; oldukça sık kullanılan bir deyim olan “kripto paraların yasaklanması” ya da daha doğru bir tabirle “mutlak bir yasaklama”, pratikte mümkün değildir. Kripto paralar ancak kısmi bir yasaklamaya konu olabilirler. Bu da pratikte kripto paralar ile “ilişkili” uygulamaların

⁴⁰⁶ Bitcoin, “Protect Your Privacy”, <https://bitcoin.org/en/protect-your-privacy#:~:text=Understanding%20Bitcoin%20traceability&text=All%20Bitcoin%20transactions%20are%20public,privately%20by%20each%20user%27s%20wallets.> (Erişim: 21.05.2022)

⁴⁰⁷ Monero, “What is Monero (XMR)?”, <https://www.getmonero.org/get-started/what-is-monero/#:~:text=Monero%20transactions%20are%20confidential%20and%20untraceable.&text=Becaus e%20every%20transaction%20is%20private,about%20blacklisted%20or%20tainted%20coins.> (Erişim: 21.05.2022)

⁴⁰⁸ Popper, Nathaniel, Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money, HarperCollins, 2015.

⁴⁰⁹ Bitcoin.org sitesinin 06.01.2009 tarihindeki arşiv görüntüsü: <https://web.archive.org/web/20100106082749/http://www.bitcoin.org/> (Erişim:21.05.2022)

yasaklanması ile olabilir. Örneğin merkezi kripto para borsalarının bir ülkede faaliyet göstermesinin engellenmesi veya kripto paraların ödemelerde doğrudan ya da dolaylı şekilde kullanılmaması (Türkiye Cumhuriyet Merkez Bankası tarafından hazırlanan “Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik⁴¹⁰”te olduğu gibi) gibi yasaklamalar söz konusu olabilir. Fakat yasaklamaların hiçbiri merkezi bir otoriteye dayanmayan, dağıtık defterlerin işlemeye devam etmelerine engel olamaz. Bunun tek yolu, internete bağlantının “tamamen” kesilmesi olacaktır⁴¹¹.

Kripto paraların tanımlanması sorununa geri dönecek olursa, çalışmanın ilk bölümünde de genişçe bahsedildiği üzere ulusal ve uluslararası kuruluşlar tarafından kripto paraların çoğunlukla daha önceden tanımlamaları yapılmış “sanal para”, “dijital para” ya da “elektronik para” statüsü içerisine dahil edilmeye çalışıldığı söylenebilir. Bununla birlikte kripto paraların ayrı bir şekilde ele alındığı bazı ulusal veya uluslararası hukuki düzenlemeler de bulunmaktadır. Henüz taslak düzeyinde olsa da, oldukça ayrıntılı bir düzenleme olan Avrupa Birliği tarafından “MiCA” olarak adlandırılan, “Kripto Varlık Piyasasına İlişkin Tüzük Tasarısı⁴¹²”ndaki tanımlamalar incelenebilir.

Kripto Varlık Piyasasına İlişkin Tüzük Tasarısı’nın olağan yasama usulü (ordinary legislative procedure) çerçevesindeki üç sütunlu metnine bakıldığında⁴¹³, tüzüğün isminden de anlaşılacağı üzere kripto para terimi yerine kripto varlık (crypto-assets) terimi üzerinde mutabık kalındığı görülmektedir. Tasarı taslağının “Tanımlar” başlıklı 3. maddesinde kripto varlıklar, “Elektronik olarak transfer edilip depolanabilen, dağıtık defter teknolojisini ya da benzeri teknolojileri kullanan, elektronik olarak transfer

⁴¹⁰ R.G., T: 16/4/2021, S: 31456.

⁴¹¹ Yine de, internet bağlantısı olmadan radyo dalgaları kullanılarak gerçekleştirilen Bitcoin transferi için bkz.; Hertig, Alyssa, “Bitcoin Coders Send International Lightning Payment Over Ham Radio”, CoinDesk, 05.03.2019. <https://www.coindesk.com/markets/2019/03/04/bitcoin-coders-send-international-lightning-payment-over-ham-radio/#:~:text=In%20what%20appears%20to%20be,lightning%20payment%20over%20radio%20waves.&text=Alyssa%20Hertig-.In%20what%20appears%20to%20be%20a%20first%2Dof%2Dits%2D,lightning%20payment%20over%20radio%20waves> (Erişim: 17.07.2022)

⁴¹² Council of the European Union, Proposal for a Regulation Of The European Parliament And Of The Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, 2020, https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF (Erişim: 22.05.2022)

⁴¹³ Council of the European Union, MiCA: Proposal for a regulation on Markets in crypto-assets - Three-column table to commence trilogues, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7694_2022_INIT&qid=1653200871902&from=EN (Erişim: 22.05.2022)

edilip saklanabilen, deęerin ya da hakkın dijital temsili” olarak tanımlanmıştır. Üç sütunlu metinde, Avrupa Parlamentosu’nun kendi taslaęındaki tanımlamada “hak” kavramını açarak düzenledięi görölmektedir⁴¹⁴. Bununla birlikte tasarıda kripto varlık teriminin FATF’nin tavsiyelerinde yer alan “sanal para”ya karşılık geldięi, bu nedenle taslakta belirtilen kripto varlık sağlayıcılarının, tavsiyede yer alan sağlayıcıların kara para aklama ve terörizmin finansmanının önlenmesi ile ilgili yükümlülükleri kapsamında olacağı belirtilmiştir⁴¹⁵. Tanımdan ve tasarıdaki kullanımdan hareketle, “kripto para” yerine “kripto varlık” teriminin tercih edilmiş olması; kripto paraların “para” olarak tanımlanmak istenmemesi ve kripto paralar dışındaki blok zincir ürünlerinin de bu kapsam altına alınmış olmasının istenmesinden kaynaklanmaktadır.

Tasarıda kripto varlıkların daha spesifik düzenlemelere ihtiyaç duyulabilen türlerinin olabildięi ve bu türlerin bazılarının aralarındaki ayırımın ortaya konması gerektiğinden hareketle, varlık kaynaklı token (asset-referenced tokens), fayda (hizmet) token’ı (utility token) ve elektronik para (e-para) token (electronic money tokens, e-money tokens) şeklinde alt kategorilere ayrılabilereği belirtilmiştir. Bununla birlikte üç sütunlu metne bakıldığında bu üç tür kripto varlığın üzerinde anlaşılmış bir tanımlamasının olmadığı görülebilir⁴¹⁶.

Tasarı taslaęında varlık kaynaklı token ve e-para token’in “stabil kripto para (stablecoin)”ları karşılayacak şekilde kullanıldığı belirtilmiştir⁴¹⁷. Tasarının 3. maddesinin 1. fıkrasının (3) numaralı bendinde varlık kaynaklı token’lar, “yasal para olan birçok itibari paranın, bir veya birçok emtianın ya da bir veya birçok kripto varlığın ya da bu varlıkların birleşimlerinin deęerini temel alarak sabit bir deęeri koruyacağını belirten bir kripto varlık türü” olarak tanımlanmıştır. Buna karşılık üç sütunlu metinde Konsey’in ve Parlamento’nun tanımlamalarında “yasal para olan itibari para” deyiminin “bir ülkenin resmi parası” olarak deęiştirilerek aktarıldığı görölmektedir⁴¹⁸. Bununla birlikte tasarıda algoritmik stabil kripto paraların varlık kaynaklı token olarak deęerlendirilemeyeceęi belirtilmiştir⁴¹⁹.

⁴¹⁴ Council of the European Union, 2022, s. 129.

⁴¹⁵ Council of the European Union, 2020, s. 17.

⁴¹⁶ Council of the European Union, 2020, ss. 130-131.

⁴¹⁷ Council of the European Union, 2020, s. 10.

⁴¹⁸ Council of the European Union, 2022, s. 130.

⁴¹⁹ Council of the European Union, 2020, s. 21.

Tasarı taslağında e-para token ise 4. bentte, “ödeme aracı olarak kullanılmak amacı taşıyan, yasal para olan bir itibari parayı referans olarak sabit bir değeri koruyacağını belirten bir kripto varlık türü” olarak tanımlanmıştır. Buna karşın tasarıdan farklı olarak Konsey, “bir ülkenin resmi parası” tabirini tercih etmiş; Parlamento ise token’ın vadettiği fiyatı koruyabilmesi için bir portföy bulundurulması gerekliliğini belirtmiştir.

Tasarıda yer alan varlık kaynaklı token ve e-para token’ın ikisi de stabil kripto paralara karşılık gelse de, e-para token’ların tek bir itibari paranın karşılığı olması nedeniyle daha çok ödeme aracı anlamıyla var oldukları, bununla birlikte varlık kaynaklı token’ların ise daha çok değer saklama aracı olarak değerlendirilebildiğini fakat istenirse ödeme aracı olarak da kullanılabilecekleri belirtilmiştir⁴²⁰. Bu anlamda mevcut kripto paralar üzerinden bir benzetme yapılacak olunursa taslakta, 1 ons altına eşit olarak ticareti yapılan “PAX Gold (PAXG)” gibi kripto paraların varlık kaynaklı token; belirli bir portfolyo tutarak 1 Amerikan dolarına eşit olan “Tether (USDT)” gibi kripto paraların da e-para token’a benzediği söylenebilir. Fakat belirtmek gerekir ki, bu durum sadece örnek olarak bir benzerlik gösterip, taslak kapsamında Tether’in bir e-para token olarak değerlendirilmesi mümkün değildir. Çünkü taslaktaki e-para token tanımlaması, mevcut elektronik paralara oldukça benzemekte olup; e-para token ihraç edecek kuruluşların kredi ya da elektronik para kuruluşu olarak yetkilendirilmesi gerekmekte, ayrıca e-para token’ı elinde bulunduranlara her zaman itibari paraya dönüş garantisi verilmektedir⁴²¹; buna karşın Tether’da USDT sahipleri 100.000 USDT’nin altında böyle bir talepte bulunamaz⁴²².

Tasarıda belirtilen bir diğer kripto varlık türü ise 3. maddenin 1. fıkrasının (5) numaralı bendinde belirtilen “fayda (hizmet) token (utility token)” olup, bu token’lar “dağıtık defter teknolojisine dayanan, bir mal ya da hizmete yalnızca bu token’ı ihraç eden nezdinde dijital olarak erişebilmeyi sağlayan kripto varlık” olarak tanımlanmıştır. Üç sütunlu metinde Parlamento tarafından bu tanıma, fayda token’larının “değiştirilebilir” nitelikte oldukları ve ödeme aracı olarak kullanılmamaları eklenmiştir⁴²³.

⁴²⁰ Council of the European Union, 2020, s. 17.

⁴²¹ Council of the European Union, 2020, s. 24.

⁴²² Minimum 100.000 Amerikan doları limit bulunmaktadır. <https://tether.to/en/fees/> (Erişim: 28.05.2022)

⁴²³ Council of the European Union, 2022, s. 24.

Avrupa Komisyonu ayrıca 7 Mayıs 2020 tarihinde, karapara aklama ve terörizmin finansmanı ile mücadele kapsamında “Aklama ve Terörizmin Finansmanının Önlenmesine Yönelik Kapsamlı bir Birlik Politikası için Eylem Planı”⁴²⁴’nı kabul etmiştir. Bu kapsamda, Avrupa Komisyonu tarafından, 20 Temmuz 2021 tarihinde aklama ve terörizmin finansmanı ile mücadele konusunda kapsamlı bir mevzuat paketi taslağı sunulmuştur. Bu paket kapsamında 2015/847 sayılı fon transferlerine ilişkin tüzüğe kripto varlık transferlerini de dahil eden revizyon teklifi bulunmaktadır⁴²⁵. Bununla birlikte bu teklifte kripto varlıklara ilişkin yeni bir tanımlamanın yapılmadığı, kripto varlık tanımında Avrupa Birliği yasal çerçevesindeki tutarlılığın sağlanması için MiCA’da yapılan tanımlamanın takip edileceği belirtilmiştir⁴²⁶.

FATF, 2014 tarihli raporunda, kripto paraları “sanal para birimi” olarak belirtmiş⁴²⁷, ardından “merkeziyetsiz sanal para birimi” türü olarak ayırmıştır⁴²⁸. FATF merkeziyetsiz sanal para birimlerini, bunların ayrıca kripto para anlamına geldiğini belirterek, “bir merkezi kontrol otoritesi tarafından yönetilmeyen, gözetilmeyen ve denetilmeyen dağıtık, açık kaynaklı, matematiksel eşlerarası bir sanal para birimi türü” olarak tanımlamış, ardından kripto paraları da “kriptografi ile korunan, matematiksel, merkeziyetsiz ve dönüştürülebilir sanal para birimi” olarak tanımlamıştır⁴²⁹. FATF, ilk olarak 2019 yayınladığı ve ardından 2021 yılında güncellenen “Sanal Varlıklar ve Sanal Varlık Servisi Sağlayıcıları” başlığını taşıyan ve karapara aklama ile terörizmin finansmanına yönelik risklerin önlenmesine yönelik tedbirsel süreçleri ifade ettiği rehberinde⁴³⁰ kripto paralardan sanal varlıkları karşılayacak şekilde bahsetmiştir. Yine sanal varlık tanımı tam olarak yapılmamış; sanal varlıklara ait bazı özellikler ele alınarak sanal varlığın belirlenmesi gerektiği belirtilmiştir. Bu doğrultuda sanal varlıkların “dijital” olmaları ve dijital ortamda transfer edilebilmeleri ile yatırım ve ödeme amacıyla

⁴²⁴ <https://www.ab.gov.tr/p.php?e=69> (Erişim: 28.05.2022)

⁴²⁵ European Commission, Proposal for a Regulation Of The European Parliament And Of The Council on information accompanying transfers of funds and certain crypto-assets (recast), 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:08cf467e-ead4-11eb-93a8-01aa75ed71a1.0001.02/DOC_1&format=PDF (Erişim:22.05.2022)

⁴²⁶ European Commission, 2021, s. 4.

⁴²⁷ FATF, 2014, s. 4.

⁴²⁸ FATF, 2014, s. 5.

⁴²⁹ FATF, 2014, ss. 4-5.

⁴³⁰ FATF, Virtual Assets And Virtual Asset Service Providers, 2021, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> (Erişim: 27.05.2022)

kullanılabilmeleri gerektiği belirtilmiştir. Bununla birlikte değiştirilemez token⁴³¹'lerin [Non-Fungible Tokens (NFT)] rehber çerçevesindeki sanal varlık tanımının dışında kaldığını, fakat bunların “finansal varlık” olarak FATF standartları içerisinde dahil edileceği belirtilmiştir⁴³².

IMF İstatistik Departmanı tarafından yayınlanan 2019 tarihli raporda da kripto para yerine kripto varlık terimi tercih edilmiş olup, kripto varlıklar “kriptografi ve dağıtık defter teknolojisi sayesinde mümkün kılınan değerın dijital temsili” olarak tanımlanmıştır⁴³³.

Finansal Endüstri Düzenleme Kurumu (FINRA) ise kripto paraları “kriptografi ile korunmakta olan, saklanan değerın dijital temsili” olarak tanımlamıştır⁴³⁴.

Türkiye’de ise kripto paralar yasal düzenlemeler içerisinde ilk kez 16 Nisan 2021 tarihinde yayınlanan Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik’in 3. maddesinin 1. fıkrasında kripto varlık adı altında, “*Kripto varlık, dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımını yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder.*” şeklinde tanımlanmıştır. “kripto varlık” teriminin tercihinde, Avrupa Birliği çalışmalarındaki kullanımın takip edildiği söylenebilir.

⁴³¹ Yakın bir zamanda Türkiye Cumhurbaşkanlığı Dijital Ofisi tarafından NFT’lerin “nitelikli fikri tapu” olarak çevrilmesi önerisinde bulunulmuştur. Fakat “N-F-T” harflerine uyumun sağlanması kaygısıyla getirilen ve NFT’lerin yapısı ve fonksiyonları tam olarak irdelenmeden gerçekleştirilen bu çeviriye katılmak mümkün gözükmemektedir. Patentler genel olarak “fikri tapu” olarak da belirtilebilse de, tapunun esas olarak taşınmaz varlıklar için var olan bir düzen olduğu kabul edildiğinde, kriptografiye dayanan bir varlığın tapu ile anılması pek uygun düşmemektedir. Bununla birlikte NFT’ler sadece resim, müzik gibi fikri eserleri de kapsamazlar. Örneğin Uniswap’te likidite belirten pozisyon NFT’leri (UNI-V3-POS) ya da Ethereum Name Service gibi isimlendirme servislerinin sağladığı cüzdanlara bağlı NFT’ler fikri eserler değildir. Türkiye’de ayrı bir kanunla düzenlenen “sınai mülkiyet” doğrultusunda özelleşen NFT’ler de bulunabilir. Bu sebeple değiştirilemez “token” kelimesi için “jeton” çevirisi dışında bir çeviri kabul edilip bu şekilde çevrilmesi daha doğru olacaktır.

⁴³² FATF, 2014, s. 24.

⁴³³ International Monetary Fund, Treatment of Crypto Assets in Macroeconomic Statistics, 2019, <https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf> (Erişim:22.05.2022)

⁴³⁴ FINRA, Cryptocurrencies, <https://www.finra.org/investors/learn-to-invest/types-investments/initial-coin-offerings-and-cryptocurrencies/cryptocurrencies#:~:text=A%20cryptocurrency%20is%20a%20digital,remain%20highly%20volatile%20and%20risky.> (Erişim: 22.5.2022)

3.3. Kripto Paraların Terörizmin Finansmanı Aracı Olarak Kullanılabilmesini Sağlayan Özellikleri Dikkate Alınarak, Kripto Paralar İle İlgili Bazı Kavram Ve Uygulamalar

Çalışmanın ikinci bölümünde blok zincir teknolojisi ile ilgili bazı kavramlar, teknolojik süreçteki yerleri ile birlikte aktarılmıştır. Bu nedenle öncelikle, çoğu kripto paralar için de geçerli olacak bu kavramların tekerrüre düşmemek adına bu başlık altında yeri geldiğinde kısaca açıklanmak ile yetinileceğini belirtmek gerekir. Bu bölümde ayrıca söz konusu kavramların dışında kalan, kripto paralar ile ilgili kavram, özellik ve kripto paralara ilişkin birtakım uygulamalar ve teknikler, bütünlüğü sağlamak amacıyla, yeri geldiğinde kripto paraların bu çerçevede terörizmin finansmanına ne derece kolaylık sağlayabildiği ve finansman amacıyla nasıl kullanılabileceğine dair açıklamalarıyla birlikte aktarılacaktır. Yine de belirtmek gerekir ki bu durum, kripto paraların irdeleneceği bu başlıkta yer alan her bilginin doğrudan terörizmin finansmanı ile ilgili olduğu anlamına gelmemektedir.

Blok zincir ve kripto paralar büyük bir teknolojik devrim olarak nitelendirilebilirse de, her teknolojik devrimde olduğu gibi burada da bu yeniliğin sağladığı faydanın karşısında zararlı faaliyetler amacıyla kullanım gerçekleşmektedir. Özellikle sağladıkları anonimlik ve yeri geldiğinde takip edilemezlik gibi özellikleri nedeniyle kripto paraların yasa dışı faaliyetler amacıyla, karapara aklama ve terörizmin finansmanı ve diğer yasaklanan faaliyetleri gerçekleştirme aracı olarak kullanılabilmesini söylemek mümkündür. Örneğin Europol, 2021 tarihli İnternet Tabanlı Organize Suçlar Tehdit Değerlendirmesi'nde⁴³⁵ [Internet Organised Crime Threat Assessment (IOCTA)], 2021 yılında DarkMarket⁴³⁶ üzerinde 500.000 kullanıcının işlem yaptığını, toplamda 140 milyon Euro değerinde işlemin gerçekleştiği ve toplamda tanımlanabilen yaklaşık 4.650 Bitcoin (rapor tarihinde yaklaşık 200 milyon Euro değerinde) ve 12.800 Monero'nun (rapor tarihinde yaklaşık 2,5 milyon Euro değerinde) transfer edildiğini açıklamıştır⁴³⁷.

⁴³⁵ Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, 2021/a, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf (Erişim: 28.05.2022)

⁴³⁶ Yasadışı faaliyetler için yasa dışı ticaretin yapıldığı, geleneksel tarayıcılar ile ulaşılamayan platformların geneli.

⁴³⁷ Europol, 2021, s. 37.

Fakat belirtmek gerekir ki, karapara aklama ya da terörizmin finansmanı gibi eylemler ilk kripto para olan Bitcoin ile ortaya çıkmamıştır. Bitcoin'den önce de kara para aklama ve terörizmin finansmanı pekala gerçekleştirilmekte olup, terörizmin finansmanında kripto paraların payı hala oldukça düşüktür⁴³⁸. Buna ilaveten kripto para işlemlerinin yalnızca %1'inin yasadışı faaliyetler gerçekleştirmek amacıyla yapıldığı, bu yasadışı faaliyetlerin de yalnızca %0.05'inin terörizmin finansmanı amacıyla yapıldığı bilinmektedir⁴³⁹. Yine de bu oranın “bilinen” işlemler üzerinden hesaplandığı vurgulanmalıdır.

Kripto paraların terörizmin finansmanı amacıyla kullanıldığı birtakım örnekler verilmesi gerekirse; bir terörist organizasyon tarafından gerçekleştirilen ilk kitle fonlaması Mücahitler Şura Konseyi⁴⁴⁰'nin basın kolu olan İbn Teymiyye Basın Merkezi tarafından 2016 yılında düzenlenmiştir⁴⁴¹. Kampanya “Bizi silahlandır.” sloganıyla yürütülmüştür⁴⁴².

⁴³⁸ Europol, Cryptocurrencies: Tracing The Evolution Of Criminal Finances, 2021/b, s. 2. <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf> (Erişim: 23.05.2022)

⁴³⁹ Wilder, Heidi, “An Overview Of The Use Of Cryptocurrencies In Terrorist Financing”, Coinbase, 22.09.2021, <https://blog.coinbase.com/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing-235df6049bc7> (Erişim:23.05.2022)

⁴⁴⁰ Türkiye Cumhuriyeti İçişleri Bakanlığı, Türkiye'nin DEAŞ İle Mücadelesi, 2017, s. 6. <https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/strateji/deneme/YAYINLAR/İÇERİK/deas%20en.pdf> (Erişim: 23.05.2022)

⁴⁴¹ Chainalysis, The 2020 State Of Crypto Crime, 2020, s. 70. <https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/257%20-%200001%20Appendix%20A%20-%202020-Crypto-Crime-Report%20Chainanalysis.pdf> (Erişim: 23.05.2022)

⁴⁴² Solomon, Ariel Ben, “Gaza-based pro-ISIS group urges Muslims on social media to donate for weapons”, The Jerusalem Post, 25.06.2016, <https://www.jpost.com/Middle-East/ISIS-Threat/Gaza-based-pro-ISIS-group-urges-Muslims-on-social-media-to-donate-for-weapons-457680> (Erişim: 23.05.2022)

Şekil 3. 1 İbn Teymiyye Basın Merkezi tarafından düzenlenen kampanya.

في صحيح مسلم عن عقبه بن عامر أن رسول الله ﷺ قال: (واعبدوا لهم ما استطعتم من قوة؛ إلا أن القوة الرمي، إلا أن القوة الرمي، إلا أن القوة الرمي)

حملة جهزونا

صاروخ "جراد" 40 دولي	صاروخ "جراد" 20 دولي	صاروخ "كتيوشا" 107 دولي	صاروخ "كتيوشا" 107 محلي	المدى
42Km	21 Km	8 Km	4.5 Km	يهود تحت النيران
574.072	155.477	31.590	6.083	عدد المستوطنات
20+	20+	21	15	عدد المدن الكبيرة
7	3	1	0	القوة التدميرية
كبيرة	كبيرة	متوسطة	متوسطة	دقة الاصابة
85%	90%	95%	75%	
الثمن = 5000 دولار	الثمن = 2700 دولار	الثمن = 950 دولار	التكلفة = 200 دولار	

bitcoin

(Kaynak: Chainalysis⁴⁴³)

Bununla birlikte Amerika Birleşik Devletleri, Birleşik Krallık, Yeni Zelanda, Avustralya, İsrail, Japonya, Kanada, Avrupa Birliği⁴⁴⁴ tarafından; bunların bir kısmının terörist örgüt olarak kabul ettiği, bir kısmının 1373 sayılı karar çerçevesinde bu şekilde listelediği ya da terörizmin finansmanının önlenmesi çerçevesinde yaptırımlara tabi tuttuğu⁴⁴⁵ silahlı bir grup⁴⁴⁶ olan İzzeddin el-Kassam Tugayları'nın 2019 yılında kripto

⁴⁴³ Chainalysis, 2020, s. 70.

⁴⁴⁴ <https://curia.europa.eu/juris/document/document.jsf?docid=211363&doclang=EN> (Erişim:23.05.2022)

⁴⁴⁵ Congressional Research Service, Foreign Terrorist Organization (FTO), 2019, <https://sgp.fas.org/crs/terror/IF10613.pdf> (Erişim: 23.05.2022); Court of Justice of the European Union, The Court of Justice upholds the acts of the Council maintaining Hamas on the European list of terrorist organisations, 23.11.2021, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210208en.pdf> (Erişim: 23.05.2022); GOV.UK, Proscribed Terrorist Groups Or Organisations, 26.12.2021, <https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2/proscribed-terrorist-groups-or-organisations-accessible-version> (Erişim:23.05.2022); Ministry of Foreign Affairs of Japan, Japan's Foreign Policy in Major Diplomatic Fields, s. 138, <https://www.mofa.go.jp/policy/other/bluebook/2005/ch3-a.pdf> (Erişim: 23.05.2022); New Zealand Police, Lists associated with Resolution 1373, <https://www.police.govt.nz/advice/personal-community/counterterrorism/designated-entities/lists-associated-with-resolution-1373> (Erişim:23.05.2022); Office of Financial Sanctions Implementation HM Treasury, Consolidated List Of Financial Sanctions Targets In The Uk, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/106076/5/Counter-Terrorism_International_.pdf (Erişim:23.05.2022); Parliament of Australia, Chapter 3 The Listings, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Former_Committees/pjcaad/terrorist_listingsc/chapter3#ham (Erişim: 23.05.2022); Turan, Deniz, Can Demircan, Kripto Paralar İle Terör Ve Diğer İlegal Aktivitelerin

Finansmanı, *Anadolu Akademi Sosyal Bilimler Dergisi*, 2021/3 (1), s. 171.

<https://dergipark.org.tr/en/download/article-file/1543533> (Erişim: 29.05.2022)

⁴⁴⁶ European Council of Foreign Relations, Mapping Palestinian Politics, https://ecfr.eu/special/mapping_palestinian_politics/introduction_armed_groups/ (Erişim:23.05.2022);

paraları araç edinerek gerçekleştirdiği fon toplama faaliyeti, yapıldığı tarihte silahlı bir grubun düzenlediği en büyük kripto para fonlamasının bir parçası olarak kabul edilmekteydi⁴⁴⁷. Bu fonlama üç aşamada gerçekleştirilmiştir.

İlk aşamada fonlama kampanyası için bir QR kod kullanılmıştır. Kripto para göndermek isteyenler bu QR kodu okutarak ulaştıkları Bitcoin adresine gönderim sağlamaktaydılar. Bu QR kod çeşitli şekillerde yayılarak fon toplanmış; fakat bu adresin Birleşik Devletler merkezli bir kripto para borsası tarafından kullanıcıya sunulan bir adres olduğu anlaşılınca, borsa uyarılarak söz konusu adres dondurulmuş, fonlar ele geçirilmiştir⁴⁴⁸.

İkinci aşamada, ilk aşamadaki haliyle bir borsa hesabı kullanıldığında, söz konusu adres üzerindeki tasarruf yetkisinin sınırlandırılabilceği ve adres ile ilişkili borsa hesabının takip edilebileceği anlaşılınca, özel bir Bitcoin adresi oluşturulup bu adrese kripto para gönderilmesi talep edilmiştir⁴⁴⁹.

Üçüncü aşamada ise çok daha gelişmiş bir yöntem kullanılmış olup, bu aşamada bağış için kullanılan web sitesi, bir bitcoin cüzdanı gömülü hale getirilmiş; para aktarmak isteyenler sitedeki reCAPTCHA doğrulamasını geçerek, her seferinde kendilerine özel üretilen adrese ulaşip para aktarmışlardır⁴⁵⁰.

Friedrich, Roland, Arnold Luethold, "Entry-Points to Palestinian Security Sector Reform", Geneva Centre For The Democratic Control Of Armed Forces (DCAF), s. 105.

<https://www.dcaf.ch/sites/default/files/publications/documents/Entry-Points%28EN%29.pdf> (Erişim:23.05.2022)

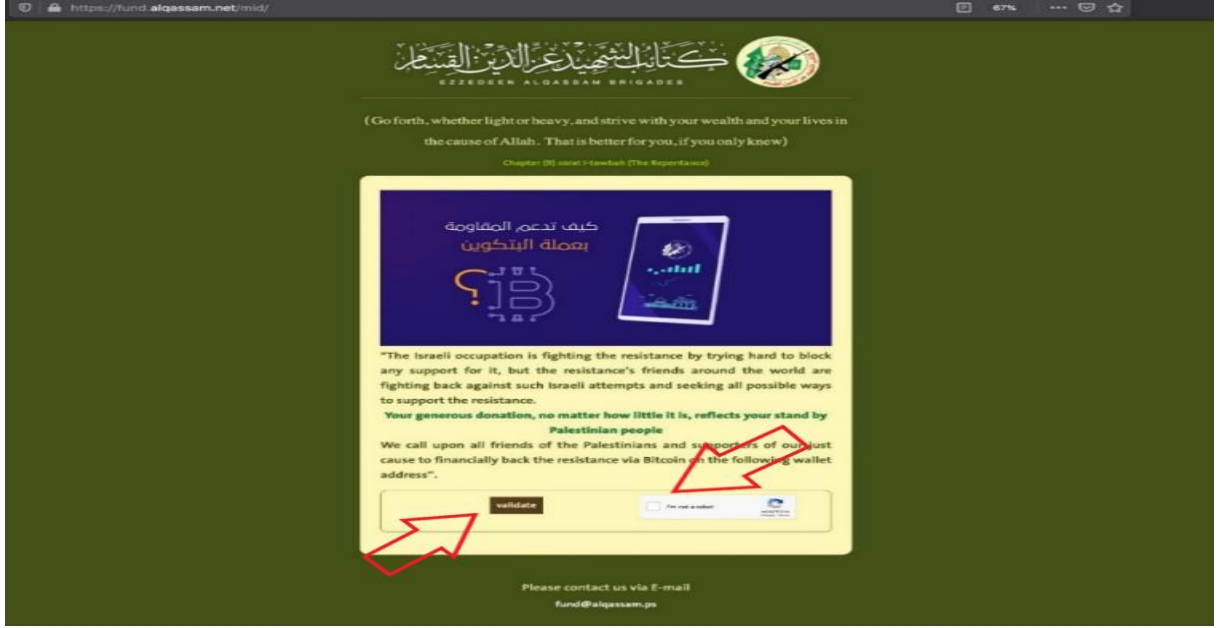
⁴⁴⁷ Chainalysis, 2020, s. 73.; The United States Department of Justice, Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, 13.08.2020. <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns> (Erişim:23.05.2022)

⁴⁴⁸ Chainalysis, 2020, s. 73.; United States District Court For The District Of Columbia, United States Of America, v. Fifty-Three Virtual Currency Accounts, One Hundred Twenty-Seven Virtual Currency Properties, Five Accounts Held At Financial Institution 1, The Alqassam.Net Domain, The Alqassam.Ps Domain and the Qassam.Ps Domain, Civil Action No. 20-cv-2227, 2020/a, s. 9. <https://www.justice.gov/opa/press-release/file/1304296/download> (Erişim:23.05.2022)

⁴⁴⁹ United States District Court For The District Of Columbia, 2020/a, s. 13.

⁴⁵⁰ United States District Court For The District Of Columbia, 2020/a, ss. 13-16; Chainalysis, 2020, s. 74.

Şekil 3. 2 Captcha kodunu geçtikten sonra her seferinde farklı bir adres üreten üçüncü aşama



(Kaynak: United States District Court For The District Of Columbia⁴⁵¹.)

Bu örnekte toplanan fonların önemli bir kısmının borsalar üzerinde hesap bulunduran gerçek kişiler üzerinden nakde çevrildiği, bu hesaplar üzerinden (tamamı terörizmin finansmanı amacıyla kullanılsa da) 90 milyon Amerikan dolarının üzerinde akış gerçekleştiği tespit edilmiştir⁴⁵².

Terör örgütü El-Kaide'nin de yakın bir tarihte kripto para aracılığıyla fonlanmaya çalışıldığı bilinmektedir⁴⁵³. Bağış yoluyla toplanan kripto paralar çok katmanlı işlemler ile gizlenmeye çalışılarak örgütü fonlamak için kullanılmıştır⁴⁵⁴. Kampanya, örgüte bağlı çeşitli yapılar aracılığıyla başta mesajlaşma uygulaması "Telegram" olmak üzere çeşitli sosyal platformlarda kripto para cüzdan adresi paylaşarak yürütülmüştür. Bağışta

⁴⁵¹ United States District Court For The District Of Columbia, 2020/a, s. 15.

⁴⁵² United States District Court For The District Of Columbia, United States Of America V. Mehmet Akti & Hüsamettin Karataş, Case: 1:20-mj-00157, 08/12/2020. <https://www.justice.gov/opa/press-release/file/1304276/download> (Erişim:23.05.2020)

⁴⁵³ Chainalysis, The 2021 Crypto Crime Report, 2021, s. 97. <https://safewayconsultoria.com/wp-content/uploads/2021/09/Chainalysis-Crypto-Crime-2021.pdf> (Erişim:23.05.2022); United States District Court For The District Of Columbia, United States Of America v. 155 Virtual Currency Assets, Civil Action No. 20-cv-2228, 2020/b. <https://www.justice.gov/opa/press-release/file/1304296/download> (Erişim:24.05.2022)

⁴⁵⁴ Chainalysis, 2021, s. 97.

Bitcoin'in yanında, izlenebilirliği engelleyen gizlilik odaklı kripto paralar olan Dash, Verge ve Monero da kabul edilmektedir⁴⁵⁵.

Şekil 3. 3 El-Kaide kampanyası için paylaşılan Bitcoin cüzdan adresi.



Kaynak: United States District Court For The District Of Columbia⁴⁵⁶.

Kampanya dahilinde 2018 ve 2020 yılları arasında yaklaşık 280.000 Amerikan doları değerinde kripto para toplandığı bilinmektedir⁴⁵⁷.

Birleşik Krallık ve Fransa tarafından yürütülen soruşturmalarda, DEAŞ terör örgütünün de 2016-2020 yılları arasında kripto para ile fonlandığı tespit edilmiştir⁴⁵⁸

Yakın tarihte Amerika Birleşik Devletleri'nde yaşanan ve terörist bir eylem olarak nitelendirilebilen⁴⁵⁹ "6 Ocak 2021 Kongre Baskını"ndan bir ay önce, eyleme dahil olan

⁴⁵⁵ European Parliament, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, 2018, s. 34.
[https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (Erişim:24.05.2022)

⁴⁵⁶ United States District Court For The District Of Columbia, 2020/b, s. 16.

⁴⁵⁷ Chainalysis, 2021, s. 97.

⁴⁵⁸ Chainalysis, 2021, s. 94.

⁴⁵⁹ House Homeland Security Committee, Examining The Domestic Terrorism Threat In The Wake Of The Attack On The U.S. Capitol, 2021, <https://www.congress.gov/event/117th-congress/house-event/LC65965/text?q=%7B%22search%3A%5B%22capitol+attack%22%5D%7D&s=1&r=7> (Erişim:24.05.2022); National Security Council, National Strategy For Countering Domestic Terrorism, 2021, ss. 5, 10. <https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf> (Erişim: 30.05.2022)

ekstremist grupların tek bir bağışçıdan, transfer edildiği tarihte değeri 500.000 Amerikan dolarının üstünde Bitcoin bağışı aldıkları tespit edilmiştir⁴⁶⁰.

Terörizmin finansmanının kripto paralar aracılığıyla gerçekleştirilmesi bu örnekler ile sınırlı değildir. Kullanılan yöntem, terörist organizasyonun blok zincir bilgisi gibi etkenler bu tür finansman sağlama faaliyetlerinin daha zor takip edilebilmesine sebep olabilir ya da bu tür faaliyetler hiç tespit edilemeyebilirler.

Mevcut bu başlığın alt başlıklarında, kripto paralar ile ilgili bazı kavram, özellik, uygulama ve teknikler açıklanacak olup; açıklamalar doğrultusunda yeri geldiğinde terörizmin finansmanı ile ilgili (finansman sağlama faaliyetine sağlanan kolaylık) özellik gösterebilen durumlara da değinilecektir.

3.3.1. Yaygın Olarak Kullanılan Bazı Kripto Paralar Hakkında Genel Bilgiler

Öncelikle bu başlığın bir giriş ya da genel bir bilgi aktarımı işlevi göreceğinin ve başlık altında bahsedilecek kripto paraların ayrıntılı olarak incelenmeyeceğinin; bunun yerine takip eden başlıklarda gerek görüldüğü takdirde daha ayrıntılı olarak inceleneceğinin belirtilmesi gerekir.

CoinMarketCap verilerine göre 24.05.2022 tarihi itibarıyla, sadece bu sitede kayıtlı 19.538 farklı kripto para bulunmakta, bu sayı her gün artmaktadır. Bu kripto paraların büyük bir çoğunluğunun, üreticilerinin ceplerini doldurmak için oluşturulmuş, bir projeden yoksun, ani değer değişimlerine konu olmakla birlikte kısa ya da uzun vadede terkedilen ya da edilecek kripto paralar olduğunu belirtmek gerekir.

Kripto paralar ile ilgili bu başlıkta bahsedilmesi gereken ilk konu, “coin” ve “token” kavramları olacaktır. Her ne kadar bu çalışmanın, bu ayrım üzerinden gerçekleştirilmesine gerek duyulmadığı ve her iki kavramın da “kripto para” çatı kavramı altında ele alınacağı belirtilmekle birlikte; uygulamada çok sık olmasa da bu iki kavramın farklı amaçlar için kullanıldığı bilindiğinden, aralarındaki farkın açıklanması yararlı olacaktır. Her iki kavramın da kullanıcıları tarafından aynı amaçlar ile kullanılmadığı ve bu nedenle bir kullanım birliğinin olmadığını belirtmekte fayda vardır. Bu doğrultuda “coin” kavramı uygulamada daha çok kendi ağı üzerinde çalışan ETH, NANO, BTC, XRP gibi kripto paralar için kullanılırken; “token” kavramı ise kendi ağı olmayan, başka

⁴⁶⁰ Chainalysis, 2021, ss. 99-104.

bir blok zincir ağından faydalanan CAKE, ANC, JOE vb. gibi kripto paralar için kullanılabilir. Bununla birlikte farklı amaçlı bir kullanım, coin kavramının temel olarak ödeme aracı olma amacını taşıyan NANO, BTC, LTC vb. kripto paralar için kullanıldığı; token kavramının ise bir ödeme aracı olma amacını taşımayan, ilgili blok zincir projesinin bir bakıma değerini ifade eden, temelde oldukça farklı kavramlar olsa da, şirketlerin hisselerine benzeyen bir kavram olarak kullanılır (Örn: STEP, AAVE, UNI vb). Tekrar belirtmek gerekir ki, bu kullanım amaçlarının arasında bir birlik olmayıp, söz konusu kavramların kripto para kullanıcıları tarafından özensiz bir şekilde kullanılması nedeniyle genel olarak kripto para olarak adlandırılmaları, bu çalışma çerçevesinde daha doğru olacaktır. Örneğin FTM, sıklıkla bir “coin” olarak adlandırılabilir da, Fantom Vakfı tarafından Fantom ağının “yerel token’ı” olarak belirtilmektedir⁴⁶¹. Bununla birlikte Bitcoin ve Ethereum dışındaki kripto paralar genel olarak “alternative coin” kısaltması anlamında “altcoin” olarak da adlandırılmaktadır.

3.3.1.1. Bitcoin (BTC)

Bu çalışmada da sıklıkla bahsedildiği üzere, ilk ve en çok bilinen kripto para Bitcoin (BTC)’dir. Bitcoin 2008 yılında Satoshi Nakamoto takma adına sahip bir kişi ya da grup tarafından ortaya konmuş olmakla birlikte; ilk Bitcoin bloğu⁴⁶², diğer isimleriyle “Block 0⁴⁶³” ya da “Genesis Block⁴⁶⁴”, 3 Ocak 2009 tarihinde, o günkü The Times gazetesi manşeti olan “Chancellor on brink of second bailout for banks (Şansölye bankalar için ikinci kurtarma paketini çıkarmanın eşiğinde)” mesajı eklenerek oluşturulmuştur. Bu mesajın bloğun kazılma tarihini ispatlama amacı gütmekle birlikte 2008 küresel finans krizi üzerinden bir mesaj verme amacıyla de seçildiği belirtilebilir.

İlk Bitcoin transferi ise 12 Ocak 2009 tarihinde, “f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16” işlem ID’si ile, Nakamoto’nun Hal Finney’nin cüzdanına 10 BTC (şu anki değeri ile yaklaşık

⁴⁶¹ Fantom Foundation, “What is FTM?”, <https://fantom.foundation/ftm-token/> (Erişim:24.05.2022)

⁴⁶² Blockchain.com, “Blok 0”,

<https://www.blockchain.com/btc/block/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f> (Erişim: 26.05.2022)

⁴⁶³ Sıfırıncı blok.

⁴⁶⁴ Yaratılış bloğu.

300.000 Amerikan doları) göndermesi ile gerçekleşmiştir. Üzerinden on üç yıl geçmiş olsa da, bu işlem herhangi bir işlem gibi hala görüntülenebilir⁴⁶⁵.

Bitcoin blok zinciri, çalışmanın üst kısımlarında da ayrıntılı olarak bahsedildiği üzere, PoW algoritmasını kullanmakta olup⁴⁶⁶, blok kazım süreçleri çerçevesinde madenciler ödüllendirilmektedir. Bitcoin'in maksimum arzı 21.000.000'dur, bu nedenle Bitcoin arzının kısıtlı olduğu söylenebilir, çünkü en fazla 21.000.000 adet Bitcoin üretilebilir. 24 Mayıs 2022 itibarıyla bu sayının 19,048,031'i üretilmiştir⁴⁶⁷. Bitcoin üretimi madencilere blok kazımı sonrası verilen blok ödülleri çerçevesinde gerçekleşmektedir. Blok ödülleri her 210.000 blokta bir yarılanır, buna yarılanma (halving) adı verilir ve yaklaşık dört yılda bir gerçekleşir. İlk yarılanma 28 Aralık 2012 tarihinde gerçekleşmiş olup, blok ödülleri 50 BTC'den 25 BTC'ye düşürmüştür. İkinci yarılanma 7 Eylül 2016 tarihinde gerçekleşmiş olup, blok ödülleri 12,5 BTC'ye düşürmüştür. Üçüncü yarılanma ise 11 Mayıs 2020 tarihinde gerçekleşmiş olup, blok ödülleri şu anki haline yani 6,25 BTC'ye düşmüştür. Bir sonraki yarılanma ise 2024 yılında gerçekleşecektir.

Çalışmanın üst bölümlerinde de sıklıkla bahsedildiği üzere, Bitcoin işlemleri herkese açıktır, ağ üzerinde gerçekleşen işlemler herkes tarafından izlenebilir ve kontrol edilebilir. Bütün işlemler görülebilir olsa da işlemleri gerçekleştirenlerin kimliği, gerçekleştiren kimse bunu bir şekilde açıklamamış ya da yaptığı işlemler takip edilerek kim olduğu bilinemediği sürece anonim kalmaktadır.

Bitcoin ağındaki aktarım işlemlerinde, işlemler çerçevesinde paraların sahipliğinin ve hesap bakiyelerinin belirlenmesinde "harcanmamış işlem çıktısı [unspent transaction output (UTXO)]"dan faydalanılır. UTXO modelinde bir işlemin çıktısı, başka bir işlemin girdisi olarak kullanılır. Model bir örnek ile açıklanacak olursa, Ali'nin 10 BTC'si var ve Ayşe'ye 2 BTC göndermek istemektedir. Bu durumda Ali'nin cüzdanından 10 BTC çıkar; bunun 2'si Ayşe'ye gider, 8'i Ali'nin kendisine gelir. Ali'nin cüzdanından çıkan 10 BTC bir kere kullanıldığından artık kullanılamaz. Ali'den çıkan 10 BTC aslında başka bir işlemin çıktısı olan bir UTXO'dur; Ayşe'ye yapılan aktarım ile harcanmış hale

465

<https://www.blockchain.com/btc/tx/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16> (Erişim: 24.05.2022)

⁴⁶⁶ Nakamoto, 2008, s. 1.

⁴⁶⁷ CoinMarketCap, "Bitcoin", <https://coinmarketcap.com/tr/currencies/bitcoin/> (Erişim:24.05.2022)

geldiğinden tekrar kullanılamaz. Ayşe'ye giden 2 BTC ve Ali'nin kendisine gelen 8 BTC de bir işlemin çıktıları olup birer UTXO'dur. Ali ve Ayşe başka bir işlem için bunları kullanabilecektir. Ayşe'ye gönderilen işlemin UTXO'su, Ayşe'nin açık anahtarının adresini barındırır (scriptPubKey). Bu nedenle bu harcanmamış çıktıyı harcayabilecek tek kişi, gizli anahtarı elinde bulduran Ayşe olacaktır. Görüldüğü üzere Bitcoin'de sahip olunan kripto paranın hesaplanmasında hesap bakiyesi modeli kullanılmaz; bunun yerine harcanmamış işlem çıktılarının toplamından faydalanılır. Yani sadece Ayşe'nin kullanabileceği UTXO'ların toplamı aslında Ayşe'nin sahip olduğu Bitcoin miktarı anlamına gelir.

Bitcoin'in piyasa değeri, verinin alındığı anda 557.292.315.616 Amerikan doları olup, piyasa değeri en yüksek olan kripto paradır⁴⁶⁸. Bitcoin sıklıkla ödeme yapma amacıyla kullanılsa da, diğer kripto paralara karşı olan konumu ile birlikte düşünüldüğünde altına benzer bir biçimde değer saklama aracı olarak kullanıldığını belirtmek mümkündür.

3.3.1.2. Ethereum (ETH)

Piyasa değeri en büyük ikinci kripto para olmakla birlikte en fazla kullanılan blok zincir ağı Ethereum (ETH)'dur. Bir günlük işlem sayılarına bakıldığında, Bitcoin ağı üzerinde yaklaşık 270.000 işlem yapılmışken⁴⁶⁹, Ethereum ağı üzerinde 1.085.000 işlem yapılmıştır⁴⁷⁰. Ethereum ağı üzerinde yapılan bu işlem sayılarına ikinci katman çözümlerinin dâhil olmadığını da belirtmek gerekir.

Ethereum ilk kez 2013 yılında, 19 yaşında olan Rus asıllı Kanadalı bilgisayar programcısı Vitalik Buterin tarafından, Mastercoin adlı bir diğer blok zincir projesine yaptığı önerilerin dikkate alınmaması üzerine ortaya çıkmış; akıllı sözleşmeler odaklı, önceki blok zincir projelerine göre çok daha ölçeklenebilir bir blok zincir ağı olarak tanıtılmıştır⁴⁷¹. Projenin white paper'ı 2014 yılında Buterin tarafından⁴⁷², daha teknik açıklama ve kodları bulunduğu yellow paper'ı ise 2015 yılında Solidity programlama

⁴⁶⁸ CoinMarketCap.

⁴⁶⁹ Blockchain.com, "Charts", <https://www.blockchain.com/charts> (Erişim:24.05.2022)

⁴⁷⁰ Etherscan, "Ethereum Daily Transactions Chart", <https://etherscan.io/chart/tx> (Erişim:24.05.2022)

⁴⁷¹ Buterin, Vitalik, A Prehistory of the Ethereum Protocol, 14.09.2017, <https://vitalik.ca/general/2017/09/14/prehistory.html> (Erişim:24.05.2022)

⁴⁷² Buterin, 2014.

(akıllı sözleşme) dilinin de mucidi olan Gavin Wood tarafından yayınlanmıştır⁴⁷³. Ardından aynı yıl projenin “ilk para arzı [initial coin offering (ICO)]” gerçekleştirilmiş olup, 1 Ethereum’un 0,311 Amerikan dolarına satışı gerçekleştirilmiş⁴⁷⁴ ve 16.000.000 Amerikan doları fon toplanmıştır⁴⁷⁵.

Ethereum her ne kadar PoW sistemi ile ortaya çıkmış olsa da⁴⁷⁶, projenin ilk aşamalarından⁴⁷⁷ bu yana PoS sistemine geçiş için çaba gösterilmektedir. Ethereum şu anda PoS sistemine geçişin son aşamasındadır. Bu doğrultuda ilk aşama olarak 1 Aralık 2020’de “Beacon Chain⁴⁷⁸” yayınlanmış olup, “The Merge⁴⁷⁹” adı verilen PoS sistemine tam geçişin Ağustos 2022 itibariyle gerçekleşeceği tahmin edilmektedir⁴⁸⁰. Bu geçiş sonrası zincir üzerinde ölçeklendirmeyi sağlayacak “parçalama (sharding)” ve “parça zincirleri (shard chains)” uygulamaları mümkün hale gelecektir⁴⁸¹. Ölçeklendirme genel olarak ağın hızı, verimi ve kapasitesi ile bunu daha uygun bir hale getirme çabasıyla ilgilidir⁴⁸². Parçalama ise ağ üzerindeki yükü azaltmak amacıyla, ağı yatay olarak bölme işlemidir.

Ethereum ağı üzerinde işlem yapmak için ödenen ücrete “gas” adı verilmekte ve gas ücreti “gwei⁴⁸³” cinsinden ifade edilmekte olup, ağ yoğunluğuna ve ağ üzerinde yapılan işlemin türüne göre ödenen bu miktar değişmektedir. Örneğin gas ücretinin 10 gwei olduğu bir durumda ağ üzerinde alım satım işlemi yapmak yaklaşık birkaç dolar ücret ödemeyi gerektirmekteyken; gas ücretinin 100 gwei ya da daha üzeri olduğu durumlarda tek bir alım satım işlemi için yaklaşık 50 dolar üzerinde işlem ücreti ödemek gerekebilir. Yapılan işlemin karmaşıklık düzeyi arttıkça daha fazla işlem ücreti ödeme gündeme gelecektir.

⁴⁷³ Wood, Gavin, “Ethereum: A Secure Decentralised Generalised Transaction Ledger Eip-150 Revision”, 2015, <http://gavwood.com/Paper.pdf> (Erişim: 24.05.2022)

⁴⁷⁴ 1 Ethereum’un değeri 25.05.2022 itibariyle 2.000 Amerikan doları civarındadır.

⁴⁷⁵ Icodrops, “Ethereum”, <https://icodrops.com/ethereum/> (Erişim: 24.05.2022)

⁴⁷⁶ Buterin, 2014, s. 18.

⁴⁷⁷ Buterin, Vitalik, “Slasher: A Punitive Proof-of-Stake Algorithm”, 2014/b, <https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/> (Erişim:25.05.2022)

⁴⁷⁸ “İşaret Ağı” olarak adlandırılabilir.

⁴⁷⁹ Ethereum, “The Merge”, <https://ethereum.org/en/upgrades/merge/> (Erişim:25.05.2022)

⁴⁸⁰ Watcher News, “Ethereum Cofounder Vitalik Buterin Confirms That The Merge is Happening Soon, Plus Other Developments”, 21.05.2022, <https://watcher.guru/news/ethereum-cofounder-vitalik-buterin-confirms-that-the-merge-is-happening-soon-plus-other-developments> (Erişim:25.05.2022)

⁴⁸¹ Ethereum, “Shard chains”, <https://ethereum.org/en/upgrades/shard-chains/> (Erişim: 25.05.2022)

⁴⁸² Wood, 2016, s. 1.

⁴⁸³ Wei Dai’ye ithafen.

Ethereum’da Bitcoin’deki gibi UTXO modeli değil, hesap bakiyesi modeli kullanılır. Yani bir adres diğer bir adrese para aktarımı yaptığında, basit bir tabirle miktar gönderen hesabın bakiyesinden düşülüp, alıcı hesabın bakiyesine eklenir⁴⁸⁴. Ethereum ağında bir transfer işlemi, göndericinin ve alıcının cüzdan bilgisini, gönderilen para miktarını, gas değerlerini ve nonce gibi bilgileri içerir⁴⁸⁵. Nonce, bir işlemde ilgili Ethereum adresinde daha önce kaç çıkış işlemi olduğunu 0’dan başlamak üzere belirtmektedir. Nonce’in önemi “tekrar saldırısı (replay attack)” çerçevesinde anlaşılabilir⁴⁸⁶.

Tekrarlama saldırısı, geçerli bir veri aktarımının kötü niyetle tekrarlanarak sistemin manipüle edilmesidir. Örneğin bir komutan telsiz ile şifreli bir geri çekilme mesajı iletmektedir. Kötü niyetli kişi bu mesajı kaydedip, daha sonradan telsizden tekrar oynatarak askerlerin geri çekilmesini sağlayabilir. Burada kötü niyetli kişinin şifreli mesajı çözmesi gerekmez, askerlerin geri çekilmesini sağlamak için kaydı oynatması yeterlidir. Bunu Ethereum’a uyarlırsak, Ali bir adet kahve almış ve ödemesini Ethereum’la yapmıştır. Ertesi gün tekrar kahve almış ve tekrar Ethereum ile ödemiştir. Her iki işlemde de gönderici, alıcı ve ödeme miktarı aynıdır. Bu haliyle ağın ilk işlem ile bilgileri tamamen aynı olan ikinci işlemi kabul etmesi demek, aynı bilgilerle üçüncü, dördüncü vd. kez işlem yapılabileceği anlamına gelecektir. Bu durumda eğer kahve dükkanı kötü niyetliyse işlem bilgilerini ağa sürüp Ali kahve almasa bile almış gibi ödeme yaptırabilecektir. İlk işlem ile aynı olan ikinci işleminin ağ tarafından kabul edilmemesi durumunu ele aldığımızda ise, bu sefer de Ali sadece bir kez kahve alabilecektir, ikinci kez kahve almak istediğinde ağ tarafından reddedilecektir. Karşılaşılabilecek bu problemleri engellemek için nonce devreye girecektir. İşleme eklenen nonce bilgisi, aynı işlemin tekrarlanmasını engeller. Ali’nin işleminin nonce ihtiva ettiğini hesaba katarsak, kahve dükkanı bunu ağa sunsa bile işlem ağ tarafından reddedilecektir; çünkü bu nonce daha önce başka bir işlem için kullanılmıştır.

⁴⁸⁴ Ethereum, 2014, s. 15.

⁴⁸⁵ Buterin, 2014, s. 15.; Ethereum, “Transactions”, <https://ethereum.org/en/developers/docs/transactions/> (Erişim:26.05.2022)

⁴⁸⁶ Zindros, Dionysis, Lecture 10: Accounts Model and Merkle Trees, EE 374: Blockchain Foundations, Stanford University, Spring 2022, ss. 2-3. https://web.stanford.edu/class/ee374/lec_notes/lec10.pdf (Erişim:26.05.2022)

Ethereum'un arzı Bitcoin gibi sınırlı değildir. Dolaşımında şu anda 120,914,182.69 ETH bulunmaktadır⁴⁸⁷. Bununla birlikte 2021 yılında gelen "EIP-1559" güncellemesi⁴⁸⁸ ile ağ üzerinde gerçekleşen işlemler için ödenen ücretlerin bir kısmı yakılmaktadır. Güncellemeden bu yana yaklaşık 2.360.000 ETH yakılmış olup⁴⁸⁹, bu değer 4.500.000.000 Amerikan dolarının üzerindedir.

Ethereum, "Ethereum Sanal Makinesi [Ethereum Virtual Machine (EVM)]" adı verilen bir yürütme modeline sahiptir⁴⁹⁰. EVM'yi basitçe izah etmek gerekirse, akıllı kontratların işlemlerinden sorumlu olan sanal bir bilgisayar olarak düşünülebilir.

Ethereum kripto paralar arasında Bitcoin'den sonra piyasa değeri en büyük ikinci kripto paradır. Ethereum'un şu anki durumu ile en önemli blok zincir olduğunu söylemek mümkündür. Bunun sebebi Ethereum'un Bitcoin gibi bir ödeme aracı olma amacıyla değil, blok zincir üzerinde merkeziyetsiz uygulamalara imkan tanıma amacı ile oluşturulmasından ötürüdür⁴⁹¹. Gerçekten de Ethereum, bütün blok zincirler arasında akıllı sözleşmelerin (smart contract), merkeziyetsiz finansın (DeFi) ya da merkeziyetsiz uygulamaların (DApp) en önemli ve en çok kullanılan adresidir.

3.3.1.3. Monero (XMR)

Bu başlık altında bahsedilmesi gerekli bir diğer kripto para, çalışmanın devamında daha ayrıntılı bir şekilde incelenecek olan ve bu çalışmayı yakından ilgilendiren Esperanto dilinde "para" anlamına gelen ve gizlilik odaklı bir kripto para olan Monero (XMR)'dur. Monero ve diğer gizlilik odaklı kripto paraların yasa dışı faaliyet gerçekleştirenlerin ilk tercihi olduğu bilinmektedir⁴⁹², özellikle yasa dışı faaliyetlerin ve bu faaliyetlerin ticaretinin gerçekleştiği ve geleneksel tarayıcılar ile ulaşılamayan Darknet'te Monero ve türevleri sıklıkla kullanılmaktadır.

Monero, 2014 yılında Bytecoin (BCN)'den çatallanarak oluşmuştur. Monero, ilk kez 2012 yılında Nicolas van Saberhagen adlı kimliği bilinmeyen bir kişi tarafından

⁴⁸⁷ CoinMarketCap, "Ethereum", <https://coinmarketcap.com/currencies/ethereum/> (Erişim:25.05.2022)

⁴⁸⁸ Github, "ethereum/EIPs", <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md> (Erişim:25.05.2022)

⁴⁸⁹ Watch the Burn, <https://watchtheburn.com> (Erişim:25.05.2022)

⁴⁹⁰ Wood, 2016, s. 10.

⁴⁹¹ Buterin, 2014, s. 34.

⁴⁹² Chainalysis, 2020, s. 81.

ortaya konan, “CryptoNote⁴⁹³” protokolünü kullanmaktadır. Monero işlemlerinde gönderici, gönderilen para miktarı ve alıcı gözükmeyen⁴⁹⁴. Monero’nun bu doğrultuda izlenemezlik ve bağlantısızlık sağladığı söylenebilir⁴⁹⁵, bu durum Monero’yu gizliliğini korumak isteyenlerin ya da kanunların yasakladığı eylemleri gerçekleştirmek isteyenlerin ilk tercihlerinden biri haline getirmektedir.

3.3.1.4. BNB

Başlık altında bahsedilecek bir diğer kripto para BNB’dir. BNB’nin arz ettiği özellik, piyasa değeri en yüksek dördüncü kripto para olmakla birlikte, merkezi bir kripto para borsası aracılığıyla ortaya çıkmış merkeziyetsiz bir kripto para olmasından kaynaklanmaktadır. BNB, dünyanın en çok kullanılan kripto para borsası olan Binance’in teşvikiyle oluşturulmuştur. BNB ağı, Ethereum ağından esinlenmekte; daha düşük miktarda bir işlem ücreti sunarak bünyesinde akıllı sözleşmeler, merkeziyetsiz finans ve merkeziyetsiz uygulamalar gibi blok zincir uygulamalarını barındırmaktadır.

3.3.1.5. Polkadot (DOT)

Başlık altında genel hatlarıyla incelenecek son ağ ve bu ağın kripto parası Polkadot (DOT) olacaktır. Polkadot 2016 yılında Ethereum kurucularından Gavin Wood tarafından oluşturulmuş olup⁴⁹⁶, Polkadot ağı 2020 yılından itibaren çalışmaktadır.

Polkadot’un özelliği heterojen bir parçalama (sharding) mimarisine sahip olmasıdır. Polkadot mimarisinde “relay chain⁴⁹⁷” adı verilen bir ana zincir bulunmaktadır. Bu zincir güvenliğin ve konsensüsün sağlanmasından sorumlu olup, bu sorumluluklara yoğunlaşması dolayısıyla akıllı kontrat çalıştırma gibi işlevleri bulunmamaktadır⁴⁹⁸. Polkadot’ta relay chain’e bağlı “parachain” adı verilen parçalar, paralel zincirler

⁴⁹³ van Saberhagen, Nicolas, “CryptoNote v 2.0”, 2013. <https://bytecoin.org/old/whitepaper.pdf> (Erişim:25.05.2022)

⁴⁹⁴ Monero, “How is Monero’s privacy different from other coins?”, <https://www.getmonero.org/get-started/faq/#anchor-different> (Erişim:25.05.2022)

⁴⁹⁵ van Saberhagen, 2013, s. 4.

⁴⁹⁶ Wood, Gavin, “Polkadot: Vision For A Heterogeneous Multi-Chain Framework”, 2016. <https://polkadot.network/PolkaDotPaper.pdf> (Erişim:25.05.2022)

⁴⁹⁷ Türkçeye “röle zincir” olarak çevrilebilir.

⁴⁹⁸ Polkadot, “Smart Contracts”, <https://wiki.polkadot.network/docs/build-smart-contracts> (Erişim:25.05.2022)

bulunmaktadır. Parachain'ler güvenlik ve konsensüs gibi unsurlarda relay chain'e bağlı olsalar da, kullanım amaçlarına göre istenilen yönde özelleşebilirler. Parachain'ler kendi konsensüs algoritmasını işletemezler, bu bakımdan relay chain'lere bağlıdırlar. Bu doğrultuda, ancak parachain'ler aracılığıyla relay chain'e bağlı bir zincir kendi konsensüs algoritmasını kullanabilir⁴⁹⁹. Polkadot ekosistemi, bu özellikleriyle “merkeziyetsiz bir federasyon”a benzetilebilir⁵⁰⁰.

3.3.2. Satoshi Nakamoto

Kripto paralar söz konusu olduğunda en çok kullanılan kavram beklenildiği üzere ilk kripto para olan Bitcoin ve Bitcoin'i ortaya çıkaran kimliği belirli olmayan bir kişi ya da grup olan Satoshi Nakamoto'dur. Nakamoto'nun ilk kripto para ve blok zincirin geliştiricisi olması, bu iki kavramın günümüzde sahip olduğu konum düşünüldüğünde Nakamoto'yu oldukça önemli bir özne haline getirmektedir.

Nakamoto'nun gerçek kimliği hakkında 2008 yılından bu yana birçok teori ve spekülasyon üretilmiş olup; kesin bir sonuca ulaşılamamıştır. Bu teoriler çerçevesinde Nakamoto'nun bilinen bazı kriptograflardan biri olduğu, ya da Nakamoto'nun bir devlet, bir kuruluş ya da bir örgüt tarafından var edildiği iddia edilebilmektedir.

Nakamoto'nun Bitcoin üzerinde 2007 yılından bu yana çalıştığı, Kriptografi Posta Listesi'nde (Cryptography Mailing List) Nakamoto'yu ilk cevaplayan James A. Donald ile Nakamoto arasında geçen diyaloglardan ulaşılmaktadır⁵⁰¹. Bununla birlikte Nakamoto'nun web üzerinde son görüldüğü tarih ise 13 Aralık 2010'dur. Nakamoto hakkında, Bitcoin kullanıcıları ve geliştiricilerini birleştiren bir platform olan “bitcointalk” forumunda son aktif olduğu söz konusu tarihten sonra hiçbir aktiflik belirtisi bulunmamakla birlikte⁵⁰², Nakamoto tarafından Bitcoin geliştiricilerine yollanan son e-postalar Nisan 2011 tarihine aittir⁵⁰³.

⁴⁹⁹ Polkadot, “Parachains”, <https://wiki.polkadot.network/docs/learn-parachains#what-is-parachain-consensus> (Erişim:26.05.2022)

⁵⁰⁰ Wood, 2016, s. 1.

⁵⁰¹ Nakamoto, Satoshi, “...I believe I've worked through all those little details over the last year and a half while coding it...”, Satoshi Nakamoto Institute, <https://satoshi.nakamotoinstitute.org/emails/cryptography/15/> (Erişim:26.05.2022)

⁵⁰² Bitcointalk, Summary – satoshi, <https://bitcointalk.org/index.php?action=profile;u=3> (Erişim:26.05.2022)

⁵⁰³ Nakamoto, Satoshi, “I've moved on to other things. It's in good hands with Gavin and everyone.”, 23.04.2011, <https://pastebin.com/syrmi3ET> (Erişim: 26.05.2022); Nakamoto, Satoshi, “I wish you

Nakamoto'nun kimliği hakkında öne sürülen ilk kişi, doğum ismi "Satoshi Nakamoto" olan "Dorian Nakamoto" adında Japon asıllı Amerikan bir bilgisayar programcısıdır. Bitcoin'i ortaya çıkaran Satoshi Nakamoto'nun belgelerde ve iletişimde kullandığı dil hatasız ve akıcı bir İngilizce iken, Dorian Nakamoto'nun yayınlamış olduğu belgelerde bozuk bir gramer kullanmış olması ve kriptografi alanı ile ilgilenmemiş olması bu kişinin Nakamoto olmadığı, sadece bir isim benzerliği olduğu kabulüne götürmektedir.

Nakamoto için öne sürülen isimlerden bir diğeri, belki de en güçlüsü; Nakamoto dışındaki ilk Bitcoin kullanıcısı, geliştiricisi ve ilk Bitcoin transferinin alıcısı olan⁵⁰⁴; ayrıca çalışmanın yukarısında da açıklanan ve Bitcoin'deki PoW sistemini oldukça andıran RPoW sistemini ortaya koyan Amerikan kriptograf Hal Finney'dir. Finney'nin Bitcoin ile belirtilen derecede yakın ilişkisinin olması ve Bitcoin'i oluşturabilecek yeterlilikte kriptografi uzmanlığının olmasının yanında; Finney'nin Dorian Nakamoto'nun aile evinin birkaç blok ötesinde yaşamış olması⁵⁰⁵ ve bu ismi kimliğini korumakla amacıyla seçmiş olması ihtimali ile birlikte; Finney'in ALS hastalığına yakalandığı tarih ile Nakamoto'nun son aktiflik tarihinin birbirine yakın olması; Finney'nin Nakamoto'nun Bitcoin üzerinde çalışmaya başladığı 2007 senesinde sosyal medya platformu Twitter'a üye olup "çalışıyorum"⁵⁰⁶ şeklinde bir paylaşımda bulunması ve söz konusu platformda Nakamoto'nun kaybolduğu tarihten oldukça kısa bir süre önce son paylaşımı yapması ile Bitcoin ağı üzerindeki diğer bazı bulgular⁵⁰⁷, Finney'nin Nakamoto olduğu ihtimallerini güçlendirmektedir.

Nakamoto ile ilişkilendirilebilecek bir diğer kişi, yine çalışmanın yukarısında bahsedilmiş, 1998 yılında öne sürülen "Bit Gold (Bit Altın)" modelinin sahibi Nick Szabo'dur⁵⁰⁸. Bit Gold gerek barındırdığı fikir gerek ise sunduğu teknolojik model

wouldn't keep talking about me as a mysterious shadowy figure, the press just turns that into a pirate currency angle. Maybe instead make it about the open source project and give more credit to your dev contributors; it helps motivate them.", 26.04.2011, <https://www.bitcoin.com/satoshi-archive/emails/gavin-andresen/1/#selection-29.0-29.252> (Erişim:26.05.2022)

⁵⁰⁴ <https://www.blockchain.com/btc/tx/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16> (Erişim: 24.05.2022)

⁵⁰⁵ Greenberg, Andy, "Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius", Forbes, 25.03.2014. <https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/?sh=5e228ca94a37> (Erişim: 26.05.2022)

⁵⁰⁶ Finney, Hal (@halfin), "working", Twitter <https://twitter.com/halfin/status/314825462?s=20&t=I4pcOgom7DXIIGWke5WL9A>

⁵⁰⁷ Taras, Payment No. 1: A Closer Look at the Very First Bitcoin Transfer, Bitcointalk, 02.11.2017, <https://bitcointalk.org/index.php?topic=234692.0> (Erişim: 26.05.2022)

⁵⁰⁸ Szabo, 2005.

anlamında Bitcoin’i andırmaktaydı. Bit Gold’da Bitcoin’e benzer şekilde PoW sistemi ön görülmüş; blok zincire benzer bir şekilde “bit⁵⁰⁹ ipi” tabiri kullanılmıştır. Bunun yanında Szabo’nun Nakamoto tarafından yayınlanan Bitcoin makalesinde kısa bir süre sonra 2005 tarihli Bit Gold yazısının⁵¹⁰ metnine dokunmaksızın yayın tarihini Bitcoin yayınından sonra olacak şekilde ayarlamış olması, parapraksi⁵¹¹ ile Bitcoin’i dizayn ettiğini söylemesi gibi sebeplerle Nakamoto olduğu öne sürülebilmektedir.

Nakamoto ile sıklıkla ilişkilendirilen bir diğer kişi ise yine bu çalışmanın yukarısında bahsedilen ve PoW modelini ilk kez ortaya koyan⁵¹², yazım teknikleri Nakamoto’ya oldukça benzeyen Adam Back’tir.

Nakamoto’nun kimliğini saklaması ve bir süre sonra ortadan kayboluşunun, Bitcoin’in bir kişi, grup ya da kuruma dayanmayan merkeziyetsiz bir ödeme aracı olması vasfını korumak amacıyla olduğu söylenebilir.

3.3.3. PoW ve PoS

PoW ve PoS mekanizmaları, blok zincir ve kripto paraların en önemli unsurlarından olup, çalışmanın yukarısında geniş bir şekilde işlenmiş olmakla birlikte, tekrere düşmemek adına aynı konulara tekrar değinilmeyecektir. PoW ve PoS çoğunlukla bir konsensüs mekanizması olarak adlandırılrsa da⁵¹³; bunların tek başına konsensüs mekanizmaları olmadıkları, sybil kontrol mekanizması oldukları öne sürülebilmektedir⁵¹⁴. Bu görüşe göre Bitcoin’de konsensüse ulaşmak için sadece PoW yeterli değildir, en uzun zincir seçimi dahilinde konsensüse ulaşılabilir. Bu doğrultuda PoW ve PoS sybil kontrol mekanizmaları, yani kötü niyetli bir kişi veya bir grubun birden

⁵⁰⁹ Veri depolama ve transferlerde en küçük birim.

⁵¹⁰ Szabo, 2005.

⁵¹¹ Psikolojide bastırılmış bir iç düşüncenin tezahürü olarak ortaya çıkmış hareket.

⁵¹² PoW sistemi ilk kez Back tarafından ortaya kosa da modelin temeli (bkz: Dwork ve Noir, 1992.) tarafından oluşturulmuştur.

⁵¹³ Ethereum, “Proof-of-Stake (PoS)”, <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#:~:text=Ethereum%20has%20used%20PoW%20since,scaling%20solutions%20to%20be%20implemented.> (Erişim:25.05.2022)

⁵¹⁴ Sirer, Emin Gün (@el33th4xor), “Ok, there is a terribly wrong framework emerging around consensus protocols. People think that PoW and PoS are consensus protocols, and that they are the only two consensus protocols out there. This is false. Let me explain...”, Twitter, 13.06.2018, <https://twitter.com/el33th4xor/status/1006931729679044608> (Erişim:26.05.2022)

fazla hesap, node, bilgisayar vb. ile ağı geçirmeye çalışması anlamına gelen sybil atakları engelleyen bir mekanizma oldukları öne sürülür.

Bitcoin, Litecoin, Dogecoin gibi kripto paralar PoW sistemi ile işlemekteyken; Solana, Cardano, Tezos gibi ağlar PoS sistemini kullanır.

PoW sistemleri madencilik işlemleri gerektirdiğinden, yoğun işlem gücü ve enerji kullanımına sebebiyet vermeleri dolayısıyla eleştirilmektedirler. PoS sisteminde ise madencilerin yerini “doğrulayıcı”lar almaktadır. PoS sisteminin madencilığe bağlı olmaması nedeniyle daha çevreci bir mekanizma olduğundan bahsedilmektedir.

3.3.4. Genel Olarak Anonimlik, İzlenemezlik ve Gizlilik (Privacy) Odaklı Kripto Paralar

Gizlilik odaklı kripto paraların bu çalışmanın konusunu yakından ilgilendirdiği söylenebilir. Çünkü bu tür kripto paralar, gizlilik sağlama amacıyla oluşturulduklarından, özellikle yasa dışı faaliyetlerde bulunacak kişilerin, çalışma bağlamında terörizmin finansmanı eylemini sağlayacak kişilerin, ilk başvurduğu kripto paralar olacaktır. Çalışmanın yukarısında da terör örgütü El-Kaide'nin gizlilik odaklı kripto paralar ile fon toplamaya çalıştığı örneği belirtilmiştir.

Blok zincirlerdeki işlemlerin, aksi şekilde oluşturulmadıkları sürece, genel olarak herkes tarafından izlenebildiğini ve takip edilebildiğini söylemek mümkündür. Fakat bu durum gizlilik odaklı kripto paralarda tersine dönmektedir. Bu tür kripto paralarda, para aktarım işleminde gönderenin, göndericinin ve gönderim miktarının bilgileri gizlidir.

Bu aşamada tekrar belirtmek gerekir ki, sahibi tarafından açıklanmadığı sürece kripto paralarda gönderici ve alıcı kimliği anonimdir. Çünkü gönderici ve alıcı kısmında gönderici ve alıcının gerçek isimleri değil, onlarca harf ve rakamdan oluşan cüzdan adresleri bulunmaktadır. Bu cüzdan adresinin kime ait olduğu bilinemez, bu nedenle anonimdir. Örneğin bağımsız bir Ethereum ağı tarayıcısı olan Etherscan üzerinden yapılan bir Ethereum işlemine bakılırsa:

Şekil 3. 4 Gerçekleştirilen ilk Ethereum transferi.

Transaction Hash:	0x5c504ed432cb51138bcf09aa5e8a410dd4a1e204ef84bfed1be16dfba1b22060
Block:	46147 14802265 Block Confirmations
Timestamp:	2484 days 10 hrs ago (Aug-07-2015 03:30:33 AM +UTC)
From:	0xa1e4380a3b1f749673e270229993ee55f35663b4
To:	0x5df9b87991262f6ba471f09758cde1c0fc1de734
Value:	0.000000000000031337 Ether (<\$0.000001)
Transaction Fee:	1.05 Ether (\$1,927.40)

(Kaynak: Etherscan⁵¹⁵)

şekil üzerinden görülebildiği üzere, gönderici ve alıcı adresleri “0x” ile başlayan ve 42 karakterle ifade edilen karışık dizilerdir. Burada gönderen ya da alıcı kimliğiyle alakalı hiçbir sonuç çıkarılamaz. Çünkü 42 karakterli bu hesabın sahibi herhangi biri olabilir, bu da anonimlik anlamına gelir. Fakat bu anonimliğin korunması, hesabı kontrol eden kişinin elindedir. Örneğin yukarıdaki İzzeddin el-Kassam Tugayları örneğinde, fon toplamının ilk aşaması merkezi bir borsa üzerinde bulunan bir hesap aracılığıyla gerçekleşmişti. Bu nedenle fon toplanan hesabın borsa üzerindeki bütün kimlik bilgilerine erişilebilmiş, hesap dondurulabilmişti. Belirtmek gerekir ki, merkezi bir kripto para borsası üzerinde açılan bir hesabı kullanıcılar kontrol etse de, hesabın asıl sahibi bu hesabın özel anahtarını elinde bulunduran borsadır. Bu örnekte alıcı hesabı her ne kadar özünde anonim olsa da, bir borsa ile ilişkilendirilebildiğinden kimlik tespit edilebilmiştir.

Anonimliğin bozulması bir beyan ile de gerçekleşebilir. Örneğin yukarıdaki şekilde, “0x” ile başlayan hesabın sahibi, bu hesabın kendisine ait olduğunu bir şekilde beyan etmiş olursa, doğal olarak bu beyandan haberdar olan kişilere karşı anonimlik

⁵¹⁵ Etherscan,
<https://etherscan.io/tx/0x5c504ed432cb51138bcf09aa5e8a410dd4a1e204ef84bfed1be16dfba1b22060>
(Erişim: 26.05.2022)

kalmayacaktır. Ya da, “0x” ile başlayan hesabın sahibi “Ethereum Name Service⁵¹⁶” gibi bir isimlendirme servisi kullanarak adresini isimlendirmiş olabilir. Bu durum ile hesabın sahibinin tam anonimliğe gerek duymadığı ya da anonim olmak istemediği zaman karşılaşılabılır. Örneğin bu şekilde hesabın sahibi, adresini diğer kullanıcılara kendi seçtiği isim doğrultusunda, “0x” ile başlayan 42 haneli adresin yanında “ahmet.eth”, “ahmetyilmaz.eth” ya da bu hesabın sahibi bir kurum olursa “inonu.eth” şeklinde isimlendirmiş olabilir. Bu isimlendirme eşsiz olup, başka bir kişi bu ismin tescil süresi bitene kadar bu ismi kullanamaz. Bu doğrultuda bu hesapların yaptığı işlemlerde “0x” ile başlayan adres yerine “ahmet.eth” ya da “inonu.eth” gibi isimler gözükeceğinden diğer kullanıcılar hesabın kime ait olduğunu bileceklerdir.

Bunun yanında bir hesabın anonimliği, hesabın gerçekleştirmiş olduğu blok zincir işlemleri incelenerek de bozulabilir. Çalışmada sıkça belirtildiği üzere, blok zincirler üzerinde yapılan bütün işlemler izlenebilir ve şeffaftır. Bir hesabın gerek alıcısı gerek göndericisi olduğu bütün kripto para aktarımları, etkileşime girdiği akıllı sözleşmeler, kısaca blok zincir üzerinde yaptığı her faaliyet herkes tarafından (istisnaları olmak kaydıyla) izlenebilir, görülebilir ve kontrol edilebilir. Hatta bir örnek üzerinden izah edilirse, Bitcoin’in kazılmaya başlandığı ilk ayda kazılan ve o tarihten (2009) bu yana hareket ettirilmeyen bir hesaba ait Bitcoin’ler yakın bir tarihte hareket ettirilmiş ve bundan herkesin haberi olmuştur; çünkü o hesabın ya da herhangi bir hesabın yaptığı ve yapacağı bütün işlemler ağ üzerinden izlenebilir. Çalışmanın yukarısında bahsedilen kripto para aracılığıyla gerçekleştirilen bazı terörizmin finansmanı girişimleri de, fonlayan ya da fonlanan hesaplar anonim olsa da, ağ üzerindeki işlemler arasındaki ilişki detaylı bir şekilde takip edilerek ortaya çıkarılmıştır. Söz konusu örneklerde de karşılaşıldığı üzere, hesabın sahipleri anonim olsa da, anonim olmayan bazı hesaplar (özellikle borsa hesapları) ile yaptıkları işlemler hesabın sahibinin kimliğini ortaya çıkarabilir; ortaya çıkarmasa da en azından bazı kişi, kurum ve örgütler ile olan ilişkisini ortaya koyabilir.

Bu aşamada dikkat çekmek gerekir ki, kripto paraların yapıları gereği her ne kadar terörizmin finansmanı amacına oldukça uygun olduğundan sıklıkla bahsedilebilmekle

⁵¹⁶ Ethereum Name Service (ENS), Ethereum cüzdanı sahiplerinin belli bir ücret karşılığında belirledikleri sene sayısınca bir Ethereum ismini tescil edebildikleri, DNS (domain, alan adı) benzeri bir uygulamadır.; Ethereum Name Service, <https://ens.domains> (Erişim: 26.05.2022)

birlikte, izlenebilirlikleri ve şeffaflıkları sayesinde yeri geldiğinde terörizmin finansmanının önlenmesini de sağlayabilecekleri göz önünde bulundurulmalıdır. Nakit para ile yapılan bir finansman sağlama örneğinde paranın kimden kime, ne zaman, hangi miktarda aktarıldığının belirlenmesi oldukça zor olsa da; kripto para aracılığıyla yapılan bu tür bir işlemde, kripto paranın hangi adresten hangi adrese, ne zaman ve hangi miktarlarda gerçekleştirildiği “herkes” tarafından görülebilir. Fakat bu çıkarımların istisnasını gizlilik odaklı kripto paralar ve diğer gizlilik sağlayan ve izlenebilirliği kesen uygulamaların teşkil ettiği de belirtilmelidir.

Gizlilik odaklı kripto paralarda, aksi seçilmemişse, gönderenin ve alıcının adresleri ve gönderim miktarı gizlidir, diğer kişiler tarafından görülemez. Bu doğrultuda “izlenebilir” diğer blok zincirler karşısında, bu tür kripto paraların “izlenemez” oldukları belirtilebilir.

Gizlilik odaklı kripto paralara, yukarıda da incelenen Monero (XMR) örnek verilebilir. Monero “CryptoNote” altyapısını ve bu altyapının bir parçası olarak RandomX iş kanıtı (PoW) algoritmasını kullanır.

Diğer çoğu gizlilik odaklı kripto paranın aksine Monero transferleri “kendiliğinden” gizli ve izlenemezdir. Yani bir kişinin Monero ile yaptığı bir işlem, herhangi bir ek özellik kullanmasına gerek kalmaksızın gizli olacaktır. Monero’da gönderenin ve göndericinin kimliği ile gönderim miktarı gizlidir. Bu demektir ki, dışarıdan işlemleri izlemeye çalışan biri bu bilgileri göremeyecektir. Hatırlatılması gerekirse, örneğin Bitcoin ve Ethereum gibi kripto paralarda işlemler herkes tarafından izlenebilir; göndericinin ve alıcının adresi ve gönderim miktarları herkes tarafından görülebilmektedir.

Monero gizliliği sağlamak için “Gizli Adres (Stealth Adres)”, “Halka İmza (Ring Signature)”, “RingCT” ve “Bulletproof (kurşun geçirmez)” adı verilen teknolojilerden faydalanır.

Bir Monero adresi oluşturulduğunda, adres sahibi, çalışmanın yukarısında açık anahtarlı şifrelemede bahsedildiği üzere, açık anahtar ve gizli anahtara sahip olacaktır. Bu açık ve gizli anahtarlar ikişer tanedir. Bunlar, açık görüntüleme anahtarı ve gizli görüntüleme anahtarı ile açık harcama anahtarı ve gizli harcama anahtarıdır⁵¹⁷.

⁵¹⁷ Monero, “Stealth Adres”, <https://www.getmonero.org/resources/moneropedia/stealthaddress.html> (Erişim: 27.05.2022)

Monero’da bir hesabın kime ait olduğu, hesaba gelen ve hesaptan çıkan işlemler ya da hesabın bakiyesi, hesap sahibi dışında kimse tarafından bilinemez. Fakat eğer hesap sahibi isterse gizli görüntüleme anahtarını biriyle paylaşabilir. Hesap sahibinin gizli görüntüleme anahtarını elde eden bu kişi, hesabın sahip olduğu çıktılarını (output) görebilir. Fakat bu çıktılar, hesaba gelen işlemleri yani hesaba giren para miktarını ifade eder. Bu çıktıların ne kadarının harcandığı, yani hesaptan çıkan para miktarı ve dolayısıyla hesabın bakiyesi; hesabın gizli görüntüleme anahtarını elde eden kişi tarafından tam olarak bilinemez⁵¹⁸. Gizli harcama anahtarı ise hesap sahibinin XMR gönderebilmesini ve gerektiğinde hesabını tekrar kurabilmesini sağlar⁵¹⁹.

Gizli Adres özelliğinde, bir kişi XMR gönderirken alıcı adına tek kullanımlık bir açık adres oluşturulur. Bu açık adres, alıcının Monero adresi hakkında bilgi vermez, bu nedenle yapılan hiçbir işlem alıcının ya da göndericinin cüzdanı ile ilişkilendirilemez. Alıcının adresini sadece alıcı ve gönderici bilmektedir.

Kriptografide “halka imza (ring signature)”, özel bir imzalama tekniğidir. Bu teknikte bir mesaj, bir grup tarafından, bu gruptaki herhangi biri tarafından imzalanır. Fakat burada imzalayanın hangi kişi olduğu bilinemez. Halka imza tekniği ilk olarak 2001 yılında Ronald Rivest, Adi Shamir ve Yael Tauman tarafından ortaya konmuştur⁵²⁰. Halka imza tekniği, 1991 yılında David Chaum ve Eug`ene Van Heyst tarafından ortaya konan “grup imza tekniği”ne benzemektedir⁵²¹. İki teknikte de imzalama gruptan biri tarafından gerçekleştirilmektedir. Grup imza tekniğinde, güvenilir bir grup yöneticisinin önceden belirlediği bir grubun içinden bir kişi, grubun adına dijital imzalama gerçekleştirir. Fakat halka imza tekniğinde gruplar önceden ayarlı değildir; grup imza tekniğinde olduğu gibi grubu belirleyen, yöneten ya da kötü niyetli imzalama gerçekleştirenlerin anonimliğini kaldırabilen bir grup yöneticisi bulunmamaktadır. Bununla birlikte gruptaki kişiler birbirleri hakkında bilgiye sahip değillerdir, grup birlikte hareket etme amacını taşımaz⁵²².

⁵¹⁸ Monero, View Key, <https://www.getmonero.org/resources/moneropedia/viewkey.html> (Erişim: 27.05.2022)

⁵¹⁹ Monero, Spend Key, <https://www.getmonero.org/resources/moneropedia/spendkey.html> (Erişim: 27.05.2022)

⁵²⁰ Rivest, Ronald L. vd., “How to Leak a Secret”, Advances in Cryptology — ASIACRYPT 2001, 2001. <https://people.csail.mit.edu/rivest/pubs/RST01.pdf> (Erişim: 27.05.2022)

⁵²¹ Chaum, David and Eug`ene Van Heyst. Group signatures. Advances in Cryptology — Eurocrypt ’91, 1991. https://chaum.com/wp-content/uploads/2021/12/Group_Signatures.pdf (Erişim:27.05.2022)

⁵²² Rivest vd., 2001, ss. 552-553.

Monero’da kullanılan halka imza göndericinin gizliliğini korur. Göndericinin imzaladığı işlem ile daha önce imzalanmış ve gerçekleştirilmiş herhangi Monero işlemleri kullanılarak dışarıdan izleyenleri yanıltmak amacıyla bir halka imza oluşturulur. Bu halka imza grubunda, imzalayanın kim olduğunu sadece gönderici bilebilir, dışarıdan bakan bir kişi ise asıl transferin kim tarafından gerçekleştirildiğini, diğer bir tabirle kim tarafından imzalandığını bilemeyeceğinden transferi gerçekleştiren gizli kalmış olur, işlem izlenemez hale gelir.

Yukarıda açıklanan ve Monero’da kullanılan bu teknolojiler sayesinde gönderici ve alıcının kimliklerinin nasıl gizli kaldığı ortaya konmuştur. Bununla birlikte Monero’da gönderilen miktar da gizlidir; bu da “RingCT⁵²³” teknolojisine ve bu teknolojinin işleyişine yardımcı olan “Bulletproof (kurşun geçirmez)” teknolojisi sayesinde mümkün olur.

Monero’nun sağladığı bir diğer özellik, Monero’nun “değiştirilebilirliğe (fungibility)” sahip olmasıdır. Değiştirilebilirlik kısaca bir para ya da emtia’nın aynı özelliklere sahip başka bir para ya da emtia ile değiştirilebilir olmasını ifade eder. Örneğin nakit 20 Türk lirası değiştirilebilirdir, çünkü bir kişinin elindeki 20 Türk lirası ile başka bir kişinin elindeki 20 Türk lirası aynı anlamı ifade eder, aynı işlevi görür. Fakat Bitcoin başta olmak üzere çoğu kripto para da değiştirilebilirlik sorunu bulunduğu kabul edilmektedir⁵²⁴. Çünkü bir Bitcoin transferinin kaynağı, istenirse ilk kazıldığı ana kadar geriye doğru takip edilebilir. Kullanılan bir Bitcoin⁵²⁵, daha önceden yasadışı bir faaliyette kullanılmış olabilir, bu da her şeyin kaydının tutulduğu blok zincir üzerinden görülebilir. Burada “hafıza” kavramı kullanılabilir. Örneğin nakit paranın hafızası yoktur, birinin bir çikolata almak için kullandığı bir para, önceden başka biri tarafından uyuşturucu satın almak için kullanılmış olabilir, bu durum paraya bakarak söylenemez.

⁵²³ Shen Noether, Ring Confidential Transactions, 2016, <https://eprint.iacr.org/2015/1098.pdf> (Erişim: 27.05.2022)

⁵²⁴ Alex Lielacher, Crypto’s fungibility problem, Brave New Coin, <https://bravenewcoin.com/insights/ryptos-fungibility-problem> (Erişim: 27.05.2022); Charlie Lee (@SatoshiLite), “Fungibility is the only property of sound money that is missing from Bitcoin & Litecoin...”, Twitter, 28.01.2019, <https://twitter.com/SatoshiLite/status/1089935081337085952> (Erişim: 27.05.2022); Monero, Fungibility, <https://www.getmonero.org/resources/moneropedia/fungibility.html> (Erişim: 27.05.2022); Ver, Roger (@rogerkver), “#BTC isn't fungible, isn't private, and doesn't scale. It can never become p2p cash for the world. It might become the government surveillance coin for the world.”, Twitter, 27.05.2022, <https://mobile.twitter.com/rogerkver/status/1530210898505347074?cxt=HHwWhMC9zY2ts7wqAAAA> (Erişim: 28.05.2022)

⁵²⁵ Daha anlaşılır olması açısından UTXO üzerinden açıklanmamıştır.

Monero işlemleri izlenemez ve dolayısıyla geriye dönük takip edilemez olduklarından Bitcoin ve benzeri kripto paraların değiştirilebilirlik “sorun”unu⁵²⁶ aşmaktadır.

Kullanımı yaygın, gizlilik odaklı bir diğer kripto para, 2014 yılında ortaya çıkan “Dash”tir. Dash’in Monero kadar gizlilik sağlamadığı söylenebilir, çünkü Dash’te gizlilik tercihe bağlıdır. Tercih edilmediği sürece işlemler kendiliğinden gizli değildir. Bu doğrultuda kullanıcılar isterlerse Dash’in sunduğu “InstantSend” özelliğini kullanarak oldukça hızlı ve düşük bir komisyonla aktarım yapabilirken, isterlerse de “CoinJoin⁵²⁷” özelliğini seçerek gizli bir aktarım tercih edebilirler. Dash klasik PoW madenciliğinin yanına “masternode” denilen PoS sistemini de ihtiva ettiğinden hibrit bir algoritmaya sahiptir. Masternode’lar InstantSend ve CoinJoin’in işlemlerini sağlarlar⁵²⁸. Eğer kullanıcı gizli gönderim tercih etmişse, gönderilen Dash, benzer miktarlardaki diğer işlemler ile karıştırılarak alıcıya aktarılır. Bu sayede gönderim miktarı ve alıcı belli iken gönderenin kimliği belli olmayacaktır.

Gizlilik odaklı kripto paralar arasında en çok bilinenlerden biri de “Zcash (ZEC)”tir. Zcash, gizliliği sağlamak için “zk-Snark” teknolojisinden faydalanmaktadır.

zk-Snark’taki “zk” harfleri “zero-knowledge” yani “sıfır bilgi” anlamına gelmektedir. Kriptografide “sıfır bilgi” ya da “sıfır bilgi ispatı (zero-knowledge proof)”, bir kanıtlayıcının başka bir doğrulayıcıya, bir şeyin bilgisine sahip olduğunun o bilgiyi açığa çıkarmadan kanıtlanması anlamına gelir. Sıfır bilgi ispatının anlaşılması için sıklıkla “Ali Baba’nın Mağarası” örneği verilmektedir.

Tek bir girişi olan bir mağara bulunmaktadır. Bu mağaraya girişten biraz ileride mağara ikiye ayrılır, bu her iki yolun sonunda diğer yola geçmeyi sağlayan ve bir şifrenin fışıldaması ile açılan sihirli bir kapı bulunmaktadır. Ali ve Emre kişileri mağaranın önünde durmaktadır. Emre, içerideki gizli kapının şifresini bilmekte; şifreyi bildiğini de Ali’ye “bu şifrenin ne olduğunu ortaya çıkarmadan” kanıtlamak istemektedir. Emre mağaraya girer ve seçtiği bir yönde (1 veya 2) ilerler. Ardından Ali mağaraya girerek yolların ayrıldığı yere kadar gelir ve seçtiği yolu bağıdır. Ali eğer “1” diye bağırsa, Emre 1 numaralı yoldan; Ali eğer “2” diye bağırsa, Emre 2 numaralı yoldan çıkmalıdır. Burada Emre 1 numaralı yolu takip etmiş fakat Ali “2” diye bağırmış olabilir. Bu durumda

⁵²⁶ Kullanıcısına göre “sorun” olurken, düzenleyiciler ve otoriteler için bir “fırsat” anlamına gelebilir.

⁵²⁷ Önceden “PrivateSend” iken, gizliliği çağrıştırdığından, regülasyonlar sebebiyle CoinJoin isminin verildiği düşünülmektedir.

⁵²⁸ Dash, Masternodes, <https://www.dash.org/masternodes/> (Erişim: 27.05.2022)

Emre'nin 2 numaralı yoldan çıkmasının tek yolu sihirli kapıyı kullanmak olacaktır, bu da sihirli kapının şifresini gerçekten bildiğini Ali'ye kanıtlaması anlamına gelecektir. Bu süreç birden fazla olacak şekilde tekrarlanır, çünkü Emre şifreyi bilmeden şans eseri Ali'nin bağıracığı yolu seçmiş ve sonucunda o yoldan geri çıkmış olabilir. Çoklu tekrarlamalar sonucu Emre her seferinde Ali'nin seçtiği yoldan çıkıyorsa; Emre Ali'ye sihirli kapının şifresini bildiğini, şifrenin ne olduğu ortaya çıkmadan kanıtlamış olacaktır. Bu durum sıfır ispat kanıtına örnek oluşturacaktır.

Burada söz konusu işlem “ancak” Ali ve Emre arasında bir anlam ifade edecektir. Örneğin Ali'nin üzerinde taşıdığı gizli bir kamera ve bu kameradan olanları izleyen Veli olsun. Veli'nin burada göreceği tek şey, Ali'nin bir yönü bağırması ve Emre'nin o yönden çıkması olacaktır. Ali ve Emre, Veli'den gizli olarak bunu planlamış olabilir, yani Emre şifreyi bilmiyor ve Ali ile anlaşmış; Ali bağıracığı yönü Emre'ye söylemiş; Emre'de her seferinde o yönden girmiş ve dolayısıyla o yönden çıkmış olabilir. Bu doğrultuda üçüncü bir kişi olan Veli, hiçbir zaman tam olarak Emre'nin şifreyi bilip bilmediğini anlayamayacaktır.

Sıfır bilgi kanıtını açıklamak için resim örneği de verilebilir. Örneğin bir milyon kişinin katıldığı bir miting alanının yüksek çözünürlüklü bir fotoğrafı bulunmaktadır. A kişisi, bu mitinge katılmış olan C kişisinin nerede bulunduğunu bildiğini iddia etmektedir. B kişisi de A'nın bu iddiasını kanıtlamasını istemektedir. Fakat A, C'nin nerede olduğunu bildiğini kanıtlamak istemekle birlikte, C'nin “tam olarak” nerede bulunduğunu açığa çıkarmak istememektedir. Eğer A, C'nin bulunduğu yeri direkt olarak gösterirse (fotoğraftaki yeri işaretleyerek ya da parmak ile göstererek), sahip olduğu bilgiyi kanıtlamakla kalmayıp bilginin kendisini de B'ye iletmış olacak; B, bir milyon kişi arasında C'nin tam olarak nerde bulunduğunu öğrenmiş olacaktır. Bunun yerine A, sıfır bilgi ispatından yararlanabilir. Bu da A'nın, fotoğraf içerisindeki C'nin görüntüsünü keserek B'ye aktarması ile mümkün olabilir. Bu durumda A, C'nin nerede olduğunu bildiğini, C'nin yerini açığa çıkarmadan B'ye karşı ispatlamış olacaktır. Sonuç olarak A, bir şeyin bilgisine sahip olduğunu, bilginin kendisini ortaya çıkarmadan ispat etmiştir.

Burada belirtmek gerekir ki, sıfır bilgi ispatının hukuk ve ceza yargılamalarında, adli bilişimde, delillerin incelenmesinde ve ticari sırların gizliliğinin sağlanmasında kullanılabileceği önerisi yerinde olacaktır. Örneğin DNA analizlerinde, DNA eşleştirmesi yapılırken DNA profillerinin incelemeyi yapan görevlilere/bilirkişiye karşı dahi tamamen

açığa çıkarılmadan gerçekleştirilebilmesi sağlanabilecektir⁵²⁹. Bu tür bir uygulama CMK'nin “Alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır.” şeklindeki 78. maddesine ve “75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.” şeklindeki 80. maddesinin ortaya koyduğu gerekliliklerin sağlanmasına da yardımcı olacaktır. Bununla birlikte iddia ve savunmaların ispatı sağlanırken ticari sırlar gibi açığa çıkarılmaları oldukça sakıncalı olan bazı bilgilerin sıfır bilgi ispatı ile açığa çıkarılmadan doğruluğunun ispat edilebilmesi de mümkündür⁵³⁰.

Zcash adresleri “korumalı” ya da “açık” olabilir. Korumalı bir adresten korumalı başka bir adrese ZEC aktarılması⁵³¹, yukarıda bahsedilen sıfır bilgi ispatı yani zkSnark ile mümkün olacaktır. Bu tür bir işlemde, gerçekleştirilen işlem herkese açık blok zincirde onaylansa da⁵³², gönderenin ve alıcının adresi ile gönderim miktarı başka kimse tarafından görülemez. Bununla birlikte göndericinin korumalı bir adres olduğu durumlarda, üçüncü kişilerin yanında alıcı da gönderici adresini göremeyecektir. Bu sayede blok zincirdeki bu tür bir işlemin doğruluğu, işlem bilgisi açığa çıkarılmadan onaylanmaktadır.

Korumalı hesaptan korumalı hesaba yapılan gönderime “gizli (private) işlem”; korumalı hesaptan açık hesaba yapılan gönderim “korumayacak⁵³³ (deshielding) işlem”; açık hesaptan korumalı hesaba yapılan transfer “koruyacak⁵³⁴ (shielding) işlem”; her iki adres de açık adres ise yapılan transfer ise “açık (transparent/public) işlem” olarak isim verilir.

⁵²⁹ Fisch vd., “Physical Zero-Knowledge Proofs of Physical Properties”, 2014, s.2.

<https://www.iacr.org/archive/crypto2014/86160292/86160292.pdf> (Erişim: 07.07.2022)

⁵³⁰ Bamberger vd., “Verification Dilemmas In Law And The Promise Of Zero-Knowledge Proofs”, *Berkeley Technology Law Journal*, 2022/37 (1), s. 101. <https://ssrn.com/abstract=3781082> (Erişim: 07.07.2022)

⁵³¹ Bu tarz bir transfer örneği için:

<https://blockchair.com/zcash/transaction/35f6674a1691f21aff6a3819467dbba82aaebf061d50c6ac55f39fbae73b9a6> (Erişim: 27.05.2022)

⁵³² Zcash, How It Works, <https://z.cash/technology/> (Erişim: 27.05.2022)

⁵³³ “Korumayı kaldıran” anlamına gelebilse de, tek bir kelime olması ile transferin son halini ve işlevini temsil edeceği düşünülerek “korumayacak” şeklinde çevrilmiştir.

⁵³⁴ “Koruma oluşturan” anlamına gelebilse de, tek bir kelime olması ile transferin son halini ve işlevini temsil edeceği düşünülerek “koruyacak” şeklinde çevrilmiştir.

Gizlilik odaklı kripto paralara Verge (XVG), Secret (SCRT), Horizen (ZEN) ya da “Mimblewimble” teknolojisini kullanan BEAM ve GRIN örnek verilebilir.

Yukarıda detaylı şekilde ortaya konduğu üzere, gizlilik odaklı kripto paralar gönderici, alıcı ve gönderim miktarını üçüncü kişilerden ve hatta yeri geldiğinde alıcıdan bile saklar. Bu durum, terörizmin finansmanı eylemini gerçekleştirmek amacıyla bu tür kripto paraları oldukça işlevsel bir konuma getirmektedir. FATF de 2021 tarihli rehberinde gizlilik odaklı kripto paraları “anonimliği artırıcı kripto para birimi [anonymity-enhanced cryptocurrency (AEC)]” olarak adlandırmıştır⁵³⁵. Bu doğrultuda FATF, AML/CFT’lerin (kara para aklamanın ve terörizmin finansmanının önlenmesi ile ilgili düzenlemeler) sanal varlık ve sanal varlık hizmeti sağlayıcıları hakkında “finansal eyleme konu olan sanal varlığın türüne bakılmaksızın” uygulanacağını belirtmekte, gizlilik odaklı kripto paraların da bu kapsama alınacağını ayrıca bildirmektedir⁵³⁶.

Sonuç olarak gizlilik odaklı kripto paraların terörizmin finansmanında, finansman sağlama eylemini gerçekleştirenler için en işlevsel araç olduğu söylenebilir. Bu duruma birçok ulusal ve uluslararası çalışmalarda da yer verilmiştir. Europol’ün 2021 IOCTA raporunda da Dark Web kullanıcıları giderek Monero kullanmaya başladıkları⁵³⁷ belirtilmektedir. Bununla birlikte yapılan Monero işlemlerinin %25’inin yasaklanan faaliyetler çerçevesinde gerçekleştiği belirtilmektedir⁵³⁸.

3.3.5. İkinci Katman (Layer 2) Çözümleri ve Zincirler Arası Köprüler

İkinci katman çözümleri, çoğunlukla Ethereum ağı çerçevesinde karşılaşılan, zincir dışı (off-chain) ölçeklendirme çözümleridir⁵³⁹.

En çok kullanılan blok zincir ağı olan Ethereum, kullanımdaki bu artış nedeniyle bazı sorunlarla karşılaşmaktadır. Örneğin gas ücretleri, ağı kullanmayı engelleyecek derecede artabilmektedir. Bu doğrultuda ölçeklendirme çözümü olarak, Ethereum zinciri üzerinde bir değişiklik yapmayı gerektirmeyen ikinci katman çözümleri ile sıklıkla

⁵³⁵ FATF, 2021, s. 3.

⁵³⁶ FATF, 2021, s. 32.

⁵³⁷ Europol, 2021/a, s. 36.

⁵³⁸ European Parliament, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, 2018, s. 33.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (Erişim: 28.06.2022)

⁵³⁹ Ethereum, Scaling, <https://ethereum.org/en/developers/docs/scaling/> (Erişim: 28.05.2022)

karşılaşılmaktadır. İkinci katman çözümleri, yan zincirler (sidechain) gibi (Örn. Polygon) kendi konsensüs protokollerini çalıştırmazlar. İkinci katmanlar bu doğrultuda güvenliklerini direkt olarak Ethereum konsensüsü üzerinden sağlarlar. İkinci katman çözümleri, Ethereum ağını yoracak işlemlerin zincir dışı gerçekleştirilebilmesini sağlar.

İkinci katman çözümlerinin en çok kullanılanları “Rollup”lardır. Rollup’lar “Optimistic Rollup” ve “zk-Rollup (zero knowledge)”lardır. Rollup’lar kısaca Ethereum ağı dışarısında işlem gerçekleştirip, bu işlemlere ilişkin kanıtları (proof) Ethereum ağına yollarlar.

Optimistic Rollup’lar “fraud proof (sahtekarlık kanıtı)” modelini kullanırlar. Bu modelde Rollup üzerinde gerçekleşen işlemler kanıt olmaksızın, doğru oldukları kabul edilerek, işlem sonucu oluşan durumun tasdiki için Ethereum ağına yollanır⁵⁴⁰. Yani işlemler aksi kanıtlanmadıkça geçerli sayılır. Optimistic Rollup’lar üzerinde yapılan işlemler için bir hesaplama işlemi gerçekleşmediğinden, yapılan işlemlerin doğruluğunun sağlanması gerekmektedir. Bu nedenle yapılan işlemlerin “sahte” olması durumunda “fraud proof” işlemi yürütülür. Optimistic Rollup’lar EVM [Ethereum Virtual Machine (Ethereum Sanal Makinesi)] çalıştırabildiklerinden oldukça kullanışlıdır. Bu durum kısaca Ethereum üzerinde yapılacak her türlü işlemin, bu tür ikinci katman çözümleri üzerinde de gerçekleştirilebileceği anlamına gelmektedir. En bilinen Optimistic Rollup’lar Optimism⁵⁴¹ ve Arbitrum⁵⁴²’dur.

Zk-Rollup’lar ise “validty proof (geçerlilik kanıtı)” kullanırlar. Optimistic olanların aksine bu tür Rollup’larda yapılan işlemlerin hesaplama aşaması Rollup üzerinde gerçekleşir, ardından işlemlerin geçerlilikleri (validity proof) ana zincire yani Ethereum zincirine iletilir⁵⁴³. En çok bilinen Zk-Rollup’lar zkSync⁵⁴⁴, Aztec⁵⁴⁵ ve StarkNet⁵⁴⁶’tir.

Rollup’ların bu çalışma doğrultusunda taşıdığı önem, bir “arka sokak” işlevi görmesidir. Çünkü rollup’lar üzerinde gerçekleştirilen işlemler tek tek Ethereum ağı

⁵⁴⁰ Ethereum, Optimistic Rollups, <https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/> (27.05.2022)

⁵⁴¹ Optimism, <https://www.optimism.io> (Erişim: 02.06.2022)

⁵⁴² Arbitrum, <https://bridge.arbitrum.io> (Erişim: 02.06.2022)

⁵⁴³ Ethereum, Validty Proof, <https://ethereum.org/en/glossary/#validity-proof> (Erişim: 29.05.2022)

⁵⁴⁴ zkSync, <https://zksync.io> (Erişim: 02.06.2022)

⁵⁴⁵ Aztec Network, <https://aztec.network> (Erişim: 02.06.2022)

⁵⁴⁶ Starkware, StarkNet, <https://starkware.co/starknet/> (Erişim: 02.06.2022)

üzerinde görüntülenemezler. Rollup'lar bu sebep ile takibi zorlaştırabilirler. Bu doğrultuda yoğun bir gizlilik sağlayan bir Rollup olan Aztec ve bu ağ üzerinde çalışan “zk.money” incelenmelidir.

Aztec Network, sıfır bilgi kanıtını kullanan gizlilik odaklı bir Rollup'tır. Aztec'i diğer Rollup'lardan ayıran özelliği, iki defa sıfır bilgi kanıtı kullanmasıdır. Gerçekleştirilen işlemler ile ilgili ayrı ayrı kanıt oluşturulur; ardından bu kanıtlar bir grup halinde toplanarak tek bir sıfır bilgi kanıtı daha oluşturulur.

Zk.money, Aztec ağı üzerinde çalışan bir gizlilik uygulamasıdır. Kullanıcılar Ethereum adresleri ile imzalama işlemi gerçekleştirdikten sonra zk.money hesabı oluşturulur. Oluşturulan hesabın bir kullanıcı ismi de bulunur. Ardından oluşturulan hesaba, ETH gönderilir. Bu gönderim işlemine “Shield (koruma/kalkan)” adı verilir. Gönderilen ETH'ler ulaştığında “shielded (korunmalı)” hale geleceklerdir. Korunmalı ETH'ler “zkETH” olarak adlandırılır. zkETH, Aztec ağı üzerindeki korunmalı ETH olarak açıklanabilir. Herhangi bir Ethereum hesabının bu şekilde bir shield işlemi gerçekleştirmesinde alıcı adres Aztec Network sözleşme adresi olarak gözükmektedir. Yani alıcının, Aztec network üzerindeki hangi hesap olduğu ile ilgili hiçbir bilgiye ulaşamaz. Örneğin aşağıda Şekil 4.5. incelendiğinde, bir shield işleminde alıcı adres “Aztec: Private Rollup Bridge” olarak gözükmektedir. Aynı şekilde Ethereum ağına para çekişleri sırasında da göndericinin Aztec network üzerindeki hangi hesap olduğu konusunda, Ethereum ağı üzerinden bir bilgi elde edilemez⁵⁴⁷. Bununla birlikte çekim işlemlerinde Aztec network ağı kontrol edilirse bu tür bir bilgi elde edilebilecektir. Bu nedenle çekim için gizliliği sağlamak isteyen bir kişinin farklı bir Ethereum adresini kullanması gerekecektir⁵⁴⁸.

⁵⁴⁷ Zk.money, What information about my transaction will be shown on explorer like Etherscan?, <https://aztec-protocol.gitbook.io/zk-money/faq/faq-privacy#what-information-about-my-transaction-will-be-shown-on-explorer-like-etherscan> (Erişim: 30.05.2022)

⁵⁴⁸ Zk.money, Are withdrawals private?, <https://aztec-protocol.gitbook.io/zk-money/faq/faq-privacy#are-withdrawals-private> (Erişim: 30.05.2022)

Şekil 3. 5 Aztec ağına gerçekleştirilen bir yatırma işlemi.

Txn Hash	Method ⓘ	Block	Age	From	To	Value	Txn Fee
> 0xaecde2d560fc90ed43...	Deposit Pending...	14871332	55 secs ago	0xd7b89e12e17526132a...	IN Aztec: Private Rollup Bri...	0.313913 Ether	0.00109227

(Kaynak: Etherscan)

Korumalı hale alınmış (shielded) zkETH'ler, başka bir zk.money kullanıcıasına gönderilebilir. Bu tür bir işlem tamamen Aztec ağı üzerinde ve uçtan uca gerçekleşmekle birlikte tamamen gizlidir.

Yukarıda bahsedilen özellikleri sayesinde Aztec ağı, terörizmin finansmanı çerçevesinde fon sağlama faaliyetine oldukça elverişlidir. Ağın bahsedilen özellikleri nedeniyle doğru kullanıldığında aktarılan fonun takibi neredeyse imkânsız hale gelmektedir. Örneğin fon sağlamak isteyen bir kişi zk.money üzerinden hesap oluşturarak buraya kripto para aktarır. Fonun aktarılmak istendiği terör örgütü de zk.money üzerinden hesap oluşturur. Fon, terör örgütünün zk.money hesabına aktarılır. Ardından terör örgütü bu fonu istediği bir Ethereum adresine çeker. Bu tür bir işlemde fonun kimden geldiği yani finansmanı sağlayan kişi bilinmeyecektir. Ayrıca terör örgütünün hangi zk.money hesabını kontrol ettiği ve finansman gerçekleştiren diğer kullanıcılar da bilinmeyecektir. Bu nedenle bilinçli bir şekilde kullanıldığında Aztec ağının terörizmin finansmanı için oldukça kullanışlı bir araç olacağını söylemek mümkündür.

Başlık altında incelenecek bir diğer blok zincir aracı köprülerdir. Köprüler zincirler arası varlık aktarımını sağlarlar. Bu kapsamda aynı ya da benzer işlevi gören birden fazla köprü bulunmaktadır. En çok bilinen zincirler arası köprüler Wormhole, Multichain, Connex, Hop Protocol ve Orbiter'dir. Köprüler çoğunlukla Ethereum ile EVM çalıştırabilen diğer ağlar (Fantom, Smart Chain, Gnosis vb.) ya da ikinci katman çözümleri arasında fon transferleri ile için kullanılmaktadır. Köprüler bir hesap üzerindeki seçili ağda bulunan bir kripto paranın, başka bir ağa taşınmasını sağlar, yani taşınan ağdaki kripto paranın sahibi de taşıyan kişi olacaktır. Fakat köprü aracılığıyla kripto para taşıyan bir kişi isterse alıcı adresi kendi adresinden başka bir adres olarak seçebilir; bu tür bir durumda alıcı adrese taşınan kripto para, ağ üzerinde işlem incelendiğinde göndericiden değil, köprüden gelmiş olarak gözükecektir. Bu nedenle fon

transferinde üçüncü kişiler tarafından takibi engellemek isteyen bir kullanıcı, köprüleri kullanabilir.

3.3.6. Stabil Kripto Paralar

Stabil kripto paralar (stablecoins), çoğunlukla değer olarak bir itibari paraya denk, bu denkliğin çeşitli mekanizmalar sayesinde sürdürüldüğü kripto paralardır. Stabil kripto paralar, söz konusu nitelikleri ve bu nitelik doğrultusunda CBDC'lere rakip olmaları nedeniyle özellikle son dönemde ulusal ve uluslararası kuruluşların yakından takip ettiği bir kripto para türüdür⁵⁴⁹.

Stabil kripto paralar, fiyat dengesini koruma yöntemlerine göre genel olarak üçe ayrılır. Stabil kripto paralar itibari para destekli, kripto para destekli ya da algoritmik olabilirler. İlk iki tür stabil kripto parada, fiyat dengesini koruyabilmek için rezerv bulundurulur. Örneğin basit bir tabir ile itibari para destekli kripto paralarda, toplam kripto para miktarı kadar itibari para rezervi bulundurulur. Belirtmek gerekir ki stabil kripto paralar her zaman stabil olamamakta, kısmi dengesizlikler ya da nihai bozulmalar ile karşılaşılabilir. Stabil kripto paraların fiyat dengesini koruyan tek etken rezervler değildir; piyasa dinamikleri, arz-talep ve fiyat eşitliğinin sağlanacağına dair güven önemli etkenlerdir. Her ne kadar çoğu stabil kripto paranın kendine ait bir denge mekanizması bulunsada, bu denge mekanizmasına ilaveten, eşitliğin tekrar sağlanacağına olan güven ile serbest kripto para piyasasındaki alım satımlar da bu mekanizmaların yanında eşitliğin tekrar sağlanmasına etki etmektedir.

Stabil kripto paralardan en çok kullanılanı ve en büyük piyasa değerine sahip olanı, değeri 1 Amerikan dolarına denk olan “Tether (USDT)”dir. 28.05.2022 itibariyle

⁵⁴⁹ FATF, FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, 2020. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf> (Erişim: 28.05.2022); European Parliament, “Stablecoins”, 2021, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698803/EPRS_BRI\(2021\)698803_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698803/EPRS_BRI(2021)698803_EN.pdf) (Erişim: 28.05.2022); Melinek, Jacquelyn, “US Treasury Secretary Janet Yellen pushes for stablecoin regulation by end of year”, Techcrunch, 10.05.2022, <https://techcrunch.com/2022/05/10/us-treasury-secretary-janet-yellen-pushes-for-stablecoin-regulation-by-end-of-year/> (Erişim: 28.05.2022); U.S. Securities And Exchange Commission, President’s Working Group Report on Stablecoins, 2021, <https://www.sec.gov/news/statement/gensler-statement-presidents-working-group-report-stablecoins-110121#:~:text=Stablecoins%20are%20crypto%20tokens%20pegged,in%20the%20last%20%20month s.&text=As%20the%20report%20notes%2C%20“stablecoins.commodities%20and%20For%20derivatives.> (Erişim: 28.05.2022)

dolaşımda 72.537.249.554 adet USDT bulunmaktadır⁵⁵⁰. Tether şirketi tarafından dolaşımdaki USDT'nin tamamının karşılığının olduğu belirtilse de, rezerv tamamen itibari paralardan oluşmamaktadır. Rezervin bir kısmı nakit yerine geçen finansal enstrümanlar vb.'den oluşmaktadır. 31 Mart 2022 tarihinde yayınlanan rapora göre her ne kadar Tether rezervlerinin tamamı nakit paradan oluşmasa da, toplam rezerv değerinin dolaşımdaki USDT'lerin tamamını karşıladığı görülmektedir⁵⁵¹. Bununla birlikte tether aracılığıyla nakit çıkışı sağlamak için minimum 100.000 Amerikan doları limit bulunmaktadır.

Piyasa değeri en yüksek ikinci stabil kripto para ise Circle tarafından ihraç edilen "USDC"dir. 28.05.2022 itibariyle dolaşımda 53.560.000.000 adet USDC bulunmaktadır. Circle tarafından USDC'lerin tamamının Amerikan doları ve kısa süreli hazine tahvili olarak bulundurulduğu belirtilmektedir.

Türk lirasına denk olan stabil kripto paralar da bulunmaktadır. Buna tamamı Türk lirası rezervi ile teminatlandırılan "TRYb" örnek gösterilebilir. TRYb, BiLira tarafından ihraç edilmiş olup, bağımsız denetçi raporuna göre⁵⁵² tamamen Türk lirası ile teminatlandırılmıştır. Rapora göre yaratılan ve satışı beklenen toplam 109.300.281 adet TRYb varken, rezerv hesaplarında tutulan Türk lirası ise 113.644.034'tür. Bununla birlikte Neutrino tarafından ihraç edilen, WAVES ağı üzerinde, Türk lirasına eşit "TRYN" adında bir stabil kripto para da bulunmaktadır. Fakat bu kripto para "DeFo" adı verilen, ağ üzerindeki diğer stabil kripto paraların akıllı kontrat üzerinden değiştirilmesi sistemine dayanmakta, rezerv sistemine dayanmamaktadır. Neutrino tarafından sunulan temel algoritmik stabil kripto olan USDN, aşağıda detaylı bir şekilde incelenecektir. TRYN'nin ve WAVES ağı üzerindeki diğer stabil kripto paraların bu bağlamda USDN'ye bağımlı bir görünüm teşkil ettikleri söylenebilir.

Bir kripto para ile teminatlandırılan stabil kripto paralara verilecek örnek "DAI" olacaktır. DAI, başka bir kripto para olan Ethereum ile teminatlandırılmıştır. DAI, "MakerDAO" adı verilen bir "Merkeziyetsiz Otonom Kuruluş [Decentralized

⁵⁵⁰ CoinMarketCap, "Tether", <https://coinmarketcap.com/currencies/tether/> (Erişim: 28.05.2022)

⁵⁵¹ MHA Cayman, Independent Accountant's Report, 2022.

https://assets.ctfassets.net/vyse88cgwfb/1np5dpcwuHrWJ4AgUgI3Vn/e0dac722de3cea07766e05c52773748b/Tether_Assurance_Consolidated_Reserves_Report_2022-03-31_3.pdf (Erişim:28.05.2022)

⁵⁵² RSM, Bağımsız Denetçi Raporu, 15.04.2022, https://uploads-ssl.webflow.com/5fb683a258cbdf70262c0b77/6261446ff9e7a60b887c67dc_BiLira%20Rapor%2015042022%20TR%20RSM%20İmzalı.pdf (Erişim: 29.05.2022)

Autonomous Organization (DAO)] tarafından oluşturulmuştur. DAO'lar bir topluluk tarafından yönetilen, merkezi olmayan oluşumlardır. DAO'ların yönetimi parlamentolara benzer; DAO'nun temel aldığı kripto paraya göre, o kripto para miktarının belli bir limitini elinde bulunduran kişi ya da gruplar değişiklikler için teklif sunar; teklif edilen değişiklikler kripto parayı elinde bulunduran kişi ya da bu kişiler tarafından seçilen vekiller aracılığıyla oylanır; kabul edilir ya da reddedilir. DAO oylamaları “Snapshot⁵⁵³” gibi platformlar aracılığıyla gerçekleştirilebilir. Bu şekilde merkeziyetsiz bir yönetim süreci izlenir.

Stabil kripto paraların en kırılgan türü algoritmik stabil kripto paralardır. Yakın zamanda Amerikan dolarına denk olması amacıyla üretilen birçok algoritmik stabil kripto paranın Amerikan dolarına denkliğinin bozulduğu görülmektedir. Bu örneklerden en büyüğü Terra USD (UST)'dir. 9 Mayıs 2022 tarihinde UST'nin Amerikan dolarına denkliği (%99'dan fazla bir düşüş) bozulmuş ve başlayan bu bozulma sonucu UST'de 18 Milyar, Luna'da 28 Milyar olmak üzere toplamda yaklaşık 46 Milyar Amerikan doları piyasa değer kaybı yaşanmış; gerek bireysel gerek de kurumsal yatırımcılar büyük bir zarara uğramıştır. UST örneğinde, dolara denkliği sağlayan algoritma kısaca, yakılan 1 UST karşılığında her zaman 1 Amerikan doları değerinde Luna elde edilebilecek şekilde çalışmaktaydı. Kaba bir örnek ile; UST'nin dengesinin bozulduğu, değerinin piyasada 0,98 Amerikan dolarına düştüğü varsayımında bir kişi, 0,98 dolar değerinde UST verir, bu UST yakılarak dolaşımdan çıkarılır; karşılığında 1 Amerikan doları değerinde Luna alınır, bu Luna satılarak yaklaşık %2'lik bir kar elde edilmiş olunur. Bu durum sürekli tekrarlanarak ve dolaşımdaki UST miktarı azaltılarak arz-talep dengesi korunurdu. Fakat UST örneğinde sistemin yeterince sağlam kurulmamış olması, fiyat dengesinin hiçbir zaman düzelemeyecek kadar bozulmasına neden olmuştur; algoritma modeli doğrultusunda sürekli UST yakılmaya çalışılmış, elde edilen 1 Amerikan doları değerindeki Luna satılmış; bu yoğun satış baskısına sürekli üretilen yeni Luna'lar da dahil olunca kısır bir döngü oluşmuş ve sistem çökmüştür.

⁵⁵³ <https://snapshot.org/#/> (Erişim:28.05.2022)

Şekil 3. 6 UST'nin 9 Mayıs 2022'de başlayan denklik bozulmasının mum grafiği. 1 Amerikan doları yerine 0,032 Amerikan doları üzerinden işlem görmektedir. (Coinbase, UST/USD paritesi)



(Kaynak: Tradingview.)

Algoritmik stabil kripto paralara verilebilecek bir diğer örnek, WAVES ağına dayanan “Neutrino USD (USDN)”dir⁵⁵⁴. USDN’de karşılaşılan algoritma modeli iki katmanlıdır. Yatırımcılar “Neutrino System Base Token (NSBT)” adında, yönetim modelinde de kullanılmak üzere bir kripto para bulundurur. NSBT’ler kitlenerek “gNSBT” adında bir yönetim parası elde edilir. USDN’in fiyat dengesi bozulduğunda, örneğin USDN değer kaybettiğinde yatırımcılar, WAVES üzerindeki akıllı kontratlar üzerinden ellerinde bulunan gNSBT miktarına oranla ve günlük bir limit ile 1 USDN’yi 1 Amerikan dolarına eşit WAVES ile değiştirebilir. Bu değişim tekrarlandıkça dolaşımdaki USDN arzı azalacak ve değer tekrar eski haline dönecektir. Fakat USDN de diğer algoritmik stabil kripto paralar gibi zaman zaman denkliliğini koruyamamaktadır.

⁵⁵⁴ <https://neutrino.at> (Erişim: 28.05.2022)

Şekil 3. 7 USDN değeri üzerindeki dalgalanmaların mum grafiği. (Kucoin, USDN/USDT paritesi)



(Kaynak: Tradingview.)

Stabil kripto paralar, bu bölümün girişinde geniş bir şekilde aktarılan ve “MiCA” olarak adlandırılan, “Kripto Varlık Piyasasına İlişkin Tüzük Tasarısı ”nda da ele alınmıştır.

Tasarı taslağında varlık kaynaklı token ve e-para token’ın “stabil kripto para (stablecoin)”leri karşılayacak şekilde kullanıldığı belirtilmiştir⁵⁵⁵. Bununla birlikte tasarıda algoritmik stabil kripto paraların varlık kaynaklı token olarak değerlendirilemeyeceği kabul edilmiştir⁵⁵⁶. Tasarı taslağının e-para token ile ilgili maddesinde, Parlamento token’ın vadettiği fiyatı koruyabilmesi için bir portföy bulundurulması gerekliliğini belirtmiştir. Bu durum doğrultusunda USDT ve USDC gibi mevcut stabil kripto paraların bulundurduğu rezervler, Parlamento tanımı ile uyumluluk göstermektedir.

3.3.7. İlk Para Arzı [Initial Coin Offering (ICO)] ve Türevleri

İlk para arzı yani ICO’lar, temel olarak çeşitli alanlarda blok zincir teknolojisini kullanan projelerin finansmanlarını, yatırımcılardan kripto para toplayarak sağladığı bir

⁵⁵⁵ Council of the European Union, 2020, s. 10.

⁵⁵⁶ Council of the European Union, 2020, s. 21.

kitle fonlaması yöntemidir⁵⁵⁷. ICO ve türevlerinin blok zincir üzerinde gerçekleşen bir fon toplama uygulamaları olması, terörizmin finansmanı doğrultusunda fon toplanmasına sebebiyet vereceklerinden incelenmeleri gereklidir. Avrupa Parlamentosu da, ICO'ların terörizmin finansmanı doğrultusunda kullanılması riskinin göz önünde bulundurulması gerektiğini belirtmektedir⁵⁵⁸. Hollanda Finansal Piyasa Otoritesi AFM de, ICO'ları terörizmin finansmanı amacıyla fon toplama faaliyeti çerçevesinde çekici bir araç olduğunu, gerekli düzenlemelerin ivedi bir şekilde yapılması gerektiğini belirtmiştir⁵⁵⁹. Türkiye'de Sermaye Piyasası Kurulu ise, Kurul Karar Organı'nın 27/09/2018 tarih ve 47/1102 sayılı kararı uyarınca yapılan duyuru doğrultusunda, "ICO'ların birçoğunun yapısı itibariyle düzenleyici kurumların yetki ve görev alanı dışında kalmakta olup, herhangi bir düzenleme ve gözetime tabi olmadıklarını" ve "çok yüksek riskli ve spekülatif yatırım" oldukları konusunda uyarıda bulunmuştur⁵⁶⁰.

Kitle fonlaması genel olarak, girişimcilerin girişimlerine ya da projelerine finansman sağlamak amacıyla kitleler üzerinden çeşitli yöntemler ve miktarlarda fon toplamasıdır. Kitle fonlamasının temelde iki amacının olduğu söylenebilir. Bunlardan ilki girişimcilerin finansman sağlamak istedikleri girişim veya projeyi kitlelere tanıtmaya fırsatı yakalamasıdır. Bir diğeri de bu girişim ya da proje için yatırımcılar vasıtasıyla finansman sağlanmasıdır⁵⁶¹. Kitle fonlaması da küreselleşme ile meydana gelen finansal serbestleşmenin, teknolojik gelişmeler sonucu kolaylaşan haberleşme ve iletişimin, ülke sınırlarını aşan finansal faaliyetlerin bir sonucudur. 2007-08 finansal krizinden bu yana, sermayelere alternatif yollardan ulaşma fikri kitle fonlamasının ortaya çıkmasında oldukça etkili olmuştur.

Kitle fonlamasının kökenleri, Nobel ödüllü Muhammed Yunus'un öncülüğünü yaptığı mikrofinans hareketi ve mikrokrediye dayanmaktadır. Mikrofinans hareketi temel olarak, çeşitli sebeplerle klasik bankacılık faaliyetlerine erişemeyen düşük gelirli

⁵⁵⁷ Fisch, Christian, "Initial coin offerings (ICOs) to finance new ventures", *Journal of Business Venturing*, 2019/34 (1), s. 3. <https://doi.org/10.1016/j.jbusvent.2018.09.007> (Erişim: 08.01.2020)

⁵⁵⁸ European Parliament, 2018, s. 45.

⁵⁵⁹ AFM, "Initial Coin Offerings (ICO's): serious risks", <https://www.iosco.org/library/ico-statements/Netherlands%20-%20AFM%20-%20Initial%20Coin%20Offerings%20Serious%20Risks.pdf> (Erişim: 29.05.2022)

⁵⁶⁰ Sermaye Piyasası Kurulu, Sermaye Piyasası Kurulu Bülteni, 2018/42, s.4. <https://www.spk.gov.tr/Bulten/Goster?year=2018&no=42> (Erişim: 29.05.2022)

⁵⁶¹ Schwartz, Andrew A., "The Gatekeepers of Crowdfunding", *Washington and Lee Law Review*, 2018/75 (2), s.885. <https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2297&context=articles> (Erişim: 23.11.2019)

bireylere veya küçük işletmelere mikrokredi ve diğer bankacılık hizmetlerini sağlayan bir finansal kalkınma modelidir⁵⁶². Mikrofinans hareketi geniş anlamda kitle fonlamasının temelini oluştursa da, kitle fonlamasının ortaya çıkışına zemin hazırlayan en önemli kavram ilk olarak Jeff Howe'un 2006 yılında Wired dergisinde yayınlamış yazısında ortaya çıkan "kitle-kaynak (crowdsourcing)"tır⁵⁶³. Kitle-kaynak kısaca bir işin internet ortamı aracılığıyla kitleler üzerinden çözülmesidir. Kitle-kaynak yöntemi ile açık çağrıda bulunularak kitleler üzerinden fikir, geribildirim ve çözüm yolları elde edilerek kurumsal faaliyetlerin sürdürülmesi amaçlanır⁵⁶⁴. Jeff Howe yazısında şirketlerin dış kaynaklardan yararlanma (outsourcing) yoluyla diğer ülkelerdeki ucuz işgücünün peşinde olmasına artık gerek olmadığını, dünyanın herhangi bir yerindeki internet kullanıcılarıyla da belirli işlerin çözülebileceğini vurgulamaktadır.⁵⁶⁵ Kitle-kaynak yöntemine verilebilecek en iyi örnek, kullanıcılarının içerikleri oluşturduğu ve düzenlediği bir ansiklopedi olan Wikipedia'dır.

Kitle fonlaması ise bir terim olarak ilk kez 2006 yılında Michael Sullivan adında bir girişimci tarafından kullanılmıştır⁵⁶⁶. Literatürde birçok kitle fonlaması sınıflandırması yapılmış bulunmakla beraber, temelde dört çeşit kitle fonlaması ile karşılaşmaktadır. Bunlar bağış temelli, ödül temelli, borç temelli ve hisse temelli kitle fonlamasıdır⁵⁶⁷.

Türk hukukunda kitle fonlaması terimi oldukça yenidir. Türkiye'de kitle fonlaması, 7061 sayılı torba Kanun'un 107-111. maddeleri ile 6362 sayılı Sermaye Piyasası Kanunu⁵⁶⁸'nda yapılan değişiklikler sonucunda kitle fonlaması hukukumuzda girmiş bulunmaktadır. 3 Ekim 2019 tarihinde yayınlanan "Paya Dayalı Kitle Fonlaması

⁵⁶² Sengupta, Rajdeep, Craig P. Aubuchon, "The Microfinance Revolution: An Overview", Federal Reserve Bank of St. Louis Review, January/February 2008, 90(1), s. 9-10.
https://www.researchgate.net/profile/Craig-Aubuchon/publication/5047480_The_Microfinance_Revolution_An_Overview/links/55195faf0cf273292e716113/The-Microfinance-Revolution-An-Overview.pdf (Erişim: 02.06.2022)

⁵⁶³ Howe, Jeff, "The Rise of Crowdsourcing", WIRED, Haziran 2016.
<https://www.wired.com/2006/06/crowds/> (Erişim: 07.12.2019)

⁵⁶⁴ Belleflamme vd., "Crowdfunding: Tapping the right crowd", Journal of Business Venturing, 2014/29 (5), s. 588. <https://www.sciencedirect.com/science/article/abs/pii/S0883902613000694> (Erişim tarihi: 07.05.2022)

⁵⁶⁵ Howe, 2006.

⁵⁶⁶ Burkett, 2011, s. 70.

⁵⁶⁷ Atsan, Nuray, Eda Oruç Erdoğan, "Girişimciler İçin Alternatif Bir Finansman Yöntemi: Kitlesele Fonlama (Crowdfunding)", *Eskişehir Osmangazi Üniversitesi İİBF Dergisi*, 2015/10 (1), s. 302.
<https://dergipark.org.tr/tr/download/issue-full-file/27324> (Erişim: 12.12.2019)

⁵⁶⁸ R.G., T: 30/12/2012, S: 28513.

Tebliğ⁵⁶⁹ de kitle fonlaması hakkındaki bir diğer düzenlemedir. Bununla birlikte Türk Ticaret Kanunu'nun 552. Maddesi uyarınca "*Sermaye Piyasası Kanunu hükümleri saklı kalmak kaydıyla, bir şirket kurmak veya şirketin sermayesini artırmak amacıyla yahut vaadiyle halka her türlü yoldan çağrıda bulunularak para toplanması yasaktır.*" denilmektedir. Burada kanun koyucu Sermaye Piyasası Kanunu hükümlerini saklı bıraktığından, bu hüküm kitle fonlamasına engel değildir.

Kitle fonlaması'nın Türk mevzuatındaki tanımı Sermaye Piyasası Kanunu'nda yapılmıştır. Kanun'un 3. maddesinin 1. fıkrasının (z) bendine göre kitle fonlaması, "*Bir projenin veya girişim şirketinin ihtiyaç duyduğu fonu sağlamak amacıyla Kurul tarafından belirlenen esaslar dâhilinde Kanunun yatırımcı tazminine ilişkin hükümlerine tabi olmaksızın kitle fonlama platformları aracılığıyla halktan para toplanması*" olarak tanımlanmıştır. Bununla birlikte kitle fonlaması platformları, Kanun'un 35/A maddesinin 1. fıkrasında "*Kitle fonlama platformları, kitle fonlamasına aracılık eden ve elektronik ortamda hizmet veren kuruluşlardır.*" şeklinde tanımlanmıştır.

Kanun'un 4. Maddesinin 1. Fıkrası uyarınca diğer kanunların yardım ve bağış toplanmasına ilişkin hükümleri saklı kalmak kaydıyla kitle fonlaması suretiyle halktan para toplanması, Sermaye Piyasası Kurulu tarafından faaliyet izni verilen platformlar aracılığıyla gerçekleştirilir. Bununla birlikte Avrupa ülkelerindeki düzenlemelere paralel bir şekilde kitle fonlaması platformları, izahname ya da ihraç belgesi hazırlama yükümlüğüne ilişkin hükümlerine tabi değildir.

Kanun'un 35/A maddesinin 2. Fıkrasına göre kitle fonlaması platformlarının kurulabilmesi ve faaliyet göstermesi Sermaye Piyasası Kurulu'nun iznine tabidir. Fıkroda "*Kitle fonlaması platformlarının kuruluşları, ortakları, pay devirleri, çalışanlarına, her bir fon sağlayıcısı tarafından yatırılacak veya proje sahipleri ile girişim şirketleri tarafından toplanabilecek paranın azami limiti ve faaliyetleri sırasında uymaları gereken diğer ilke ve esaslar ile toplanan fonların ilan edilen amacına uygun olarak kullanıldığının kontrolü ve denetimine ilişkin esaslar Kurul tarafından belirleneceği*" belirtilmektedir. Yine hukuka aykırı işlem ve faaliyette bulunduğu tespit edilen platformlar hakkında Kanun'un 92. maddesi uyarınca tedbirlerin alınmasını isteme, hukuka aykırılık hakkında

⁵⁶⁹ R.G., T: 3/10/2019, S: 30907.

tespit davası açma ve hukuka aykırı işlemde bulunanların imza yetkisini kaldırma ve görevden alma ile yerine yenilerini atama yetkisi bulunmaktadır.

Kanun'un 99. Maddesinin 1. fıkrası uyarınca Kuruldan izin almaksızın halktan para toplayan kitle fonlaması platformlarının internet siteleri, Kurulun başvurusu üzerine Bilgi Teknolojileri ve İletişim Kurumu tarafından engellenir.

Kanun'un 16. Maddesinin 3. Fıkrasına göre, pay sahibi sayısı beş yüzü aşan anonim ortaklıkların payları halka arz olunmuş sayılır. Fakat burada kanun kitle fonlaması platformlarını bunun dışında bırakmıştır.

Türk hukukundaki kitle fonlaması düzenlemeleri bu şekilde olsa da, ICO ve türevleri hakkında henüz bir düzenleme yapılmamış bulunmaktadır. Bu nedenle olası bir uyumsuzlukta yaptırımların nasıl olacağı belli değildir. ICO'ların özellik gösteren bir kitle fonlaması olması nedeniyle düzenlenmesi gerekmektedir.

ICO'lar temel olarak çeşitli alanlarda blokzincir teknolojisini kullanan projelerin finansmanlarını, yatırımcılardan kripto para toplayarak sağladığı bir kitle fonlaması yöntemidir⁵⁷⁰. Gerçekleştirilmiş ilk ICO, 2013 yılında Bitcoin ağını kullanan bir blokzincir projesi olan ve yatırımcıların Bitcoin vasıtasıyla katılım sağladıkları Mastercoin'dir⁵⁷¹. Bununla birlikte bir ICO'da toplanan en büyük fon miktarı, 4 milyar dolar ile 2017 yılında düzenlenen Eos ICO'sudur⁵⁷². ICO'lara bu denli talebin olması ve kitle fonlaması yöntemleri arasında en çok fonun ICO ile toplanmasının en önemli sebeplerinden biri yatırım getirilerinin [Return of Investment (ROI)] çok yüksek olmasından dolayıdır. Örneğin 2013 yılında düzenlenen Nxt ICO'sunun, Nxt değerinin tarihi zirvesini gördüğü 24 Aralık 2017'de getirisi yaklaşık %37.000.000 kaddır⁵⁷³. Bunun yanı sıra gerçekleştirilmiş en önemli ICO hiç kuşkusuz 2014 yılında yapılan Ethereum ICO'su olmuştur⁵⁷⁴. Bununla birlikte diğer ICO örneklerine bakıldığında ICO'ların genel olarak Ethereum ağı üzerinde gerçekleştiği söylenebilir.

Ethereum altyapısı kullanılarak gerçekleştirilen ICO'lar temel birkaç aşamadan oluşur. Proje sahibi girişimciler Ethereum platformu dahilinde bir cüzdan adresi oluştururlar. Bu cüzdan adresinde yine Ethereum tabanlı fakat projeye özgü "token"lar

⁵⁷⁰ Fisch, 2019, s. 3.

⁵⁷¹ Wikipedia, "Initial Coin Offering", https://en.wikipedia.org/wiki/Initial_coin_offering. (Erişim: 02.06.2022)

⁵⁷² Icobench, "EOS", <https://icobench.com/ico/eos> (Erişim: 02.06.2022)

⁵⁷³ Coinmarketcap, "Nxt", <https://coinmarketcap.com/tr/currencies/nxt/> (Erişim: 02.06.2022)

⁵⁷⁴ Icodrops, "Ethereum", <https://icodrops.com/ethereum/> (Erişim: 02.06.2022)

oluşturulur. Bu token'lar bir bakıma hisse işlevi görürler. Ardından akıllı sözleşme oluşturulur ve bu sözleşme adresi yatırımcılar ile paylaşılır. Yatırımcılar akıllı sözleşme adresine yatırım yapmak istedikleri miktarda Ethereum aktarırlar, başka hiçbir işleme gerek kalmaksızın yatırımcıların Ethereum aktardıkları adrese, gönderdikleri Ethereum ile orantılı olarak, otomatik bir şekilde proje için oluşturulan tokenlar gönderilir⁵⁷⁵.

ICO'lar, halka arz yöntemine benzer bir şekilde, hisse dağıtımını gibi bir token dağıtımını ihtiva etse de, projenin tokenlarını elinde bulunduranların hisseleri elinde bulunduranların sahip olduğu hiçbir hakka sahip olmaması ve girişimcilerin, tokenları elinde bulunduranlara karşı da halka arz yöntemindeki anlamıyla sorumluluklarının bulunmaması en temel farklılıklardandır.

“Initial exchange offering” anlamına gelen IEO'lar, ICO'lara pek çok bakımdan benzese de IEO'larda fonlama süreci kripto para borsaları tarafından yürütülmektedir. IEO'ya katılmak isteyen bir yatırımcının fonlamanın düzenlendiği borsada hesap açması, “Know Your Customer (KYC)” ve “Anti Money Laundering (AML)”⁵⁷⁶ prosedürlerini yerine getirdikten sonra belirlenen tarihte borsa hesabına para aktararak fonlamaya katılması yeterlidir.

IEO'ların ilk örnekleri 2017 yılının sonunda görülse de⁵⁷⁷, özellikle piyasa döngüsü içerisinde ICO'larda umduğunu bulamayan yatırımcıların da ilgisiyle beraber IEO'lar, 2019 yılının başında “Binance” borsasında düzenlenen “BitTorrent” ile büyük bir popüleriteye ulaştı. Yine 2019 yılında “Bitfinex” borsasında düzenlenen “LEO” token arzında 1 milyar doların üstünde fon toplanmıştır⁵⁷⁸.

IEO'ların ICO'lara oranla girişimcilerine sağladıkları en önemli avantaj, katılımcıların KYC ve AML prosedürlerini yerine getirmesi ve borsaların çoğunlukla hukuka uygun bir fonlama süreci gerçekleştirmesi nedeniyle ilerleyen zamanlarda hukuki problemler ile karşılaşma ihtimallerinin düşük olmasıdır.

⁵⁷⁵ Grincalaitis, Merunas, “Your Final Guide About Creating Simple and Advanced ICO Smart Contracts”, Medium, 12.08.2018. <https://medium.com/ethereum-developers/your-final-guide-about-creating-simple-and-advanced-ico-smart-contracts-50a7d363417b> (Erişim: 02.06.2022)

⁵⁷⁶ “Know Your Customer” ve “Anti Money Laundering” açılımındaki bu prosedürlerde yatırımcılar, çeşitli kimlik doğrulama işlemlerinden geçerler. Bu sayede kara para aklanmasının önüne geçilmeye çalışılmaktadır. Ülkemizde de önde gelen kriptopara borsaları 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun uyarınca bu politikayı izlemektedirler.

⁵⁷⁷ Binance, “Binance Launchpad”, <https://launchpad.binance.com/> (Erişim: 02.06.2022)

⁵⁷⁸ Icobench, “IEO”, <https://icobench.com/ieo> (Erişim: 02.06.2020)

Son olarak belirtmek gerekir ki, ICO'ların IEO dışında farklı görünimleri de mevcuttur. Örneğin fonlamanın merkeziyetsiz bir borsa üzerinde gerçekleştirildiği durumlarda IDO (Initial Dex Offering) ya da bir oyun projesi hakkında gerçekleştirildiği durumlarda IGO (Initial Game Offering) gibi değişik adlandırılmalarla da karşılaşılabilir.

3.3.8. Kripto Para Borsaları (CEX/DEX)

Kripto para borsaları, kripto paraların ticaretinin yapıldığı platformlardır. Merkezi olan kripto para borsaları CEX, merkeziyetsiz olan kripto para borsaları DEX olarak adlandırılır.

Merkezi kripto para borsaları olan CEX'ler, özel bir şirket tarafından yönetilen, alım-satımlar ve varlık transferleri kapsamında sorumluk taşıyan kripto para borsalarıdır. Kullanıcılar CEX'lere e-posta adresleri ve diğer bazı web hesapları ile üye olarak alım satım ve kripto para transferi gerçekleştirirler. CEX'ler çoğunlukla belirli bir ülkeye kayıtlı olarak faaliyet gösterdiklerinden, ulusal ve uluslararası hukuki düzenlemeler doğrultusunda kullanıcılardan bu platformlarda işlem yapmaları için KYC/AML prosedürlerini tamamlamalarını istemektedirler. Kullanıcılar bu prosedürler çerçevesinde gerekli bilgileri sağlamadıkları sürece alım satım, kripto para ya da itibari para aktarımı ve çekimi gibi işlemleri gerçekleştiremezler. Bununla birlikte bu tür prosedürleri zorunlu kılmayan CEX'ler de mevcuttur. CEX'ler üzerinde hesap oluşturan kullanıcıların kripto para adresleri kendileri tarafından kullanılmakta ise de; bu adreslerin sahipliği, adreslerin gizli anahtarlarını elinde bulunduran borsalardır. Bu nedenle CEX'lerin siber saldırıya uğramaları ya da başka sebepler dolayısıyla geçici süre ya da tamamen hizmet verememeleri, kullanıcıların CEX'ler üzerinde buldukları kripto paralara erişemeyecekleri anlamına gelecektir. Bu doğrultuda örneğin 2014 yılında saldırı sonucu kapanan Mt. GOX ve 2019 yılında saldırı sonucu kapanan Cryptopia adlı borsalarda kripto para bulunduran kullanıcılar kripto paralarına hala erişememişlerdir. En çok kullanılan CEX'lere örnek olarak Binance, Coinbase, KuCoin, Kraken gibi kripto para borsaları gösterilebilir. Paribu, BTCTurk ve Binance TR gibi borsalar da Türkiye menşeli CEX'lerdir.

DEX'ler ise merkeziyetsiz kripto para alım satım platformlarıdır. Kullanıcılar kendilerine ait kripto para cüzdanlarını DEX'lere bağlayarak alım satım gerçekleştirmektedirler. Bu nedenle CEX'lerin aksine DEX'lere erişilememesi durumu kullanıcıların kripto paralarına erişememesi sonucunu doğurmaz, çünkü kripto para cüzdanlarının sahipliği CEX'lerin aksine DEX'lerde tamamen kullanıcılar aittir. Kullanıcılar şahsi kripto para cüzdanlarını istedikleri zaman DEX'lere bağlayıp, bağlantısını kesebilirler.

Terörizmin finansmanında, çalışmanın bu bölümünde de verilen örneklerde de görüldüğü üzere merkezi kripto para borsalarının kullanılabilirdiği bilinmektedir. Fakat terörizmin finansmanında merkezi kripto para borsalarının kullanılması; cüzdanın asıl sahibinin borsa olması ve cüzdanı kullanan kullanıcının borsa kapsamında gerçekleştirdiği bütün bilgilere erişilebilmesi nedeniyle terörizmin finansmanının önlenmesi kapsamında kolaylık sağlamaktadır. Bununla birlikte terörizmin finansmanı amacıyla toplanan fonların nakit para olarak çekilebilmesi için nakit para kapısı olan kripto para borsalarının kullanılabilirdiği de, örneklerden görüldüğü üzere, bilinmektedir. Böyle durumlarda finansmanın tespiti kolay olacaktır. Sonuç olarak regülasyonlara uyum sağlayarak faaliyet gösteren CEX'ler üzerinde gerçekleşen terörizmin finansmanı ile ilişkili işlemlerin tespiti ve önlenmesi, zincir üzerinde gerçekleşen diğer işlemlere göre daha kolay olacaktır.

Bununla birlikte CEX üzerinde gerçekleşse de bazı yöntemler ile para aktarımının bir derece gizlenmesi mümkündür. Örneğin emir defteri ince olan paritelerde fon aktarımını yapmak isteyen, defterdeki alış emirlerinin toplamının oldukça üstünde bir miktarda satış gerçekleştirmesi; fonu alacak kişinin de ilgili kripto paranın piyasadaki satış fiyatının oldukça düşük bir fiyata alım emri koyması sonucu fon aktarımı gerçekleşebilir. Bu durum şekil üzerinden açıklanabilir⁵⁷⁹.

⁵⁷⁹ Verilen örnekler durumun anlaşılması için verilmiş olmakla birlikte, örnekler için kullanılan pariteleri bulunduran borsaların söz konusu faaliyetleri gerçekleştirmek için kullanıldığı anlaşılmamalıdır. Emir defteri sığ olan başka herhangi bir parite ve borsada da söz konusu teknikler gerçekleştirilebilir.

Şekil 3. 8 Bir DEX üzerinde sığ bir emir defterine sahip bir parite. (DEXE/USDT)



Fiyat(USDT)	Miktar(DEXE)	Toplam(D...)
3.133		≈ 3.12 USD
3.1	448.0458	448.0458
3.0	1,486.7219	1,934.7677
2.9	176.9779	2,111.7456
2.8	115.8321	2,227.5777
2.7	254.0590	2,481.6367
2.6	254.0590	2,735.6957
2.5	7.0590	2,742.7547
2.4	2.0618	2,744.8165
2.0	0.9990	2,745.8155
1.5	7.0000	2,752.8155
1.0	39.9550	2,792.7705
0.6	1.4900	2,794.2605
0.5	23.0000	2,817.2605
0.3	1.0096	2,818.2701
0.1	204.0000	3,022.2701
0.0	10,960.3443	13,982.6144

(Kaynak: KuCoin.)

Yukarıda Şekil 4.8.'de bir CEX üzerinde işlem gören DEXE adlı bir kripto paranın DEXE/USDT paritesi görülmektedir. İlgili kripto paranın piyasadaki değeri 3,1 USDT⁵⁸⁰'dir. Şekilde belirtilen emir defterinin alım emirleri incelendiğinde, 3,1 USDT'den 0,1 USDT'ye kadar toplamda 3.022 DEXE alım emri verilmiştir. Örneğin terör eylemini ya da örgütünü finanse etmek isteyen 1 numaralı kullanıcı ve bu fonu teslim almak isteyen 2 numaralı kullanıcı olduğunu varsayalım. Bu kullanıcılar bu işlemi emir defteri oldukça sığ olan bu paritede gerçekleştirme kararı vermiş olsunlar. 1 numaralı kullanıcının elinde 60.000 USDT değerinde yaklaşık 20.000 tane DEXE bulunmaktadır. 2 numaralı kullanıcı 0,1 USDT'ye 17.000 adet DEXE alım emri girer, bu emri girmesi için elinde 1.700 USDT olması yeterlidir. Ardından 1 numaralı kullanıcı elinde bulunan 20.000 DEXE'yi market emri⁵⁸¹ ile satar. 3.000 adet DEXE, şekildedeki emir defterinde bulunan diğer kullanıcıların emirlerini doldururken, geri kalan 17.000 adet DEXE ise 2 numaralı kullanıcının 0,1 USDT'deki alım emrini doldurur. 2 numaralı kullanıcı burada 1.700 USDT harcayarak 51.000 USDT değerinde DEXE elde etmiş olacaktır. Yani 49.300 USDT değerinde fon aktarımı gerçekleşmiş olur. Yapılan bu

⁵⁸⁰ 1 Amerikan dolarına denk stabil kripto para.

⁵⁸¹ Emir defterinde bulunan emirler üzerinden anında gerçekleşen bir emir türü.

işlemin amacı terörizmin finansmanının gerçekleştirilmesi iken dışarıdan bakan biri için herhangi bir borsa işleminden farksızdır. Ayrıca merkezi bir kripto para borsası üzerinde yapılan alım satım işlemleri ağ üzerinde değil, borsa platformu üzerinde gerçekleştiğinden; ağ üzerinde yapılan incelemede de bu tür bir işleme ulaşılamaz. Yani yapılan bu işlem bir kripto para aktarımı niteliğinde olmamaktır. Fakat bu teknik sayesinde kripto para aktarmakla aynı işlevi görmektedir. Kullanıcı 2'nin sonradan terör örgütüne fon toplayan bir kişi olduğu bilinse bile, kullandığı hesap üzerindeki kripto para transferlerinden bu şekilde bir alım satım işlemi anlaşılacaktır. Kullanıcı 2'nin alım satım işlemleri detaylı bir şekilde incelense bile, burada Kullanıcı 1, elindeki DEXE'leri büyük miktardaki varlıkların yanlışlıkla satılması anlamına gelen ve "tombul parmak (fat finger)" denilen hata ile satma durumu gerçekleştiğini öne sürebilir.

Şekil 3. 9 Bir CEX üzerinde sıg bir emir defterine sahip bir parite. (AVAX/USDT.e)

Price (USDT.e)	Amount (AVAX)	Total (USDT.e)
110,000	3,000	330,000
105,000	3,042	319,410
103,950	69,738	7.249,265
103,000	2,000	206,000
101,466	20,000	2.029,320
98,000	1,106	108,388
80,000	7,000	560,000
70,000	33,595	2.351,650
23,477	0,124	2,911
22,986 USDT.e		Spread: 0,983
22,494	14,721	331,134
22,338	14,501	323,923
22,270	15,192	338,326
12,466	160,429	1.999,908
10,500	25,190	264,495
0,222	1.257,329	279,127

(Kaynak: Dexalot)

Şekil 4.9., merkezi kripto para borsalarında olduğu gibi limit emir girmeye imkan veren bir CLOB (Central Limit Order Book) DEX'tir. Bu örnekte bir DEX söz konusu olduğundan alım satım işlemleri ağ üzerinden gerçekleşir. Şekilde AVAX/USDT.e⁵⁸²

⁵⁸² USDT.e, Avalanche ağı üzerinde bulunan USDT'dir.

paritesinin emir defteri görülmektedir. AVAX (Avalanche) bir kripto para olup normal şartlarda yaklaşık 23 USDT üzerinden işlem görmektedir. Fakat buradaki alım emirleri incelendiğinde, toplamda sadece 3.500 USDT kadar AVAX alım emrinin konulduğu görülmektedir. Ağ üzerinde kripto para transfer edildiğinde alıcı ve gönderici adreslerinin görünebileceğini bilen iki kullanıcı, yukarıdaki örneğe benzer bir işlem gerçekleştirebilirler. Bu durumda terörizmin finansmanı amacıyla fon transfer etmek isteyen Kullanıcı 1'in elinde 460.000 USDT değerinde 20.000 tane AVAX olduğunu varsayalım. Fonu teslim almak isteyen Kullanıcı 2, 0,001 USDT'ye 19.800 adet AVAX alım emri girer, bu emir için sadece 19,8 USDT kullanır. Kullanıcı 2, elindeki 20.000 adet AVAX'ı satar. Emir defterinde Kullanıcı 2'nin emri dışında sadece 200 adet AVAX alım emri bulunmaktadır. 200 adeti diğer kullanıcıların, 19.800 adeti ise Kullanıcı 2'ye ait bu emirler, Kullanıcı 1'in satışı ile dolar. Kullanıcı 2, gerçekleşen bu işlem sonucu 19,8 USDT harcayarak Kullanıcı 1'den 19.800 adet yani 455.400 USDT değerinde AVAX elde etmiş olacaktır.

Yukarıda DEX üzerinde yapılan işlemlerin ağ üzerinde gerçekleştiğini ve bu nedenle ağ üzerinden görülebileceği belirtilmişti. Fakat DEX örneğinde gerçekleşen alım satım işlemi, ağ üzerinden incelendiğinde Kullanıcı 1'in Kullanıcı 2'ye kripto para sattığı şeklinde görülmez. Örneğin platform üzerinde konulan bir emrin ağdaki görüntüsü Şekil 4.10. üzerinde görülebilir.

Şekil 3. 10 DEX üzerinde konulan bir emrin ağdaki görüntüsü.

Transaction Hash:	0xb75112ba20c93b9cafd0c2a6c5df95dc6e51b49c73192a84259a1d6ae9242880
Status:	Success
Block:	15330071 738 Block Confirmations
Timestamp:	24 mins ago (May-29-2022 12:27:05 PM +UTC)
From:	0x3a318123180ae6d69862515047e20d02587e5b27
To:	Contract 0x1d34b421a5ede3e300d3b8bcf3be5c6f45971e20 (Dexalot: Trade Pairs)
Value:	0 AVAX (\$0.00)
Transaction Fee:	0.009181084 AVAX (\$0.24)

(Kaynak: Snowtrace.io)

Şekil 4.10.'da, CLOB DEX üzerinde gerçekleşen bir emir ağ üzerinde incelendiğinde, emri koyan adres bilinmekle birlikte; gerçekleşen emrin bir alım mı yoksa satım emri mi olduğu, emrin ne zaman gerçekleştiği, emrin hangi paritede gerçekleştiği,

emrin ne kadarlık bir alım ya da satım işlemi olduğu bilinmemektedir. Bununla birlikte aynı şekilde görülebildiği üzere, işlemin alıcısı (Dexalot: Trade Pairs) adındaki, DEX'in emir defterinin akıllı sözleşme (kontrat) adresidir. Yani gerçekleşen emirlerin alıcısının kim olduğu da bilinemez. Örneğe dönülürse, Kullanıcı 1 örnekteki gibi bir satış gerçekleştirdiğinde, satışın ne zaman, hangi paritede, ne kadar miktarda gerçekleştiği bilinmemekle birlikte; ağ üzerindeki işlemde alıcı genel olarak kontrat adresi şeklinde gözüktüğünden, işlemde alıcının Kullanıcı 2 olduğu bilinemez. Ağ üzerinde herkesin görüp takip edebileceği basit bir kripto para transferi ile terörizmin finansmanı yönteminin tercih edilmesi yerine, anlatılan örneklerdeki şekilde daha detaylı teknikler kullanılarak gizli ve tespit edilemez bir şekilde finansman sağlama faaliyeti gerçekleştirilebilir. Tekrar belirtmek gerekir ki, örneklerdeki platformlar sadece gerçekleştirilen işlemlere aracı platformlar olup, bahsedilen teknikler başka herhangi bir borsa üzerinden de gerçekleştirilebilir. Yapılan bu tür işlemler ağ üzerinde takip edilmeyi zorlaştırır. Burada yapılan işlemler basit bir alım satım işlemi olsalar da, taşıdığı amaç doğrultusunda terörizmin finansmanı için yapılan kullanıcılar arası bir fon sağlama faaliyeti gerçekleştirmektedirler.

FATF, aşağıda daha ayrıntılı bahsedileceği üzere kripto para borsalarını “sanal varlık hizmeti sağlayıcısı [virtual asset service provider (VASP)]” olarak adlandırmakta ve bu kapsamda yorumlamaktadır.

Türk hukukunda kripto para borsaları ile ilk kez “Suç Gelirlerinin Aklanmasının Ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik⁵⁸³”e, 1/5/2021 tarihinde eklenen, 4. Maddenin 1. Fıkrasının (ü) bendinde yer alan “Kripto varlık hizmet sağlayıcıları” olarak karşılaşılmıştır. MASAK tarafından 4/5/2021 tarihinde yayınlanan “Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının Ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar” adlı rehberde⁵⁸⁴ kripto varlık hizmet sağlayıcıları, “kripto varlıkların alım satımlarına elektronik işlem platformları üzerinden aracılık etmekte olan kuruluşlar” olarak tanımlanmaktadır.

⁵⁸³ R.G., T: 9/1/2008, S: 26751.

⁵⁸⁴ MASAK, Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının Ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, 2021, <https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf> (Erişim: 29.05.2022)

Türkiye’de henüz kripto para borsaları ile ilgili özel bir düzenleme bulunmamaktadır. Bu tür borsalar hakkında genel ve kapsamlı bir düzenleme bulunmadığından, bu alandan sorumlu bir denetleyici ve düzenleyici otorite de bulunmamaktadır⁵⁸⁵. Türkiye’de yerleşik kripto para borsaları kullanıcılarının, borsaları kullanabilmek için kimlik doğrulama süreçlerinden geçmeleri gerekmektedir.

3.3.9. FATF’nin 10, 15 ve 16 Numaralı Tavsiyeleri Kapsamında Kripto Paralar

FATF, “Yeni Teknolojiler (New Technologies)” başlığını taşıyan 15 numaralı tavsiyesinde genel olarak ülkelere yeni teknolojiler ile ortaya çıkabilecek karapara aklama ve terörizmin finansmanı risklerini tespit etme ve değerlendirme ve bu doğrultuda tedbirler almalarını belirtmektedir. FATF, Ocak 2018 tarihinde⁵⁸⁶, 15 numaralı tavsiyesinde⁵⁸⁷ revizyona giderek “sanal varlık [virtual asset (VA)]” ve “sanal varlık hizmeti sağlayıcısı [virtual asset service provider (VASP)]” tanımlarını eklemiştir. Ardından Haziran 2019⁵⁸⁸ tarihinde 15 numaralı tavsiyenin yorumlayıcı notunda eklemeye giderek, sanal varlıkların ve VASP’lerin FATF Standartları kapsamına alınması sağlanmıştır.

Bu doğrultuda 15 numaralı tavsiyenin yorumlayıcı notunda⁵⁸⁹, “seyahat ya da dolaşım kuralı (travel rule)” olarak bilinen “elektronik transfer (wire transfer)” başlıklı terörizmin finansmanının önlenmesi amacıyla oluşturulan 16 numaralı tavsiyesi uyarınca, VASP’lere dijital varlık transferlerinde transferin kaynağı ve bu transferden yararlananın tanımlayıcı bilgilerinin kaydını tutma ve gerektiğinde yetkili otoriteler ile paylaşması sorumluluğu yüklemiştir. Bu bilgiler isim, fiziki adres, vatandaşlık numarası gibi bilgileri içermektedir⁵⁹⁰. Bununla birlikte 15 numaralı tavsiyenin yorumlayıcı notunda; 10 numaralı tavsiye doğrultusunda, bu tür işlemler için bildirim limitinin 1.000 Amerikan doları ya da EURO olduğu belirtilmiştir (Amerika Birleşik Devletlerinde “Bank Secrecy

⁵⁸⁵ Perçin vd., 2021, s. 94.

⁵⁸⁶ FATF, The FATF Recommendations, 2022, s. 138. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (Erişim: 28.05.2022)

⁵⁸⁷ FATF, 2022, s. 17.

⁵⁸⁸ FATF, 2022, s. 138.

⁵⁸⁹ FATF, 2022, ss. 76-77.

⁵⁹⁰ FATF, 2022, s. 79.

Act” doğrultusunda bu limit 3.000 Amerikan dolarıdır). Bu doğrultuda her ülke FATF tavsiyelerine uygun düzenlemelere gitmektedir.

Kripto para borsalarının da bu nedenle düzenlemelere uymak amacıyla “Müşterini Tanı [Know Your Customer (KYC)] uygulamalarını borsa kullanıcılarına zorunlu tutmaya başladığı görülmektedir. Bununla birlikte gizlilik odaklı kripto paralar hakkında yukarıda bahsedildiği üzere FATF 2021 tarihli rehberinde, AML/CFT’lerin (kara para aklamanın ve terörizmin finansmanının önlenmesi ile ilgili düzenlemeler) sanal varlık ve sanal varlık hizmeti sağlayıcıları hakkında “finansal eyleme konu olan sanal varlığın türüne bakılmaksızın, gizlilik odaklı kripto paralar dahil olmak üzere” uygulanacağını belirtmiştir. Bu doğrultuda çoğu kripto para borsasının, seyahat kuralına aykırılık oluşturacak gizlilik odaklı kripto paraları borsalarından çıkarmaya başladığı görülmektedir. Örneğin merkezi bir kripto para borsası olan Bittrex Global, 2021 yılında Monero, Zcash, Dash ve Grin’i borsadan çıkardığını açıklamıştır⁵⁹¹. Bununla birlikte merkeziyetsiz bir kripto para borsası olan Waves Exchange de Mayıs 2022 itibariyle Monero, Zcash ve Dash’e verdiği desteği tamamen kesmiştir⁵⁹². Bununla birlikte seyahat kuralı ile birlikte kripto para kullanıcılarının gizlilik odaklı kripto paralara daha çok yöneldiği belirtilmelidir⁵⁹³.

Bununla birlikte FATF tarafından merkeziyetsiz finans uygulamalarının (DeFi) VASP tanımına girmediği; fakat bu uygulamaların kurucusu, yöneticisi, sahibi gibi kişilerin her ne kadar bu tür uygulamalar merkeziyetsiz olsa da, duruma göre VASP tanımına girebilecekleri belirtilmiştir⁵⁹⁴.

⁵⁹¹ Bittrex Global, “Delisting of XMR, ZEC, DASH, and GRIN”, <https://bittrexglobal.zendesk.com/hc/en-us/articles/360018560640-Delisting-of-XMR-ZEC-DASH-and-GRIN> (Erişim: 28.05.2022)

⁵⁹² Waves.Exchange (@Waves_Exchange), “Delisting XMR, Dash and ZEC These tokens will soon be delisted from http://Waves.Exchange. Their depositing will be terminated on March 9, 2022. If you have any XMR, Dash or ZEC, we recommend withdrawing them no later than May 8, 11am UTC otherwise you will lose your coins.”, 03.03.2022, https://twitter.com/waves_exchange/status/1499429481970389002 (Erişim: 28.05.2022)

⁵⁹³ Partz, Helen, “FATF’s Regulations to Push Criminals to Privacy Coins: CipherTrace CEO”, 22.10.2019, Cointelegraph, <https://cointelegraph.com/news/fatfs-regulations-to-push-criminals-to-privacy-coins-ciphertrace-ceo> (Erişim: 28.05.2022)

⁵⁹⁴ FATF, 2021, s. 27.

3.3.10. Türkiye’deki Kripto Para Düzenlemesi

Türkiye’de kripto paralar hakkındaki tek düzenleme, yukarıda da bahsedildiği üzere “Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik”tir. İlgili yönetmelik dışında kripto paralar ile ilgili hukuki düzenlemelerde yer alan tek ifade, “Suç Gelirlerinin Aklanmasının Ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik ”e, 1/5/2021 tarihinde eklenen, 4. Maddenin 1. Fıkrasının (ü) bendinde “Kripto varlık hizmet sağlayıcıları”dır. Bununla birlikte Türkiye’de blok zincir ve kripto paralar ile ilgili kanun çalışması yapıldığı bilinmektedir.

Bu bölümün başlangıcında da ortaya konduğu üzere, yönetmelik doğrultusunda 3. madde uyarınca kripto paraların, kripto varlıklar olarak geniş bir kapsamda “dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıklar” olarak kullanıldığı görülmektedir.

Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik doğrultusunda kripto varlıkların ödemelerde doğrudan ya da dolaylı şekilde kullanılamayacağı ve buna yönelik hizmetin sunulamayacağı belirtilmiştir. Yönetmeliğin bu hali ile Borçlar Kanunu’nda bulunan sözleşme serbestisi ilkesi ile çelişen bir durum yaratacağı belirtilebilir.

Yönetmeliğin 4. Maddesi uyarınca, kripto varlıkların doğrudan veya dolaylı olarak kullanılacağı bir şekilde iş modelleri geliştirilemeyeceği ve bu tür iş modellerine ilişkin herhangi bir hizmet sunulamayacağı belirtilmiştir. Ayrıca aynı maddede ödeme ve elektronik para kuruluşlarının, kripto varlıklara ilişkin alım satım, saklama, transfer veya ihraç hizmeti sunan platformlara veya bu platformlardan yapılacak fon aktarımlarına aracılık edemeyeceği belirtilmiştir.

DÖRDÜNCÜ BÖLÜM

TERÖRİZMİN FİNANSMANI VE FİNANSMANIN ÖNLENMESİ

4.1. Giriş

Terörizmin finansmanı ve finansmanın önlenmesi, bu çalışmanın ana konusunu oluşturan unsurlardandır. Çalışmanın üst bölümünde kripto paraların terörizmin finansmanını gerçekleştirmede nasıl ve hangi yollarla kullanılabileceği, ayrıntılı örnek ve açıklamalar ve birtakım uluslararası düzenlemeler ile birlikte ortaya konmuştur. Çalışmanın bu bölümünde ise terörizmin finansmanı ve finansmanın önlenmesi üzerinde durulduktan sonra, terörizmin finansmanının kripto paralar ile gerçekleştirilmesi durumunda malvarlığının dondurulması, elkoyma ve müsadere gibi tedbirlerin uygulanmasındaki sorunlar irdelenecektir.

Çalışmanın üst kısımlarında da bahsedildiği üzere kripto paralar yapıları ve işleyişleri gereği terörizm finansmanı sağlamaya oldukça elverişlidirler; hatta bulunmaz nimet olarak tabir edilebilirler. Bu doğrultuda bu çalışmanın salt terörizmin finansmanı suçu çalışması olmadığı kabul edilip, kapsamın bu şekilde ölçeklendirilmiş olduğu göz önünde tutularak; uluslararası hukuk bağlamında terörizmin finansmanı ve finansmanın önlenmesinin, Türk hukukundaki görünümü ile birlikte genel olarak ortaya konması gerekmektedir. İlk olarak terör, terörizm, finansman ve terörizmin finansmanı gibi kavramların tanımlanması uygun olacaktır.

4.2. Terörizmin Finansmanı İle İlgili Kavramlar

4.2.1. Terör ve Terörizm Kavramları

Terör ve terörizm kavram olarak çoğu zaman birlikte ve birbirlerinin yerine düşünülüp kullanılsa da aralarında bir takım farklılıklar bulunmaktadır⁵⁹⁵. Yine de

⁵⁹⁵ Tokgöz, Havva Begüm, Uluslararası Hukuk Bağlamında Terörizmin Finansmanının Önlenmesi, (1. Baskı), On İki Levha Yayıncılık, İstanbul 2022, s. 11.

terörizm teriminin terör teriminden türediği rahatlıkla söylenebilir⁵⁹⁶. Öncelikle kısaca terör teriminden bahsedilecektir.

Terörün kavram olarak ilk kez Fransız İhtilali sonrası 1793-1794 yılları arasındaki “Terör Dönemi (*ing.* Reign of Terror, *fr.* la Terreur)” ile yer edindiği söylenebilir⁵⁹⁷. Bununla birlikte “terör” kelimesi Latince “korkutmak” anlamına gelen “terrere” kelimesinden türemiş olup; Fransızca “terreur”, İngilizcede “terror” ve Türkçede “terör” olarak kendisine yer edinmiştir.

Terör Dönemi, Fransız İhtilali sonrası kurulan Birinci Fransız Cumhuriyeti dönemi sırasında, 1793-1794 tarihleri arasında, hükümet baskısı çerçevesinde oluşan, yaklaşık 17.000’i yasal olan 40.000 civarında idam şeklinde infazın gerçekleştiği döneme denir⁵⁹⁸. Bununla birlikte 1793-1796 arasında yaşanan Vendée İsyanı sonucu gerçekleşen yüzbinlerce ölümün de Terör Dönemi çerçevesinde incelenmesi gerektiği kimi yazarlarca düşünülmektedir⁵⁹⁹. Terör, Fransız İhtilali’nin önde gelen isimlerinden Jakoben Maximilien Robespierre tarafından “günün şartları dahilinde adaletin yerine tecelli eden, adaletin istisnai bir görünümü” olarak değerlendirilmiştir⁶⁰⁰. Robespierre terörün “hızlı, şiddetli ve katı bir adaletten fazlası olmadığı”nı belirtmiştir⁶⁰¹.

Fransa’da gerçekleşen Terör Dönemi’nden günümüze kadar bazı totaliter rejim ve diktatörlüklerde karşılaşılan, devletin devlet tarafından yönetilenlere, belirli gruplara, daha ziyade devlet otoritesine karşı direnen veya rejimi sarsmaya-yıkmaya yönelik ya da öyle olduğu varsayılanlara karşı⁶⁰² uyguladığı korkutma, baskı ve cebir “devlet terörü” olarak tanımlanabilmektedir. Terör kavramı incelenirken literatürde çoğunlukla kavramın Fransız İhtilali ve Terör Dönemi ile ilişkilendirildiği görülmektedir. Bu doğrultuda Terör kavramının ortaya çıktığı Fransa örneğinde terörün devlet kaynaklı olması, terörün

⁵⁹⁶ Männik, Erik, “Terrorism: Its Past, Present And Future Prospects”, KVÜÖA toimetised, 12, 2009, s. 152. https://www.ksk.edu.ee/en/wp-content/uploads/2011/03/KVUOA_Toimetised_12-Männik.pdf (Erişim: 06.05.2022)

⁵⁹⁷ Männik, 2009, s. 152.; Yayla, Atilla, “Terörizm: Kavramsal Bir Çerçeve”, *Ankara Üniversitesi SBF Dergisi*, 1990/45 (1), s. 335. <https://dergipark.org.tr/tr/download/article-file/38276> (Erişim: 06.05.2022)

⁵⁹⁸ Tilly, Charles. “Terror, Terrorism, Terrorists.” *Sociological Theory*, 2004/22 (1), ss. 8-9. <http://www.jstor.org/stable/3648955> (Erişim: 06.05.2022)

⁵⁹⁹ Gerard, A. 1999. "Par principe d'humanite ... " *La Terreur et la Vendée* ["For the Sake of Humanity The Terror and the Vendie]. Paris, France: Fayard ve

Greer, D. 1935. *The Incidence of the Terror during the French Revolution. A Statistical Interpretation*. Cambridge, MA: Harvard University Press’ten akt. Tilly, 2004, s. 9.

⁶⁰⁰ Maximilien Robespierre’den akt. Wikipedia, “Reign of Terror”, https://en.wikipedia.org/wiki/Reign_of_Terror (Erişim: 06.05.2022)

⁶⁰¹ Maximilien Robespierre’den akt. Männik, 2009, s. 152.

⁶⁰² Yayla, 1990, s. 360.

“devlet terörü” ya da “devlet destekli terör” şeklinde tanımlamaların ortaya çıkmasına neden olabilmektedir⁶⁰³. Bu noktada devlet terörü, yukarıda bahsedildiği gibi terör ve terörizmin birbirinden ayrı terimler olarak ele alınması konusunda araç olarak da kullanılabilir. Terör kavramı devlet tarafından uygulanan terör ile, terörizm kavramı ise devlete karşı uygulanan terör ile ifade edilebildiği gibi; terörizm kavramının devlet terörünü dışladığını ileri süren görüşlerin yanı sıra terörizmin kökeninin devlet tarafından uygulanan terörün oluşturduğu da belirtilebilmektedir⁶⁰⁴. Bununla birlikte “devlet terörizmi”, “bir devletin diğer devlete ya da o devletin vatandaşlarına karşı gerçekleştirdiği terör faaliyetleri ve devletin kendi vatandaşlarına karşı geniş çaplı uyguladığı zulüm⁶⁰⁵” şeklinde tanımlanabildiği gibi; “devlet, devletin aygıtları ya da müttefikleri tarafından uygulanan terörizm⁶⁰⁶” şeklinde de tanımlanabilmektedir.

Terör ve terörizm terimlerinin farklı anlamlar ifade ettiği hususunda Austin T. Turk, terör ve terörizmin kavramsal olarak ayrılıklarını açıklarken “siyasal şiddet” kavramından faydalanmıştır. Bununla birlikte Turk’un, Water Laqueur’un terörizmin üzerinde uzlaşılan bir tanımının yapılamayacağı görüşüne de katıldığı belirtilmelidir⁶⁰⁷. Turk’e göre terörizm, siyasal şiddetin bir biçimi olarak ele alınırsa daha spesifik ve objektif bir tanımlamaya ulaşılabilir. Bu doğrultuda eylemler politikasını eylemlerin kendisinden ayırmakla başlamak gerekmektedir. Buradan hareketle terörizmin politikasını da terör eylemlerinin kendisinden ayrılması gerekir. Turk’un bu şekilde ulaştığı terörizm tanımı “terör eylemlerini doğrulayıcı ideoloji ya da bu tür eylemlere öncelik veren strateji” olmakta iken terör ise “bu ideolojiyi ifade etmek ya da stratejiyi uygulamak için kullanılan şiddet”tir⁶⁰⁸. Turk ayrıca terörün bu tanımına ek olarak terörü, “kasıt”, “amaç”, “hedef” ve “organizasyon” kıstaslarından geçirerek⁶⁰⁹; “muhalefeti yıldırım için korkuyu baskın bir şekilde kullanarak, özellikle rastgele insan ya da

⁶⁰³ Chaliand, Gérard, Arnaud Blin, T’he History of Terrorism”, University of California Press, 2016, s. 95. <https://doi.org/10.1525/9780520966000-007> (Erişim: 06.05.2022)

⁶⁰⁴ Tokgöz, 2020, ss.17-18.

⁶⁰⁵ Aust, Anthony, Handbook of International Law, Cambridge University Press, Second Edition, s. 265. https://books.google.com.tr/books?id=74Zmct-7hGIC&pg=PA265&redir_esc=y#v=onepage&q&f=false (Erişim: 06.05.2022)

⁶⁰⁶ Sluka vd., “What Anthropologists Should Know about the Concept of Terrorism’: A Response to David Price, A.T. 18(1).”, *Anthropology Today*, 2002/18 (2), s. 22. <http://www.jstor.org/stable/3694961> (Erişim: 06.05.2022)

⁶⁰⁷ Turk, Austin T. “Social Dynamics of Terrorism.” *The Annals of the American Academy of Political and Social Science*, 1982/463, s. 120. <http://www.jstor.org/stable/1043616> (Erişim: 07.05.2022)

⁶⁰⁸ Turk, 1982, ss. 120-121.

⁶⁰⁹ Turk, 1982, ss. 121-122.

yerlerin hedef alındığı, ölümcül ya da ölümcül olmayan, organize siyasal şiddet” olarak tanımlamaktadır⁶¹⁰.

Yukarıdaki tanımlamaların dışında doktrinde terör ve terörizm kavramları birlikte ya da ayrı anlamda kullanılabilir. Zeki Hafızoğulları ve Günal Kurşun, terör ve terörizm kavramlarını birbirinden ayırmadan “demokratik düzeni yıkmayı amaçlayan ve çoğu kez bir dinin, bir ideolojinin ya da sömürüldüğü iddia edilen bir etnik grubun sahibi ve savunucusu olarak ortaya çıkan örgütlü şiddet hareketleri olarak tanımlamaktadır⁶¹¹.

Hamide Zafer ise terörizmi, “insan gruplarını bir anda dehşete düşürme stratejisinden ibaret olan terör eylemlerinin belirli bir plan dahilinde sistematik olarak uygulanmasını ve dolayısıyla terör eylemlerinin bütünü ifade eden bir kavram” olarak açıklamaktadır⁶¹².

Yukarıdaki tanımlamalardan da görülebileceği üzere literatürde terör ve terörizm üzerinde uzlaşılan ortak bir tanım olmamakla birlikte iki kavram birlikte ya da ayrı şekilde de ele alınabilmektedir. Bununla birlikte bu durum Uluslararası kuruluşların terör ve terörizm tanımlamalarında da karşımıza çıkmaktadır. Zira uluslararası düzeyde üzerinde uzlaşmaya varılacak bir terörizm tanımı için öncelikle ülkelerin kendi terörizm tanımlamaları üzerinde bir sonuca ulaşmış olması gerekmektedir⁶¹³.

Birleşmiş Milletler tarafından terörizm, “sivillere yönelik olanlar dahil, öldürme, ciddi yaralama, rehin alma kastıyla gerçekleştirilen ve halkın geneli üzerinde veya belirli bir kesimi üzerinde korku oluşturmak veya devletin veya uluslararası bir örgütün görevini yapmasını engellemek amacıyla ve politik, felsefi, ideolojik, etnik, dini veya benzeri gerekçelere dayandırılmasına bakılmaksızın gerçekleştirilmek istenen her türlü suç eylemi⁶¹⁴” ya da “bir devlette terörün kışkırtılmasına, halkın korkutulmasına veya bir hükümetin ya da kuruluşun baskı altına alınmasına yönelik ciddi ve suç doğurucu şiddet eylemleri⁶¹⁵” olarak tanımlanabilmektedir.

⁶¹⁰ Turk, 1982, s. 122.

⁶¹¹ Zeki Hafızoğulları ve Günal Kurşun, “Türk Ceza Hukukunda Örgütlü Suçluluk”, Türkiye Barolar Birliği Dergisi, 2007/71’den akt. Tokgöz, 2022, ss. 11-12.

⁶¹² Zafer, Hamide, *Sosyolojik Boyutuyla Terörizm*, İstanbul, Beta Yayıncılık, Mayıs 1999, s. 3’ten akt. Tokgöz, 2022, s. 19.

⁶¹³ Sezgin, Erkan, “A Comparative Perspective of International Cooperation Against Terrorism”, A Doctor of Philosophy dissertation submitted to the Kent State University Political Science Department, August 2007, s. 38’den akt. Tokgöz, 2022, s. 36.

⁶¹⁴ Akt. Tokgöz, 2022, s. 38.

⁶¹⁵ Akt. Tokgöz, 2022, s. 39.

Avrupa Birliđi'nin 2002 tarihli "Terörizmle Mücadele Hakkında Konsey Çerçeve Kararı" ile terör ise, "bir ülkenin halkını ciddi şekilde korkutmak veya sindirmek, bir hüümeti ya da uluslararası kuruluşu bir şey yapmaya ya da yapmamaya zorlamak ve bir ülkenin ya da uluslararası kuruluşun siyasal, sosyal, ekonomik ve anayasal yapısını yıkmak veya işlemez hale getirmek amacı ile bir ülkeyi ya da uluslararası bir organizasyonu ciddi zarara uğratan kasıtlı eylemleri yapmak⁶¹⁶" olarak tanımlamaktadır.

Türk hukukunda ise terör, 3713 sayılı Terörle Mücadele Kanunu'nun 1. maddesinde "*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni deđiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğrattmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliđini, kamu düzenini veya genel sađlığı bozmak amacıyla bir örgüte mensup kiři veya kişiler tarafından giriřilecek her türlü suç teşkil eden eylemler*⁶¹⁷" şeklinde tanımlanmaktadır.

4.2.2. Finansman ve Terörizmin Finansmanı Kavramları

"Finansman" kelimesinin etimolojisine bakıldığında, kelimenin Fransızca "financement" kelimesinden doğduđu anlaşılmaktadır⁶¹⁸. Türk Dil Kurumu finansmanı "bir girişime işleyebilmesi, gelişebilmesi için gereken para ve krediyi sađlama işi" olarak tanımlamaktadır⁶¹⁹.

Terörizmin finansmanı ise kısaca "terör eylemlerinde bulunan kiři ya da grupların faaliyetlerini sürdürebilmeleri için gerekli para ve mali desteđi verme⁶²⁰" şeklinde tanımlanabilir. Bununla birlikte bir uluslararası kuruluş olan Birleşmiş Milletler'in terörizmin finansmanını, 1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme'de "niteliđi veya kapsamı itibariyle bir halkı korkutmak ya da bir hükümeti veya uluslararası kuruluşu herhangi bir işi yapmaya veya yapmamaya zorlamak

⁶¹⁶ Akt. Tokgöz, 2022, ss. 41-42

⁶¹⁷ R.G., T: 12/4/1991, S: 20843 Mükerrer.

⁶¹⁸ Wiktionary, "financement", <https://en.wiktionary.org/wiki/financement> (Eriřim: 07.05.2022)

⁶¹⁹ Türk Dil Kurumu, "finansman", <https://sozluk.gov.tr> (Eriřim: 07.05.2022)

⁶²⁰ Aydın D. ve Ç. Arslan, Suçtan Kaynaklanan Malvarlıđı Deđerlerini Aklama ve Terörizmin Finansmanı Suçu, Yetkin Yayınları, Ankara 2021, s. 89.

amacı taşıyan bir olayda bir sivil ya da silahlı çatışmaya doğrudan katılmayan herhangi bir kişiyi öldürmeye veya ağır şekilde yaralamaya yönelik olan veya Sözleşme ekinde yer alan 9 terör sözleşmesi tarafından suç sayılan eylemlerin tümünün ya da bir kısmının gerçekleştirilmesinde kullanılması niyetiyle veya kullanıldığını bilerek doğrudan veya dolaylı olarak yasa dışı bir şekilde fon sağlanması veya toplanması⁶²¹ şeklinde değerlendirdiği görülmektedir.

4.3. Terörizmin Finansmanının Önlemeye Yönelik Uluslararası Düzenlemeler

4.3.1. Birleşmiş Milletler Nezdinde Yapılan Düzenlemeler

4.3.1.1. Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme

Birleşmiş Milletler nezdinde yapılan terörizmin finansmanının önlenmesinde yönelik en önemli düzenleme şüphesiz Birleşmiş Milletler Genel Kurulu tarafından 9 Aralık 1999 tarihinde kabul edilen ve 10 Nisan 2002’de yürürlüğe giren “Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme”dir. Sözleşmenin terör faaliyetleri çerçevesinde bir dönüm noktası olan 11 Eylül Saldırısı öncesi kabul edilmiş olması önemlidir⁶²².

Sözleşmenin temel amacı, “terörizmin finansmanının engellenmesi ve failerin kovuşturulması ve cezalandırılmasına yönelik etkili önlemlerin oluşturulması ve benimsenmesi amacıyla devletler arasında uluslararası işbirliğinin acilen geliştirilmesine duyulan ihtiyaç” olarak belirtilmiştir⁶²³. Sözleşmeye taraf olan devletlere, terörizmin finansmanını engellemeye yönelik gerekli tedbirleri alma zorunluluğu, terörizmin finansmanına yönelik faaliyet gösteren sivil veya idarecileri yakalama, sözleşmenin ikinci maddesinde belirtilen suçların iç hukukta da suç olarak düzenlenmesi gibi yükümlülükler yüklenmiştir⁶²⁴.

Sözleşmede terörizmin finansman kaynakları ve finansman sağlama yöntemleri çerçevesinde önemli iki kavram olan “fon” ve “getiri” de tanımlanmıştır. Sözleşmenin 1. maddesinin 1. fıkrasında fonlara, “*Her ne suretle edinilmiş olursa olsun, maddi veya*

⁶²¹ Tokgöz, 2022, ss 53-54.

⁶²² Tokgöz, 2022, s. 65.

⁶²³ Aydın ve Arslan, 2021, s. 91.

⁶²⁴ Tokgöz, 2022, ss. 66-69.

gayri maddi, menkul veya gayrimenkul, her türlü kıymeti ve bu kıymetler üzerinde bir mülkiyet hakkı veya çıkarı kanıtlayan, elektronik veya dijital şekilleri dahil olmak üzere, her türlü görünüşteki belge ve yasal araçları ve bu çerçevede banka kredilerini, seyahat çeklerini, para havalelerini, hisse senetlerini, temintaları, tahvilleri, kredi mektuplarını, işbu tadat sınırlayıcı olmaksızın kapsar” şeklinde bir tanımlama getirilmiştir⁶²⁵.

Bununla birlikte aynı sözleşmenin 1. maddesinin 3. fıkrasında getiri ise, “2. Maddede tanımlanan türde bir suçun işlenmesi sonucunda doğrudan veya dolaylı olarak edinilen fonları veya böyle bir suçun işlenmesi sayesinde doğrudan veya dolaylı olarak temin edilen fonları kapsar” şeklinde tanımlanmıştır.

Sözleşmenin 2. maddesinin 1. fıkrası ile terörizmin finansmanını sağlamak amacıyla fon toplamak ya da fon sağlamak fiilleri yasaklanmıştır. Sözleşmenin aynı maddesine göre, sözleşme ekinde belirtilen uluslararası sözleşmeler çerçevesinde ya da “niteliği ya da kapsamı itibariyle, bir halkı korkutmak, ya da bir hükümeti veya uluslararası örgütü herhangi bir eylemi gerçekleştirmeye veya gerçekleştirmekten kaçınmaya zorlamak amacını gütmesi halinde, bir sivilin ya da bir silahlı çatışma durumunda muhasemata doğrudan katılmayan herhangi başka bir kişiyi öldürmeye veya ağır şekilde yaralamaya yönelik diğer tüm eylemler”in meydana getirdiği bir suç için fonun fiilen kullanılmış olması, terörizmin finansmanı suçunun söz konusu olması için gerekli değildir; çünkü terörizmin finansmanı suçu bir tehlike suçu olup, davranışın yapılması suçun gerçekleşmesi için yeterlidir⁶²⁶. Bununla birlikte 2. maddeden hareketle, bir devletle silahlı çatışmaya giren ve çatışmanın tarafı olan devlet dışı örgüte silah veya benzeri malzemelerin tedarik edilmesi için fon sağlanmasının, bu sözleşme kapsamında terörizmin finansmanı suçunu oluşturmadığı sonucuna varılabilir⁶²⁷. Ayrıca sözleşmenin aynı maddesine göre terörizmin finansmanı suçuna iştirak ve teşebbüs de cezalandırılmaktadır.

⁶²⁵ Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme, https://diabgm.adalet.gov.tr/arsiv/adli_yardimlasma/adli_isbirligi_ceza/suclularin_iadesi_ek/terorizmin_finansman%C4%B1n%C4%B1n_%C3%B6nlenmesine_ili%C5%9Fkin%20BM%20s%C3%B6zlesmesi.pdf (Erişim: 06.05.2022)

⁶²⁶ Aydın ve Arslan, 2021, s. 91.

⁶²⁷ Tokgöz, 2022, s. 68.

4.3.1.2. Güvenlik Konseyi Akıllı Yaptırım Kararları

Birleşmiş Milletler'in kuruluş amacı olan uluslararası barış ve güvenliğin sağlanması görevi -Genel Kurul'un da katkıda bulunma yetkisinin varlığı dahilinde- Birleşmiş Milletler'in ana organlarından Güvenlik Konseyi'ne verilmiştir⁶²⁸. Güvenlik Konseyi kendisine verilen bu görevi yerine getirebilmek için Birleşmiş Milletler Antlaşması'nın VII. bölümünde kendisine verilen geniş yetkilerden faydalanmaktadır. Bu yetkilerin kullanım örneklerinden biri de Güvenlik Konseyi'nin Birleşmiş Milletler Antlaşması'nın 41. Maddesine dayanarak aldığı "akıllı yaptırım" kararlarıdır.

Akıllı yaptırımlar kişi topluluğunun tamamını hedef almazlar; bu yaptırımlar belirli kişi ya da kişi gruplarını hedef alırlar. Bu nedenle genel olarak devletin ya da devletin vatandaşlarını ilgilendiren diğer yaptırım kararlarından ayrılırlar. Bu doğrultuda akıllı yaptırımların amacının önceden belirlenmiş kişi veya kişi gruplarını belirli yaptırımlara tabi tutmak olduğu söylenebilir⁶²⁹. Akıllı yaptırımları, yaptırımın amacına göre türlere ayırmak mümkün olmakla birlikte⁶³⁰; bu çalışmada daha çok, çalışmanın konusunu yakından ilgilendiren ve akıllı yaptırımların finansal görünümü olan malvarlığının dondurulması tedbirinden bahsedilecektir.

Güvenlik Konseyi'nin VII. bölümüne dayanarak aldığı kararlar üye devletler için bağlayıcıdır. Birleşmiş Milletler Antlaşması'nın 25. maddesine göre üye devletler Güvenlik Konseyi'nin bu kararları ve uygulanmalarını kabul eder. Bu doğrultuda akıllı yaptırım kararlarını yerine getirmenin uluslararası hukuk açısından bir yükümlülük haline geldiği söylenebilir⁶³¹.

Akıllı yaptırım kararlarından ilki 1999 tarihli 1267 sayılı karar⁶³² olup, kararda Usame bin Ladin ve Taliban Hükümeti hakkında düzenlemeler yapılmıştır. Kararda malvarlığının dondurulması ve uçuş yasağı gibi yasaklar öngörülmüştür. Uygulanacak bu yaptırımlar belirli bir süre ya da ülke ile sınırlandırılmamış; Usame bin Ladin ve Taliban ile ilişkisi olan bütün kişi ve kuruluşlara evrensel düzeyde yaptırım uygulanabileceği

⁶²⁸ Altiner Coşkun, Sümeyra, Birleşmiş Milletler Güvenlik Konseyi, Akıllı Yaptırım Kararları ve Terörizmin Finansmanının Önlenmesi, Seçkin Yayıncılık, Ankara 2015, s. 45.

⁶²⁹ Altiner Coşkun, 2015, ss. 51, 53.

⁶³⁰ Gordon, Joy, "Smart Sanctions Revisited", *Ethics & International Affairs*, 2011/25 (3), s.

321. <https://doi.org/10.1017/S0892679411000323> (Erişim: 06.07.2022)

⁶³¹ Altiner Coşkun, 2015, s. 50.

⁶³² United Nations Security Council, S/RES/1267 (1999), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/300/44/PDF/N9930044.pdf?OpenElement> (Erişim: 07.05.2022)

kararlaştırılmıştır. Kararın 4. ve 5. maddesinde “bütün ülkeler” deyiminin vurgulanması bu durumu izah etmektedir. Kararın önemli bir özelliği ise terörizmin finansmanına ilişkin düzenlemeler yapan ilk Güvenlik Konseyi kararı olmasıdır⁶³³. Bununla birlikte 1267 sayılı kararın uygulanması ve denetiminin sağlanması adına “1267 Komitesi” kurulmuştur.

1267 sayılı kararın tek başına yeterli olmadığı beklendiğinden, akıllı yaptırım kararlarının kapsamı ve içerikleri kısmen genişletilip, değiştirilerek 1267 sayılı kararı 1333, 1373, 1617, 2170⁶³⁴ gibi kararlar takip etmiştir.

2000 tarihli 1333 sayılı kararda⁶³⁵, 1267 sayılı karardaki yaptırımların yetersizliği nedeniyle, kapsamını genişletilmiştir. Kararın 15 (a) maddesinde bir “Uzmanlar Komitesi” kurulması öngörülmüş, bu komite silah ambargosu ve terörist kaplarının kapatılması ile ilgili yaptırımların yerine getirilmesi konusunda Konseye bilgi vermekle görevlendirilmiştir⁶³⁶.

Güvenlik Konseyi’nin 28 Eylül 2001 tarihinde, 11 Eylül saldırılarından 17 gün sonra almış olduğu 1373 sayılı karar⁶³⁷ önemlidir. Karara göre devletlerin, “uluslararası işbirliğini, kendi toprakları üzerindeki bütün hukuki olanaklarıyla her türlü terör eyleminin finansmanını ve hazırlığını önlemek ve cezalandırmak amacıyla ve ek önlemler almak suretiyle tamamlamaları” gerekmektedir⁶³⁸. 1373 sayılı kararın 3. Maddesinin (d) bendinde devletlere terörizm ile ilgili protokol ve sözleşmelere, özellikle de 1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme’ye taraf olma çağrısı yapılmıştır. Belirtmek gerekir ki, devletlerin terörizmle ilgili uluslararası sözleşmelere taraf olmaya bir bakıma zorlanmasının, Birleşmiş Milletler Antlaşması’nın 2. maddesinin 7. fıkrasında düzenlenen “iç işlerine karışmama ilkesi”ne aykırı bir durum oluşturmayacağı düşünülmektedir⁶³⁹. Çünkü Antlaşma’nın ilgili fıkrasında, Antlaşma’nın VII. bölümü uyarınca alınmış kararların bu ilke kapsamına girmediği belirtilmektedir.

⁶³³ Tokgöz, 2022, s. 79.

⁶³⁴ Güvenlik Konseyi’nin kararları bu kararlardan ibaret olmayıp, bu kısımda sadece bu çalışmada açıklanan kararlar zikredilmiştir.

⁶³⁵ United Nations Security Council, S/RES/1333 (2000), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/806/62/PDF/N0080662.pdf?OpenElement> (Erişim: 07.05.2022)

⁶³⁶ Altınır Coşkun, 2015, s. 57.

⁶³⁷ United Nations Security Council, S/RES/1373 (2001), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement> (Erişim: 07.05.2022)

⁶³⁸ Tokgöz, 2022, s. 80.

⁶³⁹ Altınır Coşkun, 2015, s. 65.

1373 sayılı karar 11 Eylül saldırılarından sonra alınmış bir karar olsa da, önceki kararların aksine yaptırımların kapsamının belirtilen olay ile sınırlı tutulduğuna dair bir ifade kullanılmamıştır. Bu karar ile Güvenlik Konseyi'nin ilk kez bir kanun koyucu gibi genel düzenlemelerde bulunduğu söylenebilir⁶⁴⁰. Bununla birlikte 1373 sayılı kararın 6. maddesi uyarınca bir "Terörle Mücadele Komitesi"nin kurulduğu da belirtilmelidir.

Güvenlik Konseyi, 2005 tarihli 1617 sayılı kararının 7. maddesinde⁶⁴¹ üye devletlerden, FATF'nin karapara aklama ile ilgili vermiş olduğu kırk tavsiyeyi ve terörizmin finansmanına ilişkin vermiş olduğu dokuz özel tavsiyeyi uygulamalarını talep etmiştir.

Güvenlik Konseyi'nin 2014 tarihli 2170 sayılı kararı⁶⁴² özellik arz edip, Usame bin Ladin, Taliban ya da El –Kaide odaklı verilen önceki kararların aksine ilk kez IŞİD ve El Nusra Cephesi ile ilgili düzenlemelere yer verilmiştir⁶⁴³. Kararın terörizmin finansmanı başlığı altında, 11. maddeden 21. maddeye kadar olan maddelerde devletlere terörizmin finansmanının önlenmesi kapsamındaki yükümlülükleri hatırlatılmış; söz konusu örgütler ile veya bağlantılı olanlar ile her türlü ilişki kınanmış ve bu tür ilişkinin 1267 ve 1989 sayılı kararlar doğrultusunda oluşturulan komitelerin listelediği kuruluşlara finansal destek sağlanması fiilini oluşturacağı belirtilmiştir⁶⁴⁴.

Temel hak ve özgürlüklerin korunması ve geliştirilmesi Birleşmiş Milletler'in amaçlarından biri olması ile birlikte, akıllı yaptırım kararları, bu amaca aykırı bir şekilde mülkiyet hakkı, seyahat özgürlüğü, adil yargılanma hakkı ve etkili başvuru hakkını ihlal etmeleri yönünden eleştirilmektedir⁶⁴⁵.

4.3.2. Avrupa Birliği Nezdinde Yapılan Düzenlemeler

Avrupa Birliği nezdindeki terörizmle mücadele ile ilgili önemli düzenlemelerden biri, 2002/475 sayılı Konsey Çerçeve Kararı'dır⁶⁴⁶. Kararın 2. Maddesinin 2. Fıkrasına

⁶⁴⁰ Tokgöz, 2022, s. 81.

⁶⁴¹ United Nations Security Council, S/RES/1617 (2005), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/446/60/PDF/N0544660.pdf?OpenElement> (Erişim: 07.05.2022)

⁶⁴² United Nations Security Council, S/RES/2170 (2014), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/508/49/PDF/N1450849.pdf?OpenElement> (Son Erişim: 07.05.2022)

⁶⁴³ Tokgöz, 2022, s. 94.

⁶⁴⁴ Tokgöz, 2022, s. 96.

⁶⁴⁵ Altınar Coşkun, 2022, ss.72-76.

⁶⁴⁶ The Council Of The European Union, 2002/475/JHA, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN> (Erişim: 09.05.2022)

göre terör örgütünün faaliyetlerine herhangi bir şekilde fon ya da maddi kaynak sağlanmasının örgüt faaliyetlerine iştirak olarak sayılacağı belirtilmiş, üye devletlerden bu tür faaliyetlerde bulunan kişilerin cezalandırılması talep edilmiştir. Bununla birlikte bu madde kapsamında sağlanan fonun, terör örgütünün suç teşkil eden faaliyetlerine katkıda bulunacağına bilinmesi gerekmektedir⁶⁴⁷.

Bununla birlikte Terörizmin finansmanının önlenmesine dair Avrupa Birliği nezdindeki temel belgenin, 2005/60 sayılı “Finansal Sistemin Karapara Aklama ve Terörizmin Finansmanı Amacıyla Kullanılmasının Önlenmesine Dair Direktif⁶⁴⁸” olduğu söylenebilir. Direktifin 1. maddesinde üye devletlerin karapara aklama ve terörizmin finansmanını yasaklaması gerektiği belirtilmiştir. Direktifin 2. maddesinde kredi kuruluşları, finansal kuruluşlar ve gerçek ve tüzel kişiler sayılarak bu kişi ve kuruluşlar direktifi uygulamakla yükümlü tutulmuştur. Direktifin devamında yer alan isimsiz hesap açılmasını yasaklayan, yüz yüze olmayan işlemler ve muhabir bankacılık işlemlerinin nasıl yürütülmesi gerektiği ve müşteriye özen ilkesi ile ilgili ayırtılı açıklamalar diğer önemli düzenlemelerdir⁶⁴⁹.

4.3.3. Avrupa Konseyi Nezdinde Yapılan Düzenlemeler

Avrupa Konseyi nezdinde yapılan en önemli düzenleme, 2005 tarihli “Terörizmin Finansmanı ve Suçtan Elde Edilen Gelirlerin Aklanması, Aranması, El Konması ve Müsaderesi Hakkındaki 198 Sayılı Avrupa Konseyi Sözleşmesi⁶⁵⁰”, kısaca “Varşova Sözleşmesi”dir. Sözleşmede Birleşmiş Milletler Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme’nin 2. maddesine atıfta bulunularak terörizmin finansmanı tanımlanmıştır. Bununla birlikte sözleşmede taraf devletlerin terörizmin finansmanı amacıyla kullanılan ya da bu amaç için tahsis edilen malvarlıklarının veya söz konusu suç gelirlerinin araştırılması, izlenmesi ve dondurulması konularında işbirliğine gidecekleri

⁶⁴⁷ Tokgöz, 2022, s. 106.

⁶⁴⁸ The European Parliament And The Council Of The European Union, Directive 2005/60/EC Of The European Parliament And Of The Council, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN> (Erişim: 07.05.2022)

⁶⁴⁹ Aydın ve Arslan, 2021, s. 94.

⁶⁵⁰ Council of Europe, Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, <https://rm.coe.int/168008371f> (Erişim: 09.05.2022)

vurgulanmıştır⁶⁵¹. Sözleşme'nin, terörizmle mücadelenin önleme boyutu ile terör mağdurlarının uğradığı zararların tazmin edilmesi konularını düzenleyen ilk bağlayıcı uluslararası hukuk sözleşmesi olması önemlidir⁶⁵².

Sözleşme Türkiye tarafından 28.03.2017 tarihinde imzalanıp 6665 sayılı uygun bulma kanunuyla 29.01.2016 tarihinde onaylanmıştır. Sözleşme, 19.02.2016 tarihli 29629 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Varşova Sözleşmesi'nin önemli bir yanı, terörizmin finansmanının sadece karapara aklama gibi yasa dışı yollarla değil, aynı zamanda hukuka uygun faaliyetler vasıtasıyla da sağlanabileceği gerekçesiyle daha önce çıkarılan sözleşmelere göre daha kapsamlı olmasıdır⁶⁵³.

4.3.4. FATF'nin 9 Özel Tavsiyesi

FATF, 1990 yılında karapara aklama ile ilgili 40 Tavsiye yayınlamıştır. 11 Eylül saldırılarından sonra FATF'nin mücadele görevinin kapsamı terörizmin finansmanının önlenmesi doğrultusunda genişletilmiş olup, daha önce yayınlanan 40 tavsiyeye ek, terörizmin finansmanının önlenmesine dair 9 Özel Tavsiye⁶⁵⁴ yayımlanmıştır. Tavsiyelerin 8'i 31.10.2011'de, 9.su ise 22.10.2004'te yayımlanmıştır.

Tavsiyelerden birincisi, “Birleşmiş Milletler belgelerinin onaylanması ve yürürlüğe konması” başlığına sahip olup; ülkelerin Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme'yi derhal onaylamaları ve 1373 sayılı Güvenlik Konseyi kararını derhal yürürlüğe koymaları belirtilmiştir.

Tavsiyelerden ikincisi, “Terörizmin finansmanının ve ilişkili kara para aklamanın suç haline getirilmesi” başlığına sahip olup, ülkelerin terörizmin finansmanının, terörist eylemlerin ve terörist organizasyonların suç kapsamına alınmasının sağlanması istenmiştir.

⁶⁵¹ Aydın ve Arslan, 2021, s. 94.

⁶⁵² Tokgöz, 2022, s. 120.

⁶⁵³ Tokgöz, 2022, s. 122.

⁶⁵⁴ FATF, FATF IX Special Recommendations, <https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf> (Erişim: 09.05.2022)

Tavsiyelerden üçüncüsü, “Terörist malvarlıklarının dondurulması ve müsaderesi” başlığına sahip olup, her ülkenin terörist malvarlıklarının gecikmeksizin dondurulması için gerekli adımları atmaları istenmiştir.

Tavsiyelerden dördüncüsü, “Terörizmle ilişkili şüpheli işlemlerin bildirilmesi” başlığına sahip olup, karapara aklamanın önlenmesine dair yükümlülükler sahip kuruluşların, terörizm, terörist faaliyetler ve terörist organizasyonlarla ilişkisi olabilecek şüpheli faaliyetleri bildirmesi gerekliliği vurgulanmıştır.

Tavsiyelerden beşincisi, “Uluslararası işbirliği” başlığına sahip olup, her ülkenin bir diğer ülkeye, terörizmin, terörist eylemlerin ve terörizmin finansmanına ilişkin davalar, idari araştırma ve soruşturmalar hakkında yardımda bulunması gerekliliği vurgulanmıştır⁶⁵⁵.

Tavsiyelerden altıncısı, “Alternatif havale” olup, para ve değer transferi sağlayıcılarının lisanslı ve kayıtlı olmaları sağlanarak banka ve diğer finansal kuruluşların tabi olduğu bütün FATF Tavsiyelerine tabi tutulmaları gerekliliği vurgulanmıştır.

Tavsiyelerden yedincisi, “Elektronik transfer” başlığına sahip olup, mali kuruluşların fon transferlerinde ve ilgili mesajlarda havaleyi yapan kişiye ilişkin tam ve makul bilgileri temin etmelerini gerekli kılmak için önlemler almaları belirtilmiştir⁶⁵⁶.

Tavsiyelerden sekizincisi, “Kar amacı gütmeyen kuruluşlar” olup, kar amacı gütmeyen kuruluşların terörizmin finansmanına yönelik oldukça savunmasız olduklarını ve kötüye kullanıma açık olduklarından hareketle eklenmiş bir tavsiyedir.

Tavsiyelerden dokuzuncu ve sonuncusu ise “Nakit Kuryeleri” başlığına sahip olup, ülkelerden nakit ve benzeri kıymetli evrakların yolcu beraberinde sınırlar arası transferi ile terörizmin finansmanının sağlanmasını engelleyici tedbirler almaları tavsiye edilmiştir.

Bununla birlikte yukarıda sayılan 9 Özel Tavsiye 2012 yılında diğer 40 Tavsiye ile bir araya getirilerek tekrar yayınlanmıştır⁶⁵⁷. Güncellenmiş tavsiyelerden özellikle 15 ve 16 numaralı tavsiye, bu çalışmanın da konusunu oluşturan kripto paralar ile ilgili düzenlemeler içerip, ilgili bölüm altında incelenecektir.

⁶⁵⁵ Tokgöz, 2022, s. 129.

⁶⁵⁶ Tokgöz, 2022, s. 130.

⁶⁵⁷ FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (Erişim: 09.05.2022)

Suçtan elde edilen mal varlığı değerlerinin yaygın şekilde terörizmin finansmanında kullanılması nedeniyle bu iki suç ulusal ve uluslararası belgelerde birlikte düzenlenmektedir. Fakat bu iki suçun zorunlu olarak birbirlerine bağlı oldukları anlamına gelmemektedir. Suçtan kaynaklanan malvarlığı değerlerini aklama suçu için öncül bir suç ve suçtan kaynaklanan mal varlığı bulunmalıdır. Terörizmin finansmanının konusunu oluşturan fon ya da malvarlığı ise yasadışı yoldan elde edilmiş olabileceği gibi yasal yoldan da elde edilmiş olabilir⁶⁵⁸.

4.4. Türk Hukukunda Terörizmin Finansmanı Suçu Ve Önlenmesi

Türk Hukukunda terörizmin finansmanı suçu ile ilgili temel düzenlemeyi 6415 sayılı “Terörizmin Finansmanının Önlenmesi Hakkında Kanun⁶⁵⁹” teşkil etmektedir. Bununla birlikte 6415 sayılı Kanun yürürlüğe girmeden önce; terörizmin finansmanı olarak değerlendirilebilecek fiiller ilk olarak 765 sayılı Türk Ceza Kanunu⁶⁶⁰’nun 169. Maddesinde belirtilen “silahlı çeteye yardım” kapsamında değerlendirilmekteydi. 5237 sayılı Türk Ceza Kanunu⁶⁶¹ ve 3713 sayılı terörle Mücadele Kanunu⁶⁶²’nun 29.06.2006 tarihine kadar birlikte kullanıldığı dönemde ise terörizmin finansmanına ilişkin eylemler; Terörle Mücadele Kanunu’nun 7. maddesi uyarınca “örgüt mensuplarına yardım” ve bu maddenin Türk Ceza Kanunu’nun 220. maddesinin 7. fıkrasında düzenlenen silahlı örgüte yardım hakkındaki hükmüne yaptığı atıf ile, Türk Ceza Kanunu’nun 314. maddesinde düzenlenen silahlı örgüt suçuna ilişkin genel hükümlere göre cezalandırılmaktaydı⁶⁶³. Ardından 29.06.2006 tarihinde “Terörle Mücadele Kanununda Değişiklik Yapılmasına Dair Kanun⁶⁶⁴” yürürlüğe girmiş, bu kanun ile birlikte Terörle Mücadele Kanunu’na “terörün finansmanı” başlıklı sekizince madde eklenerek, terörizmin finansmanı suçu ilk kez ayrı bir suç olarak hüküm altına alınmıştır. 7.02.2013 tarihinde TBMM tarafından

⁶⁵⁸ Aydın ve Arslan, 2021, s. 89.

⁶⁵⁹ R.G., T: 7/2/2013, S: 28561.

⁶⁶⁰ R.G., T: 1/3/1926, S: 320 (mülga).

⁶⁶¹ R.G., T: 12/10/2004, S: 25611.

⁶⁶² R.G., T: 12/4/1991, S: 20843 Mükerrer.

⁶⁶³ Yılmaz, Yeşim, Terörizmin Finansmanı Suçu, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 2020/17, s. 201. <https://dergipark.org.tr/en/download/article-file/1249893> (Erişim: 10.05.2022); Tokgöz, 2022, ss. 136-137.

⁶⁶⁴ R.G., T: 18/7/2006, S: 26232.

kabul edilen 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkındaki Kanun ile birlikte Terörle Mücadele Kanunu'nun ilgili maddesi mülga olmuştur.

4.4.1. Terörizmin Finansmanı Suçu

Terörizmin finansmanı suçu yukarıda da belirtildiği üzere 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun'da düzenlenmiştir. Kanun'da Terörle Mücadele Kanunu'nun mülga 8. maddesindeki “terörün finansmanı” ifadesi yerine “terörizmin finansmanı” ifadesi benimsenmiştir. Kanun'un 1. maddesinde kanunun amacının “*terör ve terörizmin finansmanı ile etkin mücadele edilmesi kapsamında; 1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşmenin ve Birleşmiş Milletler Güvenlik Konseyinin bu Kanun kapsamındaki terör ve terörizmin finansmanı ile mücadeleyle ilişkin kararlarının uygulanması ile terörizmin finansmanı suçunun düzenlenmesi ve terörizmin finansmanının önlenmesi amacıyla malvarlığının dondurulmasına ilişkin usul ve esasların belirlenmesi*” olduğu belirtilmiştir.

4.4.1.1. Suçun Konusu

Suçun hukuki ve maddi olmak üzere iki konusu bulunmaktadır⁶⁶⁵. İki kavram birbirinden tamamen ayrı kavramlar olarak değerlendirilemezler; aralarında doğrudan doğruya olmayan bir ilgi söz konusudur. Erem'e göre maddî konu üzerindeki bir etkinin, hukukî konuda yansımadağı iddia edilemez⁶⁶⁶.

Bununla birlikte doktrinde suçun konusu, suçun maddi konusunu ifade edecek şekilde de kullanılabilir⁶⁶⁷. Örneğin Özgenç ve Üzülmöz'e göre fiilin ihlal ettiği hukuki değer ile suçun konusu aynı olmayıp, suçun konusu “üzerinde fiilin icra edildiği eşya veya şahsın fiziki, maddi yapısı” olarak tanımlanmaktadır. Sözüer'e göre suçun konusu, “suçun üzerinde gerçekleştiği kişi veya şey”dir⁶⁶⁸.

⁶⁶⁵ Centel, Nur vd., “Türk Ceza Hukukuna Giriş, (11. Baskı), Beta, İstanbul 2020, s. 236.; Erem, Faruk, “Suçun Konusu ve Hümanist Doktrin”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 1968/25 (1-2), s. 12. <https://dergipark.org.tr/en/download/article-file/632330> (Erişim. 11.05.2022)

⁶⁶⁶ Erem, 1968, s. 24.

⁶⁶⁷ Özgenç, İ. ve İ. Üzülmöz, *Ceza Genel Hukuku*, (4. Baskı), Seçkin, Ankara 2021, s. 48.

⁶⁶⁸ Sözüer, Adem, “Ceza Hukuku Uygulama Rehberine Giriş ve Pratik Çalışma Notu”, İstanbul Üniversitesi Hukuk Fakültesi Ceza Hukuku ve Kriminoloji Araştırma ve Uygulama Merkezi, 2015, s. 12.

4.4.1.1.1. Suçun Hukuki Konusu

Doktrinde Toroslu tarafından suçun hukuki konusu “Suçtan doğrudan doğruya zarar gören şahsa veya şahıs topluluğuna, yani suçun pasif süjesine ait özel bir varlıktır (veya menfaat).” olarak tanımlanmıştır⁶⁶⁹. Hafizoğulları ve Özen’e göre de suçun hukuki konusundan; hukukça korunan, hukuk ile korunmasından ötürü “hukuki değer” veya “hukuki menfaat” olarak adlandırılan, ceza normunun bir ceza tehdidi ile olası saldırılardan korumayı amaçladığı “şey” anlaşılmaktadır⁶⁷⁰. Yazarlara göre menfaat ve değer kavramları farklı anlamlar içerse de, aynı gerçeği iki farklı şekilde ifade ettiklerinden birbirilerinin yerine kullanılmalarında sakınca yoktur⁶⁷¹. Benzer bir şekilde Erem; Toroslu ve Toroslu’ya göre de suçun hukuki konusu, “bir kanun kuralı ile korunan ve suçun ihlâl ettiği hak/hukuki varlık⁶⁷² veya menfaati” ifade etmektedir⁶⁷³. Centel vd. ise suçun hukuki konusunu “suç türünün değişmesiyle değişen ve suçla ihlal edilen hukuki varlık ya da hukuki çıkar” olarak tanımlamaktadır⁶⁷⁴. Bununla birlikte doktrinde, “suç ile korunan hukuki değer” ifadesinin hatalı bir ifade olduğu ve “suç ile ihlal edilen ve ceza ile korunan hukuki değer” şeklinde bir kullanımın daha doğru olacağı belirtilmektedir⁶⁷⁵. Terörizmin finansmanı ile ilgili literatür incelendiğinde, suçun hukuki konusunu ele alan ve almayan farklı yaklaşımlar olduğundan dolayı bu çalışmada; Hafizoğulları ve Özen’in yukarıdaki kapsayıcı tanımlamasından faydalanılarak terörizmin finansmanı suçunun “hukuki konusu” ile suçun düzenlenmesi ile “korunmak istenen hukuki değer” birlikte incelenmiştir. Zira korunmak istenen varlık; hukuki değer veya hukuki menfaatten oluşmakta ve suçun hukuki konusunu teşkil etmektedir⁶⁷⁶.

⁶⁶⁹ Toroslu, Nevzat, Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Savaş Yayınevi, Ankara 2019, s. 164.

⁶⁷⁰ Hafizoğulları Z. ve M. Özen, Türk Ceza Hukuku Genel Hükümler, (5. Baskı), US-A Yayıncılık, Ankara 2012, s. 225.

⁶⁷¹ Hafizoğulları ve Özen, 2012, s. 225.

⁶⁷² Toroslu ve Toroslu tarafından “hukuki varlık” şeklinde ifade edilmektedir.; Toroslu, N. ve H. Toroslu, Ceza Hukuku Genel Kısım, (26. Baskı), Savaş Yayınevi, Ankara, 2021, s. 110.

⁶⁷³ Erem, 1968, s. 12.; Toroslu ve Toroslu, 2021, s. 110.

⁶⁷⁴ Centel vd., 2020, s. 236.

⁶⁷⁵ Hafizoğulları ve Özen, 2012, ss. 170, 231.

⁶⁷⁶ Hafizoğulları Z. ve M. Özen, Türk Ceza Hukuku Genel Hükümler, (13. Baskı), US-A Yayıncılık, Ankara 2021, s. 199.

Doktrinde terörizm finansmanı suçu ile ihlal edilen ve korunmak istenen tek bir hukuki değer olduğu ya da birden fazla değer olduğunu belirten farklı görüşler bulunmaktadır⁶⁷⁷.

Aydın ve Arslan'a göre terörizmin finansmanı suçunun hukuki konusunu, terör suçlarıyla korunan hukuki değerler oluşturur. Buna göre bireylerin ve toplumun güvenliğinin yanı sıra toplumsal düzen ve devletin anayasal düzeninin korunması bu suçun hukuki konusunu oluşturmaktadır.

Bununla birlikte Çetin'e göre korunmak istenen hukuki yarar sadece ülke içerisinde bulunan kimselere özgü değildir. Çetin'e göre Terörizmin Finansmanının Önlenmesi Hakkında Kanun'un 4. Maddesinin 5. Fıkrası gereğince; suçun, yabancı bir devlet veya uluslararası bir kuruluş aleyhine işlenmesi durumunda, Adalet Bakanlığı'nın talebi üzerinde de olsa soruşturma ve kovuşturma yapılmaktadır. Buradan hareketle Çetin, korunmak istenen hukuki yararın sadece ülke içerisinde yaşayanların değil, yabancı ülkelerde yaşayan insanların da yararının korunması olduğunu düşünmektedir⁶⁷⁸. Çetin'e göre burada korunmak istenen hukuki yarar, insan yaşamı ve vücut bütünlüğü ile insanların huzur ve sükun içerisinde yaşama haklarıdır⁶⁷⁹. Çetin'e benzer bir şekilde, Aydın ve Arslan da terörizmin finansmanı suçu düzenlemesi ile uluslararası sözleşmelerden hareketle uluslararası toplumun genel menfaatlerinin korunduğunun amaçlandığını belirtmektedir.

Bununla birlikte doktrinde terörizmin finansmanı suçu ile korunan hukuki değer veya menfaatin, "terör örgütlerinin mali gücünü ortadan kaldırmak veya zayıflatmak yoluyla terör suçlarının önüne geçmek ve toplumu bu suçların ağır sonuçlarından korumak" olduğu da belirtilmektedir⁶⁸⁰. Gödekli ise terörizmin finansmanının terör eylemlerinin gerçekleştirilebilmesini sağladığını ve bu nedenle terörizmin finansmanının cezalandırılmasındaki temel amacın terör suçlarını henüz gerçekleşmeden engellemek amacını taşıdığından hareketle, terörizmin finansmanı suçu düzenlemesi ile korunmak istenen hukuki değer, terör eylemlerinin cezalandırılması ile korunan hukuki değer ile eşdeğer olduğunu belirtmektedir⁶⁸¹.

⁶⁷⁷ Tokgöz, 2022, ss. 148-149.

⁶⁷⁸ Çetin, Soner Hamza, Terörizmin Finansmanı Suçu, Bilge Yayınevi, (1. Baskı), Ankara, 2017, s. 36.

⁶⁷⁹ Aydın ve Arslan, 2021, s. 100.

⁶⁸⁰ Gödekli, Mehmet, "Terörizmin Finansmanı Suçu", (yüksek lisans tezi), Atatürk Üniversitesi, Kamu Hukuku Anabilim Dalı, Erzurum, 2013, s. 229.

⁶⁸¹ Gödekli, 2013, ss. 229-230.

4.4.1.1.2. Suçun Maddi Konusu

Suçun maddi konusu, suçun maddeten etkilerini üzerinde gösterdiği varlıktır; bu varlık bir kimse olabileceği gibi bir şey de olabilir⁶⁸².

Terörizmin finansmanı suçunun maddi konusu, teröriste ya da terör örgütüne sağlanan ya da toplanan fon⁶⁸³ olarak kabul edilebilir. Özgenç'e göre fon ibaresi, ekonomik değeri olan her türlü malvarlığı değerini kapsamaktadır⁶⁸⁴. Benzer bir şekilde Çetin de, Terörizmin Finansmanının Önlenmesi Hakkında Kanun'da sayılan amaçların gerçekleştirilmesi için sağlanan veya toplanan para veya değeri para ile temsil edilebilen taşınır veya taşınmazlar; maddi veya gayrimaddi her türlü mal, hak, alacak ile bunları temsil eden her türlü belge bu suçun maddi konusunu oluşturabileceğini ifade etmektedir⁶⁸⁵.

Bununla birlikte fonun kripto para olması durumunda, kripto paranın suçun maddi konusunu oluşturup oluşturmadığı şeklinde teorik birtakım sorunlar ortaya çıkabilir. Doktrinde suçun maddi konusunun “insan” olduğu durumlarda, insanın hem fiziki yönü ile hem de psikik yönü ile maddi konu olabileceği kabul edilebilmektedir⁶⁸⁶. Fakat suçun maddi konusunun bir “şey” olduğu durumlarda bu şeyin cismani olması gerektiği belirtilmektedir⁶⁸⁷. Kriptografik işlemlerin birleşerek oluşturduğu bloklara dayanan blok zincir üzerinde işleyen kripto paraların doktrindeki anlamıyla cismani olmadığı söylenebilir. Bu doğrultuda maddi konunun cismani olması gerektiğinin kabulü, terörizmin finansmanın kripto paralar ile gerçekleştirilmesi halinde suçun maddi konusunun olmaması nedeniyle teoride maddi konunun bulunmadığı hallerde ortaya çıkan işlenemez suç⁶⁸⁸ (elverişsiz teşebbüs⁶⁸⁹) haline geleceği şeklinde sakıncalı bir sonuca ulaştırabilir. Belirtmek gerekir ki doktrinde (aksi görüşler olmakla birlikte⁶⁹⁰) bazı

⁶⁸² Hafizoğulları ve Özen, 2012, s. 233.; Toroslu, 2019, s. 183.

⁶⁸³ Özgenç, İzzet, Suç Örgütleri, (14. Baskı), Seçkin, Ankara, 2022, s. 180.; Tokgöz, 2022, s. 151.

⁶⁸⁴ Özgenç, 2022, s. 180.

⁶⁸⁵ Çetin, 2017, s. 42.

⁶⁸⁶ Toroslu, 2019, ss. 184-185.; Toroslu ve Toroslu, 2021, s. 112

⁶⁸⁷ Centel vd., 2020, s. 236.; Heinrich, Bernd, Ceza Hukuku Genel Kısım – 1, (ed. Yener Ünver), (çev. Hakan Hakeri vd.), (1. Baskı), Adalet Yayınevi, Ankara, 2014, ss. 80, 441; Özgenç ve Üzülmöz, 2021, s. 48.; Toroslu, 2019, s. 186.; Toroslu ve Toroslu, 2021, s. 112.

⁶⁸⁸ Centel vd., 2020, s. 479.; Hafizoğulları ve Özen, 2021, s. 317.; Toroslu ve Toroslu, 2021, s. 314.;

⁶⁸⁹ Heinrich, 2014, ss. 440-441.

⁶⁹⁰ Karşıt görüşler için bkz. Koç, Coşkun, “Suçun Konusunun Yokluğu Durumunda Teşebbüse Elverişlilik Sorunu”, TBB Dergisi, 2020 (147), s. 54. <http://tbbdergisi.barobirlik.org.tr/m2020-147-1903> (Erişim: 13.07.2022)

suçların düzenleniş biçimleri sebebiyle maddi konularının bulunmadığı belirtilmektedir⁶⁹¹. Fakat bu suçların düzenlenişleri itibariyle maddi konuları bulunmamaktadır; elimizdeki durumda ise düzenleniş biçimi ile halihazırda maddi konusu bulunan bir suçun (terörizmin finansmanı) ve üzerinde davranışın⁶⁹² gerçekleştirildiği fakat doktrine göre cismani olmayan ve maddi konu kabul edilmeyen bir şey (kripto para) bulunmaktadır. Bu durumda doktrindeki görüşler takip edilip maddi konunun bulunmadığı kabul edilerek, işlenemez suçun meydana geldiğinden hareketle teşebbüs hükümlerinin uygulanması, gerek 6415 sayılı Kanunun gerek ise Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme amacına ters düşecektir. Kanunun amacı, terör eylemlerinin gerçekleşmesinin kaynağı olan finansmanın önlenmesidir. Bir şey nasıl tanımlanıyor olursa olsun, ekonomik bir değere ya da kıymete⁶⁹³ sahip ise terör eylemlerinin gerçekleştirilmesini sağlayabilecek nitelikte olacaktır. Yine de aşağıda ayrıntılı bir şekilde incelendiği üzere kripto paraların 6415 sayılı Kanun uyarınca hukuken “fon” sayılmalarına bir engel de bulunmamaktadır. Doktrinde yukarıdaki görüşlerin aksine, gayrimaddi şeylerin de suçun maddi konusunu oluşturabileceği belirtilmektedir⁶⁹⁴. Bu doğrultuda suçun maddi konusunun cismani olmasına (çoğunlukla el ile dokunulabilir, göz ile görülebilir anlamıyla) yönelik fikre katılmak mümkün gözükmemektedir. Zira, üzerinde suçun meydana geldiği şey, suçun maddi konusunu oluşturur⁶⁹⁵; kripto paralar failin hareketinin üzerinde icra edilmesine⁶⁹⁶ müsait şeylerdir; aktarılabilirler, saklanabilirler, ortadan kaldırılabilirler (burn/burning). Sonuç olarak kripto paraların fon olarak suçun maddi konusunu oluşturduğunu kabul etmek gerekir.

⁶⁹¹ Erem, 1968, ss. 20, 31.; Toroslu ve Toroslu, 2021, s. 112.

⁶⁹² Toroslu ve Toroslu, 2021, s. 111.

⁶⁹³ Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme'nin 1. maddesindeki fon tanımı “*her türlü kıymet*” şeklinde oldukça geniş ele alınmıştır.

⁶⁹⁴ Santoro, Arturo, Manuale di diritto penale, vol. II. Torino, 1962, s. 299'dan akt. Toroslu, 2019, s. 186.; Gianniti Francesco, L'oggetto materiale del reato, Milano, 1966, s. 110'dan akt. Erem, 1968, s. 17.

⁶⁹⁵ Alimena, Bernardino, Del concorso di reati e di pene, 1903, ss. 399-400'den akt. Toroslu, 2019, s. 183.

⁶⁹⁶ Toroslu, 2019, ss. 60-61'deki suçun maddi konusu tanımı izlenerek bu ifade kullanılmıştır.

4.4.1.2. Fiil

Ceza hukukunda kural olarak fiilsiz suç olmaz⁶⁹⁷. Ceza Hukukundan kaynaklanacak bir sorumluluğun var olabilmesinin temel koşulu, somut olayda bir insan davranışının bulunmasıdır⁶⁹⁸. Türkiye Cumhuriyeti Anayasası⁶⁹⁹'nın 38. maddesinde ve Türk Ceza Kanunu'nun 2. Maddesinde, her ne kadar TCK'nın birtakım maddelerinde bu kural kanun koyucu tarafından ihlal edilmiş olsa da⁷⁰⁰, fiilsiz suç olmayacağı kuralı pekiştirilmiştir⁷⁰¹.

Terörizmin Finansmanının Önlenmesi Hakkında Kanun'un 3. maddesinde “*Aşağıda sayılan fiillerin gerçekleştirilmesi amacıyla fon sağlanması veya toplanması yasaktır*” denilerek bu suçun fiil unsuru belirtilmiştir. Buna göre bu suçu oluşturan fiiller “fon sağlamak” ve “fon toplamak”tır. Kanun maddesine göre “sağlamak” ve “toplamak” seçimlik hareket olarak belirtilmiştir. Seçimlik hareketli bu suçta, iki hareketin de birlikte meydana gelmesi halinde (fon toplama ve sağlama) yalnızca bir terörizmin finansmanı suçu oluşacaktır⁷⁰². Fakat her halükarda seçimlik hareketli suçlarda bir suçun meydana geldiğini kabul etmek için seçimlik hareketlerin aynı konu üzerinde gerçekleştirilmiş olmaları gerekir⁷⁰³. Bununla birlikte doktrinde seçimlik hareketli suçlarda birden fazla hareketin yapıldığı durumlarda, kanunda belirtilen hareketlerden biri yapılsa bile suçun oluşmasını sağlamasından dolayı cezalandırılanın ilk hareket olduğu belirtilmektedir. Cezalandırılmayan sonraki hareketlere katılanların ise suç ortağı olarak cezalandırılmalarının mümkün olduğu belirtilmektedir.

Terörizmin finansmanı suçu kapsamında fon sağlama ve toplama hareketleri suçun oluşması için yeterli olup, zarar doğması gibi ayrıca bir neticenin gerçekleşmesine gerek yoktur⁷⁰⁴. Bununla birlikte toplanan ya da sağlanan fonun kullanılmasına da gerek yoktur; bu durum kanun koyucu tarafından Kanun'un 4. maddesinin 3. fıkrasında “*ceza*

⁶⁹⁷ Centel vd., 2020, s. 240.; Hafizoğulları Z. ve M. Özen, Türk Ceza Hukuku Genel Hükümler, (13. Baskı), US-A Yayıncılık, Ankara, 2021, s. 167; Özgenç ve Üzülmöz, 2021, s. 43.; Toroslu ve Toroslu, 2021, s. 133.

⁶⁹⁸ Heinrich, 2014, s. 106.

⁶⁹⁹ R.G., T: 9/11/1982, S: 17863 (Mükerrer).

⁷⁰⁰ Hafizoğulları ve Özen, TCK'nın 216. maddesinde düşünce, inanç ve kanaatin kendisinin suç sayılması ile; aynı kanunun 267. maddesinde de “basın ve yayın yoluyla” iftira suçunun kabul edilmesiyle fiilsiz suç olmaz ilkesinin ihlal edildiğini düşünmektedir.; Hafizoğulları ve Özen, 2012, s. 194.

⁷⁰¹ Hafizoğulları ve Özen, 2012, s. 194.

⁷⁰² Centel vd, 2020, s. 268; Özgenç ve Üzülmöz, 2021, s.46; Tokgöz, 2022, s. 156; Çetin, 2017, ss. 44-45.

⁷⁰³ Tokgöz, 2022, s. 156.

⁷⁰⁴ Tokgöz, 2022, s. 154.; Çetin, 2017, s. 45.

verilebilmesi için fonun bir suçun işlenmesinde kullanılmış olması şartı aranmaz.” şeklinde hüküm altına alınmıştır. Sonuç olarak terörizmin finansmanı suçunun zararın aranmıyor olması nedeniyle tehlike suçu; netice aranmaması nedeniyle de sırf hareket suçu olarak belirtilmesi mümkündür⁷⁰⁵.

Fon sağlamak, terörizmin finansmanında kullanılacak fonun temin edilmesine yönelik her türlü faaliyeti kapsamaktadır⁷⁰⁶. Fon toplamak ise fon olarak gösterilen değerlerin alınması, kabul edilmesi ve biriktirilmesidir⁷⁰⁷. Belirtmek gerekir ki, fon toplama fiilinin kişilere karşı yağma suçunu oluşturacak derecede cebî veya tehdit içermemesi gerekir; zira böyle bir durumda TCK madde 149 uyarınca yağma suçunun oluştuğu kabul edilir⁷⁰⁸.

Yargıtay’a göre sağlanan ya da toplanan fonun paradan ibaret olması gerekliliği bulunmamakta; değeri para ile temsil edilebilen herhangi bir varlık da kapsama dâhil edilmektedir⁷⁰⁹. Bununla birlikte Yargıtay’ın da katıldığı görüşe göre⁷¹⁰, toplanan ya da sağlanan fonun miktarının bir önemi yoktur⁷¹¹.

4.4.1.3. Fail

Terörizmin Finansmanının Önlenmesi Hakkında Kanun’un 4. Maddesinde fail yönünden herhangi bir özellik aranmamıştır; dolayısıyla terörizmin finansmanı suçu genel suç olup⁷¹², bu suçun faili herhangi bir gerçek kişi olabilir⁷¹³. Bununla birlikte Yargıtay’ın da kabul ettiği bir görüşe göre terörizmin finansmanı suçunun fon sağlanan ya da toplanan terör örgütünün kurucusu, yöneticisi veya üyesi tarafından işlenemeyeceği belirtilmektedir⁷¹⁴; bu duruma gerekçe olarak bu şekildeki bir fiilin örgüt yöneticiliği ve üyeliği suçunu oluşturan fiil kapsamında değerlendirilmesi gerekeceği öne

⁷⁰⁵ Tokgöz, 2022, ss. 154-155.; Çetin, 2017, s. 45.

⁷⁰⁶ Aydın ve Arslan, 2021, s. 102.

⁷⁰⁷ Çetin, 2017, s. 44.

⁷⁰⁸ Özgenç, 2022, s. 183.

⁷⁰⁹ Tokgöz, 2022, s. 156.

⁷¹⁰ Yargıtay Ceza Genel Kurulu, 12.3.2019 T., 2017/16-691 E., 2019/202 K.

<https://rayp.adalet.gov.tr/resimler/552/dosya/2019-ycgk-finansman06-01-202115-39.doc> (Erişim: 11.05.2022)

⁷¹¹ Aydın ve Arslan, 2021, s. 101.

⁷¹² Tokgöz, 2022, s. 158.

⁷¹³ Aydın ve Arslan, 2021, s. 100.

⁷¹⁴ Yargıtay Ceza Genel Kurulu, 13.2.2018 T., 2017/692 E., 2018/41 K.; Yargıtay Ceza Genel Kurulu, 12.3.2019 T., 2017/691 E., 2019/202 K.; Yılmaz, 2020, s. 210.

sürülmüştür⁷¹⁵. Yargıtay'ın bu içtihadı sonrasında FATF tarafından Türkiye'ye yöneltilen eleştiriler dikkate alınarak⁷¹⁶ 2020 yılında 7262 sayılı kanun⁷¹⁷ ile 6415 sayılı Kanunun 4. Maddesine ikinci fıkra olarak, “Birinci fıkrada sayılan fiillerin, örgütü kuran veya yöneten ya da örgüt üyesi tarafından gerçekleştirilmesi hâlinde bu kişiler hakkında örgüt kurmak, yönetmek veya örgüte üye olmak suçları uyarınca verilecek ceza üçte birine kadar artırılır.” hükmü eklenmiştir. Özgenç'e göre getirilen bu hüküm ile Yargıtay'ın söz konusu içtihadı etkisizleştirilmiş olsa da, FATF eleştirisine tekrardan maruz kalınacaktır⁷¹⁸.

Yargıtay'ın yukarıdaki içtihadının aksini savunanlara göre, terörizmin finansmanı suçunun ayrı bir kanun ile ayrı bir şekilde düzenlenmiş olması; terör eyleminin örgüt üyesi tarafından da finanse edilebileceğini, bu durumda birden fazla suç oluşacağının örtülü kabulü anlamına gelmektedir⁷¹⁹. Bununla birlikte Kanunun 4. Maddesine eklenen 2. Fıkranın şeklindeki fıkranın da bu görüşü desteklediği belirtilmektedir⁷²⁰. Fon sağlama veya toplama fiillerini gerçekleştiren kişilerin terör örgütü kurucusu, yöneticisi veya üyesi olma ihtimalleri, bu çalışmanın aşağısında, “Suçun özel görünüş biçimleri” başlığı altında tekrar irdelenecektir.

Son olarak belirtmek gerekir ki, her ne kadar fon sağlayan ya da toplayan kişi örgüt dışından olsa da, bu davranışların süreklilik kazanması söz konusu olduğunda failin terör örgütü üyesi olması ihtimalinin değerlendirilmesi gerekecektir⁷²¹.

4.4.1.4. Mağdur

Her suçun bir mağduru bulunur⁷²². Bir suçun mağduru, suç ile ihlal edilen ve ceza ile korunan, yani normun koruduğu hukuki değer veya menfaatin hamili konumunda olan kimsedir⁷²³. Genel itibarıyla literatürde, terörizmin finansmanı suçunun mağdurunun, toplumu oluşturan tüm bireyler olduğu belirtilmektedir⁷²⁴. Bu kaniya terörizmin

⁷¹⁵ Aydın ve Arslan, 2021, s. 100.

⁷¹⁶ Özgenç, 2022, s. 182.

⁷¹⁷ R.G., T: 31/12/2020, S: 31351 (5. Mükerrer).

⁷¹⁸ Özgenç, 2022, s. 183.

⁷¹⁹ Tokgöz, 2022, s. 171.

⁷²⁰ Tokgöz, 2022, ss. 171-172.

⁷²¹ Yargıtay Ceza Genel Kurulu, 13.2.2018 T., 2017/9-692 E., 2018/41 K.

⁷²² Özgenç ve Üzülmüş, 2021, s. 52; Toroslu, 2019, s. 198.; Toroslu ve Toroslu, 2021, s. 113.

⁷²³ Hafizoğulları ve Özen, 2012, s. 233.; Toroslu, 2019, s. 198.

⁷²⁴ Aydın ve Arslan, 2021, s. 101; Çetin, 2017, s. 41.; Tokgöz, 2021, s. 158.; Yılmaz, 2020, s. 216.

finansmanı suçunun mağdurunun, terör suçlarının mağduru ile aynı olması kabulü ile ulaşılmaktadır⁷²⁵. Bununla birlikte finanse edilen terör eyleminin doğrudan yöneldiği kimselerin de mağdur olarak belirtildiği görülmektedir⁷²⁶. Bu durumda toplumu oluşturan bireyler geniş anlamda mağdur; belirli kişi veya kişiler ise dar anlamda mağdur olarak ifade edilmektedir⁷²⁷.

Yukarıda yapılan tanımdan hareketle suçun mağduru, suçun hukuki konusundan hareketle belirlenebilir⁷²⁸. Terörizmin finansmanı suçunun hukuki konusu hakkındaki görüşlerin oldukça geniş anlamlar ifade ettiği hesaba katıldığında, suçun mağduru hakkındaki görüşlerin de toplumu oluşturan tüm bireyler olduğu görülmektedir. Fakat toplumu oluşturan tüm bireyler şeklindeki bir ifadenin, toplumdaki herkesin birey olarak “tek tek” mağdur olması anlamına gelebileceği ve bu anlamın mağdur kavramının kapsamını aşırı bir şekilde genişleteceği düşünülmektedir⁷²⁹. Mağdurun toplumu oluşturan “birey” olması⁷³⁰ fikri, CMK’da mağdur ile ilgili hükümlerin uygulanması hususunda da karışıklık yaratabilecektir⁷³¹.

Mağdurun toplum ya da aile gibi tüzel kişiliği bulunmayan topluluklar olamayacağı hakkında görüşler bulunmaktadır. Bu görüşlere göre bu tür topluluklar gerçek ve tüzel kişiler gibi hukuk sükeleri olmadığından suçun mağduru, pasif sükjesi olarak kabul edilemezler⁷³². Aile ya da toplumu suç mağduru olarak kabul etmeyen anlayış, topluma, aileye ya da kamuya yönelen suçları “mağduru belli bir kişi olmayan suçlar” olarak adlandırmaktadır⁷³³. Katoğlu’na göre toplumun suçun mağduru olamayacağı ve topluma karşı suç işlenemeyeceği düşüncesinden yola çıkılarak kabul edilen “mağduru belli bir kişi olmayan suç” kavramı, suçun mağduru kavramının sınırlandırılmasına değil, tam aksine bu kavramının sınırlarının ölçüsüzce genişlemesine yol açmaktadır⁷³⁴. Salt birey merkezli bu cezai koruma anlayışının yerine kollektif nitelik

⁷²⁵ Gödekli, 2013, s. 243.

⁷²⁶ Tokgöz, 2021, s. 158.; Yılmaz, 2020, s. 216.

⁷²⁷ Artuk vd., Ceza Hukuku Genel Hükümler, 12. Baskı, Adalet Yayınevi, Ankara, 2018.’den akt. Yılmaz, 2020, s. 216.

⁷²⁸ Katoğlu, Tuğrul, “Ceza Hukukunda Suçun Mağduru Kavramının Sınırları”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2012/61 (2), s. 661. <https://dergipark.org.tr/tr/download/article-file/624032> (Erişim: 12.05.2022)

⁷²⁹ Katoğlu, 2012, s. 677, 689-690.

⁷³⁰ Yılmaz, 2020, s. 216.

⁷³¹ Katoğlu, 2012, s. 684.

⁷³² Katoğlu, 2012, s. 678.

⁷³³ Katoğlu, 2012, s. 679.

⁷³⁴ Katoğlu, 2012, s. 690.

taşıyan varlık ya da menfaatlerin de korunabileceği kabul edilmelidir. Bu doğrultuda toplumun suçun mağduru olabileceği kabul edilmeli, menfaatleri somut olarak zarar görenler ise suçtan zarar gören olarak kabul edilecektir⁷³⁵.

Bu doğrultuda doktrindeki suçun mağdurunun toplum olabileceğine ilişkin görüşten hareketle⁷³⁶, terörizmin finansmanı suçunun mağdurunun “toplumu oluşturan bireyler” ya da “toplumu oluşturan herkes” şeklinde ifade edilmesi yerine mağdurun “toplum” olarak ifade edilmesi daha doğru olacaktır.

4.4.1.5. Manevi Unsur

Suçun manevi unsuru, icra veya ihmal hareketinin şuurlu ve iradi olmasını gerektirmekte; bu da, kast ve taksir olmak üzere iki şekilde ortaya çıkmaktadır⁷³⁷.

Terörizmin Finansmanının Önlenmesi Hakkında Kanun’un 4. maddesinde terörizmin finansmanı suçundan bahsedilirken “kullanılması amacıyla veya kullanılacağını bilerek ve isteyerek” denilerek suçun sadece doğrudan kast ile işlenebileceği öngörülmüştür. Bu doğrultuda terörizmin finansmanı suçunun sadece doğrudan kast ile işlenebileceği; olası kast ya da taksir ile işlenemeyeceği söylenebilir⁷³⁸. Özgenç, kişinin fiili işlediği sırada, fon sağladığı veya topladığı örgütsel yapının bir terör örgütü olduğunu bilmesi gerektiğini; sırf hayır düşüncesiyle bağışta bulunan kişinin fiilinin suç oluşturmayacağını belirtmektedir⁷³⁹.

4.4.1.6. Hukuka Aykırılık Unsuru

Hukuka aykırılık, fiil ile hukuk düzeni arasındaki çelişkiyi ifade eder⁷⁴⁰. Literatürde terörizmin finansmanı suçunun hukuka aykırılık hususunda bir özellik göstermeyeceği belirtilmiştir⁷⁴¹. Bununla birlikte hukuka uygunluk nedenleri de koşulları

⁷³⁵ Katoğlu, 2012, ss. 683-684.

⁷³⁶ Hafizoğulları ve Özen, 2021, s. 209.; Katoğlu, 2012, s. 683.; Toroslu, 2019, s. 173, 182.

⁷³⁷ Hafizoğulları ve Özen, 2012, s. 265.

⁷³⁸ Aydın ve Arslan, 2021, s. 194.; Çetin, 2017, ss. 50-51.; Özgenç, 2022, s. 184.; Tokgöz, 2022, ss. 159-160.

⁷³⁹ Özgenç, 2021, s. 184.

⁷⁴⁰ Yılmaz, 2020, s. 236.

⁷⁴¹ Çetin, 2017, s. 52.

gereği terörizmin finansmanı suçu bakımından uygulanamamaktadır⁷⁴². Fon sağlama ya da toplama eylemlerinin hak veya görev kaynaklanması mümkün görünmediği gibi, bu suç bakımından fiile rıza gösterecek bir kişinin veya meşru savunmaya yol açacak nitelikte bir saldırının varlığının da mümkün olmadığı söylenebilir⁷⁴³.

4.4.1.7. Kusurluluk

Terörizmin finansmanı suçu, kusurluluğu kaldıran nedenler bakımından özellik göstermese de⁷⁴⁴ bu bakımdan incelenebilir.

Türk Ceza Kanunu'nun 20. Maddesinde “*Ceza sorumluluğu şahsidir. Kimse başkasının fiilinden sorumlu tutulamaz.*” denilerek bir yandan “kolektif ceza sorumluluğunun olmadığına” diğer yandan da “kusursuz suç olmaz ilkesine işaret edilmektedir. Hafizoğulları ve Özen, Kanun’un 21. Maddesinin 1. Fıkrasında “suçun oluşması kastın varlığına bağlıdır.” ifadesinin “suçun oluşması kusurun varlığına bağlıdır” şeklinde anlaşılabilirliğini düşünmektedir⁷⁴⁵. Bu iki hükümden Kanun’un “kusursuz suç olmaz” ilkesine yer verdiği kabul edilir.

Doktrinde bir kısım yazara göre isnat yeteneği kusurluluğun ön şartı ya da bir unsuru değildir⁷⁴⁶; dolayısıyla isnat yeteneğini kaldıran sebepler ile kusurluluğu kaldıran nedenler de birbirinden farklı olmaktadır⁷⁴⁷. Isnat yeteneği kusurluluğun ön şartı olarak düşünülemez; dolayısıyla isnat yeteneğini kaldıran ve azaltan nedenler, kusurluluğu ne kaldıran, ne de azaltan nedenlerdir⁷⁴⁸. Isnat edilebilirlik, suç failinin cezalandırılması için sahip olması gereken nitelikten ibarettir⁷⁴⁹. Davranışın anormal de olsa bir süjenin iradesine bağlanabiliyor olması, bunun hukuken nazara alınması açısından yeterlidir. Bu durum Hafizoğulları ve Özen tarafından, “Bir fiilin hukuk bakımından önemi haiz olması, dolayısıyla ceza sorumluluğuna yer verebilmesi için, o fiilin, mutlaka şuurlu bir çabadan

⁷⁴² Tokgöz, 2022, s. 161.

⁷⁴³ Gödekli, 2013, s. 251.

⁷⁴⁴ Tokgöz, 2022, s. 163.

⁷⁴⁵ Hafizoğulları ve Özen, 2012, s. 271.

⁷⁴⁶ Hafizoğulları ve Özen, 2012, s. 314.; Toroslu ve Toroslu, 2021, s. 410.

⁷⁴⁷ Hafizoğulları ve Özen, 2012, s. 314.

⁷⁴⁸ Hafizoğulları ve Özen, 2012, s. 271.

⁷⁴⁹ Toroslu ve Toroslu, 2021, s. 410.

kaynaklanmasına gerek yoktur, sadece iradeyle bir biçimde bağlanabilir olması yeterlidir.” şeklinde açıklanmaktadır⁷⁵⁰.

Bununla birlikte Kanun’un “*Ceza Sorumluluğunu Kaldıran veya Azaltan Nedenler*” başlığı altında hukuka uygunluk nedenleri, kusurluluğu kaldıran nedenler, cezalandırılabilme şartı ve isnat yeteneğini kaldıran ve azaltan nedenler karışık bir şekilde belirtilmiş olup; kusurluluğu kaldıran nedenler ile ilgili Kanun’un kabul edilebilir bir sistemi bulunmamaktadır⁷⁵¹. Kanun’un, 31. maddesinin gerekçesinde isnat yeteneği, Alman Ceza Hukuku’ndan etkilenecek⁷⁵² “kusur yeteneği⁷⁵³” olarak adlandırılmıştır.

Kusurluluğun esaslı unsuru, birey ile fiili arasındaki psikolojik bağıdır⁷⁵⁴. Failin fiilinin iradi olması demek, faille fiili arasında psişik/manevi bir bağın bulunması demektir. Davranış anormal de olsa bir süjenin iradesine bağlanabiliyorsa bu durum, bunun hukuken nazara alınması açısından yeterli olacaktır⁷⁵⁵. Kusurluluğu kaldıran nedenler, fiilin iradiliğini gideren nedenlerden ve fiilin bilinmemesinden ötürü ortaya çıkmaktadır. Fiilin iradiliğini kaldıran nedenler: kendinde olmama, mücbir sebep ve maddi cebir halleridir⁷⁵⁶. Bu nedenler, davranışın psişik yönden faile ait olmasını veya geniş anlamda kusurun oluşmasını engellerler⁷⁵⁷.

Kusurluluğu kaldıran nedenler arasındaki maddi cebir, Kanun’un 28. Maddesinde “...kurtulamayacağı cebir ve şiddet ...sonucu suç işleyen kimseye ceza verilmez.” şeklinde belirtilmiştir. Bu doğrultuda maddi cebir hali kusurluluğu kaldıran bir nedendir.

Bununla birlikte manevi cebir aynı maddede “*muhakkak ve ağır bir korkutma ve tehdit*” kapsamında belirtilmiştir. Manevi cebirde, maddi cebirden farklı olarak fail ile fiil arasındaki iradi bağ kısıtlı olsa da kesilmemekte, fiilin iradiliği gelecekteki bir zarar tehdidiyle zorlanmış olsa bile devam etmektedir⁷⁵⁸. Bu durum doktrinde “istenemezlik

⁷⁵⁰ Hafizoğulları ve Özen, 2021, s. 251.

⁷⁵¹ Hafizoğulları ve Özen, 2012, s. 313.

⁷⁵² Heinrich, 2014, s. 354.

⁷⁵³ Schuldfähigkeit.

⁷⁵⁴ Toroslu, Haluk, Ceza Hukukunda İsnat Yeteneği, (Doktora Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Ankara, 2013, s. 270.; Toroslu ve Toroslu, 2021, s. 252.; Hafizoğulları ve Özen, 2012, s. 314.

⁷⁵⁵ Toroslu, 2013, s. 268.

⁷⁵⁶ Hafizoğulları ve Özen, 2012, s. 314.

⁷⁵⁷ Toroslu ve Toroslu, 2021, s. 252.

⁷⁵⁸ Hafizoğulları, Zeki, “Kusurluluğu Kaldıran Bir Neden Olarak Ceza Hukukunda İstenemezlik İlkesi (Nichtzumutbarkeit /L’inesigibilita)”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2008/57 (3), s. 363. <https://dergipark.org.tr/tr/download/article-file/626960> (Erişim: 13.05.2022); Hafizoğulları ve Özen, 2012, s. 324.; Toroslu ve Toroslu, 2021, s. 255.

ilkesi” çerçevesinde incelenmekte, kusurluluğu kaldıran bir hal olarak kabul edilmektedir⁷⁵⁹. Yani manevi cebirde, failin “iradi” fiili, kusurlu görülmediğinden, suç olmamaktadır⁷⁶⁰.

Bu doğrultuda terörizmin finansmanı suçunun kusurluluk bakımından sıkça verilen örnekleri: terör örgütlerinin insanları kaçırap karşılığında talep ettiği para ya da menfaat durumu⁷⁶¹ ya da dağ başında teröristler tarafından sıkıştırılarak silah tehdidi altında herhangi bir yardımda bulunmaya zorlanan köylü örnekleridir. Cebir veya tehdit altındaki bu durumlarda fon sağlanması ya da toplanması kusurluluğu kaldıran nedenler açısından incelenip, bu doğrultuda ceza verilmeyebilecektir.

4.4.1.8. Nitelikli Hal

Terörizmin finansmanı suçunun nitelikli hali, Terörizmin Finansmanının Önlenmesi Hakkında Kanun’un 4. maddesinin 4. fıkrasına göre, suçun bir kamu görevlisi tarafından kamu görevinin sağladığı nüfusun kötüye kullanılması suretiyle işlenmesidir. Bu durumda cezanın yarı oranında arttırılması öngörülmüştür. Kanun hükmüne göre failin kamu görevlisi olması yeterli olmayıp, bu suçu görevinin sağladığı nüfusu kötüye kullanmak ile işlemesi gerekir.

4.4.1.9. Suçun Özel Görünüş Biçimleri

Bu başlık altında terörizmin finansmanı suçu teşebbüs, iştirak ve içtima hükümleri doğrultusunda kısaca irdelenecektir.

Terörizmin finansmanı suçunda teşebbüs mümkündür; Çünkü suçun hareket kısmını oluşturan toplama ve sağlama eylemleri yapıları gereği bölünebilir niteliktedir⁷⁶².

Terörizmin finansmanı suçunu birden fazla kişinin birlikte işlemesi de mümkün olup, iştirak hükümleri söz konusu olabilecektir. Bununla birlikte terörizmin finansmanı suçu iştirak hükümlerinin uygulanması çerçevesinde bir özellik göstermemektedir.

⁷⁵⁹ Hafizoğulları, 2008, ss. 362-365.; Hafizoğulları ve Özen, 2012, s. 325.

⁷⁶⁰ Hafizoğulları, 2008, s. 364.

⁷⁶¹ Tokgöz, 2022, ss. 163-164.; Yılmaz, 2020, s. 238.

⁷⁶² Tokgöz, 2022, s. 166.; Çetin, 2017, s. 53.

Ayrıca bu suçta dolaylı faillik, müşterek faillik, azmettirme ve yardım etme halleri de mümkündür⁷⁶³.

Terörizmin finansmanı suçu için genel kuralın gerçek içtima olduğu düşünülmektedir⁷⁶⁴. Bununla birlikte bir fiilin terörizmin finansmanı suçu ile terör örgütüne (ya da silahlı terör örgütüne) yardım suçunun hangisi çerçevesinde değerlendirileceği; hem terör örgütüne maddi olmayan hem de maddi olan yardımların nasıl değerlendirileceği; terör örgütü kurucusu, yöneticisi ve üyesi tarafından işlenen terörizmin finansmanı suçunun nasıl değerlendirileceği hususlarının incelenmesinde yarar vardır.

Terör örgütüne yardım etme suçu, Türk Ceza Kanunu'nun 220. maddesinin 7. fıkrasında yer almaktadır. Fıkra yardım etme suçu genel olarak anılmış, maddi-manevi ya da parasal-parasal olmayan yardım ayrımı yapılmamıştır. Bu nedenle değeri parayla ölçülebilir bir yardım söz konusu olduğunda sonradan çıkan ve özel hüküm olan Terörizmin Finansmanının Önlenmesi Hakkındaki Kanun'un 4. Maddesinin uygulanması belirtilmektedir⁷⁶⁵. Yargıtay 16. Ceza Dairesi bir kararında belirttiği üzere, terörizmin finansmanı suçunun terör örgütlerine yardım suçunun özel bir düzenleniş biçimi olduğu, bu nedenle "terör örgütlerine veya mensuplarına para veya değeri para ile temsil edilebilen taşınır veya taşınmaz, maddi veya gayri maddi her türlü mal, hak, alacak ile bunları temsil eden her türlü belgeyi sağlayan veya toplayan kişilerin eylemleri 6415 sayılı Kanununun 4. Maddesi kapsamında olduğunu" düşünmektedir⁷⁶⁶. Yine de Yargıtay Ceza Genel Kurulu'nun 13.2.2018 tarihli kararında⁷⁶⁷,

...6415 sayılı Kanundaki düzenleme, terör örgütlerine silah ve finansman sağlamak suretiyle yardım suçunun, 5237 sayılı TCK'nun 314/3-2, 220/7. maddelerindeki terör örgütlerine yardım suçunun özel bir düzenleniş şekli olup; 5237 sayılı TCK'daki düzenlemeden farklı olarak örgütün devamlılığını sağlamak amacıyla daha organize, düzenli, süreklilik arzedecek şekilde örgüt ile hiyerarşik bağ kurulmadan, belirli bir organizasyon dahilinde ulusal veya uluslararası boyutta yapılan yardım eylemlerinin cezalandırılması amaçlanmıştır...Yukarıda yapılan açıklamalar karşısında, sanıkların eyleminin örgüte bilerek ve isteyerek yardım suçunu oluşturduğu, sanıklar

⁷⁶³ Tokgöz, 2022, ss. 167-168.; Çetin, 2017, s. 60.

⁷⁶⁴ Tokgöz, 2022, s. 168.; Aydın ve Arslan, 2021, s.

⁷⁶⁵ Tokgöz, 2022, ss. 168-169.

⁷⁶⁶ Yargıtay 16. Ceza Dairesi, 2.3.2018 T., 2018/588 E., 2018/718 K.,'dan akt. Yılmaz, 2020, ss. 244-245.

⁷⁶⁷ Yargıtay Ceza Genel Kurulu, 13.2.2018 T., 2017/16-692 E., 2018/41 K.

<https://rayp.adalet.gov.tr/resimler/552/dosya/ycgk-terorizmin-finansmani-2018-06-01-202115-41.doc>

(Erişim: 15.05.2022)

hakkında TCK'nun 314/3 ve 220/7. maddeleri delaletiyle 314/2. maddesi gereğince uygulama yapılması...

şeklinde bir hüküm kurmuş olup, terörizmin finansmanı suçunun özel bir düzenleme olduğu kabul edilse de, 6415 sayılı Kanunun gerekçesi tekrar edilip, bu tür fiillerin daha özellikli bir görünüm elde etmesi sebebiyle her türlü maddi yardımın 6415 sayılı kanun çerçevesinde cezalandırılmayacağı, Yargıtay Ceza Genel Kurulu tarafından düşünülmektedir.

Bununla birlikte terör örgütüne yardım suçu ile terörizmin finansmanı suçunun suçun konusu bakımından birbirinden ayrı olduğu ve bir eylemin hem terör örgütüne yardım hem de terörizmin finansmanı suçunu oluşturmasının mümkün olmadığını savunan görüş de bulunmaktadır⁷⁶⁸.

Sağlanan katkının hem ekonomik bir değer taşıyan hem de taşımayan bir özellik gösterdiği durumlarda farklı görüşler bulunmaktadır. Bu durumda doktrinde her iki suçtan da ceza verilmesi gerektiğini düşünen görüşler bulunmaktadır⁷⁶⁹. Bununla birlikte aksi bir görüşe göre terör örgütüne yardım etme suçu, yardım edilen örgüt silahlı olsa bile en fazla 5 yıldan 10 yıla kadar ceza alınmasını gerektireceğinden; Terörizmin Finansmanının Önlenmesi Hakkında Kanun'un 4. maddesinin "*fiili daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yıldan on yıla kadar hapis cezası ile cezalandırılır*" hükmü gereği de terörizmin finansmanı suçu 5 yıldan 10 yıla kadar ceza alınmasını gerektirdiğinden, silahlı olsun ya da olmasın bir örgüte yardım etme fiili 4. madde uyarınca daha ağır bir cezayı gerektiren başka bir suç oluşturmadığından bu tür fiillerin terörizmin finansmanı suçu çerçevesinde değerlendirilmesi savunulmaktadır⁷⁷⁰. Bu görüşe göre söz konusu durumda suçların çokluğu görünüşte olup bu durum "görünüşte içtima" durumu oluşturmaktadır. Bununla birlikte fiilin daha ağır cezayı gerektirdiği durumda zaten Türk Ceza Kanunu'nun 44. maddesinde düzenlenen fikri içtima hükmünün uygulanacağı, söz konusu 4. Maddedeki ifadenin gereksiz bir fazlalık teşkil ettiği de belirtilmektedir⁷⁷¹.

Terörizmin finansmanı suçunun failinin aynı zamanda terör örgütü üyesi olması durumunda ise 6415 sayılı Kanunun 4. Maddesinde yer alan "*Birinci fıkrada sayılan*

⁷⁶⁸ Yılmaz, 2020, s. 244.

⁷⁶⁹ Yılmaz, 2020, s. 244.; Gödekli, 2017,ss. 332-334'ten akt. Tokgöz, 2022, s. 169.

⁷⁷⁰ Tokgöz, 2022, s. 169.

⁷⁷¹ Yılmaz, 2020, s. 247.

fiillerin, örgütü kuran veya yöneten ya da örgüt üyesi tarafından gerçekleştirilmesi hâlinde bu kişiler hakkında örgüt kurmak, yönetmek veya örgüte üye olmak suçları uyarınca verilecek ceza üçte birine kadar artırılır.” hükmü çerçevesinde incelenmesi gerekir.

Bu hüküm eklenmeden önce, silahlı örgüte üye olma durumunda Terörle Mücadele Kanunu'nun 3. maddesi çerçevesinde Türk Ceza Kanunu'nun 314. maddesinde düzenlenen silahlı örgüte üye olma suçu terör suçu olarak kabul edildiğinden ve ceza yarı oranında arttırılacağı öngörüldüğünden; bu ceza terörizmin finansmanı suçundan daha ağır bir ceza gerektirdiğinden bu ceza uygulanacak ve terörizmin finansmanı suçundan ayrıca cezalandırılma olmayacaktı. Bununla birlikte suç örgütü silahlı bir örgüt olmadığında ise verilecek ceza terörizmin finansmanı suçu ile verilecek cezadan daha ağır bir ceza gerektirmediğinden ayrı ayrı cezalandırma söz konusu olacaktı⁷⁷².

Bununla birlikte bu hüküm eklendikten sonra, failin kurucusu, yöneticisi ya da üyesi olduğu örgüt silahlı olmadığı takdirde, terörizmin finansmanı suçundan ayrıca cezalandırılmayacağı, bu hüküm dâhilinde terörizmin finansmanı suçunu oluşturan fiilleri de işlemiş olması dolayısıyla yalnızca hükümde belirtilen cezalar üçte biri arttırılarak cezalandırılacağı öne sürülmektedir⁷⁷³. Fakat bu düşüncenin kabulü halinde, terörizmin finansmanı suçunu işleyen biri normal şartlarda 5 yıldan 10 yıla kadar cezalandırılacakken; silahlı olmayan bir örgüte katılıp, terörizmin finansmanı suçunu işlemesi halinde 2 yıldan 4 yıla kadar olan ceza üçte biri oranında arttırılacağından, neredeyse her halükarda 5 yıldan 10 yıla kadar olacak cezadan daha az ceza alabilmesi sonucu ortaya çıkacaktır. Yani bu düşüncenin kabulü ile, terörizmin finansmanı suçunu işlemek isteyen bir kişi, silahlı olmayan bir örgüte üye olduktan sonra bu suçu işleyerek daha az ceza alabilmektedir. Bu durumun ise hukuken ne kadar yerinde olacağı tartışılabilir. Özgenç de söz konusu düzenleme sonucunda, fıkrada sayılan kişilerin

İçtima dahilinde belirtilebilecek son husus da zincirleme suçtur. Terörizmin finansmanı suçu bakımından sağlama ve toplama fiillerinin birden fazla ve art arda işlenmesi sonucu zincirleme suç söz konusu olabilecektir⁷⁷⁴. Bununla birlikte sağlama ya da toplama fiili bir kez gerçekleştirildikten sonra, failin zamansal bütünlük içerisinde aynı

⁷⁷² Tokgöz, 2022, s. 172.

⁷⁷³ Tokgöz, 2022, s. 172.

⁷⁷⁴ Özgenç, 2022, s. 184.; Tokgöz, 2022, s. 170.

türdeki başka fonları da sağlaması ya da toplaması durumunda, hukuki anlamda fiilin tekliği öne sürülerek zincirleme suç hükmünün uygulanmayacağı belirtilmektedir⁷⁷⁵.

4.4.1.10. Muhakeme

Terörizmin finansmanı suçu, re'sen takip edilir⁷⁷⁶. Fakat 6415 sayılı Kanunun 4. maddesinin 6. fıkrası uyarınca, suçun yabancı bir devlet veya uluslararası bir kuruluş aleyhine işlenmesi halinde soruşturma ve kovuşturma yapılması Adalet Bakanı'nın talebine bağlıdır.

6415 sayılı Kanunun 4. maddesinin 7. fıkrasına göre “3713 sayılı Kanunun soruşturmaya, kovuşturmaya ve infaza ilişkin hükümleri, bu suç bakımından da uygulanır.” denilmektedir. 3713 sayılı Kanun çerçevesinde yapılacak yargılama ağır ceza mahkemeleri nezdinde gerçekleştirildiğinden, terörizmin finansmanı suçunda da ağır ceza mahkemeleri görevli olacaktır.

4.4.1.11. Yaptırım

Gerçek kişi bakımından, 6415 sayılı Kanunun 4. Maddesinde terörizmin finansmanı suçunu işleyen kişinin 5 yıldan 10 yıla kadar hapis cezası ile cezalandırılacağı hükmedilmiştir.

Tüzel kişi bakımından ise, aynı maddenin 5. fıkrası gereği suçun bir tüzel kişi faaliyeti çerçevesinde işlenmesi durumunda, bunlara özgü güvenlik tedbirlerine hükümlenacağı belirtilmiştir. Tüzel kişi hakkında uygulanabilecek güvenlik tedbirleri, 5237 sayılı Kanunun 60. maddesinde belirtilmiştir. O halde suçun bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde faaliyet izninin iptali ve müsadere güvenlik tedbirleri uygulanabilecektir.

Müsadere söz konusu olduğunda, kazanç müsadere ya da eşya müsadere hükümlerinden hangisinin uygulanacağı konusunda doktrinde görüş ayrılıkları bulunmakta olup, terörizmin finansmanı suçuna konu olan fonların kazanç ya da suç geliri

⁷⁷⁵ Tokgöz, 2022, ss. 170-171

⁷⁷⁶ Aydın ve Arslan, 2021, s. 106.; Çetin, 2017, s. 65.

olması şartının aranmamasından hareket edilerek her türlü eşyanın fon kapsamında değerlendirilmesi gerektiği belirtilmektedir⁷⁷⁷.

4.4.1.12. Terörizmin Finansmanının Önlenmesine Dair Bir Tedbir Olarak, Malvarlığının Dondurulması Tedbiri

Birleşmiş Milletler Güvenlik Konseyi'nin akıllı yaptırım kararları doğrultusunda aldığı malvarlığının dondurulması yaptırımı/tedbiri, terörizmin finansmanının önlenmesi konusunda oldukça sık başvurulan etkili bir yöntem olarak kabul edilmektedir⁷⁷⁸.

Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme'nin 8. maddesinin ilk fıkrasında “*Her Taraf Devlet, gerektiğinde müsadere edilebilmeleri amacıyla, 2. Maddede belirtilen suçların işlenmesi için kullanılan veya kullanılması için oluşturulan fonların veya bu suçlardan temin edilen kazançların tespiti, bulunması, dondurulması, el konulması için iç hukuku uyarınca gerekli tedbirleri alır.*” denilerek dondurma tedbiri anılmıştır.

Bununla birlikte uygulamada çoğunlukla malvarlığının dondurulması tedbiri ile Güvenlik Konseyi kararlarında karşılaşılmaktadır. Terörizmin finansmanının önlenmesi hakkında malvarlığının dondurulması tedbirini, Birleşmiş Milletler Güvenlik Konseyi'nin akıllı yaptırım kararlarından ilki olan 1999 tarihli 1267 sayılı kararda görebilmekteyiz. Bu kararda Taliban ile ilgili olan ve olabilecek malvarlıklarının dondurulmasına karar verilmiştir. Ardından 2001 tarihli 1373 sayılı kararın ilk maddesinde de terörist eylemleri gerçekleştiren, bunlara katılan ya da bunları kolaylaştıran ya da bu eylemlere teşebbüs eden kişilerin fonlarının ve diğer finansal varlıklarının gecikmeksizin dondurulması kararlaştırılmıştır. Burada tekrar belirtmek gerekir ki, Güvenlik Konseyi'nin VII. bölümüne dayanarak aldığı bu tür kararlar üye devletler için bağlayıcıdır. Birleşmiş Milletler Antlaşması'nın 25. maddesine göre üye devletler Güvenlik Konseyi'nin bu kararları ve uygulanmalarını kabul eder.

Belirtmek gerekir ki, malvarlığı dondurulacak olan kişi, kuruluş ya da organizasyonların belirlendiği listeler doğrudan Güvenlik Konseyi tarafından değil;

⁷⁷⁷ Tokgöz, 2022, ss. 176-177.

⁷⁷⁸ Gordon, 2011, s. 328.; Yıldırım, Zeki, “Türk Hukukunda Terörizmin Finansmanının Önlenmesi Amacıyla Malvarlığını Dondurma Tedbiri”, *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 2013/3 (1), s. 68. <https://dergipark.org.tr/tr/download/article-file/213566> (Erişim: 07.07.2022)

Güvenlik Konseyi'nin 1267 sayılı kararı ile oluşturulmuş bulunan “Komite” tarafından hazırlanmaktadır⁷⁷⁹. Bununla birlikte söz konusu listelerde bulunan kişiler hakkında herhangi bir devlet tarafından bir suç şüphesine dayanarak soruşturma ya da kovuşturma yapılması şartı aranmamakla birlikte belirli bir süre tayin edilmeksizin malvarlığının bütünü hakkında dondurma kararı verilebilmektedir⁷⁸⁰. Bu doğrultuda malvarlığını dondurma kararlarının doktrinde temel hak ve hürriyetlerin, özellikle mülkiyet hakkının ihlaline yol açabilecek nitelikte olması dolayısıyla eleştirildiği görülmektedir⁷⁸¹. Bu kapsamda Özgenç, malvarlığının dondurulması tedbirinin, Türkiye Cumhuriyeti Anayasası'nın 38. Maddesinin 10. fıkrasında yasaklanmış olan genel müsadere cezası uygulaması sonucunu doğuracak mahiyet taşıdığını belirtmektedir⁷⁸².

Malvarlığının dondurulması tedbiri, Türk hukukunda, Güvenlik Konseyi kararlarına paralel bir şekilde 6415 sayılı Kanun kapsamında düzenlenmiştir. Kanunun 5. maddesinin 1. fıkrasına göre, “*Birleşmiş Milletler Güvenlik Konseyinin 1267 (1999), 1988 (2011), 1989 (2011) ve 2253 (2015) sayılı kararlarıyla listelenen kişi, kuruluş veya organizasyonların tasarrufunda bulunan malvarlığının dondurulması kararları ve bu listelerden çıkarılanlara ilişkin malvarlığının dondurulmasının kaldırılması kararlarının uygulanmasına yönelik Cumhurbaşkanı kararı, Resmî Gazete’de yayımlanır ve gecikmeksizin uygulanır.*” denilmektedir. Maddenin ikinci fıkrasına göre alınan kararlar Dışişleri Bakanlığı tarafından Güvenlik Konseyi’ne bildirilmektedir. Güvenlik Konseyi kararlarına karşı yapılacak başvuruların ise MASAK tarafından Dışişleri Bakanlığı aracılığıyla Güvenlik Konseyi’ne iletileceği 3. fıkra da belirtilmiştir.

Güvenlik Konseyi'nin talebi dışında, başka bir devletin talebi üzerine malvarlıklarının dondurulması 1373 sayılı karar ile mümkün kılınmıştır. 6415 sayılı Kanunun 6 maddesinde de bu durum “*...Türkiye’den talepte bulunulması hâlinde, Değerlendirme Komisyonunca değerlendirilen talep Cumhurbaşkanı tarafından karara bağlanır. Değerlendirmede karşılıklılık ilkesi gözetilir.*” şeklinde düzenlenmiştir.

⁷⁷⁹ Özgenç, 2022, s. 192.

⁷⁸⁰ Özgenç, 2022, ss. 192, 193.

⁷⁸¹ Gordon, 2011, s. 330.; Özgenç, 2022, s. 194.; Yılmaz, 2020, s. 197.; Altuner Coşkun, Sümeyra, Terörizmin Finansmanının Önlenmesine Yönelik Birleşmiş Milletler Güvenlik Konseyi'nin Akıllı Yaptırım Kararları, (doktora tezi), Ankara Üniversitesi, Kamu Hukuku Anabilim Dalı, Ankara, 2015, ss. 87-88.

⁷⁸² Özgenç, 2022, s. 205.

Bununla birlikte kanunun 7. maddesi doğrultusunda Değerlendirme Komisyonu'na makul sebeplerin varlığı halinde öneride bulunma yetkisi verilmiştir. Bu durum söz konusu maddenin 1. fıkrasında, “5 inci ve 6 ncı maddelerde düzenlenen hususlar dışında, Değerlendirme Komisyonu, 3 üncü ve 4 üncü madde kapsamına giren fiilleri gerçekleştirdiği hususunda makul sebeplerin varlığına istinaden kişi, kuruluş veya organizasyonların yabancı ülkelerde bulunan malvarlığının dondurulması talebiyle Cumhurbaşkanına öneride bulunulmasına karar verebilir.” şeklinde düzenlenmiştir.

Yine aynı maddenin 3. fıkrasında “mahkemelerce terör örgütü olduğuna kesin olarak karar verildikten sonra terörizmin finansmanı suçunu gerçekleştirdiği konusunda makul sebeplerin varlığı halinde kişi, kuruluş veya organizasyonların Türkiye’de bulunan malvarlığının dondurulmasına ve kaldırılmasına Değerlendirme Komisyonunun önerisi üzerine Hazine ve Maliye Bakanı ile İçişleri Bakanı tarafından birlikte karar verilebileceği” belirtilmiştir. 4. fıkraya göre ise bu kararın “derhal uygulanacağı” ve “48 saat içerisinde Hâkimler ve Savcılar Kurulu tarafından belirlenen Ankara ağır ceza mahkemesinin onayına sunulacağı” belirtilmiştir.

Kanunun 10. maddesinde “Türk Medeni Kanunu⁷⁸³'nun iyiniyetin korunmasına ilişkin hükümleri saklı kalmak üzere, malvarlığının dondurulması kararına aykırı olarak yapılan her türlü tasarruf ve işlemin hükümsüz olduğu” belirtilmiştir.

Kanunun 12. maddesinde malvarlığının dondurulması kararlarının icrası ele alınmıştır. 12. Maddenin 4. Fıkrasında “Malvarlığının dondurulması kararı, Başkanlığın talebi üzerine 5271 sayılı Kanunun 128 inci maddesinin üçüncü ila yedinci fıkralarında belirtilen usule uygun olarak gecikmeksizin yerine getirilir.” denilerek malvarlığının dondurulmasının taşınmaz, hak ve alacaklara elkoyma usulüne göre gerçekleştirileceği belirtilmiştir.

Burada belirtmek gerekir ki, malvarlığının dondurulması tedbiri, elkoyma tedbirine oldukça benzese de aralarında birtakım farklılıklar bulunmaktadır. İki tedbir arasındaki en önemli fark, elkoyma tedbirine mahkeme tarafından karar verilirken; malvarlığının dondurulması tedbirine idari bir makam tarafından karar verilmesidir. Bu doğrultuda el koyma tedbiri bir ceza muhakemesi koruma tedbiri iken, malvarlığının dondurulması tedbirinin ise önleyici bir idari tedbir olduğunu söylemek mümkündür⁷⁸⁴.

⁷⁸³ R.G., T: 22/11/2001, S: 24607.

⁷⁸⁴ Yıldırım, 2013, s. 77, 81.

Yine elkoyma tedbiri somut delillere dayanan kuvvetli şüphenin bulunması şartına bağlı iken malvarlığının dondurulması tedbirine böyle bir şüphe oluşmadan birtakım istihbarat bilgileri ve belirtilere dayanarak karar verildiği görülmektedir⁷⁸⁵.

4.4.1.12.1. Malvarlığının Dondurulması Tedbirinin Kripto Paralar Çerçevesinde Ele Alınması

Kripto paralarla gerçekleştirilen finansmanı önlemek veya engellemek için uygulanacak tedbirlerin gerek kanuni olarak gerek ise pratikte birçok problemi barındıracağını söylemek yanlış olmaz. Kripto paraların terörizmin finansmanında nasıl kullanılabilceği üzerine ayrıntılı bilgiler bu çalışmanın “Kripto Para” bölümü altında incelenmişti. Söz konusu bölümde daha çok finansman faaliyetlerinin nasıl gerçekleştirilebileceği ve bu faaliyetler gerçekleştirilirken nasıl “gizli” ve “anonim” kalınabileceğinden bahsedilmişti. Bu başlıkta ve devam eden başlıkta ise toplanan ya da sağlanan kripto paraların malvarlığının dondurulması, elkoyma ve müsadere tedbirlerinin çerçevesinde incelenmesi söz konusu olacaktır. Malvarlığının dondurulması ile ilgili incelemeye 6415 sayılı kanun dâhilinde yapılan tanımları takip ederek başlamakta fayda vardır.

Öncelikle 6415 sayılı kanunun “Tanımlar” başlığı altında “fon” tanımına bakılmalıdır. Kanunun 2. maddesinin 1. Fıkrasının (c) bendine göre fon, “*Para veya değeri para ile temsil edilebilen taşınır veya taşınmaz, maddi veya gayri maddi her türlü mal, hak, alacak ile bunları temsil eden her türlü belge*” olarak tanımlanmıştır. Bu doğrultuda kripto paraların 6415 sayılı kanunun fon tanımında sayılan unsurlardan hangisine dahil olduğu problemi söz konusu olacaktır. 6415 sayılı kanunun amaç ve kapsamından bahsedildiği ilk maddesinde kanunun 1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme doğrultusunda hazırlandığına vurgu yapılmıştır. Bu doğrultuda kanundaki fon tanımı söz konusu Sözleşmede yapılan tanıma paralel bir şekilde hazırlanmıştır. Sözleşme ve kanunun amacının, terör örgütlerine ve terör faaliyetlerine finansal kaynak sağlanmasının önlenmesi olduğu açıktır. Bu doğrultuda Sözleşmenin 1. maddesinde yapılan fon tanımı oldukça geniş olup, “*her türlü kıymet*”in fon kapsamına gireceğinden bahsedilmektedir. Bu doğrultuda

⁷⁸⁵ Yıldırım, 2013, s. 77.

hukuken para olarak kabul edilmese bile para ile ölçülebilen değer/kıymet sağlayan kripto paraların Sözleşme kapsamındaki fon tanımına gireceği söylenebilir. 6415 sayılı Kanun da geniş bir fon tanımı amaçlanarak hazırlanmış olsa da, ilgili maddenin lafzı yönünden sözleşmedeki fon tanımı kadar kapsayıcı bir tanımlamanın yapılamadığı görülmektedir. Yine de gerek Sözleşmedeki fon tanımı gerek ise kanunun amacı ile birlikte ilgili Yönetmelikteki “kripto varlık” tanımı dikkate alınarak, kripto paraların 6415 sayılı Kanundaki fon tanımına “*gayri maddi mal*” kabul edilerek dahil olmasında sakınca bulunmamaktadır. “Gayri maddi mal” kavramı çoğunlukla fikri mülkiyet hukuku ile hukuka girmiş bir kavramdır⁷⁸⁶. Zira eşya hukukuna konu olan mallar, üzerinde hakimiyet kurmaya müsait, cismani olan maddi mallar, yani eşyalardır⁷⁸⁷. Maddi - gayri maddi mal ayrımı Anayasa Mahkemesi tarafından da yapılmış bulunmaktadır. Anayasa Mahkemesi’nin 2008 tarihli bir kararında⁷⁸⁸, “*Mülkiyet hakkının konusunu, maddi ve gayrîmaddi mallar oluşturmaktadır. Taşınır ve taşınmaz mallar, maddi mallar kapsamında iken, fikri ve sınaî mülkiyet hakları gayrîmaddi mallar kapsamında yer almaktadır.*” denilerek gayri maddi mal kavramı benimsenmiş bulunmaktadır. Yine 6502 sayılı Tüketicinin Korunması Hakkındaki Kanunun⁷⁸⁹ 3. maddesinin 1. fıkrasının (h) bendinde mal, “*Alışverişe konu olan; taşınır eşya, konut veya tatil amaçlı taşınmaz mallar ile elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri her türlü gayri maddi malları*” şeklinde tanımlanarak gayri maddi mal kavramına yer verilmiştir. Bilindiği üzere kripto paraların niteliğine ilişkin Türk mevzuatlarındaki tek düzenleme, çalışmanın yukarısında da belirtildiği üzere Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik’in 3. maddesinde bulunuyor olup, maddede yapılan tanımda gayri maddi mal kavramına yakın bir ifade ile, kripto paraların (varlıkların) hukuken para olarak nitelendirilemeyen “gayri maddi varlıklar” olarak tanımlandığı görülmektedir. Açıklanan bütün bu bilgiler doğrultusunda kripto paraların 6415 sayılı

⁷⁸⁶ Erzurumlu, Nurbanu, “Türk Hukukunda Fikrî Mülkiyete Konu Malların Cebri İcrası”, Yıldırım Beyazıt Hukuk Dergisi, 2017/3, s. 169. <https://dergipark.org.tr/tr/download/article-file/270859> (Erişim: 09.07.2022)

⁷⁸⁷ Tarakçıoğlu, Zeynep Esra, “Kripto Varlıklar Ve Ceza Hukuku Sorumluluğu”, *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, 2021/11(2), s. 327. <https://doi.org/10.54704/akdhfd.1024708> (Erişim: 08.07.2022); Özlük, Betül, “Mülkiyet ve Zilyetlik Üzerine Düşünceler”, *Selçuk Üniversitesi Hukuk Fakültesi*, 2019/27 (1), s. 143.; Özdemir, Genç, “Kripto Paraların Eşya Niteliği”, *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 2021/1 (1), ss. 298, 301.

⁷⁸⁸ Anayasa Mahkemesi, 31.1.2008 T., 2004/81 E., 2008/48 K.

⁷⁸⁹ R.G., T: 7/11/2013, S: 28835.

Kanun uyarınca bir gayri maddi mal olarak “fon” sayılmasında, kanunun amacı dikkate alınarak bir sakınca bulunmadığı düşünülmektedir. Yine de kavram kargaşasının önüne geçmek amacıyla bir düzenlemenin yapılması isabetli olacaktır.

Kripto paraların 6415 sayılı kanun çerçevesinde fon olarak kabul edildiğinden hareketle, aynı kanunun 2. Maddesinin 1. Fıkrasının (ç) bendi kapsamında “malvarlığı” tanımına da girdiğinden bahsedilebilir. Zira ilgili bentte malvarlığı “*Mülkiyetinde veya zilyetliğinde bulunan ya da doğrudan veya dolaylı olarak kontrolünde olan fon ve gelir ile bunlardan elde edilen veya bunların birbirine dönüştürülmesinden hasıl olan menfaat ve değeri*” olarak tanımlanmaktadır. Burada kripto paraların mülkiyete ve zilyetliğe konu olup olamayacağı tartışmasına girmeden kripto paraların ilgili tanımdaki “*doğrudan veya dolaylı olarak kontrolünde olan fon*” kapsamına girdiğinden bahsedilebilir. Bu doğrultuda kripto paralar 6415 sayılı Kanun kapsamında malvarlığı olarak kabul edildiklerinden, malvarlığının dondurulması tedbirine de konu olabileceklerdir.

6415 sayılı Kanunun 2. maddesinin 1. Fıkrasının (d) bendinde malvarlığının dondurulması ise, “*Malvarlığının ortadan kaldırılmasının, tüketilmesinin, dönüştürülmesinin, transferinin, devir ve temlik edilmesinin ve sair tasarrufi işlemlerin önlenmesi amacıyla, malvarlığı üzerindeki tasarruf yetkisinin kaldırılması veya kısıtlanması*” olarak tanımlanmıştır.

Yukarıda da belirtildiği üzere, malvarlığının dondurulması kararının icrası, 6415 sayılı kanunun 12. maddesinin 4. Fıkrası uyarınca taşınmaz, hak ve alacaklara elkoymayı düzenleyen CMK'nin 128. Maddesinin üçüncü ila yedinci fıkrasındaki usule göre gerçekleştirilecektir. Fakat terörizmin finansmanının kripto paralar aracılığıyla gerçekleştirilmesi durumunda taşınmaz, hak ve alacaklara el konulmasına ilişkin kanun hükümleri ile malvarlığının dondurulmasının icrasının gerçekleştirilebilmesi pratikte yalnızca söz konusu malvarlığı bir kripto para borsasında ya da bir başka merkezi kripto para uygulamasında bulunmakta ise bir anlam ifade edecektir. Bu çalışmanın yukarısında da detaylı bir şekilde bahsedildiği üzere kripto paralar, merkezi olmayan blok zincirlerde işlediklerinden bu tür kararların icrası mümkün olmayacaktır. Zira kripto paraların sahibi, kripto paranın bulunduğu adrese ait gizli anahtarı bulunduran kişidir; diğer bir deyişle kripto paraların mutlak kontrolü, adresin gizli anahtarını bulunduran kişiye aittir. Bu nedenle kimsenin tahakkümü altında olmayan, ağa erişimde bir aracı bulunmayan, dağıtık yapıdaki bu zincirler üzerindeki kripto paralar hakkında malvarlığının dondurulması ya

da diğerk ceza muhakemesi tedbirlerinin pratikte hiçbir hükmü olmayacaktır. Bununla birlikte kripto para eğer bir merkezi borsa üzerinde (CEX) bulunuyorsa, bu durumda malvarlığının dondurulması kararı icra edilebilecektir. Bu tür bir durumda, malvarlığının dondurulması kararı verilen kişinin bir CEX üzerinde bulundurduğu kripto paraların blok zincir üzerindeki sahibi aslında borsadır. Çünkü kişi, borsa üzerinde aktarım ya da çekim yaptığı cüzdan adreslerinin gizli anahtarını elinde bulundurmamaktadır. Kripto paralar hakkındaki bu durum uygulamada sıklıkla Andreas Antonopoulos'un ünlü deyimini ile "Not your keys not your coins. (Anahtar senin değilse para da senin değildir.)" şeklinde açıklanmaktadır. Yani bir adrese ait kripto paralar üzerinde tasarrufta bulunacak kişi sadece o adrese ait gizli anahtarı elinde bulunduran kişidir. Sonuç olarak eğer malvarlığı değerinin dondurulması kararı verilen kişinin merkezi bir kripto para borsasında kripto parası bulunmakta ise, bu hesap CMK 128/5 uyarınca dondurulabilecektir. Dondurulmak istenen kripto paraya eğer blok zincir üzerindeki bir şahsi cüzdandan erişiliyorsa malvarlığının dondurulması kararı alınsa bile uygulanması pratikte imkansız olacaktır.

Değindiği üzere, şahsi cüzdanda bulunan kripto paralar hakkında karar verilen tedbirlerin icra edilebilirliği oluşmayacak olsa bile, söz konusu cüzdanların çeşitli merkezi kripto para borsaları ile birlikte hareket edilerek bir "kara liste"ye alınmaları ve bu cüzdan adreslerinden kripto para borsalarına gelecek kripto paraların el konulması ya da bu cüzdan adresleri ile etkileşime giren adresler üzerinde yaptırım uygulanması mümkün olacaktır. Bu doğrultuda yapılacak düzenlemelerin bu hususu kapsamaması yerinde olacaktır.

4.4.1.13. Terörizmin Finansmanı Suçu Bakımından Elkoyma ve Müsaderenin Kripto Paralar Çerçevesinde Ele Alınması

Terörizmin finansmanı suçu bakımından elkoyma ve müsadere tedbirlerinin uygulanabileceğini söylemek mümkündür. Elkoyma ve müsadere arasında bazı temel farklılıklar bulunmaktadır. Elkoyma bir koruma tedbiriyken müsadere bir güvenlik tedbidir. Yine elkoyma geçici bir tedbir iken müsadere nihai bir tedbidir.

Terörizmin finansmanı suçunda elkoyma tedbiri hususunda özellik gösteren hüküm, Ceza Muhakemesi Kanununun 128. maddesinde düzenlenen "Taşınmazlara, hak ve alacaklara elkoyma"dır. Kanunun 123. maddesindeki basit elkoymadan farklı olarak taşınmaz, hak ve alacaklara elkoymada "somut delillere dayanan kuvvetli şüpheler"

aranmaktadır. Bununla birlikte 128. maddenin 2. fıkrasında hangi suçlar için bu elkoyma usulünün uygulanacağı sayılmıştır. Belirtmek gerekir ki bu suçlar arasında terörizmin finansmanı suçu bulunmamaktadır. Yine de bu hüküm terörizmin finansmanı suçu hakkında uygulanabilecektir. Bu duruma dayanak ise 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun⁷⁹⁰un 17. maddesidir. İlgili madde hükmünde “Aklama ve terörün finansmanı suçunun işlendiğine dair kuvvetli şüphe bulunan hallerde 5271 sayılı Ceza Muhakemesi Kanununun 128 inci maddesindeki usûle göre malvarlığı değerlerine elkonulabilir.” denilerek taşınmaz, hak ve alacaklara elkoyma hükmünün, Ceza Muhakemesi Kanununun 128. maddesinde sayılan suçlardan biri olmamasına rağmen terörizmin finansmanı suçu hakkında da uygulanabilmesi sağlanmıştır.

Terörizmin finansmanı suçunun maddi konusunu kripto para oluşturuyorsa, mevcut elkoyma ve müsadere hükümlerinin uygulanması hususunda birçok sorun ortaya çıkacaktır. Bu hususlar hem elkoyma hem de müsadere ile ilgili olarak temelde aynı sorunlar olduğundan ve terörizmin finansmanı suçunun kripto paralar kullanılarak işlenmesi durumunda elkoymanın, çalışmanın yukarısında ayrıntılı bir şekilde açıklanan blok zincire ait birtakım temel özellikler nedeniyle tek başına bir anlam ifade etmeyeceği, bu nedenle tedbirlerin icra edilebilirliği ve etkililiği konusunda bu tedbiri müsadere için takip etmesinin çoğu durumda zorunlu olacağı sebebiyle, anlatımda birlik oluşması açısından söz konusu hususlar bu başlık altındaki bulunan müsadere ile ilgili açıklamalarda ayrıntılı olarak işlenecektir. Yine de öncesinde ilgili kripto paranın (fon) merkezi bir borsa üzerinde bulunması durumunda elkoymadan bahsedilecektir.

Terörizmin finansmanı suçunun maddi konusunu oluşturan fon, kripto para olarak bir merkezi kripto para borsasında bulunuyorsa; bu kripto paraya Ceza Muhakemesi Kanununun 128. maddesinin 1. Fıkrasının (h) bendi doğrultusunda “diğer malvarlığı değeri” kapsamında elkoymaya başvurulabilir. Aynı fıkraya göre, bu madde kapsamında elkoyma yapılabilmesi için MASAK’tan rapor alınması gerekecektir. Elkoyma kararı verildikten sonra karar, 128. maddenin 5. fıkrası uyarınca kripto paranın bulunduğu borsaya bildirilecektir. Bu hükümler doğrultusunda terörizmin finansmanı suçu hakkında malvarlığını dondurma tedbirinin elkoyma tedbirine göre daha hızlı ve etkili olacağını söylemek mümkündür.

⁷⁹⁰ R.G., T: 11/10/2006, S: 26323.

Terörizmin finansmanı suçunun maddi konusunu oluşturan fon olarak kripto paranın şahsi bir adreste/cüzdanda bulunuyor olması durumunda tek başına elkoymanın oldukça yetersiz bir tedbir olacağını söylemek mümkündür. Zira elkonulacak kripto paranın bulunduğu yer aslında blok zincirdir; kişi bu kripto paranın bulunduğu adrese ait kripto paralar üzerindeki tasarruf yetkisini, aşağıda müsadere ile ilgili açıklamalarda bahsedilecek olan, birtakım bilgileri kullanarak sağlamaktadır. Bu bilgilere sahip olan herhangi bir kişi adrese ve adresin sahip olduğu kripto paralara erişim sağlayabilir. Bu nedenle pratikte kripto paraya el konulması gibi bir durum, bu çalışmanın yukarısında blok zincire ve kripto paralara ait ayrıntılı bir şekilde açıklanmış özellikler dahilinde mümkün gözükmeyp; bu kripto paranın bulunduğu adrese erişimi sağlayacak bilgiler, eğer yedeklenmiş halde bulunuyorlarsa, bu bilgilerin yer aldığı eşyalara elkonması söz konusu olacaktır. Adrese erişimi sağlayan ve aşağıda bahsedilecek bu bilgilere elkonması, bu bilgilere sahip herhangi birinin kripto paralar üzerindeki tasarruf yetkisini sonlandırmayacaktır. Bu nedenle terörizmin finansmanı suçunun kripto paralar kullanılarak işlenmesi halinde mevcut düzenlemeler kapsamında elkoyma tedbirinin tek başına oldukça işlevsiz olacağını ve elkoymayı takiben müsadereenin gerçekleştirilmesi gerektiğini söylemek mümkündür.

Müsadere, Centel vd. göre “işlenen suçun sonucu olarak, bir eşyanın veya kazancın mülkiyetinin devlete geçmesi” anlamına gelir⁷⁹¹. Toroslu ve Toroslu müsadereyi, “Yeni suçların işlenmesini önlemek amacıyla, cezai nitelikteki hukuka aykırı fiillerden kaynaklandığı veya bunların işlenmesiyle ilgili olduğu için suç düşüncesini ve suçun çekiciliğini canlı tutan eşyaya devlet lehine el konulması” şeklinde tanımlamaktadır⁷⁹². Hafizoğulları ve Özen ise müsadereyi, “suçla ortaya çıkan kriminojen ortamı gidermeye matuf ceza hukuku tedbiridir” olarak tanımlamaktadır⁷⁹³.

Türkiye Cumhuriyeti Anayasası’nın 38. Maddesinin 7. Fıkrası uyarınca kişinin malvarlığının tümü üzerindeki mülkiyetin devlete geçmesi anlamına gelen⁷⁹⁴ genel müsadere cezası verilemez. Müsadere Türk Ceza Kanununun 54. maddesinde eşya müsadere, 55. maddesinde kazanç müsadere olmak üzere iki türdür.

⁷⁹¹ Centel vd., 2020, s. 738.

⁷⁹² Toroslu ve Toroslu, 2021, s. 479.

⁷⁹³ Hafizoğulları ve Özen, 2021, s. 479.

⁷⁹⁴ Centel vd., 2020, s. 738.

Bir güvenlik tedbiri olan müsadere terörizmin finansmanı suçu hakkında uygulanabileceği söylenebilir. Bununla birlikte terörizmin finansmanı suçunda hem eşya hem kazanç müsaderesinin uygulanması mümkündür⁷⁹⁵.

Terörizmin finansmanı suçunun kripto paralar ile işlenmesi durumunda müsadere nasıl icra edileceği konusunda birçok problem bulunmaktadır. Bu konu hakkında mevzuatta herhangi bir düzenleme bulunmamaktadır; bilindiği üzere Türk hukukunda kripto paralar ile ilgili tek düzenleme Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik'tir.

Müsadere hususunu, kripto paranın bir merkezi borsada bulunması ya da kişisel cüzdanda bulunması şeklinde iki türlü inceleyebiliriz. Kripto paranın merkezi bir borsada olması durumunda müsadere kararının icra edilebilirliğinin olacağını söylemek mümkündür. Çalışmanın yukarısında da bahsedildiği üzere merkezi borsalarda bulunan hesapların blok zincir üzerindeki asıl sahibi, hesapların gizli anahtarını elinde tutan borsadır. Türk Ceza Kanununun kazanç müsaderesini düzenleyen 55. maddesi doğrultusunda terörizmin finansmanı suçunun maddi konusunu oluşturan⁷⁹⁶ ve merkezi bir kripto para borsasında tutulan fonun müsadere kararına karar verilebilecektir.

Söz konusu kripto para eğer şahsi bir cüzdanda tutuluyorsa, bu durumda kripto paranın hangi blok zincir üzerindeki hangi adreste bulunduğu biliniyor olsa bile, bu adresin üzerinde tasarrufta bulunabilecek tek kişi adrese ait gizli anahtarını elinde bulduran kişi olduğundan, müsadere kararı verilse bile icra edilebilmesi pratikte mümkün olmayacaktır. Müsadere kararının icra edilebilmesinin tek yolu, adrese ait gizli anahtarın elde edilmesidir. Zira gizli anahtar ile söz konusu adrese erişmeden, o adreste tutulan kripto paranın müsadere edilmek amacıyla başka bir adrese gönderilmesi mümkün değildir. Çalışmanın üst bölümlerinde de ayrıntılı bir şekilde aktarıldığı üzere, blok zincirde bir aracı yoktur; kullanıcılar direkt olarak blok zincire erişebilir; blok zincir üzerinde her türlü işlemi gerçekleştirmek için yalnızca bir adres ve adrese ait gizli anahtara sahip olunması yeterlidir.

Söz konusu fonun bulunduğu adres, oldukça farklı türden blok zincirden biri üzerinde olabilir; bununla birlikte tutulan fon farklı görünümde karşımıza çıkabilir.

⁷⁹⁵ Gödekli, 2013, s. 260.; Tokgöz, 2022, ss. 176-177.

⁷⁹⁶ Hafizoğulları ve Özen'e göre madde hükmünde geçen "suçun konusunu oluşturan maddi menfaat"ten suçun maddi konusunu oluşturan şeyler anlaşılmalıdır. Hafizoğulları ve Özen, 2021, s. 484.

Yine fon toplanan ya da sağlanan bu hesaba, fiili gerçekleştiren kişinin erişim yöntemleri farklı olabilir. Kripto paralar ve blok zincir hakkında bu çalışmanın yukarıdaki yapılmış detaylı açıklamalarda bu hususlar incelenmiş olsa da, mümkün olduğunca tekrara düşmeden, bu hususların müsadere sorunu üzerinden irdelenmesinde fayda vardır.

Genel olarak blok zincir üzerindeki bir adres üzerindeki tasarruf yetkisi, adrese ait gizli anahtarı elinde bulunduran kişiye aittir. Bununla birlikte söz konusu adreslere erişim yöntemlerinde çeşitlilik vardır. İlk olarak bir kişi, bir adrese direkt olarak gizli anahtarı ile erişebilir. Bir diğer yöntemde kişi adrese keystore dosyası (keystore file) ile erişebilir. Keystore dosyası, adresin gizli anahtarını barındırdığından adrese erişimi sağlar. Yine kişi isterse adrese anımsatıcı dizi (mnemonic phrase/seed phrase) ile erişim imkanı sağlayabilir. Anımsatıcı diziler, kullanılan blok zincire göre 12, 15, 18, 24 gibi farklı sayıda kelimelerden oluşan dizilerdir. Kişi, cüzdanına erişmek için bu dizileri eksiksiz bir şekilde girer; zira tek bir kelime farklılığı ya da boşluk sahip olunandan başka bir cüzdana erişime yol açacaktır. Tek bir anımsatıcı dizi genellikle birden fazla adrese de erişimi sağlar. Kullanıcı anımsatıcı dizi ile bir adres açtıktan sonra aynı dizi kapsamında birden çok adres oluşturabilir. Bu adreslerin her birinin kendi gizli anahtarları olsa da hepsine tek bir anımsatıcı dizi ile erişilebilir.

Genel olarak blok zincir üzerindeki adreslere erişmek için yukarıda bahsedilen bilgilerden herhangi biri gereklidir. Bununla birlikte kişisel adres veya cüzdanlara erişim farklı araçlar kullanılarak gerçekleştirilebilir. Bu araç mobil bir uygulama olabileceği gibi, tarayıcı eklentisi, masaüstü uygulaması, donanım cüzdanları ya da kağıt cüzdan olabilir. Kişisel adreslere erişebilmek için herhangi bir araç kullanılabilir, fakat her halükarda başlangıçta yukarıda bahsedilen bilgilerin girilmesi gerekecektir. Bahsedilen araçlar içerisinde diğerlerinden farklılaşan araç, donanım cüzdanlarıdır. Donanım cüzdanları genellikle USB bağlantı üzerinden bilgisayara ya da diğer cihazlara bağlanabilen, içerisinde kullanıcısının gizli anahtarını barındıran kripto para cüzdanlarıdır. Yaygın sanının aksine donanım cüzdanları içerisinde kripto para barındırmazlar; kripto para her halükarda blok zincir üzerindedir. Donanım cüzdanları küçük, taşınabilir bir aygıt olarak istenilen yer ve zamanda kişisel adreslere erişimi sağlar. Donanım cüzdanlarının diğer araçlara göre daha güvenli olmalarının sebebi, offline cüzdanlar olmaları sebebiyle saldırılara kapalı olmaları; internet bağlantısı gerçekleşse bile blok zincir üzerinde yapılan işlemlerin gizli anahtar ile imzalanma aşamasını kendi

donanımı içerisinde tamamlamasından dolayıdır. Kağıt cüzdanlar ise basitçe, adrese ait gizli ve açık anahtarın, QR kod şeklinde kağıda yazdırılmış halidir. Kişi cüzdanına transfer almak istediğinde açık anahtarına ait QR kodu paylaşır; cüzdanından harcama yapmak istediğinde gizli anahtarına ait QR kodunu okutur.

Bu bilgiler çerçevesinde, merkezi bir borsa gözetiminde olmayan kripto para adresi üzerinde müsadere işlemi gerçekleştirilebilmesi için doğal olarak bu adrese erişimin sağlanması gerekecektir. Bu erişim de bahsedildiği üzere adrese ait gizli anahtarın, keystore dosyasının ya da anımsatıcı dizilere erişim ile mümkün olacaktır. Arama ve el koyma faaliyetleri çerçevesinde bu bilgilere erişilemediği sürece, bu adreslerde bulunan kripto paraların müsaderesi de gerçekleşmeyecektir. Gizli anahtar, anımsatıcı diziler ya da keystore dosyasının saklanması için herhangi bir yöntem tercih edilmiş olabilir. Örneğin gizli anahtar ya da anımsatıcı diziler bir kağıda yazılmış olabilir; herhangi bir donanım aygıtında, herhangi bir bilginin saklandığı şekilde saklanıyor olabilir. Ya da kişi anımsatıcı dizileri ezberinde tutuyor olabilir veya söz konusu bilgilerin yedeğini almamış da olabilir. Görüldüğü üzere müsaderenin gerçekleştirilebilmesi için bu bilgilere ihtiyaç duyulmakta; bunun için de cüzdana ait gizli anahtar vb. bilgilerin kişi tarafından önceden yedeklenmiş olması ve yedeklenmiş bu bilgilerin bir şekilde bulunması gerekmektedir. Alman Federal Yüksek Mahkemesi 1. Ceza Dairesi'nin 27.07.2017 tarih ve 412/16 sayılı kararında da cüzdana ait gizli anahtarın kripto paralara ait fiili tasarruf yetkisinin ele geçirilmesi için zorunlu olduğunu belirtmektedir. Kararda gizli anahtarın bilinip bilinmemesinin kazanç müsaderesi kararına etki etmeyeceği, bu durumun kararın infazına ilişkin olduğu belirtilmiştir⁷⁹⁷.

Yukarıda belirtildiği üzere söz konusu adrese ait gizli anahtarın bir donanım cüzdanı ya da kağıt cüzdan ile saklanması olasılığı da mümkündür. Gizli anahtar eğer bir donanım cüzdanı ile saklanıyorsa ve bu cüzdanlar yapılan arama sonucu bulunabilmişse; cüzdana, daha doğru bir ifadeyle işlemleri onaylayacak gizli anahtara erişebilmek için aygıt üzerindeki pin kodunu girmek gerekecektir. Aygıt üzerindeki pin kodunun belirli bir sayıda yanlış girilmesi aygıtın fabrika ayarlarına dönmesine neden olacak; sonucunda gizli anahtar silinecektir. Bu tür aygıtlar yüksek güvenli olarak üreticisi tarafından üretim sırasında dışarıdan gelecek herhangi fiziksel ya da yazılımsal ataklara karşı

⁷⁹⁷ Ünver, Y. ve K. Öz (Eds.), Kripto Para ve Ceza Hukuku, Seçkin Yayıncılık, Ankara 2022, s. 456.

dirençli olarak üretilen aygıtlardır. Bu nedenle aygıt bulunsa bile cüzdana yani gizli anahtara erişim oldukça zorlu olacaktır. Bununla birlikte eğer söz konusu adres bir kağıt cüzdan şeklinde bulunuyorsa; kağıt cüzdan üzerinde adresin gizli anahtarı bir QR kod şeklinde bulunduğundan müsadere önünde bir engel bulunmayacaktır.

Terörizmin finansmanının maddi konusunu oluşturan fonun çoklu imza (multisig) gerektiren akıllı kontrat doğrultusunda çalışan bir adreste olması da mümkündür. Örneğin Gnosis Safe⁷⁹⁸ gibi platformlarda oluşturulan cüzdanlara birden fazla adres bağlanır. Bu cüzdan üzerinde gerçekleştirilecek işlemler için cüzdan oluşturulurken belirlenen sayıda adresin imza gerekecektir. Örneğin bir terör faaliyetini finanse etmek için dört cüzdan ile Gnosis Safe üzerinde bir çoklu imza cüzdanı oluşturulmuş olup, fonlar bu cüzdanda toplanıyor olsun. Bu cüzdanda bulunan fonları çekebilmek için de dört cüzdanın en az üçünün imzalaması gerektiği şartı konuyor olsun. Bu doğrultuda bu fonlara el koyabilmek ve müsadere edebilmek için imzalayıcı cüzdanların en az üçüne erişim gerekecektir. Çünkü bu fonların müsadere edilebilmesi için gerçekleştirilecek aktarım işleminin söz konusu dört cüzdandan üçü tarafından onaylanması gerekecektir. Bu durum yukarıda birden çok olasılıkla izah edilen tek bir adresin kontrolündeki fonların müsaderesinden katbekat daha zor olacaktır.

Yukarıda finansmana konu olan ve kişisel bir cüzdanda bulunan kripto paraların müsaderesine ilişkin birtakım olasılıklar değerlendirilmiştir. Fakat belirtmek gerekir ki; arama, elkoyma ya da müsadere için karar verilene ve bu kararlar uygulanana kadar, adrese ait gizli anahtarlara başarılı bir şekilde erişilmişse bile; söz konusu adrese ait gizli anahtarı, keystore dosyasını ya da anımsatıcı dizileri elinde tutan başka biri çoktan adreste bulunan kripto paraları başka bir adrese taşımış olabilecektir. Tekrar vurgulanırsa, bir adrese ait gizli anahtarı elinde bulunduran herkes o adres üzerinde istediği işlemi gerçekleştirebilir.

Müsaderenin gerçekleştirilebilmesi adına yukarıda sayılan engellerden hiçbirinin olmadığını farz edelim; kripto paranın bulunduğu adres tespit edilebilmiş, adrese erişimi sağlayacak bilgiler elde edilmiş ve bu aşamalar gerçekleşirken adres üzerindeki kripto paralar başka biri tarafından başka bir adrese taşınmamış bulunsun; bu durumda dahi müsadereyi engelleyecek birtakım etkenler bulunabilir. Örneğin kripto paralar bir akıllı

⁷⁹⁸ <https://gnosis-safe.io/> (Erişim: 21.07.2022)

sözleşme vasıtasıyla herhangi bir dApp⁷⁹⁹ üzerinde belirli bir süreliğine (1 ay, 1 yıl, 4 yıl vs.) kilitlenmiş olabilir. Bu ihtimalde söz konusu kripto para üzerinde kilit süresi bitene kadar herhangi bir tasarruf yapılamayacaktır. Yine de eğer ilgili dApp, kilitlenen kripto paralara denk bir şekilde token oluşturup, bu tokenları transfer etmeye ya da ikincil marketlerde satma imkanı sağlıyorsa; bu şekilde kilitlenen kripto paralar müsadere edilebilecektir.

Müsaderenin gerçekleşebilmesinin önündeki bir diğer engel ise, söz konusu adresin tuttuğu kripto paraların hangi ağlarda, protokollerde ya da dApp'ler üzerinde bulunduğu sorunudur. Tek bir adres, birden fazla blok zincir üzerinde kripto para bulunduruyor olabilir. Bu konuda en çok karşılaşılan örnek EVM⁸⁰⁰ uyumlu adreslerdir. EVM uyumlu bir adres, EVM uyumlu birden çok blok zincir⁸⁰¹ üzerinde kripto para işlemi yapabilir; bu nedenle EVM uyumlu farklı blok zincirler üzerinde farklı adres açılmasına gerek yoktur. Çoğunlukla bir adresin EVM uyumlu blok zincirlerde bulundurduğu kripto paranın miktarı, çeşidi ya da ağ üzerinde olmakla birlikte bu ağlar üzerinde oluşturulmuş merkeziyetsiz platformlar ile etkileşimde bulunan kripto paranın miktarı ve çeşidini, etkileşime girilen akıllı kontratlar da dahil olmak üzere yapılan bütün işlemleri, çeşitli ağ tarayıcıları kullanılarak tespit etmek mümkündür⁸⁰². Yine de bu tür tarayıcılar kullanılarak ağlar üzerinde tutulan bütün kripto paralar tespit edilemeyebilir. Örneğin çalışmanın yukarısında detaylı bir şekilde bahsedildiği üzere, söz konusu kripto paralar gizlilik sağlayan bir Rollup olan Aztec Network gibi ikincil katmanlarda/platformlarda tutuluyorsa, bunun tespiti söz konusu blok zincir tarayıcıları kullanılarak yapılamayacaktır. Bu nedenle her platformun teker teker incelenmesi gerekebilecektir.

Müsaderenin başarılı bir şekilde tamamlanabilmesi, müsadere edilecek kripto paraların (ya da NFT gibi yüksek değer taşıyabilen ERC-721 standartlı varlıklar) güvenli bir adrese taşınması ile tamamlanacaktır. Bu adresin kim tarafından kontrol edileceği, güvenliğinin nasıl sağlanacağı gibi hususların gerçekleştirilecek hukuki düzenlemeler ile usulen ortaya konması gerekecektir.

⁷⁹⁹ *En.* Decentralised Application. *Tr.* Merkeziyetsiz Uygulama.

⁸⁰⁰ Çalışmanın yukarısında incelenmiştir.

⁸⁰¹ Örneğin Ethereum, Fantom, Polygon, BNBChain, Avalanche C-Chain vb.

⁸⁰² Örn.: <https://etherscan.io/>, <https://debank.com/>, <https://blockscout.com/>.

Şu anki düzenlemeler çerçevesinde, kripto paraların müsadereesine ilişkin en çok başvurulacak kanun düzenlemesi şüphesiz Türk Ceza Kanununun 55. Maddesinin 2. Fıkrası olacaktır. Zira uygulamada çoğunlukla söz konusu kripto paralara erişilemeyeceğinden, bunların karşılığını oluşturan değerlerin müsadereesine karar verilebilecektir. Zira ilgili fıkra da “*Müsadere konusu eşya veya maddi menfaatlere elkonulmadığı veya bunların merciine teslim edilmediği hallerde, bunların karşılığını oluşturan değerlerin müsadereesine hükmedilir.*” denilmektedir.

Terörizmin finansmanı suçunda fon olarak kullanılan kripto paraların müsadereesi ile ilgili açıklamalar bitirilmeden önce, yapılacak müsadereenin eşya müsadereesi mi yoksa kazanç müsadereesi mi olacağı konusuna değinmek gerekecektir. Bu başlık altında değinildiği üzere kripto paraların müsadereesi kazanç müsadereesi çerçevesinde gerçekleştirilecektir; zira terörizmin finansmanı suçunun maddi konusunu oluşturan fon bu durumda kripto para olmakla birlikte zaten kripto paraların hukuken eşya niteliğinde olduğunu söyleme mümkün değildir. Bununla birlikte donanım cüzdanı, kağıt cüzdan; ya da söz konusu adrese erişimi sağlayan gizli anahtar, keystore dosyası ve anımsatıcı dizi gibi bilgileri içeren kağıt ya da teknolojik aygıtların müsadereesinin hangi müsadere çeşidine gireceği tartışılabilir. Donanım cüzdanı, kağıt ya da bilgileri saklayan dijital diğer donanım aygıtlarının fiziki yapıları gereği eşya sayılmaları mümkündür. Zira üzerinde gizli anahtar yazılı olsa da sonuçta kağıt bir eşyadır; ya da içerisinde kripto para adresine ait keystore dosyasını buldursa da bilgisayar bir eşyadır. Bu eşyaların Türk Ceza Kanununun 54. Maddesi gereği müsadere edilmelerinde bir sakınca yoktur. Doktrinde Hafizoğulları ve Özen’in savunduğu görüşe göre, eşya müsadereesi ile ilgili 54/1 hükmünde bahsedilen “*suçun işlenmesinde kullanılan eşya*”, “*suçun işlenmesine tahsis edilen eşya*” ya da “*suçtan meydana gelen eşya*” suçun maddi konusunu oluşturan eşya değildir. Bu nedenle suçun konusunu oluşturan eşya, müsadere konusu eşya değildir⁸⁰³. Bu görüşe katılmakla birlikte; bu görüşün donanım cüzdanı, kağıt cüzdan ya da ilgili adrese erişimi sağlayan diğer bilgileri içeren eşyaların eşya müsadereesi hükümlerine göre müsadere edilmelerinde bir sakınca bulunmayacaktır; zira donanım cüzdanı da olsa, kağıt cüzdan da olsa bu eşyalar kripto paranın kendisi değildir; kripto para blok zincirde bulunur; bu eşyalar bir bakıma kripto paralara erişimi sağlayan

⁸⁰³ Hafizoğulları ve Özen, 2021, s. 480.

eşyalardır. Bu doğrultuda terörizmin finansmanı suçunun maddi konusunu oluşturan fon olan kripto paralara erişimi sağlayan bu eşyalar “suçun işlenmesinde kullanılan eşya” olarak kabul edilerek eşya müsaderesine konu olabilir. Tekrar vurgulamak gerekir ki terörizmin finansmanı suçunun maddi konusu bu eşyalar değil, blok zincir üzerinde, ilgili adreste bulunan kripto paradır. Fakat yine de belirtmek gerekir ki, bu tür eşyaların eşya müsaderesi ile müsadere edilmesi pratikte gereksiz olacaktır; zira bu eşyalar müsadere edilse bile erişimi sağladıkları adreste bulunan kripto paralar müsadere edilmiş olmayacaktır; kripto paralar blok zincir üzerinde yine aynı adres üzerinde duracaktır. Sonuç olarak asıl amaç bu kripto paraların blok zincir üzerinde müsadere edilecek başka bir cüzdana taşınması olacağından; ilgili eşyaların elkoyma tedbirini takiben kazanç müsaderesi ile adreste bulunan kripto paraların müsadere edilmesine karar verilmesi daha isabetli olacaktır.

SONUÇ

Blok zincir kriptografik işlemlerin gruplaşarak meydana getirdiği bloklardan oluşan, kurcalamayı belli eden ve kurcalamaya dayanıklı dağıtık dijital defterler ya da bir diğer tabir ile dağıtık veri tabanlarıdır. Blok zincir teknolojisi bir kişinin, bir kurumun, bir merkezi otoritenin, bir aracının tahakkümü altında değildir. Blok zincir, güvenilir üçüncü tarafın, merkezi bir otoritenin sağlayabildiği kısmi güveni; dağıtık yapı mimarisisiyle tek bir lidere bağımlı olmaksızın mutlak güvene dönüştüren bir teknolojidir.

Beşeri ilişkilerde güvenilir bir kuruma olan ihtiyaç, insanlığın başlangıcından itibaren var olmaktadır. Kurumlar, insanlar arasında bir aracı işlevi görerek, güven bunalımının kısmen giderilmesine hizmet etmek amacıyla, toplum tarafından oluşturulurlar. Bu doğrultuda kurum, yeri geldiğinde devlet, yeri geldiğinde yasa, yeri geldiğinde bir banka olabilir. Toplum, gündelik hayatta kendi içerisinde etkileşimde bulunurken ihtiyaç duyduğu güveni sağlamak amacıyla, kendiler tarafından oluşturulan ve “güvenli” olduğuna inanılan bu kurumlara güvenirler. Fakat merkezi olan bu yapıların, dışarıdan müdahalelere açık olması, bir kişi, grup ya da başka bir kurum tarafından kontrol edilebilmesi, ne derece güvenli olabileceği konusunda soru işaretleri barındırmaktadır. Bu doğrultuda güveni sağlamak amacıyla güvenilirliği sorgulanabilen bir yapıya dayanmak çelişkili bir durum oluşturmaktadır. İşte blok zincir teknolojisi tam da bu aşamada devreye girmektedir. Merkezi olmayan ve dolayısıyla herhangi bir kişi, grup kurum ya da aracının tahakkümü altında olmayan bu teknoloji, kısmi güveni mutlak güvene dönüştürmektedir. Çünkü blok zincir tamamen şeffaf ve tamamen tarafsızdır.

Blok zincir merkeziyetsiz olduğundan ve herhangi bir kişi ya da grubun istekleri doğrultusunda işlemediğinden, blok zincirlerin hangi amaç doğrultusunda kullanılacağı da merkeziyetsiz bir şekilde kullananların isteği doğrultusunda, farklı görünüm çerçevesinde ortaya çıkabilirler. Bu çalışmada daha çok blok zincirin “ödeme aracı” olan görünümü yani kripto paralar üzerinde durulmuştur.

2008 yılında Satoshi Nakamoto'nun “Bitcoin: A Peer-to-Peer Electronic Cash System” adlı makalesi ile ortaya çıkan kripto paralar, “dağıtık bir yapıya sahip, merkezi bir otoriteye dayanmayan, herkese açık, şifrelemeye dayalı para” olarak tanımlanabilir. Oldukça özellik ihtiva eden kripto paraların, genel olarak paranın ortaya çıkış süreci ve

blok zincirin ortaya çıkış süreci çerçevesinde incelenmesi, bulunduğu konumu ortaya koymak adına gereklidir.

Bu doğrultuda çalışmaya, Smith ve takip eden ekonomistler tarafından “paranın kökeni” olarak kabul edilen “takas” kavramı açıklanarak giriş yapılmıştır. Fakat çağdaş antropologların birçoğunun kabul ettiği görüşe göre bu yaklaşımın doğru olmadığı, paranın kökenlerinin takasa dayanmadığı açıklanmıştır.

Tarih boyunca birçok şey para amacıyla kullanılmıştır. Deniz kabuğundan, yerinden oynatılamayacak kadar büyük kayalara; gümüşten, canlı hayvanlara kadar oldukça geniş bir yelpazede gerçekleşen para kullanımı, bir şeyin para olma gücünü nereden aldığı sorusunu da akla getirir. Bu doğrultuda paranın para olma gücünü kendisinden aldığı, toplumdaki aldığı, devletten aldığı ya da kurumsal yapıdan aldığı belirtilmiştir. Para olarak kullanılan şeylere bakıldığında, bunların bu görüşlerden bir veya birden fazlasını karşılayabildiği görülmektedir.

Lidyalılardan bu yana en baskın para türü, değeri kendiliğinden gelen ve yukarıdaki görüşlerin birden fazlasına uyan emtia para olmuştur. Parasal sistem, günümüze kadar çoğunlukla emtia paralar, özellikle altın ve gümüş etrafında şekillenmiştir. Bu doğrultuda uluslararası para sistemlerinden olan gümüş ve altın standartları, her ikisini ihtiva eden çift metal sistemi, altın değişim standardı ve dolara dayalı altın sistemi olan Bretton Woods sistemlerinin altın ve gümüş emtialarına dayanması bu durumu doğrulamaktadır.

Bretton Woods sisteminin 70’li yılların başında yerini dalgalı kur sistemine bırakmasından milenyuma doğru, teknolojik ilerlemelerin parabolik bir artışla hız kazanması, yeni ödeme sistemlerini ve yeni para türlerini de ortaya çıkarmıştır. Para olarak kullanılan ilk nesnelere bu yana fiziki olan paranın yerini, 1’ler ve 0’lardan oluşan, elle tutulamayan paralar almıştır. Bunlar elektronik, dijital, sanal ve kripto paralardır.

Kripto paraların sayılan paralar arasında en özellik gösteren para türü olduğu söylenebilir. Oldukça yeni bir teknolojiye, karmaşık ve bir yandan da dinamik bir yapıya sahip olması; anonimlik, gizlilik, takip edilemezlik ve izlenemezlik gibi özelliklere sahip olması kişilerin, toplulukların, ulusal ve uluslararası aktörlerin yakın takibine neden olmuştur. Bunlar arasında kripto paraları yakından takip eden azımsanmayacak bir kısım, kripto paraları hukukun yasakladığı eylemleri gerçekleştirmek amacıyla kullananlardan

oluşmaktadır. Bu çalışmanın konusunu da bu eylemlerden olan terörizmin finansmanının, kripto paralar aracıyla gerçekleştirilmesi oluşturmaktadır.

Her teknoloji gibi blok zincirin de hukukun yasakladığı bazı eylemlerin gerçekleştirilmesinde bir araç olarak kullanılabilceğini söylemek mümkündür. Diğer teknolojilerde olduğu gibi, teknolojinin yasak bir eylemi gerçekleştirmek için kullanılmış olması, teknolojinin kullanılmaya devam edilmesine engel oluşturmaz. Örneğin basitçe bir bankayı soymak için otomobilin bir araç olarak kullanılması; bir dolandırıcılık eylemi için mobil iletişimin kullanılması; ya da yasadışı bahis sitesi için Web ağının kullanılmış olması durumlarında otomobilin, mobil iletişimin ya da İnternet ağı gibi teknolojilerin kullanımının yasaklanması gibi sonucun ortaya çıkması beklenilmez. Aynı şekilde blok zincir teknolojisinin de hukukun yasakladığı eylemleri gerçekleştirilmek için kullanılması, bir daha kullanılmayacağı ya da yasaklanacağı anlamına gelmemelidir. Bu anlama getirilmesi durumunda bile, blok zincirin merkezi bir otoriteye dayanmaması ve dağıtık bir yapıda olması sebebiyle yasaklanması pratikte mümkün değildir, ancak blok zincir ile ilişkili bazı uygulamaların yasaklanması söz konusu olabilir. Çünkü blok zincire erişim herkese, “bir aracı olmaksızın” açıktır.

Fakat yine de bu durum, yasa koyucuların ve otoritelerin elleri bağı bir şekilde olanları izleyeceği anlamına da gelmeyecektir. FATF'nin “Yeni Teknolojiler” başlıklı 15 numaralı tavsiyesine göre, ülkeler ve finansal kuruluşlar, yeni ve gelişen teknolojilerin kullanımına bağılı olarak ortaya çıkabilecek terörizmin finansmanı riskini tespit etmeli ve değerlendirmelidir. FATF'nin söz konusu tavsiyesi ve diğer tavsiyeleri uyarınca devletler gerekli hukuki düzenlemeleri gerçekleştirmeye çalışsa da, blok zincir teknolojisi ve kripto paraların on dört yıldır kullanıldığı düşünöldüğüne henüz çoğu düzenlemenin taslak haline bile varamamış olması düşündürücü ve kaygı vericidir. Mevcut bu boşluktan faydalanarak terörizmin finansmanının kripto paralar ile gerçekleştirildiğı birçok örnek mevcuttur. El Kaide, DEAŞ gibi terör örgütlerinin kripto paralar kullanılarak finanse edildikleri bilinmekle birlikte, henüz bilinmeyen ya da gelecekte ortaya çıkacak çeşitli fon sağlama eylemlerinin kontrol altına alınabilmeleri ise ancak blok zincirin ve kripto paraların temel prensiplerinin oldukça iyi bilinmesi ve bu doğrultuda düzenlenmeleri ile mümkün olabilir. Aksi takdirde yapılan düzenlemeler pratikte bir anlam ifade etmeyecektir.

Terörizmin finansmanı “terör eylemlerinde bulunan kişi ya da grupların faaliyetlerini sürdürebilmeleri için gerekli para ve mali desteği verme” şeklinde tanımlanabilir. Terörizmin finansmanı ile ilgili en önemli belge, 1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme’dir. Sözleşmeye taraf olan devletlere, terörizmin finansmanını engellemeye yönelik gerekli tedbirleri alma zorunluluğu, terörizmin finansmanına yönelik faaliyet gösteren sivil veya idarecileri yakalama, sözleşmenin ikinci maddesinde belirtilen suçların iç hukukta da suç olarak düzenlenmesi gibi yükümlülükler yüklenmiştir.

Barış ve güvenliğin sağlanması amacını taşıyan Birleşmiş Milletler Güvenlik Konseyi’nin, Birleşmiş Milletler Antlaşması’nın VII. bölümüne dayanarak aldığı kararlar üye devletler için bağlayıcıdır. Antlaşması’nın 25. maddesine göre üye devletler Güvenlik Konseyi’nin bu kararları ve uygulanmalarını kabul eder. Bu kapsamda Güvenlik Konseyi’nin Birleşmiş Milletler Antlaşması’nın 41. Maddesine dayanarak aldığı ve çoğunlukla belirli bir kişi ve kişi gruplarını hedef alan “akıllı yaptırım” kararları, terörizmin finansmanının önlenmesi konusunda bağlayıcılığı olan oldukça önemli belgelerdir.

Terörizmin finansmanının önlenmesi doğrultusunda Avrupa Birliği bünyesinde hazırlanan “Finansal Sistemin Karapara Aklama ve Terörizmin Finansmanı Amacıyla Kullanılmasının Önlenmesine Dair Direktif”, “2002/475 sayılı Konsey Çerçeve Kararı” ve Avrupa Konseyi tarafından hazırlanan ve Türkiye’nin de taraf olduğu “Varşova Sözleşmesi” diğer önemli belgelerdir.

Terörizmin finansmanının önlenmesi konusunda uluslararası standartlar belirleyen ve Türkiye’nin de üye olduğu Mali Eylem Görev Gücü’nün (FATF) daha önceden yayınlanan 9 özel tavsiyenin de bulunduğu 40 tavsiyesi, terörizmin finansmanının önlenmesi konusunda uluslararası örgüt ve belgelerin de atıfta bulunduğu temel prensipleri barındırması dolayısıyla oldukça önemlidir. Özellikle 15 ve seyahat kuralı (travel rule) olarak da adlandırılan 16 numaralı tavsiyeler, blok zincir ve kripto paralar ile ilgili yapılan düzenlemelerde belirleyici rol üstlenmektedir.

Türk Hukukunda terörizmin finansmanı suçu ile ilgili temel düzenlemeyi 6415 sayılı “Terörizmin Finansmanının Önlenmesi Hakkında Kanun” teşkil etmektedir. Kanunun ilk maddesinden düzenlemenin Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme’nin ve Birleşmiş Milletler Güvenlik Konseyi’nin kararlarının

uygulanmasının amaçlandığı belirtilmektedir. Kanunun 3. Maddesi uyarınca, “fon sağlama” ve “fon toplama” fiilleri yasaklanmıştır. Sağlanan ya da toplanan fonun paradan ibaret olması gerekliliği bulunmamakta; değeri para ile temsil edilebilen herhangi bir varlık da kapsama dâhil edilmektedir.

Bununla birlikte belirtmek gerekir ki terörizmin finansmanı suçunda failin kim olabileceği konusunda bir takım görüş ayrılıkları bulunmaktadır. Bu ayrılık, terör örgütü üyesinin ayrıca terörizmin finansmanı suçunun faili olup olamaması çerçevesinde gerçekleşip gerek literatür, gerek Yargıtay kararlarında bir birliğin bulunmadığı belirtilmiştir.

Türk hukukunda, terörizmin finansmanının önlenmesine dair tedbirlerden olan malvarlığını dondurma tedbiri ile Güvenlik Konseyi kararları kapsamında düzenlenen 6415 sayılı kanunda karşılaşılmaktadır. Fakat bu tedbirin pratikte kripto paralar hakkında uygulanabilmesinin sadece söz konusu kripto paranın merkezi bir aracı üzerinde tutulması durumunda gerçekleşeceği söylenebilir.

Yukarıda da belirtildiği üzere kripto paralar hakkında işlevsel düzenlemelerin yapılması, ancak kripto paraların dayandığı prensiplerin ve işleyişlerindeki dinamiklerin kavranması doğrultusunda mümkün olabilir. Bu düşünceyi takiben, bu çalışmada da blok zincir ve kripto paraların dayandığı temel prensipler, ortaya çıktıkları süreç içerisinde, yeri geldiğinde detaylandırılarak anlatılmıştır. İlk genel amaçlı dağıtık veri tabanı olan SDD-1’den başlamak üzere, kriptografik hash, Merkle ağacı, Paxos protokolü, dijital belgelerin iş kanıtı ile doğrulanması gibi kriptolojinin meydana getirdiği ürünler ve prensipler, blok zincirin dayandığı unsurları ihtiva etmekte ve Nakamoto’nun 2008 yılında Bitcoin’i ortaya çıkarabilmesini sağlamış bulunmaktadır.

Nakamoto’nun merkeziyetsiz bir ödeme aracı olarak kullanmak amacıyla oluşturduğu blok zincirin, bu amacın oldukça ötesine geçtiği söylenebilir. Günümüzde blok zincir merkeziyetsiz yönetim modellerinden, merkeziyetsiz finansa; kitle fonlamalarından, endüstri 4.0’a kadar birçok konuda temel işleyiş modeli haline gelmektedir. Fakat yine de blok zincirin ödeme aracı olan görünümü olan kripto paralar, hala en popüler blok zinciri uygulaması olarak varlıklarını sürdürmektedir.

Çalışmada kripto paralar detaylı bir şekilde incelenmiş olup, özellikle terörizmin finansmanı aracı olarak kullanılmaya oldukça müsait olan gizlilik odaklı kripto paralar ile; herkese açık bir blok zincir üzerinde olsa dahi, takip edilebilirliği kesen bir takım

teknik ve uygulamalar detaylandırılarak anlatılmıştır. Bu kapsamda her ne kadar terörizmin finansmanı suçunun işlenmesi için hala en çok başvurulan kripto para Bitcoin olsa da, başta Monero olmak üzere gizlilik odaklı kripto paraların da kullanımının giderek arttığı bilinmektedir. Bu tür kripto paralar ile yapılan basit bir aktarım işlemi gizlilik, izlenemezlik ve anonimlik sağlarken; normal şartlarda izlenebilir kripto paraların da çeşitli teknikler ile izlenebilirliklerinin kesilmesi de mümkündür. Özellikle kripto para borsaları üzerinde yapılan bazı alım satım teknikleri ve Ethereum'un ölçeklenmesi kapsamında geliştirilmiş gizlilik odaklı ikinci katman çözümleri, terörizmin finansmanı doğrultusunda henüz geniş çaplı uygulamalara konu olmamış olsa da, başvurulacak ilk yöntemler arasındadır. Belirtmek gerekir ki, çalışmada da örnek verilen bazı terör örgütleri dahilinde ortaya çıkmış kripto paralar ile terörizmin finansmanının sağlanması faaliyetleri, örgütlerin ve fon sağlayanların kripto paralar hakkındaki “bilgisizliklerinden dolayı” tespit edilebilmiştir. Bu nedenle blok zincirin ve kripto paraların bu kişiler tarafından “farkında olarak” kullanımları durumunda, bu tür finansman sağlama faaliyetlerinin oldukça zor tespit edileceğinin ya da hiç tespit edilmeyeceğinin söylenmesi yanlış olmaz.

Kripto paraların terörizmin finansmanı eylemini gerçekleştirmede sağladıkları kolaylıklar bir yana; sağlanan ya da toplanan fonun tespit edilmesi halinde fon üzerinde birtakım tedbirlerin uygulanabilmesini zorlaştırdığı da söylenebilir. Çalışmada bu doğrultuda malvarlığının dondurulması, elkoyma ve müsadere gibi tedbirlerin mevcut düzenlemeler kapsamında kripto paralar hakkında uygulanmalarının oldukça zor olduğu ortaya konmuştur. Zira karar verilen bu tedbirlerin uygulanabilmesi çoğu zaman ancak söz konusu kripto paranın merkezi bir kripto para borsasında bulunması halinde mümkün olacaktır. Çünkü bir merkez ya da aracı olmaksızın işleyen blok zincir üzerinde bu tür kararların icra edilebilirliğini sağlayacak bir mekanizmadan söz edilemez. Kripto paraların bulunduğu adresler üzerindeki tasarruf yetkisi ancak ve ancak bu adreslere ait gizli anahtar, keystore dosyası ya da anımsatıcı dizi gibi bilgilere sahip olan, yani adreslere erişebilen kişilere aittir. Bu tür bir adres üzerinde bu bilgilere erişmeden alınacak söz konusu tedbirler pratikte bir anlam ifade etmeyecektir.

Yeri geldiğinde temel hak ve özgürlükleri de kısıtlayabilen hukuki düzenlemelerin oluşumuna katkı sağlayan hukukçuların ve bu hukuki düzenlemelere son halini veren yasa koyucuların düzenleme getirilen konu ile ilgili donanımlı olmaları şarttır. Bu çalışma

da, söz konusu şekilde bir kaygı güdülerek oluşturulmuştur. Bu nedenle blok zincir ve kripto paralar ile ilgili gelecekte yapılacak düzenlemelerin; bu teknolojilerin çalışma prensiplerinin, uygulamadaki dinamiklerinin ve blok zincir ile kripto para ekosistemine dahil olan aktörlerin davranış biçimleri göz ardı edilmeyecek bir biçimde hazırlanması gerekmektedir. Aksi takdirde yapılan düzenlemelerin ihtiyaca cevap vermemesi riski dâhilinde, pratikte bir anlam ifade etmemeleri sonucu ortaya çıkacaktır. Bu nedenle terörizmin finansmanı aracı olarak kullanılacak kripto paralar kapsamında, bu eylemi gerçekleştirenlerden her daim bir adım önde olmak şarttır.



KAYNAKÇA

- Adrian, Tobias ve Mancini-Griffoli, Tommaso, “The Rise Of Digital Money”, International Monetary Fund, 2019. <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097> (Eriřim: 28.04.2022)
- AFM, “Initial Coin Offerings (ICO’s): serious risks”, <https://www.iosco.org/library/ico-statements/Netherlands%20-%20AFM%20-%20Initial%20Coin%20Offerings%20Serious%20Risks.pdf> (Eriřim: 29.05.2022)
- Akdoğan, Ece Ceylan, “Uluslararası Para Sisteminin Gemiři, Bugünü ve Geleceęi”, *Çankaya Üniversitesi Hukuk Fakültesi Dergisi*, 2020/5 (1), ss. 91-120. <http://earsiv.cankaya.edu.tr:8080/xmlui/bitstream/handle/20.500.12416/4711/Akdoğan%2C%20Ece%20C..pdf?sequence=1&isAllowed=y> (Eriřim: 15.04.2022)
- Ali vd., “Innovations in Payment Technologies and the Emergence of Digital Currencies”, Bank of England Quarterly Bulletin, 2014/54 (3). <https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/innovations-in-payment-technologies-and-the-emergence-of-digital-currencies.pdf> (Eriřim: 24.04.2022)
- Altınır Cořkun, Sümeyra, Birleřmiř Milletler Güvenlik Konseyi, Akıllı Yaptırım Kararları ve Terörizmin Finansmanının Önlenmesi, Seçkin Yayıncılık, Ankara 2015.
- Altınır Cořkun, Sümeyra, Terörizmin Finansmanının Önlenmesine Yönelik Birleřmiř Milletler Güvenlik Konseyi’nin Akıllı Yaptırım Kararları, (doktora tezi), Ankara Üniversitesi, Kamu Hukuku Anabilim Dalı, Ankara, 2015.
- Amato, Massimo, Fantacci, Luca, “Back to which Bretton Woods? Liquidity and clearing as alternative principles for reforming international Money”, *Cambridge Journal of Economics*, 2014/38 (6), ss. 1-14. https://www.researchgate.net/publication/228461779_Back_to_which_Bretton_Woods_Liquidity_and_clearing_as_alternative_principles_for_reforming_international_money (Eriřim: 19.04.2022)

Anayasa Mahkemesi, 31.1.2008 T., 2004/81 E., 2008/48 K.

Araujo vd., On the Origin of Money, 2016.
https://extranet.sioe.org/uploads/sioe2017/araujo_bignon_breton_camargo.pdf
(Eriřim:01.06.2022)

Asadov, Alam, Masih, Mansur, “Reversal of monetary history: Is return to trimetalism a viable alternative?”, 2016.
https://www.researchgate.net/publication/319814437_Reversal_of_monetary_history_Is_return_to_trimetalism_a_viable_alternative (Eriřim: 17.04.2022)

Ateřen, Kerem, “Paxos Algoritması”, <https://bag.org.tr/?p=508>. (Son eriřim: 30.03.2022)

Atsan, Nuray, Oruç Erdoğan, Eda, “Giriřimciler İin Alternatif Bir Finansman Yöntemi: Kitlesele Fonlama (Crowdfunding)”, *Eskiřehir Osmangazi Üniversitesi İİBF Dergisi*, 2015/10 (1), ss. 297-320. <https://dergipark.org.tr/tr/download/issue-full-file/27324> (Eriřim: 12.12.2019)

Aust, Anthony, Handbook of International Law, Cambridge University Press, Second Edition. https://books.google.com.tr/books?id=74Zmct-7hGIC&pg=PA265&redir_esc=y#v=onepage&q&f=false (Eriřim: 06.05.2022)

Aydın, Devrim ve Arslan, Çetin, Sutan Kaynaklanan Malvarlığı Deđerlerini Aklama ve Terörizmin Finansmanı Suu, Yetkin Yayınları, Ankara 2021.

Back, Adam, “Hashcash - A Denial of Service Counter-Measure”.
https://www.researchgate.net/publication/2482110_Hashcash_-_A_Denial_of_Service_Counter-Measure (Son eriřim: 05.04.2022)

Bamberger vd., “Verification Dilemmas In Law And The Promise Of Zero-Knowledge Proofs”, *Berkeley Technology Law Journal*, 2022/37 (1), s. 101.
<https://ssrn.com/abstract=3781082> (Eriřim: 07.07.2022)

Bank for International Settlements, Central bank digital currencies: foundational principles and core features, 2020. <https://www.bis.org/publ/othp33.pdf> (Eriřim: 27.04.2022)

- Bank of England, One Bank Research Agenda, 2015. <https://www.bankofengland.co.uk/-/media/boe/files/research/one-bank-research-agenda---summary.pdf?la=en&hash=B2C820FBF6A960C4A625C2DAB5B5B6CE4FEDF120> (Erişim: 25.04.2022)
- Barrdear, John, Kumhof, Michael, “The Macroeconomics Of Central Bank Issued Digital Currencies”, Staff Working Paper No. 605, 2016. <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1> (Erişim: 26.04.2022)
- Bech, Morten, Garratt, Rodney, Central Bank Cryptocurrencies, BIS Quarterly Review, 2017. https://www.bis.org/publ/qtrpdf/r_qt1709f.html (Erişim: 27.04.2022)
- Belleflamme vd., “Crowdfunding: Tapping the right crowd”, Journal of Business Venturing, 2014/29 (5), ss. 585-609. <https://www.sciencedirect.com/science/article/abs/pii/S0883902613000694> (Erişim tarihi: 07.05.2022)
- Ben Laurie, “An Efficient Distributed Currency”, 2011. <https://www.links.org/files/distributed-currency.pdf> (Erişim: 26.04.2022)
- Bernstein vd., "The Concurrency Control Mechanism of SDD-1: A System for Distributed Databases (The Fully Redundant Case)," *IEEE Transactions on Software Engineering*, 1978/4 (3). <https://ieeexplore.ieee.org/document/1702517> (Erişim: 03.05.2022)
- Bewley, Truman, “The Optimum Quantity of Money, 1979, <https://www.kellogg.northwestern.edu/research/math/papers/383.pdf> (Erişim: 09.04.2022)
- Binance, “Binance Launchpad”, <https://launchpad.binance.com/> (Erişim: 02.06.2022)
- Bitcoin, “Protect Your Privacy”, <https://bitcoin.org/en/protect-your-privacy#:~:text=Understanding%20Bitcoin%20traceability&text=All%20Bitcoin%20transactions%20are%20public,privately%20by%20each%20user%27s%20wallets.> (Erişim: 21.05.2022)

- Bitcoincore, “*Bitcoin Core requires a one-time download of about 400GB...if you enable pruning, you can store as little as 6GB total without sacrificing any security...*”, <https://bitcoincore.org/en/download/> (Erişim:05.05.2022); Statista, “*Size of the Bitcoin blockchain from January 2009 to April 4, 2022*”, <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/> (Erişim: 05.05.2022)
- Bitcointalk, Summary – satoshi, <https://bitcointalk.org/index.php?action=profile;u=3> (Erişim:26.05.2022)
- Bittrex Global, “Delisting of XMR, ZEC, DASH, and GRIN”, <https://bittrexglobal.zendesk.com/hc/en-us/articles/360018560640-Delisting-of-XMR-ZEC-DASH-and-GRIN> (Erişim: 28.05.2022)
- Blizzard, “Trading Items and Services for Real Money”, <https://us.battle.net/support/en/article/269874#:~:text=You%20are%20not%20allowed%20to,or%20services%20for%20real%20money.> (Erişim: 01.05.2022)
- Blizzard, “Using a WoW Token”, <https://eu.battle.net/support/en/article/000031218> (Erişim: 01.05.2022)
- Blockchain.com, “Blok 0”, <https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f> (Erişim: 26.05.2022)
- Blockchain.com, “Charts”, <https://www.blockchain.com/charts> (Erişim:24.05.2022)
- Board Of Governors Of The Federal Reserve System, Money and Payments: The U.S.Dollar in the Age of Digital Transformation, The Federal Reserve System, 2022, s.1. <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf> (Erişim: 28.04.2022)
- Bordo vd., "Gold, Fiat Money, and Price Stability." *B.E. Journal of Macroeconomics: Topics in Macroeconomics* 7, 2007, s. 5. <https://www.nber.org/papers/w10171> (Erişim: 20.04.2022)
- Bordo, Michael D. ve J. Schwartz, Anna, A Retrospective on the Classical Gold Standard, 1821-1931, University of Chicago Press, 19841 <http://www.nber.org/books/bord84-1> (Erişim: 17.04.2022)

- Bordo, Michael D., Gold Standard, <https://www.econlib.org/library/Enc/GoldStandard.html> (Erişim: 16.04.2022)
- Boughtan, James M., Why White, Not Keynes? Inventing the Post-War International Monetary System, International Monetary Fund, 2002. <https://www.imf.org/external/pubs/ft/wp/2002/wp0252.pdf> (Erişim:19.04.2022)
- Bozkurt Yüksel, A. Ebru, “Elektronik Para, Sanal Para, Bitcoin Ve Linden Doları’na Hukuki Bir Bakış”, *İÜHFM*, 2015 (2), ss. 173-220. <https://dergipark.org.tr/tr/download/article-file/230763> (Erişim: 30.04.2022)
- Brinton, Crane. “The History of Paper Money to the War.”, *The Journal of Modern History*, 1934/6 (3), ss. 308-318. <http://www.jstor.org/stable/1871279> (Erişim: 21.04.2022)
- Brunner, Karl, Meltzer, Allan H., “The Uses of Money: Money in the Theory of an Exchange Economy.” *The American Economic Review*, 1971/61 (5), ss. 784-805. <http://www.jstor.org/stable/1813142> (Erişim: 13.04.2022)
- Buterin, Vitalik, “Ethereum: A Next-Generation Smart Contract and Decentralized Application” Platform, 2014. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_White_Paper_-_Buterin_2014.pdf (Erişim: 05.04.2022)
- Buterin, Vitalik, “Slasher: A Punitive Proof-of-Stake Algorithm”, 2014/b, <https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/> (Erişim:25.05.2022)
- Buterin, Vitalik, A Guide to 99% Fault Tolerant Consensus, 2018, https://vitalik.ca/general/2018/08/07/99_fault_tolerant.html (Erişim: 19.05.2022)
- Buterin, Vitalik, A Prehistory of the Ethereum Protocol, 14.09.2017, <https://vitalik.ca/general/2017/09/14/prehistory.html> (Erişim:24.05.2022)
- Castro, Miguel, Liskov, Barbara, “Practical Byzantine Fault Tolerance”, Massachusetts Institute of Technology, 1999. <https://pmg.csail.mit.edu/papers/osdi99.pdf> (Erişim: 17.05.2022)

- Centel, Nur vd., “Türk Ceza Hukukuna Giriş, (11. Baskı), Beta, İstanbul 2020,
- Chainalysis, 2020, s. 73.; The United States Department of Justice, Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, 13.08.2020. <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns> (Erişim:23.05.2022)
- Chainalysis, The 2020 State Of Crypto Crime, 2020. <https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/257%20-%200001%20Appendix%20A%20-%202020-Crypto-Crime-Report%20Chainanalysis.pdf> (Erişim: 23.05.2022)
- Chainalysis, The 2021 Crypto Crime Report, 2021. <https://safewayconsultoria.com/wp-content/uploads/2021/09/Chainalysis-Crypto-Crime-2021.pdf> (Erişim:23.05.2022)
- Chaliand, Gérard ve Blin, Arnaud, “The History of Terrorism”, University of California Press, 2016. <https://doi.org/10.1525/9780520966000-007> (Erişim: 06.05.2022)
- Chapman, Anne, “Barter as a Universal Mode of Exchange”, *L'Homme*, 1980. https://www.persee.fr/doc/hom_0439-4216_1980_num_20_3_368100 (Erişim: 10.04.2022)
- Charapko vd., “Bridging Paxos and Blockchain Consensus.”, *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018. <https://cse.buffalo.edu/~demirbas/publications/bridging.pdf> (Erişim: 31.03.2022)
- Chaum vd., “Untraceable Electronic Cash”, *Advances in Cryptology - CRYPTO '88, LNCS 403*, 1990. http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf (Erişim:21.05.2022)
- Chaum, David L., *Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups*, University of California, Berkeley, 1982. https://chaum.com/wp-content/uploads/2022/02/chaum_dissertation.pdf (Erişim: 01.05.2022)

- Chaum, David, "Blind Signatures for Untraceable Payments", *Advances in Cryptology*. Springer, Boston, MA, 1983. https://doi.org/10.1007/978-1-4757-0602-4_18 (Erişim: 05.05.2022)
- Chaum, David, "Security Without Identification: Card Computers To Make Big Brother Obsolete", 1987. <https://ir.cwi.nl/pub/5519/5519D.pdf> (Erişim: 10.05.2022)
- Chaum, David, "Security Without Identification: Transaction Systems To Make Big Brother Obsolete", *Communications of the ACM*, 1985/28 (10), ss. 1030-1044. <https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf> (Erişim: 05.05.2022)
- Chevalier, Michel, *On the Probable Fall in the Value of Gold*. D. Appleton and Company, 1859. <https://oll.libertyfund.org/title/cobden-on-the-probable-fall-in-the-value-of-gold> (Erişim: 17.04.2022)
- Cirillo, Renato, "Leon Walras' Theory of Money." *The American Journal of Economics and Sociology*, 1986/45 (2), ss. 215-221. <http://www.jstor.org/stable/3486926> (Erişim: 17.04.2022)
- Clower, Robert W.. "A Reconsideration Of The Microfoundations Of Monetary Theory." *Economic Inquiry*, 1967/6, ss. 1-8. <https://www.semanticscholar.org/paper/A-RECONSIDERATION-OF-THE-MICROFOUNDATIONS-OF-THEORY-Clower/416792d58f668aafc6cb0b9a56aef70daeb1c7b2> (Erişim: 09.04.2022)
- CoinMarketCap, "Bitcoin", <https://coinmarketcap.com/tr/currencies/bitcoin/> (Erişim:24.05.2022)
- CoinMarketCap, "Ethereum", <https://coinmarketcap.com/currencies/ethereum/> (Erişim:25.05.2022)
- Coinmarketcap, "Nxt", <https://coinmarketcap.com/tr/currencies/nxt/> (Erişim: 02.06.2022)
- CoinMarketCap, "Tether", <https://coinmarketcap.com/currencies/tether/> (Erişim: 28.05.2022)

- Committee on Payments and Market Infrastructures (CPMI), Central bank digital currencies, Bank for International Settlements, 2018. <https://www.bis.org/cpmi/publ/d174.pdf> (Erişim: 27.04.2022)
- Committee on Payments and Market Infrastructures (CPMI), Digital Currencies, 2015, Bank For International Settlements. <https://www.bis.org/cpmi/publ/d137.pdf> (Erişim: 22.04.2022)
- Congressional Research Service, Foreign Terrorist Organization (FTO), 2019, <https://sgp.fas.org/crs/terror/IF10613.pdf> (Erişim: 23.05.2022)
- Cooper, Richard N. vd., “The Gold Standard: Historical Facts and Future Prospects.” *Brookings Papers on Economic Activity*, 1982/1, ss. 1-56. <https://doi.org/10.2307/2534316> (Erişim: 16.04.2022)
- Council of Europe, Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, <https://rm.coe.int/168008371f> (Erişim: 09.05.2022)
- Council of the European Union, MiCA: Proposal for a regulation on Markets in crypto-assets - Three-column table to commence trilogues, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7694_2022_INIT&qid=1653200871902&from=EN (Erişim: 22.05.2022)
- Council of the European Union, Proposal for a Regulation Of The European Parliament And Of The Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, 2020, https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF (Erişim: 22.05.2022)
- Court of Justice of the European Union, The Court of Justice upholds the acts of the Council maintaining Hamas on the European list of terrorist organisations, 23.11.2021, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210208en.pdf> (Erişim: 23.05.2022)

- Crosby, Mark, "Currency Unions, Currency Boards and Other Fixed Exchange Rate Arrangements", *The Australian Economic Review*, 2001/34, ss. 367-372. <http://neyapti.bilkent.edu.tr/Readings/CU-CB.pdf> (Eriřim: 17.04.2022)
- Çetin, Soner Hamza, *Terörizmin Finansmanı Suçu*, Bilge Yayınevi, (1. Baskı), Ankara, 2017.
- Dai, Wei, "b-money", 1998, <http://www.weidai.com/bmoney.txt> (Son eriřim: 03.04.2022)
- Dalton, George. "Barter." *Journal of Economic Issues - Association for Evolutionary Economics*, 1982/16 (1), ss. 181-190. <http://www.jstor.org/stable/4225147> (Eriřim: 11.04.2022)
- Danezis, George, Meiklejohn, Sarah, "Centrally Banked Cryptocurrencies", 2015. <https://eprint.iacr.org/2015/502.pdf> (Eriřim: 25.04.2022)
- Davidson, Paul. "Money and the Real World." *The Economic Journal*, 1972/82 (325), ss. 101-115. <https://doi.org/10.2307/2230209> (Eriřim: 12.04.2022)
- Davies, Glyn, *A History of Money*, University of Wales Press, 2002. https://books.google.com.tr/books?hl=tr&lr=&id=cU2uBwAAQBAJ&oi=fnd&pg=PR3&dq=money+definition&ots=UjkXlZ5BH&sig=YRtg5lQ3x22RW2ec7dktDXsbwVM&redir_esc=y#v=onepage&q=money%20definition&f=false (Eriřim: 14.04.2022)
- de Vegh, I. "The International Clearing Union.", *The American Economic Review*, 1943/33 (3), ss. 534-556. <http://www.jstor.org/stable/1812989> (Eriřim: 18.04.2022)
- de Vries, Margaret Garritsen, *The IMF in a Changing World, 1945-85*, International Monetary Fund, 1986. <https://www.elibrary.imf.org/view/books/071/07050-9780939934652-en/07050-9780939934652-en-book.xml> (Eriřim: 02.06.2022)
- Demir Abaan, Ernur, "Para: Teorik Bir Tarama ve Tartıřma", Türkiye Cumhuriyeti Merkez Bankası, 1997. <https://www.tcmb.gov.tr/wps/wcm/connect/c0f93298-5bb3-40bb-8d38-f8555426ab64/1997-3.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-c0f93298-5bb3-40bb-8d38-f8555426ab64-m3fw5z-> (Eriřim:20.05.2022)

- Diffie, Whitfield, Hellman, Martin E., “New Directions in Cryptography”, *IEEE Transactions On Information Theory*, 1976/22 (6), ss. 644-654. <https://ee.stanford.edu/~hellman/publications/24.pdf> (Eriřim: 03.05.2022)
- DigiCash, “Bank Austria and Den norske Bank to issue ecash the electronic cash for the Internet”, 1997, <https://chaum.com/wp-content/uploads/2022/01/04-14-1997-Bank-Austria-and-Den-norske-Bank-to-issue-ecash™-the-electronic-cash-for-the-Internet.pdf> (Eriřim:14.05.2022)
- DigiCash, “DigiCash’s Ecash to be Issued by Deutsche Bank”, 1996, https://chaum.com/wp-content/uploads/2022/01/05-07-96-DigiCash_s-Ecash™-to-be-Issued-by-Deutsche-Bank.pdf (Eriřim: 14.05.2022)
- DigiCash, “First Bank to Launch Electronic Cash”, 1995, <https://chaum.com/wp-content/uploads/2022/01/10-23-95-First-Bank-to-Launch-Electronic-Cash.pdf> (Eriřim: 14.05.2022)
- DigiCash, “World’s first electronic cash payment over computer networks.”, 1994. https://chaum.com/wp-content/uploads/2022/01/05-27-94-World_s-first-electronic-cash-payment-over-computer-networks.pdf
- Dwork, Cynthia, Naor, Moni, “Pricing Via Processing or Combatting Junk Mail.”, *Advances in Cryptology: CRYPTO 1992*, Annual International Cryptography Conference, 1992. <https://web.cs.dal.ca/~abrodsky/7301/readings/DwNa93.pdf> (Son eriřim: 05.04.2022)
- Ellison, M., Monetary Economics, Chapter 4 – Cash in Advance Model, lecture notes. <https://users.ox.ac.uk/~exet2581/msc/ec924cia.pdf> (Eriřim: 09.04.2022)
- Erdem, Mete, “BRICS Kořullu İhtiyat-Fonu Düzenelemeı: Hukuksal ve Kurumsal İnceleme”, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 2016/7 (1), ss. 295-350. <https://doi.org/10.21492/inuhfd.387923> (Eriřim: 02.07.2022)
- Erem, Faruk, “Suçun Konusu ve Hümanist Doktrin”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 1968/25 (1-2), ss. 11-33. <https://dergipark.org.tr/en/download/article-file/632330> (Eriřim. 11.05.2022)

- Erzurumlu, Nurbanu, “Türk Hukukunda Fikrî Mülkiyete Konu Malların Cebrî İcrası”, Yıldırım Beyazıt Hukuk Dergisi, 2017/3. <https://dergipark.org.tr/tr/download/article-file/270859> (Erişim: 09.07.2022)
- Ethereum, “Proof-of-Stake (PoS)”, <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> (Erişim: 20.05.2022)
- Ethereum, “Proof-of-Stake (PoS)”, <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#:~:text=Ethereum%20has%20used%20PoW%20since,scaling%20solutions%20to%20be%20implemented.> (Erişim:25.05.2022)
- Ethereum, “Shard chains”, <https://ethereum.org/en/upgrades/shard-chains/> (Erişim: 25.05.2022)
- Ethereum, “The Merge”, <https://ethereum.org/en/upgrades/merge/> (Erişim:25.05.2022)
- Ethereum, “Transactions”, <https://ethereum.org/en/developers/docs/transactions/> (Erişim:26.05.2022)
- Etherscan, “Ethereum Daily Transactions Chart”, <https://etherscan.io/chart/tx> (Erişim:24.05.2022)
- Etherscan, <https://etherscan.io/tx/0x5c504ed432cb51138bcf09aa5e8a410dd4a1e204ef84bfe d1be16dfba1b22060> (Erişim: 26.05.2022)
- European Central Bank (ECB), Electronic Money, https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html (Erişim: 30.04.2022)
- European Central Bank (ECB), Virtual Currency Schemes – a further analysis, 2015. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> (Erişim: 24.02.2022)
- European Central Bank (ECB), Virtual Currency Schemes, 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> (Erişim: 23.04.2022)
- European Commission, Proposal for a Regulation Of The European Parliament And Of The Council on information accompanying transfers of funds and certain crypto-

- assets (recast), 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:08cf467e-ead4-11eb-93a8-01aa75ed71a1.0001.02/DOC_1&format=PDF (Erişim:22.05.2022)
- European Council of Foreign Relations, Mapping Palestinian Politics, https://ecfr.eu/special/mapping_palestinian_politics/introduction_armed_groups/ (Erişim:23.05.2022);
- European Parliament, “Stablecoins”, 2021, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698803/EPRS_BRI\(2021\)698803_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698803/EPRS_BRI(2021)698803_EN.pdf) (Erişim: 28.05.2022)
- European Parliament, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, 2018. [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (Erişim:24.05.2022)
- Europol, Cryptocurrencies: Tracing The Evolution Of Criminal Finances, 2021/b. <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf> (Erişim: 23.05.2022)
- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, 2021/a, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf (Erişim: 28.05.2022)
- Fantom Foundation, “What is FTM?”, <https://fantom.foundation/ftm-token/> (Erişim:24.05.2022)
- FATF, FATF IX Special Recommendations, <https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf> (Erişim: 09.05.2022)
- FATF, FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, 2020. <https://www.fatf->

[gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf](https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf) (Erişim: 28.05.2022)

FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (Erişim: 09.05.2022)

FATF, The FATF Recommendations, 2022. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (Erişim: 28.05.2022)

Fay, C. R. “Newton and the Gold Standard.” *Cambridge Historical Journal*, 1935/5 (1), ss. 109-117. <http://www.jstor.org/stable/3020836> (Erişim: 16.04.2022)

Fayazmanesh, Sasan, Money and Exchange: Folktales and reality, Routledge, 2006. <https://library.oapen.org/bitstream/id/ba173030-dbe5-4ecd-a8b3-6ae249a39407/1005953.pdf> (Erişim: 13.04.2022)

Ferrari vd., “Central Bank Digital Currency In An Open Economy”, European Central Bank, 2020. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2488~fede33ca65.en.pdf> (Erişim: 28.04.2022)

FINRA, Cryptocurrencies, <https://www.finra.org/investors/learn-to-invest/types-investments/initial-coin-offerings-and-cryptocurrencies/cryptocurrencies#:~:text=A%20cryptocurrency%20is%20a%20digital,remain%20highly%20volatile%20and%20risky>. (Erişim: 22.5.2022)

Financial Action Task Force, FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, 2014. <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (Erişim:22.04.2022)

Finney, Hal (@halfin), “working”, Twitter <https://twitter.com/halfin/status/314825462?s=20&t=I4pcOgom7DXIIGWke5WL9A>

- Finney, Hal, Reusable Proofs of Work, 2004.
<http://web.archive.org/web/20071222072154/http://rpow.net/> (Son erişim: 07.04.2022)
- Fisch vd., “Physical Zero-Knowledge Proofs of Physical Properties”, 2014,
<https://www.iacr.org/archive/crypto2014/86160292/86160292.pdf> (Erişim: 07.07.2022)
- Fisch, Christian, “Initial coin offerings (ICOs) to finance new ventures”, *Journal of Business Venturing*, 2019/34 (1). <https://doi.org/10.1016/j.jbusvent.2018.09.007> (Erişim: 08.01.2020)
- Fisher, Irving, The Purchasing Power of Money, its Determination and Relation to Credit, Interest and Crises, 1922, Macmillan. <https://eet.pixel-online.org/files/etranslation/original/Fisher%20The%20Purchasing%20Power%20of%20Money.pdf> (Erişim:20.04.2022)
- Flandreau, Marc, The Glitter of Gold: France Bimetallism and the Emergence of the International Gold Standard 1848-1873, Oxford University Press, 2003.
<https://books.google.com.tr/books?id=Uw5REAAAQBAJ&pg=PA158&dq=chevalier+parachute+theory&hl=tr&sa=X&ved=2ahUKEwiMofzm3pr3AhUgRvEDHU7oB4sQ6AF6BAgKEAI#v=onepage&q=chevalier%20parachute%20theory&f=false> (Erişim: 17.04.2022)
- Friedman, Milton, “Bimetallism Revisited.” *The Journal of Economic Perspectives*, 1990/4 (4), ss. 85-104. <http://www.jstor.org/stable/1942723> (Erişim: 16.04.2022)
- Friedrich, Roland, Luethold, Arnold, “Entry-Points to Palestinian Security Sector Reform”, Geneva Centre For The Democratic Control Of Armed Forces (DCAF).
<https://www.dcaf.ch/sites/default/files/publications/documents/Entry-Points%28EN%29.pdf> (Erişim:23.05.2022)
- Geva, Benjamin. "From Commodity to Currency in Ancient History--On Commerce, Tyranny, and the Modern Law of Money." *Osgoode Hall Law Journal*, 1987/25, ss. 115-158.
<https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1847&context=ohlj> (Erişim: 15.04.2022)

- Giffen, Robert. "The Gresham Law." *The Economic Journal*, 1891/1 (2), ss. 304-306.
<https://doi.org/10.2307/2956251> (Eriřim: 16.04.2022)
- Github, "ethereum/EIPs", <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md> (Eriřim:25.05.2022)
- Gkritsi, Eliza, "BSV Suffers 51% Attack: Report", Coindesk, 04.08.2021,
<https://www.coindesk.com/markets/2021/08/04/bsv-suffers-51-attack-report/>
(Eriřim: 20.05.2022)
- Goldberg, Dror, "Famous Myths of 'Fiat Money.'", *Journal of Money, Credit and Banking*, 2005/37 (5), ss. 957-967. <http://www.jstor.org/stable/3839155> (Eriřim: 20.04.2022)
- Gordon, Joy, "Smart Sanctions Revisited", *Ethics & International Affairs*, 2011/25 (3).
<https://doi.org/10.1017/S0892679411000323> (Eriřim: 06.07.2022)
- GOV.UK, Proscribed Terrorist Groups Or Organisations, 26.12.2021,
<https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2/proscribed-terrorist-groups-or-organisations-accessible-version>
(Eriřim:23.05.2022)
- Gödekli, Mehmet, "Terörizmin Finansmanı Suçu", (yüksek lisans tezi), Atatürk Üniversitesi, Kamu Hukuku Anabilim Dalı, Erzurum, 2013.
- Graeber, David, *Debt: The First 5000 Years*, Melville House, 2011.
https://warwick.ac.uk/fac/arts/english/currentstudents/undergraduate/modules/fullist/special/statesofdamage/syllabus201516/graeber-debt_the_first_5000_years.pdf (Eriřim: 11.04.2022)
- Graeber, David, *Towards an Anthropological Theory of Value*, Palgrave, 2001.
https://monoskop.org/images/3/36/Graeber_David_Toward_an_Anthropological_Theory_of_Value.pdf (Eriřim: 12.04.2022)
- Greenberg, Andy, "Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius", *Forbes*, 25.03.2014.
<https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos->

neighbor-the-bitcoin-ghostwriter-who-wasnt/?sh=5e228ca94a37 (Erişim: 26.05.2022)

Grincalaitis, Merunas, “Your Final Guide About Creating Simple and Advanced ICO Smart Contracts”, Medium, 12.08.2018. <https://medium.com/ethereum-developers/your-final-guide-about-creating-simple-and-advanced-ico-smart-contracts-50a7d363417b> (Erişim: 02.06.2022)

Güven, Vedat, Şahinöz, Erkin, BLOKZİNCİR – KRİPTO PARALAR – BITCOIN, Satoshi Dünyayı Değiştiriyor, (2. Baskı), Kronik Kitap, İstanbul 2018.

H.R. 7231 - Electronic Currency And Secure Hardware (ECASH) Act, 2022, <https://lynch.house.gov/cache/files/1/7/17e47e5a-2bff-42c1-b509-eb8a50931fa6/BDDFF183213326821B5C88B7F326EABB.ecashact-lynch.pdf> (Erişim: 30.04.2022)

Haber, Stuart, Stornetta, Scott, “How to Time-Stamp a Digital Document.”, In: Menezes, A.J., Vanstone, S.A. (eds) Advances in Cryptology-CRYPTO’ 90. CRYPTO 1990. Lecture Notes in Computer Science, vol 537. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-38424-3_32 (Son erişim: 02.04.2022)

Hafizoğulları, Zeki ve Özen, Muharrem, Türk Ceza Hukuku Genel Hükümler, (5. Baskı), US-A Yayıncılık, Ankara 2012.

Hafizoğulları Zeki ve Özen, Muharrem, Türk Ceza Hukuku Genel Hükümler, (13. Baskı), US-A Yayıncılık, Ankara 2021.

Hafizoğulları, Zeki, “Kusurluluğu Kaldıran Bir Neden Olarak Ceza Hukukunda İstenemezlik İlkesi (Nichtzumutbarkeit /L’inesigibilita)”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2008/57 (3), ss. 337-369. <https://dergipark.org.tr/tr/download/article-file/626960> (Erişim: 13.05.2022)

Hart, Keith, “Notes Towards An Anthropology Of Money”, *Kritikos*, 2005/2. https://intertheory.org/hart.htm?fbclid=IwAR30etRsErMO-39RaHQFkTC2msAwX5BJcE1WY8xCs5_sQJOtpAJf8k9wtNU (Erişim: 12.04.2022)

- Hayashi, Fumio, Matsui, Akihiko, “A Model of Fiat Money and Barter”, *Journal of Economic Theory*, 1996/68 (1), ss. 111-132.
<https://doi.org/10.1006/jeth.1996.0006> (Eriřim: 09.04.2022)
- Heinrich, Bernd, Ceza Hukuku Genel Kısım – 1, (ed. Yener Ünver), (çev. Hakan Hakeri vd.), (1. Baskı), Adalet Yayınevi, Ankara 2014.
- Hertig, Alyssa, “Bitcoin Coders Send International Lightning Payment Over Ham Radio”, CoinDesk, 05.03.2019.
<https://www.coindesk.com/markets/2019/03/04/bitcoin-coders-send-international-lightning-payment-over-ham-radio/#:~:text=In%20what%20appears%20to%20be,lightning%20payment%20over%20radio%20waves.&text=Alyssa%20Hertig-.In%20what%20appears%20to%20be%20a%20first%2Dof%2Dits%2D,lightning%20payment%20over%20radio%20waves> (Eriřim: 17.07.2022)
- House Homeland Security Committee, Examining The Domestic Terrorism Threat In The Wake Of The Attack On The U.S. Capitol, 2021,
<https://www.congress.gov/event/117th-congress/house-event/LC65965/text?q=%7B%22search%22%3A%22capitol+attack%22%7D&s=1&r=7> (Eriřim:24.05.2022)
- Howe, Jeff, “The Rise of Crowdsourcing”, WIRED, Haziran 2016.
<https://www.wired.com/2006/06/crowds/> (Eriřim: 07.12.2019)
- Hozumi, Fumio. “The Characteristics Of The History Of Chinese Money.” *Kyoto University Economic Review*, 1954/24 (2), ss. 18-38.
<http://www.jstor.org/stable/43217017> (Eriřim: 20.04.2022)
- Humphrey, Caroline, “Barter and Economic Disintegration”, *New Series*, 1985/20 (1), ss. 48-72.
<https://voidnetwork.gr/wp-content/uploads/2016/09/Barter-and-economic-disintegration-by-Caroline-Humphrey.pdf> (Eriřim: 11.04.2022)
- Icobench, “EOS”, <https://icobench.com/ico/eos> (Eriřim: 02.06.2022)
- Icobench, “IEO”, <https://icobench.com/ieo> (Eriřim: 02.06.2020)
- Icodrops, “Ethereum”, <https://icodrops.com/ethereum/> (Eriřim: 24.05.2022)

- Igwe, Isaac O.C., “History of the International Economy: The Bretton Woods System and its Impact on the Economic Development of Developing Countries”, *Athens Journal of Law*, 2018/4 (2), ss. 105-125. <https://www.athensjournals.gr/law/2018-4-2-1-Igwe.pdf> (Eriřim: 18.04.2022)
- IMF History Volume 3 (1945-1965). USA: International Monetary Fund, 1996. <https://doi.org/10.5089/9781451972511.071> (Eriřim: 18.04.2022)
- International Monetary Fund, Treatment of Crypto Assets in Macroeconomic Statistics, 2019, <https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf> (Eriřim:22.05.2022)
- Irigoin, Maria Alejandra. “Inconvertible Paper Money, Inflation and Economic Performance in Early Nineteenth Century Argentina.”, *Journal of Latin American Studies*, 2000/32 (2), ss. 333-359. <http://www.jstor.org/stable/158568> (Eriřim: 21.04.2022)
- Iwamoto, Takekazu. “The Keynes Plan for an International Clearing Union Reconsidered.”, *Kyoto University Economic Review*, 1995/65 (2), ss. 27-42. <http://www.jstor.org/stable/43217486> (Eriřim: 18.04.2022)
- İnanç Sönmez, Bade, “Blok zinciri tabanlı ilk seçim Sierra Leone’de gerekleřtirildi”, *Dünya Halleri*, 13.03.2018. <https://www.dunyahalleri.com/blok-zinciri-tabanli-ilk-secim-sierra-leonede-gerceklestirildi/> (Eriřim:21.05.2022)
- Jevons, William Stanley, A Serious Fall in the Value of Gold Ascertained: And Its Social Effects Set Forth, 1863. https://books.google.com.tr/books?id=4IcBAAAQAAJ&printsec=frontcover&dq=A+serious+fall+in+the+Value+of+Gold+ascertained,+and+its+social+effects+set&hl=tr&sa=X&redir_esc=y#v=onepage&q&f=false (Eriřim: 17.04.2022)
- Jevons, William, Money and the Mechanism of Exchange. New York: D. Appleton and Company, 1875. <https://oll.libertyfund.org/title/jevons-money-and-the-mechanism-of-exchange>
- Kara, Kübra, “Geliřtirdiđi uygulamayla noter iřlemlerini "sanal" ortama tařıdı”, *Anadolu Ajansı*, 10.05.2022. <https://www.haberler.com/guncel/gelistirdigi-uygulamayla-noter-islemlerini-sanal-14929714-haberi/> (Eriřim:21.05.2021)

- Katođlu, Tuđrul, “Ceza Hukukunda Suçun Mađduru Kavramının Sınırları”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2012/61 (2), ss. 657-693. <https://dergipark.org.tr/tr/download/article-file/624032> (Eriřim: 12.05.2022)
- Kereiakes vd., “Terra Money: Stability and Adoption”, 2019. https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf (Eriřim: 24.04.2022)
- Kiyotaki, Nobuhiro, Randall Wright. “On Money as a Medium of Exchange.” *Journal of Political Economy* 97, 1989/4, ss. 927-954. <http://www.jstor.org/stable/1832197> (Eriřim: 13.04.2022)
- Koç, Cořkun, “Suçun Konusunun Yokluđu Durumunda Teřebbüse Elveriřlilik Sorunu”, *TBB Dergisi*, 2020 (147), s. 54. <http://tbbdergisi.barobirlik.org.tr/m2020-147-1903> (Eriřim: 13.07.2022)
- Korkmaz Sürer, Mukaddes. "Uluslararası Para Hukuku", *Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni*, 2005/25, ss. 213-228. <https://dergipark.org.tr/tr/pub/iuhmhohb/issue/9365/117182> (Eriřim: 13.04.2022)
- Kraken, “What is Reddit MOON?”, <https://www.kraken.com/learn/what-is-reddit-moon> (Eriřim: 01.05.2022)
- Krzyzanowski, Paul, “Understanding Paxos”, 2019. <https://people.cs.rutgers.edu/~pxk/417/notes/paxos.html>
- Laidler, David, “Rules, Discretion and Financial Crises in Classical and Neoclassical Monetary Economics”, *Economic Issues*, 2002/7 (part 2), ss. 11-33. https://www.researchgate.net/publication/237137945_Rules_Discretion_and_Financial_Crises_in_Classical_and_Neoclassical_Monetary_Economics (Eriřim: 17.04.2022);
- Laidler, David, *The Golden Age of the Quantity Theory*, Princeton University Press, 1991. https://books.google.com.tr/books?id=tLgABAAAQBAJ&printsec=frontcover&dq=The+Golden+Age+of+the+Quantity+Theory&hl=tr&sa=X&redir_esc=y#v=onepage&q&f=false (Eriřim:17.04.2022)

- Laidler, David. "British Monetary Orthodoxy in the 1870." *Oxford Economic Papers*, 1988/40 (1). <http://www.jstor.org/stable/2663255> (Eriřim:17.04.2022)
- Lamport vd., "The Byzantine Generals Problem, *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, 1982/4 (3), ss. 382-401. <https://lamport.azurewebsites.net/pubs/byz.pdf> (Eriřim: 12.05.2022)
- Lamport, Leslie, "The Part-time Parliament.", *ACM Trans. Comput. Syst.*, 1998/16 (2), 133–169. <https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Part-Time-Parliament.pdf> (Son eriřim: 30.03.2022)
- Lamport, Leslie, Paxos Made Simple, 2001. <https://lamport.azurewebsites.net/pubs/paxos-simple.pdf>
- Lapavitsas, Costas. "Money and the Analysis of Capitalism: The Significance of Commodity Money." *Review of Radical Political Economics*, 2000/32 (4), ss. 631-656. [https://doi.org/10.1016/S0486-6134\(00\)90004-4](https://doi.org/10.1016/S0486-6134(00)90004-4) (Eriřim: 14.04.2022)
- Law vd., "How To Make A Mint: The Cryptography Of Anonymous Electronic Cash", National Security Agency Office of Information Security Research and Technology, 1996. <https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm> (Eriřim: 21.05.2022)
- Ljungberg, Jonas, Ögren, Anders, "Discipline or international balance: the choice of monetary systems in Europe", *The European Journal of the History of Economic Thought*, 2021, ss. 218-245. <https://doi.org/10.1080/09672567.2021.1946121> (Eriřim: 17.04.2022)
- Macleod, Henry Dunning, *The Elements of Political Economy*, 1858. https://books.google.com.tr/books?hl=tr&lr=&id=sA8ZAAAAYAAJ&oi=fnd&pg=PA1&dq=Henry+Dunning+Macleod&ots=THnYsyvQo8&sig=1s61jFp-K7wwgxbH1Z1fz9jJWq4&redir_esc=y#v=onepage&q=gresham&f=false (Eriřim: 16.04.2022)
- Männik, Erik, "Terrorism: Its Past, Present And Future Prospects", *KVÜÕA toimetised*, 12, 2009. <https://www.ksk.edu.ee/en/wp->

content/uploads/2011/03/KVUOA_Toimetised_12-Männik.pdf (Erişim: 06.05.2022)

MASAK, Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının Ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklerle İlişkin Temel Esaslar, 2021, <https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf> (Erişim: 29.05.2022)

May, Timothy C., 1988, The Crypto Anarchist Manifesto, 1988. <https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html> (Son erişim: 03.04.2022)

Melinek, Jacquelyn, “US Treasury Secretary Janet Yellen pushes for stablecoin regulation by end of year”, Techcrunch, 10.05.2022, <https://techcrunch.com/2022/05/10/us-treasury-secretary-janet-yellen-pushes-for-stablecoin-regulation-by-end-of-year/> (Erişim: 28.05.2022)

Merkle, Ralph C., “Secure Communications Over Insecure Channels”, *Communications of the ACM*, 1978/21 (4), ss. 294-299. <https://doi.org/10.1145/359460.359473> (Erişim: 03.05.2022)

Merkle, Ralph, Secrecy, Authentication, And Public Key Systems, Department Of Electrical Engineering Stanford University, 1979. <https://www.merkle.com/papers/Thesis1979.pdf> (Erişim: 04.05.2022)

MHA Cayman, Independent Accountant’s Report, 2022. https://assets.ctfassets.net/vyse88cgwfb/1np5dpcwuHrWJ4AgUgI3Vn/e0dac722de3cea07766e05c52773748b/Tether_Assurance_Consolidated_Reserves_Report_2022-03-31_3_.pdf (Erişim:28.05.2022)

Ministry of Foreign Affairs of Japan, Japan’s Foreign Policy in Major Diplomatic Fields. <https://www.mofa.go.jp/policy/other/bluebook/2005/ch3-a.pdf> (Erişim: 23.05.2022);

Monero, “How is Monero’s privacy different from other coins?”, <https://www.getmonero.org/get-started/faq/#anchor-different> (Erişim:25.05.2022)

- Monero, “Stealth Address”, <https://www.getmonero.org/resources/moneropedia/stealthaddress.html> (Erişim: 27.05.2022)
- Monero, “What is Monero (XMR)?”, <https://www.getmonero.org/get-started/what-is-monero/#:~:text=Monero%20transactions%20are%20confidential%20and%20untraceable.&text=Because%20every%20transaction%20is%20private,about%20blacklisted%20or%20tainted%20coins.> (Erişim: 21.05.2022)
- Nakamoto, Satoshi, “...I believe I've worked through all those little details over the last year and a half while coding it...”, Satoshi Nakamoto Institute, <https://satoshi.nakamotoinstitute.org/emails/cryptography/15/> (Erişim:26.05.2022)
- Nakamoto, Satoshi, “Bitcoin open source implementation of P2P currency”, P2P Foundation, 15.02.2009, <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493> (Erişim:17.05.2022)
- Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, <https://bitcoin.org/bitcoin.pdf> (Son erişim:08.04.2022)
- Nakamoto, Satoshi, “I've moved on to other things. It's in good hands with Gavin and everyone.”, 23.04.2011, <https://pastebin.com/syrmi3ET> (Erişim: 26.05.2022)
- Nakamoto, Satoshi, Bitcoin P2P e-cash paper, Cryptography Mailing List, 13-11-2008, <https://satoshi.nakamotoinstitute.org/emails/cryptography/11/#selection-15.0-15.10> (Erişim: 19.05.2022)
- Narayanan, Arvind, Clark, Jeremy, “Bitcoin's Academic Pedigree: The Concept Of Cryptocurrencies Is Built From Forgotten Ideas In Research Literature”, *Communications of the ACM*, 2017/60 (12), ss. 20-49. <https://doi.org/10.1145/3134434.3136559> (Erişim:16.05.2022)
- National Security Council, National Strategy For Countering Domestic Terrorism, 2021. <https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf> (Erişim: 30.05.2022)

- New Zealand Police, Lists associated with Resolution 1373, <https://www.police.govt.nz/advice/personal-community/counterterrorism/designated-entities/lists-associated-with-resolution-1373> (Eriřim:23.05.2022)
- Newcomb, Simon. "The Standard of Value." *The North American Review*, 1879/129, ss. 223-237. (274). <http://www.jstor.org/stable/25100790> (Eriřim: 14.04.2022)
- Niantic, <https://niantic.helpshift.com/hc/en/6-pokemon-go/faq/94-using-pokecoins-to-make-purchases-in-the-shop-1582065532/>, (Eriřim: 01.05.2022)
- Office of Financial Sanctions Implementation HM Treasury, Consolidated List Of Financial Sanctions
- Officer, Lawrence H., "Silver Standard", In: Durlauf, S.N., Blume, L.E. (eds) *Monetary Economics. The New Palgrave Economics Collection*. Palgrave Macmillan, London. https://doi.org/10.1057/9780230280854_38 (Eriřim: 15.04.2022);
- Okan, Oya, *Kurumlar Sosyolojisi Ders Notları*, İstanbul, 2021.
- Orville R. Keister, "Commercial Record-Keeping in Ancient Mesopotamia", *The Accounting Review* 1963/38 (2), ss. 371-376. <https://www.jstor.org/stable/242928> (Eriřim:02.05.2022)
- Özdemir, Gençer, "Kripto Paraların Eřya Nitelięi", *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 2021/1 (1).
- Özgenç, İzzet ve Üzülmöz, İlhan, *Ceza Genel Hukuku*, (4. Baskı), Seçkin Yayıncılık, Ankara 2021.
- Özgenç, İzzet, *Suç Örgütleri*, (14. Baskı), Seçkin, Ankara, 2022.
- Özlük, Betül, "Mülkiyet ve Zilyetlik Üzerine Düşünceler", *Selçuk Üniversitesi Hukuk Fakültesi*, 2019/27 (1).
- Öztürk, Nazım, "İMF'nin Deęişen Rolü ve Geliřmekte Olan Ülke Ekonomilerine Etkiler", *Ankara Üniversitesi SBF Dergisi*, 2002/57. <https://dergipark.org.tr/tr/pub/ausbf/issue/3098/42876> (Eriřim: 19.04.2022)
- Paribu, "Merkle Tree", 2021, <https://www.paribu.com/blog/sozluk/merkle-tree-nedir/> (Eriřim: 04.05.2022)

- Parliament of Australia, Chapter 3 The Listings, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Former_Committees/pjcaad/terrorist_listingsc/chapter3#ham (Erişim: 23.05.2022);
- Partz, Helen, “FATF’s Regulations to Push Criminals to Privacy Coins: CipherTrace CEO”, 22.10.2019, Cointelegraph, <https://cointelegraph.com/news/fatfs-regulations-to-push-criminals-to-privacy-coins-ciphertrace-ceo> (Erişim: 28.05.2022)
- Peirce, Michael, O'Mahony, Donal, “Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set”, WWW4, 1995, <https://www.w3.org/Conferences/WWW4/Papers/228/> (Erişim:14.05.2022)
- Peneder, Michael, Andreas Resch, Schumpeter's Venture Money, Oxford University Press, 2021. https://books.google.com.tr/books?id=qrwcEAAAQBAJ&pg=PA76&dq=michel+chevalier+parachute+effect&hl=tr&sa=X&ved=2ahUKEwi02cXM9Jr3AhWER_EDHTEuBi8Q6AF6BAgHEAI#v=onepage&q=michel%20chevalier%20parachute%20effect&f=false (Erişim: 17.04.2022)
- People’s Bank of China, Working Group on E-CNY Research and Development of the People’s Bank of China, Progress of Research & Development of E-CNY in China, People’s Bank of China, 2021. <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf> (Erişim: 29.04.2022)
- Perçin, Önder vd., Sorularla Fintek: Elektronik Para Kuruluşları Ve Ödeme Kuruluşları - Açık Bankacılık - Kriptopara Ve Kriptopara Alım Satım Platformları, On İki Levha Yayıncılık, 2021.
- Polkadot, “Parachains”, <https://wiki.polkadot.network/docs/learn-parachains#what-is-parachain-consensus> (Erişim:26.05.2022)
- Polkadot, “Smart Contracts”, <https://wiki.polkadot.network/docs/build-smart-contracts> (Erişim:25.05.2022)

- Popper, Nathaniel, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, HarperCollins, 2015.
- Preneel, Bart, *The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition*, Katholieke Universiteit Leuven, 2010. <https://www.esat.kuleuven.be/cosic/publications/article-1532.pdf> (Eriřim: 03.05.2022)
- Reddit, “reddit coins”, <https://www.reddit.com/coins> (Eriřim: 01.05.2022)
- Reddit, “vault”, <https://www.reddit.com/vault/> (Eriřim: 01.05.2022)
- Redish, Angela. “The Evolution of the Gold Standard in England.”, *The Journal of Economic History*, 1990/50 (4), ss. 789-805. <http://www.jstor.org/stable/2122455> (Eriřim: 17.04.2022)
- Rivest, Ronald L. vd., “How to Leak a Secret”, *Advances in Cryptology — ASIACRYPT 2001*, 2001. <https://people.csail.mit.edu/rivest/pubs/RST01.pdf> (Eriřim: 27.05.2022)
- Ross, Edward Alsworth. “The Standard of Deferred Payments.”, *The Annals of the American Academy of Political and Social Science*, 1892/3, ss. 37-49. <http://www.jstor.org/stable/1008596> (Eriřim: 14.04.2022)
- Rothnie vd., “Introduction to a System for Distributed Databases (SDD-1)”, *ACM Transactions on Database Systems*, 1980/5 (1), ss. 1-17. <https://dl.acm.org/doi/pdf/10.1145/320128.320129> (Eriřim: 02.05.2022)
- Royal Mint, What was the Gold Standard?, <https://www.royalmint.com/invest/discover/gold-news/what-was-the-gold-standard/> (Eriřim: 17.04.2022)
- RSM, Bağımsız Denetçi Raporu, 15.04.2022, https://uploads-ssl.webflow.com/5fb683a258cbdf70262c0b77/6261446ff9e7a60b887c67dc_BiLira%20Rapor%2015042022%20TR%20RSM%20İmzalı.pdf (Eriřim: 29.05.2022)
- Schwartz, Andrew A., “The Gatekeepers of Crowdfunding”, *Washington and Lee Law Review*, 2018/75 (2).

<https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2297&context=articles> (Eriřim: 23.11.2019)

Second Life, “Buying & Selling Linden Dollars”, <https://lindenlab.freshdesk.com/support/solutions/articles/31000138105-buying-selling-linden-dollars> (Eriřim: 01.05.2022)

Sekniqi vd., “Avalanche Platform”, 2020. https://assets.website-files.com/5d80307810123f5ffbb34d6e/6008d7bbf8b10d1eb01e7e16_Avalanche%20Platform%20Whitepaper.pdf (Eriřim: 24.04.2022)

Selgin, George. "Synthetic commodity money." *Journal of Financial Stability*, 2005/17, ss. 92-99. <https://doi.org/10.1016/j.jfs.2014.07.002> (Eriřim: 14.04.2022)

Sengupta, Rajdeep, Aubuchon, Craig P., “The Microfinance Revolution: An Overview”, Federal Reserve Bank of St. Louis Review, January/February 2008, 90(1). https://www.researchgate.net/profile/Craig-Aubuchon/publication/5047480_The_Microfinance_Revolution_An_Overview/inks/55195faf0cf273292e716113/The-Microfinance-Revolution-An-Overview.pdf (Eriřim: 02.06.2022)

Sermaye Piyasası Kurulu, Sermaye Piyasası Kurulu Bülteni, 2018/42. <https://www.spk.gov.tr/Bulten/Goster?year=2018&no=42> (Eriřim: 29.05.2022)

Sherman vd., “On the Origins and Variations of Blockchain Technologies”, University of Maryland, 2018. <https://arxiv.org/ftp/arxiv/papers/1810/1810.06130.pdf> (Eriřim: 30.04.2022)

Sirer, Emin Gün (@el33th4xor), “Ok, there is a terribly wrong framework emerging around consensus protocols. People think that PoW and PoS are consensus protocols, and that they are the only two consensus protocols out there. This is false. Let me explain...”, Twitter, 13.06.2018, <https://twitter.com/el33th4xor/status/1006931729679044608> (Eriřim:26.05.2022)

- Sluka vd., “What Anthropologists Should Know about the Concept of Terrorism’: A Response to David Price, A.T. 18(1).”, *Anthropology Today*, 2002/18 (2), ss. 22-23. <http://www.jstor.org/stable/3694961> (Eriřim: 06.05.2022)
- Soderberg, Gabriel, “Behind the Scenes of Central Bank Digital Currency”, *International Money Fund*, 2022. <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174> (Eriřim: 28.04.2022)
- Solomon, Ariel Ben, “Gaza-based pro-ISIS group urges Muslims on social media to donate for weapons”, *The Jerusalem Post*, 25.06.2016, <https://www.jpost.com/Middle-East/ISIS-Threat/Gaza-based-pro-ISIS-group-urges-Muslims-on-social-media-to-donate-for-weapons-457680> (Eriřim: 23.05.2022)
- Sözüer, Adem, “Ceza Hukuku Uygulama Rehberine Giriř ve Pratik Çalışma Notu”, *İstanbul Üniversitesi Hukuk Fakültesi Ceza Hukuku ve Kriminoloji Arařtırma ve Uygulama Merkezi*, 2015.
- Spencer, Adam Hal, Lecture 6: Cash in Advance, lecture notes, *Advanced Monetary Economics 2020*, The University of Nottingham, 2020. https://static1.squarespace.com/static/6109a70ff6be433c1a1339fe/t/6112c69da1c3e55c3df1b735/1628620447733/L6_CIA_2020_Mar16.pdf (Eriřim: 09.04.2022)
- Szabo, Nick, “Bit Gold”, 2005, <http://unenumerated.blogspot.com/2005/12/bit-gold.html> (Son Eriřim: 07.04.2022)
- Szabo, Nick, “Secure Property Titles with Owner Authority”, 1998. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/securetitle.html> (Son eriřim: 06.04.2022)
- Tarakçıođlu, Zeynep Esra, “Kripto Varlıklar Ve Ceza Hukuku Sorumluluđu”, *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, 2021/11(2). <https://doi.org/10.54704/akdhfd.1024708> (Eriřim: 08.07.2022)

Taras, Payment No. 1: A Closer Look at the Very First Bitcoin Transfer, Bitcointalk, 02.11.2017, <https://bitcointalk.org/index.php?topic=2346992.0> (Erişim: 26.05.2022)

Targets In The Uk, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060765/Counter-Terrorism_International .pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060765/Counter-Terrorism_International.pdf) (Erişim:23.05.2022)

Taskinsoy, John, “From Primitive Barter to Inflationary Dollar: A Warless Economic Weapon of Mass Destruction”, 2020. <http://dx.doi.org/10.2139/ssrn.3542145> (Erişim: 11.04.2022)

Tekben, Tuğçe, “Noterin Hukuki Statüsü Ve Noterlik Kanunu’nun 162. Maddesi Uyarınca Sorumluluğu Üzerine Bir İnceleme”, *İzmir Barosu Dergisi*, Eylül 2021, ss. 69-150. <https://www.izmirbarosu.org.tr/pdfdosya/noterin-hukuki202214145432429.pdf> (Erişim:21.05.2021)

Terra, “The Terra blockchain was officially halted at a block height of 7603700. <https://lcd.terra.dev/blocks/latest> Terra validators have decided to halt the Terra chain to prevent governance attacks following severe \$LUNA inflation and a significantly reduced cost of attack.”, 12.05.2022 https://twitter.com/terra_money/status/1524785058296778752?s=20&t=MU8IOWUUnw4ZrS4nxxCtYFA (Erişim: 20.05.2022)

The Council Of The European Union, 2002/475/JHA, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN> (Erişim: 09.05.2022)

The European Parliament And The Council Of The European Union, Directive 2005/60/Ec Of The European Parliament And Of The Council, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN> (Erişim: 07.05.2022)

Tilly, Charles. “Terror, Terrorism, Terrorists.” *Sociological Theory*, 2004/22 (1), ss. 5-13. <http://www.jstor.org/stable/3648955> (Erişim: 06.05.2022)

- Tobin, James. "A Case for Preserving Regulatory Distinctions.", *Challenge*, vol. 30, no. 5, 1987/30 (5). <http://www.jstor.org/stable/40720529> (Eriřim: 27.04.2022)
- Tokgöz, Havva Begüm, Uluslararası Hukuk Baęlamında Terörizmin Finansmanının Önlenmesi, (1. Baskı), On İki Levha Yayıncılık, İstanbul 2022.
- Toroslu, Haluk, Ceza Hukukunda İsnat Yeteneęi, (Doktora Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Ankara, 2013.
- Toroslu, Nevzat ve Toroslu, Haluk, Ceza Hukuku Genel Kısım, (26. Baskı), Savaş Yayınevi, Ankara 2021.
- Toroslu, Nevzat, Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Savaş Yayınevi, Ankara 2019.
- Townsend, Robert M. "Models of money with spatially separated agents." *Models of monetary economies*, 1980, ss. 265-303. <http://m.robertmtownsend.net/sites/default/files/files/papers/published/ModelsofMoney1980.pdf> (Eriřim: 09.04.2022)
- Turan, Deniz, Demircan, Can, Kripto Paralar İle Terör Ve Dięer İlegal Aktivitelerin Finansmanı, *Anadolu Akademi Sosyal Bilimler Dergisi*, 2021/3 (1). <https://dergipark.org.tr/en/download/article-file/1543533> (Eriřim: 29.05.2022)
- Turk, Austin T. "Social Dynamics of Terrorism." *The Annals of the American Academy of Political and Social Science*, 1982/463, ss. 119-128. <http://www.jstor.org/stable/1043616> (Eriřim: 07.05.2022)
- Türk Dil Kurumu, "finansman", <https://sozluk.gov.tr> (Eriřim: 07.05.2022)
- Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji Ve Bütçe Başkanlığı, On Birinci Kalkınma Planı (2019-2023), Temmuz 2019, <https://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf> (Eriřim: 22.05.2022)
- Türkiye Cumhuriyeti İçişleri Bakanlığı, Türkiye'nin DEAŞ İle Mücadelesi, 2017. https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/strateji/deneme/YAYI_NLAR/İÇERİK/deas%20en.pdf (Eriřim: 23.05.2022)
- Türkiye Cumhuriyeti Merkez Bankası (TCMB), Merkez Bankası Dijital Türk Lirası Ar-Ge Projesi Hakkında Basın Duyurusu, 2021,

<https://www.tcmb.gov.tr/wps/wcm/connect/TR/TCMB+TR/Main+Menu/Duyurular/Basin/2021/DUY2021-40> (Erişim: 28.04.2022)

U.S. Securities And Exchange Commission, President’s Working Group Report on Stablecoins, 2021, <https://www.sec.gov/news/statement/gensler-statement-presidents-working-group-report-stablecoins-110121#:~:text=Stablecoins%20are%20crypto%20tokens%20pegged,in%20the%20last%2020%20months.&text=As%20the%20report%20notes%2C%20“stablecoins,commodities%20and%20For%20derivatives>. (Erişim: 28.05.2022)

United Nations Security Council, S/RES/1267 (1999), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/300/44/PDF/N9930044.pdf?OpenElement> (Erişim: 07.05.2022)

United Nations Security Council, S/RES/1333 (2000), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/806/62/PDF/N0080662.pdf?OpenElement> (Erişim: 07.05.2022)

United Nations Security Council, S/RES/1373 (2001), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement> (Erişim: 07.05.2022)

United Nations Security Council, S/RES/1617 (2005), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/446/60/PDF/N0544660.pdf?OpenElement> (Erişim: 07.05.2022)

United Nations Security Council, S/RES/2170 (2014), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/508/49/PDF/N1450849.pdf?OpenElement> (Son Erişim: 07.05.2022)

United States District Court For The District Of Columbia, United States Of America, v. Fifty-Three Virtual Currency Accounts, One Hundred Twenty-Seven Virtual Currency Properties, Five Accounts Held At Financial Institution 1, The Alqassam.Net Domain, The Alqassam.Ps Domain and the Qassam.Ps Domain, Civil Action No. 20-cv-2227, 2020/a. <https://www.justice.gov/opa/press-release/file/1304296/download> (Erişim:23.05.2022)

- United States District Court For The District Of Columbia, United States Of America V. Mehmet Akti & Hüsametdin Karataş, Case: 1:20-mj-00157, 08/12/2020. <https://www.justice.gov/opa/press-release/file/1304276/download> (Erişim:23.05.2020)
- United States District Court For The District Of Columbia, United States Of America v. 155 Virtual Currency Assets, Civil Action No. 20-cv-2228, 2020/b. <https://www.justice.gov/opa/press-release/file/1304296/download> (Erişim:24.05.2022)
- Ünver, Yener ve Kerem Öz (Eds.), Kripto Para ve Ceza Hukuku, Seçkin Yayıncılık, Ankara 2022.
- van Saberhagen, Nicolas, “CryptoNote v 2.0”, 2013. <https://bytecoin.org/old/whitepaper.pdf> (Erişim:25.05.2022)
- Voell, Zack, “Ethereum Classic Hit by Third 51% Attack in a Month”, Coindesk, 30.08.2020, <https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/> (Erişim: 20.05.2022)
- Wallace, Neil, “The Overlapping Generations Model of Fiat Money”, Models of Monetary Economies, Federal Reserve Bank of Minneapolis, <https://www.minneapolisfed.org/~media/files/pubs/books/models/cp49.pdf?la=en> (Erişim: 09.04.2022)
- Wandschneider, Kirsten. “The Stability of the Interwar Gold Exchange Standard: Did Politics Matter?”, *The Journal of Economic History*, 2008/68 (1), ss. 151-181. <http://www.jstor.org/stable/40056779> (Erişim: 17.04.2022);
- Watch the Burn, <https://watchtheburn.com> (Erişim:25.05.2022)
- Watcher News, “Ethereum Cofounder Vitalik Buterin Confirms That The Merge is Happening Soon, Plus Other Developments”, 21.05.2022, <https://watcher.guru/news/ethereum-cofounder-vitalik-buterin-confirms-that-the-merge-is-happening-soon-plus-other-developments> (Erişim:25.05.2022)
- Waves.Exchange (@Waves_Exchange), “Delisting XMR, Dash and ZEC These tokens will soon be delisted from <http://Waves.Exchange>. Their depositing will be terminated on March 9, 2022. If you have any XMR, Dash or ZEC, we recommend

- withdrawing them no later than May 8, 11am UTC otherwise you will lose your coins.”, 03.03.2022,
https://twitter.com/waves_exchange/status/1499429481970389002 (Erişim: 28.05.2022)
- Weatherford, Jack, *The History of Money*, 2009,
https://books.google.com.tr/books?hl=tr&lr=&id=v8oxCs1eWgsC&oi=fnd&pg=PR11&dq=history+of+money&ots=sHobjRSPX0&sig=bB55zxJSKg3BCLArhGus9gCVH_A&redir_esc=y#v=onepage&q=history%20of%20money&f=false
2009, s. 20. (Erişim: 08.04.2022)
- Wikipedia, "Initial Coin Offering", https://en.wikipedia.org/wiki/Initial_coin_offering.
(Erişim: 08.01.2020)
- Wikipedia, "Reign of Terror", https://en.wikipedia.org/wiki/Reign_of_Terror (Erişim: 06.05.2022)
- Wikipedia, "Temple of Juno Moneta",
https://en.wikipedia.org/wiki/Temple_of_Juno_Moneta (Son erişim: 12.04.2022)
- Wikipedia, Merkle's Puzzles, https://en.wikipedia.org/wiki/Merkle%27s_Puzzles
(Erişim: 03.05.2022)
- Wiktionary, "financement", <https://en.wiktionary.org/wiki/financement> (Erişim: 07.05.2022)
- Wilder, Heidi, "An Overview Of The Use Of Cryptocurrencies In Terrorist Financing",
Coinbase, 22.09.2021, <https://blog.coinbase.com/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing-235df6049bc7> (Erişim:23.05.2022)
- Williams, John H., "Currency Stabilization: The Keynes and White Plans.", *Foreign Affairs*, 1943/21 (4), ss. 645-658. <https://doi.org/10.2307/20029784> (Erişim: 18.04.2022)
- Wong, Eugene, "Retrieving dispersed data from SDD-1: A system for distributed databases," 1977 Berkeley Workshop on Distributed Data Management and Computer Networks, University of California, Berkeley, CA.
- Wood, Gavin, "Ethereum: A Secure Decentralised Generalised Transaction Ledger Eip-150 Revision", 2015, <http://gavwood.com/Paper.pdf> (Erişim: 24.05.2022)

- Wood, Gavin, “Polkadot: Vision For A Heterogeneous Multi-Chain Framework”, 2016.
<https://polkadot.network/PolkaDotPaper.pdf> (Erişim:25.05.2022)
- World Gold Council, Key documents in the history of gold, s. 130
<https://www.gold.org/sites/default/files/documents/1819may21.pdf> (Erişim: 17.04.2022)
- Yaga vd., “Blockchain Technology Overview”, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg.
<https://doi.org/10.6028/NIST.IR.8202> (Erişim: 30.03.2022)
- Yalçınsoy, Hakan, “Paxos Konsensüs Protokolü”, <https://hknycnsy.medium.com/paxos-konsensüs-protokolü-f7787e57df3c>
- Yalta, A. Yasemin, Para Teorisi ve Politikası Ders Notları.
https://acikders.tuba.gov.tr/pluginfile.php/4391/mod_resource/content/3/ders-notları-kitap-%28s1%2C1%29.pdf (Son erişim: 12.04.2022)
- Yargıtay Ceza Genel Kurulu, 12.3.2019 T., 2017/16-691 E., 2019/202 K.
<https://rayp.adalet.gov.tr/resimler/552/dosya/2019-ycgk-finansman06-01-202115-39.doc> (Erişim: 11.05.2022)
- Yargıtay Ceza Genel Kurulu, 13.2.2018 T., 2017/16-692 E., 2018/41 K.
<https://rayp.adalet.gov.tr/resimler/552/dosya/ycgk-terorizmin-finansmani-2018-06-01-202115-41.doc> (Erişim: 15.05.2022)
- Yargıtay Ceza Genel Kurulu, 13.2.2018 T., 2017/9-692 E., 2018/41 K.
- Yayla, Atilla, “Terörizm: Kavramsal Bir Çerçeve”, *Ankara Üniversitesi SBF Dergisi*, 1990/45 (1). <https://dergipark.org.tr/tr/download/article-file/38276> (Erişim: 06.05.2022)
- Yıldırım, Zeki, “Türk Hukukunda Terörizmin Finansmanının Önlenmesi Amacıyla Malvarlığını Dondurma Tedbiri”, *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 2013/3 (1). <https://dergipark.org.tr/tr/download/article-file/213566> (Erişim: 07.07.2022)
- Yılmaz, Yeşim, Terörizmin Finansmanı Suçu, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 2020/17. <https://dergipark.org.tr/en/download/article-file/1249893> (Erişim: 10.05.2022);

Yin vd., “Scalable and Probabilistic Leaderless BFT Consensus through Metastability”, Cornell University, 2020. https://assets.website-files.com/5d80307810123f5ffbb34d6e/6009805681b416f34dcae012_Avalanche%20Consensus%20Whitepaper.pdf (Erişim: 19.05.2022)

Zhou vd., “The Semi-join Query Optimization in Distributed Database System”, National Conference on Information Technology and Computer Science (CITCS 2012), 2012. <https://doi.org/10.2991/citcs.2012.232> (Erişim: 03.05.2022)

Zindros, Dionysis, Lecture 10: Accounts Model and Merkle Trees, EE 374: Blockchain Foundations, Stanford University, Spring 2022. https://web.stanford.edu/class/ee374/lec_notes/lec10.pdf (Erişim:26.05.2022)

