

**T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI**

**KRİPTO PARA, TERÖRÜN FİNANSMANI VE MİLLİ
GÜVENLİK İLİŞKİSİ**

**YÜKSEK LİSANS TEZİ
Zeynep ORUK**

**Danışman
Prof. Dr. Şafak Ertan ÇOMAKLI**

Ankara – 2021

T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI

KRİPTO PARA, TERÖRÜN FİNANSMANI VE MİLLİ
GÜVENLİK İLİŞKİSİ

YÜKSEK LİSANS TEZİ
Zeynep ORUK

Danışman
Prof. Dr. Şafak Ertan ÇOMAKLI

Ankara – 2021



ÖNSÖZ

Bu tez çalışması süresince engin bilgi birikimi, yol göstericiliği ve tecrübesiyle yardımlarını hiçbir zaman esirgemeyen değerli tez danışmanım Prof. Dr. Şafak Ertan ÇOMAKLI'ya ve çalışmalarımın her aşamasında bana destek olan aileme gösterdikleri anlayış ve sabırdan dolayı teşekkürlerimi sunarım.



ÖZET
T.C.
Polis Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Stratejileri ve Yönetimi Anabilim Dalı
Kripto Para, Terörün Finansmanı ve Milli Güvenlik İlişkisi
Hazırlayan: Zeynep ORUK
Yüksek Lisans
Tez Danışmanı: Prof. Dr. Şafak Ertan ÇOMAKLI
2021 – 193 Sayfa (Ekler hariç)

Son yıllarda finansal teknolojilerde meydana gelen hızlı gelişmeler, blok zincir teknolojisi ile bir dönüm noktası oluşturmuş ve kripto para kavramının ortaya çıkmasına neden olmuştur. Birçok teknolojik yenilik gibi kripto para teknolojilerinin de karanlık tarafları bulunmaktadır. Kripto-anarşist felsefeye dayanan ve merkez bankaları ile hükümetlerden bağımsızlık sergileyerek ortaya çıkan kripto paralar, kara para aklama ve terörün finansmanı gibi yasa dışı faaliyetlerde kullanılma durumları açısından son yıllarda dünya üzerindeki hemen hemen tüm ülkelerin güvenlik konularında baş etmesi gereken birtakım zorlukları da beraberinde getirmiştir. Kripto paraların sağladığı teknolojik avantajların terör örgütleri tarafından kullanılıp kullanılmadığı ve bu durumun milli güvenlik açısından risk taşıyıp taşımadığı irdelenmeye çalışılmıştır. Bu çalışma kripto paralara yönelik uluslararası ortak düzenleme yapılması konusunda gerek politika yapıcıların gerekse de kripto para ile çalışan ve yatırım yapan kurum, kuruluş ve paydaşların dikkatini çekmelidir.

Anahtar Kelimeler: Milli Güvenlik, Kara Para Aklama, Kripto Para, Blok Zincir, Terörün Finansmanı, Kripto-Anarşist

ABSTRACT
The Republic of Turkey
Police Academy
Institute of Security Sciences
Department of Strategies and Administration of Security
Cryptocurrency Relationship with Terror Financing and National Security
Zeynep ORUK
Master's Thesis
Supervisor: Prof. Dr. Şafak Ertan ÇOMAKLI
2021 – 193 Pages (Excluding appendices)

In recent years, the rapid developments in financial technologies have created a milestone with the blockchain technology and caused the emergence of the term of cryptocurrency. Like many technological innovations, cryptocurrency technologies have also dark sides inside. Cryptocurrencies based on the crypto-anarchist philosophy emerging by showing independence from central banks and governments bring along some challenges almost all countries around the world have to deal with in security issues in that using in illicit activities such as money laundering and terrorist financing recently. It has been tried to studied whether the technological advantages which is provided by the cryptocurrencies are exploited by terrorist organizations and whether this situation have a risk with regard to national security. This study should take attention both policy makers and institutions, organization and stakeholders who deal with cryptocurrencies in their business or investment regarding international joint action regulation of cryptocurrencies.

Key Words: National Security, Money Laundering, Cryptocurrency, Blockchain, Financing Terrorism, Crypto-Anarchist

KRİPTO PARA, TERÖRÜN FİNANSMANI VE MİLLİ GÜVENLİK İLİŞKİSİ

İÇİNDEKİLER

	Sayfa
TEZ ONAY SAYFASI	II
TELİF HAKLARI BEYANNAMESİ	III
ÖNSÖZ	IV
ÖZET.....	V
ABSTRACT.....	VI
İÇİNDEKİLER	VII
KISALTMALAR LİSTESİ.....	XI
ŞEKİLLER LİSTESİ	XIII
GİRİŞ	1

BİRİNCİ BÖLÜM

KAVRAMSAL VE KURAMSAL ÇERÇEVE

1.1.	GELENEKSEL PARA KAVRAMI.....	5
1.2.	PARANIN TARİHÇESİ	6
1.3.	ELEKTRONİK PARA KAVRAMI.....	9
1.4.	SANAL PARA KAVRAMI	12
1.5.	DİJİTAL PARA.....	15
1.6.	KRİPTO PARA KAVRAMI	16
1.7.	KRİPTO PARA ÇEŞİTLERİ	23
1.7.1.	Bitcoin	23
1.7.1.1.	<i>Bitcoin'in İşlemlerde Anonim Olmasının Bazı Yöntemleri.</i>	32
1.7.1.1.1.	Bitcoin Karıştırıcı	32
1.7.1.1.2.	ToR Kullanmak	33
1.7.1.1.3.	VPN Kullanarak.....	34
1.7.1.1.4.	İşlemler İçin Yeni Adresler Oluşturmak.....	35

1.7.1.1.5.	Bitcoin Nakit Yoluyla Alım Satımını Gerçekleştirme ..	35
1.7.1.1.6.	Joinmarket.....	35
1.7.2.	Ethereum (ETH)	36
1.7.3.	Ripple, XRP (XRP)	39
1.7.4.	Monero (XMR).....	41
1.7.5.	Dash (DASH)	43
1.7.6.	Verge (XVG).....	43
1.7.7.	ZCash (ZEC)	45
1.7.8.	Tether (USDT).....	45
1.7.9.	Binance USD (BUSD).....	48
1.7.10.	USD Coin (USDC).....	48
1.7.11.	İlk Kripto Para Arzı; ICO (Initial Coin Offerings)	49
1.8.	BLOK ZİNCİR TEKNOLOJİSİ	50
1.9.	DÜNYA ÜLKELERİNİN KRİPTO PARALARA YAKLAŞIMI	52
1.9.1.	Amerika Kıtası	56
1.9.1.1.	Bolivya.....	56
1.9.1.2.	Ekvador	56
1.9.1.3.	Amerika Birleşik Devletleri	57
1.9.1.4.	Kanada	67
1.9.2.	Avrupa Kıtası	68
1.9.2.1.	Fransa	68
1.9.2.2.	Estonya.....	69
1.9.2.3.	Lüksemburg	70
1.9.2.4.	İspanya	70
1.9.2.5.	İsviçre	71
1.9.2.6.	Birleşik Krallık.....	72
1.9.2.7.	Belçika.....	75
1.9.2.8.	Danimarka	76
1.9.2.9.	Finlandiya	77
1.9.2.10.	Almanya	77
1.9.2.11.	Polonya.....	78
1.9.2.12.	İsveç.....	79
1.9.2.13.	İzlanda.....	80
1.9.3.	Orta Doğu ve Kuzey Afrika	80

1.9.3.1.	<i>İsrail</i>	80
1.9.3.2.	<i>Mısır</i>	81
1.9.4.	Merkez Asya	81
1.9.4.1.	<i>Kazakistan</i>	81
1.9.4.2.	<i>Özbekistan</i>	82
1.9.5.	Güney Asya	82
1.9.5.1.	<i>Hindistan</i>	82
1.9.5.2.	<i>Nepal</i>	83
1.9.6.	Doğu Asya ve Pasifik Bölgesi	83
1.9.6.1.	<i>Avustralya</i>	83
1.9.6.2.	<i>Japonya</i>	84
1.9.7.	Güney Asya ve Pasifik	85
1.9.7.1.	<i>Güney Kore</i>	85
1.9.7.2.	<i>Çin</i>	86
1.10.	KRİPTO PARA VE TÜRKİYE	89

İKİNCİ BÖLÜM

KRİPTO PARA VE KARA PARA AKLAMA SİSTEMİ

2.1.	KARA PARA AKLAMA SİSTEMİ	100
2.1.1.	Kara Para Tanımı	100
2.1.2.	Kara Para Aklamanın Tarihi	101
2.1.3.	Kara Para Aklama Aşamaları	102
2.1.3.1.	<i>Yerleştirme Aşaması</i>	103
2.1.3.2.	<i>Ayrıştırma Aşaması</i>	103
2.1.3.3.	<i>Bütünleştirme Aşaması</i>	103
2.1.4.	Kara Para Aklama Yöntemleri	104
2.1.4.1.	<i>Parçalama (Structuring) Yöntemi</i>	104
2.1.4.2.	<i>Fonların Fiziki Olarak Ülke Dışına Kaçırılması; Nakit Kaçakçılığı</i>	104
2.1.4.3.	<i>Kumarhane ve Gazinolar</i>	104
2.1.4.4.	<i>Şirinler (Smurfing) Yöntemi</i>	105
2.1.4.5.	<i>Paravan (Kâğıt Üstündeki) Ya Da Hayali Şirketler</i>	105

2.1.4.6.	<i>Alternatif Havale Sistemleri (Hawala vs.)</i>	105
2.1.5.	Kara Para Aklama İle Mücadele	110
2.1.6.	Kara Para Aklama Sisteminde Kripto Paranın Yeri	113
2.2.	TERÖRÜN FİNANSMANI VE KRİPTO PARA	115
2.3.	İNTERNET VE KARANLIK İNTERNET	128
2.3.1.	İnternetin Kısa Tarihi	128
2.3.2.	Darknetin Kısa Tarihi	130
2.3.3.	Derin İnternet (Deep Web), Karanlık Ağ (Dark Web) ve Darknet Kavramları	133

ÜÇÜNCÜ BÖLÜM

KRİPTO PARA VE MİLLİ GÜVENLİK BOYUTU

3.1.	MİLLİ GÜVENLİK KAVRAMI	139
3.1.1.	Ulusal Güvenlik	143
3.1.2.	Askeri Güvenlik	145
3.1.3.	Ekonomi Güvenliği	147
3.1.4.	Ulusal Güvenlik ve Ekonomi Güvenliği	152
3.1.5.	Kripto Para ve Ekonomi Güvenliği	153
3.1.6.	Milli Güvenlik ve Kripto Para	159
SONUÇ		162
KAYNAKÇA		174
ÖZGEÇMİŞ		192

KISALTMALAR LİSTESİ

AEAT	: Spanish Tax Agency
AIFC	: Astana International Financial Centre
AML	: Anti Money Laundering
AMLD	: Anti Money Laundering Directive
ASIC	: Application Specific Integrated Circuit
ATM	: Automatic Teller Machine
ATO	: Australian Taxation Office
BDDK	: Bankacılık Düzenleme ve Denetleme Kurumu
BIS	: Bank for International Settlements
BM	: Birleşmiş Milletler
BTC	: Bitcoin Core
CFTC	: Commodity Futures Trading Commission
COVID-19	: Koronavirüs Salgını
CPMI	: Committee on Payments and Market Infrastructures
CPU	: Central Processing Unit
CSA	: Canadian Standards Association
DDos	: Distributed Denial of Service
DES	: Data Encryption Standard
EBA	: European Banking Authority
ECB	: European Central Bank
EFTS	: Elektronik Fon Transfer Sistemi
ESMA	: European Securities and Markets Authority
FATF	: Financial Action Task Force
FBI	: Federal Bureau of Investigation
FED	: Federal Reserve
FCA	: Financial Conduct Authority
FINMA	: Swiss Financial Market Supervisory Authority
FSMA	: Financial Services and Markets Authority

FinCEN	: Financial Crimes Enforcement Network
FPGA	: Field Programmable Gate Array
FSA	: Financial Services Authority
GPU	: Graphics Processing Unit
GUS	: The Central Statistical Office of Poland
HRMC	: HM Revenue & Customs
ICO	: Initial Coin Offerings
IMF	: International Monetary Fund
IMoLIN	: International Money Laundering Information Network
IOCTA	: Internet Organised Crime Threat Assessment
IRS	: Internal Revenue Service
IOU	: Gayri Resmi Borç Sertifikaları
I2P	: The Invisible Internet Project
MASAK	: Mali Suçları Araştırma Kurulu
MHAFP	: İspanya Maliye ve Kamu Hizmetleri Bakanlığı Maliye Bölümü
NBS	: National Bureau of Standards
NSA	: National Security Agency
PoW	: Proof of Work
PPATK	: Indonesian Financial Transaction Reports and Analysis Center
P2P	: Peer to Peer
SEC	: U.S. Securities and Exchange Commission
ToR	: The Onion Router
UNODC	: United Nations Office on Drugs and Crime
VAT	: Value Added Tax
VPN	: Virtual Private Network
WoW	: World of Warcraft

ŞEKİLLER LİSTESİ

	Sayfa
Şekil 1.1: Paranın Fonksiyonları	6
Şekil 1.2: Sanal Paranın Sınıflandırılması.....	15
Şekil 1.3: Madencilik İçin Kullanılan ASIC Makineler.....	26
Şekil 1.4: Bulut Madenciliği Yapan Sunucular	27
Şekil 1.5: Bitcoin Madenciliğinden Daha Fazla veya Daha Az Elektrik Tüketen Ülkeler.....	29
Şekil 1.6: Dolaşımdaki Bitcoin Sayısı.....	30
Şekil 1.7: Bitcoin'in ABD Doları Karşısındaki Değeri.....	31
Şekil 1.8: Bitcoin'in Piyasa Değeri.....	31
Şekil 1.9: Bitcoin Karıştırıcı.....	32
Şekil 1.10: Bitcoin Mixer.....	33
Şekil 1.11: ToR.....	33
Şekil 1.12: ToR Sayfası.....	34
Şekil 1.13: VPN.....	34
Şekil 1.14: CoinJoin İşlemleri.....	36
Şekil 1.15: Blok Zincir Çalışma Şekli	52
Şekil 1.16: Bitcoin'in Ülkelere Göre Yasal Durumu.....	55
Şekil 1.17: Türkiye İş Bankası Blok Zincir Konusunda Önemli Adım Attı....	92
Şekil 1.18: Türkiye, Dijital Dönüşümde Atak Yapıyor.....	93
Şekil 1.19: Blok Zincirinin Yıldızları Aranıyor.....	93
Şekil 1.20: Türk Kripto Para Borsaları ve Son 24 Saatlik İşlem Hacimleri....	95
Şekil 1.21: Küresel Kripto Para Kabullenme Endeksi.....	96
Şekil 1.22: Bitcoin İle En Çok İşlem Gören Ulusal Para Birimleri.....	97

Şekil 1.23: İstanbul Çevresindeki Toplam Bitcoin ATM’lerinin Sayısı.....	97
Şekil 1.24: İstanbul Çevresindeki Bitcoin Makinelerinin Yerleşke Listesi.....	98
Şekil 1.25: Türkiye’de Kripto Para Borsalarının İşlem Hacmi.....	98
Şekil 2.1: İnternetin Katmanları.....	134
Şekil 2.2: Derin İnternet Temsili.....	135
Şekil 3.1: Kripto Paranın Finansal Sistem Üzerindeki Potansiyel Tehditleri...	155
Şekil 3.2: Merkez Bankası Dijital Para Birimi Gelişim Haritası.....	158



GİRİŞ

İnternetin ve kişisel bilgisayarların icat edilmesinden sonra en büyük yenilik ve değişim olarak nitelendirilen blok zinciri teknolojisinin finansal sistemlere uygulanması ile ortaya çıkan kripto paralar sahip oldukları piyasa değeri ve işlem hacmi ile son on yıldır dünya gündemini oldukça meşgul etmektedir. Kripto paralar ve altında yatan teknoloji yeni bir teknoloji olmakla birlikte dijital paraların çok da yeni bir teknoloji olduğu söylenemez. Paranın banka sistemleri aracılığıyla elektronik olarak elde edilmesi birkaç on yıl öncesine dayanmaktadır. Dağıtık muhasebe defteri teknolojisinin para birimleri ve ödeme sistemleri için kriptografi ile birleştirilmesi ile kripto paranın ortaya çıktığı ifade edilmektedir.¹ Herhangi bir merkezi otoriteye bağlı olmayan, herhangi bir resmi kuruma ihtiyaç duymayan, internet aracılığı ile para transferlerine olanak sağlayan ve ilk kripto para olma özelliği taşıyan Bitcoin, 2008 yılında Satoshi Nakamoto takma adlı anonim kişi veya kişiler tarafından yayınlanan “Kullanıcıdan Kullanıcıya Elektronik Nakit Sistemi” adlı makale ile tüm dünyaya duyurulmuştur. Bitcoin işlemlerinde ihtiyaç duyulan güven sisteminin herhangi bir kuruluşa ya da kişiye karşı olmadığı, burada duyulan güvenin sadece değişmez matematik kurallarına karşı olduğu belirtilmektedir.²

Avrupa Merkez Bankası (European Central Bank - ECB), kripto parayı sanal paranın bir alt kümesi olarak sınıflandırmıştır. ECB’nin “Sanal Para Birimleri Şemaları 2012” adlı raporu bu tür para birimlerini, geliştiricileri tarafından çıkarılan ve kontrol edilen ve belirli bir sanal topluluğun üyeleri arasında kullanılan ve kabul edilen ayrıca herhangi bir düzenlemeye tabi olmayan dijital para biçimi olarak tanımlamaktadır.³

Avrupa Merkez Bankasının Sanal Para Birimleri Şemaları ile ilgili 2015 yılında yayınladığı raporda ise ECB, sanal para birimlerinin tanımını geniş ölçüde güncellemiş olup sanal paranın herhangi bir merkez bankası, kredi kurumu ve

¹ Amber Wadsworth, “What Is Digital Currency”, *Reserve Bank*, Vol. 81, No:3, 2018, s.2.

² Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.38.

³ European Central Bank, *Virtual Currency Schemes*, Almanya, 2012, s.13.

elektronik para kuruluđu tarafından verilmeyen bazı durumlarda paranın yerine alternatif olarak kullanılabilecek bir değerin dijital temsili olarak tanımlanmaktadır.⁴

Sanal paralar son zamanlarda çok yaygın hale gelmeye başlamıştır. Şimdiye kadar sanal paralar bir fiat para olamamıştır ve çoğu hükümet sanal paraları yasal ödeme aracı olarak kabul etmemiştir. Bugün merkez bankaları hükümet adına fiat para basmaktadır. Fiat para deste ve bozuk para olmak üzere fiziksel paradan oluşan yasal ödeme aracıdır. İnsanlar hükümetin iflas etmeyeceğine ve ulusal ekonominin hiçbir zaman çökmeyeceğine inandıkları için fiat paraya güvenmektedirler. Bugün paranın dijital formda ve onu çıkarandan bağımsız olarak herhangi bir sınırlamaya sahip olmadan da ihraç edilebildiği ifade edilmektedir.⁵

Sanal para onu kullanan belirli bir topluluğun değişim aracı olarak değer almaktadır. Sanal paralar çevrimiçi oyun topluluklarında bir fiat para birimi olarak, bir değere sahip olmayan ve paraya çevrilebilen üyelik kredilerini takip etmek amacıyla kullanılmaktaydı. Önceleri çevrimiçi oyunlarda ve uçuş millerinde sıklıkla kullanılan sanal paraların yalnızca topluluğun menfaatlerine uygun olan değer depolama amacıyla hareket etmek üzere tasarlandığı belirtilmektedir.⁶

Şifreleme ve bilgisayar ağı iletişimi ile desteklenen yeni teknolojiler küresel ekonomide dönüşümsel bir değişime neden olmaktadır. Sanal para birimlerinin ortaya çıkması bu süreçte en önemli gelişme olarak nitelendirilmektedir. Sanal para birimleri geleneksel merkezi takas odalarının yerine eşler arası (P2P) iletişimi mümkün kılan özel sektör sistemleri olarak nitelendirilmektedir. Peer to Peer (P2P) kavramı, merkezi otoriteye ihtiyaç duymadan dağıtık olarak kişiler arasında bilgi, data veya varlık paylaşılması esasına dayanan bir kavram olarak tanımlanabilmektedir.⁷ Sanal para birimleri ve bunlarla ilişkili blok zinciri üzerinde dağıtık muhasebe defteri sistemine dayanan diğer teknolojiler hızla gelişmekte ve evrilmektedir. Sanal paraların özellikle sınır ötesi ödeme ve transfer işlemlerinde hızlı ve verimlilik sağlaması ve finansal katılımı teşvik etmesi gibi birçok potansiyel fayda sunduğu düşünülmektedir. Sanal

⁴ European Central Bank, *Virtual Currency Schemes – a further analysis*, Almanya, 2015, s.4.

⁵ Wadsworth, “What Is Digital Currency”, s.4.

⁶ Joshua Baron, Angela O’Mahony, David Manheim ve Cynthia Dion-Schwarz, “National Security Implications of Virtual Currency Examining the Potential for Non-state Actor Deployment”, *Rand Corporation*, Santa Monica 2015, s.7-8.

⁷ Peer to peer nedir?, www.paribu.com, (Erişim:15.02.2021).

para birimlerinin altında yatan dağıtık muhasebe defteri teknolojisi (büyük bir ağda işlemlerin dağıtık yenilikçi bir sistemde takip edilmesi) sanal para birimlerinin de ötesinde potansiyel bir fayda sunmaktadır. Aynı zamanda sanal para birimleri kara para aklama, terörün finansmanı, vergi kaçakçılığı ve dolandırıcılık için potansiyel bir araç olarak risk oluşturmaktadır. Bugüne kadar sanal para birimleri ile ilgili etkin bir düzenleyici sistem mekanizması geliştirilememiştir. Sanal para birimlerinin ulusal seviyede, küresel ölçekte farklı kurumlar için sınır aşan bir sorumlulukta olduğu için düzenlenmesinin oldukça zor olduğu ifade edilmektedir.⁸

Terör örgütleri yasa dışı faaliyetlerini finanse edebilmek amacıyla çeşitli yollardan mali kaynak temin etme yoluna giderler. Terörün finansmanı yasa dışı kaynaklardan elde edilebileceği gibi bazen yasal kaynaklar vasıtasıyla da elde edilmektedir. Terör örgütleri başta uyuşturucu ve silah kaçakçılığı olmak üzere, kara para aklama, vakıf, dernek gibi kuruluşlardan temin edilen aidat ve bağışlar vasıtasıyla yasa dışı faaliyetleri için finans temininde bulunmaktadır. Kripto para modern teknolojiler arasında terör örgütleri tarafından ihtiyaç duydukları finansal kaynak temini için yaygın olarak kullanılmaktadır. Kripto paranın doğası gereği sahip olduğu merkezi olmayan dağıtık ödeme sistemi, işlemlerin kriptolojik protokoller üzerinden anonim olarak yapılabiliyor olması ve madencilik denilen yöntemle kolaylıkla elde edilebiliyor olması terörist gruplar için potansiyel finans kaynağı oluşturmaktadır.

Bu çalışmanın genel planı üç bölümden oluşmaktadır. Birinci bölümde kavramsal ve kuramsal çerçevede geleneksel para kavramından ve paranın tarihçesinden bahsedilerek, elektronik para, sanal para, dijital para ve kripto para kavramları açıklanmıştır. Ardından yaygın bilinen ilk kripto para olma özelliği taşıyan Bitcoin ve sonrasında geliştirilen diğer kripto para çeşitleri ele alınmıştır. Bitcoin'in temelini oluşturan ve internetten sonra bir devrim olarak nitelendirilen blok zincir teknolojisi ve bu teknolojinin günümüzdeki uygulama alanlarından bahsedilmiştir. Dünya ülkelerinin kripto paralara ve en yaygın örneği olan Bitcoin'e olan yaklaşımları ve kripto paranın yasal durumu ele alınmış olup kripto paranın Türkiye'deki yansımaları irdelenmiştir.

⁸ International Monetary Fund, *Virtual Currencies And Beyond: Initial Consideration*, January 2016, s.5.

İkinci Bölümde kripto paranın kara para aklama sistemi ve terörün finansmanı ile ilişkisi açıklanmıştır. Kara para aklamanın tarihçesine değinilerek, kara para aklama aşamaları, yöntemleri ve kara para aklama ile mücadele konuları anlatılmıştır. Kripto paranın yasa dışı kullanıldığı diğer alanlardan bahsedilerek internet ve karanlık internetin tarihçesine değinilmiştir. Derin internet, karanlık ağ ve dark net kavramları açıklanmıştır ve darkweb suç ekosistemine yer verilmiştir.

Üçüncü Bölümde kripto paranın milli güvenlik boyutu ele alınmış olup öncelikle çeşitli güvenlik tanımlamalarına yer verilmiş, ardından milli güvenlik kavramı açıklanmıştır. Ulusal güvenlik, askeri güvenlik ve ekonomi güvenliği kavramlarına değinilerek, ulusal güvenlik kavramı ile ekonomi güvenliği arasındaki bağ açıklanmıştır. Ekonomi güvenliği, kripto para bağlamında değerlendirilmiş olup son kısım olan milli güvenlik ve kripto para bölümünde ise yeni nesil teknolojilerden biri olan blok zincir teknolojisinin finansal sistemlerdeki bir yansıması olarak ortaya çıkan kripto paranın sahip olduğu karanlık tarafların ekonomi güvenliği ile yakın ilişkide bulunan milli güvenlik açısından ne tür riskler oluşturabileceğinin analizi yapılmıştır.

BİRİNCİ BÖLÜM

KAVRAMSAL VE KURAMSAL ÇERÇEVE

1.1. GELENEKSEL PARA KAVRAMI

İnsan hayatında önemli bir iktisadi fonksiyona sahip olan ve dilimize Farsçadan geçmiş olan para, toplumların mübadele yani değişim ve değer biçimi olarak kullanmayı benimsediği araç şeklinde ifade edilmektedir.⁹ Para kelimesi birçok şeyi ifade edebilir. Günlük konuşma dilinde birden fazla farklı yan anlamda kullanılmaktadır. Diğer taraftan çok paraya sahip olduğunu söyleyen birisinin genellikle zengin olduğu anlamı çıkarılır. Diğer taraftan ekonomistlere göre para çok özel bir anlama sahiptir. Ekonomistler parayı mal ve hizmetlerin ödemesinde veya borçların geri ödemesinde kullanılan genel olarak kabul edilen herhangi bir şey olarak tanımlamaktadır. İster altın, ister kâğıt, ister boncuk ister bıçak olsun herhangi bir ekonomi için paranın üç geleneksel fonksiyonu bulunmaktadır.¹⁰

Para aynı zamanda bir değer biçimi, değer saklama ve tasarruf aracı olarak da tanımlanmaktadır. Paranın mübadele aracı işlevi; mal ve hizmetlerin trampa ekonomisinde mal ve mal şeklinde, parasal ekonomilerde ise mal ve para şeklinde birbirleri ile değiştirilebilmesi olarak ifade edilmektedir. Mal ve hizmetlerin değerlerinin para ile ölçülmesi paranın değer ölçüsü işlevini ifade etmektedir. Paranın ileride kullanılabilmesi ihtiyacına karşılık saklanması ve biriktirilmesi ise paranın değer saklama ve biriktirme işlevi olarak tanımlanmaktadır.¹¹

Bir diğer ifadeyle para, herkes tarafından kabul edilen, kolay taşınabilir olması, zaman içerisinde değerini muhafaza etmesi sebebiyle biriktirilebilir olması, bölünebilir olması, dayanıklı olması ve sınırlı sayıda olması gibi özelliklere sahiptir. Bir varlığın para olarak değerlendirilebilmesi için bu işlevleri her zaman yerine getirmesi beklenmez. Farklı varlıklar çeşitli zamanlarda paranın sahip olduğu bu fonksiyonların bir kısmını veya tamamını yerine getirmiş olabilir. Radford 1945

⁹ Sadun Aren, *100 Soruda Para ve Para Politikası*, İstanbul 1991, s.7.

¹⁰ Susanne König, "The Evolution of Money From Commodity Money to E-Money", *UNICERT IV Program*, June 2001, s.4.

¹¹ Mahfi Eğilmez, *Makroekonomik Denge*, İstanbul 2009, s.167.

yılında, İkinci Dünya Savaşı sırasında Nazi savaş kamplarında esir olan mahkûmlar arasında sigaranın para vazifesi gördüğünü ve paranın bu üç işlevini de yerine getirdiğini belgelemiştir.¹²

Şekil 1.1: Paranın Fonksiyonları¹³



1.2. PARANIN TARİHÇESİ

Tarih öncesi çağlarda bugün kullandığımız şekliyle para kullanılmıyordu, insanoğlu bunun yerine maddeyi para olarak kullanılıyordu ve bu durum mal para kavramının ortaya çıkmasına neden olmuştur. İnsanoğlu, ilk çağlarda yaptığı avcılık, balıkçılık gibi ticari faaliyetlerinde para yerine hayvan derileri, balık gibi çeşitli eşyaları takas olarak kullanmışlardır. Takas, alışverişte mal bedelinin diğer bir malla ödenmesi olarak tanımlanmaktadır.¹⁴ Trampa olarak da adlandırılan malın mal ile değişimi olayı daha sonra gerçekleşecek olan pazar ekonomisinin de temelini oluşturmaktadır.¹⁵

Toplumlar gelişmeye ve değişmeye başladıkça mal para olarak kullanılan unsur da değişmeye başlamıştır. Tarım ve hayvancılığın gelişmeye başladığı dönemde buğday ve arpa gibi tarım ürünleri ve çeşitli hayvanlar mal para olarak kullanılmaktaydı. Endüstrinin gelişmesine müteakip her ülkenin sahip olduğu, çeşitli endüstri ürünleri de mal para olarak kullanılarak tarihteki yerini almıştır. Bunun yanı sıra süs eşyaları, deniz kabukları da mal para olarak kullanılmıştır. Değerli madenler ise mal paralar içerisinde en önemli yere sahip olan ve bugün de bu önemi koruyan varlıklar olmuştur. Devletlerin egemenliğinin göstergesi olan para basımının tarihte ilk

¹² Robleh Ali, John Barrdear, Roger Clews ve James Southgate, “The Economics of Digital Currencies”, *Bank of England Quarterly Bulletin*, İngiltere 2014, p.3.

¹³ European Central Bank (ECB)

¹⁴ Ali Keleş, *İslam’a Göre Para Kavramı*, Doktora Tezi, Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Bursa 1998, s.2.

¹⁵ Osman Eskicioğlu, *İslam ve Ekonomi*, İzmir 1999, s.51.

olarak kim tarafından ve nerede basıldığı ile ilgili çeşitli bilgiler yer almaktadır. 1924 yılında Hintli bir bilgin olan Barnaji bugünkü Pakistan sınırları içerisinde yer alan aşağı İndus Mohanjodaro kazısında M.Ö. 2900 yılına ait paralar bulmuştur. Asur hükümdarı Sennashareb'in M.Ö. 700'li yıllarda bastırmış olduğu gümüş külçeler de bilinen en eski sikkeler arasında sayılmaktadır. Çin'de ise en eski paralar Çin Hanedanı tarafından basıldığı bilinmektedir. Anadolu'da ise Lidya kralı Gyges ve Croesos M.Ö. 7. yüzyılda ilk para basımını gerçekleştirdiği söylenmektedir.¹⁶

Tarihi gelişimine göre para çeşitleri mal para, temsili para, kaydi para ve para benzerleri ve para ikamesi olmak üzere dört kısımda sınıflandırılmaktadır. Tarih boyunca trampa usulü olarak kullanılan ve ilk para çeşidi olarak tanımlanan mal para; kendi değeri satın alma gücüne eşit olan para olarak ifade edilmektedir.¹⁷ Emtia para olarak da adlandırılan ve üretildiği maddeden değerini alan mal para genellikle altın ve gümüş sikkelerden oluşmaktadır. Değeri, ağırlığı ve saflığına bağlı olan altın ve gümüş sikkeler devlet tarafından çıkarılabilmektedir. Sonuç olarak emtia bazlı bir para biriminin değerini uygulamak için merkezi bir otorite gerekli değildir. Emtia bazlı para birimleri de oldukça anonimdir. İşlemlerin hiçbirinde kullanıcılarını veya kullanımlarını izleyen bir kayıt tutulmamıştır. Birçok emtia tabanlı para birimleri zaman içerisinde istikrarlı bir değere sahip olsa da emtia tabanlı para birimleri herhangi bir parasal otoritenin kontrolünün ötesinde değer dalgalanmalarına karşı savunmasız kalmıştır. Bunun nedeni, para biriminin değer tabanının mal için arz ve talebi yansıtmasıdır.¹⁸

Kökeni çok eskilere dayanan, kendi değeri olmayan temsili para bir yerde depo edilen (örneğin bankalarda) mal para veya madeni külçe ve sikkelerin karşılığında çıkarılan paradır. M.Ö. 6. yüzyılda Babil'de o dönemin banka işlevini gören kurumlarda madeni paraları temsil yerine kâğıt para kullanılıyordu. Hollanda ve İtalya'da ise 17. yüzyıldan itibaren insanlar depo edilen madenler karşılığı kendilerine verilen sertifikaları para olarak kullanmışlardır.¹⁹ İlk kâğıt paranın M.S. 806 yılında

¹⁶ Vildan Serin, *Para Politikası (Tarihi – Teorik Gelişmeler ve Türkiye Uygulaması)*, Marmara Üniversitesi Yayın No:440, Hukuk Fakültesi Yayın No:4, İstanbul 1987, s.26-27., Keleş, *İslam'a Göre Para Kavramı*, Doktora Tezi, s.7.

¹⁷ Keleş, *İslam'a Göre Para Kavramı*, s.10.

¹⁸ Baron, ve diğerleri, "National Security Implications of Virtual Currency Examining the Potential for Non-state Actor Deployment", *Rand Corporation*, s.6.

¹⁹ Serin, *Para Politikası (Tarihi – Teorik Gelişmeler ve Türkiye Uygulaması)*, s.29.

Çin’de ortaya çıktığı bilinmektedir. 17. yüzyılın sonlarında ise Batıda basılmaya ve kullanılmaya başlayan kâğıt paranın 1690’lı yıllarda Amerika Birleşik Devletleri’nde Massachusetts Hükümeti tarafından, İngiltere’de ise kuyumcular tarafından basımının yapıldığı ve dolaşıma çıkarıldığı bilinmektedir.²⁰ Bankacılığın Floransa’lı Medici ailesi tarafından keşfi ile Avrupa para ve finans merkezi olarak uzun bir süre dünya ticaretinde yer almıştır.²¹ Bankacılık sisteminin batıda doğmasının ardından 19. yüzyılın ortalarında bankacılık sektöründe ihtisaslaşan İngiliz bankacıları tarafından geliştirilen ve bankadaki vadesiz mevduatlarda bulunan para da kaydi para (yazı para veya banka parası) olarak tanımlanmaktadır.²² Bunların dışında kredi kartları, vadeli banka mevduatları, devlet tahvilleri, hazine bonoları ve banka yatırım fonları ise para ikamesi olarak kullanılmaktadır.

Finansal yenilikler insanlara ekonomik işlemlerini fiziksel para birimlerinin getirdiği kısıtlamaların ötesinde gerçekleştirebilmelerine olanak sağlamaktadır. Çek hesabındaki paranın karşılığında yazılan çek ile benzer şekilde ülkelerin para birimleri olarak ifade edilen kambiyo senetleri 1200’lü yıllarda Avrupa’da ticaret fuarlarında kasabadan kasabaya ve/veya ülkeden başka bir ülkeye yüklü miktarda altın göndermemek için ticareti kolaylaştırmak amacıyla ortaya çıkmıştır. Çok yakın zamanda meydana gelen teknolojik yenilikler kullanıcılara kâğıt tabanlı değişim veya ödeme sistemlerinin mobil hesaplama programları aracılığıyla radyo iletişimini mümkün kılan (örneğin akıllı telefonlar üzerindeki uygulamalar gibi) yakın alan iletişim teknolojisinin kullanıldığı (kredi kartlarının bir kart okuyucusunda kaydırılıp okutulması gibi) elektronik sistemlere geçiş yapmaya imkân sağlamıştır ve sağlamaktadır.²³

1609 yılında kurulan ilk kamu bankası olma özelliği taşıyan Amsterdam Bankası madeni paranın karşılığı olmayan kâğıt parayı basan ilk banka olarak tarihteki yerini almıştır.²⁴ Birinci Dünya Savaşı’na kadar genellikle altın olarak değerlendirilen mal para, devletlerin bastıkları kâğıt paralarla temsil ediliyordu. Fakat İkinci Dünya

²⁰ Türkiye Cumhuriyet Merkez Bankası, *Kâğıt Paranın Tarihçesi*, s.2.

²¹ Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.50.

²² Keleş, *İslam’a Göre Para Kavramı*, s.27.

²³ Baron, ve diğerleri, “National Security Implications of Virtual Currency Examining the Potential for Non-state Actor Deployment”, *Rand Corporation*, s.7-8.

²⁴ Eğilmez, *Kolay Ekonomi*, s.98.

Savaşı'ndan sonra bu durum değişmiştir. 1944 yılında Amerika Birleşik Devletlerinin New Hampshire eyaletinin Bretton Woods kasabasında Birleşmiş Milletler tarafından düzenlenen ve 44 ülkeden 730 delegenin katıldığı Birleşmiş Milletler Para ve Finans Konferansında altına endeksli Dolar basılması ve dünyadaki diğer para birimlerinin de Dolara göre değer bulması şeklinde bir karar alınmıştır.²⁵ Fakat 1971 yılında altın karşılığında Dolar basma uygulaması diğer bir ifadeyle altın-döviz standardı sistemi terk edilmiştir diğer para birimlerinin Dolara endeksli olması sebebiyle de tüm dünyadaki para birimleri karşılıksız kalmıştır. Bu tarihten sonra itibari para sistemi denilen yani karşılığı sadece devletin itibarını teşkil eden bir yeni bir finans düzeninin başladığı ifade edilmektedir. İkinci Dünya Savaşı sonrasında uygulamaya konulacak sistemin temellerinin atıldığı Bretton Woods'un en önemli çıktısının; altının en güvenilir rezerv varlık ve nihai değer ölçüsü olarak kabul edilmesi ve diğer taraftan da Doların rezerv para olarak tanımlanması şeklinde olduğu belirtilmektedir.²⁶

1.3. ELEKTRONİK PARA KAVRAMI

Paranın formları yüzyıllar boyunca ekonomideki teknolojik gelişmeler ile yakından ilişkili olmuştur. Ödeme sistemleri de paranın farklı formlarıyla birlikte değişim göstermekte ve gelişmektedir. Basit ekonomiler daha karmaşık ekonomilere doğru geliştikçe para farklı ekonomik koşullara her zaman uyum sağlamıştır. Bilgisayar endüstrisindeki en son yeniliklere göre paranın yeni biçimi olarak elektronik para gelişmiştir.²⁷

Bilgisayar ve ileri telekomünikasyon teknolojilerindeki gelişmeler nedeniyle ödeme sistemlerinde elektronik para transfer sisteminin icat edilmesi gibi yeni gelişmeler meydana gelmiştir. Bu teknoloji bankamatik kart okuyucu ve kişisel bilgisayarlar aracılığıyla ödeme sistemlerine bireysel erişimi başlatmıştır. Günümüzde merkez bankaları, ticari bankalar veya kuruluşlar fon transferi için Elektronik Fon

²⁵Doğaç Özdemir, "Bretton Woods Düzeni (1944-71)", 15.08.2015, <http://www.gazetebilkent.com/2015/08/15/bretton-woods-duzeni-1944-71/> (Erişim: 25.12.2017).

²⁶ Lerzan İskenderoğlu, *Uluslararası Para Sisteminin Sorunları ve İyileştirme Çalışmaları*, Türkiye Cumhuriyet Merkez Bankası Araştırma Planlama ve Eğitim Genel Müdürlüğü, Tartışma Tebliği No: 8807, Ankara 1998, s.6.

²⁷ König, "The Evolution of Money From Commodity Money to E-Money", s.3.

Transfer Sistemi'ni (EFTS) kullanmaktadırlar. EFTS ile bağlantılı olarak bankamatik kartı ve kredi kartı gibi plastik kartlar yaygınlaşmaya başlamıştır.²⁸

Günümüzde iletişim teknolojileri alanında yaşanan ilerlemeler ve gelişmelerin finansal alanlara uygulanmasıyla birlikte ve internet kullanımının da yaygınlaşması insanların artık nakit kullanmayı tercih etmeyen bir toplum haline dönüşmesine neden olmuştur. Nakit para taşımanın zorluğu ve riski, bunun yanı sıra devletlerin vatandaşlarının varlıklarını rahatlıkla izleyebilmeleri gibi hususlarında buna eklenmesi elektronik para kavramının ortaya çıkma ihtiyacını doğurmuştur. Bilgisayar ve iletişim teknolojilerindeki gelişmeler politika üreticilerinin yeni perakende ödeme sistemlerinin gelişmesi ve büyümesine yönelik olarak bazı önemli değişiklikler yapmasına neden olmuştur. Dikkate değer en önemli gelişme elektronik para ve finansal işlemlerin evden veya herhangi bir yerden kişisel bilgisayarlar kullanılarak gerçekleştirilmesi olmuştur.²⁹ Elektronik ödeme sistemlerindeki gelişmeler bilgi teknolojilerindeki ilerlemeler ve global ekonomi karakteristikleri ile ilişkilidir. Bu proses lineer ve düz bir formda değildir. Birçok faktör yeni elektronik sistem özelliklerini etkilemektedir. Örneğin bir ülkenin gelişme seviyesi ve o ülkenin global pazara açılması ve farklı para piyasaları ile entegrasyonu, ülkenin yeni teknolojileri kabul etme kapasitesi yani teknolojiye açıklığı ve ülkenin eğitim seviyesinin önemi hayati faktörler arasında sayılabilmektedir.³⁰

Kredi kartı, sanal kart, ATM, mağaza kartı gibi akıllı kart olarak nitelendirilen taşınabilir plastik kart olarak hayatımıza yerleşen elektronik para, geniş bir ifadeyle parasal değerlerin banka hesaplarını kullanmayı gerektirmeksizin ön ödemeli araç olarak kullanıldığı ve teknik bir cihaz üzerinde elektronik olarak saklanan para olarak tanımlanmıştır. Elektronik para, paranın var olan diğer formlarından değişik şekillerde farklılık göstermektedir. Yalnızca fiziksel güvenlik özellikleri kullanan nakit ile karşılaştırıldığında, elektronik para ürünleri doğrulama işlemleri ve gizliliği ve verinin doğruluğunu korumak amacıyla kriptografi kullanmaktadır.³¹ Kredi kartı tanımı ilk

²⁸ Age, s.12.

²⁹ *An Introduction to Electronic Money Issues Toward Electronic Money and Banking: The Role of Government*, Washington DC, September 1996, s.4.

³⁰ Neda Popovska-Kamnar, "The Use Of Electronic Money And Its Impact On Monetary Policy", *JCEBI*, Vol.1, No:2, 2014, s.80.

³¹ European Central Bank, *Report On Electronic Money*, 1998, s.7.

defa 1887 yılında yazar Edward Bellamy tarafından “*Looking Backwards From 2000 to 1887*” isimli kitabında ortaya atılmıştır. O dönemde kredi hesapları genellikle Amerikalı tüccarlar tarafından güvendikleri müşterileri arasında borçların daha sonra ödenebilmesine imkân sağlamak amacıyla kullanılıyordu.³² Mikroelektronik endüstrinin gelişmesinin akabinde mikroelektronik aygıtların plastik kartlara ilk uygulanması Kunitaka Arimura tarafından 1970 yılında yapılmıştır.³³ Sonrasında Fransız gazeteci Roland Monero patentini aldığı bu teknoloji sayesinde 1974 yılında ilk akıllı kartları icat etmiştir.³⁴ Bu alanda en büyük çığır açıcı gelişme ilk defa 1984 yılında Fransa’da o dönemdeki adıyla PTT (Postes, Télégraphes et Téléphones) kurumunda başarıyla uygulamaya geçmiştir.³⁵

Avrupa Birliği 2009/110 sayılı *Elektronik Para Kuruluşlarının Kurulması, Faaliyetlerinin Sürdürülmesi, Denetimi Direktifinin* 2. Maddesi uyarınca ise elektronik para; fon alımı üzerine düzenlenen ve çıkarılan parasal değerden daha az olmayan, kendisini ihraç edenler dışındakiler tarafından ödeme aracı olarak kabul edilen ve elektronik olarak depo edilen parasal değer şeklinde ifade edilmektedir.³⁶

Üretimi reel fakat transferi ve saklanması dijital ortamda gerçekleştirilen elektronik para, parayı çıkaran kuruluş dışındaki kişilerce de kabul edilmektedir, yasal olarak düzenlenmektedir, gözetimi ve denetimi yapılmaktadır ayrıca Türk Lirası ve Avro gibi para birimlerine de tedavülü bulunmaktadır. Elektronik parayı belirtmek üzere kullanılan birçok farklı isim bulunmaktadır: dijital nakit, dijital para, siber para, e-nakit vs. Elektronik para bir değişim aracı veya değer deposu olarak hizmet veren dijital ödeme mesajı olarak nitelendirilmektedir.³⁷

Para ve elektronik para arasındaki en büyük farklılık elektronik paranın şahsa bağlı olmaması ve sanal olmasıdır. Kredi kartı ve banka kartının aksine elektronik para her zaman önceden ödenmiştir. Tekniği farklı olan örneğin elektronik coin, kredi kart çipi ve dijital çekler şeklinde çok sayıda elektronik para sistemi bulunmaktadır. Çok

³² John Klernan, “When Were Credit Cards Invented? A Complete History”, 2015, s.1.

³³ Wolfgang Rankl and Wolfgang Effing, *Smart Card Handbook*, Giesecke & Devrient GmbH, Germany 2010, s.3.

³⁴ Efraim Turban ve Debbie McElroy, “Using Smart Cards in Electronic Commerce”, California 1998, s.1.

³⁵ Rankl ve Effing, *Smart Card Handbook*, s.3.

³⁶ European Central Bank, *Virtual Currency Schemes*, 2012, s.16.

³⁷ König, “The Evolution of Money From Commodity Money to E-Money”, s.15.

çeşitli formdaki bu dijital paralar değer depolama ve transfer şeklinde halen milli para birimi olarak kullanılmaktadır. Ödeme aracı olarak çok geniş bir kullanıma sahip olan kredi kartlarına ek olarak elektronik çekler de kullanılmaktadır.

1.4. SANAL PARA KAVRAMI

Teknolojinin ve internetin çok hızlı bir değişim ve gelişim gösterdiği günümüz dünyasında sanal dünya olarak tabir edilen ve oldukça yaygınlaşan kavramın ortaya çıkmasıyla birlikte teknolojinin finansal sektörler üzerinde yoğunlaşması sanal ekonomi kavramının doğmasına neden oldu. Sanal ekonomi beraberinde sanal para kavramını getirmiştir. Sanal paralara olan ilgi her geçen gün önemli ölçüde artmaktadır. Bu ilgi ve alaka risk sermayedarlarından siber güvenlik uzmanlarına diğer taraftan ekonomistlere kadar birçok topluluğa göre farklılık göstermektedir. Bununla birlikte teşkilatlı gruplar ve hükümetler sanal paraların çok çeşitli yasal ve yasal olmayan amaçlarının ne olduğu araştırmakta ve/veya benimsemektedir. Sanal para teriminin tek global bir tanımı bulunmamaktadır. Bununla birlikte Fransız ve Alman Maliye Bakanlıkları bu teknolojileri tarif ederken para birimi teriminin kullanılmasının yanıltıcı olduğunu ve yeni bir terim olarak da bu teknolojilere “kripto varlıklar” denmesinin uygun olabileceğini ifade etmişlerdir.³⁸

Sanal para elektronik paranın bir çeşidi olarak nitelendirilmektedir. Sanal paranın üzerinde birliğe varılmış tek bir tanımı bulunmamaktadır. Örneğin Avrupa Bankacılık Otoritesi’ne (European Banking Authority – EBA) göre sanal para, ne merkez bankası veya kamusal bir otorite tarafından çıkarılan ne de fiat para birimi ile ilişkilendirilmiş; fakat bir değişim aracı olarak elektronik yolla transfer edilebilen, depo edilebilen veya ticareti yapılabilen bir değer dijital temsili olarak tanımlanmaktadır.³⁹

Mali Eylem Görev Gücü’ne (Financial Action Task Force – FATF) göre sanal para, dijital olarak alınıp satılabilen, değişim aracı, hesap birimi ve bir değer deposu özelliklerine sahip olan fakat yasal ödeme aracı olmayan bir değer dijital temsili

³⁸European Parliament, *Virtual Currencies and Terrorist Financing: Assessing The Risks and Evaluating Responses*, May 2018, s.12.

³⁹ European Parliament, *Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead*, July 2018, s.7.

olarak ifade edilmektedir. Sanal para elektronik paradan, elektronik paranın sahip olduğu “fiat paranın dijital temsili” ifadesinden dolayı farklılık göstermektedir.⁴⁰

Avrupa Merkez Bankası’nın tanımına göre sanal para, ağ ortamında yasal tedavülü bulunmayan, hukuki bir düzenleme içermeyen, denetime tabi olmayan ve geliştiren kişi veya gruplar tarafından kontrol edilen ve kullanıcıları tarafından kabul edilen para birimleri olarak ifade edilmektedir. Ayrıca Avrupa Merkez Bankası ileride teknolojik gelişmelerin değişmesi ve gelişmesi sonucu sanal para meydana gelen değişiklikler nedeniyle bu tanımın değişebileceğini de belirtmektedir. Sınıflandırması kolay olmayan birçok sanal para sistemi bulunmaktadır. Mümkün olan en iyi sınıflandırma ile sanal para sistemlerini, sanal paraların gerçek para ve ekonomilerle olan ilişkisi göz önünde bulundurularak üç kısımda ifade etmek mümkündür. Belli bir topluluk içerisinde kullanılan ve gerçek ekonomi ile hiçbir ilişkisi bulunmayan sanal paralar kapalı sistem sanal paralar olarak adlandırılır. “sadece oyunda” ifadesi ile anılan bu sanal paralarda kullanıcı genellikle abonelik ücretini öder ve çevrimiçi performansına göre sanal para kazanır ve kazanılan para yalnızca oyun içerisinde sanal mal ve hizmet alımlarında kullanılabilir ve sanal sistemin dışında kısıtlı kullanım imkânına sahiptir, örnek olarak World of Warcraft (WoW) oyunu verilebilir.⁴¹

Diğer sanal para sistemi olan tek yönlü akışa sahip sanal para sisteminde, sanal para belli bir kur farkıyla reel para kullanılarak satın alınabilir fakat tekrar reel paraya dönüştürülemez. Örnek olarak Facebook Credits verilebilir. Çift yönlü akışa sanal para sisteminde ise kullanıcı reel parasını belli bir değişim oranı/kur üzerinden sanal para alımında kullanabilir ve aynı zamanda satabilir. Ayrıca sanal paranın mal ve hizmet alımı ödemelerinde kullanımını kabul eden işletmelerde de kullanılabilir.⁴²

Linden Doları ve Bitcoin çift yönlü akışa sahip çok yaygın olarak kullanılan sanal paralar olarak kabul edilmektedir. Bir varlığın veya değer paranın sahip olduğu işlevleri ne ölçüde karşıladığı kişiden kişiye ve zamana göre farklılık gösterebilir. Teorik olarak sanal paralar internet erişimi olan bilgisayar veya bu işlevi gören cihazlara sahip olan kişiler için para olarak kullanılabilir. Günümüzde sanal paralar

⁴⁰ Anna Wisniewska, “Bitcoin As An Example of Virtual Currency”, *Institute of Economic Research Working Papers*, Poland 2016, s.10.

⁴¹ European Central Bank, *Virtual Currency Schemes*, 2012, s.13.

⁴² European Central Bank, *Virtual Currency Schemes*, s.14.

sadece bu sistemi kullanan belirli kişilere göre para vazifesi görmektedir. Diğer bir ifadeyle sanal para, paranın sahip olduğu üç işleve sahip olarak dünya genelinde sadece birkaç milyon kişiye hizmet etmektedir.⁴³

Mali Eylem Görev Gücü'ne göre sanal para, dijital olarak ticareti yapılabilen ve bir değişim aracı olarak bir hesap birimi ve bir değer deposu olan fakat yasal bir ödeme aracı olmayan bir değerın dijital temsili olarak tanımlanmaktadır. Sanal paralar hiçbir emtia veya ülkenin resmi para birimi ile ilişkili olmadıkları için gerçek bir değeri yoktur. Sanal paraların değeri, yalnızca elektronik ekosistemi içerisindeki değerin bir yerden diğer bir yere transfer edilebilmesi yeteneğinden kaynaklanır ve herhangi bir kimseyi sanal paranın ödeme aracı olarak kabul ettirilmesinin yasal bir yolu olmadığı için yalnızca kullanıcılar arasındaki güven ilişkisine dayanır. Ülkelere göre sanal paranın, paranın karakteristiklerini eksiksiz olarak karşılayıp karşılamadığı tartışmalı bir konu olarak hala dünya gündemini meşgul etmektedir. Örneğin, Söderberg (2018), Kanada Bankası 2014 yılında, İngiltere Bankası (2014), ve Yermack (2013) yılında diğerlerine göre sanal paraların ekonomi literatürüne göre paranın geleneksel tanımını karşılamadığı görüşünü savunmuşlardır. Özellikle Jevons tarafından 1875 yılında ifade edilen paranın sahip olduğu üç temel fonksiyonu karşılamadığını düşünmektedirler. Eleştirilere göre sanal paralar çok sınırlı bir alanda ödeme aracı olarak hizmet göstermektedir. Çok sınırlı sayıda tüccarın sanal paraları kabul edip işlem yaptıkları için, sanal paralarla yapılan işlem hacimlerinin ülke parasının işlem hacmine göre çok önemsiz seviyede olduğu ve sanal paraları yasal ödeme aracı olarak kabul eden hükümetlerin bulunmadığını iddia etmektedirler.⁴⁴

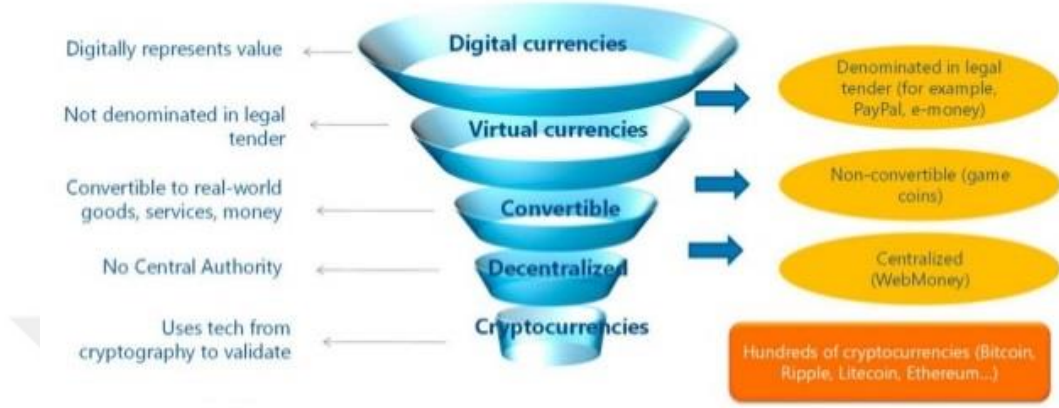
Bir değerın dijital temsili olarak sanal paralar dijital para birimleri kategorisinde daha geniş bir yere sahiptir. Sanal paralar fiat para birimleri için bir dijital ödeme mekanizması olan elektronik paralardan farklılık göstermektedir ve kendi hesap birimine sahiptir. Elektronik paranın geleneksel para birimine bağlı olarak yasal olarak düzenlendiği ve hesap biriminin yaygın olarak kabul edildiği, sabit olduğu ve kontrol edilebildiği ve kullanıcının çoğunlukla operasyonel bir risk aldığı belirtilmektedir. Diğer taraftan sanal para kavramının yeni bir kavram olduğu,

⁴³ Ali, Barrdear, Clews ve Southgate, "The Economics of Digital Currencies", s.4.

⁴⁴ European Parliament, *Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead*, s.7.

düzenlemeye tabi olmadığı ve dar bir sanal topluluk tarafından kabul edildiği ve arzının sabit olmadığı çıkarıcısının kararına bağlı olduğu ve üzerinde herhangi bir kontrol mekanizmasının olmadığı ifade edilmektedir.⁴⁵

Şekil 1.2: Sanal Paranın Sınıflandırılması⁴⁶



1.5. DİJİTAL PARA

Dijital para elektronik olarak transfer ve depo edilebilen bir değer geniş bir parasal değişim ortamı olarak tanımlanmaktadır. Sanal paralar ve kripto paralar dijital paranın bir formudur. Dijital paralar; hediye kartları, ürün indirim kartları, uçuş milleri, kredi kartı nakit geri ödülleri gibi birçok ürünü içerebilmektedir. Bütün bunların hepsinin ortak özelliğinin gerçek dünyada bir değerinin yani karşılığının olması ve herhangi bir mal veya hizmet alımlarında kullanılabilmesi olarak ifade edilmektedir. Sanal paralar, sanal dünyada değişim ortamı olarak kullanılan internet tabanlı merkezileştirilmiş sanal paralardır. Sıklıkla çevrimiçi oyunlar ve sosyal medya platformları tarafından kullanılmaktadır. Kripto paraların dijital paranın bir formu olması resmi para olarak tanımlanmaması ve merkezi otoriteler tarafından kontrol edilmemesi bakımından dijital paradan farklılık göstermektedir.⁴⁷ Dijital para internet üzerinde kullanılan bir para çeşididir. Dijital para sadece dijital form olarak varlığını sürdürmekte ve gerçek dünyada fiziksel olarak yer almamaktadır. Fakat geleneksel paranın tüm karakteristik

⁴⁵European Central Bank, *Virtual Currency Schemes*, October 2012 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, (Erişim: 02.01.2021), s.16.

⁴⁶ IMF Staff Discussion Note, *Virtual Currencies and Beyond: Initial Considerations*, January 2016, s.8.

⁴⁷ Grant Thornton, "Digital, Virtual And Crypto Currencies: Issues and Accounting Risks", 2016, s.1.

özelliklerine sahiptir. Dijital para mobil veya internet aracılığıyla çevrimiçi olarak herhangi bir hizmet veya ürün almak için kullanılabilir. Dijital paranın coğrafik veya politik sınırları bulunmamaktadır. İşlemler dünyanın herhangi bir yerinden gerçekleştirilebilmektedir.⁴⁸

1.6. KRİPTO PARA KAVRAMI

Kripto para hiçbir merkezi otoriteye bağlı olmayan, hiçbir resmi kuruma ihtiyaç duymadan internet aracılığı ile herkesin ulaşabileceği açık kaynak kodlu yazılımlar kullanılarak geliştirilmektedir. Kripto para işlemleri, bir coinin bir sanal cüzdandan diğer sanal cüzdana aktarılmasıyla yapılmaktadır.⁴⁹ Kripto para ilk defa ticari olarak David Chaum tarafından bilgisayar devriminin başladığı yıllar olan 1990 yılında DigiCash ile ortaya çıktığı belirtilmektedir. DigiCash kripto paranın transfer işlemleri ikili harcamayı önlemek için kriptografik protokollerin kullanılması ile çevrimiçi veya çevrimdışı olarak gerçekleştiriliyordu. Kriptografik protokoller ayrıca kullanıcıların gizliliğini korumak için kör imza yönteminde de kullanılmaktadır⁵⁰. David Chaum'un bu dâhiyane buluşu ödeme yapan kişinin kimliğini koruyarak, alacaklı kişinin kimliğini tam olarak açık bir şekilde tanımlayabilen kriptografik bir yapı olarak ifade edilmektedir. David Chaum'un New York ve Kaliforniya üniversitelerinde öğretim elemanı olarak görev yaptığı ve bu süre zarfında dijital teknoloji ve kriptografinin para ve oylama gibi birçok önemli konuda kökten değişimlere neden olacak kullanımı ile ilgili konularda bilimsel makaleler kaleme aldığı ve en az on yedi patent başvurusunda bulunduğu bilinmektedir.⁵¹

Kripto paranın en bilinen ve yaygın kullanıma sahip örneği Bitcoin'dir. Bugün Bitcoin yalnız olmamakla birlikte 8.400'den fazla alt coin (taklitçi girişim⁵²) bulunmakta ve kripto para pazarının liderliğini elinde bulundurmaktadır. Bitcoin'in

⁴⁸ Andrew Tar, "Digital Currencies vs. Cryptocurrencies, Explained", (13.12.2017), <https://cointelegraph.com/explained/digital-currencies-vs-cryptocurrencies-explained> (Erişim:12.10.2020).

⁴⁹ Hari Karishnan, Sai Saketh ve Venkata Tej Vaibhav, "Cryptocurrency Mining – Transition to Cloud", International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, India 2015, s.115.
⁵⁰ David Lee Kuo Chuen, *Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments and Big Data*, U.S. 2015, s.8.

⁵¹ Vigna, ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması, Kriptopara Çağı*, s.82-83.

⁵² Age, s.103.

yanı sıra Ethereum, Ripple, Litecoin, Namecoin, PPCoin, Dogecoin, Devcoin, Primecoin gibi alt coinler de mevcuttur.

Her geçen gün sayıları artmakla birlikte Coinmarketcap.com internet sitesinde yer alan bilgilere göre bu tezin yazıldığı dönemde 8.481 tane alt coin bulunmaktadır. Kripto para birimi endüstrisi Bitcoin'den çok daha fazlasını içermektedir. Kripto para birimi endüstrisi içerisinde Bitcoin'in güncel payı %61 olarak 915 milyar ABD Doları piyasa değerine sahiptir. Kripto para işlemlerinin nakit işlemlerinden çok daha şeffaf olduğu fakat diğer çevrimiçi ödeme sistemlerinden ise çok daha anonim olduğu da ifade edilmektedir.⁵³

Kripto paralar banka veya diğer finans kuruluşları gibi güvenilir bir üçüncü tarafa bel bağlamadan işlemlerini doğrulamak ve ağ etkinliği ile ilgili fikir birliğini sağlamak amacıyla kriptografik kanıtlara dayanan açık kaynak kodlu P2P olarak adlandırılan eşten eşe değer transfer ağları olarak da ifade edilmektedir.⁵⁴

Bir görüşe göre, kripto para teknolojisinin amacının esasında geleneksel merkezileşmiş varlık zalimliğinden diğer bir ifadeyle bankalarda, hükümetlerde ve Afganistan'daki aşiret reislerinde yani merkezi bir gücün elinde var olan para ve bilgi gücünü alarak bu gücü gerçek sahipleri olan halka vermek olduğu da ifade edilmektedir.⁵⁵

Avrupa Merkez Bankası gibi Uluslararası Para Fonu (International Monetary Fund – IMF) da kripto para birimlerini özel geliştiricileri tarafından çıkarılan/ihraç edilen ve kendi hesap birimlerinde belirtilen bir değer dijital temsili olarak sanal para birimlerinin alt kategorisi olarak sınıflandırmaktadır. IMF'ye göre sanal para birimleri kavramı basit IOUs Gayriresmi Borç Sertifikaları'ndan internet veya mobil kuponlar ve havayolları milleri arasında değişen geniş bir dizi para birimlerini kapsadığı belirtilmektedir.⁵⁶

Uluslararası Ödemeler Bankası'nın (Bank for International Settlements – BIS) bir kuruluşu olan Ödemeler ve Piyasa Altyapıları Komitesi (Committee on Payments

⁵³ <https://coinmarketcap.com/coins/views/all/>, (Erişim:01.02.2021).

⁵⁴ Virtual currencies and terrorist financing: assessing the risks and evaluating responses, s13.

⁵⁵ Vigna, ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.17-21.

⁵⁶ International Monetary Fund *Virtual Currencies And Beyond: Initial Consideration*, s.7.

and Market Infrastructures – CPMI) kripto paraları dijital para birimleri veya dijital para birimi taslağı olarak sınıflandırmaktadır. Bu taslakların aşağıdaki temel özellikleri gösterdiği söylenmektedir:

- 1) Değeri arz ve talebe göre belirlenen altın gibi emtialara benzer fakat sıfır içsel değere sahip olan
- 2) Dağıtık muhasebe defterlerini kullanan eşten eşe elektronik değer alışverişinde bulunmalarına izin veren taraflar arasında güven olmadığında araçlara ihtiyaç duymayan
- 3) Herhangi bir özel bireysel veya kurum tarafından yönetilmeyen⁵⁷

Avrupa Bankacılık Otoritesi, kripto paraların sanal para olarak ifade edilmesini önermektedir ve sanal paraları da bir merkez bankası veya kamu otoritesi tarafından ihraç edilmeyen veya zorunlu olarak bir fiat para birimi ile ilişkilendirilmeyen fakat gerçek veya tüzel kişiler tarafından bir değişim aracı olarak kullanılan ve elektronik olarak transfer edilebilen, depo edilebilen ve elektronik olarak ticareti yapılabilen bir değer dijital temsili olarak tanımlamaktadır.⁵⁸

Avrupa Menkul Kıymetler ve Piyasa Otoritesi (European Securities and Markets Authority – ESMA), kripto paraları sanal para olarak belirtmiştir ve EBA’nın tanımına tamamen uygun olarak sanal paraları, bir merkez bankası veya kamu otoritesi tarafından çıkarılmayan ve garanti edilmeyen, yasal para veya para statüsüne sahip olmayan bir değer dijital temsili olarak tanımlamaktadır.⁵⁹

Dünya Bankası kripto paraları basit bir dijital ödeme mekanizması olan ve fiat parayla temsil edilen e-money’den farklı olarak kendi hesap birimlerinde ifade edilen, dijital para birimlerinin bir alt kategorisi olarak bir değer dijital temsili olarak tanımlamaktadır. Birçok politika yapıcılarının aksine Dünya Bankası kripto paraları

⁵⁷ Committee on Payments and Market Infrastructures, “Digital currencies”, November 2015, <https://www.bis.org/cpmi/publ/d137.pdf> , , (Erişim: 05.08.2019), s.3.

⁵⁸ European Banking Authority, *Designing a Regulatory and Supervisory Roadmap for FinTech*, Mart 2018, s.5.

⁵⁹ ESMA, EBA & EIOPA, “Warning on the risks of Virtual Currencies https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currencies1.pdf , (Erişim: 05.08.2019), s.1.

konsensüs elde etmek için kriptografik tekniklere dayanan dijital para birimleri olarak tanımlamaktadır.⁶⁰

Basit bir tanım yapmak gerekirse kripto para, kriptografi ve para ile ilişkili bir kavramdır. Kriptografi, gizlilik ve kimlik doğrulama gibi bilgi güvenliği alanına giren konularda matematiksel tekniklerin kullanıldığı bir çalışma alanı olarak nitelendirilmektedir. Kriptografi kopyalama ve çalma gibi kötü niyetli işlemleri önleme ve tespit etme ile ilgili bir kavramdır. Kriptografi, bilgi güvenliğini sağlamanın yanı sıra bu alanda çeşitli metotların ve tekniklerin geliştirilmesine olanak sağlar.⁶¹ Kriptografi yalnızca mesajların şifrlenmesi veya şifrelerinin çözülmesi ile ilgilenmez, aynı zamanda bilgi güvenliği gerektiren gerçek dünya problemlerinin çözülmesine de yardımcı olur.⁶² Bugünkü haliyle olmasa da kriptografinin kullanımı eski Yunanlılara dayanmaktadır ve bilgisayarın dolayısıyla işlemci güçlerinin gelişmesiyle birlikte Bitcoin'in işlemleri gizlilikle yapabilmesinin temelini oluşturmaktadır.⁶³

Bir kripto para, değişim ortamını ve bir hesap birimini temsil eden dağıtık muhasebe defteri üzerinde bir token (dijital varlık) olarak ifade edilebilmektedir. Token, temel olarak bir servis kapsamında yaratılıp sunulan ve o servisin tüm işlevlerini yerine getirilmesinde kullanılan dijital bir varlık türü olarak tanımlanabilir. Kripto para elektronik olarak elde edilebilir, erişilebilir, depo edilebilir/saklanabilir ve iş görebilir. Üçüncü taraf bir aracıya gerek duymadan uçtan uca/eşten eşe özelliği sayesinde aktivitelerini yürütür.⁶⁴

Kripto para dijital paraların bir çeşidi olarak nitelendirilmektedir. Kripto para alım satım işlemlerinde kullanılan bir çeşit varlık olarak da ifade edilmektedir. Oluşumu kriptografiye dayandığı için güvenilir olduğu düşünülmektedir. Kriptografinin ilk amaçlarından birisi iletişimin güvenli bir şekilde gerçekleşmesini sağlamaktır. Algoritma ve protokoller oluşturup analiz ederek üçüncü taraflarla

⁶⁰ World Bank Group, *Distributed Ledger Technology (DLT) and Blockchain*, FinTech note, No:1., Washington D.C. 2017 s.5.

⁶¹A. Menezes, P. Van Oorschot, ve S. Vanstone, *Handbook of Applied Cryptography*, USA 1996, s.4.

⁶² Wade Trappe ve Lawrence C. Washington. "Introduction to Cryptography with Coding Theory", *Overview of Cryptography and Its Applications*, U.S. 2006, s.9.

⁶³Misha Tsukerman, "The Block Is Hot: A Survey Of The State Of Bitcoin Regulation And Suggestions For The Future", *Berkeley Technology Law Journal*, Vol. 30:385, s.1136.

⁶⁴ Accenture Consulting, *The (R)evolution of Money Blockchain Empowered Digital Currencies*, 2017, s.4.

yapılan görüşmeler sırasında bilginin değiştirilmesi veya kesilmesine olanak tanımamaktadır. Kriptografi temeli matematiğe dayanan birçok disiplinin karışımı ile oluşmaktadır. Kripto paralar dağıtık muhasebe defteri ve blok zincir teknolojisini kullanmaktadır. Ağda gerçekleşen hiçbir işlem faaliyeti hiçbir kontrol mekanizması tarafından kontrol edilememektedir.

Blok zincir ile Bitcoin madenciliği yapanlar, gerçekleştirilen işlemlerin içeriklerini, hesapların tarihi kayıtları ile birlikte karşılaştırma imkânı sunan kronolojik sıralanmış bloklar şeklinde takip edebilmektedir.⁶⁵

Kripto paralar dijital paranın bir çeşidi olmakla birlikte dijital paradan birtakım özellikleri nedeniyle farklılık göstermektedir. Bu özellikler; yapı, anonimlik ve şeffaflık, işlem manipülasyonu ve hukuki yönleri olarak beş başlıkta belirtilmektedir. Dijital paralar ağdaki bir grup insan ve bilgisayarlar tarafından işlemlerin regüle edildiği diğer bir ifadeyle düzenlendiği merkezi bir yapıya sahiptir. Kripto paralar ise topluluğun büyük bir kısmı tarafından işlemlerin regüle edildiği dağıtık bir yapıya sahiptir.

Dijital paralar işlemleri gerçekleştirebilmek için kullanıcı kimliğine ihtiyaç duymaktadır. Kamu otoriteleri tarafından onaylanmış bazı dokümanlar ve işlemi gerçekleştirecek şahsa ait fotoğrafın sisteme yüklenmesi gerekmektedir. Diğer taraftan kripto paralar alım, satım, yatırım veya herhangi bir işlem için bu gereksinimlere ihtiyaç duymamaktadır. Bununla birlikte kripto paraların tam anlamıyla da anonim olmadığı ifade edilmektedir. Herhangi bir adres, isim veya gizli bilgi içermemekle birlikte gönderici ve alıcı adresleri açık olarak bilinmekte ve her bir işlem kayıt altına alınmaktadır. Böylelikle her bir işlemin izi sürülebilmektedir. Dijital paraların şeffaf olmadığı işlem yapılacak cüzdanın adresi seçilememekte ve tüm para transferleri görülemediği de belirtilmektedir. Bu bilgi dijital hesaplar için gizlilik arz etmektedir. Buna karşılık kripto paraların şeffaf olduğu da ifade edilmektedir. Gelir akışları ortak bir zincirde yer aldığı için herkes herhangi bir işlemi herhangi bir zaman diliminde görebilmektedir. Dijital paralar işlemleri gerçekleştirebilmek için merkezi bir otoriteye sahiptir. Herhangi bir şüpheli işlem durumunda örneğin kara para aklama durumunda

⁶⁵ Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.99.

otorite tarafından işlemler durdurulabilmekte veya iptal edilebilmektedir. Kripto paralar topluluk tarafından regüle edilmektedir. Kullanıcıların blok zincir içerisindeki bu çeşit değişiklikleri fark edip onaylaması pek mümkün değildir. Birçok ülke dijital paralarla ilgili bazı yasal çerçeveler oluşturmuşlardır. Örneğin Avrupa Birliği'nin Directive 2009/110/EC kararı veya Amerika Birleşik Devletleri'nde Article 4A of the Uniform Commercial Code kararı bulunmaktadır. Kripto paralar için şu ana kadar herhangi bir ortak yasal düzenleme bulunmamaktadır. Bir çok ülkede kripto paraların yasal statüleri tanımlanmamıştır. Bir grup insanın tüm sistemden sorumlu olduğu merkezi bir sistemde, işlemlerle ilgili bir hata yapıldığında şirkete müracaat edildiği takdirde başarılı bir şekilde geri dönüş alınabilmektedir. Dağıtık bir sistemde bunu yapmak mümkün olmamaktadır. Diğer taraftan merkezi yapı kullanıcılarla ilgili birçok gizli bilgiye erişim sağlamaktadır. Bu bilgi mahkeme talepleri doğrultusunda ilgili kurumlara aktarılabilir. Fakat dağıtık sistemlerde bu işlemleri yapmanın mümkün olmadığı ifade edilmektedir.⁶⁶

Tarihsel olarak baktığımızda kriptografi çoğunlukla askeri, gizli servisler ve istihbarat teşkilatları tarafından gizli bilginin dışarı sızmasını engellemek amacıyla kullanılmıştır. Bu alandaki akademisyenlerin çoğu herhangi bir hükümete veya banka gibi aracı bir kuruma bağlı olmayan bağımsız dijital para biriminin sahip olduğu anonimlik ve serbestiyeti özellikleri nedeniyle dikkat çekici olduğuna inandıkları ifade edilmektedir. Hem yerel hem de uluslararası coğrafik bölgelerde para transferleri resmi düzenlemelere ihtiyaç duymadan kolay ve hızlı bir şekilde gerçekleştirilebilmektedir. ABD'de kriptografinin öncüsü federal kayıtlarda 17 Mart 1975 tarihinde yayınlanan Data Şifreleme Standardı (Data Encryption Standard – DES) ile Horst Fietsel olarak kabul edilmektedir. Fietsel o dönemde IBM'de Lucifer Şifresi olarak bilinen 48-bitlik blok şifreleme sistemi projesinde araştırmacı olarak çalışmaktaydı. Bu proje Lloyds Bankası tarafından ATM işlemlerini şifrelemek amacıyla devreye alınmıştır. 1972 yılında Ulusal Standartlar Bürosu (National Bureau of Standards – NBS) gizli olmayan fakat hassas devlet belgelerini şifreleme için

⁶⁶ Tatiana Revoredo, "A comparative analysis between money, currency, digital money, fiat money, electronic money and cryptocurrencies" 15.09.2018, <https://medium.com/@tatianarevored/a-comparative-analysis-between-money-currency-digital-money-fiat-money-electronic-money-and-36bbcfacea9b> (Erişim: 30.10.2018).

şifreleme standartları ihtiyacını belirlemiştir ve 1973 yılının Mayıs ayında böyle bir sistem için teklif istemiştir. NBS daha sonra Ulusal Güvenlik Ajansı'nın (National Security Agency – NSA) onayı ile IBM'in algoritmasının modifiye edilmiş bir sürümünü seçmiştir. Bu proje Lloyds Bankası tarafından ATM işlemlerini şifrelemek için devreye alınmıştır. Orijinal algoritma Walter Tuchman'ın liderliğindeki bir ekip ve Carl Meyer'in yardımlarıyla 56-bit olacak şekilde güçlendirilmiştir. DES'in yayınlanması akademik çevre ve sivil alanda birçok tartışmaya neden olmuştur. Stanford Üniversitesi'nden Martin Hellman ve Whitfield Diffie gibi bazı akademisyenler orijinal 56-bit blok şifrenin NSA'nın emirleri doğrultusunda NSA'ya Subramanian ve Chino gibi kriptografik sistemlerde arka kapı sağlamak için IBM tarafından değiştirildiğini düşünmüşlerdir. Aynı zamanda 56-bit şifrelemenin güvenliği ile ilgili ortaya çıkan sorular olmuştur. Fakat bunlara rağmen DES çok popüler olmuştur ve sonunda uluslararası şifreleme standardı olarak kabul edilmiştir. Kripto paranın ortaya çıkmasına katkı sağlayan diğer bir gelişmenin ise 1990'lı yıllarda ortaya çıkan "Cypherpunk Hareketi" olduğu belirtilmektedir. Cypherpunk Hareketi, katılımcıları ile sosyal ve politik değişim inşa etmek ve kriptografik tekniklerle güvenliği ve gizliliği artırarak statükoyu yıkmak isteyen eylemci bir hareket olarak ifade edilmektedir. Julian Assange ve kendisinin yayın organı WikiLeaks'in de Cypherpunk Hareketi'nden doğduğu da söylenmektedir.⁶⁷ Cypherpunk grubunun kurucuları Berkeley'den matematikçi Eric Hughes, Intel ilk başkanı olan bilim adamı Timothy May ve SunMicrosystem'in ilk çalışanlarından, Cygnus Support'un kurucularından ve aynı zamanda Elektronik Frontier Vakfı'nın kurucularından olan John Gilmore olduğu belirtilmektedir. Bu üç adamın da zengin ve güçlü özgürlük yanlı bir yol paylaştıkları ifade edilmektedir. Bu grup 1992 yılında San Francisco'da Körfez bölgesinde çalışmalarına başlamıştır. Cypherpunk mail listesini 1992 yılında oluşturmaya başlamışlardır ve bu çalışma iki yıl içerisinde 600 katılımcıya ulaşarak tamamlanmıştır. Kripto paranın ortaya çıkmasına bir diğer büyük katkı ise David Chaum tarafından sağlanmıştır. David Chaum Kaliforniya Berkeley Üniversitesi'nde doktorasını tamamlamış bir kriptolojisttir. David Chaum 1980 yılında doktora öğrencisiyken, gizli haberleşme ve gizli finansal işlemlerle ilgili çok sayıda

⁶⁷ Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.68.

konsept ve method keşfetmiştir. 1981 yılında David Chaum, “İzlenemeyen Elektronik Posta, İade Adresleri ve Dijital Anonimler” adı altında bir makale yayınlamıştır. Açık anahtar kriptografiyi kullanarak e-posta iletişiminde kullanıcının kimliğini ve bunun yanı sıra e-postanın içeriğini gizlemeyi sağlayan bir yöntemi tanımlamıştır. Chaum, seçimlerde seçmenlerin kimliğini açıklamadan tüm oyların doğru bir şekilde sayıldığına doğrulandığı bir kullanımının olduğunu belirtmiştir. Chaum’un kriptografiye dayanan dijital para birimlerinin ortaya çıkmasındaki en büyük katkısının ise e-Cash’i geliştirmesiyle olmuştur. 1990 yılında elektronik para ticari kuruluşu olan DigiCash şirketini kurmuştur. Dünyanın ilk elektronik nakit ödemesi 1 Mayıs 1994 tarihinde gerçekleşmiştir. İşe yarar kripto para girişimlerinin çoğu tüketici tarafından kabul görmekte başarısız olmuştur.⁶⁸

1.7. KRİPTO PARA ÇEŞİTLERİ

1.7.1. Bitcoin

Bitcoin 2008 yılında Satoshi Nakamoto takma adını kullanan bir kişi veya grup⁶⁹ tarafından yayınlanan “*Kullanıcıdan Kullanıcıya Elektronik Nakit Sistemi*” isimli makale⁷⁰ ile ortaya çıkmıştır. 3 Ocak 2009 tarihinde ise Bitcoin yazılımı tüm dünyada açık kaynak kodlu olarak işlevsel hale gelmiştir. Bitcoin 2010 yılına kadar alım satım işlemlerinde kullanılmamıştır. Bu tarihten sonra programcılar, sistemin geliştiricisi Satoshi Nakamoto ile birlikte açık kaynak kodlu Bitcoin yazılımını revize ederek ikinci versiyonunu yayınlamışlardır. İlk Bitcoin işlemi de 21 Mayıs 2010 tarihinde Bitcoin rumuzlu Laszlo Hanyecz tarafından o zamanki karşılığı 41 Dolar olan 10 bin Bitcoin ile pizza siparişi vermesiyle gerçekleştirilmiştir.⁷¹ Florida’da yazılım mühendisi olan Laszlo Hanyecz ayrıca GPU temelli Bitcoin çıkarma işlemini bulan bir yazılımcı olarak da belirtilmektedir.⁷²

⁶⁸ Flamur Bunjaku, ve diğerleri, “Cryptocurrencies – Advantages and Disadvantages”, s.35.

⁶⁹ Dört teknoloji şirketi (Samsung, Toshiba, Nakamichi ve Motorola) tarafından tasarlandığı ve geliştirildiği iddia edilmektedir.

⁷⁰ Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, s.3.

⁷¹ Conrad Barski and Chris Wilmer, *Bitcoin For The Befuddled*, San Francisco 2015, s.112.

⁷² Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sistemde Meydan Okuması; Kriptopara Çağı*, s.117.

2013 yılının Mart ayında Güney Kıbrıs'ta meydana gelen ekonomik kriz sonrası Kıbrıs vatandaşlarının ve Rusların çok yüksek miktardaki varlıklarını Bitcoin'e dönüştürmeleriyle 10 Doların altında bir değere sahipken; Nisan 2013 itibarıyla 200 Doları aşarak yıldızı parlayan Bitcoin, Çin'li zenginlerin de Yuanlarını Bitcoin'e çevirmeye başlamasının ardından, Çin'in önlem alıp 2013 yılının Aralık ayında Bitcoin'i yasaklaması sonrası büyük bir değer kaybetmiştir.⁷³

Ülkesi olmayan, merkezi olmayan, herhangi bir merkez bankası veya resmi kuruluş ile ilişkisi olmayan dolayısıyla hiçbir ülkenin ekonomisinden etkilenmeyen kripto para ve ödeme sistemi olan Bitcoin gün geçtikçe finansal dünya gündemini meşgul etmeye devam etmektedir. Sembölü ₿ kısaltması BTC olarak adlandırılan Bitcoin internet erişimi olan dünyanın herhangi bir yerinden, herhangi bir aracı kuruma ihtiyaç duymadan kripto para transferine imkân sağlamaktadır. Bitcoin kripto para biriminin en küçük değerli birimi bir Bitcoin'in 100 milyonda birine eşittir.⁷⁴ Bitcoin'in en büyük avantajının çifte harcama problemini ortadan kaldırması olduğu ifade edilmektedir.⁷⁵ Çifte harcama kavramı, aynı fonların aynı anda iki alıcıya harcanması durumu olarak ifade edilmektedir ve dijital nakit sisteminin potansiyel bir sorunu olarak belirtilmektedir.⁷⁶

Bitcoin gerçek para ile alınabileceği gibi bir ürün veya hizmetin satılması karşılığında da alınabilmektedir. Ayrıca karmaşık matematiksel formüllerin bilgisayar işlemci gücü ile çözülmesi anlamına gelen madencilik ile de elde edilmektedir. İsteyen herkes istediği donanım ile birlikte ağa katılarak Bitcoin madenciliği yapabilmektedir. Bitcoin ağın nasıl çalışacağını tanımlayıcı kurallardan oluşan bir protokol, bu protokolün uygulandığı bir yazılım projesi ile bilgisayar ağları ve Bitcoin elde etmek için yazılımların çalıştığı donanımlardan oluşmaktadır. Madencilik; Bitcoin ağının yönetilmesinde temel fonksiyon olarak belirtilmektedir. Madenciler de Bitcoin madenciliğinde çok önemli bir yere sahiptir. Madencilik; işlemlerin doğrulanması, çifte harcamanın engellenmesi, işlem ücretlerinin toplanması ve para arzını

⁷³ Nishibe, *The Enigma of Money Gold, Central Banknotes and Bitcoin*, s.50.

⁷⁴ Hanna Halaburda ve Miklos Sarvary, *Beyond Bitcoin The Economics of Digital Currencies*, New York 2016, s.104-108.

⁷⁵ *Bitcoin and Money Laundering, Developments In Banking Law*, 2016-2107, s.161.

⁷⁶ Double Spending Explained, <https://academy.binance.com/en/articles/double-spending-explained> , (Erişim:15.02.2021).

oluşturması olarak tanımlanmaktadır. Her 10 dakikada bir yeni blok üretilmesine imkân sağlayan Bitcoin madenciliği ilk işlevsel hale geldiği 2009 yılında, madencilik işlemi ile bilgisayar sistemleri sayesinde çözüm bulan kullanıcılara ödül olarak 50 Bitcoin vermektedir. Bu ödülün her dört yılda bir yarılanarak 2140 yılında tamamen bitmesi öngörülmektedir ve şuan için verilen ödül ise 12,5 BTC olmuştur. Bu teşvik sistemi yani her dört yılda bir 210.000 blokta Bitcoin arzını yarıya indirmektedir. Bu tabloya göre Bitcoin ilk başlarda yüklü bir miktarda dağıtılmaktaydı. 21 milyon olan toplam adedinin yarısından fazlasının ilk altı yıl içerisinde tamamlanmış olması Bitcoin'e zaman içerisinde nadir bulunma özelliği kazandıracağı ve böylelikle geleneksel para politikasına benzer şekilde bir politika benimsendiği de ifade edilmektedir.⁷⁷ Bitcoin madencisi yeni bir blok bulduğunda yeni Bitcoin ve herhangi bir işlem ücretini de elde etmektedir. Bitcoin madenciliğinde yaygın olarak kullanılan yöntem güçlü ekran kartları ile bunların GPU birimlerini kullanarak Bitcoin elde etme yöntemidir. Madencilik, bilgisayarda özelliği olan bir sayıyı aratıp bilgisayardan bu özel olarak tabir edilen sayıyı buldurma işlemidir. Bunun için belli bir işlem gücü üreten bilgisayarlar ve daha fazla Bitcoin elde etmek için kullanılan CPU⁷⁸, GPU⁷⁹, FPGA⁸⁰, ASIC⁸¹ gibi algoritma çözme ve elektrik kullanımı konusunda birbirinden farklı özelliğe sahip makineler tarafından yapılmaktadır.⁸²

Blok zincir üzerinde kriptografik bir bulmaca çözerek işlemlerin onaylanmasını sağlayan katılımcılar madenci olarak tanımlanmaktadır. Madencilik süreci iş ispatı (PoW) konsensüs mekanizmasına dayanan kripto paralarla ilişkilidir. Bir madenci işlemleri doğrulamak için bilgisayarın işlem gücünü kullanarak ağa destek verir ve yeni coinler ile ödüllendirilir. Bitcoin'in ilk çıktığı yıllar olan 2009 yılında madencilik yöntemiyle Bitcoin elde etmek daha kolay yapılmakta ve yüksek enerji harcayan cihazlara ihtiyaç bulunmamaktaydı. Yıllar geçtikçe daha fazla kullanıcının sisteme dâhil olmasıyla birlikte madencilik zorlaştı ve performansı yüksek cihazlar kullanılmaya başlandı. Bu cihazların kullanımı ile soğutucu cihazların da

⁷⁷ Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.192.

⁷⁸ Merkezi işlem birimi, En gelişmiş özelliklere sahip işlemci türüdür.

⁷⁹ Ekran kartı işlemcisi

⁸⁰ Yüksek Programlamalı İşlemci

⁸¹ Bitcoin algoritmasına göre matematiksel işlemleri yapan cihazlara denir.

⁸² David R. Sterry, *Introduction to Bitcoin Mining, A Guide Gamers, Geeks, and Everyone Else*, 2012, s.10-14.

kullanılması ihtiyacı doğdu. Dolayısıyla madencilik için başlangıçta çok fazla bir maliyet gerekmezken, şu an gün geçtikçe maliyetler hızlı bir şekilde artmaktadır.⁸³ Güçlüğün artmasındaki temel düşüncenin, kısa sürede kripto paraların piyasadaki sayısının artmasının önüne geçmeye çalışmak ve blok oluşturma hızını belli bir seviyede tutabilmek için zorluk seviyesini otomatik olarak ayarlamak şeklinde ifade edilmektedir. Bu işlem blok zincir denilen teknoloji sayesinde gerçekleşmektedir. Sisteme katılan kullanıcı sayısının her geçen gün artması tek başına madencilik yöntemi ile blok oluşturmaya zorlaştırmaktadır. Bu nedenle ortaya çıkan bir kavram olan madencilik havuzu; bir grup madencinin bir araya gelerek blok oluşturma ve kazanılan ödülün o gruptaki madenciler arasında paylaşılması olarak tanımlanmaktadır.

Şekil 1.3: Madencilik İçin Kullanılan ASIC Makineler⁸⁴



Gerçek madenciliğin yanı sıra, bulut madenciliği ile de Bitcoin üretme işlemi gerçekleştirilmektedir. Bulut Madenciliği, Bitcoin üretiminde kullanılan güçlü donanım aygıtlarının sunucular üzerinden belirli şartlar karşılığında kiralanması ile Bitcoin elde etme işlemidir. Gerçek madencilikten en önemli farkı Bitcoin elde etmek için bilgisayara entegre edilen çeşitli donanım aygıtlarının masraflarının

⁸³ Hari Karishnan, Sai Saketh ve Venkata Tej Vaibhav, “Cryptocurrency Mining – Transition to Cloud”, International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, India 2015, s.115.

⁸⁴ Eric Limer, “The World’s Most Powerful Computer Network Is Being Wasted on Bitcoin”, 05.13.2013, <https://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-504503726>, (Erişim: 15.12.2017).

olmamasıdır.⁸⁵ Havalandırma maliyetlerinin düşük ve ucuz elektrik fiyatlarından faydalanmak için soğuk iklime sahip İzlanda, Washington, Utah ve İsveç gibi bölgelerde kurulan bu sunucuların Bitcoin madenciliğini çok kısa bir sürede büyük bir endüstriyel iş koluna dönüştürdüğü ifade edilmektedir.⁸⁶

Şekil 1.4: Bulut Madenciliği Yapan Sunucular⁸⁷



Singapur Ulusal Üniversitesinde görevli bilim adamı Divesh Aggarwal ve meslektaşları tarafından yapılan bir araştırmaya göre; gelecek 10 yıl içerisinde kuantum fiziği yasalarından “Heisenberg Belirsizlik İlkesi” esasına dayandırılarak geliştirilen kuantum bilgisayarların günümüzde kullanılan bilgisayarların bit olarak adlandırılan ve sıfır ve bir sayılarını kullanarak işlem yapması yerine, qubitlerin kullanılarak mevcut bilgisayar sistemlerinden milyonlarca kez daha hızlı işlem gücü ile çalışmasının, hem Bitcoin madenciliği hem de Bitcoin şifreleme algoritmaları için bir tehdit oluşturduğunu ortaya koyduğu belirtilmektedir.⁸⁸

Bitcoin madencilik denilen bir yöntemle 7/24 hiç durmadan ciddi bir elektrik ve enerji tüketimi sonucunda elde edilmektedir. İnsanoğlu harcadığı fiziki bir emeğin

⁸⁵ Karishnan, Saketh ve Vaibhav, “Cryptocurrency Mining – Transition to Cloud”, International Journal of Advanced Computer Science and Applications, s.115.

⁸⁶ Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.201-202.

⁸⁷ Oğuzhan Karakaya, “Cloud Mining Nedir? Bulut Madenciliği Nasıl Yapılır?”, 28.02.2017, <https://oguzhankarakaya.com/cloud-mining-nedir-bulut-madenciligi>, (Erişim: 15.12.2017).

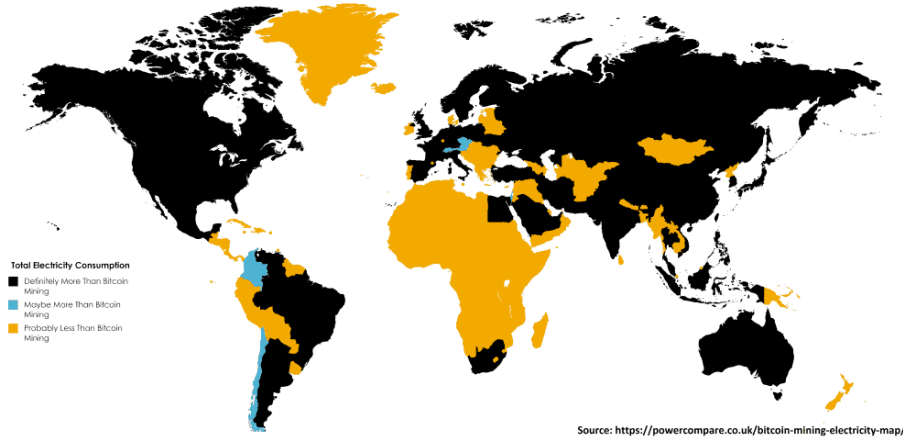
⁸⁸ “Quantum Computers Pose Imminent Threat to Bitcoin Security”, 08.11.2017, <http://www.comp.nus.edu.sg/news/news-media/2176-2017-quantum-computers/>, (Erişim:15.12.2017).

karşılığında para kazanırken, bilgisayarların da madencilik ile işlem gücünü kullanarak Bitcoin elde ettikleri bilinmektedir.

Digiconomist Bitcoin Enerji Tüketim İndeksi'ne göre 2018 yılı sonu itibarıyla Bitcoin madenciliğinin yılda 55,63 ile 73,12 TWh arasında elektrik tüketimi gerçekleştirdiğinin tahmin edildiği belirtilmektedir. Bunun Bitcoin madenciliğinin şu an dünya üzerindeki 175 ila 181 ülkenin tükettiği elektrikten daha fazla olduğu anlamına geldiği de ifade edilmektedir. Bir Bitcoin madenciliği sırasında 94.000 KWh elektrik tüketimi yapıldığının da tahmin edildiği belirtilmektedir. Bitcoin madenciliğinin potansiyel tüketiminin dünya nüfusunun %10'nu teşkil eden 750 milyon elektrik kullanıcısının tüketiminden daha fazla olduğu ifade edilmektedir. 186 milyonluk nüfusu ile en kalabalık nüfusa sahip Nijerya'nın bile dünya çapındaki Bitcoin madenciliğinden daha az elektrik tükettiği de belirtilmektedir. Diğer taraftan 5,2 milyon ile en az nüfus yoğunluğuna sahip ülke konumundaki Norveç'in dünya çapındaki Bitcoin madenciliğinden daha fazla elektrik tüketimi gerçekleştirdiği de vurgulanmaktadır. Bitcoin madenciliğinin tükettiği elektrik miktarının Avustralya'nın %33'ü, Birleşik Krallığı'nın %24'ü, Kanada'nın %14'si ve ABD'nin ise %2'si ne eşdeğer olduğu belirtilmektedir. Dünya üzerindeki 66 ülkede kişi başı elektrik tüketiminin bir Bitcoin işlemi sırasında tüketilen elektrik miktarından daha düşük olduğu belirtilmektedir. Sadece 38 ülkenin hala Bitcoin madenciliğinden daha fazla elektrik tüketimi gerçekleştirdiği ifade edilmektedir.⁸⁹

⁸⁹ "Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018", <https://powercompare.co.uk/bitcoin-mining-electricity-map/> (Erişim: 29.12.2020).

Şekil 1.5: Bitcoin Madenciliğinden Daha Fazla veya Daha Az Elektrik Tüketen Ülkeler

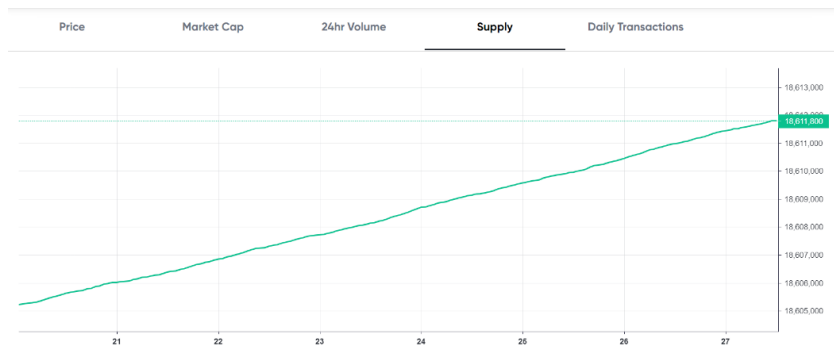


Genesis Mining şirketinde operasyonların başı olan Philip Salter'in yeni doğan bir endüstri için en büyük gelişmelerden biri olarak nitelendirdiği madenciliğin Çin'den Norveç ve İsveç gibi kuzey ülkelerine kaydığını ifade ettiği belirtilmektedir. Batı ülkelerin, şu anda büyük küresel hashrate silahlanma yarışının hüküm sürdüğü Komünist Çin'in aksine daha güvenli ve istikrarlı olduğunun fark edildiği ifade edilmektedir. Bitcoin yatırımcısının daha halka açık hale gelmesi ve daha kritik bir güven istemesi gibi nedenlerden dolayı madencilikte Çin'den İsveç gibi Batılı ülkelere çok önemli stratejik bir kayma gerçekleştiği belirtilmektedir. Salter'in şirketinin Boden tabanlı veri merkezinin karlılığının normalden üç kat daha arttığını ifade ettiği belirtilmektedir. Bitcoin'den uzun yıllar boyunca Çin coin/i olarak bahsedildiğini ve Ripple'ın kurucu ortağı Chris Larsen'in elinde bir kanıt sunmadan ülkenin otoriter hükümetinin blok zincirindeki işlemleri bloke edebileceği ve geri çevirebileceği ile ilgili bir makale yayınladığını belirttiği ifade edilmektedir. Kripto para madenciliğinin en az yüzde 65'inin Çin'de yoğunlaştığı ve Çin hükümetinin bu protokoller üzerinde onları kontrol edebilmek için yönlendirme ve işlemleri etkin bir şekilde bloke etme veya geri çevirebilme imkânına sahip olduğu anlamına geldiği ifade edilmektedir. Ripple şirketinin, ABD Menkul Kıymetler ve Borsa Komisyonu (U.S. Securities and Exchange Commission – SEC) kurumunun bir davasında Bitcoin ve Ethereum'un Çin tarafından kontrol edilen kripto paralar olduğunu iddia ettiği ve bu iddiaların her iki topluluğun üyelerinden sert eleştiriler aldığı da belirtilmektedir. Ayrıca Çin'in madenciler için engel oluşturmaya devam ettiği ve diğer taraftan da madencilik sektöründeki baskın gücünü kaybettiği ifade edilmektedir. Kullanıcıların 2020 yılının

Kasım ayında, coinlerin Çin'in resmi para birimi olan Renminbiye çeviremedikleri için elektrik faturalarını ödemekte zorluk çektikleri belirtilmektedir. 2017 Eylül ayından beri Çin'de kripto para alım satım işlemlerinin yasaklandığı da ifade edilmektedir. İklim değişikliğinin çok önemli siyasi bir konu olmasıyla birlikte güce aç olarak tabir edilen Bitcoin'in karbon ayak izlerinin endişe uyardığı da ayrıca belirtilmektedir. Ekim 2020'de New York Finansal Hizmetler Departmanı'nın kripto para şirketlerinin ilgili riskleri göz önünde bulundurmaları ile ilgili çağrıda bulunduğu ifade edilmektedir. Norveç gibi ülkelerin yeşile dayandığı düşünüldüğünde bu devam eden kaymanın Bitcoin madenciliği ile ilişkilendirilen CO₂ emisyon miktarını azaltacağı da belirtilmektedir.⁹⁰

Bitcoinin değerini Bitcoin piyasasındaki arz talep dengesi ve dolaşımdaki miktarı belirlemektedir. Bitcoin blok zinciri tabanlı dağıtılmış bir dijital muhasebe defteri olarak da tanımlanmaktadır. Satoshi Nakamoto'nun 2008 yılında yayınladığı makaleye göre 2140 yılına kadar 21 milyon adet Bitcoin basımının olacağı belirtilmektedir. Sistemin kendisini bu tarihe kadar zorluk seviyesini artırarak veya azaltarak ayarlayacağı tahmin edilmektedir. Şu an dolaşımda olan Bitcoin sayısı 1 Şubat 2021 itibarıyla 18,6 milyona ulaşmış bulunmaktadır. 2017 yılının başlarında Bitcoin'e olan talep çok hızlı bir şekilde artış göstermiştir ve bu büyüme üstel olarak ifade edilebilir hale gelmiştir. Bu tezin yazıldığı dönemde 1 Şubat 2021 tarihinde Bir Bitcoin'in değeri 33 bin ABD Dolarını geçmiş olup piyasa değeri 626 milyar ABD Dolarına ulaşmıştır.

Şekil 1.6: Dolaşımdaki Bitcoin Sayısı⁹¹



⁹⁰ China Coin No More: Bitcoin Mining Shifting to Sweden and Norway, 27.12.2020, <https://u.today/china-coin-no-more-bitcoin-mining-shifting-to-sweden-and-norway> (Erişim: 28.12.2020).

⁹¹ Money Supply, www.bitcoin.com, (Erişim: 01.02.2021).

Çıktığı ilk yılın son aylarına kadar herhangi bir değer kazanmazken, Mayıs 2010 itibarıyla 1 BTC değeri 0,09 Amerikan Doları olmuştur ve zaman içerisinde çeşitli dalgalanmalar göstererek 1 Şubat 2021 tarihinde 33.667 ABD Doları yani 244.971 TL'ye ulaşarak değer kazanmıştır.

Şekil 1.7: Bitcoin'in ABD Doları Karşısındaki Değeri⁹²



Bitcoin'in Şubat 2021 itibarıyla piyasa değeri 626,69 milyar ABD Dolarına ulaşmış durumdadır.

Şekil 1.8: Bitcoin'in Piyasa Değeri⁹³



Bitcoin çok çeşitli kripto para borsaları aracılığıyla satın alınabilir ve doğrudan fiat para birimine dönüştürülebilmektedir. Bitcoin'in şu an dolaşımda olan tüm kripto para birimleri arasında fiat para birimine dönüştürülebilen en kolay kripto paralardan olduğu belirtilmektedir. Bitcoin aralarında Microsoft¹³⁹, Expedia¹⁴⁰, playboy¹⁴¹, Virgin Galactic¹⁴², LOT Polish Airlines¹⁴³ gibi büyük şirketlerin de olduğu çok sayıda şirket sahibi tarafından meşru bir fon kaynağı olarak görülmektedir. Bu Bitcoin'in bir değişim aracı olarak nitelendirildiğini gösterdiği belirtilmektedir.⁹⁴

⁹² Bitcoin Price, www.bitcoin.com, (Erişim: 01.02.2021).

⁹³ Market Cap, www.bitcoin.com, (Erişim: 01.02.2021).

⁹⁴ European Parliament, *Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion*, July 2018, s.33.

1.7.1.1. Bitcoin'in İşlemlerde Anonim Olmasının Bazı Yöntemleri

Kripto para özelinde Bitcoin'i işlemlerde anonim yapabilmek için birkaç yöntem ifade edilmektedir ve bu yöntemler doküman şeklinde internet sitelerinde de yer almaktadır. Bu yöntemler; Bitcoin Karıştırıcı, ToR kullanmak, VPN kullanmak, işlemler için yeni adresler oluşturmak, Bitcoin'in nakit yoluyla alım satımını gerçekleştirme ve Joinmarket olarak aşağıda açıklanmıştır.

1.7.1.1.1. Bitcoin Karıştırıcı

Bitcoin alım satım işlemleri herkese açık muhasebe defterinde kaydedilmektedir. Herhangi birisi herkese açık Bitcoin adresinden işlemlerin hangi adresten hangi adrese gönderildiğinin izini sürebilmektedir. Bu noktada herhangi bir gizlilik protokolü bulunmamaktadır. Bitcoin Karıştırıcı, kimliğin gizlenmesi için gerekmektedir. Bitcoin Karıştırıcı, bağlantıları ve izlenebilirliği ortadan kaldırmak amacıyla gerçekleştirilen bir çeşit yöntem olarak ifade edilmektedir.

Şekil 1.9: Bitcoin Karıştırıcı

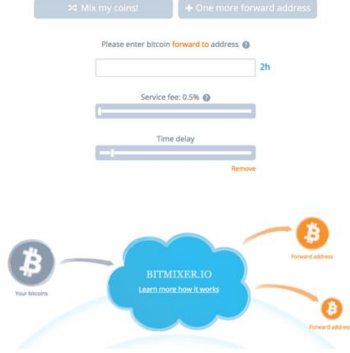


Karıştırıcı, Bitcoin adresleri arasındaki bağlantıyı, geçici adresler oluşturarak veya aynı değerdeki diğer adreslerle coin değişimi yaparak kırmaktadır. Bu işlem blok zincirindeki takip edilebilirliği zorlaştırmaktadır. Bitcoin Karıştırıcı aynı zamanda Bitcoin Aklama, Bitcoin Cambazlığı olarak da ifade edilen ücretli bir hizmet olarak belirtilmektedir. BitBlender ve Bit Mixer internet sitelerinin bir çeşit Bitcoin Karıştırıcı servisi olarak hizmet verdiği ifade edilmektedir.

Şekil 1.10: Bitcoin Mixer

High volume bitcoin mixer

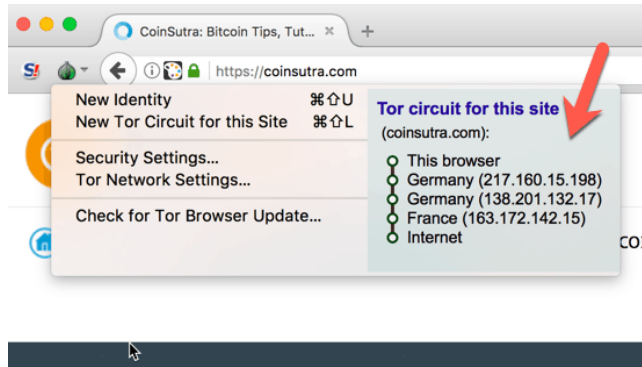
"I believe that any violation of privacy is nothing good." - Lech Walesa



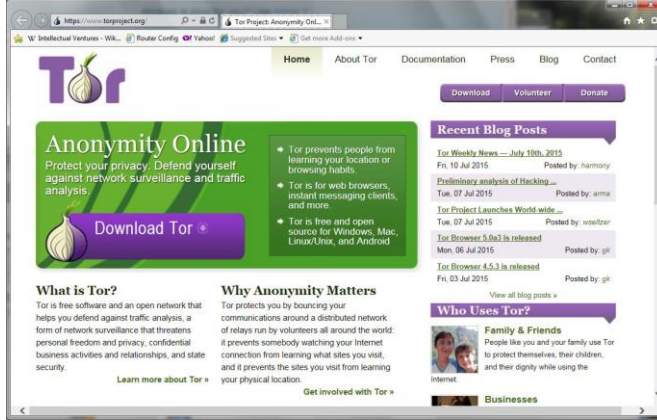
1.7.1.1.2. ToR Kullanmak

ToR tarayıcı kullanarak Bitcoin networküne ulaşılabilir. ToR anonimlik ve gözetimsiz internet kullanımına inanan gönüllü bir topluluk tarafından oluşturulmuştur. ToR düğümleri internet trafiğini şifreleyerek ve son hedefine ulaşmadan önce ToR ağındaki rastgele herhangi bilgisayar düğümlerine yönlendirmektedir. Böylelikle mesajın ve işlemlerin yayınlandığı IP adreslerinin belirlenmesini zorlaştırmaktadır. Bu ücretsiz yazılım anonim iletişime imkân sağlamaktadır. ToR'un aslında ilk ortaya çıkışının ABD istihbarat topluluğu adına geliştirildiği ifade edilmektedir. Fakat şu an suçlular, bilgisayar korsanları, kolluk kuvvetleri tarafından farklı amaçlar doğrultusunda kullanılmaktadır. ToR tarayıcısı kullanarak erişilen internet siteleri işlemleri gerçekleştirmek için Bitcoin ve diğer kripto paraları kullanmaktadırlar.

Şekil 1.11: ToR



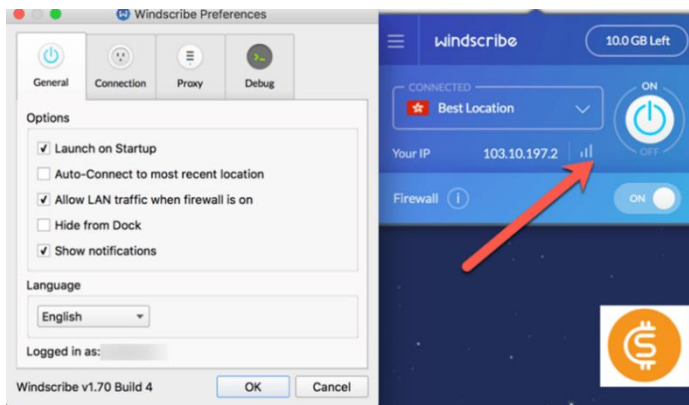
Şekil 1.12: ToR Sayfası



1.7.1.1.3. VPN Kullanarak

Bitcoin işlemlerinin gizliliğini artırmanın başka bir yolu da kayıt tutmayan VPN kullanmak olarak ifade edilmektedir. Kayıt tutmayan VPN internet faaliyetlerinin geçmişini sunucularında saklamayan bir ağıdır. Tüm internet trafiğini şifreler ve son hedefine gelmeden önce seçilen birden çok sunucu yoluyla farklı konumlara yönlendirmektedir. Fakat Bitcoin işlemlerinde gerçekleştirilen faaliyetlerin kaydedilmemesi için VPN servis sağlayıcısına güvenilmesi gerektiği ifade edilmektedir. Windscribe, VPNArea, Mullvad, IPVanish, NordVPN, AirVPN örnek olarak verilmektedir.

Şekil 1.13: VPN



1.7.1.1.4. İşlemler İçin Yeni Adresler Oluşturmak

Popüler Bitcoin cüzdanlarının çoğu HD yani hiyerarşik deterministik⁹⁵ cüzdanlardır. Böylelikle her bir kripto para alımında veya gönderimi sırasında yeni bir adresin türetilmesi ile bakiyenin gizli kalmasının sağlandığı ifade edilmektedir. Herhangi bir sayıda Bitcoin adresi oluşturabilir ve herhangi bir yerden her zaman oluşturduğunuz yeni adresinizle Bitcoin alabilirsiniz. Anonimlik sağlamak için bu iyi bir uygulama olarak ifade edilmektedir.

1.7.1.1.5. Bitcoin Nakit Yoluyla Alım Satımını Gerçekleştirme

Bitcoin işlemlerinin gizliliğini sağlamak için gerçekleştirilen diğer yöntemlerden birisi de yüz yüze nakit olarak gerçekleştirilen Bitcoin alım satımı olarak ifade edilmektedir.

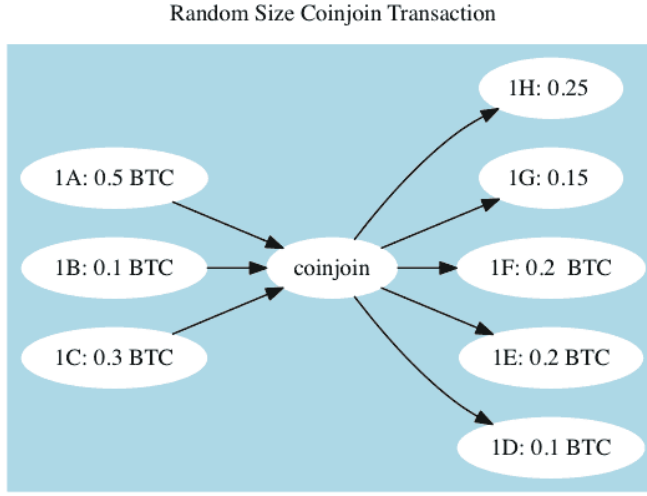
1.7.1.1.6. Joinmarket

JoinMarket'in bir yazılım veya hizmet olmadığı sadece bir tür pazar olarak tanımlandığı ifade edilmektedir. JoinMarket'de piyasa yapıcıları ve alıcıları CoinJoin işlemleri yapmak için bir araya gelmektedir. Bu piyasa doğru zamanda ve doğru yerde doğru miktarda parayı düzenlemektedir. Bu piyasanın alıcıları coinlerini anonimlik özelliği kazandıracak üreticilerine bir miktar ücret ödemektedir. Coin Join mekanizması Escrow veya merkezileştirilmiş taraflar olmadan Bitcoin'e anonimlik özelliği kazandırmaktadır. Bu tür işlemlerde özel anahtarlar her zaman kullanıcıların kontrolündedir. Fakat bu pazarın şu an çok popüler olmadığı ve bu nedenle bu pazarda çok fazla trafik bulunmadığı ifade edilmektedir.⁹⁶

⁹⁵ Laura M, "Kapsamlı Jaxx vs Exodus İncelemesi", 11.10.2020, <https://tr.bitdegree.org/crypto/tutorial/jaxx-vs-exodus>, (Erişim: 01.01.2021).

⁹⁶ "6 Ways To Guarantee Anonymity When Making Bitcoin Transactions", 16.07.2019, (<https://coinsutra.com/anonymous-bitcoin-transactions/>) (Erişim: 20.07.2019).

Şekil 1.14: CoinJoin İşlemleri



1.7.2. Ethereum (ETH)

Diğer bir kripto para olarak geliştirilen Ethereum ilk olarak Vitalik Buterin ve ekibi tarafından Kuzey Amerika Bitcoin Konferansında 30 Temmuz 2015 tarihinde tanıtılmıştır. Ethereum blok zincir veri tabanında özel bir yazılım geliştirilerek merkezi olmayan yazılım protokollerinin geliştirilmesine olanak sağlamaktadır. Geliştiricisi Vitalik Buterin Ethereum’u şu şekilde ifade etmiştir:⁹⁷

“Eğer kripto paralar ile dünyada bulunan değerli kaynakları karşılaştırıyorsak ve Bitcoin’i ALTIN, Litecoin’i GÜMÜŞ olarak kabul ediyorsak, Ethereum PETROL’dür. Çünkü Ethereum’un altında yatan teknoloji dünyanın internet sistemindeki enerji kaynağı olacaktır. Dünyada petrol nasıl birçok sektör ve teknolojide kullanılıyorsa Ethereum teknolojisi için de aynı şey geçerlidir. Bu nedenle biz Ether’i ‘kripto yakıt’ olarak adlandırıyoruz. Ethereum platformunun ihtiyaç duyduğu enerji Ether (ETH) ile sağlanacak.”

Ethereum da işlemlerini gerçekleştirmek için Bitcoin gibi blok zincir teknolojisini kullanmakta fakat birkaç noktada Bitcoin’den farklılık göstermektedir. Ethereum’da işlemler Bitcoin’e göre çok daha hızlı olarak 14-15 saniyede gerçekleşmektedir. Bitcoin’de bu zaman 10 dakikayı bulmaktadır. Bitcoin kripto parasında her geçen zamanda üretilen Bitcoin sayısı azalmakta iken Ethereum’da her yıl sınırsız olarak sabit sayıda yeni paralar yaratılmaktadır. Ethereum, Bitcoin’den farklı olarak maliyet

⁹⁷ “Ethereum Nedir?”, 10.10.2017, <http://blockchain.org.tr/ethereum-nedir/>, (Erişim: 15.12.2017).

işlemleri yöntemine sahiptir. Bitcoin’de ilk önce işlemi doğrulayan madenci en fazla kazanan olurken, Ethereum’da madencinin kazandığı oran zamanla artmaktadır.⁹⁸

Bitcoin ve Ethereum blok zincir teknolojisi ile geliştirilen kripto paralardır. Her iki kripto para her ne kadar aynı teknoloji kullanılarak geliştirilmiş olsalar da farklı sistemlere sahiptirler. Bitcoin kullanıcıdan kullanıcıya şifrelenmiş dağıtık ödeme sistemidir. Tüm işlemler şeffaf ve ağdaki tüm kullanıcılara açık gerçekleşmektedir. Güvenlik konusu Bitcoin için birinci sırada yer almaktadır. Güvenlik konusu dışarıdan veri saklanması olarak değil, oluşturulduktan sonra o verinin fark edilmeden değiştirilemeyeceğini ifade etmektedir. Bitcoin 70’e yakın özel komut ile C++ programlama dilini kullanır. Madencilik Ethereum, Bitcoin gibi sadece ödeme sistemi için değil, yüksek güvenli ve düşük maliyetli akıllı kontratlar gibi farklı amaçlara hizmet etmek için geliştirilmiştir. Ethereum ise esneklik ve işlevselliğinin artırılarak Ethereum sistemi içerisinde farklı şekillerde akıllı kontratların oluşturulmasına imkân sağlamak için tasarlanmıştır. Ethereum Bitcoin’in kullandığı C++ programlama dilinden çok farklı olarak yedi farklı programlama dili kullanılarak geliştirilmiştir. Ethereum, aynı zamanda Bitcoin’den farklı doğrulama (hash) algoritması kullanır. Dolayısıyla Ethereum madenciliği Bitcoin madenciliğinden farklı olarak ETHASH algoritmasını kullanan GPU ile yapılmaktadır.⁹⁹ Hash, kriptografik hash fonksiyonları kullanılarak oluşturulan dijital dosyanın dijital parmak izi olarak tanımlanmaktadır. Bitcoin SHA256 olarak adlandırılan kriptografik hash fonksiyonu kullanmaktadır. SHA256 algoritmasını bir dijital dosya, e-posta, PDF veya bir Netflix filmine uygulandığında numara ve harflerden oluşan tek (eşsiz) bir dizi oluşturmaktadır. Eğer dijital dosyada büyük veya küçük herhangi bir değişiklik yapılırsa sonuçta üretilen hash tamamen farklı olacaktır. SHA256 ve diğer benzer hash fonksiyonlarının en ilginç özelliği herhangi birinin dijital bir dosyanın orijinalliğini kontrol edebilmesi olarak belirtilmektedir.¹⁰⁰

Ethereum 2.0, Ethereum’un bir taraftan güçlü yönlerinin önemine vurgu yaparken diğer taraftan da yinelenen kısıtlamaları ortadan kaldırması için planlanmış mevcut Ethereum blok zincirinin gelişmiş sürümü olarak ifade edilmektedir. Mevcut

⁹⁸ European Parliament, *Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead*, s.13.

⁹⁹ Julianne Harm, Josh Obregon ve John Stubbendick, *Ethereum vs. Bitcoin*, California, s.3.

¹⁰⁰ *Virtual Currencies Mining the Possibilities*, Allen&Overy, 2015, s.4.

Ethereum ağının en çok belgelenen eksikliğinin ölçeklenebilirlik eksikliği olduğunu gören geliştirme ekibinin daha sağlam altyapılar uygulamak ve işlem hızının artırılması için Ethereum 2.0'ı geliştirdiği belirtilmektedir.¹⁰¹

Piyasa değerine göre ikinci en büyük kripto para olarak ifade edilen Ethereum'un beş yıllık tarihinde en önemli güncellemesini gerçekleştirdiği ifade edilmektedir. Ethereum blok zinciri evriminde çok önemli bir gelişmeyi temsil eden ve Eth2 olarak adlandırılan Ethereum 2.0 yolunda önemli bir dönüm noktasının başarıldığı belirtilmektedir. Ethereum'un piyasaya sürülmesinden bu tarafa dünyanın yeni blok zincirleri ve dağıtık diğer bir ifadeyle merkezi olmayan uygulamalar forumundaki yeni teknolojilerin geliştirilmesinde keskin bir yükselişe şahit olduğu ifade edilmektedir. Ethereum platformunun, Dağıtık Finans (DeFi) sistemi içindeki en büyük ve en yenilikçi gelişmelerden bazılarına uzun süredir el üstünde tutulan ve güvenilir temel sağladığı belirtilmektedir. Ethereum ağının popülaritesinin arttıkça ve yaygınlaştıkça ölçeklenebilirlikle ilgili sorunların ortaya çıktığı ve Ethereum 2.0 güncellemesi ile bu sorunların çözülmesi amaçladığı ve blok zincir kapasitesinin 64 kat daha etkin bir şekilde artacağı ifade edilmektedir. Saniyede sadece 30 işlemi destekleyebilen Ethereum 1.0 ağı ile karşılaştırıldığında Ethereum 2.0 ağının saniyede 100 bin işlemi gerçekleştirebildiği belirtilmektedir. Ethereum 2.0 ile ağın kullanım potansiyelinin ve işlevselliğinin üstel olarak artırılmasının hedeflendiği ifade edilmektedir. Ethereum 2.0 güncellemesinin en dikkat çekici yeni özelliklerinden birisinin de Hisse Kanıtı (Proof of Stake) protokolü yani çok sayıda işlemin aynı anda gerçekleştirilebilmesine olanak sağlayan Bölünmüş Zincirler (Shard Chains) ve İşaret Fişegi Zinciri (Beacon Chain) olarak adlandırılan tamamıyla yeni bir blok zincirinin tanıtımını içereceği belirtilmektedir. Bu yeni özelliklerin Ethereum ağındaki hızı, verimliliği ve ölçeklenebilirliği artırarak işlemlerin daha iyi bir şekilde gerçekleşmesini sağlayarak böylelikle mevcut tıkanıklık sorunlarının önlenileceği ifade edilmektedir. Bölünmüş Zincirlerin (Shard Chains) blok zinciri ile benzer özelliklere sahip olduğu fakat bölünmüş zincirde bir blok zincirinin sadece bir bölümünü içerdiği belirtilmektedir. Bölünmüş zincirlerin, düğümlere ağın dilimlerini

¹⁰¹What is Ethereum 2.0? (Release, Roadmap, Phases), 23.11.2020, <https://www.benzinga.com/markets/cryptocurrency/20/11/18489382/what-is-ethereum-2-0-release-roadmap-phases> , (Erişim: 19.01.2021).

yönetmesine imkân sağladığı ifade edilmektedir. Ethereum 2.0 ağının 64 adet bölünmüş zincir oluşturacağı ve böylelikle ağ üzerinde 64 kat daha fazla işlem hacmi sağlanacağını beklendiği belirtilmektedir. İşaret Fişegi Zincirinin (Beacon Chain) Ethereum 2.0 ağının merkezi bir bileşeni olduğu belirtilmektedir. Bu yeni blok zincirinin parçalar arasında bilgi paylaşımına izin verdiği ve ona paralel çalışan bölünmüş zincirleri desteklediği ifade edilmektedir. Ağ üzerindeki ölçeklenebilirliğin geliştirilmesi için parçalar ve Beacon zincirinin gerekli olduğu da belirtilmektedir. Ethereum ağına erişmek için kullanılan düğümlerin her birinin ağda şimdiye kadar gerçekleşen tüm işlemlerin bir kopyasını içerdiği ifade edilmektedir.¹⁰²

1.7.3. Ripple, XRP (XRP)

Bitcoin'in dünya çapındaki başarısının ardından çok sayıda alt coin ortaya çıkmaya başlamıştır ve hala da çıkmaya devam etmektedir. Ripple, Bitcoin gibi alternatif bir kripto para değildir, 2012 yılında kripto para aktarımını tanımlayan bir protokol olarak ortaya çıkmıştır. Açık kaynak kodlu, dağıtık bir protokolle ortaya çıkmış olmasına rağmen, şu anki geliştirilmesi yalnızca Ripple Laboratuvarlarında yapılmaktadır. 100 milyar Ripple ile üretimi sınırlı tutulmuştur.¹⁰³ Blok zincir teknolojisine sahip olmayan bunun yerine global ortak muhasebe defterini kullanan bir kripto para olan Ripple protokolü daha çok büyük bankalar ve iş dünyası gibi kurumsal aktörler tarafından kullanılmaktadır.¹⁰⁴ Son kullanıcıya para transferini gerçekleştirmeye yarayan kendine ait bir algoritması olan ve Google'ın yatırım yaptığı kripto para birimidir.¹⁰⁵ Ripple, geleneksel finansal sistemden farklı olarak dünyanın herhangi bir yerinden, herhangi bir para biriminde, her hangi bir zamanda güvenli işlemlerin yapılmasına olanak sağlayan bir ağ protokolüdür. Ripple'da Bitcoin'den farklı olarak madencilik yapılmamaktadır. Ripple'ın kendine ait bir algoritması bulunmaktadır. Ripple,

¹⁰²What is Ethereum 2.0? Overview, Features and Price Implications, 27.11.2020, <https://www.diginex.com/insights/what-is-ethereum-2-0-overview-features-and-price-implications/> , (Erişim:19.01.2021).

¹⁰³ Frederik Armknecht; Ghassan O. Karame; Avikarsha Mandal; Franck Youssef ve Erik Zenner, *Ripple: Overview and Outlook*, 2015, s.2-3.

¹⁰⁴Garrick Hileman ve Michel Rauchs, *Global Cryptocurrency Benchmarking Study*, University of Cambridge, Cambridge 2017, s.17.

¹⁰⁵ David Meyer, "Google Ventures invests in OpenCoin, the firm behind Bitcoin exchange Ripple", 14.05.2013, <https://gigaom.com/2013/05/14/google-ventures-invests-in-opencoin-the-firm-behind-bitcoin-exchange-ripple/>, (Erişim: 15.12.2017).

Bitcoin'e göre işlemlerin daha kısa sürede ve daha az işlem ücreti ile gerçekleşmesine imkân sağlamaktadır. Ripple'ın geliştirilmesinden sonra Ripple'ın mucitleri XRP kripto parayı da geliştirmişlerdir. XRP, finansal kuruluşların sınır ötesi ödemelerini bankalar gibi günümüzdeki küresel ödeme ağlarından daha hızlı ve daha ucuz gerçekleştirebilmek için geliştirilmiş köprü para birimi olarak nitelendirilmektedir. Ripple'a göre XRP saniyede 1.500'den fazla işlemi gerçekleştirebildiği ifade edilmektedir. Başlangıçta bir girişim olarak geliştirilen Ripple'ın kısa sürede çok sayıda kripto para kullanıcısı tarafından benimsendiği belirtilmektedir. Ripple'ın (XRP) Proof of Work veya Proof of Security tabanlı olmadığı, işlemlerin geçerliliği için kendi özel protokollerinin olduğu ifade edilmektedir.¹⁰⁶ XRP, Ripple ve RippleNet arasındaki farkı anlamak çok önemlidir. XRP, XRP Ledger olarak adlandırılan veritabanı üzerinde RippleNet dijital bir ödeme platformunda çalışan para birimidir. RippleNet ise blok zincirine dayanmayan, dağıtık defter veritabanına dayanan açık kaynak kodlu XRP Ledger olarak ifade edilmektedir. RippleNet ödeme platformu, gerçek zamanlı olarak küresel çapta para transferlerine olanak sağlayan bir platform olarak belirtilmektedir.¹⁰⁷

Bitcoin'in sahip olduğu şeffaflık ve yarı anonim özellikleri nedeniyle işlemlerin ağdaki herkes tarafından izlenebilir olması gizlilik içeren kripto para kavramını ortaya çıkardığını ifade etmek mümkündür. Gizlilik içeren kripto paralar blok zincir teknolojisi kullanılarak dağıtık bir şekilde kişiler arası işlem aktarımına gizlilik ve anonimliği sağlayarak imkân tanımaktadır. Tam anonimlik sağlayan kripto paraların faaliyetlerini gizlilik içinde yürütmek isteyen kripto para kullanıcıları için daha cazip hale geldiği ve bu kripto paralara yönelimin giderek arttığı söylenebilmektedir. Gizlilik içeren kripto paraların doğası gereği sahip oldukları tam anonimlik özelliğinin kara para aklama ve yasa dışı faaliyetleri daha ulaşılabilir kılması ve ekonomi güvenliğine bir tehdit oluşturabilmesi ihtimaliyle hükümetlerin bu kripto paralara daha temkinli yaklaşma zorunluluğunu getireceğini ifade etmek mümkündür. Kripto para ekosisteminde çok sayıda gizlilik içeren kripto para

¹⁰⁶ European Parliament, *Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion*, July 2018, s.35.

¹⁰⁷ <https://coinmarketcap.com/tr/currencies/xrp/> (Erişim:15.02.2021).

geliştirilmiştir. Yaygın olarak bilinen ve kullanılan gizlilik içeren kripto para çeşitlerinden birkaç tanesi aşağıda özetlenmeye çalışılmıştır.

1.7.4. Monero (XMR)

Bitcoin'den sonra geliştirilen bir diğer kripto para olan Monero, Bitcoin'den farklı olarak herkese açık bir işlem defteri kullanmaz, işlemlerinin tamamen gizli olduğunu iddia etmektedir. CryptoNote protokolünün uyarlanmasına dayanarak tek kerelik imza ve gizli adresleri kullanarak böylece blok zincirini opak haline getirdiği iddia edilmektedir. Bununla birlikte geliştiriciler işlemlerde yer alan IP adreslerini gizlemek için de Invisible Internet Project (I2P) entegrasyonu üzerinde çalışmalarını sürdürmektedir. Gizlilik iddiaları göz önüne alındığında bu ödeme yapısının çalınan verilerden veya usulsüz işlemlerden DDoS saldırılarına kadar veya veri çalkalama programları için kullanıldığını seyredeceğiz. Ağustos 2016 yılında karanlık internet pazarlarından olan AlphaBay ve Oasis Monero'yu ödeme kaynağı olarak desteklemeye başlayacaklarını duyurmuşlardır. Bir sonraki ay da Monero'nun değeri %669'luk bir artış göstermiştir. Monero'nun pazar değeri 2016 yılında 5 Milyon ABD Dolarından 185 Milyon ABD Dolarına ulaşmıştır. Bununla birlikte Monero, Massive Multiplayer Online Role Paying Game CryptoKingdom oyun piyasasına da dâhil edilmiş olup artan karanlık internet ve clearnet¹⁰⁸ kumar konsorsiyumlarında kabul edilmiştir.¹⁰⁹

Monero (XMR) 2014 yılının Nisan ayında kamuoyuna duyurulan “özel ve sansüre dayanıklı işlemlere odaklanan” açık kaynak kodlu, P2P prensibine dayanan ve CryptoNote PoW algoritması olarak bilinen kripto para olarak tanımlanmaktadır. Monero kullanıcılarına işlemlerini özellikle tam gizlilik içerisinde gerçekleştirmesine imkân sağlamak amacıyla geliştirilmiştir. Monero özellikle hem gönderim hem de alım adreslerini ve bunun yanı sıra işlem tutarlarını korumak amacıyla kriptografiyi kullanmaktadır. Monero (XMR) tamamen geri ödenebilir olarak karakterize edilmektedir. Bunun anlamı; iki Monero birimi her zaman karşılıklı olarak yer değiştirebildiği ve önceki işlemlerde birleşmeleri nedeniyle satıcılar veya borsalar

¹⁰⁸ Halka açık internete atıfta bulunan bir terimdir.

¹⁰⁹ Benjamin Brown, “2016 State of the Dark Web”, Akamai, Threat Advisory, s.6.

tarafından belirli Monero birimlerinin kara listeye alınmasının mümkün olamayacağı şeklinde ifade edilmektedir. Bitcoin ve Litecoin gibi karşılanabilir olmayan kripto paralar teorik olarak kara listeye karşı kolay etkilenmektedir. Eğer geçmişte yasa dışı faaliyetlerde kullanılmışsa bu bilgi sonsuza dek blok zinciri içerisinde yer alacaktır. Monero'da Bitcoin gibi izinsiz bir blok zinciri üzerinde çalışmaktadır. Herhangi bir merkezi yönetici tarafından onaylanmasına gerek kalmadan ağa katılabilme imkânına sahiptir. Monero çok fazla sayıda bulunan kripto para borsaları üzerinden doğrudan fiat para birimlerine dönüştürülebilmektedir. Tamamen şeffaf özellikte olan Bitcoin ve Ethereum blok zinciri gibi işlemler herhangi biri tarafından her zaman açık bir şekilde doğrulanabilmekte ve izlenebilmektedir. Her ne kadar zor olsa da uygulamada bu tür işlemler için gönderim ve alım adresleri bir kişinin gerçek kimliği ile ilişkilendirilebilmektedir. Ama Monero'da bu durum biraz farklıdır ve Monero kendisini güvenli, gizli ve izlenemeyen bir kripto para olarak konumlandırmaktadır. Monero bu yüksek standarttaki anonimliğini Ring Confidential Transactions (RingCT) ve gizli adresler olarak adlandırılan iki teknikle sağlamaktadır. RingCT, kripto topluluğunda gizli işlemler kavramı olarak ifade edilen teknik ile halka imza tekniklerinin birleşiminden oluşmaktadır. Halka imzaları, bir kullanıcının hesap anahtarlarını Monero'nun blok zincirinden elde edilen halka açık anahtarlarından birleştirerek dışarıdan gözlemcilerin imza ile kullanıcıyı ilişkilendiremeyeceği anlamına gelmektedir. Gizli adreslerle birlikte Monero kullanıcılarının hem gönderici hem de alıcıların kimliğini gizlemeye izin vermektedir. Gizli işlemler her bir işlemin miktarını da gizleyerek ek bir gizlilik sağlamaktadır. Gerçek sayıları açığa çıkarmadan girdi miktarlarının çıktı miktarları toplamı ile aynı olduğuna dair kriptografik kanıt içermektedir. RingCT'ye ek olarak Monero aynı zamanda gizli adreslemeyi de kullanmaktadır. Gizli adresler alıcı adına gönderen tarafından her bir işlem için rastgele oluşturulmaktadır. Alıcıya gönderilen tüm ödemeler gönderici ve alıcı adresleri arasında blok zinciri üzerinde bir ilişki oluşturmamasını garanti etmek için bu adresler aracılığıyla yönlendirilmektedir.¹¹⁰

¹¹⁰ European Parliament, *Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion*, July 2018, s.45-46.

1.7.5. Dash (DASH)

Önceleri Darkcoin olarak bilinen Dash, açık kaynak kodlu P2P gizlilik merkezli olan bir kripto para olarak tanımlanmaktadır. İlk olarak X11 Proof of Work (PoW) algoritmasına dayalı olarak 2014 yılının Ocak ayında ortaya çıkmıştır. Dash'i diğer kripto paralardan ayıran ve farklı kılan şey Dash'in iki katmanlı ağına sahip olmasıdır. 'Masternodes' olarak adlandırılan Dash'in blok zinciri güvenlidir ve bununla birlikte iş ispatı madenciler tarafından yapılmaktadır. Masternode, Dash ağına bağlı bir sunucudur ve Dash'in anonimliği ve anlık işlem özellikleri ile ilgili kavramlar olan PrivateSend ve InstantSend ile ilgili belirli görevleri yerine getirmek için minimum düzeyde performans ve işlevsellik garanti eder. Geleneksel kripto paralar ile yapılan işlemler çok zaman alabilmektedir. Bunun nedeni işlemlerin geri döndürülemez ve aynı zamanda çift ödeme durumlarının yaşanmaması için yeterli bloğun geçmesi gerektiğidir. Dash masternode özelliğini kullanarak bu sorunu çözmektedir. Dash'in kredi kartları gibi nerdeyse anlık işlem sistemleri ile rekabet ettiği ifade edilmektedir. Dash de Monero gibi izinsiz bir blok zincirinde çalışmaktadır. Herhangi biri merkezi bir yönetici tarafından onaylanmasına gerek duyulmadan ağına katılabilmektedir. Dash doğrudan çeşitli kripto para borsaları aracılığıyla fiat para birimlerine dönüştürülebilmektedir. Bitcoin'in blok zinciri gibi Dash'in blok zinciri de default olarak şeffaftır yani işlemler her zaman açık bir şekilde doğrulanabilir ve blok zincirinde izlenebilir. Dash ayrıca kullanıcılarına gerçek finansal gizlilik sağlamak için PrivateSend olarak adlandırılan bir özelliği kullanma seçeneği sunmaktadır. PrivateSend karıştırma olarak bilinen bir yöntemle kullanıcılarının fonlarının kaynağını gizlemektedir.¹¹¹

1.7.6. Verge (XVG)

Verge, Tor ve I2P ağı katmanlarını kullanarak işlem yapan katılımcıların konumu ve IP adreslerini gizleyerek tamamıyla anonim işlemler sunan açık kaynak kodlu, merkezi olmayan bir kripto para olarak tanımlanmaktadır. Verge'in XVG sembolü ile önde gelen kripto para borsalarında işlem gördüğü de belirtilmektedir. 2014 yılında

¹¹¹ European Parliament, *Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion*, July 2018, s.48.

DogeCoinDark adı altında ortaya çıkan Verge'nin 2016 yılında Verge adı altında yeniden isimlendirildiği ifade edilmektedir. Verge'nin kullanıcılarının IP adreslerini gizleyerek işlemlerin tamamen izlenemez olmasını sağlayarak anonimlik üzerine odaklandığı belirtilmektedir. Verge kurucularının Bitcoin gibi yaygın kripto paraların katılımcıların tam anonimliğini korumada genellikle zorlukla karşılaştığını düşündükleri için, bu zorlukları ortadan kaldıracak gizlilik içeren bir kripto para geliştirdikleri ifade edilmektedir. Verge cüzdanlarında yerleşik olarak ToR entegrasyonunun bulunduğu ve ekstra güvenlik seviyesinin de eklenerek SSL şifreleme algoritması ile desteklendiği belirtilmektedir. Verge kripto paranın Monero veya Dash gibi büyük ölçüde kriptografiye dayanmadığı bunun yerine kullanıcılarının kimliklerini korumak için ToR ve I2P ağ teknolojisine güvendiği ifade edilmektedir. Verge'nin kurucularının katılımcıların işlemlerini doğrulamak için açık bir kayıt defterinin zorunlu olduğunu ve diğer katılımcıların blok zincirinde meydana gelen tüm gelişmelerin doğrulanması için katılımcıların kimliklerine ihtiyaç duymadığını da ifade ettikleri belirtilmektedir.¹¹² Verge blok zincirinin açık kaynak kodlu olduğu ve herhangi birisinin önerilerde bulunup Verge'e katkı sağlayabileceği de ifade edilmektedir. XVG sembolü ile bilinen Verge'nin maksimum arzının toplamda 16,5 milyar ile sınırlı olduğu da belirtilmektedir. Verge ile işlemlerin 30 saniyede gerçekleştiği de ifade edilmektedir. Verge kripto paranın bir diğer önemli sayılabilecek özelliğinin ise sahip olduğu Scrypt, X17, Lyra2rev2, Myr-groestl ve Blake2s olan beş madencilik algoritması olduğu belirtilmektedir. Blok zincirinin olmazsa olmazı olarak tabir edilen ve işlemlerin doğrulanması için gereken madencilik işleminin Bitcoin'in gerektirdiği çok pahalı donanımların yerine Verge kripto paranın CPU, GPU veya ASIC gibi herkesin temin edebileceği ekipmanları kullanarak yapabileceği ifade edilmektedir. Verge ile gerçekleştirilen işlemlerde ekstra gizlilik için Bitcoin'den farklı olarak Wraith protokolünün kullanıldığı belirtilmektedir. Wraith protokolünün başarılı olduğu takdirde Verge kripto paranın da değerinin artmaya devam edebileceği ifade edilmektedir. Verge'nin ayrıca Rootstock adı verilen ve Verge için gerçek bir başarı olabilecek bir gelişme olan Verge blok zincirinin akıllı kontratları işlemesine

¹¹² Ake Frankenfield, "Verge XVG (Cryptocurrency)", 05.01.2020, <https://www.investopedia.com/terms/v/verge-xvg-cryptocurrency.asp> (Erişim:19.01.2021).

izin veren bir proje üzerinde çalıştığı da belirtilmektedir. XVG'nin yalnızca özel anahtarlara erişimi olmayan birkaç cüzdan ile uyumlu olduğu ifade edilmektedir.¹¹³

1.7.7. ZCash (ZEC)

ZCash'in 2016 yılının Ekim ayında Zooko Wilcox tarafından geliştirildiği ifade edilmektedir. Wilcox'un insanların anonim olarak birbirlerine para gönderip almasına izin veren bir blok zinciri geliştirmek için yola çıktığı belirtilmektedir. Bu düşüncesini gerçekleştirmek için de Bitcoin'in orijinal kodundan bir çatal oluşturduğu ve böylece Bitcoin'den sadece daha özel değil aynı zamanda daha hızlı özelliklere sahip değişikliklerle bir kripto para ortaya çıkardığı ifade edilmektedir. ZCash'in kripto para efsanesi olarak tabir edilen Roger Ver'den ve eski bankacı olan Barry Silbert'ten özel yatırım aldığı da belirtilmektedir. Bitcoin gibi maksimum arzının 21 milyon olacağı ve bu miktara 2032 yılında ulaşılabilirliğinin öngörüldüğü de ifade edilmektedir. Bununla birlikte ZCash blok zincirinin işlemleri Bitcoin'e göre daha hızlı işleyebileceği ve aynı zamanda daha ölçeklenebilir olduğu belirtilmektedir. Ölçeklenebilirlik, bir blok zincirinin birden çok işlemi aynı anda işleyebileceği anlamına gelmesi bakımından önemli olduğu ifade edilmektedir. ZCash'in de diğer gizlilik içeren kripto paralarda olduğu en temel özelliğinin göndericisi ve alıcısının kimliklerini gizleyebilmesi özelliği olduğu vurgulanmaktadır. ZCash işlemlerinde görülebilecek olan tek bilginin işlemin tarihi ve saati olduğu da belirtilmektedir. Bitcoin gibi ZCash'in de merkezi olmayan bir yapısının olduğu ve blok zincirindeki işlemlerin bir zaman ve elektrik gücü karşılığında ZCash coinleri kazanan madenciler tarafından sürdürüldüğü ifade edilmektedir.¹¹⁴

1.7.8. Tether (USDT)

Tether'in 2014 yılının Temmuz ayında RealCoin adıyla ilk olarak piyasaya sürüldüğü ve Kasım ayında ise fiat para biriminin rezerv tutarlarının korunmasından sorumlu

¹¹³ Aaron S., "Verge Cryptocurrency: What is Verge Coin?" 04.01.2021, <https://www.bitdegree.org/crypto/verge-coin>, (Erişim: 19.01.2021).

¹¹⁴ Laura M., "What Is ZCash? The Complete ZCash Review", 11.01.2021, <https://www.bitdegree.org/crypto/what-is-zcash>, (Erişim: 19.01.2021).

olan Honkong merkezli Tether Limited şirketi tarafından yeniden markalanarak Tether ismini aldığı ve 2015 yılının Şubat ayında ise işlem görmeye başladığı belirtilmektedir. Tether dolaşımdaki kripto paralarının belirlenmiş bir banka hesabında tutulan Dolar, Avro veya Japon yeni gibi geleneksel fiat para birimleri ile eşdeğer miktarda desteklenen blok zinciri tabanlı Omni Layer protokolü ile geliştirilen bir kripto para olarak tanımlandığı ifade edilmektedir. Tether ağının yerel tokenleri olan Tether tokenlerinin USDT sembolü altında işlem gördüğü ifade edilmektedir. Tether'in Bitcoin ve Ethereum gibi diğer yaygın kripto paralarda gözlemlenen geniş dalgalanmaların aksine kripto para değerlemelerini sabit tutmayı amaçlayan yeni bir istikrarlı kripto para birimi olarak ortaya çıktığı belirtilmektedir. Tether'in istikrarlı kripto para olması özelliğinin spekülasyon yatırımlar için bir araç olarak kullanılmasının yerine bir değişim aracı ve değer deposu olarak kullanılmasına imkan sağladığı ifade edilmektedir. Tether'in özellikle itibari para birimleri ve kripto paralar arasında gerekli köprüyü kurmak ve kullanıcılara istikrar, şeffaflık ve düşük işlem ücretleri sunmak için tasarlandığı belirtilmektedir. Üreticisi Tether Limited şirketinin dolaşımdaki her bir Tether'in değerinin 1 ABD Doları değerinde olduğunu ifade ettiği belirtilmektedir. İstikrarlı para kategorisinde anılan Tether'in ihraç edilmesiyle Tether Limited şirketinin hizmet şartları uyarınca Bitcoin veya diğer herhangi bir kripto paralar gibi fiat para birimlerine çevrilebildiği, aktarılabilirdiği, depolanabildiği ve harcanabildiği de ifade edilmektedir. Rezerv üzerindeki fiat para biriminin kripto paranın sahip olduğu özellikleri kazandığı ve değerinin de sürekli olarak fiat para birimine bağlı olduğu belirtilmektedir. Tether'in daha az gelişmiş/test edilmiş alt coin blok zinciri yerine Bitcoin blok zinciri üzerinde yer aldığı da ayrıca ifade edilmektedir. Tether'in Bitcoin gibi uçtan uca, yarı anonim, dağıtık ve kriptografik olarak güvenli bir ortamda kullanılabildiği belirtilmektedir. Tether'in ayrıca Bitcoin veya diğer kripto paralar kadar kolay bir şekilde borsalara ve cüzdanlara entegre edilebildiği de ifade edilmektedir.¹¹⁵

2019 yılının Nisan ayında New York Başsavcısı (New York Attorney General – NYAG), Tether'i kripto para borsası Bifinex'in 850 milyon ABD Dolarlık zararını

¹¹⁵ Ake Frankenfield, "Tether (USDT)", 25.06.2019, <https://www.investopedia.com/terms/t/tether-usdt.asp#:~:text=Tether%20is%20a%20blockchain%2Dbased,trade%20under%20the%20USDT%20symbol>. (Erişim: 19.01.2021).

örtbas etmek ile suçladığı belirtilmektedir. Tether bu suçlamayı kötü niyet ve yanlış iddialar olarak değerlendirdiği ifade edilmektedir. New York Başsavcısının ayrıca Bitfinex ve Tether'in ana şirketi olan iFinex'e de dava açtığı ifade edilmektedir. Yargıç Joel Cohen'in Mayıs 2019'daki ihtiyati tedbir sırasında davanın devam etmesi veya reddedilmesi konusunda nihai bir karar vermeye hazır olmadığı için süreyi 90 gün daha uzattığı belirtilmektedir. Ağustos 2019'da New York Başsavcısı'nın Bitfinex ve Tether'in 850 milyon ABD Dolarlık zararı örtbas etmesinin dışında Bitfinex ve Tether'in New York müşterilerine iddia ettiklerinden daha uzun süre hizmet ettiği iddiasında bulunarak başka bir delil sunduğu da ifade edilmektedir. NYAG daha sonra iFinex'in hareketini "yasal bir soruşturmayı engellemek için uygunsuz bir girişim" olarak ifade ettiği belirtilmektedir. Yargıç Cohen'in Tether ve Bitfinex'in finansal ilişkilerini açıklayan belgeleri hazırlaması gerektiği ile ilgili karar vermesinin ardından Eylül 2020'de davanın seyrinin ilginç bir hal aldığı ifade edilmektedir. 9 Aralık 2020 tarihinde Başsavcı Letitia James'in süre uzatımının 15 Ocak'a ertelenmesini talep eden bir belge sunduğu belirtilmektedir. iFinex'in USDT ve Bitcoin le ilgili Bitfinex üzerindeki faaliyetlerini açıklamasının yanı sıra Tether'in USDT stable coinlerinin ihracı ve itfa işlemlerini detaylandıran bir belge hazırlaması gerektiği de ifade edilmektedir.¹¹⁶ Nisan 2019'da New York Başsavcısı Letitia James'in Tether Limited'in ana şirketi ve Kripto para borsası Bitfinex operatörü olan iFinex'i 850 milyon Dolarlık müşterek ve kurumsal fonların yatırımcılardan gizlenmesi konusunda suçladığı ifade edilmektedir. Mahkeme kayıtlarının bu fonların Kripto Capital Corp. adlı Panama kuruluşuna müşterilerinin para çekme taleplerini yerine getirmek için herhangi bir sözleşme veya anlaşma olmaksızın verildiğini söylediği belirtilmektedir. Bitfinex'in paranın kaybolduktan sonra oluşan boşluğu gizlemek için Tether'in nakit rezervlerinden en az 700 Milyon ABD Doları aldığının iddia edildiği ifade edilmektedir. Şirketlerin yaptıkları açıklamada dosyaların kötü niyetle yazıldığı ve yanlış iddialarla dolu olduğunu söyledikleri belirtilmektedir. Aksine Kripto Capital'in tutarlarının kaybolmadığını aslında ele geçirildiği ve korunduğu bilgisinin taraflarına

¹¹⁶ Bhushan Akolkar and Sunil Sharma, "Tether (USDT) Conspiracy Tosses Again As We Arrive at The D-Day of January 15", 15.01.2021, <https://coingape.com/tether-usdt-conspiracy-tosses-again-as-we-arrive-at-the-d-day-of-january-15/>, (Erişim: 19.01.2021).

bildirildiği ifade edilmektedir.¹¹⁷ Bitfinex ve Tether, Kripto Capital'in banka hesaplarında çok sayıda yabancı hükümet tarafından uygulanan bir dizi varlık dondurulması şeklinde paranın bloke olduğunu iddia ettikleri de ayrıca ifade edilmektedir. Kripto Capital'in CEO'sunun 2019 yılında dolandırıcılıkla suçlandığı ve şirket başkanının uyuşturucu ve kara para aklama suçlamalarıyla Polonya'ya iade edildiği de belirtilmektedir. Dikkate değer bir Kripto Capital operatörü olan Reginald Fowler'ın ise dijital varlık tüccarları için lisanssız para aktarımı işini yürütmekle suçlandığı ifade edilmektedir.¹¹⁸

1.7.9. Binance USD (BUSD)

Fiyat istikrarına dayalı olarak istikrarlı coinlerin işlemlerde, ödemelerde, takas durumlarında ve merkezi olmayan finasta (DeFi) çok önemli rol oynadığı ifade edilmektedir.¹¹⁹ Tether'in dışında 5 Eylül 2019 tarihinde piyasaya sürülen Binance USD'nin (BUSD) Doların istikrarını blok zinciri teknolojisi ile birleştirmek olduğu belirtilmektedir. Binance USD (BUSD) New York Eyaleti Finansal Hizmetler Departmanı (New York State Department of Financial Services – NYDFS) tarafından onaylanan ve düzenlenen FDIC sigortalı ABD bankalarında tutulan ABD Doları ile %100 desteklenen Binance ve Paxos ile ortaklaşa çıkarılan istikrarlı coin olarak tanımlanmaktadır. BUSD'un en üst düzeyde müşteri korumasını sağladığı da ayrıca belirtilmektedir. BUSD, ERC-20 olarak BEP-2'yi destekleyen (Binance blok zinciri temelli bir kripto para) dijital fiat para birimi olarak ifade edilmektedir.¹²⁰

1.7.10. USD Coin (USDC)

USD Coin'in (USDC) Circle ve Coinbase arasında bir ortaklık olan Center konsorsiyumu tarafından geliştirildiği ifade edilmektedir. Teknoloji ve yönetim çevresinin Center tarafından geliştirildiği belirtilirken, ilk ticari ihraççılarının Circle

¹¹⁷ Ake Frankenfield, "Tether (USDT)", 25.06.2019, <https://www.investopedia.com/terms/t/tether-usdt.asp#:~:text=Tether%20is%20a%20blockchain%2Dbased,trade%20under%20the%20USDT%20symbol>. (Erişim: 19.01.2021).

¹¹⁸ Jordan Atkins, "Crypto Crime Cartel: The end is nigh for Tether", 15.01.2021, <https://coingeek.com/crypto-crime-cartel-the-end-is-nigh-for-tether/>, (Erişim: 19.01.2021).

¹¹⁹ Binance USD, <https://crypto.com/price/binance-usd>, (Erişim:20.01.2021).

¹²⁰ What is Binance USD (BUSD)?, <https://www.paxos.com/busd/>, (Erişim:20.01.2021).

ve Coinbase olduğu vurgulanmaktadır. USDC 26 Eylül 2018 tarihinde Circle ve Coinbase işbirliği ile piyasaya sürülen, fiyatı ABD Dolarına sabitlenmiş bir istikrarlı coin olarak tanımlanmaktadır. USDC'nin USD destekli diğer kripto paralara (ör. Tether (USDT)) alternatif olduğu da belirtilmektedir. USD Coin, ABD Dolarını tokene çevirmek, internet ve halka açık blok zinciri üzerinde kullanımını kolaylaştırmak için bir hizmet olarak geliştirildiği ifade edilmektedir. USDC tokenlerinin herhangi bir zamanda tekrar USD'ye çevrilebileceği de belirtilmektedir. USDC tokenlerinin ihraç ve itfa işlemlerinin ERC-20 (Ethereum ağında bir protokol standardı) akıllı kontratlar ile sağlandığı da ayrıca ifade edilmektedir. USDC'nin de diğer istikrarlı coinler gibi kripto paralarda ihtiyaç duyulan istikrarı sağladığı belirtilmektedir. Circle şirketinin resmi bir Para Transferi Kuruluşu olarak Jeremy Allaire ve Sean Neville girişimcileri tarafından 2013 yılında kurulduğu ifade edilmektedir. Para Transferi Kuruluşlarının ABD para hizmetleri işletmeleri olduğu ve bu nedenle federal yasalara ve düzenlemelere uymakla yükümlü oldukları belirtilmektedir. USDC'nin ihraç edilmeden önce eşdeğer miktardaki USD'nin Circle şirketinin akredite ortaklarının birinde olduğu da ifade edilmektedir. Bu nedenle tüm USDC tokenlerinin düzenlendiği, şeffaf olduğu ve doğrulanabildiği de vurgulanmaktadır.¹²¹

1.7.11. İlk Kripto Para Arzı; ICO (Initial Coin Offerings)

Kripto paranın ortaya çıkmasıyla sıklıkla kullanılan kavramlardan biri olan ilk kripto para arzı (ICO), bir şirketin halka genellikle büyük kripto para veya fiat para karşılığında önceden tanımlanmış sayıda dijital token (dijital varlık) satması anlamına gelen bir terim olarak belirtilmektedir. ICO'lar dünya genelinde yargılama yetkisine dayanarak güvenlik, hizmet veya dijital para içerecek şekilde farklı formlarda değişken bir şekilde düzenlenmiştir. ICO'ların artan bir şekilde günümüzde girişim sermayesi ve özel sermaye şirketleri ve bankaları tarafından gerçekleştirilen klasik borç/sermaye finansmanına alternatif olduğu ifade edilmektedir.¹²² ICO'nun girişimcilik finansmanı açısından önemli bir yenilik olduğu düşünülmektedir. Bir ICO'da blok zinciri tabanlı girişim token olarak adlandırılan kriptografik olarak güvenli dijital varlıkları satarak

¹²¹ USD Coin (USDC), <https://cryptonews.com/coins/usd-coin/> , (Erişim:20.01.2021).

¹²² Daniel Diemers, Henri Arslanian, Grainne McNamara, Günther Dobruaz ve Lukas Wohlgemuth, "Initial Coin Offerings A Strategic Perspective", pwc, June 2018, s.2.

sermayesini artırmaktadır. Bu girişimler genellikle geleneksel olarak melek veya risk sermayesi tarafından finanse edilen start-uplara (yeni girişim) benzemektedir.¹²³ ICO'lar esasında 2009 yılında Bitcoin'in geliştirilmesiyle ortaya çıkan büyük blok zincir fenomeninin türevleri olarak ifade edilmektedir.¹²⁴

1.8. BLOK ZİNCİR TEKNOLOJİSİ

Blok zincir teknolojisi internet ortamında kişiler arasında yüksek güvenli bir şekilde para transferi yapılmasına imkân sağlamaktadır. Bitcoin, blok zincir teknolojisi ile geliştirilen ilk kripto paradır. Blok zincir (blockchain) teknolojisinin çıkış noktası P2P olarak adlandırılan kullanıcıdan kullanıcıya ya da diğer bir ifadeyle uçtan uca transferi sağlayan sistemdir. Blok zincir değer içeren para, kimlik, değerli kâğıtlar gibi verilerin yüksek güvenli ortamlarda depolanması ve yönetilmesi şeklinde geliştirilmiş bir ağ teknolojisidir. Blok zincir, Bitcoin ve benzeri kripto paraların alt yapısını oluştursa da temelinde yatan teknoloji sayesinde farklı servis ve hizmetlere alternatif çözümler üretme noktasında internetten sonra ortaya çıkan en büyük yenilik ve devrim niteliği taşıyan ağ teknolojisi olarak nitelendirilmektedir.¹²⁵

Blok zincir teknolojisi asimetrik kriptoloji ve dağıtık sistem olması gibi iki önemli özelliğe sahiptir. Asimetrik kriptolojide, şifreleme işleminde şifrelenen kısım herkes tarafından görülürken şifrenin çözülmesi için gereken anahtarın yalnızca bir veya en fazla birkaç kişide olmasıdır ve böylelikle asimetrik şifrelemelerin çözülmesi daha zordur. Blok zincir alt yapısına sahip Bitcoin üzerinden örnek verecek olursak her Bitcoin kullanıcısı matematiksel olarak ilişkilendirilmiş özel (private) ve genel (public) olmak üzere iki kriptografik anahtara sahiptir. Genel anahtar 27-34 karakter uzunluğunda, göndericinin alıcıya Bitcoin gönderebilmesi için blok zincirde listelenen ve herkesin görebildiği bir anahtardır. Özel anahtar ise yalnızca Bitcoin kullanıcısının bildiği (kaybettiği takdirde Bitcoin'lerini de kaybedeceği) ve işlemleri onaylamak için

¹²³ Sabrina T. Howell, Marina Niessner ve David Yermack, "Financing Growth with Cryptocurrency Token Sales", 2018, s.1.

¹²⁴ Howell, Niessner ve Yermack, "Financing Growth with Cryptocurrency Token Sales", s.6.

¹²⁵ Ahmet Usta ve Serkan Doğantekin, "Finans ve Teknolojinin Yeni Birlikteliği, *Blockchain 101*, Zeynep Hale Akman, (Ed.), İstanbul 2017, s.27.

kullandığı bir çeşit dijital imza olarak ifade edilmektedir.¹²⁶ Blok zincir teknolojisinin bir diğer özelliği ise paylaşılma esasına dayanan dağıtık sistem olmasıdır. Nakamoto tarafından ortaya çıkarılan en önemli yenilik olan blok zincir temelde verilerin kaydedildiği, her işlemin denetlendiği ve hiçbir zamanda silinemediği, değiştirilemediği ve geri alınamadığı, ağdaki herkese açık dijital kayıt defteri olarak tanımlanmaktadır. Blok zincir her bir verinin şifrelenmiş halinin bir nevi parmak izinin alınmış halinin zincir şeklinde sıralanmasıyla oluşur. Blok zincir işlemleri bloklar halinde tutar ve uç noktalara gönderir. Her bir blok kendinden bir önceki bloğun özetini yani kimliğini içermektedir. Blok zincir verileri aynı zamanda o blok zincir ağında bulunan tüm bilgisayarlar da depolanmaktadır. Her bir işlem hareketi ise ağdaki tüm kullanıcılar tarafından da görülebilmektedir. Böylelikle aynı Bitcoin'in ikinci defa harcanmasının önüne geçilmektedir. Blok zincir her 10 dakikada bir zincire yeni blok eklenmesi esasına göre tasarlanmıştır. Blok zincir, madencilere blok oluşturma rekabeti ve kazandıkları ödülleri ağdaki tüm kullanıcılara duyurma imkânı sağlamaktadır.¹²⁷

Sürekli uzamakta ve değişmekte olan blok zincir teknolojisinde zincire eklenen her bir kayıt eklenmeden önce bir önceki kayıtla karşılaştırılmakta ve doğrulaması yani hangi işlemlerin geçerli hangilerinin geçersiz olduğu ise Bitcoin madenciliği yapan kişiler tarafından gerçekleştirilmektedir.¹²⁸

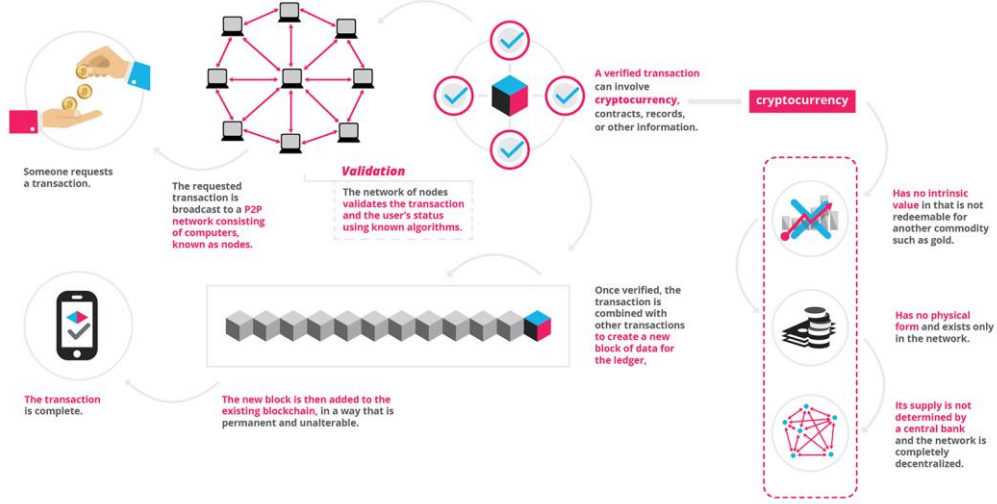
Blok zincir Bitcoin örneği ile finans sektöründeki işlem kaydı yönetiminin yeni bir şekli olarak ilk defa karşımıza çıkmıştır. Blok zincir Bitcoin ile gerçekleştirilen işlemlerin güvenlik seviyesinin yüksek dijital bir imza ile onaylanıp gerçekleştirilebileceğini göstermiş olması açısından önem teşkil etmektedir. Blok zincirini ve dolayısıyla Bitcoin'i tüm dünyadaki parasal akışların takip edilebilir, herkese açık olması ve şeffaflığın ön planda tutulması amacıyla ortaya çıkmış bir teknoloji olarak da ifade edilmesi mümkündür.

¹²⁶ Tsukerman, "The Block Is Hot: A Survey Of The State Of Bitcoin Regulation And Suggestions For The Future", s.1136.

¹²⁷Khaled Baqer; Danny Yuxing Huang ve Damon McCoy, Stressing Out: Bitcoin "Stressing Out: Bitcoin Stress Testing", *Financial Cryptography and Data Security*, Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner ve Kurt Rohloff (Ed.), 2016, s.4.

¹²⁸ Vigna ve Casey, Bitcoin ve Dijital Paranın Küresel Ekonomik Sistemde Meydan Okuması; Kriptopara Çağı, s.177.

Şekil 1.15: Blok zincir Çalışma Şekli¹²⁹



1.9. DÜNYA ÜLKELERİNİN KRIPTO PARALARA YAKLAŞIMI

Dünya geneli itibarı ile hükümetler şu an kripto paralar arasında en bilinen ve değeri en yüksek olan Bitcoin'in ve türevlerinin göz ardı edilemeyecek kadar önemli olduğunu anlamış bulunmaktadır. Küresel çapta hükümetlerin kripto paralara ve özelinde Bitcoin'e olan yaklaşımları birbirinden farklılık göstermektedir. Bazı hükümetler Bitcoin'i yasa dışı ilan ederken (Tayland Bitcoin'i ilk yasaklayan ülke olmuştur.¹³⁰) bazıları düzenleme yolunu seçmiştir.¹³¹ Uluslararası alanda kripto paraların yasal durumunu tanımlayan genel bir sözleşme veya anlaşma bulunmamaktadır. Avrupa Merkez Bankası'na göre Bitcoin'in Avrupa Birliği'nin Elektronik Para Direktifi'nde (2009/110/EC) yer alan "elektronik paranın sahip olması gereken üç kriterden sadece ikisini sağladığı ve elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilmesi" özelliğini ise sağlamadığı belirtilmektedir. Ayrıca Bitcoin'in madencilik denilen yöntemle herhangi bir fon alınmadan çıkartıldığı için de elektronik paranın sahip olduğu bu kriterleri tam anlamıyla taşımadığı ifade edilmektedir. Diğer taraftan Ödeme Hizmetleri Direktifi'nde (2007/64/EC) yer alan "ödeme kuruluşları elektronik para çıkaramaz"

¹²⁹ "What is Blockchain Technology? A Step-by-Step Guide For Beginners", 15.11.2017, <https://blockgeeks.com/guides/what-is-blockchain-technology/>, (Erişim: 15.12.2017).

¹³⁰ Alan Brill ve Lonnie Keene, *Cryptocurrencies: The Next Generation of Terrorist Financing?*, New York 2014, s.23.

¹³¹ Brill ve Keene, *Cryptocurrencies: The Next Generation of Terrorist Financing?*, s.16.

ifadesine de uymadığı için Bitcoin'in bu kapsamda da değerlendirilemeyeceği Avrupa Merkez Bankası tarafından ifade edilmiştir.¹³² Avrupa Merkez Bankası Ekim 2017'de yaptığı açıklama ile Bitcoin'in düzenleme yapılacak kadar yeteri olgunluğa erişmediğini ifade etmiştir.¹³³ Mali Eylem Görev Gücü'nün 2015 yılında yayınladığı raporda finansal yenilikleri onayladığını fakat aynı zamanda sanal para ödeme servislerinin kara para aklama ve terörizm finansmanında kullanılabilme ihtimalinin bir risk oluşturduğunu ve bu riskin tanımlanması ve azaltılması gerektiğini belirtilmektedir.¹³⁴

Uluslararası Para Fonu, merkez bankası dijital para birimleri ile ilgili Kasım 2020'de yayınlamış olduğu raporda kanuni bir dayanağı olmayan Bitcoin, Ethereum ve Ripple'in gayri resmî para benzeri birim olarak tanımlanabileceğini belirtmektedir.¹³⁵ Raporda ayrıca Bitcoin'in yasal olarak emtiaya daha yakın olduğu da ifade edilmektedir.¹³⁶ Raporda dijital muhasebe defterinin bir sonucu olarak istikrarlı coinler olarak nitelendirdiği sanal paraların yanı sıra blok zincir ve diğer teknolojik ilerlemeler sonucu geliştirilen kripto paraların, merkez bankası topluluğu tarafından "merkez bankası dijital para birimi" (CBDC) olarak değerlendirildiği ifade edilmektedir. Dünya üzerindeki birçok merkez bankasının kripto paraların ihraç edilmesinin uygunluğu ve geçerliliği ile ilgili konularda detaylı bir araştırma içerisinde olduğu belirtilmektedir. Araştırmaların bu aşamada çoğu merkez bankasının CBDC'nin servis edilmesindeki birtakım zorlukları açıklığa kavuşturmuş olsa da faydalarının maliyetlerinden daha fazla olacağı konusunda henüz ikna olmadıklarını ortaya koyduğu ifade edilmektedir. Uluslararası finansal kurumların da bu tartışmaya katkı sağladıkları belirtilmektedir. IMF, Staff Discussion Note'da CBDC'nin henüz evrensel bir kabullenme olmasa da paranın evriminde bir sonraki dönüm noktası olabileceğine karar verdiğini ifade etmektedir. Raporda ayrıca Asya Kalkınma Bankası Kurumu'ndan da benzer bir görüş geldiği belirtilmektedir. Ödeme ve Piyasa

¹³² European Central Bank, *Virtual Currency Schemes*, 2012, s.43.

¹³³ Sujha Sundararajan, "ECB President: Bitcoin Not 'Mature' Enough to Be Regulated", 20.10.2017, <https://www.coindesk.com/ecb-president-bitcoin-not-mature-enough-to-be-regulated/>, (Erişim: 15.12.2017).

¹³⁴ Financial Action Task Force, (2015), *Guidance For a Risk-Based Approach to Virtual Currencies*, s.3.

¹³⁵ International Monetary Fund, *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*, 2020, s.30.

¹³⁶ Age, s.36.

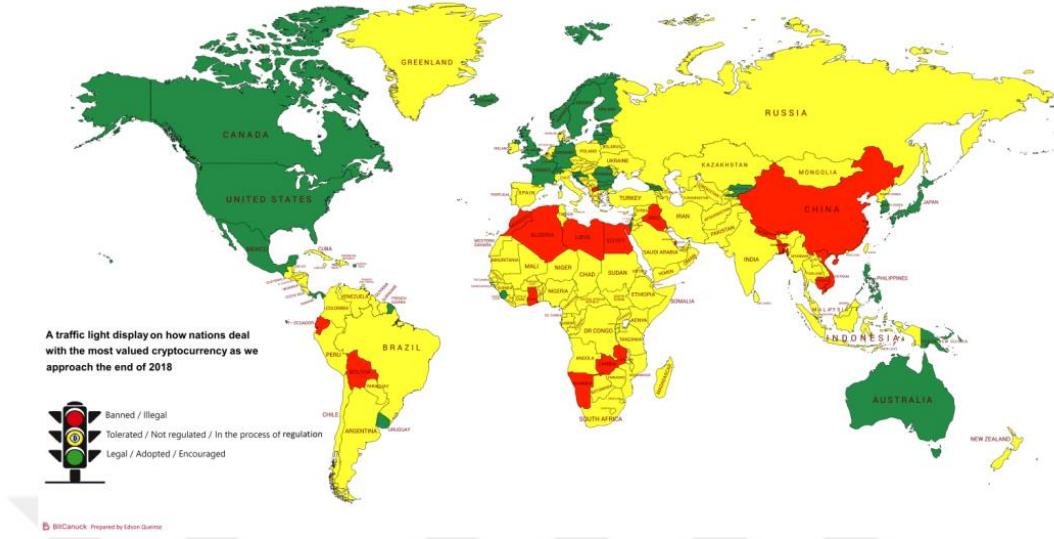
Altyapıları Komitesi (CPMI), CBDC'nin iyi tanımlanmış bir terim olmadığını belirtmektedir. Bu terimin birçok sayıdaki kavramı nitelendirmek için kullanıldığı belirtilmektedir. CBDC'nin birçok kurum tarafından hem bir değişim aracı hem de değer deposu olarak işlev gören ve bir merkez bankası sorumluluğu altında merkez bankası parasının yeni bir formu olabileceği düşünülmektedir. IMF, CBDC'yi dijital olarak ihraç edilmiş, merkez bankası tarafından yasal ödeme aracı olarak servis edilmesi planlanan paranın yeni bir formu olarak tanımlamaktadır.¹³⁷ CBDC'nin merkez bankası ve para hukuku kapsamında önemli soruları da beraberinde getirdiği ve bu hukuk organları altındaki yasal muamelenin de CBDC'nin tasarım özelliklerine bağlı olacağı ifade edilmektedir. Her halükarda token ve hesap tabanlı CBDC'nin yasal olarak paranın formundan çok farklı kavramlara sahip olduğu da belirtilmektedir. Yasal olarak token tabanlı CBDC bir merkez bankası yükümlülüğü altında dijital bir tokene dâhil olan ve bu tokenin transfer edilmesiyle transfer edilen paranın tamamen yeni bir formu olabileceği ifade edilmektedir. Buna karşılık hesap tabanlı CBDC'nin paranın sadece dijital formda ifade edilen “book money” olduğu görüşü de raporda ayrıca belirtilmektedir.¹³⁸ Book Money terimi esasen banka hesap bakiyelerini ifade etmektedir. Book Money teriminin bir merkez bankası veya para otoritesi tarafından çıkarılan sınırlı bir efektif para arzının bir parçası olmaması bakımından baz para kavramından farklı olduğu belirtilmektedir. Mevduat sahibi ve ticari bir banka arasında bir borç anlaşması olduğu ifade edilmektedir.¹³⁹

¹³⁷ *Age*, s.4-5-6.

¹³⁸ *Age*, s.41.

¹³⁹ “Book Money”, <https://www.moneyland.ch/en/book-money-definition> , (Erişim: 08.12.2020).

Şekil 1.16: Bitcoin'in Ülkelere Göre Yasal Durumu¹⁴⁰



Sanal paralar ilk bakışta paranın elektronik çeşidi olarak işlev görmektedir. Fakat daha yakından incelendiğinde sanal paraların altında yatan teknolojinin üçüncü bir aracı kuruma ihtiyaç duymadan işlemlerin gerçekleştirilmesine imkân sağlayan bir ödeme aracı gibi davrandığını ortaya koymaktadır. Bu sürecin sistemin doğası gereği asıl işlemlerin sanal kontratlar gibi davranması gerçeğiyle mümkün olduğu belirtilmektedir. Sanal paraların tecrübe ettiği son zamanlardaki fiyat dalgalanmalarının, yapıları itibarıyla paradan çok varlıklara benzer olabileceği şeklinde bir görüş de sunmaktadır. Eğer sanal paralar, paranın dijital bir çeşidi olarak tanımlanıyorsa geleneksel paranın sahip olduğu fonksiyonları takip etmeli midir sorusunu da gündeme getirmektedir. Sanal paralar halen belirli durumlarda değişim aracı olarak ve hesap birimi olarak kullanılmaktadır. Sanal paranın değer deposu olarak kullanılıp kullanılamayacağı, maddi olmayan varlık olarak değerlendirilip değerlendirilemeyeceği ve nasıl işlem göreceği gibi konulara bu güne kadar ülkeler farklı cevaplar vermişlerdir. Hükümetler ve merkez bankaları tarafından sanal paralara olan uluslararası yaklaşım her ülkenin yasama ve düzenleme çerçevelerini ve sanal paralara nasıl davrandığına ilişkin kendi görüşlerini yansıtmaktadır. Bu güne kadar sanal paraların niteliği ile ilgili küresel olarak kabul edilen bir standart bulunmamaktadır. Yalnızca 2014 yılında sanal paraların tanımı, terörün finansmanı ve

¹⁴⁰ Evangelina Chapkanovska, "Bitcoin Regulation: Where is Bitcoin Legal in 2020?" (30.11.2020), <https://spendmenot.com/blog/bitcoin-regulation/>, (Erişim:31.12.2020).

kara para aklama işlemleri için risk oluşturabileceği ile ilgili Mali Eylem Görev Gücü tarafından yayınlanan rapor bulunmaktadır.¹⁴¹ Aşağıda dünya üzerindeki farklı bölgeler açısından bazı ülkelerin kripto paralara olan yaklaşımları incelenmiştir.

1.9.1. Amerika Kıtası

1.9.1.1. Bolivya

Bolivya Merkez Bankası 2014 yılında merkez bankası tarafından ihraç edilmeyen ya da düzenlenmeyen her türlü para veya madeni parayı yasaklamıştır. Bankanın bu şekilde bir karar vermesinin anlamı ülkenin ulusal kurumları tarafından daha önce onaylanmayan herhangi bir para biriminin vatandaşları tarafından değerler isimlendirmesini yasaklamıştır. Banka ayrıca diğer merkez bankaları tarafından desteklenmediğinden dolayı Bitcoin'in bir varlık olmadığını ifade etmiştir. Feathercoin, Namecoin, Peercoin, Quark ve Primecoin Merkez Bankasının yasaklı sanal paraları aarsında yer almakta olduğu belirtilmektedir.

1.9.1.2. Ekvador

Ekvador hükümeti 2014 yılında Bitcoin'i ve tüm dağıtık sanal paraları ülkenin para ve finansal yasalarında yapılan reformların bir parçası olarak yasaklamıştır. Aynı zamanda bu reformun hükümetin sanal paralar olarak ödeme yapmasına da imkân sağladığı belirtilmektedir. Ayrıca merkez bankası tarafından desteklenen Ekvador hükümeti sanal parasının geliştirilmesini de önermektedir. Hükümetin Bitcoin'i yasa dışı ilan etmesine rağmen, Bitcoin kullanımı halen ülkede durdurulmamıştır. LocalBitcoins.com internet sitesinde ülkedeki Bitcoin alıcıları ve satıcılarının listeleri yer almaktadır. Bitcoin çevrimiçi cüzdanlarla Paypal aracılığıyla alınabilmektedir. Ekvador'da büyüyen bir Bitcoin topluluğu bulunmaktadır.¹⁴²

¹⁴¹ Department of Finance, "Virtual Currencies and Blockchain Technology", Dublin, March 2018, s. 6.

¹⁴² Age, s.17.

1.9.1.3. Amerika Birleşik Devletleri

Kripto para açısından ilk gerileme 2013 yılında yaşanan FBI tarafından gerçekleştirilen Silk Road baskını olduğu belirtilmektedir. Bu baskından sonra Bitcoin hem halkın gözünde hem de hükümet yetkilileri gözünde kötü bir izlenim bırakmasına rağmen bu yaşanan olayın Bitcoin düzenlemesine katkı sağladığı ifade edilmektedir. Bu baskından kısa bir süre sonra ABD Hazine Bakanlığı'na bağlı Finansal Suçlarla Mücadele Birimi (FinCEN), Bitcoin ödeme işlemlerine yönelik yasal düzenlemelerin yapılacağını duyurmuştur. 15 Mart 2014 tarihinde ABD Gelir İdaresi Kuruluşu Bitcoin'in bir para birimi olmadığını fakat emlak veya hisse senedi gibi bir varlık olarak değerlendirilebileceğini ve kazanç vergilerine tabi tutulacağını belirtmiştir. Böylelikle Bitcoin'in yasal bir statüye oturtulduğu ifade edilmektedir.¹⁴³ Diğer taraftan Amerika Birleşik Devletleri Federal Hükümetinin henüz sanal paraları düzenleme yetkisine sahip olmadığı ifade edilmektedir. Amerika Gelir İdaresi (IRS), 2014 yılında sanal paralarla yapılan ticaret, alım veya satım işlemlerinden elde edilen kazançların sermaye kazanımları için mülk olarak değerlendirilebileceğini belirten 2014/21 Bildirimi yayınlamıştır. 13 Mart 2018 tarihinde 2018 ABD Kongresi Ortak Ekonomi Raporu, gelecek yılda sanal paraların ve blok zincirinin ABD ekonomisi üzerindeki etkisine ilişkin öngörü sağlamak için analiz ve tavsiyeler içermektedir ve bütün bölümü sadece bunun için ayrılmıştır.¹⁴⁴ FinCEN, kripto paraların alım satımını gerçekleştiren işletmelere yönelik düzenlemelerle ilgili "kripto paralarda para aktarma işi" adı altında bir yönerge yayınlamıştır.¹⁴⁵

22 Aralık 2020 tarihinde yayınlanan bir habere göre kripto para sektörünün en önemli şirketlerinden biri olan Ripple, ABD Menkul Kıymetler ve Borsa Komisyonu'nun kendilerine lisansız menkul kıymetler satışı iddiası ile ilgili sürpriz bir dava açmaya hazırlandığını ifade etmiştir. Ripple'ın kurucu ortağı olan Chris Larsen ve CEO'su Brad Garlinghouse'un sanık olarak gösterildiği belirtilmektedir. ABD Menkul Kıymetler ve Borsa Komisyonu, şirketin ve yöneticilerin 1,3 milyar ABD Doları tutarında kayıtsız menkul kıymetler satışı gerçekleştirdikleri iddiasında

¹⁴³ Vigna ve Casey, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, s.354-360.

¹⁴⁴ Department of Finance, "Virtual Currencies and Blockchain Technology", s.13.

¹⁴⁵ Brill ve Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?", s.8.

bulunduđu ifade edilmektedir. Ŗirket ve kurum arasında dijital para birimi olan Ripple ile iliřkili olan XRP'nin ABD Menkul Kıymetler ve Borsa Komisyonu tarafından kayıtlı olması gereken bir hisse senedi gibi bir menkul kıymet mi yoksa bir para birimi olduđu ile ilgili tartıřmanın önümüzdeki yıllarda da devam edeceđi belirtilmektedir. XRP'nin güncel piyasa deđerı 23 milyar ABD Doları olduđu ve kripto para endüstrisindeki üçüncü sırada en deđerli kripto para olarak yer aldıđı ifade edilmektedir. Ripple'ın kararının bu řekilde önceden duyurulmasının alışık olunmadık bir davranıř olduđu ve Garlinghouse'un Biden yönetiminin kripto para endüstrisine Trump yönetiminde daha dostça yaklařabileceđini öngördüđu ve bu nedenle Ripple'ın önceden tedbir alınmıř duyurusunun siyasi bileřenlerinin olabileceđi belirtilmektedir. ABD Menkul Kıymetler ve Borsa Komisyonu son yıllarda en deđerli kripto para olan Bitcoin ve Ethereum'un bir menkul kıymet olmadıđını kısmen hiçbir řirketin veya kiřinin kontrol edemediđi dađıtık bir yapıya sahip olduklarına karar verdikleri belirtilmektedir. XRP'nin Bitcoin ve Ethereum'dan Bitcoin ve Ethereum'un madencilik denilen bir sistemle devam eden bir süreçte kademeli olarak elde edildiđi bakımından farklı olduđu belirtilmektedir. Buna karřılık Larsen ve diđerlerinin 2012 yılında Ripple Laboratuvarları olarak adlandırılan řirket için tek seferde 100 milyar adet XRP oluřturdukları ifade edilmektedir. Ripple'ın XRP'nin aslan payına sahip olmaya devam ederken hazinesinin büyük bir kısmının planlanmıř tahsislerde satılmak üzere yedekte tutulduđu ifade edilmektedir. Ayrıca Garlinghouse ve Larsen'in de önemli miktarda XRP'ye sahip olduđu da ifade edilmektedir. Bu düzenlemenin bazı gözlemcilerin XRP'yi bir para biriminden ziyade řirket hissesine daha çok benzer gördüğüne yol açtıđı da belirtilmektedir. Ripple, XRP'nin yıllardır bir menkul kıymet olduđu görüşü üzerine hırçın bir řekilde geri adım attıđı belirtilmektedir. Ŗirketin, XRP'nin giderek artan bir řekilde dađıtık bir yapıya sahip olduđu bankaların ve diđer tüccarların sınır ötesi işlemlerinde bir köprü olarak kullandıkları için rezerv fonlarının istenildiđi gibi kullanım yetkisinin olmadıđını belirttiđi de ifade edilmektedir. Garlinghouse'a göre ABD Menkul Kıymetler ve Borsa Komisyonu'nun Ripple tarafından menkul kıymet olarak kontrol edilen XRP ile ilgili olarak petrolün bir menkul kıymet olarak Exxon tarafından kontrol edilmesi benzetmesi yaptıđı da belirtilmektedir. ABD Menkul Kıymetler ve Borsa Komisyonu'nun kısa bir süre önce müřterileri için kripto para tokeni çıkaran Kik adlı bir mesajlařma uygulaması ile ilgili

davayı kazandığı ifade edilmektedir. Yargıcın bu davada söz konusu edilen tokenin lisanssız menkul kıymetler olduğunu ifade ettiği belirtilmektedir. Yasal sorunun Larsen ve diğer Ripple yöneticilerinin şirketin genel merkezinin düzenleyiciler tarafından zorlayıcı davranışların duyurulmasına bir cevap olarak ABD dışında bir yere taşıyabileceğini önermesinden aylar sonra geldiği de belirtilmektedir. Garlinghouse'un ABD Menkul Kıymetler ve Borsa Komisyonu'nun XRP'yi bir menkul kıymet olarak değerlendirmeyi reddeden Singapur, İsviçre ve Japonya gibi dava etmeye karar vermesinin şaşırtıcı olduğunu ifade etmektedir. Garlinghouse'un ayrıca Bitcoin ve Ethereum'un Çinde yaratıldığı buna karşılık Ripple'ın milliyetçilik vurgusu ile bir Amerikan şirketi olduğunu da belirtmektedir. ABD Menkul Kıymetler ve Borsa Komisyonu'nun kripto para endüstrisi için zorluk çıkartan tek kurum olmadığı geçen hafta Hazine Bakanlığı'nın coin tabanlı banka ve borsa alım satım işlemleri için Bitcoin ve diğer kripto para işlemleri için kullanılan barındırılmamış cihazlar ve yazılım cüzdanların kimlik doğrulaması ile ilgili bir dizi kural önerdiği belirtilmektedir. Eleştirmenlerin bu önerilen kuralların dağıtık finans olarak bilinen yeni gelişmekte olan endüstriyi boğabileceğini ve on beş gün gibi kısa bir süre içinde görüşe açılmasının çok kısa bir süre olduğunu belirttikleri ifade edilmektedir. Garlinghouse'un Hazine Bakanlığı ve ABD Menkul Kıymetler ve Borsa Komisyonu'nun aldıkları kararların kripto paralara düşman olan Trump yönetiminin ayrılırken yaptığı bir hamle olduğu ifade edilmektedir. Biden yönetimi ile kripto para endüstrisinin daha fazla ilgi göreceği de belirtilmektedir. Garlinghouse'un ayrıca kripto endüstrisi içindeki herkesin ayağa kalkması ve ABD Menkul Kıymetler ve Borsa Komisyonu'nun sektöre zorbalık yapmasına izin vermemeleri gerektiğini ve tarihin sağ tarafında yer alacaklarını ifade ettiği belirtilmektedir.¹⁴⁶

ABD Adalet Bakanlığı'nın 2 Mart 2020 tarihinde, Tian Yinyin ve Li Jiadong isimli Çin uyruklu iki kişinin 2018 yılında Kuzey Kore adına kripto para borsasından 250 milyon ABD Doları değerinde kripto para çaldıkları gerekçesi ile suçlandıklarını ifade etmiştir. Çalınan bu kripto paranın çoğunu bir yazılım programı ile Çin bankalarında reel para birimlerine çevirdikleri de belirtilmektedir. Hazine

¹⁴⁶ Jeff John Roberts, "Ripple says it will be sued by the SEC, in what the company calls a parting shot at the crypto industry", 22.12.2020, <https://fortune.com/2020/12/21/ripple-to-be-sued-by-sec-cryptocurrency-xrp/> (Erişim:27.12.2020).

Bakanlığının ise her iki kişiye de yaptırım uyguladığı ifade edilmektedir. Bu durumun kripto paraların gizleme aracı özelliğinin ve tekniğinin ABD'nin ulusal güvenliğine yönelik bir finansal tehdit olarak giderek büyüyen bir rol oynadığı vurgulanmaktadır. ABD düşmanlarının, blok zincir teknolojisini daha yakından tanıdıkça, düşmanca siber operasyonlarının giderek artan bir şekilde kripto para birimi faaliyetlerine bağlanmasının muhtemel olacağı da ayrıca belirtilmektedir. Haydut devletlerin ABD'nin ekonomik yaptırımlarının etkisini azaltmaya çalıştıkça, kripto para kullanımında muhtemelen daha yenilikçi olacakları da vurgulanmaktadır. Yeni nesil Kuzey Kore aklama planının yasa dışı finansmanının; kripto para borsasından çalma işlemi, çalınan bu kripto paranın aklanma işlemi ve tokenlerin reel para birimine dönüştürülmesi olarak üç aşamada gerçekleştiği belirtilmektedir. İlk adımın temel bir siber güvenlik farkındalık oryantasyonuna katılan her hangi biri için bilindik taktikler içerdiği belirtilmektedir. Kuzey Kore ilişkili Lazarus Grup bilgisayar korsanlarının isimsiz bir borsa çalışanının bilgisayarına kötü amaçlı bir yazılım indirilmesini sağlayan aldatıcı bir e-posta gönderdiği ifade edilmektedir. Bu kötü amaçlı yazılımın bilgisayar korsanlarına borsa çalışanının bilgisayarına uzaktan erişimi mümkün kıldığı, borsa çalışanının özel dijital anahtarlarını ele geçirdiği ve böylelikle kripto para cüzdanının kontrolünü ele geçirdiği belirtilmektedir. Lazarus Grup bilgisayar korsanlarının 234 milyon ABD Doları değerindeki kripto parayı çalıp kendi hesaplarına gönderdiği ve ardından fonları aklamak için hackleme ile ilgisi yokmuş gibi gözüken kripto cüzdanlara taşıdıkları ifade edilmektedir. Kripto para işlemlerinin çevrimiçi halka açık işlem defterlerini takip eden herkes tarafından görülebileceği belirtilmektedir. Lazarus Grup'un hackleme ile çok açık bir iş yaptıkları için çaldıkları tokenleri kripto para borsalarında direk satamadıkları bunun yerine Kuzey Kore'de bulunan ajanları ile, Kuzey Kore'ye ait olmayan sahte kimlik belgeleri kullanarak çok çeşitli kripto para borsalarında birden çok hesap açtıkları ifade edilmektedir. Ardından bilgisayar korsanlarının çaldıkları kripto parayı programlama komut dosyası kullanarak oluşturdukları yüzlerce yeni dijital cüzdan adresinden Kuzey Kore kontrolündeki hesaplarına otomatik olarak transfer etikleri belirtilmektedir. Fonların bir kısmının da parayı nakde çevirmeden önceki birkaç ayı ek aklama yaparak geçiren Tian ve Li'nin kripto para hesaplarına gönderdikleri belirtilmektedir. Kripto paranın nakde çevrilme aşamasının çok katmanlı olduğu ifade edilmektedir. Tian ve Li'nin

çalınan kripto paranın fiat para birimine dönüştürülmesi ve borsadaki müşterilerine bir ücret karşılığında transfer edilmesi şeklinde kayıtsız bir kripto para ticareti operasyonu yürüttükleri belirtilmektedir. Temmuz 2018'den Nisan 2019 yılına kadar çeşitli uçtan uca kripto borsa web siteleri üzerinden müşterileri ile ticaret yaptıkları ve bu ticaretlerden kazandıkları paraları saklamak için çok sayıda Çin bankalarında hesap açtıkları ifade edilmektedir. Lazarus Grup'un hackleme işlemiyle bu ikilinin 100 milyon ABD Dolarından fazla haksız elde ettikleri kripto parayı akladıkları ve Çin'deki banka hesaplarına binlerce kez para yatırdıkları belirtilmektedir. Bu teknik aklama planının Kuzey Kore için muhtemelen herhangi bir teknik zorluk oluşturulmadığı da belirtilmektedir. Bilgisayar korsanların dakikalar içerisinde binlerce adet dijital cüzdan oluşturmak için kullandığı açık kaynak kodlu yazılım programlarının çevrimiçi ücretsiz olarak ulaşılabilir olduğu ve öğrencilerle tamamlanabildiği ve blok zincir geliştirici toplulukları içerisinde çok popüler olduğu da vurgulanmaktadır. Bu cüzdanların herhangi bir kripto para borsası tarafından kontrol veya bloke edilemediği ve üçüncü taraflar tarafından da kapatılamayacağı için "barındırılmamış" veya "gözetim altında tutulmayan" cüzdanlar olarak adlandırıldıkları belirtilmektedir. Borsalarda kullanılan cüzdanların aksine ulaşmak için herhangi bir kimlik doğrulamasının da gerekmediği ifade edilmektedir. Bu cüzdanların tamamen sahte araçlar oldukları belirtilmektedir. Adalet Bakanlığı Lazarus Grup'un daha geniş siber operasyonlarının bir kısmını hackledikleri kripto paralarla finanse ettiklerini açıklamıştır. Barındırılmamış cüzdanlarına gönderdikleri fonları kullanarak web sitesi barındırma, alan adları ve özel sanal ağları ile Bitcoin ile ödeme yaptıkları ifade edilmektedir. Bu servislerin bilgisayar korsanlarına diğer borsalara kötü amaçlı kod gönderen sahte web siteleri oluşturmalarına izin vererek kimlik avı kampanyalarını desteklediği belirtilmektedir. Aklama ve hackleme işlemlerinin bu şekilde bir döngü olarak devam ettiği belirtilmektedir. Kuzey Kore olayının barındırılmayan cüzdanlara erişim ve kara para aklamayı önleme yasalarındaki esneklikle birlikte dünya çapında kripto para alım satımı yapan borsaların varlığının kripto para aklamayı mümkün kıldığı belirtilmektedir. ABD'nin 2013 yılından beri kripto para borsalarını düzenlemeye başladığı fakat diğer birçok ülkenin ise kripto para faaliyetlerine kara para aklama önleme kurallarını uygulamanın gerisinde kaldığı belirtilmektedir. Hükümetler arası fonksiyona sahip Mali Eylem Görev Gücü'nün, 2019 yılında küresel

kara para aklama standartları belirlediği ve tüm ülkelerin sanal varlık sektörlerini nasıl düzenlemeleri gerektiği ile ilgili resmi bir rehber yayınladığı ifade edilmektedir. Fakat yasa dışı aktörlerin, anonim kripto ticaretini yapabilecekleri uyumlu olmayan borsalar bulmak için ülkelerin ulusal düzenleme rejimlerindeki farklılıkları kullanmaya devam edecekleri de belirtilmektedir. Barındırılmamış cüzdanların çok tehlike oluşturduğu da ayrıca ifade edilmektedir. Bir finansal aracı olmadan taraflara işlem imkanı sağlaması kripto para birimi teknolojisinin çığır açıcı temel özelliği olarak vurgulanmaktadır. Blok zincir meraklılarının sıklıkla, barındırılmamış cüzdanların finansal hizmetlere ulaşmak için bu engeli azalttığı ve bankasız ve banka hesabı olmayan nüfuslara finansal bir katılım sağlamayı getirdiğini iddia ettiği belirtilmektedir. Sonuç olarak finansal kurumların açık kaynak kodlu bu yazılımı sınırlamaya imkanı olmadığı ve bu nedenle mevcut düzenleyici çerçevenin kişilerin kripto para birimi borsalarındaki nakit değişimlerini açma ve kapama rampalarını düzenleyebileceği belirtilmektedir. ABD Hazine Bakanlığının banka hesaplarını ve diğer varlıkları belirlediği gibi şimdi de kripto para adreslerini belirleyebildiği belirtilmektedir. Adalet Bakanlığının Kuzey Kore aklama işlemlerindeki 113 kripto para birimi hesabında tutulan fonları elde etmeye çalıştığı da ifade edilmektedir. Kripto para birimleri, devlet destekli siber operasyonları ve ABD ulusal güvenliği arasındaki bağın bir bakıma yüzeye çıktığı belirtilmektedir. bir diğer Adalet Bakanlığı iddianamesine göre, Rusya askeri istihbarat görevlilerinin siber operasyonlarını desteklemek için ve 2016 ABD Başkanlık seçimlerinde bilgi savaşını desteklemek için 90 Bin ABD Doları değerinde kripto para akladıkları ve harcadıkları ifade edilmektedir. İran'ın ABD ile artan geriliminin İran rejiminin bilgi savaşını desteklemek amacıyla kullandığı kripto paradan kaynakladığı da ayrıca belirtilmektedir. ulusal güvenlik yetkililerinin bankalardan ziyade yeni gelişen blok zincir üzerinde gerçekleşen kara para aklama durumu ile mücadele etmek için kripto para birimleri konusunda çok daha akılcı davranması gerektiği de ifade edilmektedir.¹⁴⁷

Teröristlerin kripto para edinmesine ilişkin belgeli örneklerin suç amaçlı kullanımı ile karşılaştırıldığında nispeten daha seyrek olduğu belirtilmektedir. 2019

¹⁴⁷ Yaya J. Fanusie, "Cryptocurrency Laundering Is a National Security Risk", 27.03.2020, <https://www.lawfareblog.com/cryptocurrency-laundering-national-security-risk>, (Erişim 02.01.2021).

yılı boyunca terör örgütlerinin mal varlıklarını Bitcoin gibi kripto paralardan elde ettme ve depolamaya yöneldiği ifade edilmektedir. Ağustos 2020’de ABD Adalet Bakanlığı’nın terör örgütleri ile ilişkili bugüne kadar en büyük sanal varlıklarını ele geçirdiği belirtilmektedir. Adalet Bakanlığı’nın, Hamas, El Kaide ve DAESH (Irak ve Şam Devleti) ile ilişkili 300’den fazla kripto para birimi hesabından milyon ABD Dolarına eş değer tutarda miktar ele geçirdiklerini duyurduğu ifade edilmektedir. 2019 yılında Hamas’ın askeri kanadının anonim bağışları teşvik etmek için sosyal medya aracılığı ile çevrimiçi kripto para bağış toplama kampanyası başlattığı belirtilmektedir. Yaygın inanın aksine anonimliğin sıklıkla kripto para ile adlandırılmasının yanlış bir betimle olduğu da ifade edilmektedir. Hamas planının en sonunda çözüldüğü ve 150 kripto para hesabının ele geçirildiği ifade edilmektedir. El-Kaide’nin Suriye’deki faaliyetlerini kripto para birimi ile desteklemek amacıyla bağışçıların ilgisini çekmek için sosyal medya kullanarak kripto para kullanımı yönünde yayılım gösterdiği belirtilmektedir. Adalet Bakanlığı’nın El – Kaide ile ilişki 100 kripto para hesabını ele geçirdiği ifade edilmektedir. Hamas ve El-Kaide’nin kripto para birimlerine ilgisinin Adalet Bakanlığı duyurusundan önce geldiği fakat bu tip fonlama sisteminin diğer finans kaynaklarına göre daha az dikkat çektiği de belirtilmektedir. 2017 yılında Zoobia Shahnaz’ın DAESH’e 85 bin ABD Doları temin ettiği bunu da kredi kartlarını maksimuma çıkararak Bitcoin satın aldığı ve sonrasında faaliyetlerini gizlemek için de Bitcoin’i nakite çevirdiği ifade edilmektedir. Shahnaz örneğinden iki yıl önce Ali Şükrü Emin’in insanlara Bitcoin’in nasıl temin edildiği ve örgüte nasıl Bitcoin gönderildiğini göstererek DAESH’e maddi destek sağladığı gerekçesi ile suçlu bulunduğu belirtilmektedir. Şu an en güncel kripto para birimi çabasının, N95 yüz maskesini de içeren ve kişisel koruyucu ekipmanların satıldığı bir web sitesi oluşturan DAESH bilgisayar korsanı olan ve Shahnaz ile ilişkisi tespit edilen Murat Çakar tarafından gerçekleştirildiği ifade edilmektedir. COVID-19 salgını ve yüz yüze finansal girişimlerle ilişki zorluklar göz önüne alındığında 2020 yılının Ağustos ayındaki durumun da organize terör örgütlerinin sanal varlıklar elde etmeye yönelmesinin bir dönüm noktası oluşturabileceği belirtilmektedir. Özellikle DAESH’in bazılarının kripto para birimi içerebilecek siber etkin operasyonlar aracılığıyla servet biriktirme çabalarını devam ettirmesinin muhtemel olduğu ifade edilmektedir. 2020 yılında Mali Eylem Görev Gücü’nün, hükümetlerarası bir kuruluş olarak özellikle

COVID-19 salgını süresince terör örgütlerinin kripto para birimine olan ilgisinin olası artışı ile ilgili uyarı yaptığı belirtilmektedir. Mali Eylem Görev Gücü'nün Mayıs 2020'de koronavirüs salgınının, yasa dışı fonların taşınması ve gizlenmesi için sanal varlıkların ve çevrimiçi finansal hizmetlerin kötüye kullanımında artışlara neden olabileceği ile ilgili bir rapor yayınladığı ifade edilmektedir. Adalet Bakanlığı'nın duyurusundan yaklaşık bir ay kadar sonra Mali Eylem Görev Gücü'nün sanal varlıkların terörist finansörleri ve kara para aklayıcıları tarafından kullanılabileceği ile ilgili kırmızı bayrak göstergeleri hakkında başka bir rapor yayınladığı da belirtilmektedir. Göstergelerin eşsiz işlem örneklerinden sanal varlıkların kötüye kullanımının belirtilebileceği coğrafik risk profillerine kadar uzanabileceği ifade edilmektedir. Bu göstergelerin yasa dışı aktörlerin kripto para birimini kullanmasını önlemek amacıyla Finansal İstihbarat Birimlerine, sanal varlık hizmet sağlayıcılarına ve finansal kuruluşlara faydalı bir rehber olduğu belirtilmektedir. Mali Eylem Görev Gücü'nün yayınlamış olduğu bu rehber ve Ağustos 2020'deki ABD Adalet Bakanlığı'nın Hamas, El-Kaide ve DAESH'in finansal varlıklarını ele geçirdiğini duyurmasına rağmen, teröristlerin servetlerini biriktirmek ve depolamak amacıyla kripto para kullanımlarında artma eğiliminde oldukları ifade edilmektedir. Bu durumun özellikle COVID-19 aşılarının 2021 yılında dağıtılacağı planlamasıyla bile işin sanal olarak yürütülmesine bağlılığın devam etmesi nedeniyle aynı şekilde devam edeceği görüşü de vurgulanmaktadır. Gün geçtikçe günlük tüketicilerin kripto para kullanımının artmasının genel işlem hacminde "örtmek" ve "gizlenme" arayışında olan terör örgütleri için fırsat oluşturacağı ifade edilmektedir. 2020 yılının başında yaklaşık 7 bin ABD Doları olan Bitcoin'in 4 Aralık 2020 tarihinde 19 bin ABD Dolarına yükseldiği ve tarihsel dalgalanmasının da göz önüne alındığında kripto para birimlerine yatırımın terör örgütleri için de bir risk oluşturduğu belirtilmektedir. On yıldan daha fazla önce bir Bitcoin'in 30 sent olduğu düşünüldüğünde sanal varlıkların terör örgütleri için kar elde edebilecekleri bir yatırım olarak düşünülebileceği ifade edilmektedir. Fakat Bitcoin'in değerinin birçok kere düştüğü ve en önemli düşüşünün ise 2013 yılında üç günlük bir periyotta %87 oranında bir kayıpla olduğu belirtilmektedir. Bu belirsizliğin Monero, Zcash ve Dash gibi sözde gizli coinlerle ilişkili kodları kırmak için özel sektör adımlarıyla birleştiğinde terör örgütleri için sanal varlıklara bel bağlamaları arayışı için bir risk oluşturduğu ifade edilmektedir.

Özel sektör şirketlerinin şu an ABD hükümetinin teröristlerin sanal varlık faaliyetlerinin izlerini sürmelerinde onlara destek olarak çok önemli rol oynadıkları belirtilmektedir. Kripto para biriminin izlenmesinde kamu özel sektör işbirliğindeki gelişmelerin, yüksek teknoloji terörizm finansmanı ve suç oluşturan kara para aklama operasyonları ile mücadelenin geleceğini temsil ettiği de ayrıca vurgulanmaktadır.¹⁴⁸

Amerika üst düzey finans düzenleyici kurumlarının daha önce de olduğu gibi kripto para şirketlerinin suç faaliyetlerini kolaylaştırmak için kripto paraların kötüye kullanılmasını engellemek amacıyla şirketlerin kara para aklama durumlarına karşılık denetim ve kontrollerin sıklaştırılması gerektiği ile ilgili uyarılarda bulunduğu belirtilmektedir. ABD Vadeli İşlemler Komisyonu (Commodity Futures Trading Commission – CFTC), ABD Menkul Kıymetler ve Borsa Komisyonu, Federal Rezerv ve Hazine Bakanlığı’ndan oluşan ABD Başkanı’nın Finansal Pazar üzerine olan Çalışma Grubu açıklamayı 23 Aralık 2020 tarihinde yayınladığı belirtilmektedir. Yeni yayınlayan bu raporda federal finans düzenleyicileri stablecoinlerin/sabitcoin riski en etkili bir şekilde yönetecek ve ABD’nin iç ve uluslararası finansal ve para sistemlerinin kararlılığını sağlayabilecek şekilde kullanılması gerektiği ifade edilmektedir. Stablecoin, stablecoin veya diğer bir adıyla sabitcoin fiyatının oynaklığını diğer bazı istikrarlı varlıklara veya varlık sepetlerine göre en aza indirmek için tasarlanmış güvenlik ve gizlilik ilkeleriyle ödeme işlemlerinde kullanılabilen bir kripto para birimi olarak ifade edilmektedir. Stablecoinin bir kripto para birimine, fiat paraya veya borsada işlem gören varlıklara sabitlenebileceği de belirtilmektedir.¹⁴⁹ Raporda yasa dışı finansal akışları engelleme gerekliliği dışında, stablecoin sağlayıcılarının yeterli nakit rezervlerini koruması gerektiği vurgulanmaktadır. Finansal düzenleme otoriteleri grubunun ayrıca stablecoin operatörlerinin coinlerin büyük ölçekli itfa (paraya çevirme) durumlarında baş edebilmesi için yeteri kadar dirençli olacak şekilde dizayn edilmesi gerektiği ifade edilmektedir. Grup ayrıca operatörlere güçlü rezerv yönetimi uygulamalarının 1:1 rezerv oranını ve kayıpları absorbe etmek ve likidite ihtiyaçlarını karşılamak için yeterli finansal kaynakları sağlamayı içermesi gerektiğini belirttiği ifade edilmektedir. Grup ayrıca stablecoin sağlayıcılarının güçlü risk yönetimi ve siber

¹⁴⁸ IntelBrief: Terrorists’ Use of Cryptocurrency, <https://thesoufancenter.org/intelbrief-2020-december-10/> 10.12.2020, (Erişim:29.12.2020).

¹⁴⁹ “Stablecoin”, <https://en.wikipedia.org/wiki/Stablecoin> , (Erişim:30.12.2020).

güvenlik korumalarına sahip olması gerektiğini ve barındırılmamış cüzdan kullanan kişilerin dâhil, işlem yapan tüm tarafların kimliklerini elde etmesi ve doğrulaması gerektiği de ifade edildiği belirtilmektedir. Trump tarafından atanan bir düzine yönetici tarafından yeni yayınlanan belgenin üzere uzun süreli finansal kuralların kripto endüstrisinin artan popülaritesine uygulanması için yönetimin yaptığı en son hamle olduğu değerlendirilmektedir. Trump'ın kripto para birimleri ile ilgili sert duruşunun 2019 Haziran ayında Libra stablecoini başlatma niyetinde olan Facebook dahil birçok yöneticiyi için hayal kırıklığına uğrattığı ifade edilmektedir. Stablecoinlerin normal olarak ABD Doları gibi fiat paraya sabitleştirildiği belirtilmektedir. Stablecoinlerin düşük oynaklıkları sebebiyle sıklıkla yatırımcılar tarafından sanal işlemlerle hızlı bir şekilde Bitcoin gibi kripto varlığı satın alabilmek için kullanıldığı ifade edilmektedir. Tether'in (değeri ABD Dolarına sabitlenmiş stablecoin) dünya çapında tahmini %75 Pazar payı ile kripto borsası tarafından kullanılan önde gelen bir stablecoin olduğu belirtilmektedir. Circle ve Coinbase tarafından işletilen ve yönetilen USD coin, New York Eyaleti Finansal Hizmetler Departmanı tarafından onaylanan Paxos Standar ve Winklevoss tarafından işletilen Gemini Dollar diğer popüler stablecoinler için örnek olarak ifade edilmektedir.¹⁵⁰

ABD istihbarat topluluğunun ABD Menkul Kıymetler ve Bors Komisyonu ile birlikte yaptıkları Çin Komünist Partisinin dijital para birimleri üzerindeki etkisi ile ilgili çalışmada endişelerinin arttığını ifade ettikleri belirtilmektedir. Kripto para birimi, merkez bankası dijital para birimi ve e-cash'in dünya ekonomisinin liderliği için Pekin'e karşı çok cepheli bir küresel rekabete çekildiği ifade edilmektedir. Trump yönetiminin beşinci nesil kablosuz teknoloji pazarının çoğuna hâkim olmayı başaran Çin'li Telekom devi olan Huawei şirketine olan tavrının da raporda hatırlatıldığı belirtilmektedir. Bu arada uzmanların ve sektör liderlerinin görüşüne göre Çin'in dijital para birimi yarışında ABD'yi geride bırakabileceği de ifade edilmektedir. Ulusal İstihbarat Direktörü John Ratcliffe'ın ABD Menkul Kıymetler ve Bors Komisyonu Başkanı Jay Clayton'a 2020 yılının Kasım ayı başında bir mektup yazdığı belirtilmektedir. Mektupta ABD'nin Çin'in dijital para üzerindeki etkisinden

¹⁵⁰ Nicholas Otieno, "U.S. Financial Regulators Warn Crypto Firms to Tighten Stablecoin AML Risk Controls", 21.12.2020, <https://blockchain.news/news/u.s.-financial-regulators-warn-crypto-companies-on-stablecoins-risks> (Erişim:28.12.2020).

bahsedildiği ve dünyanın yarısından fazla kripto para madencilik operasyonlarının bu ülkede yapıldığı ve Çin hükümetinin kendi devlet kontrollü dijital para birimlerini nasıl yorumladığı ve bu durumun ABD’li inovasyon ve şirketlerin rekabeti için zor olması sebebiyle endişe duyduklarının belirtildiği ifade edilmektedir. Başkan Clayton’un dijital varlıklar ve dijital ödeme alanlarında ABD yatırımcı koruması ve kara para aklamayı önleme kanunları ile uyumlu yenilikleri teşvik etmekte kararlı olduğu belirtilmektedir. Kasım ayının başlarında Trump’ın ABD’deki herhangi biri ile Çin Halk Kurtuluş Ordusu’na bağlı birçok şirket arasındaki işlemleri yasakladığını duyuran bir başkanlık emri yayınladığı ifade edilmektedir. Yayımlanan bu emirde Çin’in kendi askeri gelişimi ve modernizasyonunu finanse etmek için ABD’li yatırımcıları kullandıkları konusunda uyarıların yer aldığı belirtilmektedir. Bu başkanlık emrinin ayrıca Çin ile bağlantısı bulunan dijital para birimi şirketlerine de uygulanabileceğinin belirtildiği ifade edilmektedir. Üst düzey bir istihbarat şefinin Çin kontrolündeki Bitcoin ve Ethereum ile ilgili birçok ulusal güvenlik endişeleri olduğunu ifade ettiği de belirtilmektedir.¹⁵¹

1.9.1.4. Kanada

Kanada’lı kanun yapıcılar sanal para politikasına karşı öncelikle kara para aklama endişelerine odaklanan “düzenleme ve kucaklama” şeklinde bir yaklaşım sergilemektedirler. Sanal paralar Kanada’da yasal ödeme aracı değildirler. 2013 yılının başlarında Kanada Gelir Kurumu mal veya hizmetlerde Bitcoin kullanımına takas işlem kurallarının ve vergi düzenlemelerinin uygulandığını ifade etmişlerdir. Bununla birlikte Bitcoin’in bir varlık olarak alımı veya satımının sermaye kazancı vergisine tabi olduğu da belirtilmektedir. 2014 yılında Kanada kara para aklama karşıtı yasaları, Kanada’nın kara para aklama ve teröristlerle mücadele finansman rejimlerine tabi kılan para hizmetleri işletmeleri olarak sanal paralarla uğraşan kişileri belirleyebilmek için değiştirilmiştir. Bu yasa Kanada’da sanal paralarla ilgilenen işlerle uğraşan kişileri ve bunun yanı sıra Kanada’daki müşterilerine bu hizmeti sağlayan Kanada dışındaki kişilere uygulanmaktadır. 2017 yılının başlarında Kanada Menkul Kıymetler İdaresi

¹⁵¹ Jerry Dunleavy, “Trump spy chief seeks SEC scrutiny of Chinese dominance in cryptocurrency”, (24.11.2020), <https://www.washingtonexaminer.com/news/trump-spy-chief-seeks-sec-scrutiny-of-chinese-dominance-in-cryptocurrency> (Erişim: 28.12.2020).

(CSA), işletmelerin yeni finansal ürünleri, hizmetleri ve uygulamaları test etmeleri için bir düzenleme alanı başlatmıştır. CSA Başkanı ve Autorite des Marchés Financiers'ın Başkanı ve CEO'suna göre bu yeni girişimin amacının yeniliği desteklemek ve teşvik etmek olduğu belirtilmektedir. CSA Başkanı bu programın, çevrimiçi kitle fonlaması ve borç verme portalları, alım satımlar veya tavsiyeler için yapay zekâ ve dağıtık muhasebe defteri teknolojilerine sahip girişimleri içeren iş modellerini göz önünde bulunduracağını ifade etmiştir. Ayrıca İngiltere'nin Mali İşbirliği Kurumu ile finansal teknoloji firmalarının birbirlerine yardımcı olması ve birbirlerinin pazarlarında genişleyebilmesi için bir anlaşma imzalandığı da belirtilmektedir. 2017 yılı kasım ayında Kanada Bankası bir merkez bankasının herkes tarafından kullanılabilecek bir merkez bankası dijital parasının çıkarmasının (CBDC) gerekip gerekmediği ile ilgili bir tartışma belgesi yayınlamıştır. Potansiyel risk ve faydaları ile birlikte banka, perakende ödemelerde sürekliliği artıracığı için CBDC'yi çıkarmanın en güvenilir motivasyon olduğu, istenmeyen tam anonimlik durumunun suç işlemesini teşvik edebileceği, sanal para birimi ihracını düşünen bankaların temkinli ve değişen artımsal bir davranış sergilemesi gerektiği konularıyla ilgili birkaç sonuca ulaşmıştır.¹⁵²

Kanada 2014 yılında kara para aklama ve terörizm finansmanı ile mücadele mevzuatına sanal para ile ilgili ticari faaliyette bulunan kişi veya teşebbüsleri de içerecek şekilde düzenleme yapmıştır.¹⁵³

1.9.2. Avrupa Kıtası

1.9.2.1. Fransa

2013 yılının Aralık ayında Fransa Merkez Bankası sanal paraların güvenlik riski oluşturabileceği, merkezi bir düzenleme otoritesinin yokluğunun spekülasyon ve dalgalanmaya neden olabileceği, yasal risklerin olduğu ve sanal paraların yasa dışı faaliyetlerde kullanılabileceği ile ilgili uyarıda bulunmuştur. 2014 yılının başlarında Fransa Ekonomi Bakanlığı sanal paralardan gelen gelirlerin vergilendirilebilir gelir

¹⁵² Department of Finance, “*Virtual Currencies and Blockchain Technology*”, s.7-8.

¹⁵³ Financial Action Task Force, (2015), Guidance For a Risk-Based Approach to Virtual Currencies, s.16.

olduğunu belirtmiştir. Fransa Bankacılık Federasyonu sanal paraların satışından elde edilen kişisel banka hesabına yapılan havale gelirlerinin bankaya Fransız kara para aklama kurumundan alınan bir belge ile dosyalanması gerektiğini belirtmiştir. Aynı yıl finans üzerine bir Fransa Senatosu komitesi sanal paraların gelişmesiyle ortaya çıkan sorunlar hakkında ifade veren şahitleri dinlediğini ifade etmiştir. Komite uzun vadeli eğilime sahip sanal paralarının yükselişinin kamu otoriteleri tarafından göz ardı edilemeyeceğini belirtmektedir. Komite ayrıca risklerine rağmen blok zincir ve sanal paraların gelecek için çok sayıda fırsatları beraberinde getireceği ve kamu otoritelerinin dengeli bir düzenleyici çerçeve üzerinde çalışılması gerektiğini vurgulamaktadır. 2016 yılı Aralık ayında Fransa Bankası SEPA Kredi Tanımlayıcılarının yönetiminde veya Tekli Avro ödeme alanında alacaklarının kimliğini belirlemek amacıyla hipotetik kullanım için bir blok zincir prototipi olan start-up Labo Blockchain ve Caisse des Depots et Consignation ile birlikte test edildiğini belirten bir basın açıklaması yayınlamıştır. 2017 yılının Ağustos ayında Fransa, bankalara ve finansal teknoloji şirketlerine listelenmeyen menkul kıymetlerin anında işlem görmelerine imkân sağlayan platformlar oluşturmaları için komisyoncular ve saklama bankaları gibi aracılara kesmelerine izin verecek yeni yasalar çıkarmıştır. Fransa Maliye Bakanı listelenmeyen menkul kıymetler için daha hızlı, daha ucuz daha şeffaf ve daha güvenli yeni ticaret platformlarının ve işlemlerin gelişmesine izin verileceği şeklinde bir ifade yayınlamıştır.¹⁵⁴

1.9.2.2. Estonya

2014 yılının başlarında Estonya Merkez Bankası ödeme ve uzlaştırma sistemi Başkanı dağıtık sistemlerin doğası ve potansiyel Ponzi Şemalarını içeren Bitcoin ile ilişkili risklerle ilgili endişelerini dile getirmiştir. Aynı yıl Estonya Vergi Dairesi Bitcoin işlemlerinden elde edilen gelirlerin vergilendirmeye tabi sermaye kazancını oluşturduğunu belirtmiştir. 2015 yılı Kasım ayında Estonya Yüksek Mahkemesi Maliye Bakanlığı, İç İşleri Bakanlığı, Estonya Merkez Bankası ve Estonya Mali Denetim Otoritesi dâhil olmak üzere çeşitli hükümet kurumlarından ve yetkililerinden hükümetin Bitcoin'in yasallığı konusundaki tutumu hakkındaki soruları cevaplamaları

¹⁵⁴ Department of Finance, “Virtual Currencies and Blockchain Technology”, s.8.

için talepte bulunmuştur. 2016 yılının Kasım ayında Estonya Yüksek Mahkemesi Bitcoin'e karşı bir karar vermiştir. Bitcoin ticaretine müşterilerle yüz yüze görüşme ve tüm müşterilerin kimliğinin kopyalarını tutma ve ayda 1.000 Avro'dan fazla işlem yapan kişilerin raporlama gerekliliği şeklinde ekstra düzenlemelerin uygulanmasına karar vermiştir. Bu kural ayrıca Bitcoin ve diğer tüm sanal paralara uygulanmıştır. 2017 yılının Ağustos ayında Estonya devlet tarafından yönetilen Estcoin adında kendi sanal parasını çıkarmayı teklif etmiştir. Fakat Avrupa Merkez Bankası Estonya'nın bu planına karşı eleştiride bulunmuş ve hiçbir üye ülkenin kendi sanal parasını çıkarmasına izin vermeyeceğini ifade etmiştir.¹⁵⁵

1.9.2.3. Lüksemburg

2016 yılının Nisan ayında Lüksemburg Bitstamp'a tamamen düzenlenmiş ve lisanslı Bitcoin alım satımı için lisans vermiştir. Böylece Bitstamp şirketinin dünyada ilk ulusal olarak lisanslı Bitcoin alım satımı yapan bir şirket unvanına sahip olduğu da belirtilmektedir.¹⁵⁶

1.9.2.4. İspanya

Sanal paraların kumar yasaları uyarınca elektronik ödeme sistemi olarak işlem görebileceği ve vergi amaçlı ticaret geliri olarak düşünülebileceği ifade edilmektedir. 2014 yılının Mayıs ayında İspanya Vergi Kurumu (Spanish Tax Agency – AEAT) sanal paraların yasa dışı faaliyetler için kullanılıp kullanılmadığının izlendiğini belirtmiştir. 2014 yılının Eylül ayında ise İspanya Maliye ve Kamu Hizmetleri Bakanlığı Maliye Bölümü, İspanya merkezli açık kaynak kodlu Bitcoin takas platformu olan Coinffeine'nin İspanya'daki Bitcoin tabanlı çevrimiçi kumar şirketlerinin lisans için başvuru yapıp yapmamaları konusundaki sorusu için bir karar vermiştir. 2015 yılının Nisan ayında İspanya Maliye ve Kamu Hizmetleri Bakanlığı Maliye Bölümü (MHAFP) sanal paraların Katma Değer Vergisi'nden (VAT) muaf olduğu onaylamıştır. MHAFP'nin Bitcoin'in para transferini sağlayan ödeme

¹⁵⁵ Age, s. 9.

¹⁵⁶ Age, s.10.

sistemleri ile bağlantılı “finansal hizmet” tanımı, Bitcoin transferlerinin “özel risk” faaliyetleri varsayımı yani diğer bir ifadeyle sanal paralarla işlem gören tüm İspanya şirketlerinin kara para aklama karşısı (Anti Money Laundering – AML) kurallara uyması gerektiği anlamına gelmektedir. 2016 yılında İspanya Vergi Kurumu madencilik faaliyetlerinin vergilendirilebilir bir faaliyet olduğunu açıklamıştır. Bu yeni yönergede tüm sanal para madencilerinin madencilikten elde ettikleri kazançların vergilerini vermeden önce İspanya otoritelerine kendilerini kaydettirmeleri gerektiği ifade edilmektedir. Kara para aklama, vergi kaçakçılığı ve siber suç faaliyetlerine potansiyel bağlantı oluşturmalarını ve fidye yazılımı gibi araçların kontrol altına alınması bu mevzuatın ana nedenlerini oluşturduğu belirtilmektedir. İspanya Maliye Bakanlığı yeni vergi kurallarının uygulanmasından sorumlu olduğu ve sanal para uzmanından danışmanlık hizmeti alınması konusunda da yetkili bir makam olduğu ifade edilmektedir. İspanya Bankası sanal paralar için uygun yasal bir çerçeve sağlamanın önemini açıkça ifade etmiş olsa da ICO’larla ilgili herhangi bir kapsamlı kural veya kılavuz yayınlanmamıştır. Bu doğrultuda İspanya’daki ICO’larla ilgili herhangi bir faaliyetin ödeme hizmetleri ve kara para aklama düzenlemeleri tarafından (Avrupa Birliği Direktifleri kapsamında) dikkatli bir şekilde değerlendirilmesi gerektiği ifade edilmektedir.¹⁵⁷

1.9.2.5. İsviçre

İsviçre sanal paraları diğer birçok küresel savunucular gibi aynı şekilde düzenleyici olmayan bir yaklaşım olarak benimsemeye karar vermiştir. İsviçre Federal Konseyi sanal paralarla ilgili şu anda düzenleme gerektiren bir durum olmamasına rağmen sanal paraların menkul kıymetler olarak statüsünü ve buna karşı gelen vergilendirme durumlarını belirlemek için finansal sektörün bunları nasıl kullanacağı ile ilgili yasalar üzerinde çalıştığını belirtmiştir. İsviçre kar amacı gütmeyen ve yeni blok zincir teknolojisinin İsviçre ekosistemine dahil edilmesini sağlamak için tasarlanmış bir kuruluş olan Crypto Valley Association gibi hızla gelişen blok zincir start-up çevresine ev sahipliği yapmaktadır. İsviçre’de ulaşım ücretleri ve diğer belediye ücretleri Bitcoin ile ödenmektedir.

¹⁵⁷ Age, s.11.

2017 yılının sonlarında İsviçre'nin Finansal Denetim Otoritesi (Swiss Financial Market Supervisory Authority – FINMA) ICO üzerine bir kılavuz yayınlamıştır. Bununla birlikte FINMA birçok ICO'yu, ICO'yu geliştirenlerin mevcut düzenlemeleri ihlal edip etmediğini de araştırmaktadır.¹⁵⁸

FINMA kripto bankacılık lisansı ile faaliyet gösteren İsviçre Bankası SEBA Bankasının 19 Kasım 2020 tarihinde yayınladığı bir duyuruya göre, dijital ekosistemine Bitcoin Cash ve USD Coin olmak üzere iki yeni kripto parayı dahil edeceği belirtilmektedir.¹⁵⁹

3 Aralık 2020 tarihinde yayınlanan bir habere göre İsviçre merkez bankasının ülkenin ana borsasında işlemlerin anında gerçekleşmesi için Frangın dijital versiyonu üzerindeki denemelerinin başarılı bir şekilde tamamlandığı belirtilmektedir. Fakat İsviçre Ulusal Bankası'nın (Swiss National Bank – SNB) bu projeyi hayata geçirip geçirmeyeceği konusunda henüz bir karar vermediği de ifade edilmektedir. Test koşullarında İsviçre Ulusal Bankası'nın menkul kıymetlerin alım satım işlemlerinde kullanılmak üzere bir merkez bankası dijital para birimi oluşturduğu belirtilmektedir.¹⁶⁰

1.9.2.6. Birleşik Krallık

Birleşik Krallık sanal paraların ilk destekçilerinden biri olarak belirtilmektedir. 2013 yılı Haziran ayında İngiltere Gelir ve Gümrük İdaresi (HM Revenue & Customs – HMRC) sanal paralara Birleşik Krallık vergi mevzuatının uygulandığını ve herhangi biri tarafından bir mal veya hizmet alımında kullanıldığında o kişinin bir tüccar olduğu kabul edildiği ve bu nedenle sanal paraların vergilendirildiği ifade edilmektedir. 2014 yılının Ocak ayında HMRC, Bitcoin'i sermaye kazancı vergisine tabi tutulmadan özel para olarak sınıflandırmayı dikkate almıştır. Aynı yılın Ocak ayında Mali Tutum

¹⁵⁸ Age, s.11.

¹⁵⁹ Zug, “SEBA adds Bitcoin Cash and USD Coin to its Digital Ecosystem”, 19.11.2020, <https://www.seba.swiss/media-and-investors/bitcoin-cash-and-usd-coin-added-to-digital-ecosystem/> , (Erişim:20.01.2021).

¹⁶⁰ Gaetan Bally, “Swiss central bank trials new type of digital currency”, 03.12.2020, <https://www.swissinfo.ch/eng/swiss-central-bank-trials-new-type-of-digital-currency/46200862> (Erişim: 20.01.2021).

Otoritesi (Financial Conduct Authority – FCA), FCA Innovate oluşturarak, İngiltere’de Fintech ve RegTech girişimlerini desteklemiştir. Bu oluşum ayrıca blok zincir gibi bazı özel konularda araştırma yazıları da hazırlamaktadır. 2015 yılının Mart ayında Birleşik Krallık Hazine Kurumu Bitcoin alım satım borsalarının kara para aklama karşıtı düzenlemelerle birlikte düzenlenme planları olduğunu duyurmuştur. Bu yıldan sonra Birleşik Krallık Hazine Kurumu kara para aklama ve terörist finansmanı ile ilgili bir risk değerlendirmesi raporu yayınlamıştır. Bu rapora göre çevrimiçi piyasalarla ilgili yasa dışı işlem faaliyetlerinin büyük bir kısmının kara para aklama faaliyetlerinden çok madde ve ateşli silahların satın alınmasından kaynaklandığı ifade edilmektedir. 2016 yılının Nisan ayında HRMC, Bitcoin ve diğer sanal paralarla ilgili işlemlere katma değer vergisinin uygulanabilirliği için şu şekilde ek açıklamalar yayınlamıştır:

- Bitcoin madenciliği faaliyetlerinden elde edilen Bitcoin’in katma değer vergisi için bir ekonomik faaliyeti oluşturmadığı için katma değer vergisinin dışında tutulacağı
- Madenciler ve diğerleri tarafından belirli Bitcoin işlemlerinin yapılması için yapılan ödemelerin katma değer vergisinden muaf tutulacağı
- Bitcoin mal ve hizmetlerin alım satımında kullanılması durumunda Bitcoin’in kendi değerinden hiçbir katma değer vergisi alınmayacağı

Aynı yılın Aralık ayında Birleşik Krallık devlete ait olan Royal Mint Kurumu yeni bir altın ticaret sistemini yürütmek için blok zincir teknolojisini kullanmayı planladıklarını duyurmuştur. Bu projenin yatırımcıların blok zincir üzerinde 1 Milyar Dolar değerinde altına erişimi ile müşterilerin Royal Mint Gold (RMG) adında sanal tokenler kullanarak Royal Mint’in kasalarında depolanan altın paylarını almaları ve ticaretini yapmalarına imkân sağlayacağı ifade edilmektedir. Her bir RMG’nin 1 gram altına eş değer olacağı belirtilmektedir. 2017 yılının başlarında İngiltere Merkez Bankası Başkanı, finansal teknoloji sektörünün finansal hizmetler kurumları gibi aynı seviyede düzenlemeye ihtiyacı olmadığını ifade etmiştir. Yine aynı yıl Londra Menkul Kıymetler Borsası, menkul kıymetler sertifika verilerini dijitalleştirmek için IBM ile bir blok zincir modeli geliştirilmesi için ortaklık yaptıklarını duyurmuştur. 2017 yılı sonunda FCA, müşterilerine sanal para sözleşmelerine yatırım yapmanın riskleri hakkında bir uyarıda bulunmuştur. Bu riskler şu şekilde ifade edilmektedir:

- Fiyat oynaklıkları
- Yatırımcının uğradığı kayıpların potansiyel çarpımı
- Ücretler
- Fiyat şeffaflığının olmaması

FCA ayrıca ICO'larla ilgili ICO'ların çok yüksek riske sahip olduğu, spekülative bir yatırım aracı olduğu ve yatırımcıların bu risklerin bilincinde olması gerektiği ve bu özel projenin kapsamlı bir şekilde araştırılması gerektiği ile ilgili bir uyarı yayınlamıştır. 2018 yılının Ocak ayında İngiltere Merkez Bankası merkez bankası tarafından dijital para birimi ihraç etmeyi planlamadıkları açıklanmıştır.¹⁶¹

Blok zinciri ve kripto para ekosistemi geliştikçe Londra'nın gelişmekte olan bu endüstrinin küresel merkezi haline gelme olasılığının arttığı belirtilmektedir. güçlü bir yargılama sistemi, iyi niyetli düzenlemeler, sermayeye erişim ve küresel bankacılık sisteminin Birleşik Krallık'ı Kanada ve Avustralya'nın yanı sıra blok zinciri ve kripto girişimcileri için cazibe oluşturduğu ifade edilmektedir. Girişimlerin bir gecede bir merkezden başka bir merkeze taşınabilmesi ihtimali söz konusu olduğu için, doğru düzenleyici çerçevenin şekillendirilmesinin hayati bir önem taşıdığı da vurgulanmaktadır.¹⁶²

23 Ekim 2020 tarihinde yayınlanan bir habere göre, San Francisco merkezli Ripple şirketinin ABD düzenleyici çevresi SEC ile yaşadığı sıkıntı sebebiyle şirket merkezini yurt dışına taşıma kararı aldığı ve bu kapsamda gerçekleştirdiği Londra ziyareti sonrasında CEO'su Brad Garlinghouse İngiltere'nin Mali Tutum Otoritesi'nin XRP kripto para birimini bir menkul kıymet olarak görmediğini ifade ettiği belirtilmektedir. XRP'nin bir menkul kıymet olmadığı ve bir para birimi olarak kullanıldığının makamlarca kabul edilmesinin Ripple için Birleşik Krallık'ta faaliyet göstermesi için bir avantaj olduğu da CEO tarafından ifade edilmektedir.¹⁶³

Diğer taraftan Ocak 2021'de yayınlanan bir habere göre de Birleşik Krallık Mali Tutum Otoritesi tarafından önerilen değişiklikler sonrasında 6 Ocak 2021

¹⁶¹ Age, s.11-12

¹⁶² Benjamin Yablon, "Why London Is Becoming a Global Blockchain Hub", 28.08.2018, <https://www.entrepreneur.com/article/318570> , (Erişim:19.01.2021).

¹⁶³ Ryan Browne, "\$10 billion crypto firm Ripple considers relocating to London over U.S. regulation", 23.10.2020, <https://www.cnbc.com/2020/10/23/crypto-firm-ripple-considers-relocating-to-london-over-us-regulation.html> , (Erişim:20.01.2021).

tarihinde belirli türdeki kripto varlıkların ve türevlerinin ve borsada işlem gören senetlerin (Electroneum – ETN) tüketicilere perakende satışının resmi olarak yasaklandığı belirtilmektedir. FCA'nın, kripto para ve türevlerinin fiyat hareketlerindeki dalgalanma, piyasa suistimali, mali suçlar ve sektördeki dolandırıcılıklar gibi çeşitli nedenler belirterek bu ürünlerin tüketiciler için uygun olmadığını ifade ettiği belirtilmektedir.¹⁶⁴

1.9.2.7. Belçika

2013 yılında Belçika Finans Bakanı Koen Geens, Belçika Ulusal Bankası'nın Bitcoin'i yasaklama niyetinin olmadığını ve bankanın sanal paraların kara para aklama faaliyetlerinde kullanıldığına dair herhangi bir delil olmadığını belirtmiştir. 2014 yılı başlarında Belçika Ulusal Bankası ve Belçika Finansal Hizmetler ve Pazar Otoritesi (FSMA), sanal paralara karşı yatırımcılara ortak bir uyarıda bulunmuşlardır. Uyarı sanal paraların bir merkez bankası tarafından ihraç edilmediği, düzenlenmediği ve güvenlik, hacklenme ve dolandırıcılık gibi risk taşıdıkları ve değer oynaklığından dolayı da yasal ödeme aracı olmadığı şeklinde belirtilmektedir. 2017 yılı Mayıs ayında şimdi Adalet Bakanı olan Belçika Finans Eski Bakanı Koen Geens sanal paraları finansal hizmet sektörüne uyarlamak için aynı katı düzenlemeye tabi tutma niyetini açıklamıştır. Aynı yılın Haziran ayında Ulusal Belçika Bankası sanal paraların para politikasına yönelik tehdidi üzerine bir rapor yayınlamıştır. Raporda özel oyuncular tarafından çıkarılan sanal paraların parasal istikrar üzerindeki herhangi bir tehditin bu noktada oldukça sınırlı olduğu sonucuna varıldığı ifade edilmektedir.¹⁶⁵

¹⁶⁴Charlie Osborne, “UK ban on cryptocurrency derivatives, ETNs comes into force today”, 06.01.2021, [https://www.zdnet.com/article/uk-ban-on-cryptocurrency-derivatives-comes-into-force-today/#:~:text=The%20ban%20has%20now%20become,crypto%20assets%20to%20retail%20consumers.%22&text=The%20value%20of%20these%20products,%20or%20Ethereum%20\(ETH\)](https://www.zdnet.com/article/uk-ban-on-cryptocurrency-derivatives-comes-into-force-today/#:~:text=The%20ban%20has%20now%20become,crypto%20assets%20to%20retail%20consumers.%22&text=The%20value%20of%20these%20products,%20or%20Ethereum%20(ETH)) , (Erişim: 20.01.2021).

¹⁶⁵ Department of Finance, “Virtual Currencies and Blockchain Technology”, s.13.

1.9.2.8. *Danimarka*

2013 yılında Danimarka Finansal Denetim Otoritesi (Financial Supervisory Authority – FSA), sanal para yatırımlarının riskleri ile ilgili bir uyarı yayınlamıştır. Bu uyarıda şu maddeler yer almaktadır:

- Borsalarda para kayıpları
- Sanal cüzdan hırsızlıkları
- Fiat para birimine dönüştürememe olasılıkları
- Hızlı fiyat dalgalanmaları
- Suç faaliyetleri için potansiyel bağlantı oluşturmaları

FSA, sanal paraların, elektronik para, döviz borsası, aracılık veya mevduat hizmetleri için geçerli olan mevcut düzenleme çerçeveleri kapsamında olmadığını yinelemiştir. 2014 yılı Mart ayında Danimarka Merkez Bankası sanal Bitcoin'in para birimi olmadığını belirten bir açıklama yayınlamıştır. Banka ayrıca Bitcoin'in altın ve gümüş ile karşılaştırıldığında gerçek bir alım satım değerine sahip olmadığını bu nedenle Bitcoin'in daha çok “cam boncuk”a benzetilebileceğini ifade etmiştir. Danimarka Merkez Bankası açıkça Bitcoin'in mevduat garantisi gibi garantilerle veya ulusal yasalarla korunmadığının altını çizmiştir. Aynı ay Danimarka Vergilendirme Kurulu, Bitcoin'in vergi ve KDV amaçlı bir resmi para birimi olarak değerlendirilemeyeceği ile ilgili bir karar çıkarmıştır. Bununla birlikte Bitcoin'in değerindeki dalgalanmalar para birimi üzerindeki kazançlar ve kayıplar olarak borç ve Alacaklara İlişkin Sermaye Kazançları ve Kayıpları Vergi Kanunu kapsamında vergilendirilmediği ifade edilmektedir. 2017 yılının Aralık ayında Danimarka Ulusal Bankası merkez bankasının ihraç ettiği bir sanal para olan “krone”un faydaları ve uygun olup olmadığı ile ilgili bir çalışma yayınlamıştır. Bu çalışma bir merkez bankası dijital para biriminin Danimarka'daki mevcut ödeme çözümleri kapsamında bir gelişme olmayacağı sonucuna varmıştır. Merkez bankası dijital para biriminin Danimarka Ulusal Bankasının finansal sistem içerisindeki rolünü tamamen değiştireceği ve onu ticari bankalara doğrudan rakip yapacağı ifade edilmektedir. Merkez bankası dijital para biriminin tanıtılmasının potansiyel faydalarının Danimarka'daki haneler ve işletmeler için önemli derecede zorluklarla eşleşmeyeceği ifade edilmektedir. Bu nedenle Danimarka Ulusal Bankası merkez bankası dijital para birimi çıkarma planları

olmadıkları açıklamıştır. Finansal Hizmetler Otoritesi ve Danimarka Hükümeti Bitcoin ile ilgilenen tüm işletmelerin vergi ödemek zorunda olacaklarını ve mevcut yasalardaki bu değişikliklerin Bitcoin dâhil tüm sanal paraları düzenlemek için gerekli olacağını açıklamıştır.¹⁶⁶

1.9.2.9. Finlandiya

2012 yılı başlarında bir televizyon röportajı sırasında Finlandiya Merkez Bankası Başkanı Bitcoin'lerin yasal olduğunu ve yatırım amaçlı kullanılabileceğini belirtmiştir. Herhangi bir garantisi olmasa da düzenlemeye tabi olmayan sanal paraların fiat para birimi cinsinden takasının yapılabileceği ifade edilmiştir. 2013 yılında Finlandiya vergi Otoritesi Bitcoin ile ilgili vergi yorumları yayınlamıştır. 2014 yılının Kasım ayında ise Finlandiya Merkez Vergi Kurulu Bitcoin'i bankacılık hizmetlerine yakın finansal hizmetler olarak değerlendirmiş ve 034/2014 yasası gereği de Bitcoin'i Avrupa Birliği KDV direktiflerine göre muaf tutmuştur. 2017 yılı Kasım ayında Finlandiya'nın Finansal Denetim Otoritesi (Finnish Financial Supervisory Authority – FSA) ICO'lar ve sanal paraların riskli ve yüksek spekülasyon yatırım olduğu ile ilgili uyarılarda bulunmuştur. FSA, ayrıca müşterilerini Bitcoin ve diğer sanal paraların değer istikrarsızlığı ile ilgili Avrupa Birliği Bankacılık Otoritesi tarafından 2013 yılında yayınlanan sanal paraların riskleri raporuna atıfta bulunarak uyarmıştır. FSA, token satışlarıyla ilgili dolandırıcılık, sermaye kayıpları, değer dalgalanmaları, yetersiz bilgi ve teknoloji riskleriyle gibi birkaç riski listelemiştir.¹⁶⁷

1.9.2.10. Almanya

Sanal paraların Alman yasalarına göre finansal araçlar olduğu ve özellikle “özel para” formunda sermaye olarak vergilendirilebileceği ifade edilmektedir. Bazı kullanımlarının lisans veya izin gerektireceği de belirtilmektedir. Alman finansal denetim otoritesinin daha önceki kılavuzlarında sanal paraların emtia olduğu ve hem Bitcoin satışın hem de Bitcoin karşılığı mal satışı sırasında vergilendirmeye tabi

¹⁶⁶ Age, s.14.

¹⁶⁷ Age, s.14.

olduğu ifade edilmektedir. 2011 yılı başlarında Almanya finansal denetim otoritesi (BaFin) Bitcoin'in yasal ödeme aracı olmamasından dolayı elektronik para tanımından muaf olduğu belirtilmiştir. Bunun yerine vergilendirmeye tabi tutulan emtia olarak işlem gördüğü ifade edilmektedir. 2013 yılının yaz aylarında Almanya Maliye Bakanlığı sanal paraların elektronik para veya yabancı ülke parası olmadığını fakat Alman bankacılık yasalarına göre finansal bir araç olduğunu ifade etmiştir. Sanal paralar bu nedenle "özel para"ya benzer şekilde sermaye olarak vergilendirilebilir olacağını belirtmiştir. 2017 yılında Avusturya ve Alman hükümetleri sanal paraların organize suç faaliyetlerinde kullanımı ile ilgili araştırma çalışmalarına fon ayırmaya karar vermiştir. 2017 yılının sonlarında BaFin, ICO'ları sermaye piyasası düzenlemelerine tabi olmayan yüksek spekülasyon yatırım aracı olarak tanımlamakta ve müşterilerine ICO'ların riskleri ile ilgili uyarılarda bulunmuştur.¹⁶⁸

1.9.2.11. Polonya

Polonya Lodz Eyalet Ofisi Vergi Dairesi madencilik yoluyla elde edilen Bitcoin'lerin satışının Bitcoin madenciliğinin belirli bir hizmet ücretine sahip olması düşüncesiyle % 23 oranında Polonya katma değer vergisine tabi olduğunu bir görüş vermiştir. Polonya'nın Sanal İşler Bakanlığı 2016 yılının Haziran ayında nakitsiz çözümlerin geliştirilmesi ve elektronik tanımlamaların uygulanması gibi sanal kamu hizmetlerini teşvik etmek için geniş bir dijitalleşme planını duyurmuştur. Aynı yıl Maliye Bakanlığı sanal paraların Polonya yasalarına göre herhangi bir ayrı düzenlemeye tabi olmamalarına rağmen Polonya'da kullanımlarının tamamen yasal olduğunu ve gelir vergisine tabi olduklarını belirtmişlerdir. Polonya'nın Merkezi İstatistik Ofisi (Central Statistical Office – GUS) 2017 yılının başlarında sanal paraların madencilik faaliyetleri ve alım satım işlemlerinin resmi ekonomik faaliyet olarak tanındığını belirtmiştir. Bu durum ülkedeki sanal paraların ilk düzenlenmesi olarak ifade edilmektedir.¹⁶⁹

27 Kasım 2020 tarihinde yayınlanan bir habere göre, Polonya'nın Olsztyn kentinin acil durum hizmetlerinin sağlanmasına yardımcı olmak için Ethereum'un blok zincirinden

¹⁶⁸ Age, s.15.

¹⁶⁹ Age, s.15.

yararlanan dağıtık defter teknolojisinin somut kullanım örneği olarak dünyadaki ilk şehir olduğu ifade edilmektedir. Olsztyn'nin polis, itfaiye ve ambulans hizmetlerine yardımcı olmak için blok zincirini fiziksel varlıklarla birleştiren bir köprü teknolojisi olan Smartkey'in başarılı deneme çalışmasını tamamladığı belirtilmektedir. Smartkey'in yerel kurtarma ekipleri tarafından kullanılan Teltonika akıllı cihazlarına akıllı bir sözleşme bağlanmasıyla işlerini daha verimli bir şekilde gerçekleştirmelerine olanak sağlayacağı ifade edilmektedir. Bu bağlantının acil durum ekiplerinin şehirdeki herhangi bir binaya izin beklemeye gerek kalmadan veya anahtar sahibinin izini sürmek zorunda kalmadan girmelerini sağladığı belirtilmektedir.¹⁷⁰

1.9.2.12. İsveç

İsveç Vergi Ajansı 2014 yılında resmi olarak sanal paraların sanat eseri veya antika gibi bir varlık olduğunu ama para birimi olmadığını ifade etmiştir. Bu yılın sonunda İsveç Merkez Bankası sanal paraların perakende ödeme piyasalarını etkileyip etkilemediği ile ilgili bir rapor yayınlamıştır. Bu kurum 2015 yılında ise bazı Bitcoin madencilik faaliyetlerinden elde edilen gelirlerin istihdamdan elde edilen gelirler olarak değerlendirilebileceğini ifade etmiştir. İsveç'in Merkez Bankası 2016 yılı sonlarında toplumu tarafından önemli derecede nakit kullanımında azalma ile karşı karşıya kalmıştır. Bu nedenle bir merkez bankasının desteklediği dijital para biriminin toplum tarafından nasıl görüneceği ve hangi zorlukları beraberinde getireceği ile ilgili bir proje başlattığını duyurmuştur.¹⁷¹

11 Aralık 2020 tarihinde yayınlanan bir habere göre İsveç hükümeti, Uluslararası Ödemeler Bankası'nın 2018 yılında dünyanın en nakitsiz toplumu olarak nitelendirdiği İsveç'in dijital para birimine geçilmesi için gerekli çalışmaların başlatılacağı ve fizibilite çalışmalarının 2022 yılının Kasım ayında tamamlanacağı belirtilmektedir. Haberde ayrıca İsveç'in dijital para birimini sunmayı düşünen dünyadaki ilk ülkelerden birisi olarak ifade edilmektedir. İsveç Merkez Bankası'nın

¹⁷⁰ Sam Bourgi, "Polish city becomes first to adopt Ethereum blockchain for emergency services", (27.11.2020), <https://cointelegraph.com/news/polish-city-becomes-first-to-adopt-ethereum-blockchain-for-emergency-services>, (Erişim: 20.01.2021).

¹⁷¹ Department of Finance, "Virtual Currencies and Blockchain Technology", s.16.

Accenture Plc ile birlikte hâlihazırda blok zinciri teknolojisine dayanan elektronik kron pilot projesini yürüttüğü de belirtilmektedir.¹⁷²

1.9.2.13. İzlanda

İzlanda hükümeti Döviz Yasası'na göre sermayenin ülkeden kaçmasından endişe ederek 2013 yılı başlarında Bitcoin'i yasaklamıştır. 2014 yılında İzlanda'da Bitcoin'e alternatif olarak Auroracoin ortaya çıkmıştır. Bitcoin gibi Auroracoin de anonim bir kişi veya gruplar tarafından geliştirilmiştir. Auroracoin Bitcoin'in ortaya çıkış metodolojisini takip etmiş ve Litecoin tabanlı bir iş ispatı algoritması kullanmıştır. İzlanda finansal krizin ortaya çıktığı 2008 yılında getirdiği sermaye kısıtlamasını 2017 yılının Mart ayında kaldırmıştır.¹⁷³

1.9.3. Orta Doğu ve Kuzey Afrika

1.9.3.1. İsrail

Merkez Bankası ve Maliye Bakanlığı 2014 yılında sanal paraların kullanımına karşı Avrupa Bankacılık Otoritesi'ne benzer şekilde uyarılarda bulunmuştur. Bu uyarılar sanal paraların yasal ödeme aracı olmadığını belki dalgalanmaya maruz kalabileceği kara para aklama veya terörist finansmanı gibi faaliyetlerde kullanılabileceği ile ilgili uyarıları kapsamaktadır. İsrail hükümeti 2017 yılının Aralık ayında sanal paraları maddi veya maddi olmayan varlıklar gibi kategorize ederek Bitcoin satışlarına sermaye kazancı vergisi uygulayacağını açıklamıştır. İsrail Vergi Otoritesi (Israel Tax Authority – ITA) Bitcoin ve Litecoin gibi sanal paraları içeren faaliyetlerle ilgili olarak elde edilen gelirlerin vergilendirilmesini düzenleyen bir genelge taslağı yayınlamıştır. Sanal para madenciliği veya satışı ile ilgilenen bireylerin iş vergi oranlarına tabi olacakları belirtilmektedir. Bununla birlikte Bitcoin'in herhangi bir ticari satışı veya

¹⁷² Rafaela Lindeberg ve Ott Ummelas, “Sweden Explores Moving to a Digital Currency”, 11.12.2020, <https://www.bloomberg.com/news/articles/2020-12-11/sweden-explores-the-feasibility-of-moving-to-a-digital-currency> , (Erişim: 20.01.2021).

¹⁷³ Department of Finance, “Virtual Currencies and Blockchain Technology”, s.17.

alım satım işlemlerinin katma değer vergisine (KDV) tabi olacağı ifade edilmektedir.¹⁷⁴

1.9.3.2. Mısır

Mısır Merkez Bankası, 2018 yılının Ocak ayında aşırı yüksek riski nedeniyle Bitcoin gibi kripto paraların alım satımı işlemlerine karşı bir uyarı yayınlamıştır. Merkez Bankası ayrıca ticaretin sadece banka tarafından onaylanan kâğıt para birimleri ile sınırlı olduğunu belirtmektedir. Diğer taraftan Mısır Fetva Kurumu, Bitcoin ile gerçekleştirilen işlemlerin İslam Hukuku açısından uygun olmadığını belirterek haram olarak değerlendirildiği yönünde de fetva vermiştir. Ayrıca merkezi finansal sistemlere zarar verebileceği ve terörün finansmanında kullanılabileceği de belirtilmektedir.¹⁷⁵

1.9.4. Merkez Asya

1.9.4.1. Kazakistan

2014 yılı başlarında Kazakistan'ın mali kuruluşlarının ülkenin Merkez Bankası tarafından Bitcoin kullanmaları yasaklanmıştır. Ülkede kara para aklama ile mücadele etmek için yasalar bulunması sebebiyle (bankaların kimliği belirsiz taraflara işlem hizmetine izin verilememektedir) Bitcoin içeren işlemler mali kuruluşlar için yasaklanmıştır. 2016 yılında Merkez Bankası yeni Müdürü kendi tabiriyle “vekil para birimleri”nin fizibilite çalışmaları için bir görev gücünün kurulacağını duyurmuştur. İlk Bitcoin ATM'si Almatı'ya kurulmuştur. Sanal paralar için bölgesel merkez olmayı hedeflemek için 2017 yılının Haziran ayında Kazakistan blok zincir tabanlı tahvil satışının başlayacağı planını duyurmuştur. Ayrıca ülkenin Başkanı uluslararası ödeme birimini başlatma imkânını araştırmanın tam zamanı olduğunu ifade etmiştir. Bu durumun kara pazarlama ve piyasalardaki oynaklığı azaltarak dünyanın parasal

¹⁷⁴ Age, s.15-16.

¹⁷⁵ Regulation of Cryptocurrency Around the World, Egypt, <https://www.loc.gov/law/help/cryptocurrency/world-survey.php#egypt> , (Erişim:15.02.2021).

savaştan kurtulmasına yardımcı olacağını ifade etmiştir. Sanal paranın basit ve şeffaf bir emisyon mekanizmasına sahip olması gerektiğini belirtmiştir. Dijitalleştirme ve blok zincir gelişmeleri göz önünde bulundurularak sanal para formunda bir ödeme biriminin oluşturulabileceğini ifade etmiştir. 2017 yılının Ekim ayında Astana Uluslararası Finans Merkezi (Astana International Financial Centre – AIFC) Maltalı şirket Exante ile eski Sovyet Ulusunun kullanılmayan sanal para piyasasını geliştirmek için bir işbirliği imzaladıklarını duyurmuştur. Kazakistan’ın sanal para ekosistemine girişinin Exante’nin yeni blok zincir platformu olan “Stasis” tarafından destekleneceği ifade edilmektedir.¹⁷⁶

1.9.4.2. Özbekistan

2017 yılının Eylül ayında Merkez Bankası terörün finansmanı ve diğer suç faaliyetlerinin olasılığı nedeniyle kripto paralarla işlem yapılmasına izin verilmesinin uygun olmadığı görüşlerini dile getirmiştir. 19 Şubat 2018 tarihinde Cumhurbaşkanı Shavkat Mirziyoyev Özbekistan Merkez Bankası ve diğer bazı kurumlarla 1 Eylül 2018 tarihine kadar Özbekistan topraklarında dijital paranın kullanımına yönelik yasal bir çerçevenin geliştirilmesi ile ilgili bir kararname imzalamıştır.¹⁷⁷

1.9.5. Güney Asya

1.9.5.1. Hindistan

Hindistan hükümeti sanal para borsalarını düzenlemekle yetkili olmadığı belirtilmektedir. İngiltere Rezerv Bankası sanal paraların riskleri ile ilgili kamuya uyarılarda bulunmuştur. 2017 yılının Temmuz ayında Hindistan Menkul Kıymetler ve Borsa Kurulu, Hindistan menkul kıymetler piyasası için fırsatlar üzerine en son küresel finansal teknoloji gelişmelerini araştırmak ve raporlamak için 10 kişilik danışman üyeden oluşan bir grup kurmuştur. Bu yeni Finansal ve Düzenleme Teknolojileri

¹⁷⁶ Department of Finance, “Virtual Currencies and Blockchain Technology”, s.10.

¹⁷⁷ Regulation of Cryptocurrency Around the World, Ozbekistan, <https://www.loc.gov/law/help/cryptocurrency/world-survey.php#kyrgyz> , (Erişim: 15.02.2021).

Komitesinin amacı Hindistan'ı finansal teknoloji çözümlerini benimsemeye ve ülke içindeki yenilikleri teşvik etmeye hazırlamak olduğu ifade edilmektedir. Aynı yılın sonunda Hindistan Yüksek Mahkemesi Bitcoin düzenlemesi için verilen bir dilekçeye cevap verilmesi ile ilgili merkez bankası ve bazı diğer kuruluşlara duyuru yayınlamıştır. Dilekçede sanal paraların hazineye karşı hesap verebilir olmasını sağlanması ve sanal para işlemlerinin anonimliği ile ilgili endişelerin belirtildiği ifade edilmektedir.¹⁷⁸

1.9.5.2. Nepal

13 Ağustos 2017 tarihinde Nepal Rastra Bankası Bitcoin ile gerçekleştirilen tüm işlemlerin yasa dışı olduğunu belirten bir bildirim yayınlamıştır. 2017 yılının Ekim ayı başlarında Nepal Polis Merkezi Soruşturma Bürosu ülkenin çeşitli yerlerinden Bitcoin borsası işi yürüttükleri gerekçesiyle ilk defa yedi kişiyi tutuklamıştır.¹⁷⁹

1.9.6. Doğu Asya ve Pasifik Bölgesi

1.9.6.1. Avustralya

Avustralya blok zincir teknolojisini ve sanal paraları benimseyen bir yaklaşım sergileyerek ikisi arasında faydalı bir denge bulmaya çalışmaktadır. Avustralya Vergi Dairesi (Australian Taxation Office – ATO) 2013 yılında Bitcoin işlemlerinin elektronik ödeme aracı olarak değerlendirilebileceğini ve bu nedenle sanal paraların mal ve hizmet vergisine ayrıca gelir vergisine tabi olduğunu onaylamıştır. Avustralya Vergi Dairesi, Bitcoin için vergi uygulaması konusunda rehberlik etmektedir. ATO, Bitcoin'in ne para ne de yabancı para birimi olduğunu ancak sermaye kazancı vergisi amacıyla sanal mülk olarak varlık olduğu sonucuna varmıştır. Kişisel kullanım veya tüketim amacıyla mal veya hizmet satın almak için Bitcoin kullanarak elde edilen 10 bin AUD Doları veya altındaki sermaye geliri veya kaybı dikkate alınmayacağı belirtilmiştir. Avustralya Hazine Bakanlığı 2015 yılının başlarında Bitcoin gibi sanal

¹⁷⁸ Department of Finance, "Virtual Currencies and Blockchain Technology", s.15.

¹⁷⁹ Regulation of Cryptocurrency Around the World, Nepal, <https://www.loc.gov/law/help/cryptocurrency/world-survey.php#nepal> , (Erişim:15.02.2021).

paralarla ilgili vergi şirketlerinin uygun bir şekilde nasıl belirlenebileceği konusunda bir bildiri yayınlamıştır. 2016 Ocak ayında Avustralya Başsavcısı, 2018 yürürlüğe girmiş olan sanal paraları düzenlemek amacıyla Danışma Dokümanı hazırlamıştır.¹⁸⁰

1.9.6.2. Japonya

Japonya tartışmasız sanal paraların en güçlü küresel savunucusu konumundadır. 2014 yılında diğer ülkeler Bitcoin'i yasaklarken ve sanal paralara karşı düşmanca veya ihtiyatlı bir duruş sergilerken Japonya Tokyo merkezli Bitcoin borsası olan MtGox'un çöküşünden sonra bile sanal paraları düzenleme olasılığını değerlendirmeye devam etmeye niyetli olduğunu açıklamıştır. 2016 yılı başlarında Mali Hizmetler Ajansı (Financial Services Agency – FSA) sanal paraların geleneksel para birimlerine eşit olarak tanınacağını bildiren bir yasa önermiştir. 2016 yılı Mart ayında Japonya'nın sanal paralarla ilgili ilk kanun tasarısı Ulusal Parlamento'ya sunulmuştur. Sunulan bu kanun tasarısında aşağıdaki maddeler yer almaktadır:

- Sanal paraların ve sanal para alım satım hizmetlerinin tanımlarını sağlamak,
- Sanal para alım satım hizmetlerinin kaydedilmesini talep etmek,
- Sanal para alım satım hizmet sağlayıcılarının işiyle ilgili düzenlemeler yapmak,
- Suç Gelirlerinin Transferini Önleme Kanunu anlamında sanal para alım satım hizmet sağlayıcılarını “belirlenmiş iş operatörleri” olarak atayarak müşteri kimliğinin verilmesi gibi bazı yükümlülükleri uygulamaya koymak.

Bu yasa 2016 yılının Mayıs ayında onaylanmıştır. 2017 yılının Nisan ayında Mali Hizmetler Ajansı, sanal paraların diğer para birimleri ile aynı yasal statüde olacak şekilde ödeme yöntemi olarak kullanılmasıyla ilgili de yeni bir yasa çıkarmıştır. Bu yasa siber güvenlik ve operasyonel düzenlemelerin yanı sıra borsalar için de sermaye koşullarını devreye sokmaktadır. 2017 yılının Eylül ayında Mali Hizmetler Ajansı sanal para borsaları için ilk lisanslı 11 şirketi onaylamıştır. Şirketlerin lisansı alabilmek için bireysel müşteri hesaplarının ayrılması ve bilgisayar sistemlerinin güçlendirilmesi gibi bazı katı gereksinimleri karşılamak zorunda olduğu belirtilmiştir. Bu lisansların verildiği sırada Japonya Bankalarının bir konsorsiyumu 2020 Tokyo Olimpiyatları

¹⁸⁰ Department of Finance, “Virtual Currencies and Blockchain Technology”, s. 6-7.

öncesinde sanal bir para tanıtacaklarını duyurmuştur. Bu yeni proje Mizuho Finansal Grup ve Japonya Postası liderliğinde Japonya Merkez Bankası ve Mali Hizmetler Ajansı'nın destekleriyle Japon halkının akıllı telefonları ile mal ve hizmet alımı için ödeme yapmalarını sağlamak için sanal bir para geliştirmeyi amaçlamaktadır. JCoin Japon Yen'ine bire bir bazda dönüştürülebilir ve akıllı telefon uygulamasıyla çalışan ve mağazalarda kare kod (QR kodlarının) taranması ile kullanılmaktadır. Bu hizmetin bedava sağlanması karşılığında bankaların tüketici harcama örnekleri üzerinde daha fazla bilgi toplanmalarına fayda sağlayacağı ifade edilmektedir. JCoin'in Japonya'yı tüm işlemlerin %70'ine denk gelen nakit para kullanımının ağır bağımlılığından kurtarmak için tasarlandığı belirtilmektedir. Bu değer herhangi bir gelişmiş ülkedeki ortalama %30 olan nakit kullanımından çok daha yüksektir. Konsorsiyum JCoin kullanımının Japonya ekonomisine nakit kullanımını azaltarak ve tüketiciler ve perakendeciler için takas ücretlerini keserek, 10 milyar Yen (yaklaşık olarak 75 Milyon Avro) kazandıracağını tahmin etmektedir.¹⁸¹

1.9.7. Güney Asya ve Pasifik

1.9.7.1. Güney Kore

Strateji ve Maliye Bakanlığı, Kore Bankası, Finansal Hizmetler Komisyonu ve Finansal Denetleme Hizmetleri 2013 yılında “siber para birimi”nin “gerçek yasal para birimi” olmadığını ve para birimi işlemleriyle ilgili standart düzenlemelere uymadığını ifade etmişlerdir. Kurumlar ayrıca Bitcoin'in değerindeki yüksek dalgalanma ve içsel değer eksikliği nedeniyle uyarılarda da bulunmuşlardır. Mali Hizmetler Komisyonu 2016 yılının başlarında borsa için yeni düzenlemeleri tanıtmak amacıyla yeni sanal para görev gücü başlatmıştır. Güney Kore'nin Mali Hizmetler Komisyonu 2017 yılında Bitcoin vadeli alım satım işlemlerini yasakladı ve birçok menkul kıymetler firmasının Bitcoin vadeli yatırımcıları için Aralık ayında planladıkları seminerleri iptal etmesini istemiştir. Kore Hükümeti doğrudan Bitcoin borsalarını yasaklamadıklarını

¹⁸¹ Age, s.9-10.

sadece ICO'lar ve vadeli alım satım işlemlerinin yasağa maruz kaldığını ifade etmiştir.¹⁸²

1.9.7.2. Çin

Çin Halk Bankası, Endüstri ve Bilgi Teknolojileri Bakanlığı, Bankacılık Düzenleme Komisyonu, Sigortacılık Düzenleme Komisyonu ve Menkul Değerler Düzenleme Komisyonu ortaklığında 2013 yılında “Bitcoin’in Risklerini Önleme Üzerine Bildiri” yayınlamıştır. Bu bildiri, kurumlara ülkede Bitcoin ile işlem yapan ve Bitcoin alım satımı gerçekleştiren işletmelerin kara para aklama ve Terörün finansmanı ile mücadele yükümlülüklerinin yerine getirilmesi ve müşterilerinin kimlik bilgilerini belirlenmesi ve kaydedilmesi için gerekli önlemlerin alınması zorunluluğunu getirmiştir. Ayrıca finans kurumları ve ödeme servis sağlayıcılarının olası riskleri önlemek adına Bitcoin hizmet sağlayıcılarını gözetim altına alınması gerektiği belirtilmektedir.¹⁸³ Bu bildirinin akabinde Çin Halk Bankası ülkede sana para ile ticaret yapan bankalara yasak getirmiştir. Endonezya 13 Şubat 2014 tarihinde benzer bir adım atarak Bitcoin ve diğer sanal paraların ne para birimi ne de yasal ödeme aracı olarak kabul edilebileceğini ifade etmiştir.¹⁸⁴

İlk başlarda düzenlemenin olmaması Çin’e blok zincir uzayında özellikle Bitcoin alım satımı ve Bitcoin madenciliğinin ilk benimseyicisi olması noktasında yardım etmiştir fakat 2017 yılı başlarında bu durum tam tersi haline gelmiştir. Ülkeden Bitcoin aracılığıyla ne kadar miktarda sermaye kaçtığından korkan Çin aniden Bitcoin ticareti üzerine katı düzenlemeler getirmiştir. Finansal kurumlar ve üçüncü parti ödeme sağlayıcılar için sanal paraların kabulü, kullanımı veya satılması işlemleri yasaklanmıştır. Kullanımının yasal kalmasına rağmen Çin Halk Bankası uygun düzenleme otoriteleri ile borsa işlemleri için kayıt olunması gerekliliği ve bu sayede piyasayı yakından izleyeceğini önermiştir. Çin Halk Bankasının bankalara sanal paralarla işlem yapan işletmelerle ilgili uyarıda bulunduğu iddia edilmektedir. Çin, ICO’ların ülkede yasa dışı faaliyet olarak değerlendirmesi sebebiyle tüm şirket ve

¹⁸² Age, s.18.

¹⁸³ Financial Action Task Force, *Guidance For a Risk-Based Approach to Virtual Currencies*, s.16.

¹⁸⁴ Brill ve Keene, *Cryptocurrencies: The Next Generation of Terrorist Financing*, s.23.

bireylere ÷lkede ICO faaliyetleri ile fon toplamalarını yasaklamıştır. Çin Halk Bankası, Çin Menkul Kıymetler Düzenleme Komisyonu ve Çin Sigorta Düzenleme Komisyonu dâhil birkaç kurum sanal paraların yasaklanması ile ilgili ortak bir ifade yayınlamışlardır.¹⁸⁵

Çin Halk Bankası'nın 27 Aralık 2020 tarihinde başlattığı ikinci dijital para birimi pilot programını sonuçlandırdığı belirtilmektedir. Merkez bankasının Çin'i böyle bir sistemi uygulamaya koyan dünyanın en büyük ekonomisi yapabilecek resmi bir ürünü görücüye çıkarmasına daha fazla yaklaştığı ifade edilmektedir. Aralık 2020 içerisinde Doğu Çin'de bulunan Suzhou şehrinde yetkililerin değeri 3,1 milyon ABD Doları olan 20 milyon dijital yuani piyango aracılığı ile yerel sakinlere ücretsiz dağıttığı belirtilmektedir. 100 bin kazananın her birinin çevrimiçi veya çevrimdışı harcayabileceği yeni dijital para biriminde 200 yuan aldığı ifade edilmektedir. Suzhou pilot bölgesinin Ekim ayında Çin'in güneyinde yürüt÷len hükümet destekli dijital para birimi denemesinin ilk pilot şehri olan Shenzhen'e göre iki kat daha fazla sakin ve üç kat daha fazla tüccar bulunduran bir yer olduğu da vurgulanmaktadır. Pilot programa katılmak için seçilen bir Suzhou sakini olan 39 yaşındaki Wang Ju'nun Yuan talimatları takip ederek oluşturduğu dijital cüzdan uygulamasında eyalet kurucuları olan Mao Zedong'un resminin bulunduğu pastel renkli yuan banknotunun bir kopyasını bulduğundan çok etkilendiğı de ifade edilmektedir. Bir başka pilot katılımcı olan Ms. Wang ise kendisine tahsis edilen dijital para ile ailesinin tüm yıl boyunca karşılayacak olan deterjan ihtiyacını karşıladığını ve dijital parayı çevrimiçi alış veriş platformu olan JD.com Inc'de harcadığını ifade ettiğı belirtilmektedir. Çin'li yetkililerin Metituan ve Didi Chuxing teknoloji devleri ile birlikte yemek dağıtımı ve internet aracılığı ile araç çağırma gibi uygulamalar için dijital yuani birlikte test etmek için hareket ettikleri de ifade edilmektedir. Suzhou pilot programının ilk 24 saati içerisinde JD.com şirketinden 20 bin siparişin dijital yuan ile verildiğinin belirtildiğı ifade edilmektedir. Suzhou pilot programının çevrimiçi ödeme sistemini test etmesinin yanı sıra, çevrimdışı ödeme fonksiyonu olarak da denendiğı belirtilmektedir. Resmi kurumlar tarafından görücüye çıkartılan bu sistemin, ödemelerin giderek artan bir şekilde nakitsiz gerçekleştiğı Çin'de zaten ulaşılır bir şekilde her yerde var olan

¹⁸⁵ Department of Finance, "Virtual Currencies and Blockchain Technology", s.17.

elektronik ödeme sistemlerinden farklı yeni bir platform olduğu da belirtilmektedir. Ant Group şirketinin Alipay ve Tencent Holdings Ltd şirketinin WeChat Pay gibi ödeme sistemlerinin aksine merkez bankasının çevrimdışı ödeme özelliğinin hücresel hizmetin yetersiz olduğu bölgelerde ödeme faaliyetlerini kolaylaştırmak için internet bağlantısı gerektirmediği de yetkililer tarafından ifade edildiği belirtilmektedir. Müşteri ve satıcı arasında kısa bir cihaz dokunuşu ile işlemlerin tamamlanabileceği belirtilmektedir. Washington merkezli Peterson Enstitüsü Uluslararası Ekonomi bölümünde araştırmacı olan Martin Chorzempa'nın bugün bebek bezi veya sigara satın alınması ile kimsenin ilgilenmediği, asıl mevzunun daha çok makro hedefleme prosedürü için paranın ekonomi içerisinde nasıl hareket ettiğinin daha gerçek zamanlı anlaşılması olduğunu ifade ettiği belirtilmektedir. Pilot programa katılan bir Suzhou tüccarının programın her iki fonksiyonunu da memnuniyetle karşıladığı belirtilmektedir. Alış veriş merkezinin zemin katında yer alan bir kuruyemiş dükkânının müşterilerin ödeme için WeChat Pay ve Alipay kullandıklarında zayıf cep telefonu sinyalleri nedeniyle birçok problem ile karşılaştıkları ifade edilmektedir. Suzhou pilot programında yer almak üzere katılan kuruyemiş satıcısından sonra, ülkenin iki numaralı varlık kredisi veren ve yeni dijital para ile ilgili hükümetin deneyinde ona destek olan Çin İnşaat Bankasının kuruyemiş dükkânı satıcısına çevrimdışı ödemelere imkân veren yerli üretim bir akıllı telefon sağladığı ifade edilmektedir. Her 1.000 Yuanlık alış veriş için 3 veya 4 Yuan işlem ücreti alan banka ve ödeme sistemlerine göre bu sistemde işlem ücretlerinin de olmamasının bu sistemi kullanmanın kendileri için bir başka teşvik olduğu da satıcı tarafından ifade edilmektedir. Hükümet destekli ve işlem ücreti de olmayan dijital paranın çok fazla tasarruf sağlaması nedeniyle kendisi tarafından tercih sebebi olduğunu da vurguladığı ifade edilmektedir. Çin Merkez Bankası'nın kendi dijital para birimi ürerinde çalışmaya 2014 yılında DC/EP dijital para birimi/elektronik ödeme olarak bilinen adıyla başladıkları ifade edilmektedir. Yeni Yuanın hükümet tarafından desteklenen fiziki fiat paranın dijital uzantısı olduğu ve yeni tanıtılmak istenen para biriminin Çin'in dolaşımda olan nakit para tabanının bir kısmının dijital olarak değiştirilmesi olduğu ifade edilmektedir. Suzhou ve Shenzhen pilot uygulamalarına göre Çin'in mevcut olan ticari ödeme sistemleri ile benzer şekilde tüketicilerin bu yeni sistem için akıllı telefonlarına parayı depolayabilecekleri bir dijital cüzdan yüklemek durumunda

oldukları ve her bir işlem sırasında ödeme işlemi için bir karekod diğer bir ifadeyle QR (Quick Response Code) kod üretmeleri gerektiği ifade edilmektedir. Chorzempa yeni dijital para biriminin cazibesinin bir kısmının merkez bankası için halka açık ve iki kişinin tekelinde olan Alibaba ve Tencent'in ödeme sistemlerine alternatif olması ve işlem verilerine daha fazla erişim elde etmek olduğunu ifade ettiği belirtilmektedir. Dijital Yuanın yaygın bir şekilde kullanılmaya başlanmasıyla Çin'li düzenleyici kurumlara para akışlarıyla ilgili daha fazla bilgi verebileceği ve yetkililerin kara para aklama ve terörist finansmanı için kullanımını izleyebilmelerine olanak sağlayacağı da ifade edilmektedir. Analistler, yeni para biriminin ayrıca aşırı ekonomik durumlarda tüketicileri harcamaya teşvik etmek için merkez bankasının nakit üzerinde eksi faiz oranları koymasına izin verebileceğinin tahmin edildiği ifade edilmektedir. Hem kamu hem de özel alanlarda birçok denemesinin gerçekleştirilmesine rağmen Çin hükümeti tarafından tam anlamıyla uygulamaya geçileceği ile ilgili bir zaman çizelgesinin hazırlanmadığı belirtilmektedir. Çin Merkez Bankası Başkanı Yi Gang'ın daha fazla kural ve düzenlemeye ihtiyaçları olduklarını ifade ettiği belirtilmektedir.¹⁸⁶

1.10. KRİPTO PARA VE TÜRKİYE

Türkiye'de elektronik para; 27.06.2013 tarihli ve 28690 sayılı Resmi Gazete 'de yayımlanarak yürürlüğe giren 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun göre şu şekilde tanımlanmaktadır:

“Elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, bu Kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değeri”

2013 tarihinde BDDK'nın yaptığı açıklama ile Bitcoin'in elektronik para kanunu kapsamında değerlendirilemeyeceği, gözetimi ve denetiminin mümkün olmadığı ifade edilmiş olup, kullanıcıların ileride oluşabilecek risklere karşı dikkatli olması gerektiği ve bu risklerden devletin sorumlu olmayacağı belirtilmiştir. Bu nedenle, kripto paralar

¹⁸⁶ Jonathan Cheng, “China Envisions Its Digital-Currency Future, With Lotteries and a Year's Worth of Laundry”, 27.12.2020, <https://www.wsj.com/articles/china-envisions-its-digital-currency-future-with-lotteries-and-a-years-worth-of-laundry-11609066819> (Erişim:29.12.2020).

lkemizde pozitif hukuka gre elektronik para olarak nitelendirilmemektedir. Trkiye’de yasal bir bořluk vardır dolayısıyla kripto para reten ve kullananlar hibir kurula uymak zorunda deęillerdir. Kripto paraların alım-satımı ve kullanımı hibir mevzuat hkmyle dzenlenmemiřtir veya yasaklanmamıřtır.

Sermaye Piyasası Kurulu (SPK) Aralık 2016’da “Kripto-Para Bitcoin” adı altında bir kitapık yayınlamıřtır. 27 Kasım 2017 tarihinde ise Sermaye Piyasası Kanunu’nda sanal paralarla ilgili herhangi bir dayanak teřkil edecek unsurlar bulunmadıęı iin Bitcoin ve benzeri sanal paralara ynelik iřlem yapılması uyarısında bulunmuřtur.¹⁸⁷ Eyll 2018’de ise yayınlamıř olduęu bltende ICO’lara deęinerek, ICO’ların speklatif yn bulunan ve yksek risk ieren yatırımlar olduęu belirtilerek, dijital varlık (token) satıřları hakkında kurumun dzenleme ve gzetimi dıřında kaldıęı ifade edilmektedir. Ayrıca dzenlemelerin devam ettięi ve token satıřı konusunun kurum dzenlemesine tabi olup olmayacaęı ile ilgili farklı yaklařımlar olabileceęi belirtilmektedir.¹⁸⁸

Borsa İstanbul’un 14 Aralık 2017 tarihinde yaptıęı aıklamada kendi kripto para birimi BISTcoin zerinde alıřmaların yapıldıęı ifade edilmektedir.¹⁸⁹

Hazine ve Maliye Bakanlıęı tarafından Eyll 2018’de yayınlanan 2019 – 2021 yıllarını kapsayan Yeni Ekonomi Programı’nda (YEP) modern ve aynı zamanda yeni nesil finansman yntemi olarak adlandırılan ICO’ların dijital dnřm teřvik etmek amacıyla yeniliki projelerin finansmanını saęlamak iin yaygınlařtırılacaęı ifade edilmektedir.¹⁹⁰

7 Ocak 2020 tarihinde yayınlanan habere gre Sermaye Piyasası Kurulu’nun (SPK) 2020 yılına kadar Bitcoin ve kripto paralarla ilgili dzenleme alıřmalarını hızlandıracaaęı belirtilmektedir. BeInCrypto Turkey’e gre SPK’nın muhtemelen genel olarak kripto para birimlerinin yanı sıra Bitcoin’in gzetim, dzenleme ve denetimi

¹⁸⁷SPK’dan Bitcoin Aıklaması, 01.12.2017, <https://uzmanpara.milliyet.com.tr/haber-detay/gundem2/spkdan-bitcoin-aciklamasi/76000/76545/>, (Eriřim:20.01.2021).

¹⁸⁸Sermaye Piyasası Kurulu Blteni, 27.09.2018, <https://spk.gov.tr/Bulten/Goster?year=2018&no=42>, (Eriřim: 20.01.2021), s.4.

¹⁸⁹ Eser řahin, “Borsa İstanbul, BISTcoin Adında Kendi Kripto Para Birimi zerinde alıřtıklarını Duyurdu!” 14.12.2017, <http://www.webtekno.com/bistcoin-nedir-h37894.html>, (Eriřim: 17.12.2017).

¹⁹⁰ Hazine ve Maliye Bakanlıęı, Yeni Ekonomi Programı Dengeleme-Disiplin-Deęiřim 2019-2021, Eyll 2018, <https://ms.hmb.gov.tr/uploads/2018/10/yeni-ekonomi-programi.pdf>, (Eriřim: 20.01.2021), s.17.

konularına önem vereceği ifade edilmektedir. Bu güne kadar Türkiye’de herhangi bir yasal düzenlemenin olmadığı da vurgulanmaktadır. Bitcoin kullanımının Türkiye’de Avrupa’daki ülkelere nazaran daha geniş çapta kullanıldığı da ifade edilmektedir. Avrupa’da Bitcoin kullanan AB nüfusunun %25 civarında olduğu belirtilmektedir. Türkiye’de ise nüfusun %45’inden fazlasının Bitcoin ve diğer kripto para birimleri kullanımında aktif olduğu vurgulanmaktadır. SPK’nın yalnızca kripto para birimleri için değil, kripto para alım satımı gerçekleştiren borsalara yönelik de düzenlem adımları atabileceği belirtilmektedir.¹⁹¹

Türkiye İş Bankası’nın dünyanın en fazla katılımcı ağına sahip konumda olan R3 blok zincir platformunun açık kaynak kodlu Corda platformuna 30 Mart 2020 tarihinde üye olarak R3 Blok Zincir Birliği’ne katılım sağlayan ilk Türk Bankası olduğu belirtilmektedir.¹⁹² Bu gelişmelerin akabinde Türkiye İş Bankası’nın 27 Mayıs 2020 tarihinde gerçekleştirilen ilk işlem ile dış ticaret finansmanında blok zinciri teknolojisini kullanarak ödeme garantisini sağlayan ilk Türk Bankası olarak da anılmaktadır. Corda teknolojisini kullanan Marco Polo platformunun sağladığı Dağıtık Defter Teknolojisi ağı ile İş Bankası, Şişecam, Kuraray Europe GmbH ve Commerzbank arasında gerçekleşen dış ticaret işleminde tarafların bilgilerinin herkese açık olmayacak bir şekilde gerektiği kadar bilginin sadece firma ve bankaların onay verdiği taraflar ile paylaşıldığı ve böylelikle gizliliğin sağlandığı ifade edilmektedir.¹⁹³

¹⁹¹Max Moeller, “Turkey’s Regulatory Board CMB Moves Against Bitcoin”, 07.01.2020, <https://beincrypto.com/turkeys-regulatory-board-cmb-moves-against-bitcoin/>, (Erişim:20.01.2021).

¹⁹²İş Bankası R3 Blockchain Birliği’ne katılan ilk Türk bankası oldu, 29.04.2020, <https://www.isbank.com.tr/bankamizi-taniyin/is-bankasi-r3-blockchain-birligine-katilan-ilk-turk-bankasi-oldu>, (Erişim: 19.01.2021).

¹⁹³İş Bankası, blockchain teknolojisiyle dış ticarete ödeme garantisi veren ilk Türk Bankası oldu, 03.06.2020, <https://www.isbank.com.tr/bankamizi-taniyin/is-bankasi-blockchain-teknolojisiyle-dis-ticarete-odeme-garantisi-veren-ilk-turk-bankasi-oldu>, (Erişim: 19.01.2021).

Şekil 1.17 Türkiye İş Bankası Blok Zincir Konusunda Önemli Adım Attı



23 Temmuz 2019 tarihinde Resmi Gazete 'de yayınlanan 2019 – 2023 yıllarını kapsayan On Birinci Kalkınma Planı'nda duyurulan ve 4 Kasım 2019 tarihli Resmi Gazete'de yer alan “2020 Yılı Cumhurbaşkanlığı Yıllık Programı”nın onaylanması Cumhurbaşkanlığı Kararında ise detayı yer alan Türkiye Cumhuriyet Merkez Bankası ve TÜBİTAK işbirliğinde blok zincir teknolojisinin kullanılmasıyla geliştirilecek Anlık Ödeme Sistemi olarak ifade edilen dijital merkez bankası parasının uygulamaya konulmasının hedeflendiği ifade edilmektedir.¹⁹⁴

18 Kasım 2019 tarihinde yayınlanan habere göre, On Birinci Kalkınma Planı'nda yukarıda belirtilen blok zinciri teknolojisi ile ilgili düzenlemenin ardından Mali Suçları Araştırma Kurulu'nun (MASAK) kripto para alım satımına aracılık eden kripto para borsalarına gerçekleştirilen para transferlerinin kategorisini kaldırdığı belirtilmektedir.

¹⁹⁴ Resmi Gazete, “On Birinci Kalkınma Planı (2019-2023)”, (23.07.2019), <https://www.resmigazete.gov.tr/eskiler/2019/07/20190723M1-1-1.pdf> “2020 Yılı Cumhurbaşkanlığı Yıllık Programı'nın Uygulanmasına Dair Karar”, (04.11.2019), <https://www.resmigazete.gov.tr/eskiler/2019/11/20191104M1-1-1.pdf> , (Erişim:31.12.2020).

Şekil 1.18: Türkiye, dijital dönüşümde atak yapıyor



25 Aralık 2020 tarihinde yayınlanan habere göre, Türkiye Cumhuriyet Merkez Bankası'nın 2021 yılının ikinci yarısında ilk pilot uygulamalarının başlayacağı dijital para çıkarılması ile ilgili bir Ar-Ge projesinin olduğu ve çalışmaların teorik ve kavramsal kısımlarının tamamlandığı belirtilmektedir.¹⁹⁵

Türkiye'nin kripto para ve blok zinciri konusunda yaptığı araştırma ve geliştirme faaliyetlerinin kamu tarafındaki yansımalarından birisi de 28 Aralık 2020 tarihinde T.C. Ticaret Bakanlığı'nın resmi Twitter hesabından yaptığı paylaşımda Blok zincirinin Yıldızları Aranıyor başlıklı duyurusu ile olmuştur. Duyuruda 30 Aralık 2020 tarihi itibarı ile ilana çıkılacağı belirtilmektedir.

Şekil 1.19: Blok Zincirinin Yıldızları Aranıyor¹⁹⁶



¹⁹⁵ Merkez Bankası Başkanı Ağbal'dan kripto para açıklaması, 25.12.2020, <https://www.cnnturk.com/ekonomi/son-dakika-merkez-bankasi-baskani-agbal-enflasyon-hedefini-acikladi>, (Erişim:20.01.2021).

¹⁹⁶ Türkiye Cumhuriyeti Ticaret Bakanlığı Resmi Twitter Hesabı

Blok zincir teknolojisi Bitcoin ile adını duyurmuş bir teknoloji olsa da, finansal sektör dışında birçok alanda uygulama alanı bulunmaktadır. Merkezi bir sistem tarafından yönetilen aklımıza gelebilecek her şeyin dağıtık ve merkezi olmayan, şeffaf, güvenilir bir sistem olma özelliğine sahip bu teknoloji ile yeniden dizayn edilmesi çok yakın bir gelecekte tartışılıyor olacaktır. Ülkemizde blok zincir alanında yaşanan son gelişmelerden ilki 2019 yılında bir diğeri ise 2020 yılında uygulamaya konulmuştur.

29 Aralık 2020 tarihinde yayınlanan 2020-2023 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı olmuştur. Yayınlanan bu planda yeni nesil teknolojiler arasında yer alan blok zincir teknolojisinin siber güvenlik planlamalarında öncelikli yer alacağı ifade edilmekte olup milli teknoloji hamlesi ilkesi blok zincir teknolojisinin siber güvenlik alanındaki kullanımı ile ilgili gerekli Ar – Ge çalışmalarının yapılacağı belirtilmektedir.¹⁹⁷

Türkiye’de kripto paralar ile ilgili yasal bir düzenlemenin yapılması gerekmektedir. Kripto paralara yönelik bir tanım getirilebilir. Örneğin, kripto para mal varlığı olarak değerlendirilebilir ve düzenlemeler bu tanıma göre yapılabilir. Diğer taraftan, kripto para kavramı, para veya varlık olarak değil bir veri transferi gibi teknik bir kavram olarak da değerlendirilebilir ve Bitcoin ile işlenen suçlarda bilişim alanında işlenmiş suçlar kapsamında değerlendirilebilir. Kripto paranın dijital üretim aşaması olan madencilik işleminde kullanılan cihazlarla yapılan işlemler de bilişim alanında suçlar kapsamında değerlendirilebilir. Ödemeyi gerçekleştiren ve alacaklı kişinin bilgilerinin açıkça belirtildiği izlenebilirlik sistemi geliştirilerek kripto para işlemlerinin gizliliği ortadan kaldırılabilir. Kripto paraların alım satımına aracılık eden borsalara yönelik böyle bir düzenlemenin yapılması bu alanda kısmen bir çözüm oluşturabilir. Anonimlik ve sistemin dağıtık yapısının kara para aklama ve terörizm finansmanı işlemlerinde kolaylık sağlaması nedeniyle tamamen yasaklanması da söz konusu olabilir fakat yasaklama tüm sorunları ortadan kaldırmayacağının da bilinmesi gerekmektedir.

Kripto para birimlerinin yanı sıra reel para birimleri ile de alım satım işlemlerine olanak sağlayan kripto para borsaları sadece internet üzerinden işlem

¹⁹⁷ T.C. Ulaştırma ve Altyapı Bakanlığı, “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023”, 29.12.2020, <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf> (Erişim:30.12.2020).

yapabilen çevrimiçi platformlardır. Sayıları her geçen gün artmakla birlikte dünya genelinde bu tezin yazıldığı dönem itibarıyla 296 adet kripto alım satımı gerçekleştiren borsa bulunmaktadır.¹⁹⁸ Türkiye’de ise şu an işlem gören on iki tane kripto para borsası bulunmakta olup son 24 saatlik işlem hacimleri aşağıda belirtilmektedir. Tablodan da anlaşılacağı üzere dünya genelindeki pek çok ülke gibi Türkiye’de de kripto paralara olan talebin artma yönünde eğilim gösterdiği görülmektedir. En fazla işlem hacmine sahip olan 1 Temmuz 2013 tarihinde kurulan ve 2020 yılı itibarı ile 1 milyon kullanıcısı bulunan BtcTurk’un Türkiye’nin ilk, dünyanın ise dördüncü Bitcoin alım satımı gerçekleştiren kripto para borsası olduğu belirtilmektedir. 2019 yılında Türkiye Süper Lig takımı olan Yeni Malatyaspor’a gerçekleştirdikleri forma ve isim sponsorluğu, 2020 yılında ise kadın ve erkek olmak üzere iki ayrı kategoride Futbol Milli Takımlarına sağladıkları ana sponsorlukla dünyada bir ilki gerçekleştirdikleri ifade edilmektedir.¹⁹⁹

Şekil 1.20: Türk Kripto Para Borsaları ve Son 24 Saatlik İşlem Hacimleri²⁰⁰

Son 24 Saatlik Toplam İşlem Hacmi
(Volume in the last 24 Hours)

9.127.272.700 TRY
(1.303.896.100 USD)

Son Güncelleme 22:08:26
(Last Update)

Borsa	Parite	Alış	Satış	Son İşlem	Değişim	Hacim (₺)	Borsa Toplam Hacim (₺)	
BtcTurk	BTCTRY	237.400,00	237.460,00	237.276,00	5.5%	422.778.264	2.687.249.031	Git
PARIBU	BTCTRY	235.498,00	235.949,00	235.749,00	4.5%	286.145.003	2.577.067.438	
THODEX	BTCTRY	237.887,70	238.039,62	238.039,62	-	75.640.980	1.966.827.353	
bitexen	BTCTRY	236.640,66	236.806,05	236.806,05	3.94%	293.258.244	705.162.085	Git
BITCOIN	BTCTRY	236.477,00	236.774,00	236.477,00	-	47.111.191	282.091.777	
coinzo	BTCTRY	237.383,00	238.054,00	238.054,00	5.66%	81.964.373	207.116.693	
Bitci	BTCTRY	238.229,94	238.556,04	238.556,04	5.77%	74.285.418	113.848.735	
BitTurk	BTCTRY	230.108,00	243.450,00	230.108,00	-	1.114.513	9.978.856	
bithesap	BTCTRY	232.710,00	240.000,00	232.698,00	8.11%	7.565.012	9.837.497	
koinim	BTCTRY	237.000,00	237.499,00	237.000,00	1.50%	671.397	3.657.649	
BARIMEKS	BTCTRY	237.304,50	238.640,80	237.321,00	6.42%	121.697	121.697	

14 Şubat 2017 tarihinde faaliyete başlayan bir diğer Türk kripto para alım satım platformu olan Paribu ise 700 bin kullanıcısı ile 2017 Aralık ayında 5.800 BTC’lik işlem hacmi ile ABD merkezli kripto para piyasalarının analizini ve takibini gerçekleştiren CoinMarketCap-World sıralamasında 16. sırada yer aldığı

¹⁹⁸ Top Cryptocurrency Spot Exchanges, <https://coinmarketcap.com/tr/rankings/exchanges/> (Erişim:28.01.2021).

¹⁹⁹ Hakkımızda, <https://www.btcturk.com/btcturk/hakkimizda> (Erişim: 21.01.2021).

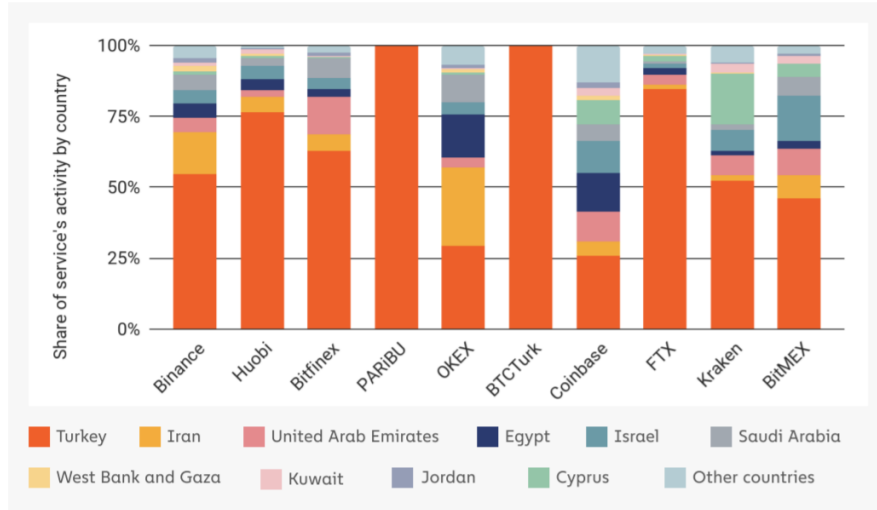
²⁰⁰ Türk Bitcoin Borsaları, <https://coin-turk.com/piyasalar> (Erişim:28.01.2021).

belirlenmektedir.²⁰¹ 9 – 20 Ekim 2020 tarihleri arasında gerçekleşen 39. İstanbul Film Festivali'nin tema sponsorluğunu gerçekleştiren Paribu'nun Türkiye'de ilk kez gerçekleşen bir uygulama ile UNICEF Türkiye'nin Paribu üzerinden kripto para ile bağış yapılmasına imkan sağladığı da ifade edilmektedir.²⁰²

Blok zinciri analiz şirketi Chainalysis'in 2020 yılında yayınlamış olduğu rapora göre Ortadoğu ülkeleri bölümünde değerlendirilen Türkiye'nin Küresel Kripto Para Kabullenme Endeksi'ne göre 52. sırada olan Mısır ve 64. sırada olan İran'ı geride bırakarak 154 ülke arasından 29. sırada yer aldığı ve bölgedeki en fazla toplam işlem hacmine sahip olduğu belirtilmektedir. Raporda ayrıca Türkiye'deki iki yerel kripto para borsalarının Paribu ve BtcTurk'un sırasıyla 4. ve 6. sırada yer alarak işlem hacmi ile önemli bir etkinlik oluşturduğu da ifade edilmektedir.²⁰³

Şekil 1.21: Küresel Kripto Para Kabullenme Endeksi

Top ten services in Middle East by country | Jul '19 to Jun '20



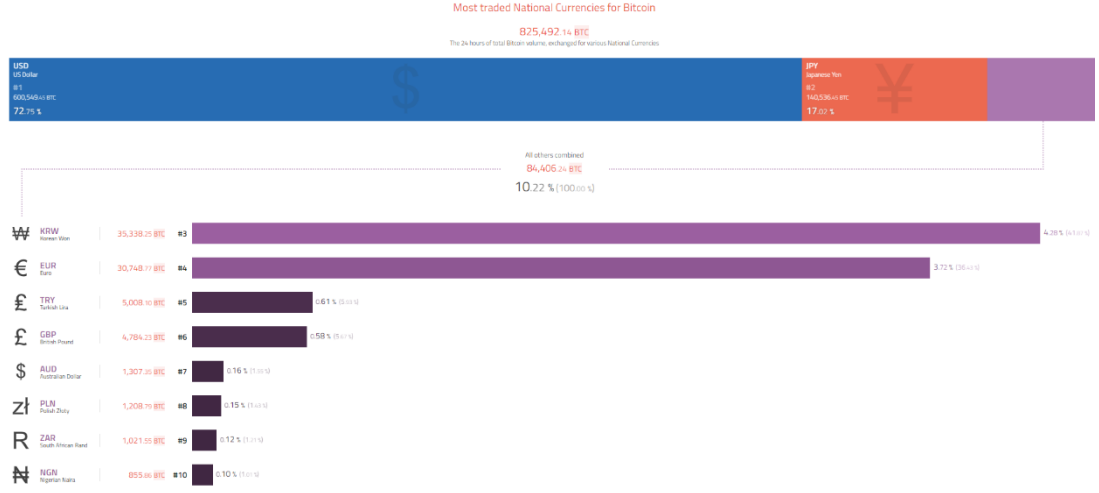
Bitcoin ile en çok işlem gören ulusal para birimleri sıralamasında birinci sırada Kore Wonu % 43,45 pay ile yer alırken, Avro % 32,69 ile ikinci sırada ve Türk lirasının ise % 8,11 pay ile ilk üç sırada yer aldığı belirtilmektedir.

²⁰¹Paribu Nedir?, <https://destek.paribu.com/hc/tr/articles/115005841469-Paribu-Nedir->, (Erişim:21.01.2021).

²⁰²UNICEF Türkiye, Paribu üzerinden Türkiye'de ilk kez kripto parayla bağış kabulüne başladı, <https://www.paribu.com/blog/haberler/unicef-turkiye-paribu-uzerinden-turkiyede-ilk-kez-kripto-parayla-bagis-kabulune-basladi/> (Erişim: 21.01.2021).

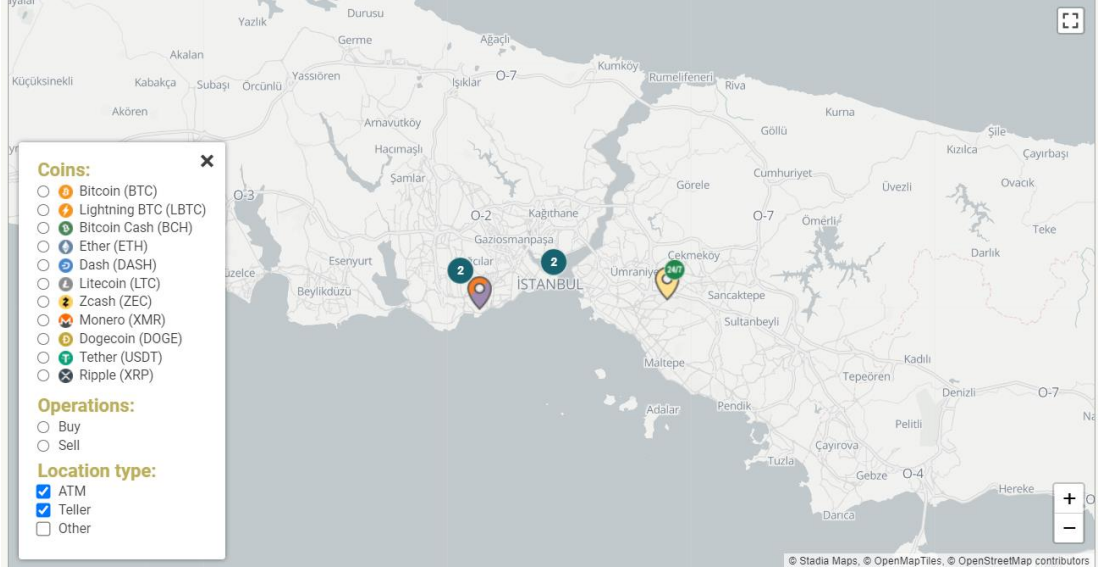
²⁰³ Chainalysis, "The 2020 Geography of Cryptocurrency Report, Analysis of Geographic Trend in Cryptocurrency Adoption, Usage, and Regulation", September 2020, (Erişim:21.01.2021), s.92.

Şekil 1.22: Bitcoin İle En Çok İşlem Gören Ulusal Para Birimleri²⁰⁴



Dünya üzerindeki 71 ülkede Bitcoin ATM'lerinin bulunduğu ve en fazla Bitcoin ATM'lerinin de 12 bin 17 lokasyonla Amerika Birleşik Devletleri'nde olduğu, Türkiye'de ise İstanbul'da 6 lokasyonda yer aldığı belirtilmektedir.²⁰⁵

Şekil 1.23: İstanbul Çevresindeki Toplam Bitcoin ATM'lerinin Sayısı



²⁰⁴ Most traded National Currencies for Bitcoin, <https://www.coinhills.com/market/currency/> , (Erişim:28.01.2021).

²⁰⁵ Bitcoin ATMs by Country, <https://coinatmradar.com/countries/> , Erişim: 28.01.2021).

Şekil 1.24: İstanbul Çevresindeki Bitcoin Makinelerinin Yerleşke Listesi²⁰⁶

Select operation:
☒ Buy ☐ Sell

Select cryptocurrency:
☒ Bitcoin (BTC) ☐ Lightning BTC (LBTC) ☐ Bitcoin Cash (BCH) ☐ Ether (ETH) ☐ Dash (DASH)
☐ Litecoin (LTC) ☐ Zcash (ZEC) ☐ Monero (XMR) ☐ Dogecoin (DOGE) ☐ Tether (USDT) ☐ Ripple (XRP)

Sort by: ☒ best fee ☐ city ☐ score

Transaction size (TRY):

☐ Ignore fixed fees and online priority (sorting happens only by % commission, no differentiation between online reported and manually defined fees)
☒ Show current city on top (display listings from current city on top of list, the rest listings for cities around below)

	Kale Outlet Center	Istanbul	Buy: 5.2% Sell: 1.7%	Score: 0	Details
	Carusel Shopping Center	Istanbul	Buy: 5.2% Sell: 1.7%	Score: 0	Details
	CITY'S Nisantasi Alışveriş Merkezi	Istanbul	Buy: N/A Sell: N/A	Score: +2	Details
	Qoet Bağcılar	Istanbul	Buy: N/A Sell: N/A	Score: +1	Details
	Qoet Ataşehir	Istanbul	Buy: N/A Sell: N/A	Score: 0	Details
	Coinsefera Bitcoinshop	Istanbul	Buy: N/A Sell: N/A	Score: 0	Details

4 Ocak 2021 tarihinde yayınlanan habere göre Türkiye’de işlem gören kripto para borsasının ocak ayı başından bu yana günlük işlem hacminin, günlük işlem hacmi 40 milyar TL olan Borsa İstanbul’un yaklaşık dörtte biri işlem hacmi ile 1 milyar ABD Dolarını aştığı belirtilmektedir. Kripto para borsasının Borsa İstanbul ile yarışacak seviyeye geldiği de ayrıca vurgulanmaktadır.²⁰⁷

Şekil1.24: Türkiye’de Kripto Para Günlük İşlem Hacmi



Bloomberg HT > Kripto Para

Türkiye’de kripto para günlük işlem hacmi 1 milyar doları aştı

²⁰⁶ <https://coinatmradar.com/city/1952/bitcoin-atm-istanbul/>, (Erişim:21.01.2021).

²⁰⁷ “Türkiye’de kripto para günlük işlem hacmi 1 milyar doları aştı”, 04.01.2021, <https://www.bloomberght.com/turkiye-de-kripto-para-gunluk-islem-hacmi-1-milyar-dolari-asti-2271922> (Erişim:21.01.2021).

İKİNCİ BÖLÜM

KRİPTO PARA VE KARA PARA AKLAMA SİSTEMİ

Reel para birimlerinin dijital sistemler vasıtasıyla kripto paralara dönüştürülmesi ve bunların da kara para aklama gibi yasa dışı faaliyetlerde kullanılması ülkeler için her zaman risk oluşturmıştır. Yasal bir zeminde olmayan paranın yani diğer bir ifadeyle kara paranın yasal bir zemine çekilmesi için kullanılan ideal yöntemlerden birisi kripto para kullanarak aklama yöntemidir. Avrupa Merkez Bankası suç faaliyetlerinin takibini devre dışı bırakması ve anonimlik özellikleri nedeniyle Bitcoin'in bazen kara para aklama ve uyuşturucu kaçakçılığı gibi suçlarla anılmakta olduğunu ifade etmektedir.²⁰⁸

Kripto paraların icadı bir yandan internet aracılığıyla güvenli bir şekilde işlem yapılmasını kolaylaştırırken, diğer taraftan da sayısız siber suçu kolaylaştırmakta ve suçluların gelirlerini güvenli bir şekilde aklamalarına yardımcı olmaktadır. Bitcoin şu an binlerce adet olan kripto paralardan sahip olduğu anonimlik, güvenlik, işlemlerin geri dönüşümsüzlüğü ve dağınık olması özelliklerinden dolayı kripto paranın sömürülen en bilinen örneği olarak tanımlanabilmektedir. Bitcoin'in suçlulara fırsatları ulaşılabilir kıldığı belirtilmektedir. Bitcoin'in çökmesi/patlaması gibi bir durumun kara para aklama faaliyetlerinde kripto paranın kullanımına son verileceği anlamına gelmediği de ifade edilmektedir.²⁰⁹

Bitcoin Terörün finansmanı ve yasa dışı ürünlerin kaçakçılığı işlemlerinde kara para aklamak için kullanılabilmektedir. Her ne kadar bu kaygılar şu anda görüldüğünden daha teorik olsa da Bitcoin gerçekten de yasa dışı elde edilen parayı gizlice taşımak isteyenler için bir seçenek olabilir. Bitcoin'in kara para aklama faaliyetlerinde potansiyel olma durumunun; özel, merkezi ve Kosta Rika tabanlı dijital para birimi hizmeti olan ve kara para aklama faaliyetleri nedeniyle kapatılan Liberty Reserve'den sonra daha da körüklendiği ifade edilmektedir.²¹⁰

²⁰⁸ European Central Bank (ECB), *Virtual Currency Schemes*, 2012, s.25.

²⁰⁹ Sagwadi Mabunda, "Cryptocurrency: The New Face of Cyber Money Laundering", *2018 International Conference on Advances in Big Data, Computing and Data Communication*, Durban, South Africa. 2018, s.9.

²¹⁰ Jerry Brito ve Andrea Castillo, "Bitcoin: A Primer For Policymakers", George Mason University, Arlington, 2013, s.25-26.

Ödemelerin kaydının olmaması sebebiyle, uyuşturucu veya benzeri yasa dışı maddelerin alımının internet aracılığıyla Bitcoin ile gerçekleştirilmesi rahatlıkla yapılabilmektedir. Bitcoin'in doğası gereği sahip olduğu anonimlik özelliğinin, internetin karanlık yüzü olan gizli internet ağları ile birleştiği zaman terörle mücadelede devletlerin işlerini daha da zorlaştırabileceği ifade edilmektedir.²¹¹

2.1. KARA PARA AKLAMA SİSTEMİ

2.1.1. Kara Para Tanımı

Kara para; milli muhasebe hesaplarına girmeyen kayıt dışı ekonominin unsurlarından bir tanesidir. Kara para ekonomisini; toplumun genel olarak reddettiği, insanlığın genel ilkelerine aykırı olan uyuşturucu kaçakçılığı, kadın ticareti, silah kaçakçılığı vb. olaylardan meydana gelen ekonomi oluşturmaktadır.

Kara para aklama ve terörizm ile mücadele kapsamında politika geliştirme, uluslararası standartları belirleme ve denetleme amacıyla faaliyet gösteren Mali Eylem Görev Gücü'ne göre kara para aklama; suçtan elde edilen gelirlerin, meşrulaştırılması amacıyla yasa dışı kaynağının gizlenmesi işlemi olarak tanımlanmaktadır.²¹²

Palermo Sözleşmesi olarak da bilinen, Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesi kara para aklamayı şu şekilde tanımlamaktadır: Gelirin, cezayı gerektirecek bir suçtan elde edildiğini bilerek;

- Yasa dışı kaynağını gizlemek veya suçun oluşmasında yer alan kişilerin işlemiş oldukları suçun hukuki sonuçlarından kaçınmasını sağlamak amacıyla gelirin/varlığın dönüştürülmesi ve transfer edilmesi işlemidir.
- Gelirin kaynağı, konumu, kullanımı ve hareketi gibi mülkiyet haklarının gizlenmesidir.
- Gelirin, cezayı gerektirecek bir suçtan elde edildiğini bilerek, gelirin veya varlığın kazanılması veya kullanılması işlemidir.²¹³

²¹¹ Brill ve Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?", s.14.

²¹² OECD, *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, 2009, s.11.

²¹³ UNODC, *Article 6: "Criminalization of the Laundering Of Proceeds Of Crime", UN Convention Against Transnational Organized Crime*, Vienna 2000, s.8.

2.1.2. Kara Para Aklamanın Tarihi

Kara para aklama kavramının ortaya ne zaman çıktığına dair herhangi bir delil bulunmamakla birlikte bu kavram tarihsel anlamda birkaç şekilde kullanılmıştır. Amerikan tarihçi Sterling Seagrave tarafından 1995 yılında kaleme alınan *Lords of the Rim* kitabında Seagrave, M.Ö. 3000 yıllarında Çin’de zenginlerin paralarını ya da varlıklarını sakladıkları, yer değiştirdikleri ve Çin dışında harcadıklarını belirtmektedir. Bu durum ayrıca yasa dışı fonların taşınır varlıklara dönüştürülmesi ve sonrasında diğer yasal ekonomilerde harcanmak üzere kaynağından uzaklaştırılmasını da içermektedir. Kara para kavramının o tarihlerde ortaya çıkmadığı fakat yöntemlerinin var olduğu ifade edilebilmektedir.²¹⁴

Kara para kavramının 1920’li yıllarda Amerika Birleşik Devletleri’nde (ABD) Al Capone gibi suç örgütlerinin, uyuşturucu, adam öldürme, fuhuş ve kumar gibi yasa dışı faaliyetlerle kazandıkları çok yüksek miktardaki nakit paranın yasa dışı kaynağını belirsiz hale getirmek için kurdukları çamaşırhaneler ile ortaya çıktığı bilinmektedir. Çamaşırhanelerin kullanılmasının sebebi bu sistemin nakitle çalışıyor olmasıdır. Devletin elde etmiş oldukları bu gelirlere el koymasını engellemek için de perakende satış yapan; bar, içerisine para atılarak yiyecek ve içecek gibi ürünlerin satın alınabildiği makine, otel ve restoran gibi hizmet sektörüne yönelik işletmeler kurmuşlardır. Bu yapmış oldukları yasal gibi gözükten ticaretlerle, yasa dışı elde ettikleri kazançları, yasal yoldan elde ettikleri kazançlarla karıştırarak, yasal ticaretin toplam kazancı olarak göstermekteydiler. Bu tekniği kullanarak yasa dışı kazançları aklamışlardır ve para serbest bir şekilde dolaşarak hukuki yaptırım otoritelerinin dikkatinden uzaklaştırılmıştır.²¹⁵

Bir diğer kaynağa göre, kara para aklama kavramı 1932 yılından sonra ABD’de Meyer Lansky ile kullanılmaya başlanmıştır. Lansky, İsviçre Bankasında Louisiana

²¹⁴ “The Nature of Money Laundering Activities”, *Money Laundering Activities: Explaining the Nature and Emerging Trends*, s.17-18, <https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjB8rnY6NDYAhUCdCwKHRTkCdUQFggoMAA&url=https%3A%2F%2Fpub.eur.nl%2Fpub%2F37747%2FD-%2520Chapter%25201-%2520Money%2520Laundering%2520Activities.pdf&usg=AOvVaw1VNeD9WcHisRB2dBPlkdT2> (Erişim: 05.01.2018).

²¹⁵ “The Nature of Money Laundering Activities”, *Money Laundering Activities: Explaining the Nature and Emerging Trends*, s.18.

Valisi Huey Long'un suçtan elde ettiği gelirleri saklamak için bir offshore hesabı açmıştır. Lansky daha sonrasında New Orleans'da slot makine evi kurmuştur ve İsviçre Bankası Lansky & Co şirketine kredi fonu sağlamıştır. Bu yöntem sayesinde yasa dışı paranın ABD'ye geri dönmesine izin verilmiştir. Bu dönemden sonra kara para aklama faaliyetleri teknolojik gelişmelerin kullanılmasıyla ilerlemiştir. Kara para terimi kavram olarak 1970'li yılların başında ABD'nin Banka Gizlilik Kanunu'na (Bank Secrecy Act) geçmesinden sonra kullanılmaya başlandığı da belirtilmektedir.²¹⁶ Banka Gizlilik Kanunu; kara para ile mücadele amacıyla, ABD'nin finansal kurumlarının banka müşterilerinin 10.000 Dolar ve üstü para transferlerini içeren işlemlerin kayıtlarının tutulması gerekliliği ile 1970 yılında çıkarmış olduğu yasadır.²¹⁷ BSA içindeki kayıtlar, Şüpheli İşlem Bildiri (ŞİB), Para Transferi Raporu, yabancı banka hesabı ile ilgili bilgi raporu ve para transferinin sınır ötesi hareketliliği ile ilgili rapor ve izleme raporlarından oluşmaktadır.

Kara para aklama 1980'li yılların sonunda ortaya çıktı ve sadece uyuşturucu kaçakçılığından elde edilen gelirlerin aklanması olarak anılıyordu. Fakat daha sonra uyuşturucu dışındaki dolandırıcılık, yolsuzluk, rüşvet, silah ve insan kaçakçılığı gibi diğer suçlardan da elde edilen gelirlerin bu sistemle yasal ekonomiye dâhil edilmesi şeklinde etki alanı genişlemiş oldu. Önce suçtan elde edilen gelirlerin gizlenmesi ve vergi ödememek için de vergi cenneti olarak adlandırılan yöntemle vergiden kaçırılması, vergi suçlarının kara para aklama faaliyetleri için öngörülen suç olarak anılmasına neden olmaktadır.²¹⁸

2.1.3. Kara Para Aklama Aşamaları

Mali Eylem Görev Gücü, kara para aklamanın aşamalarını; suçtan elde edilen gelirlerin sisteme sokulması olan yerleştirme (placement), gelirin elde edildiği kaynağın kökeninin gizlenmeye çalışıldığı ayırıştırma (laundering) ve aklanan paranın yasal ekonomi içerisine dâhil edilmesi olan bütünleştirme (integration) olmak üzere üç

²¹⁶ "The Nature of Money Laundering Activities", *Money Laundering Activities: Explaining the Nature and Emerging Trends*, s.18.

²¹⁷ Bank Secrecy Act, "Anti-Money Laundering, and Office of Foreign Assets Control", 1970, s.8.1-1

²¹⁸ European Parliament, *Offshore Activities And Money Laundering: Recent Findings and Challenges*, Brussels 2017, s.7.

kısımda tanımlamaktadır.²¹⁹ Tüm kara para aklama işlemlerinde bu üç aşama kullanılmamaktadır. Bazı durumlarda çok daha fazla aşamalarda bulunmaktadır.²²⁰

2.1.3.1. Yerleştirme Aşaması

Fiziksel paranın finansal sisteme girmesi kara para aklama işleminin ilk aşaması olan yerleştirme aşamasını oluşturmaktadır. Suçtan elde edilen gelirlerin banka ve finansal sistemlere yerleştirilmesi anlamına gelen bu aşama şüpheli işlem bildirimi olarak dikkat çekme ihtimali yüksek olduğu için riskli bir aşama olarak belirtilmektedir.²²¹ Bu nedenle yerleştirme; yüksek miktardaki nakit paranın şüphe çekmemek için küçük miktarlara ayrıştırılarak bankaya yatırılması şeklinde gerçekleştirilebilmektedir.²²²

2.1.3.2. Ayrıştırma Aşaması

Ayrıştırma aşamasında, kara para aklayıcı sisteme yerleştirdiği kara parayı yasa dışı kaynağından uzaklaştırmak için karmaşık banka işlemlerini içeren birtakım faaliyetler gerçekleştirmektedir.²²³ Bu aşamada amaç; özellikle off-shore mekanizmalarının sıklıkla kullanıldığı bir dizi finansal yöntemler kullanarak, sisteme yerleştirilen kara paranın, araştırmaları yanıltmak amacıyla paranın yasal bir kaynaktan geldiği görünümünü vermektir. Kara para ile mücadele tedbirlerini kabul etmeyen ülkelerde gerçekleştirilen bankacılık işlemleri araştırmacıların para izini takip etmesini zorlaştırmaktadır.²²⁴

2.1.3.3. Bütünleştirme Aşaması

Aklama işleminin son aşaması olan bütünleştirme aşamasında ise yasal ekonomiye yeniden giren paranın, gayrimenkul, araba, değerli metal, mücevher veya antika gibi

²¹⁹ Mustafa Miynat ve Selim Duramaz, “Kara Para Aklama Aracı Olarak Yeni Bir Mali Suç: Siber-Aklama”, *Yönetim ve Ekonomi* 20/1, Manisa 2013, s.317.

²²⁰ “Money Laundering: Methods and Markets”, s.25.

²²¹ Jean-François Thony, “Money Laundering and Terrorism Financing”, France 2010, s.3.

²²² Crime and Misconduct Commission, “Background Intelligence Brief, Money Laundering”, 2005, s.3.

²²³ Crime and Misconduct Commission, “Background Intelligence Brief, Money Laundering”, s.4.

²²⁴ Thony, “Money Laundering and Terrorism Financing”, s.3.

ürünlerin satın alınarak yasal bir şekilde kazanıldığı izlenimi verilmektedir. Alternatif olarak bu fon yatırım amaçlı da kullanılabilir. Yasa dışı paranın yerleştirme ve ayrıştırma aşamalarında herhangi bir denetim geçmişi yoksa bütünleştirme aşamasında tespit edilebilmesi çok zordur.

2.1.4. Kara Para Aklama Yöntemleri

Suçlular, suçtan elde ettikleri gelirleri finansal sisteme akıtabilmek için çok çeşitli metot ve teknikler geliştirmişlerdir. Bu yöntemler ülkeden ülkeye göre değişebilmektedir. Kara para aklama yöntemlerinden en sık olarak kullanılan yöntemler şu şekilde belirtilmektedir:

2.1.4.1. Parçalama (Structuring) Yöntemi

Yüksek miktardaki kara paranın küçük miktarlara parçalanarak çok sayıda farklı kişinin farklı bankalardaki hesaplarına yatırılması şeklinde yapılmaktadır.

2.1.4.2. Fonların Fiziki Olarak Ülke Dışına Kaçırılması; Nakit Kaçakçılığı

Nakit paranın genellikle kurye tarafından veya yük gemileri ile yasal denetimi az olan ülkelere çıkarılması ile yapılmaktadır.²²⁵

2.1.4.3. Kumarhane ve Gazinolar

Kumarhaneler, doğası gereği sahip olduğu hız ve müşterilerine çok geniş ölçekte sunduğu finansal hizmetler nedeniyle kara para aklayıcılar için tercih edilmektedir.²²⁶

²²⁵ Crime and Misconduct Commission, “Background Intelligence Brief, Money Laundering”, s.4.

²²⁶ Constantin Nedelcu, “Money Laundering Techniques Commonly Used. General Approaches”, Bucharest, s.36-39.

2.1.4.4. Şirinler (Smurfing) Yöntemi

Bu yöntemde suçtan elde edilen gelir, bankaların şüpheli işlem bildirimine takılmamak için bankalar tarafından belirlenen eşik değerin altındaki bir meblağda bankalara yatırılmaktadır. Bankalara yatırılan bu para kıyı bankacılığı yapan banka hesaplarına aktarılmaktadır.²²⁷

2.1.4.5. Paravan (Kâğıt Üstündeki) Ya Da Hayali Şirketler

İlgili ülkenin mevzuatlarına göre ve genel olarak vergilendirmenin az veya hiç olmadığı ülkelerde kurulan fakat herhangi bir üretim veya ticaret faaliyetinde bulunmayan bu şirketler üzerinden fon transferleri sağlanarak kara para aklama işlemi gerçekleştirilmektedir.

2.1.4.6. Alternatif Havale Sistemleri (Hawala vs.)

Hawala, alternatif para transfer sistemi olarak tanımlanmaktadır. Geleneksel bankacılık sisteminin veya finansal kanalların dışında gerçekleşen para transferi Hindistan’da Western bankacılık uygulamasının öncesinde geliştirilmiş bir yöntemdir. Yer altı bankacılığı olarak da adlandırılan bu sistemde para hareket ettirilmeden yer değiştirmektedir.²²⁸

Çomaklı 2018 tarihli Hawala Method in Terrorism Financing and Money Laundering isimli makalesinde özellikle Amerika Birleşik Devletleri’nde gerçekleştirilen 11 Eylül saldırılarından sonra hawala ve alternatif havale sistemleri gibi kayıtdışı banka sistemlerinin terörist finansmanı ve kara para aklama ile ilişkilendirildiğinin düşünüldüğünü belirtmektedir. Diğer taraftan hawala ve alternatif havale sistemlerinin Terörün finansmanı ve kara para aklama gibi yasa dışı amaçlar doğrultusunda kullanıldığı ile ilgili verilerin sınırlı olduğu da ifade edilmektedir. Alternatif havale sistemlerinin resmi olmayan ve sıklıkla lisanssız/yetkisiz bir şekilde paranın diğer bir coğrafik bölgeye transfer edilmesine olanak sağlayan güvene dayalı

²²⁷ OECD, “Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors”, 2009, s.37.

²²⁸ Patrick M. Jost ve Harjit Singh Sandhu, “The Hawala Alternative Remittance System and its Role in Money Laundering”, Financial Crimes Enforcement Network Report, USA, s.5.

bir mekanizma olduđu belirtilmektedir. Bu tür mekanizmalarda gerçek nakitin yerine bir çeşit değerin transfer edildiđi ifade edilmektedir. Alternatif havale sistemlerinin ismi ve sistemi kullanılan bölgede zaman zaman değışiklik gösterse de genellikle Güney Asya, Orta Dođu ve Afrika'nın bazı bölgelerinde yaygın olarak kullanıldığđı belirtilmektedir. Hawala sisteminin resmi finansal kurumlardan bağımsız olarak hem iç hem uluslararası para transferlerinin düşük maliyetlerde, hızlı ve güvenli bir şekilde yapılmasını sağladığđı ifade edilmektedir. Hawala ve alternatif havale sistemlerinin ilk olarak özellikle bankacılık sistemlerinin gelişmediđi ya da az gelişmiş bölgeler gibi uzak yerler arasındaki ticareti daha kolaylaştırmak amacıyla geliştirildiđinin söylenebileceđi belirtilmektedir. Arapça'dan türetilen hawala kelimesindeki h-w-l'nin köken anlamının çek ve borç senedini tanımlamak için, değıştirmek ve transfer etmek anlamlarında kullanıldığđı ifade edilmektedir. Para transferini gerçekleştiren komisyoncunun ise "hawala komisyoncusu" veya "hawaladar" olarak isimlendirildiđi de belirtilmektedir. Ayrıca hawala komisyoncularının birbirlerine ve müşterilerine karşı dürüst oldukları ve sistemin tamamıyla dürüstlük üzerine kurulu olduđu da ifade edilmektedir. Hawalanın Güney Asya'da ortaya çıkan çok eski bir sistem olduđu ve kökeninin klasik İslam Hukuku olan Şeriat olduđu ve sekizinci yüzyılın başlarında İslam Hukuku'nda yer aldığđı da belirtilmektedir. Hawala sisteminin Çin ve Hindistan'daki tüccarların İpek yolundaki soygunlar sebebiyle çok yüksek miktardaki parayı yollarında taşımamak için aradıkları bir yol olarak ortaya çıktığđı düşünüldüğü de ifade edilmektedir. Hawala sisteminin ilk kullanıcılarının Hindistan, Dođu Asya, Afrika ve Dođu Avrupa'dan Kuzey Amerika Avrupa ve Basra Körfezi'ne göç eden kişiler olduđu belirtilmektedir. Hawala'nın bankacılık sistemleri ile karşılaştırıldığında daha düşük komisyon ücretleri ile paranın daha hızlı, güvenli ve uygun bir şekilde transfer edilerek daha çok göçmenlere olanak sağladığđı da ifade edilmektedir. Hawala sisteminin bazı eyaletler ve diğer bazı bölgelerde yasa dışı sayılmasına karşılık Birleşik Arap Emirlikleri, Pakistan, Afganistan ve Hindistan gibi birçok ülkede yasal ve efektif bir sistem olarak kullanıma elverişli olduđu da belirtilmektedir. Birçok ülkede yurt içi ve yurt dışı para transferlerini gerçekleştirecekler için lisanslandırma koşullarının belirlendiđi ve bu koşulların sıkı denetim altında olduđu ifade edilmektedir. Buna karşılık hawala komisyoncularının sıklıkla meşru bir işe sahip olduđu ve bu durumun da hawala komisyoncularının kişisel

olarak tanımlanmasını zorlaştırdığı belirtilmektedir. Diğer taraftan Hindistan ve Pakistan gibi Güney Asya ülkelerinde resmi döviz kuru ve yerel para spekülasyonu dışında yabancı para birimlerinin alım satım işlemlerinin kanunlarca yasaklandığı ve bu durumun da var olan hawala sistemini yasa dışı kıldığı ifade edilmektedir. Tüm bunlara karşılık hawala sisteminin geleneksel bankacılık sistemine bir alternatif sistem olarak varlığını sürdürdüğü de belirtilmektedir. Hawala, paranın fiziksel olmayan bir şekilde transfer edilmesi olarak ifade edilmektedir. Hawala komisyoncularının Avrupa ve Kuzey Amerika'nın kaldırım bankaları ve mütevazı ofislerinden, arka odalar ve gizli yerlere kadar Güney Asya'nın birçok yerinde çalıştığı belirtilmektedir. Hawala sisteminin banka makbuzu veya sözleşme gibi arkasında herhangi bir kayıt tutmadan çalıştığı ifade edilmektedir. Hawala ağını kullanan birisinin dünyanın herhangi bir yerinde ve herhangi bir zamanında üzerinde binlerce Doları taşıyabileceği belirtilmektedir. Hawala sistemindeki tek kısıtın, paranın gönderici tarafından transfer edilmesi ve parayı alan hawala komisyoncusunun finansal kapasitesi ile ilgili riskler olduğu ifade edilmektedir. Geleneksel hawala yönteminde parayı gönderen, parayı alan ve iki hawala komisyoncusu olmak üzere dört kişiye ihtiyaç olduğu belirtilmektedir. Genellikle göçmen olarak çalışan bir kişi müşteri olarak hawala komisyoncusuna ulaştığı ve diğer bir şehir veya ülkede yer alan alıcısına gitmek üzere Dolar veya diğer tahvili mümkün bir para biriminde ödeme yaptığı ifade edilmektedir. Hawala komisyoncularının şehir veya ülke içerisinde telefon veya faks ile iletişim kurduğu da belirtilmektedir. Kadın veya erkek bu kişiler genellikle kişisel veya iş ağıları sebebiyle birbirlerini tanımakta olduğu ifade edilmektedir. Hawala komisyoncusu bu kişiye alıcıya gitmek üzere alıcının adı, adresi ve telefon numarası ile birlikte bir sonraki işlemde borcu kapatmak için de söz vererek parayı teslim ettiği belirtilmektedir. Parayı gönderen müşterinin gerçekleştirilen işlemle ilgili hiçbir zaman bir makbuz alamayacağı bunun yerine bir işlem kodu alabileceği de ifade edilmektedir. Alıcılar şehirde nerede yaşıyorlarsa hawala komisyoncuları ile iletişim kurdukları ve daha önce kendilerine verilen işlem kodundan başka hiçbir kimlik numarası gibi bir belge ibraz etmek zorunda kalmadan kendilerine gönderilen parayı yerel para birimi cinsinden alabildikleri belirtilmektedir. Bu işlem için ne bir kayıtlı anlaşma ne de yazılı bir sözleşme yapıldığı da ifade edilmektedir. Anlaşmanın kişiler arasında korunan güvene dayalı olduğu ve iki taraf arasına gerçekleştirilen işlemin

yasal olarak geriye dönük sorgulanamayacağı da belirtilmektedir. Delhi’de ismini gizleyen bir hawala komisyoncusunun ifadesine göre dünyanın herhangi bir yerine para transferini sekiz saat içerisinde gerçekleştirebileceği belirtilmektedir. Hawala komisyoncusunun ayrıca paranın yasal veya yasa dışı yollardan gelip gelmemesinin kendileri için hiçbir önemi olmadığı da vurgulanmaktadır. Resmi finans kurumlarının para transferlerinde toplam paranın %10 ila %15’i arasında değişen çok yüksek komisyon ücretleri talep ettiği belirtilmektedir. Hawala sisteminin komisyon ücreti uzaklık ve gönderilecek miktarın doğasına bağlı olarak resmi finans kurumlarının üzerinde ekonomik olarak önemli bir avantaj sağladığı ifade edilmektedir. Hawala komisyoncularının güçlü etnik ve akrabalık bağları olan bireylerden özellikle de göçmenlerden para transferlerini teşvik etmek için ücret talep etmedikleri de belirtilmektedir. Diğer taraftan hawala sisteminin sermaye veya idari kontrollerden kaçınmak için kullanılması durumunda çok daha yüksek ücretlendirmeler yapıldığı ifade edilmektedir. Böylelikle hawala komisyoncularının düşük olan genel işlem maliyetlerinin bu şekilde karşılandığı da belirtilmektedir. Alternatif havale sistemleri bankacılık sistemlerinin olmadığı veya çok yavaş ve pahalı olduğu ülkelerde, yurt içi veya yurt dışı para transferlerinde etkili bir fonksiyona sahip olduğu ifade edilmektedir. Bazı durumlarda hükümet kurumlarının acil insani yardımlar için değer transferlerinde alternatif havale sistemleri yöntemine başvurması gerektiği de belirtilmektedir. Avrupa Komisyonu tarafından finanse edilen çeşitli yardım gruplarının Afrika ve Asya’nın çeşitli ülkelerine gerçekleştirdikleri fon transferlerinde sıklıkla alternatif havale sistemlerinin kullanıldığı ifade edilmektedir. Hawala sisteminin sahip olduğu avantajlara ek olarak, 11 Eylül saldırılarından sonra hawala sisteminin Terörün finansmanı ve kara para aklama ile ilişkili birçok ciddi suçlarda potansiyel bir role sahip olduğu şüphesi giderek artarak dikkat çektiği belirtilmektedir. Terör örgütlerinin sürekli daha yenilikçi ve karmaşık yöntemler geliştirme arayışı içerisinde olduğu ifade edilmektedir. Terörün finansmanı ve kara para aklama için hangi alternatif havale sistemlerinin kullanıldığı ile ilgili deneye dayalı bulgular için doğası gereği çok az olduğu belirtilmektedir. Hawala sisteminin ruhsatlı bankacılık sistemlerinin ve okuryazarlığın olmadığı durumlarda göçmen çalışanlar için ihtiyaca binaen yasal amaçlarla kullanılmasının yanı sıra gizlilik için sosyo-ekonomik ve siyasi nedenlerden dolayı da kullanıldığı ifade edilmektedir. Terörün finansmanı, vergi

kaçakçılığı, kara para aklama ve uyuşturucu ticareti gibi yasa dışı işbirliği ağları için eşsiz ve çok etkili bir sistem olduğu da belirtilmektedir. Hawala sisteminin doğası gereği kayıt dışı işlemleri suç örgütleri ve terör örgütleri için bu sistemi çekici kıldığı ifade edilmektedir. İşlem sırasında gizliliğin sağlanmasıyla birlikte para transfer işlemleri gerçekleştirildikten sonra olası bir denetim ve sorgulama durumları yapılması ihtimaline karşılık sistemin arkasında kayıtlı belge bulundurmadığı da belirtilmektedir. Hawala sistemi müşterileri ve yıllar içerisinde müşterileri ile gelişen ilişki arasındaki itibar ve güvene dayandığı ve bu nedenle kimsenin hata yapmaya cesaret edemeyeceği ifade edilmektedir. Sadece sistem içerisindeki ortakların birbirlerine güvenme ihtiyacı olmadığı, aynı zamanda hiç kimsenin yasa dışı faaliyet ağları ile irtibat kurmadığından emin olunması gerektiği de belirtilmektedir. Çünkü böyle bir durumun sürdürülebilir bir yaşam için para kazanan sistemdeki tüm kırılgan yapıların sonunu getireceğinin düşünüldüğü ifade edilmektedir. Mutlak güven ağına ihanet edenler, kendileri ve aile üyelerinin sosyal ve ticari olarak dışlanacağını bildikleri belirtilmektedir. Denetimlerin sıkı olmadığı fakir bölgeler veya resmi kurumlarda büyük miktardaki nakit transferlerinde büyük kayıplar ve çeşitli risklerle karşılaşıldığı ifade edilmektedir. Hawala sisteminin ise böyle yüksek riskli ülkelerde güvenilir bir para transferi aracı olduğu belirtilmektedir. Bu nedenle terör örgütlerinin hawala yöntemini tercih etmemesi için hiçbir neden olmadığı da vurgulanmaktadır. Hawala sisteminin potansiyel kötüye kullanımın yaratılmasındaki rolün büyük ölçüde 11 Eylül saldırıları nedeniyle kaynaklandığı ifade edilmektedir.²²⁹

Bunların dışında; kıyı bankacılığı, oto-finance borç yöntemi (loan-back), döviz büroları, nakit para kullanılan işyerlerinin işletilmesi (göstermelik şirketler), sahte fatura (hayali ihracat), internet bankacılığı ve elektronik para, nakit değişimi, sigorta şirketleri yoluyla, spor kulüpleri kurulması ve piyango ve talih oyunları yoluyla kara para aklama işlemleri gerçekleştirilmektedir.²³⁰

²²⁹ Şafak Ertan Çomaklı ve Murat Uzun, “Hawala Method in Terrorism Financing and Money Laundering”, *International Congress On Political, Economic and Social Studies*, Pesa Publications, 2018.

²³⁰ MASAK, “Aklama Yöntemleri”, <http://www.masak.gov.tr/tr/content/aklama-yontemleri/59> (Erişim: 30.12.2017).

2.1.5. Kara Para Aklama İle Mücadele

Suç, önce kişinin kendisine daha sonra üçüncü şahıslara ve neticede bir bütün olarak topluma maddi ve manevi olarak zarar vermektedir. Kara para aklama, toplumun avukatlık, muhasebecilik, noter gibi güven ilişkilerinin esas teşkil ettiği bazı mesleklere ve emlakçılık, bankacılık ve diğer finansal kuruluşlar gibi ekonomik sektörlerle karşı bir güvensizlik ortamının oluşmasına neden olabilmektedir. Suçtan elde edilen gelirlerin harcanması iş dünyası ve girişimciler arasındaki rekabeti de bozabilmektedir. Kara para aklama, suçlu kişiye faaliyetlerini ekonominin meşru zemininde başlatmasına, devam ettirmesine ve genişletmesine imkân sağlamaktadır.²³¹

Ülkenin kanunlarla tanımlamış olduğu suç kriterleri çerçevesinde suç işleyen bir kişi bu hareketinin öncelikle vergi otoriteleri, polis ve diğer hukuki yaptırım otoriteleri tarafından fark edilmesinin önüne geçmeye çalışmaktadır. Pozitif hukuka göre suç işleyen kişi, suçtan elde ettiği gelirlerini harcamadan önce, vergi denetmenlerinin denetimine takılmadan, gelirin yasal bir yolla elde edildiği görünümü kazandırmaya çalışarak “aklama” ile sisteme aktarma amacı taşımaktadır.²³² Suçlular; yasa dışı olarak elde ettikleri gelirlerin devlet otoriteleri tarafından tespit edilip, el konulmasının önüne geçmek, bir diğer ifadeyle yasa dışı yollarla elde edilen gelirlerin müsadere edilmesini engellemek, yasa dışı fonları kendilerinden uzaklaştırarak herhangi bir şekilde yargılanmalarının önüne geçmek, fonlardan elde ettiği kazançları vergiden uzaklaştırmak, yasa dışı fonları tekrar yatırım amaçlı ticarete kullanmak ve aklanan fonları kullanarak bir iş kurmak ve bu işin de meşru olduğunu göstermek amacıyla kara para aklamaya ihtiyaç duyarlar.²³³

Olağan dışı gerçekleşen işlemlerin tespiti, suçluların kimliğini ve yasa dışı faaliyetlerini belirlemeye yardımcı olabilmektedir ve bu bilgilerin kanun uygulayıcı otoritelerle paylaşılması suç araştırmalarının başlamasına imkân sağlamaktadır. Olağan dışı işlemlerin tespiti, para akışının ve otomobil, yat, gayrimenkul ve banka hesabı şeklinde aklanmış suç gelirlerinin hedefine ilişkin içyüzünü gösterebilmektedir.

²³¹ OECD, *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, s.12.

²³² OECD, *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, 2009, s.9.

²³³ Australian Government Australian Transaction Reports and Analysis Center, *Introduction to Money Laundering*, Avustralya 2008, s.2.

Ayrıca suç araştırması sırasında hukuki olarak bu varlıklara el konulabilmesine de olanak sağlamaktadır.²³⁴

Uyuşturucu kaçakçılığı, insan kaçakçılığı, hırsızlık, yatırım dolandırıcılığı, gasp, rüşvet, yolsuzluk ve vergi kaçırma gibi suçlar işleyerek önemli miktarlarda para elde etmektedirler. Kara para aklama, yasal ekonomiyi tehdit eden ve üzerinde önemle durulması gereken ciddi bir unsurdur ayrıca finansal kurumların bütünlüğünü etkilemektedir. Bazı sektörlerde de ekonomik gücün değişmesine bile neden olabilmektedir. Bu nedenle kara para aklama ile mücadele çeşitli amaçlara hizmet etmektedir.²³⁵

Kara para aklayıcılar, kara para aklama faaliyetlerinin belirlenmesine ve denetlenmesine yönelik kanunların az veya hiç olmadığı yerleri tercih etmektedirler. Bu durum kara para aklama faaliyetinin dünya çapında uluslararası bir problem oluşturduğu sonucu doğurmaktadır. Kara para aklama ile mücadelede ülkelerin uluslararası arenada işbirliği yapması çok büyük önem taşımaktadır. Bu nedenle kara para aklama ve terörizm finansmanı ile mücadele kapsamında dünya genelinde birçok kurum gerekli tedbirlerin alınmasına yönelik faaliyetlerde bulunmaktadırlar. Dünya çapında kara para aklama ile mücadele kapsamında politika geliştiren dört büyük kurum şu şekildedir.²³⁶

- Mali Eylem Görev Gücü
- Uluslararası Kara Para Bilgilendirme Ağı (IMoLIN)
- Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC) (Birleşmiş Milletler kara para aklama ile mücadelede önemli faaliyetler gösteren ilk uluslararası kuruluştur.²³⁷)
- Interpol

Dünya çapında faaliyet gösteren bu kurumlar ve Mali Eylem Görev Gücü, üye ülkelerle bölgesel işbirliği kapsamında birlikte çalışır ve bilgi paylaşımında bulunmaktadır. Bu kurumlar aynı zamanda; Uluslararası Para Fonu (IMF), Dünya Bankası (World Bank), Avrupa Merkez Bankası ve Asya Kalkınma Bankası gibi

²³⁴ Age, s.12.

²³⁵ Age, s.11.

²³⁶ Consulting Technology Outsourcing, “The Growing Threat of Money Laundering”, s.14.

²³⁷ The World Bank, Paul Allan Schott, “Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism”, Washington 2006, s.III-2.

küresel ve bölgesel kurumlarla kara para aklama ve terörizm finansmanı ile mücadele kapsamında bilgi paylaşımında bulunmaktadırlar. Bununla birlikte, uluslararası kara para aklama ve bununla ilgili mali suçların giderek artan problemleri, Mali İstihbarat Birimleri olarak adlandırılan bu alanda özelleşmiş devlet kurumlarının ortaya çıkmasına neden olmuştur. Bu birimlerin başlıca görevi, finansal hizmet kurumları ve yargı alanları arasındaki sürekli bilgi alış verişini sağlamaktır.²³⁸

Kara para aklama ile mücadele kapsamında, 1970 yılından bu yana ülkelerin finansal kuruluşlarının gerekli tedbirleri alması amacıyla uluslararası tavsiye kararları alınmıştır.

İlk olarak 1970 yılında çıkarılan Banka Gizlilik Kanunu çerçevesinde kişiler, banka ve diğer finansal kuruluşlar arasında yapılan 10.000 Dolar ve üzeri para transfer işlemlerin kaydının tutulması ve raporlama yapılmasına yönelik yükümlülük getirilmiştir. Böylelikle, para kaynağının ve paranın hareketinin kolaylıkla belirlenmesine imkân sağlanmıştır.²³⁹

1988 yılında banka gözetim ve denetim kurumları ve merkez bankaları temsilcileri tarafından çıkarılan Basel Komitesi İlkeler Bildirisi ile kara paranın mali sistem ile aklanmasına yönelik alınacak tedbirler belirlenmiştir. Ayrıca 1988 yılında Türkiye'nin de katkı sunduğu Viyana Sözleşmesi yayınlanmıştır.²⁴⁰

Mali Eylem Görev Gücü, ilk olarak 1990 yılında Kara Paranın Aklanması ve Terörizm Finansmanı ile Mücadele Kapsamında çıkardığı 40 tavsiye Kararı'nı 1996 yılında güncellemiştir.²⁴¹

1991 yılında Mali Sistemin Kara Para Aklama Amacıyla Kullanılmasının Önlenmesi'ne dair Avrupa Birliği Konseyi Direktifi yayınlanmıştır. Avrupa Konseyi ve Avrupa Parlamentosu tarafından 2001 yılında yayınlanan direktifle, kara para aklama ile mücadeledeki öncül suç kapsamı genişletilmiştir. Ayrıca 2005 yılında Avrupa Komisyonu tarafından çıkarılan Finansal Sistemin Kara Para Aklama ve

²³⁸ Consulting Technology Outsourcing, "The Growing Threat of Money Laundering", s.16.

²³⁹ History of Anti-Money Laundering Laws, <https://www.fincen.gov/history-anti-money-laundering-laws> (Erişim: 01.01.2018)

²⁴⁰ Kayahan Çelik, Kara Para Aklama Suçuyla Ulusal Ve Uluslararası Düzeyde Mücadele Ve Türkiye Örneği, Atatürk Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisan Tezi, Erzurum 2011, s.57.

²⁴¹ FATF, International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation – The FATF Recommendations, 2017, s.6

Terörün Finansmanı Amacıyla Kullanılmasının Önlenmesine Dair 2005/60 sayılı Direktif ile 1991 yılında yayınlanan Direktif yürürlükten kaldırılmıştır.²⁴²

Uluslararası bir suç olan kara para aklama ile mücadele kapsamında ülkeler ilk olarak yasal reformlar yapmak yerine bankacılık düzenlemeleri ve etik kurallar çerçevesinde konuyu ele almıştır. Bu önlemlerin yeterli gelmemesi üzerine ülkeler yasa dışı finansal akışları ve kara para aklamayı kontrol etmek amacıyla ulusal ve uluslararası seviyede bir dizi sözleşme, çözüm önerileri ve eylem planları yayınlamışlardır. 1988 yılında Viyana Konvansiyonu ve Mali Eylem Görev Gücü Tavsiyeleri, yine aynı yılda yayınlanan Siyasi Deklarasyon ve İlgili Eylem Planı, 2000 yılında yayınlanan Palermo Sözleşmesi, uyuşturucu ile mücadele kapsamında 2009 yılında yayınlanan eylem planı şeklinde ifade edilmektedir. Kara para aklamanın yasal tarihçesi, Viyana Uyuşturucu Sözleşmesi kapsamında uyuşturucudan elde edilen gelirlerin suç kabul edilmesiyle başladığı belirtilmektedir. Bu nedenle uyuşturucu ile ilgili suçlar, kara para aklamanın ilk ve tek öncül suç unsurunu oluşturmaktaydı. Başlangıç aşamasında sadece uyuşturucuya bağlı suç gelirlerini aklamaya çalışmak kara para aklama suçu olarak kabul edilir ve yargılama buna göre yapıldı. Daha sonra kara para aklamanın öncül suç tanımları genişletilmiştir.²⁴³

2.1.6. Kara Para Aklama Sisteminde Kripto Paranın Yeri

Uzun yıllar boyunca suçluların farklı ekonomi alanlarındaki kullanımlarından elde ettikleri yasa dışı gelirlerini meşrulaştırmak veya aklamak için yollar bulmaya çalıştıkları açıktır. Günümüzde dijital para aklama kripto paraların sahip olduğu özellik olan anonim özelliğini kullanarak başarılı bir şekilde gerçekleştirilebilmektedir.

²⁴² Oktay Üstün, Kara para Aklama ve Terörün Finansmanı ile Mücadelede Uluslararası Girişimler ve Araçlara Toplu Bakış, Bankacılar Dergisi, Sayı 65, 2008, s.23.

²⁴³ Kumar, Krishna, "Functioning of anti money laundering legislation in India a critical study", Tamil Nadu Dr. Ambedkar Law University Doktora Tezi, 2015, https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0ahUKEwiPp9zIo9DYAhVkyZoKHV_nBUUQFghSMAU&url=http%3A%2F%2Fshodhganga.inflibnet.ac.in%2Fbitstream%2F10603%2F76711%2F7%2F07_chapter%25201.pdf&usg=AOvVaw0SIC6Uan454RKXEdeujyV, (Erişim: 05.01.2018), s.29.

Kara para aklama belirli bir gizlilik hedefi için gelirin asıl kaynağının gizlendiği finansal işlem ve diğer faaliyetler olarak tanımlanabilmektedir. Dünya pratiğine bakıldığında tarihte en büyük kara para aklama örneğinin Liberty Reserve olduğu bilinmektedir. Amerika Birleşik Devletleri Adalet Bakanlığı 2013 yılının Mayıs ayında yedi yönetici ve çalışanının bulunduğu Liberty Reserve şirketine (elektronik işlemlerinin Kosta Rika’da yapıldığı) karşı suçlamalarda bulunmuştur. Liberty Reserve şirketi 6 milyon ABD Dolarından fazla miktarda yasa dışı gelirin para transferi hizmetleri ve kara para aklama şeklinde kayıt dışı ticari faaliyetlerde bulunması sebebiyle suçlanmıştır. Bu sistem ABD’deki 200 bin kullanıcı da dâhil olmak üzere tüm dünyada milyonlarca kullanıcıyı da içeren devasa boyutlarda faaliyet gösterdiği bilinmektedir. Sisteme göre yaklaşık olarak neredeyse hepsinin yasa dışı olduğu belirlenen 55 milyon işlem gerçekleştirildiği tespit edilmiştir. Sistem içerisinde Liberty Dollars adında işlem parasının başlangıç ve bitiş noktalarında fiat para birimine dönüştürülerek saklanan kendi kripto paraları da yer almaktaydı.

Modern teknolojiler kripto paranın sahip olduğu aşağıda belirtilen birtakım özelliklerden dolayı özellikle kara para aklama işlemlerinde kolaylaştırmaktadır.

- Kripto para adresi ve protokolleri müşteri kimliği bilgisini gerektirmediğinden dolayı gerçek kişi ile sanal para arasındaki bağları ortadan kaldırmaktadır.
- Herhangi bir insana ihtiyaç duymadan basitleştirilmiş sistemleri kullanarak iletişim kurmak mümkündür. Sanal paraların alım satım işlemlerinde katı düzenlemeler mevcut değildir.
- Sınırsız sayıda hesap oluşturma imkânı ile tüm işlemlerin kontrol edilmesini olanaksız bırakmaktadır.
- Kripto para gönderen sanal cüzdan adreslerinin izlenmesi durumunu ortadan kaldırmak için birkaç işlemin karıştırılarak bir araya getirilmesiyle ve Dark Wallet gibi araçlar kullanarak özel faaliyetlerin geri izlenmesi engellenmektedir. Bununla birlikte işlemleri belirli web trafiğini çeşitli röleler üzerinden yönlendiren ToR ağı üzerinden gerçekleştirerek gerçek kullanıcının IP adreslerinin gizlenmesini sağlamaktadır.

Bu nedenle kripto para teknolojisinin suçluların tespit edilme imkânını neredeyse ortadan kaldırarak farklı kara para aklama uygulamalarına izin verdiği ifade edilmektedir. Bu özellik kanun uygulayıcı kurumlara kara para aklama soruşturmaları

için yeni yöntemleri bulma konusunda yeni zorluklar getirmektedir. Ayrıca yukarıda belirtilen kripto paranın karakteristik özellikleri tüm dünyadaki kanun yapıcılarını kripto paranın ödeme aracı olarak kullanımı ile ilgili yasama sistemini tek biçimli hale getirmek için güdülemektedir. Kripto paranın devlet tarafından tanınmamasının kara para aklamayı önlemek ve mücadele etmek işlemlerini nerdeyse imkânsız kılacağı ifade edilmektedir.²⁴⁴

2.2. TERÖRÜN FİNANSMANI VE KRİPTO PARA

Terör örgütleri yasa dışı faaliyetlerini finanse edebilmek amacıyla çeşitli yollardan mali kaynak temin etme yoluna giderler. Terörizm finansmanı yasa dışı kaynaklardan elde edilebileceği gibi bazen yasal kaynaklar vasıtasıyla da elde edilmektedir. Terör örgütleri başta uyuşturucu ve silah kaçakçılığı olmak üzere, kara para aklama, vakıf, dernek gibi kuruluşlardan temin edilen aidat ve bağışlar vasıtasıyla yasa dışı faaliyetleri için finans temininde bulunmaktadır.²⁴⁵ Terör örgütlerinin finans faaliyetleri, finansal kaynak toplama, yasa dışı uyuşturucu ve silah kaçakçılığı, havale/transfer, saldırı fonu ve operasyonel fonlama şeklinde beş kategoride tanımlanabilmektedir:

- Finansal kaynak toplama, terör örgütlerinin tüm diğer faaliyetlerini destekleyebilmek için silah satın alımı, saldırıların desteklenmesi ve diğer operasyonel faaliyetlerden oluşmaktadır.
- Yasa dışı uyuşturucu ve silah kaçakçılığı terör örgütlerini desteklemek için bir diğer gelir kaynağı olabilmektedir.
- Terör örgütleri, maaşlı çalışanları dâhil üyelerinin ve ortaklarının nakit ihtiyaçlarını karşılayabilmek için havale ve transfer işlemlerine gereksinim duymaktadır.
- Terör örgütleri, silah satın alımı veya diğer operasyonel giderler dâhil terörist saldırıların desteklenmesi için saldırı fonlamasına ihtiyaç duymaktadırlar.

²⁴⁴ Valeria Dyntu ve Oleh Dykyi, “Cryptocurrency In The System of Money Laundering”, *Baltic Journal of Economic Studies*, Vol. 4, No. 5, 2018, s.78-79.

²⁴⁵ “Terörün Finans Kaynakları”, <http://www.masak.gov.tr/tr/content/terorun-finans-kaynaklari/72>, (Erişim: 15.12.2017),

- Terör örgütleri genel güvenlik, iletişim ve örgütün yönetilmesi ve finanse edilmesi için operasyonel faaliyetlere ihtiyaç duymaktadırlar.²⁴⁶

Kripto para kullanımının terörist gruplar tarafından potansiyel bir araç olduğunu anlamının ilk yolu, terör örgütlerinin parayı nasıl kullandığını düşünmenin ve bu tür kullanımlar için ihtiyaç ve fırsatlarını belirlemenin faydalı olacağı ifade edilmektedir. Terör örgütlerinin parayı kullanımının hasılat, yönetim ve harcama şeklinde üç kısımdan oluştuğu düşünülmektedir. Hasılat kısmı; en yaygın terörist fon kaynakları devlet kaynaklı, hayırsever veya kişisel bağışlar, yasa dışı faaliyetler (uyuşturucu kaçakçılığı ve diğer kaçakçılık faaliyetleri, dolandırıcılık, haraç ve küçük suçlar), ve yasal kaynaklar olarak belirtilmektedir. Bu kaynaklardan hangisini ve/veya hangilerini tercih edecekleri terör örgütünün tercihlerine, uygunluk durumuna ve zamana göre değişiklik gösterebilmektedir. Terör gruplarının terör örgütleri için para toplama kapasitelerinin istihbarat ve kolluk kuvvetleri tarafından kısıtlanması, terör örgütlerini alternatif fon oluşturma aramalarına itmektedir bu durumda da yetkililerin bu duruma karşı yeni yöntemler geliştirmesi gerekliliği de ortaya çıkmaktadır.²⁴⁷ Fon sağlandıktan sonra terör örgütleri parayı yönetmek durumundadırlar bu kısım da yönetim ve transfer kısmını oluşturmaktadır. Eğer temin edilen para terör örgütlerinin direk kontrolü altında değilse veya operasyonel güvenlik endişeleri nedeniyle transfer edilemediyse bu durumda kara para aklama ve diğer transfer mekanizmaları kullanılabilir. Bu durum harici bir fonlamaya bel ağılayan terör örgütleri için çok kritik bir konudur ama DAES gibi dış bir fonlamaya çok gereksinim duymayan terör örgütleri için ise daha az kritik bir konu haline gelmektedir. Hizbullah terör örgütü daha çok devlet destekli bir fonlamaya sahip iken ve İran ve Libya bankacılık sistemlerine erişme imkânına sahipken El – Kaide terör örgütü ise diğer metotları daha çok kullanmaktadır.²⁴⁸ Terör örgütleri tarafından fon yönetimi kripto para açısından ilgi çekici olabilmektedir. Mali Eylem Görev Gücü büyük örgütlerin çok sayıda yönetim, raporlama, hesaplama ve finansal planlama ile birlikte gelişmiş finansal alt yapılara bel bağladıklarını belirtmektedir.²⁴⁹ Terörist gruplar topladıkları fonları

²⁴⁶ Cynthia Dion ve diğerleri, “Terrorist Use Of Cryptocurrencies: Technical and Organizational Barriers and Future Threats”, *RAND Corporation*, Santa Monica, 2019, s.15.

²⁴⁷ *Age*, s.8.

²⁴⁸ *Age*, s.10.

²⁴⁹ *Age*, s.12.

harcamaktadırlar bu harcama kısmını oluşturmaktadır. Farklı terörist gruplar kendi ihtiyaç ve amaçları doğrultusuna göre bütçe yapmaktadırlar. Birçok terörist grubun faaliyet gösterdikleri bölgelerdeki sınırlı erişim ve kullanım nedeniyle kripto para kullanma kapasiteleri şu an itibarıyla sınırlı olduğu söylenmektedir. Örneğin Orta Doğu’da birkaç Bitcoin ATM’si bulunmaktadır ve bu durum Bitcoin’in fiat para karşılığında alım satımını zorlaştırmaktadır.²⁵⁰

Modern teknolojinin gelişmesiyle birlikte güvenlik alanındaki önem ve ilgi, sahip olduğu düşük bağlantı maliyetleri, gizlilik ve potansiyel asimetrik savunmasızlık gibi karakteristik özellikleri sebebiyle güvenlik riski oluşturan siber netik uzay kavramını ortaya çıkarmıştır²⁵¹. Bugün dünyanın her tarafında terör örgütleri, örgütün finansal ihtiyaçlarını siber saldırılar, çevrimiçi propaganda veya açık kaynak bilgi toplama gibi faaliyetlerle siber netik uzayı kendi amaçları doğrultusunda kullanmaktadır. Diğer suç örgütlerinde de olduğu gibi terör örgütlerinin amacı etkin finansal altyapılar inşa edebilmek ve bunun devamlılığını sağlayabilmektir. Bu nedenle interneti kullanarak çevrimiçi fonlama, çevrimiçi materyal satışı gerçekleştirme veya kripto para elde etme şeklinde finansal kaynak geliştirme yoluna gitmişlerdir. Kripto para modern teknolojiler arasında terör örgütleri tarafından ihtiyaç duydukları finansal kaynak temini için yaygın olarak kullanılmaktadır. Kripto paranın doğası gereği sahip olduğu merkezi olmayan dağıtık ödeme sistemi, işlemlerin kriptolojik protokoller üzerinden anonim olarak yapılabilmesi ve madencilik denilen yöntemle kolaylıkla elde edilebiliyor olması terörist gruplar için potansiyel finans kaynağı oluşturmaktadır.²⁵² Terör örgütleri dolandırıcılık, kara para aklama ve diğer yasa dışı aktivitelerle paranın her türlü formunu kullanmaktadırlar. Fakat Bitcoin’in ödeme işlemlerinin hızlı ve kolaylıkla yapılabilmesi ve bunun yanı sıra gizlilik özelliğinin oluşturduğu cazibe, suç girişimcilerine ilham kaynağı oluşturmaktadır.

İnternet bir taraftan anonimlik sunarken, diğer taraftan ulusal sınırların göz ardı edilmesine neden olmaktadır. Birçok ülke siber uzay tehditleri ve özellikle ulusal güvenliğe sorun teşkil eden siber terörizme karşı derin endişe etmektedirler.

²⁵⁰ Age, s.13.

²⁵¹ Carata, “Modern Methods of Financing Terrorism In A Global and Intercultural Society: Crypto-Currency”, s.192.

²⁵² Age, s. 193.

Anonimlikle ilintili deep web ve dark web iletişim ve ticareti gizlemektedir. Bu durum örgütlü suçlara ve terör örgütlerine gelecek faaliyetleri için ticaret, iletişim, plan ve özel saldırı şeklinde yeni fırsatlar sunmaktadır.²⁵³

Teröristlerin 1990 yılından beri çeşitli çevrimiçi platformlarda faaliyetlerini sürdürdüğü ifade edilmektedir. Yüzey ağının kullanılması anonimlik arayan teröristler için çok riskli olduğu belirtilmektedir. Yüzey ağ üzerinde teröristlere ait birçok internet sitesi ve sosyal medya hesabı terörle mücadele kurumları tarafından sıklıkla hacklenmiş veya kapatılmıştır. Ama dark web üzerinde merkezi olmayan ve anonim ağlar bu terörist platformlarının kapatılmasını ve teröristlerini yakalanmasına engel olduğu bilinmektedir. Teröristlerin dark webi yüzey ağını kullandıkları gibi uzun yıllardır kullanmakta oldukları belirtilmektedir. Fakat dark web teröristlerin daha çok siber meraklı üyelerine yeni fırsatlar sunduğu ifade edilmektedir. Teröristler interneti örgütün diğer üyeleri ile iletişimde bulunmak, işe almak ve radikalleşme çalışmalarında, propaganda yaymak, fon sağlamak ve eylem ve saldırıları koordine etmek için kullandıkları belirtilmektedir. Bu faaliyetlerin tümü artık günümüzde internetin daha derin katmanlarında doğru kaydığı ifade edilmektedir. Teröristler için propaganda malzemesinin artık günümüzde dark web’te toplandığı belirtilmektedir. Teröristler daha öncekinden daha güvenli olarak iletişimde bulunmak için dark webi kullandığı ifade edilmektedir. Uzun bir süre terörist saldırıların gizli ağlardan koordine edildiği sanılsa da, sağlam kanıtların 2013 yılında elde edildiği belirtilmektedir. ABD Ulusal Güvenlik Ajansı, Arap Yarımadası’nda El – Kaide lideri Ayman Al-Zawahiri ile Yemen merkezli El Kaide lideri Nasir Al – Wuhaysi arasındaki şifreli iletişimi çözmüştür. Ulusal Güvenlik Araştırmaları Enstitüsü yaklaşık on yıl boyunca dünya çapındaki El Kaide ağının liderleri arasındaki iletişimin darknet veya deep web aracılığıyla yapıldığını açığa çıkarmıştır. Dark netin sanal paraları kullanarak gizli fon transferi için suçlularla birlikte teröristler tarafından da kullanıldığı belirtilmektedir. Bu yeni eğilimin Terörün ve dark netin kabiliyetlerinin en çok endişe verici kombinasyonlarından biri olarak nitelendirildiği ifade edilmektedir. Nakit paranın dijital eşdeğeri olarak nitelendirilen kripto para sıklıkla yasa dışı ticaret, şantaj ve kara para aklama ile ilgili ödemelerde suçlular tarafından kullanıldığı belirtilmektedir.

²⁵³ MJ Aschmann, L. Leenen ve JC Jansen van Vuuren, “The Utilisation of The Deep Web For Military Counter Terrorist Operations”, South African National Defence Force, South Africa s.1.

Teröristler dark web'i Bitcoin ve diğer kripto para birimlerini kullanarak kaynak toplama, para transferi gerçekleştirme ve yasa dışı patlayıcı ve silah alımı için kullanabilmektedirler. Bazı raporlar dark webin bazı terör örgütleri için karaborsa insan organlarını (ellerinde bulunan tutsaklarının) satmak için kullandıkları bir araç olduğunu ortaya koymaktadır. Terörist grupların dark webi kullanma konusundaki artan eğilimin hükümetler, terörle mücadele ajansları ve güvenlik servisleri için zorlu bir mücadele meydana getirdiği belirtilmektedir. Teröristlerin dark webi kullanımını takip ve analiz etmek için yeni yöntemlerin geliştirilmesine acil ihtiyaç duyulduğu ifade edilmektedir. Amerikan İleri Savunma Araştırmaları Projeleri Ajansı (Defense Advanced Research Projects Agency – DARPA), cevabın deep web sitelerinin daha iyi kataloglanmasını sağlayan MEMEX yazılımında bulunabileceğine inandığı belirtilmektedir. Dark webin küresel terörizm ve suç faaliyetleri için büyük bir platforma dönüştüğü ile ilgili açık deliller sunmak, bununla mücadele edilmesi için gerekli araçların geliştirilmesini sağlamada ivme kazandırmak için kesinlikle önemli olduğu vurgulanmaktadır. MEMEX, başlangıçta deep webte insan kaçakçılığı faaliyetlerini izlemek için geliştirilmiş olsa da aynı ilkelerin neredeyse her türlü yasa dışı deep web faaliyetlerine uygulanabildiği ifade edilmektedir.²⁵⁴

Terörist operasyonları desteklemede fonlamanın kilit rolü göz önüne alındığında terörle mücadele çabaları özellikle terör finansmanı ile mücadele genellikle saldırıları ve diğer terörist faaliyetleri desteklemek için kullanılabilecek finansal işlemleri engellemek için banka hesapları aracılığıyla para akışlarını izlemeye odaklanmaktadır. Terör finansmanı ile mücadelenin başarısı fiat para birimlerinin yani devlet tarafından çıkarılan para birimlerine terörist erişimini azaltarak terörist organizasyonlarda Bitcoin gibi bu tip dijital kripto paraların kullanımını artırabileceği endişesine de yol açtığı ifade edilmektedir. Kripto paraların terörist grupların karmaşık ve teknolojik kapasitelerinin ve gelecekteki teknolojik gelişmeler de göz önüne alındığında potansiyel kullanımlarının tanımlanması ve izlenmesi için terörist faaliyetlerinde kullanım potansiyelinin tam olarak anlaşılabilmesi gerekmektedir. Kripto paraların meydan okuması aslında Bitcoin'in ötesine uzanmaktadır. Birçoğu teröristlerin ihtiyaçlarına uygun olabilecek şekilde tasarlanmış farklı özelliklere sahip

²⁵⁴ Gabriel Weinmann, "Terrorist Migration to the Dark Web, Perspectives on Terrorism", Vol. 10, Issue 3, s.41-42-43.

birçok kripto para ortaya çıkmıştır. Altcoin olarak adlandırılan ve Bitcoin'den çok daha özel ve güvenli bu nedenle yasa dışı faaliyetler için kişiye uygun gözüken bu kripto paralara örnek olarak MasterCoin, BlackCoin ve Monero gösterilmektedir. İşlemlerin herhangi bir sahibi tarafından kimliğinin belirlenemeyeceği ve bu nedenle yüksek derece gizlilik sunan bir başka kripto para olarak ZCash verilmektedir. ZCash'in ayrıca yüksek derecede sahip olduğu gizlilik, yasa dışı faaliyetlerin izlenmesi için kanuni yaptırımını zorlaştırmaktadır. Hawk gibi sunulan diğer formdaki kripto paralar Ethereum blok zincir üzerinde işlemlerin tamamen özel kontratlarla yapılmasına olanak sağlamaktadır. Teröristler tarafından artan kripto para kullanımı terör finansmanı ile mücadele faaliyetlerine zarar verdiği ifade edilmektedir. Eski yöntemler daha efektif olduğu için terörist organizasyonlar her ne kadar yeni metotları kullanmakta gönülsüz olsalar da terör finansmanı ile mücadelenin baskıları terörist grupların yenilik yapması için teşvikler oluşturabileceği de belirtilmektedir. Terörist grupların alternatif finansal sistemlere erişimleri kısıtlı olduğu durumlarda veya kripto paraların kendilerine önemli derecede fayda sağladığı durumlarda bu grupların kripto para kullanımlarını genişletebileceği ifade edilmektedir.²⁵⁵

Haziran 2015 tarihinde DAESH militanının sosyal medya hesabı Twitter üzerinden Bitcoin kullanarak terör örgütlerini nasıl finanse edebilecekleri ile ilgili paylaşımlarda bulunmuş ve aynı zamanda DAESH için yardım topladığı gerekçesi ile FBI tarafından yakalanarak 11 yıl hapis cezasına çarptırılmıştır.

Endonezya'nın Ulusal Terörle Mücadele Ajansı, İstihbarat Ajansı ve Finansal İşlem Raporları ve Analizi Merkezi'nin (Financial Transaction Reports and Analysis Centre – PPATK) birlikte yapmış oldukları çalışma çevrimiçi bağışların pratik olması sebebiyle terör gruplarını finanse etmek için tercih edilen bir yöntem olduğunu ortaya koymuştur. 2016 yılındaki Jakarta Saldırıları'nın beyni olduğu iddia edilen Bahrin Naim'in terörist faaliyetlerini finanse edebilmek ve militanlarına para transferi yapabilmek için PayPal ve Bitcoin kullandığı belirtilmiştir. Amerika vatandaşı olan Zoobia Shahnaz'ın Aralık 2017'de DAESH terör örgütünü desteklemek amacıyla yurtdışına 62 bin Dolar değerinde Bitcoin ve diğer kripto para transferi girişiminde bulunduğu ve banka dolandırıcılığı ve birden fazla kara para aklama suçlarından

²⁵⁵ Dion ve diğerleri, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats", s.2-3.

suçlandığı belirtilmektedir. Terörist grupların yasa dışı faaliyetleri finanse etmek amacıyla kripto paraları kötüye kullanması nedeniyle Mısır Büyük Müftüsü Shawki Allam Ocak 2018’de Bitcoin kullanılmasını yasaklayan bir fetva yayınlamıştır. Kripto paraların kullanım kolaylığı nedeniyle kara para aklama işlemlerinde, kaçakçılıkta ve kumar karakteri taşıyan (Maysir) işlemlerde kullanılmasına paralel olarak Mısır Büyük Müftüsü ayrıca herhangi bir düzenlemeye tabi olmayan sanal paraların dolandırıcılık risklerini taşıdığını ve bu nedenle bireylere, gruplara ve kurumlara zarar verdiğini ifade etmektedir. Suudi Arabistan Bakanı Assim Al – Hakeem dijital paraların suçlara anonimlik sağlaması sebebiyle yasak (haram) olduğunu belirtmiştir. Bitcoin ve diğer kripto paralar ticaret dünyasında her geçen gün daha fazla kabul görmeye başladığından dolayı kullanımı ile ilgili düzenleyici yasaların ve hukuki yaptırımların getirilmesi zorunlu bir hal almıştır. Yetkili makamların kripto paraların potansiyelini kullanmaları ve terör finansmanında kullanılmasının önüne geçmek ve erkenden önlemine almak için kripto paraların mekanizmasını anlaması gerekmektedir. Yetkili makamlar eğer bunu yapmakta başarısız olursa, siber güdümlü terörizm tarafından tamamen sömürülmeyi bekleyen bağımsız potansiyel olarak büyük finansal aracın gelişmesine imkân sağlayacaktır.²⁵⁶

Kripto paraları ve kripto para oyuncularını özellikle de kullanıcılarını verimli bir şekilde yakalamak için gereken kilit noktanın anonimliklerini (yarı ve tam anonimlik) yasal yollarla açığa çıkarmak olduğu ifade edilmektedir.²⁵⁷ Kara para aklama ve terör finansmanı ile mücadelede en büyük problemin ise anonimlikten kaynaklandığı belirtilmektedir. Anonimlik kripto para transferlerinin verimli bir şekilde izlenmesini engellemekte ve düzenleyici çevreden uzak bir şekilde gölgeli işlemlerle suç örgütlerinin kripto paraların temiz erişim sağlayabilmelerine izin vermektedir. Ali Shukri Amin’in Twitter üzerinden Bitcoin’in DAESH’e fon temininde nasıl kullanılacağı ile ilgili dokümanlar yayınlaması kripto paraların terör finansmanı ile ilişkili olarak anonimliğinin oluşturduğu riskin çarpıcı örneği olarak nitelendirilmektedir.²⁵⁸

²⁵⁶ Cryptocurrencies: Potential For Terror Financing?, Ahmad Helmi Hasbi and Remy Mahzam, s.2-3.

²⁵⁷ International Monetary Fund (IMF), “Virtual Currencies and Beyond: Initial Considerations”, January 2016, <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, 27.

²⁵⁸ Financial Action Task Force on Money Laundering (FATF), *Report on Emerging Terrorist Financing Risks*, October 2015, s.36.

Teröristlerin, suç örgütleriyle karşılaştırıldığında sanal paraları anlamlı ölçekte kullandığın çok az delillerinin mevcut olduğu, en çok atıfta bulunulan örneğin; DAESH (Irak ve Şam Devleti)'in destekçileri tarafından Bitcoin yoluyla internet üzerinden bağış topladığı durum olduğu belirtilmektedir. Teröristlerin sınırlı durumlarda faaliyetlerini finanse edebilmek için Bitcoin gibi kripto para birimlerini kullanmayı düşündükleri ile ilgili yeterli delil bulunmadığı, bu araçların popülerlik kazanmış olsalar da son yıllarda terörist kurumlarda bu yeniklerin yayılmasının çok daha yavaş olduğu ve bu teknolojilerin kullanımının uluslararası suçlarda henüz eşleşmediği ifade edilmektedir. Bu durumun devlet dışı aktörlerin politik, ekonomik ve operasyonel olarak güç elde etmeleri durumunda ileride değişebileceği ve sanal para kullanımının artabileceği sonucunu doğurduğu da belirtilmektedir.²⁵⁹

Devlet dışı aktörlerin sanal para kullanımlarının sosyal ve politik dayanakları arasında, kendi para birimlerini kontrol edebilmeleri, örneğin isyancı gruplar gibi devlet dışı aktörlere kendi politik ve ekonomik kaldıraçlarını artırmak için önemli bir araç sağlayabilmeleri yer almaktadır. Tarihsel olarak, isyancılar kendi politik ve ekonomik kontrollerini ileri sürmek için yeni para birimleri çıkarmışlardır. 13 Kasım 2014 tarihinde DAESH'in deklere ettiği kendi emtia tabanlı para biriminin bu kapsamda uyduğu söylenebilir. DAESH'in sanal para birimi yerine emtia tabanlı para birimleri seçiminin, sanal paraların siyasi olarak tartışmalı bölgelerdeki düşük fiziksel altyapı ve düşük penetrasyonlu haberleşme teknolojileri nedeniyle olmuş olabileceği belirtilmektedir. DAESH altın ve gümüş tabanlı para birimlerini kullanma eğilimlerinin uluslararası emtia borsalarında değer gören ekonomik güvenilirliği olan para birimlerini kullanmak istemesinden kaynaklanmaktadır. Bugüne kadar sanal paralar fiat para birimlerine rakip olarak çok büyük ölçekte başarılı bir şekilde kullanılmamışlardır. Sanal paraların büyük teknolojik altyapı gereksinimleri göz önüne alındığında sanal paralar sivil çatışmalarda yer alan isyancılar için tercih edilen bir araç olmamıştır. İskoçya gibi gelişmiş ülkelerdeki bazı ayrılıkçı hareket destekçileri halk desteği olmadan Scotcoin'i çıkarmıştır. Auroracoin İzlanda'da hükümetin katı sermaye kontrolleri rejimine itiraz etmek için başlatılmıştır. Bu nedenle sanal paralar, isyancılar veya ayrılıkçılar için bir araç değil, hükümetin

²⁵⁹ Aaron Brantly, "Financing Terror Bit By Bit", Volume 7, Issue 10, October 2014, <https://ctc.usma.edu/financing-terror-bit-by-bit/>, (Erişim: 10.12.2020).

makroekonomik politikalarına karşı politik bir protesto olarak değerlendirilmektedir. Geliştiriciler, “bir millet fiat para biriminin zincirlerini kırıyor” sloganını benimsemişlerdir. Sanal para olarak Auroracoin İzlanda’nın sermaye denetimleri rejimine rağmen, İzlanda nüfusunun yerel para birimi olan Krona’dan Auroracoin’e geçmekte isteksiz kalması nedeniyle kullanıcıların ilgisini çekemediği ve başarısızlıkla sonuçlandığı ifade edilmektedir. Bu örnekler, hem devlet dışı aktörlerin sanal para kullanımının teknolojik fizibilitesini hem de devlet dışı aktörlerin geleneksel para birimlerinin ulaşılabilirdiği bir ortamda yeni sanal para birimlerine katılımı teşvik etmek için karşılaşılan zorlukları göstermektedir.²⁶⁰

Kripto paralar kara para aklama ve terörün finansmanı dışında da birçok alanda yasa dışı faaliyetleri yürütmek için kullanılabilmektedir. Örneğin kripto paralar kayıt dışı alanı oluşturan önemli bir unsur olan vergi kaçırma faaliyetlerinde de kullanılabilmektedir. Yasal yollarla elde edilen kazançların vergi cenneti denilen yöntemde kullanıldığı gibi vergi dışına çıkarılması mümkündür. Kripto paralar anonim olarak, internet ortamında herhangi bir denetim mekanizmasına ihtiyaç duymadan işlem gördüğü için herhangi bir vergilendirmeye de tabi değildir. Kripto paraların hukuksal boşluğundan yararlanmak isteyen kötü niyetli kripto para kullanıcısı vergi ödeyerek yapması gereken ticari işlemini kripto paralar üzerinden gerçekleştirerek herhangi bir vergi ödemesi gerekmez. Birçok sanal cüzdan sahipleri kripto paraları genellikle yatırım hesabı olarak; kripto para göndermek için değil sadece kripto para alımı için kullanmaktadır. Bu tür yolla elde edilen kazançlar gönüllü olarak beyan edilmedikçe vergi otoritelerinin bu bilgilere ulaşması zordur. Araştırmalar birçok kripto para kullanıcısının ayırma ve birleştirme yöntemi kullandığını ifade etmektedir. Çok büyük miktardaki kripto paraların aynı kişiye ait çok sayıda sanal cüzdanlar üzerinden küçük miktarlar şeklinde bölünerek aktarılmaktadır. Bu yöntem fon kaynağını ve hedefi saklamak amacıyla vergi kaçakçılığı ve kara para aklama yöntemlerinde yaygın bir şekilde kullanılmaktadır.²⁶¹ Anonimlik vergi kaçakçılığı noktasında çok önemli bir konu olarak gündeme gelmektedir. Vergilendirilebilir kripto para işlemlerinde vergi ödmeden gerçekleştirilen işlemler vergi kaçakçılığına

²⁶⁰ Baron, ve diğerleri, “National Security Implications of Virtual Currency Examining the Potential for Non-state Actor Deployment”, s.23-24.

²⁶¹ Omri Marian, “Are Cryptocurrencies Super Tax Havens?”. Law Review First Impressions, Vol. 112:38, Michigan 2013, s.44.

girmektedir. Ancak vergi otoriteleri kripto paraların doğası gereği sahip olduğu anonimlik özelliği nedeniyle kimin vergilendirilebilir işlemlere girdiğini tespit edememesi bu oluşan vergi kaçakçılığını belirleyememektedir.²⁶² Bu durum da kripto paraları vergi kaçakçıları için cazip bir hale getirmektedir. Bazı yorumcuların bu nedenle kripto paraları “geleceğin vergi cenneti” olarak tanımladığı ifade edilmektedir.²⁶³ Kripto para, yüksek miktarda kaynağı belli olmayan fiziki veya nakit para taşıma problemini, geleneksel bankacılıktaki takip süreçlerini atlatarak bir yerden başka bir yere kolaylıkla transfer etmeye imkân sağladığı için de kara para aklama işlemlerinde rahatlıkla kullanılabilir. Kripto paraların dolandırıcılık işlemlerinde de kullanılması söz konusu olabilmektedir. Örneğin; ödemesinin Bitcoin vb. diğer kripto paralar ile gerçekleştirildiği internet üzerinden alınan bir malın veya hizmetin teslim edilmemesi gibi durumlarda paranın geriye alınamaması gibi bir durum ortaya çıkabilir. Bunların yanı sıra birçok kripto para kullanıcısı, ülkeleri etkileyen küresel siber saldırılar gibi olaylarda veya bilgisayarlarına bulaşan zararlı yazılımlar nedeniyle kişisel olarak kripto para cüzdanlarını kaybetme riski taşıdıklarını iddia etmektedirler.²⁶⁴ Kripto para sisteminin doğasında işlem iptali olmadığı için yanlış işlemlerle transfer edilen kripto paraların veya siber saldırılar sonucu hackerler tarafından ele geçirilen sanal cüzdanları geri almak için herhangi bir mekanizma bulunmamaktadır. 2014’ten bu yana Europol’ün İnternet Organizeli Suç Tehdit Değerlendirmesi raporları (Internet Organised Crime Threat Assessment – IOCTA) kripto paraların siber suçların bir etkeni olarak nasıl davrandığını göstermektedir. Europol’ün 2017 raporuna göre kripto paralar fidye yazılımı ve DDoS saldırıları gibi siber ilişkili gasplarda bir ödeme şekli olarak tercih edilmektedir. Kurbanların dosyalarına veya verilerine ulaşmaları karşılığında ödeme talep eden ransom ware saldırıları iddialı ve kararlı bir şekilde artarak büyümektedir. Kripto paranın ayrıca siber hırsızlık oranlarını da artırdığı ifade edilmektedir. Blok zincirini analiz eden bir firma olan Chainalysis tarafından gerçekleştirilen bir araştırmada 2017 yılında Bitcoin borsalarını hedef alan hırsızlığın 75 milyon ABD Doları tutarında olduğu belirtilmektedir. Bir diğer kazancı yüksek olan siber suç türü ise kripto para elde etmek

²⁶² International Monetary Fund “*Virtual Currencies And Beyond: Initial Consideration*”, s.43.

²⁶³ Tera Manjee, “Bitcoin, its Legal Classification and its Regulatory Framework”, *Journal of Business & Securities Law*, Vol.15, Issue, 2015, s.188.

²⁶⁴ European Central Bank, *Virtual Currency Schemes*, 2012, s.25.

için kurbanın haberi olmadan tarayıcısına bir yazılım yükleyerek “kripto kiralama” gerçekleştirmek. Check Point’in 2017 Global Tehdit Endeksi’ne göre dünya çapındaki işletmelerin %55’inin en çok aranan üç suç olan “kripto kiralama”, malware, citing ‘Coinhive’, ‘Rig ek’ ve ‘Cryptoloot’tan etkilendikleri belirtilmektedir. İngiltere’nin Ulusal Siber Güvenlik Merkezi ve Ulusal Suç Ajansı 2018 – 2019 yılında kripto jacking olayının büyük bir tehdit olabileceğini ifade etmiştir. Kripto paralar doğası gereği sahip olduğu özellikler nedeniyle ayrıca Dark web veya ToR protokolü gibi kullanıcıların kimliklerini ve iletişimini gizlemek amacıyla şifrelenmiş hizmetlere dayanan web ortamlarında tercih edilmektedir. Dark web pazarları silah, uyuşturucu, sahte para, sahte pasaport, çalıntı kredi kartı bilgileri gibi yasa dışı materyallerin alım ve satımının yanı sıra suçun hizmet olarak sağlanması ile eş anlamlı olarak tanımlanmaktadır. Bu pazarlar Amazon ve eBay gibi faaliyet gösteren kullanıcılarının yasa dışı ürün ve hizmetlerini daha düşük fiyatlarla gözden geçirebilmelerine olanak sağlamaktadır. Ayrıca kripto paraların organize suç grupları tarafından kara para aklama işlemlerinde daha fazla kullanıldığına dair kanıtların bulunduğu ifade edilmektedir. Europol’ün ilk direktörlerinden Rob Wainwright kripto paraların Avrupa’da elde ettiği yıllık gelirlerin 3 – 4 milyar Avro kadarını yasa dışı gelirlerin oluşturduğunu ifade etmektedir. Basında yer alan haberlerde ise Kolombiya’daki uyuşturucu kaçakçılığı yapan organize suç grupları Avrupa’dan Kolombiya’ya yapılan narkotik satışların gelirlerini aklamak için Avrupa’daki Bitcoin ATM’lerinin yasal düzenlemeye tabi olmayan statüsünü kullandıkları belirtilmektedir. Kolluk kuvvetleri Avrupa genelinde kripto paraların kullanılarak yapılan kara para aklama işlemlerinin arttığını da ayrıca belirtmektedirler.²⁶⁵ Ekim 2017’de ülkemizde meydana gelen olayda ise Bitcoin kullanarak uyuşturucu temin eden beş üniversite öğrencisinden ikisi tespit edilmelerinin ardından tutuklanmıştır.²⁶⁶ Kripto para, uyuşturucunun yanı sıra silah alımı, rüşvet, şantaj, porno içerikler, kiralık katil, çocuk kaçırma ve insan kaçakçılığı gibi çok sayıda yasa dışı hizmet ve ürün için ödeme aracı olarak da kullanılabilir.

²⁶⁵ European Parliament, “Virtual Currencies and Terrorist Financing: assessing the risks and evaluating responses”, s.17.

²⁶⁶ Sanal Para Bitcoin’le Uyuşturucu Siparişi Verdiler, 12.11.2017, <http://www.haberturk.com/bitcoinle-uyusturucu-siparisi-verdiler-1710096>, (Erişim: 17.12.2017).

Kötü niyetli kripto para kullanıcısı kara para aklamak için birden fazla hesap açabilir. Bu hesaplardan elde ettiği kripto paraları yasa dışı hem mal veya hizmet alımlarında kullanabilir hem de reel para birimlerine dönüştürüp herhangi bir yasal takibe takılmamak için de bu iş için geliştirilmiş özel yazılımlar kullanarak bankalara yönlendirip, nakit olarak elde edebilir. Bitcoin kripto parasının suç faaliyetlerinde kullanımının en bilinen örneği “Silk Road” internet sitesidir. Silk Road uyuşturucu ticaretinin yapıldığı en büyük sanal market olarak ifade edilmektedir. Silk Road ayrıca Bitcoin – Dolar çevrimiçi uyuşturucu pazarı olarak da bilinmektedir. Bu internet sitesinin yasa dışı işlem aktiviteleri için özel olarak tasarlandığı bilinmektedir. 2011 yılında yasa dışı ticaretin büyük bir çoğunluğu (uyuşturucu, zararlı yazılım, çocuk pornografisi, silah satışı) Silk Road üzerinden Bitcoin kullanılarak gerçekleştirilmiştir. Çünkü Bitcoin’in kolay olan ve üçüncü kişilerin bilmek zorunda olmadığı işlem aktiviteleri için cazip bir yol oluşturmaktadır. Bu internet sitesi üzerinden yapılan tüm işlemler Bitcoin aracılığıyla gerçekleştirilmiştir ve kullanıcılara anonimlik ise ToR yazılımı kullanarak Darknet ile sağlanmıştır. “Silk Road” herhangi bir kullanıcının internet sitesi aracılığıyla işlem yapmak için bir hesaba sahip olduğu özel Bitcoin bankası olarak fonksiyon göstermekteydi. Satın alma işlemi için bir kullanıcı madencilikle elde edilmiş Bitcoin’i Silk Road internet sitesinin Bitcoin adresine göndermekteydi. Bu satın alma işleminin gerçekleşmesinden sonra kullanıcının para birimi işlem tamamlanana kadar sistemin emanet hesabına transfer edilir ve sonrasında kullanıcının veya müşterinin Bitcoin’i emanet hesaptan Silk Road satıcısının hesabına gönderilmekteydi. Aralık 2014 tarihinde Amerika Birleşik Devletleri’nde Charlie Shrem isimli şahıs Silk Road internet sitesi üzerinden uyuşturucu ticareti yapan kişilere 1 milyon Doların üzerinde Bitcoin transferini kolaylaştırdığının tespit edilmesiyle iki yıl hapis cezasına ve kara paranın aklanması ve yasa dışı uyuşturucu operasyonlarını desteklemesi suçlarından dolayı 950 bin Dolar para cezasına çarptırılmıştır.²⁶⁷ Ross William Ulbricht Silk Road’un kurucusu ve yasa dışı faaliyetler nedeniyle tutuklanmıştır ve Silk Road 2013 Ekim ayında FBI tarafından kapatılmıştır. FBI önce değeri 3,5 milyon Dolar olan 26.000 Bitcoine, ardından değeri 28.5 milyon Dolar olan 144 bin Bitcoin’e el koymuştur. Bu dönemde toplam 87 milyon Dolarlık

²⁶⁷ Christopher Burks, “Bitcoin: Breaking Bad Or Breaking Barriers?”, *North Carolina Journal Of Law & Technology* Volume 18, 2017 s.252.

Bitcoin'e el konulmuştur. Mayıs 2015'te Ulbricht yasa dışı para aklama faaliyetinden dolayı hapse mahkûm edilmiştir.²⁶⁸

Devlet dışı aktörlerin özellikle siber suçluların mevcut sanal paraları kullandığının kanıt niteliği taşıyabilecek örnekleri mevcuttur. Bu aktörler sanal paralar ile düzenli olarak standart ekonomik ticaretini gerçekleştirmezler, daha ziyade sanal paraları güvenlik ve anonimlik gerektiren özel hizmetleri için kullanırlar. Yani örgütlü grupların sanal para birimlerini geliştirip uyguladıklarına dair bir kanıt yoktur fakat yasa dışı işlemleri için Bitcoin gibi kripto paraları kullandıklarının kanıtları mevcuttur. Kripto paraların özellikle Bitcoin'in suç amaçlı kullanılmasının en yaygın olanı siber suçluların kurbanın verilerini şifrelediği ve şifre çözümünün ancak Bitcoin karşılığında yapılabileceğini söyledikleri ransom ware (fidye yazılımı) vakalarıdır. Florida kanunları İnternet ve teknolojinin kullanılarak işlendiği çok çeşitli beyaz yaka suçlarını düzenlemektedir. Florida'da bir mahkeme Bitcoin transferi ile kara para aklama suçundan yargılanan bir kişinin ceza almamasına hükmetti. Finansal işlemin para ile gerçekleşebileceği ve Bitcoin'in de sanal olması sebebiyle suçlamaların reddedilmesi gerektiğini savundu. Bitcoin'lerin internet dünyası dışında herhangi bir parasal karşılığının olmadığı, Hazine Bakanlığı tarafından dağıtık dijital para olarak kabul edilmesi sebebiyle Bitcoin'lerin para olmadığı, bu nedenle kara para aklama olayının gerçekleşmesinin de zahiri olduğu gösterilerek suçlamalar reddedilmiştir. Fakat ileride kanunlarda Bitcoin ile ilgili bir düzenlemeye gidildiği takdirde kara para aklama kanunu kapsamında değerlendirilebileceği ifade edilmiştir.²⁶⁹

5 Mart 2018 tarihinde Rusya'da resmi adı Federal Nükleer Merkezi olan Sarov Tesisi'nde görev yapan mühendisler, kripto madenciliği yapmak için tesisin yüksek hızdaki süper güçlü bilgisayarlarını kullanmak istemişlerdir fakat gizlilik nedeniyle internet bağlı olmayan bu bilgisayarları çevrimiçi hale getirmeye çalışınca güvenlik güçlerinin dikkatini çekmişlerdir ve yakalanmışlardır. Bu mühendisler hem kişisel

²⁶⁸ Pradipta Kumar Sahoo, "Bitcoin as digital money: Its growth and future sustainability", Vol. XXIV, No. 4(613), India 2017, s.61.

²⁶⁹ <https://www.lexology.com/library/detail.aspx?g=9fdabfd9-506e-458b-a94d-c501578c07a3>, (Erişim Tarihi: 19.05.2018).

kazanç elde etmek için görevi kötüye kullanmışlardır hem de yüksek gizlilik içeren ulusal verilerin güvenliğini riske atmışlardır.²⁷⁰

2.3. İNTERNET VE KARANLIK İNTERNET

2.3.1. İnternetin Kısa Tarihi

İnternet, serbest bir iletişim ağı olarak tanımlanan ve birbirinden bağımsız bilgisayarların birbirleriyle iletişim kurmaları için birbirine bağlandıkları ve bu iletişimi yöneten protokollerden oluşan bir sistemdir.²⁷¹ İnternetin temelini aslında ABD'nin nükleer faaliyet gösteren ve çeşitli bölgelerde yer alan birliklerinin iletişimini sağlıklı bir şekilde sürdürmeleri için bir arayış sonucu ortaya çıktığı ve daha sonraları birçok açıdan devrim niteliği taşıyan bu fikrin bir düşünce kuruluşu olan RAND'da görev yapan Paul BARAN tarafından “dağıtık haberleşmeyi konu edindiği” bir projesiyle ortaya atıldığı belirtilmektedir.²⁷² RAND Amerika Birleşik Devletleri'nde İkinci Dünya Savaşı döneminde ordunun ihtiyaçları üzerine savaşların bilimsel çalışmalar sayesinde kazanılabileceği düşüncesinin gelişmesiyle kurulan bir düşünce kuruluşudur. İnovasyon yuvası olarak tabir edilen RAND bünyesinde çalışan bilim adamları ile bugüne kadar sayısı binleri aşmış araştırma ve geliştirme faaliyeti yürütmektedir. RAND, Douglas Hava Şirketinde Hava Kuvvetleri adına uzun vadeli araştırma geliştirme faaliyetleri yürütmek üzere sınırsız yetkiye sahip bağımsız bir birim olarak kurulmuştur.²⁷³

Lawrance Landweber'in Ulusal Bilim Vakfı'na (National Science Foundation – NSF) bilimsel bilgisayar ağının kurulması önerisinin ardından bu önerinin İleri Araştırma Projeleri Ajansı (ARPA) tarafından da desteklenmesi ile 1982 yılında internetin askeri kullanımından sivil kullanıma geçiş sürecinin başladığı belirtilmektedir.²⁷⁴

²⁷⁰ “Nükleer Tesiste Kripto Para Madenciliği yaparken Kısıvrak Yakalandılar”, (12.02.2018), <http://fintechtime.com/tr/2018/02/nukleer-tesiste-madencilik-skandali/> (Erişim: 06.05.2018).

²⁷¹ Johnny Ryan, *İnternetin Geçmişi ve Dijital Gelecek*, (Çev. Birsek Keleş), Ankara 2019, s.26.

²⁷² *Age*, s.4-5-6.

²⁷³ *Age*, s.13-14.

²⁷⁴ *Age*, s.100-101.

İnteraktif programlama grafik ve ağ kurma alanlarında çalışmış olan ve 1965 yılı sonlarında Bilgi İşlem Teknikleri Ofisi başına geçen Bob Taylor aynı zamanda ARPA'nın ağ geliştirme projesini başlatmasını sağlayan (ileride geliştirilecek olan ARPANET'in) ilk kişi olarak tarihe geçmiştir.²⁷⁵

İsviçre ve Fransa sınırındaki bölgede 1954 yılında kurulan Avrupa Nükleer Araştırma Merkezi (European Organization for Nuclear Research – CERN) dünyanın en büyük parçacık fiziği laboratuvarı olarak faaliyet göstermektedir. Dünyanın farklı yerlerinden gelen araştırmacılara destek veren CERN'in, 1980'li yıllarda her bir araştırmacının sahip olduğu birbirinden farklı bilgisayarlar ve bu bilgisayarların birbirleriyle olan uyumsuzluğu nedeniyle karmaşık bir hal aldığı belirtilmektedir. Girişimci olan Tim Barners-Lee'nin farklı programlar, farklı insanlar ve farklı sistemlerin oluşturduğu bu ağ ilişkilerini haritalandırmak üzere 1980'li yıllarda geliştirdiği Enquire isimli yazılımın daha sonraları kendisinin icat edeceği World Wide Web (www) yönünde atılan ilk adım olduğu ifade edilmektedir.²⁷⁶ Barners-Lee, 1990 yılında CERN'deki daha önce geliştirmiş olduğu SGML dilini temel alarak geliştirdiği ve HTML olarak adlandırdığı hiper metin işaretleme dili ile bir devrim niteliği taşıyan iletişim tarihinin en önemli ve en değerli buluşu olan fakat o dönemde değeri anlaşılmayan www'yi icat etti.²⁷⁷

Ulusal Bilim Vakfı'nın, 1993 yılında internetin özelleştirilmesi ile ilgili adım attığı ve bunun sonucunda 1969 yılında ARPANET in Amerikan hükümeti himayesinde başlayan internetin askeri yolculuğunu 30 Nisan 1995 tarihinde tamamladığı ve ticari yasağının kalktığı belirtilmektedir. Soğuk savaş döneminde yaşanan sıcak teknolojik savaş olarak nitelendirilebilecek gelişmelerin devrim niteliğindeki karşılığı olan internetin artık devlet tarafından finansmanının sona erdiği ve devlet savunması için gerçekleştirilen araştırma ve geliştirme faaliyetlerinin e-ekonomi olarak tabir edilen ekonominin temellerini attığı ifade edilmektedir.²⁷⁸

²⁷⁵ Age, s.18-19-20.

²⁷⁶ Age, s.117.

²⁷⁷ Age, s.120.

²⁷⁸ Age, s.138.

2.3.2. Darknetin Kısa Tarihi

Kaliforniya Üniversitesinde öğrenci olan Charley Kline, 9 Ekim 1969 tarihinde Pentagon İleri Savunma Araştırmaları Projeleri Ajansı tarafından geliştirilen ve internetin öncüsü olarak tabir edilen ARPANET tarafından birbirleriyle iletişimde olan bilgisayarlara ilk mesajı gönderen kişi olarak ifade edilmektedir. Sadece iki harfinin gönderildiği “LOGIN” kelimesinin Stanford Üniversitesi’ndeki bilgisayarlara kadar uzandığı belirtilmektedir. Bu olayı takip eden çok kısa bir süre içerisinde de ARPANET ile birlikte çok sayıda gizli ağın ortaya çıktığı ifade edilmektedir. Bunlardan bazılarının ise daha sonraları “karanlık ağlar” olarak bilinir hale geldiği de vurgulanmaktadır.

İnternet iletişim kuralı paketinin 1982 yılında standardizasyonu ile belirgin hale gelen modern web ’in ortaya çıkmasıyla birlikte hassas veya yasa dışı verilerin depolanması probleminin büyük önem taşıdığı belirtilmektedir. Bu problemlere erken çözümlerin ise Karayipler’de vergi cennetlerinin bilgisel analogu olarak tabir edilen “veri cennetleri” olarak kumar operasyonlarından, yasa dışı pornografiye kadar her şeyi barındıracağı sözünü içerdiği ifade edilmektedir. 90’lı yılların sonlarında internetin yaygın hale gelmeye başlaması ve akabinde dosya sıkıştırma meydana gelen olumlu gelişmelerle birlikte düşen depo maliyetleri, kullanıcıların telif hakkı materyallerin paylaşımını yapmaya başlamasıyla “darknet” faaliyetlerinde patlamaya neden olduğu belirtilmektedir. Kısa süre içerisinde internetin eşler arası veri aktarımının dağıtık veri aktarma merkezlerini doğurmasına neden olduğu da ifade edilmektedir. Bu verilerin çoğunlukla şifrelerle korunan ve yalnızca içerideki kişiler tarafından bilinen bir sistemde yasa dışı müzik ve film dosyalarından oluştuğu ve her gün milyonlarca dosya aktarımının gerçekleştirildiği belirtilmektedir.

Yazılımcı olan Ian Clarke’ın 2000 yılında çocuk pornografisinden patlayıcıların nasıl yapılacağına dair bilgilere kadar her türlü şeye ulaşılabilen internetin en karanlık alanlarına gizli geçişler sağlayan devrim niteliğinde olan Freenet yazılımını yayınladığı ifade edilmektedir. Ian Clarke’ın New York Times’a verdiği bir röportajda Freenet’in “mükemmel yakın bir anarşi” olarak tanımladığı ve ücretsiz dosya paylaşımını durdurmaya çalışan şirketlere de bundan vazgeçmeleri gerektiğini söylediği belirtilmektedir. Özgürlükçü bilgisayar korsanı olan Ryan Lackey ve Sean

Hasting Britanya kıyıları açıklarında İkinci Dünya Savaşı'ndan kalma tuhaf, sözde bağımsız bir devlet olan Sealand'da Haziran 2020'de işe koyuldukları ifade edilmektedir. HavenCo olarak adlandırdıkları girişim ile kalenin ayaklarına gizlenmiş yüksek teknoloji nitrojen kaplanmış sunucularında istenmeyen e-posta, çocuk pornografisi ve kara para aklama faaliyetleri dışında sınırlı verileri barındıracaklarını öngördükleri ifade edilmektedir. Girişimin ciddi ilgi uyandırmasına rağmen, HavenCo şirketinin çok kısa bir süre içerisinde para kaybettiği belirtilmektedir. 20 Eylül 2002 tarihinde ABD Deniz Araştırma Laboratuvarı'ndaki araştırmacıların, yazılımı indiren kişilerin IP adresini ve konumu gizleyebildikleri ToR'un olarak adlandırdıkları tarayıcının ilk versiyonunu yayınladığı ifade edilmektedir. ToR'un aslında Amerikan ajanların ve muhaliflerin Çin gibi baskıcı ülkelerdeki faaliyetlerinde kimliklerini gizleyebilmeleri için tasarlandığı belirtilmektedir. ToR'un darknet müdavimleri için doğal bir seçim aracı olabileceği de ifade edilmektedir. 2005 yılının ocak ayında Wired dergisinin darknet pazarının her gün yarım milyondan fazla filmin paylaşıldığını tahmin ettiği belirtilmektedir. Hollywood'un gişe rekorları kıran filmlerinden, Microsoft Office programlarına kadar telif hakkı ihlallerini içeren yeraltı ağının hızla artan bant genişliğiyle desteklendiği ifade edilmektedir. Bilişim teknolojileri şirketi olan IDC'nin bir çalışmasına göre sadece yazılım korsanlığının 2005 yılında dünya çapında işletmelere 34 milyar ABD Dolarına mal olduğunun tahmin edildiği belirtilmektedir. 3 Ocak 2009 tarihinde kendisini Satoshi Nakamoto olarak tanıtan bir kişinin izi sürülemeyen Bitcoin olarak adlandırdığı bir kripto para çıkardığı belirtilmektedir. Kullanıcılarının paralarını tam anlamıyla kopyalamalarının önüne geçebilecek bir sistem olmadığından başarısızlıkla sonuçlanan diğer dijital para birimlerinin aksine Bitcoin'in yenilikçi genel muhasebe defterini kullanmasının çifte harcamanın önüne geçmesini sağladığı ifade edilmektedir. Şaşırtıcı olmayan bir şekilde kripto paranın darknette kısa bir süre içinde hit olması onun doğası gereği sahip olduğu gizlilik özelliğinin kara para aklama ve suç faaliyetlerinde tercih edilen bir araç haline getirdiği belirtilmektedir. 2010 yılında siber güvenlik ve istihbarat şirketi olan Procysive, darknetin 50 binden fazla radikal internet sitesi ve 300'den fazla terörist forumlarına ev sahipliği yaptığını tahmin ettiği ifade edilmektedir. Korsan dijital içeriğin yasa dışı satışı terör operasyonların finans kaynağı olduğunun da raporda belirtildiği ifade edilmektedir. 1 Haziran 2011 tarihinde Gawker ile ilişkili bir blog

sayfasında Silk Road internet sitesinden yasa dışı uyuşturucu alım ve satımının yapılmasının herhangi bir elektronik bir cihaz almak kadar kolay olduğu ifade edilmektedir. Silk Road sitesinin Amazon internet sitesi gibi olduğu Amazon'dan farkının ise sadece Bitcoin hesabı olan ToR kullanıcıların ulaşabildiği de ifade edilmektedir. Değeri 10 Amerikan Doları olan Bitcoin'in günden güne artarak 30 ABD Doları'na çıktığı ve İpek Yolu internet sitesindeki trafiğin de hızla arttığı belirtilmektedir. 1 Ağustos 2013 tarihinde İrlandalı yetkililer FBI'ın gezegendeki en büyük çocuk pornosu kolaylaştırıcısı olarak tanımladığı Eric Eoin Marques'e Dublin'deki dairesinde baskın yaptıkları belirtilmektedir. Marques'in tutuklanmasının, darknetin uçsuz bucaksız alanlarının gizemli bir şekilde kapatılması ile iddiaya göre ToR kullanıcılarını belirlemek için Firefox web tarayıcısındaki bir ihlalden faydalanan FBI'ın da bir parçası olduğu operasyon ile aynı zamana denk gelmesi ifade edilmektedir. Kullanıcıların kimliklerinin Kuzey Virginia'daki sunuculara geri gönderildiğinin bildirildiği ifade edilmektedir. 4 Ağustos 2013 tarihinde Amerikan hükümetinin El – Kaide lideri Ayman al-Zawahiri ve Arap yarımadasındaki Yemen merkezli el Kaide'nin başı olan Nasir al-Wuhayshi arasındaki gizli iletişimine engel olduğu ifade edilmektedir. Bu çevrimiçi sohbet ABD'nin Müslüman olan 21 ülkedeki elçiliklerini kapatmasına neden olduğu da belirtilmektedir. İsrail Ulusal Güvenlik Çalışmaları Enstitüsündeki araştırmacılara göre üst düzey El – Kaide görüşmelerinin internetin bazen deepnet, blacknet veya darknet olarak adlandırılan bölümünde gerçekleştirildiği ifade edilmektedir. 4 Ekim 2013 tarihinde The Guardian gazetesinin NSA'nın defalarca, kendi bilgisayarlarında diğer yazılımların güvenlik açıklarından yararlanarak ToR kullanan kişileri hedef gösterdiğini bildirdiği ifade edilmektedir. Eski NSA analisti Edward Snowden tarafından 2007 yılında basına sızdırılan çok gizli bir sunuma göre ajansın hiçbir zaman ToR kullanıcılarının anonimliğini çözemeyeceği sadece manuel analiz ile ToR kullanıcılarının çok küçük bir oranının anonimliğini çözebileceği ifade edilmektedir. Ekim 2013 tarihinde teknoloji haberleri sitesi olan Verge'de açıkça uyuşturucu reklamı yapan Black Market Reloaded ve Deepbay gibi çevrimiçi pazarların trafiğinde bir artış olduğu ifade edilmektedir. İpek Yolu moderatörünün sitenin kapatılmasından sonra “şüphesiz hepimiz başka bir yerde toplanacağız hepinizi tekrar görmeyi dört gözle bekliyorum hala kişisel ilişkilerinize hükümetin dâhil olmadığı serbest ticaretle

uğraşıyorsunuz” şeklinde bir mesaj yayınladığı da belirtilmektedir. Kasım ayında orijinalinin kapatılmasından sadece bir ay sonra Silk Road 2.0 olarak adlandırılan yeni anonim darknet pazarının çevrimiçi olduğu da ifade edilmektedir.²⁷⁹ Silk Road internet sitesinin kapatılmasından sonra onun yerinde birçok benzer sitenin geldiği ve bugün de gelmeye devam ettiği ifade edilmektedir. Orijinal taklitçi pazarlarının çoğu Silk Road’dan kısa bir süre sonra ele geçirildiği fakat yeniden değiştirildiği ifade edilmektedir. Talep ve teknolojinin var olduğu sürece yeni karanlık pazarların devam edeceği ve yetkilerin kapatmayı başardıkları yerin yenisini kısa bir sürede tekrar alacağı vurgulanmaktadır.²⁸⁰

2.3.3. Derin İnternet (Deep Web), Karanlık Ağ (Dark Web) ve Darknet Kavramları

Modern karaborsalar ticareti kolaylaştırmak ve kanuni yaptırımlardan kaçınmak amacıyla çok sayıda kuruma ev sahipliği yapmaktadır. Nakit, işlemleri takip edilemez yapmakta, hiyerarşiyi ve rol ve sorumlulukları belirlemekte ve şiddet katılımcılarına normlara uymayı teşvik etmektedir. İnternetin ortaya çıkması ile bu sistem yıkılıyor ve bu ortamda karaborsa ticareti için yeni çözümler gerekliliği ortaya çıkmaktadır. Artan anonimlik sayesinde borsadaki hukuki yaptırım tarafından belirlenme riski de düşmektedir.²⁸¹ Derin internet ve Darknet (karanlık net) kavramları 1990’lı yılların ortalarında popüler hale gelen world wide web’ ten bu yana var olsa da Dread Pirate Robert adlı şahsın namı diğer Ross William Ulbricht’in 2013 yılında tutuklanmasına kadar kamuoyunun dikkatini çekmemiştir. Derin internet ve Darknet ayrıca bir muhabirin Başkan Yardımcısını kirletmek için bu yapı aracılığıyla bir bilgisayar korsanı kiralaması ile de ABD’de kilit bir rol oynayarak popüler kültürde kısa sürede demirbaş haline gelmiştir.²⁸² Derin İnternet, Karanlık İnternet ve Darknet terimleri medya tarafından her ne kadar birbirlerinin yerine kullanılsa da bu terimler internetin

²⁷⁹ Ty McCormick, “The Darknet: A Short History”, 09.11.2013 <https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/> (Erişim: 25.12.2020).

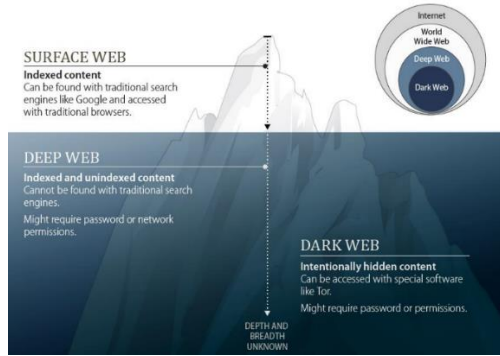
²⁸⁰ Kristin Austin, “The Origins And History Of The Dark Web”, 17.10.2019, <https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/> (Erişim: 26 Aralık 2020).

²⁸¹ Robert Augustus Hardy ve Julia R. Norgaard, “Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web, *Journal of Institutional Economics*, 2015, s1.

²⁸² Daniel Sui, James Caverlee ve Dakota Rudesill, “The Deep Web And The Darknet: A Look Inside the Internet’s Massive Black Box”, *Wilson Center*, Washington DC, 2015, s.5.

farklı fakat birbiri ile ilgili bölümlerini temsil etmektedir. Derin internet standart internet tarayıcıları ve bağlantı yöntemleri aracılığıyla erişilebilen fakat büyük arama motorları tarafından endekslenmemiş sayfa ve hizmetleri ifade eder. Derin internet genellikle internet siteleri veya servislerin arama listeleme işlemleri, iptal istekleri, ödeme duvarları, kayıt gereksinimleri veya diğer içerik erişim sınırlamaları gibi yanlış yapılandırılması nedeniyle arama motorları tarafından endekslenmez. Karanlık internet; internet hizmetleri ve kasıtlı olarak gizlenmiş sayfalarla ilgili olan derin internetin çok küçük bir kısmını ifade etmektedir. Bu hizmetlere ve sayfalara sadece standart tarayıcılar kullanılarak erişilemez. Bu hizmetler ve sayfalar, proxy yapılandırmaları veya doğrudan özel yazılım şeklinde belirli erişim hakkı gerektiren yer paylaşım ağının kullanılmasına güvenirlir. Darknetler, ToR veya I2P gibi erişimin ağ düzeyinde kısıtlandığı çerçeveler olarak ifade edilmektedir. Özel VPN'ler ve örgü ağların da bu kategoriye girdiği ifade edilmektedir. Bu çerçeveler üzerinden ağ trafiği; hangi sitelerin ziyaret edildiği veya sitelerin içeriği hakkında bilgi verilmesine gerek kalmadan sadece hangi Darknet ile bağlanıldığı ve ne kadar veri taşındığı ile ilgili bilgi verir ve bu şekilde maskeleye yapılmaktadır.²⁸³

Şekil 2.1: İnternetin katmanları²⁸⁴



Web'i bir veri okyanusu olarak düşünürsek, çoğu insan dalgalı, şeffaf, kolayca gezilebilir bir yüzey ağı ile etkileşime girmektedir. Yüzey ağ (Surface Web), web 'in Google ve Bing gibi standart arama motorları tarafından taranan ve endekslenen bir kısmını oluşturmaktadır. Aşağıdaki şekilde de gösterildiği gibi karanlık kısım ise

²⁸³ Benjamin Brown, "Threat Advisory: 2016 State of the Dark Web", 2016, s.2.

²⁸⁴ Congressional Research Service, "Dark Web", Mart 2017. <https://fas.org/sgp/crs/misc/R44101.pdf>, (Erişim: 10.11.2019).

elektronik termoklinin altındaki görünmeyen ağ veya gizli ağ olarak da ifade edilen ağın taranmamış ve dizine alınmamış ve böylece standart arama motorlarının ulaşmasına imkân olmayan kısmı olarak nitelendirilmektedir. Derin internetin boyutunu doğru olarak tahmin etmek teknik olarak imkânsızdır. Ancak en büyük arama motoru olarak kabul edilen Google’ın yüzey ağının yalnızca %4-16’sını endekslediği belirtilmektedir. Derin internetin yüzey ağından 400 – 500 kat daha büyük olduğu ifade edilmektedir. Ayrıca sadece en büyük 60 derin internet sitesinin depoladığı verinin tüm yüzey ağının depoladığı veri miktarından 40 kat daha büyük olduğu tahmin edilmektedir.

Şekil 2.2: Derin İnternet Temsili



Başlangıçta Darknet internet tarafından erişilemeyen herhangi veya tüm network ana sistemlerini belirtmekteydi. Fakat Darknet bu network ana sistemlerini kullanmaya başladığında genellikle gizli dosyaların dağıtılmış bir ağ üzerinden endekslenmemiş standart arama motorları tarafından, derin internetin önemli bir parçası haline gelmiştir. Yüzey interneti üzerindeki veya derin internetin birçok bölümündeki trafiğinin aksine Darknet sitelerine sadece anonim olarak erişilebilmektedir.²⁸⁵

Başlangıç çalışmaları derin internetin aslında en büyük genişleyen taze bilgi deposu içerdiğini ortaya koymaktadır. Bu internet siteleri genellikle dardır fakat standart yüzey siteleri ile karşılaştırıldığında çok fazla derin içerikli materyale sahip olduğu ifade edilmektedir. Bununla birlikte birçok materyal korunaklı içerik olduğundan dolayı derin internetten elde edilen içeriğin kalitesinin yüzey internetinin sahip olduğundan çok daha iyi ve değerli olduğu belirtilmektedir. Ayrıca derin internet

²⁸⁵ Sui ve diğerleri, “The Deep Web And The Darknet: A Look Inside the Internet’s Massive Black Box”, s.6.

içeriğinin %50'sinden fazlasının konuya özel dizinlerde (www.thehiddenwiki.net) yer aldığı ve bu durumun daha fazla erişilebilir ve hedeflenen aramalarla daha ilgili yapmakta olduğu ifade edilmektedir. Derin internet ve Darknet her geçen gün büyümektedir. Aynı zamanda her yerde bulunan bilgisayarlar, dağıtık/bulut tabanlı bilgisayarlar, mobil bilgisayarlar ve algılayıcı ağlar gibi çoklu teknolojilerin tümü derin internetin genişlemesine katkıda bulunmaktadır.

Güvenli ve aynı zamanda anonim olarak nitelendirilen internet host hizmetleri, kripto para/dark wallet ve yazılım kullanarak yasa dışı faaliyetlerde meydana gelen gelişmeler darknetin büyümesine de katkı sağlamaktadır. Bitcoin, Darkcoin veya Peercoin gibi çeşitli kripto paraların darknet pazarında anonim ticari işlemlerde kullanıldığı ifade edilmektedir. Kiralık olarak kullanılan bilgisayar korsanları ve çok dilli çağrı merkezleri de darknetin büyümesini hızlandırmaktadır. Bunun yanı sıra elbette gazeteciler, muhalif siyasiler, muhbirler ve insan hakları savunucuları tarafından darknetin birçok meşru kullanımının da bulunduğu ifade edilmektedir. Chelsea eski adıyla Bradley ve Edward Snowden'in faaliyetleri için darknete çok fazla güvendiği de ifade edilmektedir.²⁸⁶

Darknette hem gezinti yapanlar hem de internet sitesi sahipleri tamamen anonimdir ve bu anonimliklerini genellikle ToR kullanarak başardıkları ifade edilmektedir. Kara market olarak tabir edilen Abraxas, Agora Marketplace, Middle Erath Marketplace, Nucleus ve Silk Road 1, 2 ve 3 şeklinde birçok pazar yeri bulunmaktadır. Dark Web, kullanıcının kimliği gizlemek için anonim yönlendirme tekniklerinden yararlanmaktadır. Dark web ilk olarak basın özgürlüğünü desteklemek ve siyasi baskı olmadan açık tartışmaları taahhüt etmek amacıyla önerilmiş olsa da zararlı içerik reklamları ve komuta ve kontrol hizmetleri gibi kötü niyetli amaçlar için suistimal edilmiştir. Örneğin dark web'deki bir elektronik ticaret pazarı bilinen en büyük uyuşturucu ticareti sitelerinden olduğu bilinmektedir. En ünlü fidye yazılımı olan WannaCry yazılımı, dark web'deki komuta kontrol hizmetlerini yönetmek için kullanılmıştır. Kripto para da benzer bir durum sunmaktadır. merkezi bir sunucudan ayrı olarak kripto paralar herhangi bir merkezi otorite olmaksızın insanlara eşten eşe, ya da diğer bir tabirle uçtan uca iletişimi mümkün kılar ve bu nedenle ticareti

²⁸⁶ Age, s7.

gerçekleştiren tarafları belirlemek çok zordur. Dark web'deki duruma benzer şekilde kripto paralar da finansal ticaret mekanizmalarının yeniden dizayn edilmesi bakımından yeni iş modellerini güdüleyerek topluma fayda sağlarken diğer taraftan da kara para aklama gibi finansal suçlar tarafından da benimsenmektedir. Aslında son yıllarda yapılan birkaç çalışma Bitcoin'in Ponzi Şemaları ve fidye yazılımı ödemeleri için kullanıldığına işaret etmektedir.²⁸⁷

Dark web ve kripto parayı içeren yasa dışı yeraltı işlemlerinin reklam, keşif, müzakere, ödeme ve yerine getirme şeklinde beş aşamadan oluştuğu ifade edilmektedir. Dark web'te yasa dışı ürünlerin veya hizmetlerin reklamını yapmak yasal ürünlerin veya hizmetlerin yüzey ağ üzerinden tanıtımından daha farklı yaklaşımlar gerektirmektedir. Geleneksel arama motorları dark web üzerinde içerik indekslemesi yapmamaktadır. Eğer bir dark web sitesi satışları teşvik etmek için oluşturulursa ToR gibi gizli ağlar aracılığıyla bu bilgilerin dark web üzerinde sağlanan bir dizin servisine kayıt ettirilmesi gerekmektedir. Bu kayıt potansiyel ziyaretçilere yüzey webe erişim bilgileri gönderilerek duyurulur. Reklam için alternatif yaklaşım ise dark web sitelerinin genel amaçlı dark web arama motorlarına (Ahmia ve Haystack) veya pazar platformlarına (Silk Road ve Dream Market) reklam vermesi olarak belirtilmektedir. Alıcılar, topluluklar veya dark web arama motorları aracılığıyla yasa dışı teklifler satan satıcılara giriş noktaları keşfetmek gibi bir satıcının reklam stratejilerinin liderlerinden de benzer yaklaşımları takip ederler. Ayrıca alıcılar giriş bilgilerini diğer alıcılarla paylaşabilmektedir. Alıcı ödeme yöntemleri, fiyat, özelleştirme hizmetleri ve nakliye yöntemleri ile ilgili konularda satıcı ile işleme devam etmek için görüşme yapmak durumundadır. Bu detaylar ürün ve hizmete göre de değişiklik göstermektedir. Örneğin bilgisayar korsanlığı hizmet sağlayıcıları istenilen bilgisayar korsanlığı hizmetleri ve hedefler hakkında ek ayrıntılar gerekebilir. Dark web üzerinden ödemeler, alıcı ve satıcılar arasındaki işlemlere aracılık eden üçüncü bir tarafın varlığına bağlı olarak genelde iki şekilde yapılmaktadır. Üçüncü bir taraf ara bulucusu olmayan işlem yapan taraflar satıcıların ücretlerini toplamak için alıcılara sağladıkları kripto para adresleri ile doğrudan ücret almak ve göndermek için

²⁸⁷ Seunghyeon Lee, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, Yongdae Kim, Dongsu Han, Soel Son ve Seungwon Shin, "Cybercriminal Minds: An Investigative Study of Cryptocurrency Abuses in The Dark Web", *Network and Distributed Systems Security (NDSS) Symposium 2019*, San Diego 2019, s.1.

anlaşma yapmaktadırlar. Yerleşik hizmet sağlayıcıları daha yüksek bir üne sahip olma eğiliminde olduklarından dolayı işlem yapan tarafların kimliklerindeki belirsizliğin üstesinden gelmek için emanet sistemi de kullanılabilmektedir. Emanet hizmet sağlayıcıları, alıcılara otomatik ödeme sistemini destelemektedir ve hizmet ücretlerini satıcılara yüklemektedir. Satıcı elektronik ticaret hizmetlerinde olduğu gibi fiziki ürününü (uyuşturucu ve silah) önceden anlaştıkları dağıtım yöntemiyle, çevrimiçi hizmetler sağlayarak (bilgisayar korsanlığı ve yasa dışı içerik) veya gerçek dünya çevresinde suç aktivitelerini (suikast) yerine getirmektedir. Anonimlik ağı ve kripto para anonimlik isteyen kişilerin gizliliğinin korunmasına katkıda bulunmaktadır. Aynı zamanda suç işleyen kişiler de kimliğini gizleyerek bu durumu kötüye kullanmaktadır. Dark web anonimlik ağlarına dayanan yasa dışı içerik ve kara borsa yasa dışı ürünlerin ticaretine ev sahipliği yapan bir web ortamıdır. Kripto para yasa dışı parasal işlemlerde bulunan insanların kimliklerinin gizlenmesinde de rol oynamaktadır. Yarı anonim Bitcoin adresi ve Bitcoin'in merkezi olmayan yapısı yasa dışı finansal faaliyetlerin incelenmesini zorlaştırmaktadır. Kripto para ve dark web ile ilgili kolluk kuvvetlerinin ve araştırma topluluklarının yoğun dikkatine rağmen, dark web üzerinde yasa dışı kripto para işlemlerinin miktarını veya popülaritesini tahmin eden geniş kapsamlı ve derinlemesine bir ölçüm çalışması yapılmamıştır.²⁸⁸

²⁸⁸ Age, s.3.

ÜÇÜNCÜ BÖLÜM

KRİPTO PARA VE MİLLİ GÜVENLİK BOYUTU

3.1. MİLLİ GÜVENLİK KAVRAMI

Güvenlik insanlık tarihi kadar eski bir kavram olmakla birlikte uluslararası ilişkilerin esas konularından birini teşkil etmektedir. Bireyin var olması ile başlayıp dünyadaki varlığını devam ettirebilmesi için alması gerekli olan tedbirler olarak tanımlanan güvenlik kavramının diğer taraftan kişi, koşul ve zamana göre değişiklik ve esneklik gösterebilme özelliklerine de sahip olduğu ifade edilebilmektedir.

Güvenlik kavramı iç güvenlik ve dış güvenlik olmak üzere iki boyutta farklı açılardan ifade edilse de temelinde sahip olduğu özelliklerin aynı olduğunu söylemek mümkündür. İlk başta herhangi bir güvenlik önleminin alınmasına gerek olmayan bir durum veya koşulun farklı bir zaman içerisinde risk oluşturabilecek bir hale gelmesi ve en kısa sürede tedbir alınmasını gerektirecek durum oluşturması söz konusu olabilmektedir. Güvenlik kavramı riskin neden olduğu tehdit ve tehlike durumlarına karşı güvenliğin tahsis edilmesi için amaçlanan koşul ve durumların oluşturulması olarak ifade edilebilmektedir. Birbirleriyle iç içe kavramlar olarak belirtilen tehdit, risk ve tehlike kavramları güvenlik kavramını çevreleyen unsurlar olarak belirtilmektedir. Tehlike kavramı riskin gerçekleşme ihtimaline göre oluşmakta, tehdit ise tehlike kavramının idrak edilmesi ve öngörüsü ile ortaya çıkmaktadır. Tehlike her türlü risk sonucunda oluşabilmekte ve tehdit ise tehlikenin zayıf veya güçlü seviyede gerçekleşmesi durumunda oluşmaktadır ki bu da gerçek bir tehditin varlığının ve öngörüsünün yapılabilmesini zorlaştırabilmektedir. Tedbir alınmasını gerektiren güvenliğin konu olduğu olay ve durumlar karşısında sadece anlık durum değerlendirmesinin yapılması sarf edilen emeklerin heba olmaması bakımından önem arz etmektedir. Güvenlik kavramı bireyin sahip olduğu varlığı muhafaza etmesi ve devam ettirebilmesi bakımından hedeflenen amaca yönelik anlam taşımakta olup iç veya dış kaynaklı tehditlerin var olması durumunda meydana gelen değişim ile de şekil değiştirmekte ve yeni güvenlik bakış açılarının ortaya çıkmasına neden olduğu ifade edilebilmektedir.

Güvenlik kavramı uluslararası anlamda, devletlerin sahip oldukları coğrafi açı dâhil ülke bütünlüğü ve toplumun her bir ferдинin huzurunu ilgilendiren konularda risk oluşturan ve tehdit olarak nitelendirilen durumlara karşı bir aksiyon almak üzere alınması gereken tedbirler olarak tanımlanabilmektedir. Uluslararası anlamda değerlendirildiğinde dünya üzerindeki her bir ülke sahip oldukları farklı konum ve çıkarlara göre farklı güvenlik anlayışlarına sahip olabilmekte ve bunun sonucu olarak bazı durumlarda birlikte hareket etmekte veya kendilerinden çok daha iyi bir konumda olanın koruması altında yer alabilmektedir.²⁸⁹

Güvenlik kavramının genel bir tanımını yapmak ve güvenlik kavramını sınırlandırmak mümkün olmamakla birlikte çok çeşitli olarak bireyden başlayarak devlete kadar uzanan ve içinde bulunulan durum, zaman ve mekâna göre de değişiklik gösteren tanımları da içerdiğini söylemek mümkündür.²⁹⁰

Luciani, dışarıdan gelecek her türlü tehlikeler karşısında bireyin kendi kendini korumasını güvenlik olarak nitelendirmiştir.²⁹¹

Bellany güvenlik tanımını devletlerin normal zamanlarda sahip oldukları ülke sınırlarını olası tehlikelere karşı koruması ve yaşanması muhtemel tehlikeli durumlar karşısında süreci başarıyla yürütebilmesi olarak ifade etmektedir.²⁹²

İnsanoğlunun yaratılışından itibaren hep birlikte toplu olarak yaşamaya başladıktan sonra barınma, hayatını devam ettirme, emniyeti sağlama ihtiyaçlarının sağlanmasını güvenlik olarak tanımlamaktadır.²⁹³

Gün geçtikçe her an ve koşulda değişim gösterebilme özelliğine sahip tehdit ve tehlike kavramlarının güvenlik kavramını da etkileyerek zaman içerisinde değişmesine neden olduğunu söylemek mümkündür. Önceleri sadece bireyin hayatta kalması, barınması ve yiyecek temin etmesi gibi temel ihtiyaçlarını karşılaması gibi nedenlerle ortaya çıkan güvenlik kavramı zamanla günün koşullarına uyum sağlayarak değişmekte ve ortaya çıkan farklı gereksinimler için de bir anlam oluşturmaktadır.

²⁸⁹ Beril Dedeoğlu, Uluslararası Güvenlik ve Strateji, YeniYüzyıl Yayınları, İstanbul 2008.

²⁹⁰ David A. Baldwin, The Concept of Security. Review of International Studies (1997), 23. s. 5-26.

²⁹¹ Giacomo Luciani, (1989). The Economic Content Of Security. Journal of Public Policy. (S.8). 1989, s.149-158.

²⁹² Ian Bellany, Towards a Theory of International Security. Political Studies. (29/1), 1981, s. 99-108.

²⁹³ Sertif Demir, Avrupa Güvenlik Mimarisinin Tarihsel Gelişimi ve Türkiye'nin Bu Güvenlik Mimarisindeki Yeri, Güvenlik Stratejileri Dergisi. (S. 9), 2009), s. 9-50.

Örneğin Soğuk Savaş döneminde ülkelerin güçler ilkesi ile bir araya gelerek öteki bloktaki ülkelere karşı ortak bir savunma mekanizması geliştirmesi ve caydırıcılık politikası izlemesi güvenlik kavramının farklı bir anlam taşıması olarak yorumlanabilmektedir.²⁹⁴

İkinci Dünya Savaşı sonrasında güvenlik konularında askeri boyutta gerçekleştirdiği çalışma ve projelerle dikkat çeken ülkenin Amerika Birleşik Devletleri'nin olduğunu söylemek mümkündür. Soğuk Savaş döneminde daha çok askeri nitelik taşıyan ve yüksek politika olarak nitelendirilen güvenlik kavramının günümüzde bu kimliğinden sıyrılarak biraz daha siyasi bir kavram haline geldiği ifade edilmektedir. Adalet, demokrasi, serbest piyasa ekonomisi, ekonomik refah gibi çeşitli konuların güvenlik kavramı içinde mevcut olması ve sonrasında bilim ve teknolojik ilerlemelerin neticesinde siber uzayı ilgilendiren konuların da ortaya çıkması ve bu alanın yeni zafiyetler oluşturması güvenlik kavramının geniş bir alana yayıldığını göstermektedir.²⁹⁵

Devletlerin güvenlik kavramlarını yeniden gözden geçirmesi gerekliliğinin İkinci Dünya Savaşı sonrası ortaya çıktığı söylenebilir. Güvenlik kavramının uluslararası arenada yaşanan ve yaşanmakta olan değişim ve gelişmeler neticesinde etkilendiğini ve önceleri askeri bir unsur olarak değerlendirilen bu kavramın günün şartlarının gerektirdiği konulara evrilerek sosyal, çevresel, kültürel, siber, siyasi ve ekonomi gibi çok yönlü olarak ele alındığı ifade edilebilmektedir.²⁹⁶

Devletlerin siyasi, hukuki, askeri, sosyal ve ekonomi başta olmak üzere milli güç unsuru olarak nitelendirilebilen hemen hemen her alanda toprak bütünlüğü ve devamlılığı için kendi menfaatleri doğrultusunda hareket etme gayesinin, içeriden veya dışarıdan gelebilecek her türlü tehdite karşı kendisini korumaya alma ihtiyacının milli güvenlik kavramını doğurduğu ifade etmek mümkündür.

²⁹⁴ H. Tarık Oğuzlu, Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Açılıyor mu? Güvenlik Stratejileri Dergisi. (S.6), 2007 s. 7-42.

²⁹⁵ Cuma Özçoban, "21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü", Harp Akademileri Stratejik Araştırmalar Enstitüsü Yüksek Lisans Tezi, İstanbul 2014, s. 4-6-10-12.

²⁹⁶ Kadir Sancak, "Güvenlik Kavramı Etrafındaki Tartışmalar Ve Uluslararası Güvenliğin Dönüşümü, Sosyal Bilimler Dergisi, s.132.

Milli Güvenlik kavramı, resmi olarak 2945 sayılı Milli Güvenlik Kurulu ve Milli Güvenlik Kurulu Genel Sekreterliği Kanunu'nun 2. maddesinin a bendinde şu şekilde tanımlanmaktadır:

*“Devletin anayasal düzeninin, milli varlığının, bütünlüğünün, milletlerarası alanda siyasi, sosyal, kültürel ve ekonomik dahil bütün menfaatlerinin ve ahdi hukukunun her türlü dış ve iç tehditlere karşı korunması ve kollanmasını” ifade eder.*²⁹⁷

Bu tanımdan yola çıkarak milli güvenlik kavramının devletin meşru yapısının içeriden veya dışarıdan gelebilecek her türlü tehdiye karşı savunulması ve emniyetinin sağlanması şeklinde ifade edilmesi mümkündür. Milli güvenlik kavramı kısıtlı ve kapsamlı olmak üzere iki bakış açısı ile değerlendirildiğinde farklı anlamlar ihtiva etmektedir.

Milli sınır güvenliği, ulusal huzurun sağlanması ve olağan dışı durumlarda acil durum yönetimi ile güvenliğin tahsisi için gerekli tedbirlerin alınması kısıtlı bir anlam olarak değerlendirilirken, sosyal hayatı ilgilendiren hemen hemen her şeyin milli güvenlik hususu içerisinde ele alınması kapsamlı anlam olarak değerlendirilmektedir.²⁹⁸ Tüm uluslar için vazgeçilmez bir kavram olan milli güvenlik kavramının hukuki, siyasi, kültürel ve ekonomik yönleri sahip olduğu dikkat çekmektedir. İkinci Dünya Savaşı milli güvenlik kavramının şekillenmesinde büyük rol oynamıştır. İkinci Dünya Savaşı'na kadar daha çok siyasal ve psikolojik açıdan ele alınan milli güvenlik kavramının askeri anlamda ele alınamayacak konuların savaş sonrası teknolojik gelişmelerinde etkisi ile sosyal, kültürel, ekonomi gibi diğer boyutlarıyla çok yönlü olarak değerlendirilmesi gerçeğini ortaya koyduğu ifade etmek mümkündür.²⁹⁹

İç güvenlik ve dış güvenlik olmak üzere birbirleriyle yakından ilişkili iki farklı cephesi bulunan milli güvenlik kavramının temelde devletin varlığını tehdit eden unsurların ortadan kaldırılmasına yönelik gerçekleştirilen faaliyetleri kapsadığı söylenebilmektedir. Her ne kadar yabancı devletlerin tehdit ve saldırılarına karşı milli güç unsurları ile karşı koyma devletin bağımsızlığı açısından büyük önem teşkil etse de, devletin yapısına içeriden gerçekleştirilecek herhangi bir müdahalenin veya tehdit

²⁹⁷ <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2945.pdf>

²⁹⁸ Hasan Tunç ve Ayhan Döner, “MGK ve Milli Güvenlik Kavramı”, s.3.

²⁹⁹ Rona Aybar, “Milli Güvenlik Kavramı ve Milli Güvenlik Kurulu”, s.60.

unsurunun kültürel milli güç unsuru ile bertaraf edilmesinin de öneminin devletin bağımsızlığı açısından önem teşkil ettiğini söylemek mümkündür.³⁰⁰

3.1.1. Ulusal Güvenlik

Bir devletin ulusal çıkarlarının iç ve dış tehditlere karşı önlemler geliştirilmesi suretiyle korunması ulusal güvenlik olarak tanımlanmaktadır.³⁰¹

İlk zamanlarda sadece savaş dönemlerinde devletin emniyetinin sağlanması olarak bir anlam taşıyan ulusal güvenlik kavramının sonraları barış dönemlerinde de bir anlam kazanarak politika oluşturulması şeklinde nitelendirilmesi mümkün olmaktadır. Ulusal güvenlik kavramı, bir ülkenin çıkarları doğrultusunda içsel veya dışsal gerçekleşebilecek her türlü tehdite karşı devletin ve toplumunun düzenini koruması olarak tanımlanabilmektedir.³⁰²

Ulusal Güvenlik kavramının 18 Ekim 1947 tarihinde dönemin ABD Başkanı Henry S. Truman başkanlığında kongre tarafından yayınlanan Ulusal Güvenlik Yasası (National Security Act) ile yaygınlık kazandığı belirtilmektedir. Siyasi bir kavram olarak ortaya çıkan ulusal güvenlik kavramı ile birlikte devletlerin güvenlik politikalarını belirlemeye başladığı ifade edilmektedir. Ulusal çıkarlar ve tehditlerin ulusal güvenliğin temelini oluşturan iki önemli unsur olduğu belirtilmektedir.³⁰³

Ulusal çıkar kavramı, devletler arası ilişkilerin anlaşılması için kullanılan uluslararası ilişkiler alanında en geniş kapsamlı teori olarak kabul edilen “Gerçekçi (Realist) Yaklaşım”ın en köklü kavramlarından biri olarak ifade edilmektedir.³⁰⁴ Ulus devlet tanımlaması ile ortaya çıkan bir kavram olan ulusal çıkar, 18. yüzyıldan itibaren bu isimlendirme ile günümüzdeki anlamını karşılayacak şekilde dönüşüme uğrayarak kullanılmaya ve devletler tarafından kabul görmeye başladığı ifade edilmektedir.³⁰⁵

³⁰⁰ Hasan Tunç ve Ayhan Döner, “MGK ve Milli Güvenlik Kavramı”, s.5-6.

³⁰¹ Sait Yılmaz, 21. Yüzyılda Güvenlik ve İstihbarat, Milenyum Yayınları, İstanbul, 2007.

³⁰² Cuma Özçoban, “21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü”, Harp Akademileri Stratejik Araştırmalar Enstitüsü Yüksek Lisans Tezi, İstanbul 2014, s.24.

³⁰³ Fikret Birdişli, “Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri”, Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Sosyal Bilimler Enstitüsü Dergisi Sayı: 31 Yıl:2011/2, s.151.

³⁰⁴ Mitat Çelikpala “Geçmişten Günümüze Vazgeçilmeyen Kavram: Ulusal Çıkar”, H.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi, Cilt 23, Sayı 1, 2005, s.440.

³⁰⁵ Age, s.447.

Ulusal çıkar, devletlerin varlıklarını korumak ve devamlılığını sağlamak için uluslararası arenadaki stratejilerinin ve ilişkilerinin şekillendirilmesinde etkin bir kavram olarak nitelendirilmektedir.³⁰⁶

Tehdit kavramı ulusal güvenliğin bir diğer önemli unsuru olarak değerlendirilmektedir. Devletlerin varlığını tehlikeye sokacak, nüfusunun yaşam kalitesini düşürecek, hükümetin strateji olanaklarının çeşitliliğini azaltacak, tüzel kişilikleri, bireyleri ve toplulukları etkileyebilecek iç veya dış her türlü faaliyet tehdit olarak tanımlanabilmektedir.³⁰⁷

Ulusal güvenliğin, Marksizm, Liberalizm, Realizm ve İdealizm düşünce akımlarından yola çıkarak biçimlendiği değerlendirilmektedir.

İdealizmin ilk düşünürleri olarak kabul edilen ve politika kavramının ilk kullanım şeklinin görüldüğü Platon ve Aristo'ya göre düşmanlık ve tehdit kavramlarının gerçekte var olmadığı ve çevresel etkilerin insan davranışlarına tesir ettiği, tehditin de bu kapsamda insanların davranışları neticesinde ortaya çıktığı savunulmakta olup insan davranışlarının çevresel koşulların değiştirildiğinde değişebileceği şeklinde idealist bir görüş hâkimdir.³⁰⁸

Realizmin, idealizmin karşıt bir görüşü olarak devletlerin ulusal güvenlik politikalarının temelini oluşturduğu kabul edilmektedir. Merkezine devleti alan realist güvenlik yaklaşımının öncüsü kabul edilen Machiavelli'ye göre iyi kanunları ile otoriter bir yönetim ve güçlü ordusu ile sağlam bir savunma sisteminin, güvenliği sağlamanın en temel kaynağı olduğu görüşü benimsenmiştir.³⁰⁹

İnsan doğasına önem veren ve realizm ve idealizme göre daha yaygın bir konuma sahip olan liberalizmin güvenlik kavramına yaklaşımının politik ve ekonomik çıkarların korunması prensibine dayandığı belirtilmektedir.

³⁰⁶ Age, s.458

³⁰⁷ Nasih Sarp Ergüven, "Uluslararası Hukuk Açısından Güvenlik Kavramının Teorik Temelleri", Ankara Üniversitesi Hukuk Fakültesi Doktora Tezi, 2016, s.776.

³⁰⁸ Fikret Birdişi, "Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri", Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Sosyal Bilimler Enstitüsü Dergisi Sayı: 31 Yıl:2011/2, s.154.

³⁰⁹ Age, s.155.

Güvenlik politikalarına eleştirel düzeyde yaklaşım sergileyen Marksizm’de ise güvenlik politikasının devletin varlığını devam ettirebilmesi için kullandığı bir araç olarak nitelendirildiği ifade edilmektedir.³¹⁰

3.1.2. Askeri Güvenlik

Askeri güvenlik, bir devlete yabancı devletler tarafından gelebilecek tehdit ve tehlikelere karşı askeri tedbirlerin kullanılması olarak tanımlanabilmektedir. Güvenlik kavramı her ne kadar çok eski bir kavram olsa da bu alanda gerçekleştirilen akademik çalışmaların son zamanlarda başladığı ifade edilmektedir. İkinci Dünya Savaşı’ndan sonra, güvenlik kapsamının çok kısıtlı tutularak daha çok askeri alana ağırlık verilmesi suretiyle güvenliği ilgilendiren konularda yapılan faaliyetlerin ilk olarak ABD’de gerçekleştiğini ve realist yaklaşımla ele alındığını ifade etmek mümkündür.³¹¹ Realist yaklaşımın güvenlik olgusunu daha çok askeri boyutu ile ele aldığı ve devletlerin uluslararası politikalarının temel konusunu güvenlik kavramının oluşturduğu, ulusal güvenlik kavramının esas olarak askeri ve siyasi meselelerden meydana geldiği ifade edilmektedir. İkinci Dünya Savaşı sonrası askeri alandaki güvenlik konuları “yüksek politika” olarak sağlık, ekonomi, çevre ve diğer konular ise “alçak politika” konuları olarak tanımlanmaktadır.³¹²

Ulusal çıkarların devletlerin uluslararası politikalarında etken unsur olduğu görüşünün hâkim olduğu klasik realist yaklaşımda bu çıkarların korunması için de savaşların meşru olabileceği savunulmaktadır. Klasik realist yaklaşımda insan doğasının özünde var olan bencillik ve kendi çıkarını düşünme özelliklerinin savaşların olmasına neden olarak gösterildiği, neorealist yaklaşımda ise anarşik yapıda olduğu düşünülen uluslararası sistemin savaşların nedeni olduğu düşüncesinin hâkim olduğu belirtilmektedir. Devletlerin varlıklarını koruyabilmeleri için güvenliklerini sağlamalarının zorunlu olduğu ve bu güvenliğin askeri güç ile sağlanarak silahlanma yoluna gidilmesi gerekliliğinin ortaya çıktığı ifade edilmektedir.³¹³

³¹⁰ Age, s.163.

³¹¹ Sait Yılmaz, 21. Yüzyılda Güvenlik ve İstihbarat, Milenyum Yayınları, İstanbul, 2007. S.70.

³¹² H. Tarık Oğuzlu, Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Açılıyor mu? Güvenlik Stratejileri Dergisi. (S.6), 2007 s. 13-14.

³¹³ Kadir Sancak, “Güvenlik Kavramı Etrafındaki Tartışmalar Ve Uluslararası Güvenliğin Dönüşümü, Sosyal Bilimler Dergisi, s.126.

Ulusal güvenlik politikası ile dış politika neredeyse birbirinden ayıramayacak şekilde örtüşmektedir ancak ulusal güvenliğin, dış politikadan sadece iki konuda ayrıldığını ifade etmek de mümkündür. Birincisi, ulusal güvenliğin amaçları daha dar bir şekilde güvenlik, emniyet ve millet kavramları üzerine yoğunlaşmaktadır. İkincisi, ulusal güvenliğin öncelikle gerçek ve potansiyel düşmanlarla ve onların sahip olduğu güç ile ilgilenmesi olarak belirtilmektedir. Dış politika ulusal güvenliğin bir ayağını oluşturmaktadır diğer ayağını ise milli savunma oluşturmaktadır.

Dış politika, bir ülkenin diğer ülkeler ve uluslararası konular bakımından başarmayı hedeflediği amaç veya bir dizi amaçlar olarak tanımlanabilmektedir. Devletler uluslararası politikada tek aktör değildir. Bir ülkenin dış politikası, diğer uluslararası aktörlerle etkileşimleri içermek amacıyla, uluslararası kurumlar, çokuluslu şirketler, müttefikler, bölgesel kuruluşlar şeklinde diğer ülkelerle ilişkilerin ötesinde artan bir şekilde genişlemektedir. Dış politika ayrıca bir ülkenin uluslararası amaçlarını başarmak amacıyla kullandığı araçları da içermektedir. Dış politika bir ülkenin nasıl karar verdiğini neye karar verdiğini ve nasıl hareket ettiğini içermektedir.³¹⁴

Dış politika süreci, bir ülkenin politika üzerinde nasıl karar verdiğini ve bu kararın nasıl uygulandığını olarak tanımlanmaktadır. Politika seçimleri, kimin karar verdiğinden ve bu kararların nasıl alındığından etkilenmektedir. Demokratik hükümetlerde, tek bir dış politika süreci yerine çok çeşitli dış politika süreçleri bulunmaktadır. Politika süreçlerinin neden ve nasıl değiştiği ile ilgili birçok açıklama da mevcuttur. En genel açıklama, farklı şekildeki konuların, birbirinden farklı olarak işlenmesi olarak ifade edilmektedir.³¹⁵

İkinci Dünya Savaşı'ndan sonra savaştan galibiyetle ayrılan iki süper güç olarak adlandırılan Amerika Birleşik Devletleri ve Sovyetler Birliği'nin (Sovyet Sosyalist Cumhuriyetler Birliği – SSCB) arasındaki ilişki, anlaşmazlık ve çatışmanın herhangi bir şiddete başvurmadan ve doğrudan silah kullanılmadan sürdürülmeye çalışıldığı belirli bir tarihsel dönem olarak adlandırılan Soğuk Savaş dönemi 1917

³¹⁴ Hakan Fidan, *Intelligence and Foreign Policy: A Comparison Of British, American and Turkish Intelligence Systems*, Yüksek Lisans Tezi, 1999, s.26.

³¹⁵ Hakan Fidan, *Intelligence and Foreign Policy: A Comparison Of British, American and Turkish Intelligence Systems*, s.28.

tarihinden beri süregelen Doğu-Batı çekişmesinin bir tezahürü olarak nitelendirilebilmektedir, .³¹⁶ İkinci Dünya Savaşı'nın akabinde dünya yaklaşık yirmi yıl ABD ve SSCB'nin etrafında “iki kutuplu” hale gelmiş ve savaştan tamamen harap ve bitap çıkan Avrupa devletleri de bu iki “süper” devletin çevresinde kümelenmişlerdir.³¹⁷ Soğuk Savaş, bu iki süper gücün arasında başlayan ve tüm dünyaya yayılan gerilim tırmandırma politikası, casusluk, dış yardımlar, ittifaklar, propaganda ve vekâlet savaşları şeklinde politik, stratejik ve ideolojik mücadele olarak da ifade edilebilmektedir. ABD, İkinci Dünya Savaşı'nın sonrasında Monroe Doktrini'nden vazgeçmek suretiyle bir dünya devleti olmuş ve dünya siyasetine yön veren birinci ülke konumuna geçmiştir. SSCB'de, 1945'ten itibaren takip etmiş olduğu aktif, yayılmacı ve emperyalist politikasıyla beraber, teknolojik gelişmede ilerleyerek dünya sahnesinin birinci planına geçmiştir. İkinci Dünya Savaşı'ndan galipleri durumunda olan ve “süper güç” olarak konumlanan SSCB ile ABD arasındaki rekabet, dünya düzenine ilişkin görüş farklılığı ve çıkar çatışmasından kaynaklanmış ve bu gergin hal “Soğuk Savaş” dönemini doğurmuştur.³¹⁸ Soğuk Savaş döneminde güvenlik olgusunun ideolojik, siyasal, ekonomik ve askeri temeller üzerine kurulduğu ve daha etkin olan unsurun askeri güvenlik olduğu ifade edilmektedir.

3.1.3. Ekonomi Güvenliği

Ekonomi güvenliği, sürekli değişen ekonomik çevreden ve ekonominin iç ve dış tehditlerinden etkilenen karmaşık bir sosyo-ekonomik kategori olarak tanımlanmaktadır. Ekonomi güvenliğinin devletin ulusal güvenliğinin temelini oluşturduğu ifade edilmektedir. Ulusal güvenliğin sağlanmasının ekonomi temsilcilerinin yakın işbirliği ile devletin birincil sorumluluğu altında olduğu belirtilmektedir. Ulusal güvenliğin devletin siyasi, hukuki ve ekonomi kurumlarının ulusal ekonomik gelenek ve değerlerinin kilit varlıklarını korumak için konuyla ilgili yeteneklerinin bir yansıması olduğu ifade edilmektedir. Bu nedenle ekonomi güvenliğinin gelişiminin ulusal güvenlik devletin oluşumu bağlamında görülmesi gerektiği belirtilmektedir. Devlet için ulusal ekonomiyi tehdit eden iç veya dış bir

³¹⁶ Oral Sander, Siyasi Tarih: 1918-1994, 24. bs., Ankara, İmge Kitabevi, Ekim 2014, s. 224.

³¹⁷ Age, s.201.

³¹⁸ Armaoğlu Fahir, 20. Yüzyıl Siyasi Tarihi, 18. bs., İstanbul, Alkım Yayınevi, Nisan 2012, s. 512.

tehdinin olmaması durumunda mutlak bir ekonomi güvenliğınden söz edilemeyeceğı de ifade edilmektedir. Ülkenin ekonomi güvenliğınin ana faktörlerinin coğrafi konum, doğal kaynaklar, tarımsal potansiyel, sosyo-demografik gelişim derecesi ve kamu yönetimin kalitesi olduğu belirtilmektedir. Ayrıca internet teknolojilerinin ekonomi üzerindeki etkilerinin ve bu faktörün ekonomi güvenliğınin yeni faktörlerinden olduğunun ve göz ardı edilmemesi gerektiğinin belirtildiğı ifade edilmektedir. Artık e-ticaret ve e-iş teknolojileri üzerinde ağ ekonomisi kavramının ortaya çıktığı belirtilmektedir. Bu kavramın devletlerin ekonomi güvenliğınin geliştirilmesi kapsamında göz önünde bulundurulması gerektiğı de vurgulanmaktadır.³¹⁹

Ekonomi bilimi, artan bir eğilim göstermekle birlikte gün geçtikçe değişen, sayısız insan ihtiyaçlarının karşılanabilmesi için üretilen mal ve hizmetlerin değiş tokuşu, paylaşılması ve tüketilmesi gibi ekonomik faaliyetler olarak tanımlanmaktadır.³²⁰ Ekonomi biliminin sadece bireysel ülke bazında değil dünya genelinde diğer bilimlerden farklı olarak sosyal, politik süreçler ve ekonomik gelişim piyasaları ile yakından ilişkili olduğu ifade edilmektedir. Küreselleşmenin ve sosyal değişimin sadece ekonomik anlayışı değil aynı zamanda ekonomik teori kavramını da etkilediğı belirtilmektedir. Ekonomi güvenliğı kavramının yakın bir geçmişte 20. yüzyılda ortaya çıktığı ifade edilmektedir. Ekonomi güvenliğı kavramının 1934 yılında ABD Başkanı T. Roosevelt tarafından federal bir ekonomi güvenliğı komitesi kurması ile dünyaya tanıtıldığı belirtilmektedir.³²¹ Ekonomi güvenliğınin ana konusunu oluşturan unsurun yasama, yürütme ve yargının ekonomi güvenliğı içerisindeki fonksiyonlarını yerine getiren devlet olduğu ifade edilmektedir. Ulusal güvenlik çıkarlarının, ekonomi güvenliğı sistemi içinde kilit rol oynadığı da belirtilmektedir. Ulusal ekonomi çıkarlarını belirlemek için birçok aksiyonun alınmasının yanı sıra mevcut ekonomik durumun analizinin yapılması ve eğilimlerin tanımlanması gerektiğı ifade edilmektedir. Devletin sosyo-ekonomik gelişimini gösteren ekonomik göstergelerinin de geliştirilmesinin bu kapsamda önemli olduğu belirtilmektedir. Ekonomi güvenliğınin aktivite göstergeleri olarak da ifade edilebilen

³¹⁹ Ekaterina Grigoreva ve Liliya Garifova, "The economic security of the state: the institutional aspect", *Procedia Economics and Finance* 24, July 2015, Russia, S.266-267.

³²⁰ Zeytinoglu, E.; *Ekonomik Sistemler*, M.Ü. Yayını, No: 429, İstanbul 1985, s.1, 2; Üstünel, B.; *Ekonominin Temelleri*, Ankara 1975, s.27, 33

³²¹ Zaneta Simanaviciene, "Economic Security and National Competitiveness", *Public Security and Public Orde* 2015 (15), s.127.

belirli kriterlere göre değerlendirildiği ifade edilmektedir. Bu göstergelerin en önemlileri şu şekilde ifade edilebilmektedir; Gayri Safi Yurtiçi Hâsıla (GSYİH), endüstriyel kalkınma ve yatırım hızı, büyüme oranı, doğal kaynaklar, ülkenin endüstriyel ve bilimsel-teknik potansiyeli, kaynakların verimli kullanımı, iç ve dış pazarda ekonomik rekabet, enflasyon, işsizlik oranı, yaşam kalitesi, gelir eşitsizliği, kamu hizmetlerinin erişebilirlik derecesi, bütçe açığı, kamu borcu, enerji bağımlılığı.

Ekonomi güvenliğinin analizinin bu göstergelerin sınırlarını belirtmek için önemli olduğu belirtilmektedir. Bu sınırların aşılması durumunun ekonomi güvenliği için bir tehdit oluşturabileceği ifade edilmektedir. Bu limitlerin belirlenmesinin yanı sıra daha önemli olanın ekonomi tehditlerinin tanımlanmasına yardımcı olan devletin ekonomi güvenliği kavramını açıklaması olduğu belirtilmektedir. Babachinaite'nin bireysel, ulusal ve uluslararası olmak üzere üç seviyeden oluşan güvenlik kavramını belirlediği ifade edilmektedir. Nüfusu oluşturan bireyler ve grupların çevresel koruma ve kalite faktörlerinin yanı sıra askeri, siyasi, ekonomik ve diğer sosyal faktörlerin ekonomi güvenliği üzerinde bir etki oluşturduğu belirtilmektedir. Cepaitien'in güvenlik kavramı fikrinin en dar askeri güvenlik anlayışı işe başlayarak 8. ve 9. yüzyıllarda daha geniş bir konu yelpazesini içerecek şekilde geliştiğini daha derinleşerek uluslararası ya da küresel güvenlik konularından bireysel düzeyde insan güvenliğine kayarak büyük bir dönüşüm geçirdiğini belirttiği ifade edilmektedir.³²²

Ekonomi kavramı insan ihtiyaçlarının karşılanması amacıyla her türlü mal ve hizmetlerin üretilmesi ve dağıtılmasından, ticareti ve tüketimine kadar olan süreçlerin tamamını içeren bir insan faaliyeti olarak tanımlanmaktadır. Bu kapsamda ekonomi güvenliğinin insan faaliyetlerini içeren olağandışı halleri kapsadığı ve üretim, ticaret, dağıtım ve tüketim alanlarında farklı manalara geldiği ifade edilmektedir. Ekonomi güvenliği kavramının risk ile iç içe bir kavram olan finans alanında da farklı anlamı ifade ettiği belirtilmektedir. Ekonomi güvenliği, güvenliğin ana unsurunun birey olduğu ve bireyin geçim düzeyi ile yaşam standardının korunması olarak nitelendirilen "bireylerin ekonomi güvenliği" kavramı ile ilişkilendirilmektedir.³²³ Ekonomi kavramının bir diğer anlamı ile güvenlik konularının devlet ve uluslararası düzeydeki iktisat faaliyetleri ile ilişkilendiren Siyasal Ekonomiye kastettiği de belirtilmektedir.

³²² Age, 128-129.

³²³ Mesjasz, Krakov, "Ekonomik Güvenlik", Uluslararası İlişkiler, Cilt 5, Sayı 18 (2008), s. 128-129.

Ekonomi kavramının bilimsel ifadesinin insanların ihtiyaçlarını karşılamaları için kullandıkları sınırlı kaynakların farklı kullanım biçimlerine göre yaptıkları seçimler olarak tanımladığı ifade edilmektedir. Ekonomi terimine güvenlik kavramının eklenmesi ile ekonomi güvenliği kavramının rasyonalite, iyileştirme, etkinlik ve fayda kategorilerinde değerlendirildiği ve bu kategorilerin bazılarının olmaması durumunun da tehdit kavramını doğurduğu belirtilmektedir. Devlet güvenliğinin küresel, devlet seviyesinde ve devletler arası seviyeler olmak üzere farklı seviyelerde toplumun refah düzeyi üzerindeki etkisinin ekonomi kavramıyla değerlendirildiği ifade edilmektedir. Bunun yanı sıra bireylerin, şirketlerin, kurumların ve bölgelerin güvenliğinin ekonomi kavramının gelişimine etkisi olduğu belirtilmektedir. Ekonomi güvenliği ile ilgili ilk kaynakların Aristo ile ilişkilendirildiği bu kavramın oluşturduğu kurumsal sorunların ise 17. ve 18. yüzyıllara dayandığı ifade edilmektedir. Ekonomi güvenliği kavramının ulusal güvenlik kavramından ayrı değerlendirilemeyeceği de belirtilmektedir.³²⁴

Sosyalist bakış açısı ile değerlendirildiğinde ekonomi güvenliğinin güçsüz olanın güçlü olana karşı korunması ve ulusal ekonomik menfaatlerin devlet dışı müdahalelere karşı korunması olarak ifade edilmektedir.³²⁵

Ekonomi güvenliği kavramının bireylerin yaşam kalitesinden devletin varlığına kadar geniş bir yelpazedeki konu gruplarıyla ilişkilendirildiği ifade edilmektedir.³²⁶

Referans nesnesi, sorunlar, hassasiyetler, tehdidin öngörülmesi, eylemler, toplumsal sistemlerin güvenliğinin yapısal unsurları ve güvenli bir referans nesnesinin vasıfları ekonomi güvenliği konuları ve bağlamları olarak sıralanabilmektedir.³²⁷

Devletlerin karşı devletleri ve politikalarını etkilemek amacıyla kullanabileceği araçlar ekonomik araç olarak değerlendirilmektedir. Ekonomi güvenliğinin ekonomi araçlarını kullanan diğer devletlerin idaresinden bağımsız olmak anlamına geldiği ifade edilmektedir. Devlet güvenliğini oluşturan bir unsur olarak günümüz siyasi hayatın içinde sıklıkla kullanılan bir kavram olan ekonomi

³²⁴ *Age*, s.130.

³²⁵ *Age*, s.131.

³²⁶ *Age*, s.135.

³²⁷ *Age*, s.139-140.

güvenliği devlet kurumları tarafından toplumsal refahın ve iyileşen yaşam kalitesinin bir göstergesi olarak değerlendirilmektedir.³²⁸

Ekonomi güvenliği devletin vatandaşlarına daha iyi yaşam kalitesi sağlamasının yanı sıra ulusal ve devletler arası iş ortamının güvenli, adil ve dinamik bir yapıda sağlaması durumu olarak ifade edilmektedir. ABD Ekonomi Güvenliği Yasası'nın ekonomi güvenliği kavramını ekonomik espionaj faaliyetlerine karşı koyma kapsamında da değerlendirdiği belirtilmektedir.³²⁹ Bireylerin içinde yaşadığı toplumun gelişmişlik derecesine göre geçim garantisi veya yaşam kalitesinin korunması veya geliştirilmesi bireylerin ekonomi güvenliği kavramını ifade ettiği belirtilmektedir.³³⁰

Bir ülkenin enerji ve hammadde kaynaklarının arz ve güvenlikleri ile ilgili konuların ekonomi güvenliği kapsamı içerisinde değerlendirilmesi önem arz etmektedir. Bu bağlamda enerji güvenliği ekonomi güvenliğinin kritik bir faktörü olarak değerlendirilmektedir. Petrol ve doğalgaz gibi olmazsa olmaz enerji kaynaklarının elde edilmesi hususu, ekonomi güvenliğini günümüzde de en çok etkileyen ve savaşlara sebebiyet verebilecek faktörler arasında yer almaktadır.³³¹

ABD, enerji kavramının ülkesi açısından ekonomik refahın temel unsurlarından olduğunu belirtmektedir. Enerji arzı ve talebinin ülkenin ulusal güvenlik açısından ve ekonomik çıktılar bağlamında giderek hayati bir rol oynadığını ifade etmektedir. Bir ulusu korumak ve ulusal güvenliği sağlamak için yeterli enerji kaynaklarına sahip olunmasının sağlanmasının gerekliliği ve muasır medeniyetlere güç verecek yeterli enerji olmadan güvenlikten söz etmenin mümkün olamayacağı belirtilmektedir.³³²

³²⁸ Age, s.141.

³²⁹ Age, s.142.

³³⁰ Hasan Aykın, Jeopolitikten Jeoekonomiye: Ekonomik, Güvenliğin Yükselişi", s.3.

³³¹ Kenan Turgutoğlu, "Güvenlik Perspektifinden Ekonomiye Bakış: Ekonomik Güvenliğin Ulus Devlete Etkilerinin Analizi", Uludağ Journal of Economy and Society / B.U.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi Cilt / Volume 36, Sayı / Issue 1, 2017 s.118.

³³² Sheila R. Ronis, Economic Security Neglected Dimension of National Security?, Center for Strategic Conferencing Institute for National Strategic Studies by National Defense University Press Washington, D.C., 2011, s.64.

3.1.4. Ulusal Güvenlik ve Ekonomi Güvenliği

Son yıllarda küreselleşme ve ekonomik entegrasyon bağlamında ekonomi ve ulusal güvenlik arasındaki ilişkinin giderek birbirine daha fazla bağlı hale geldiği ifade edilmektedir.³³³

Ulusal güvenlik, dışarıdan gelen saldırılara karşı koyabilme kabiliyeti olarak tanımlanmaktadır. Ulusal güvenlik kavramı halkın güvenliği ve emniyetinin sağlanması refah içinde yaşayabilmesi yasal düzenin korunması ile iç politika, ülkenin diğer ülkeler ve uluslararası konular bakımından başarmayı hedeflediği amaç veya bir dizi amaçlar olarak nitelendirildiği dış politika bağlamı kapsamında değerlendirilebilmektedir.³³⁴

Ekonomi güvenliğinin bir ülkenin toplumunun refahı, huzuru ve ekonomi sisteminin işleyişine tehlike oluşturabilecek potansiyel tehditlerle ilgili olduğu belirtilmektedir. Bu tehditlerin de bir ülkenin diğer ülke ekonomisinin ekonomik gücünü zayıflatmak ve bununla birlikte ekonomik yöntemleri de kullanarak dış politika emellerine ulaşmak için oluşturulan tehditler olduğu ifade edilmektedir. Ekonomi güvenliği bir taraftan ülkenin mevcut durumdaki ekonomi yapısını korumayı hedeflerken diğer taraftan ekonomi kaynaklı tehditleri göz önünde bulundurarak devletin toplumunun refahını artırmak için ülke menfaatlerinin emniyet altına alınması anlamına gelmektedir.³³⁵

Genel bakış açısı ile bakıldığında ulusal güvenlik anlam ve içerik bakımından sistematik bir şekilde ekonomi güvenliğine yaklaştığı ifade edilmektedir.³³⁶

Ekonomi güvenliği kavramının ülkenin büyüklüğü, siyasi sistemin istikrarı, uluslararası ekonomi çevresi ve dış bağlantıların kurumsallaşması arasındaki ilişki, iç ve dış koşullarda meydana gelen değişikliklere kurumsal ve sosyal adaptasyon faktörlerinden kaynaklanan doğrudan devletin ekonomik gücünün bir sonucu olduğu

³³³ Lucia Retter, Erik J. Frinking, Stijn Hoorens, Alice Lynch, Fook Nederveen, William D. Phillips, "Relationships between the economy and national security Analysis and considerations for economic security policy in the Netherlands", RAND Corporation", 2020, s.1.

³³⁴ Murat Şengöz, Türkiye Cumhuriyeti'nin Ulusal Güvenlik Paradigması Üzerine Bir Değerlendirme, Takvim-i Vekayi ISSN: 2148-0087, 2020.

³³⁵ Hasan Aykın, Jeopolitikten Jeoekonomiye: Ekonomik, Güvenliğin Yükselişi", s.4.

³³⁶ Marius Petre, Economic Security, Organic Dimension of National Security, MPRA Paper No. 17936, 18 Oct 2009.

belirlenmektedir. Güvenlik kavramının sadece tehditlere, tehlikelere veya tehlike oluşturabilecek risklere karşı bir koruma sistemi anlamına gelmediği ifade edilmektedir. Teknolojinin ve bilhassa internetin gelişmesiyle birlikte güvenlik kavramının tanımında değişikliğe gidilmesinin zorunlu hale geldiği de söylenebilmektedir. Bu kapsamda geleneksel bir anlayıştan daha modern ve esnek sınırlara evrilen güvenlik kavramının yeni bir boyut kazandığını ifade etmek mümkündür.

ABD'nin dış politika alanında görüşlerini yansıttığı strateji belgelerinden ilki olarak kabul edilen Monro doktrini, ABD'nin kuruluşundan bu yana ulusal güvenlikle ekonomi güvenliğinin birbirinden ayrılmaz bir parça olduğunu benimsemiş çabaları olarak yorumlanmaktadır. ABD Başkanı Roosevelt'in güvenlikleştirme adımlarını atmaya başladığı ve bu kapsamda bireysel ekonomi güvenliği kavramının geleceğine yönelik düşüncelerini ifade ettiği 1944 yılında yapmış olduğu konuşmasında ulusal güvenliğin öncelikli ele alınması gereken konusu olarak her bir vatandaşının kâfi düzeyde ekonomik yaşam seviyesinin sağlanması olduğunu vurguladığı ifade edilmektedir. Bill Clinton'ın Başkan olduğu dönemde hükümet, dış politika gündeminin öncelikli konuları arasında ekonomi güvenliğinin tesis edilmesi ve sürdürülmesine yer vererek ve 25 Ocak 1993 tarihinde "Ekonomi Güvenliği Konseyi" birimini kurmuştur. Çin, ekonomi güvenliğinin olmaması durumunda ulusal güvenlik kavramının yükümlülüklerini yerine getiremeyeceği, güvenlik kavramının sözde kalacağını belirterek bu kavramın stratejikliğine dikkat çekmiştir.³³⁷

3.1.5. Kripto Para ve Ekonomi Güvenliği

Yeni bir elektronik ödeme kolaylığı olarak ortaya çıkan kripto paraların özellikle kontrol mekanizmaları ile ilgili bir dizi tartışmalara neden olduğunu ifade etmek mümkündür.

Kripto para birimlerinin durumunu tanımlayacak ve işlemler için yasal çerçeveyi uyumlu hale getirecek küresel düzeyde tek bir düzenleme, ulus üstü bir sözleşme veya çok taraflı bir anlaşmanın bulunmadığı ifade edilmektedir. Bu nedenle

³³⁷ Turgutoğlu, "Güvenlik Perspektifinden Ekonomiye Bakış: Ekonomik Güvenliğin Ulus Devlete Etkilerinin Analizi", s.136.

kripto para birilerinin yasal durumunun devletten devlete farklılık gösterdiği belirtilmektedir. Birinci bölümde detaylı olarak anlatıldığı gibi bazı ülkeler bu alanı düzenleme yoluna gitmiş, kullanımı ve ticaretine izin vermiş, bazıları ise bu alanı düzenlemiş veya önemli ölçüde kısıtlamış veya açıkça yasaklamıştır. Kripto paraların dezavantajlarının bir taraftan siyasi ve ekonomik güç merkezlerinden bağımsızlık sağlayarak fayda sağladığı ifade edilirken, diğer taraftan spekülasyonlar ve yasa dışı suç faaliyetleri için cazip bir araca dönüştüğü ifade edilmektedir. Kripto para birimleri ile gerçekleştirilen işlemlerin resmi bankacılık sistemlerinden bağımsız olması vergi sistemi ile takip edilmesini neredeyse imkansız kıldığı ve anonimlik özelliğinin kara para aklama aracı için kripto paraları mümkün hale getirdiği belirtilmektedir.³³⁸

Kripto para birimlerinin Endüstri 4.0'ın bir elementi olduğu ve güvenlik konuları üzerinde çok disiplinli etkiye sahip olduğu ifade edilmektedir. Schwab'a göre bilgi teknolojilerinin Dördüncü Sanayi Devriminin güç merkezlerini değiştireceğinin yanı sıra devlet ve uluslararası güvenlik arasındaki bağlarını da değiştireceği ifade edilmektedir. 2016 yılında Dünya Ekonomik Forumu'nda blok zincir tabanlı Bitcoin teknolojisinin gelecek finansal altyapının temelini oluşturabileceği ifade edildiği belirtilmektedir. Kripto para birimlerinin hakikati ve milli güvenlik sorununun son birkaç yıldır artma eğilimi gösterdiği ifade edilmektedir. Limba ve diğerlerinin kripto para birimlerini yıkıcı teknoloji olarak tanımladığı ve etkisinin ülkelerin milli güvenliği ile ilgili olabileceği belirtilmektedir. Son yıllarda INTERPOL'ün darknet pazarında, kripto para birimlerinde ve belirli Bitcoin karıştırıcı suçlarında keskin bir yükselişe şahit olduğu ifade edilmektedir.³³⁹

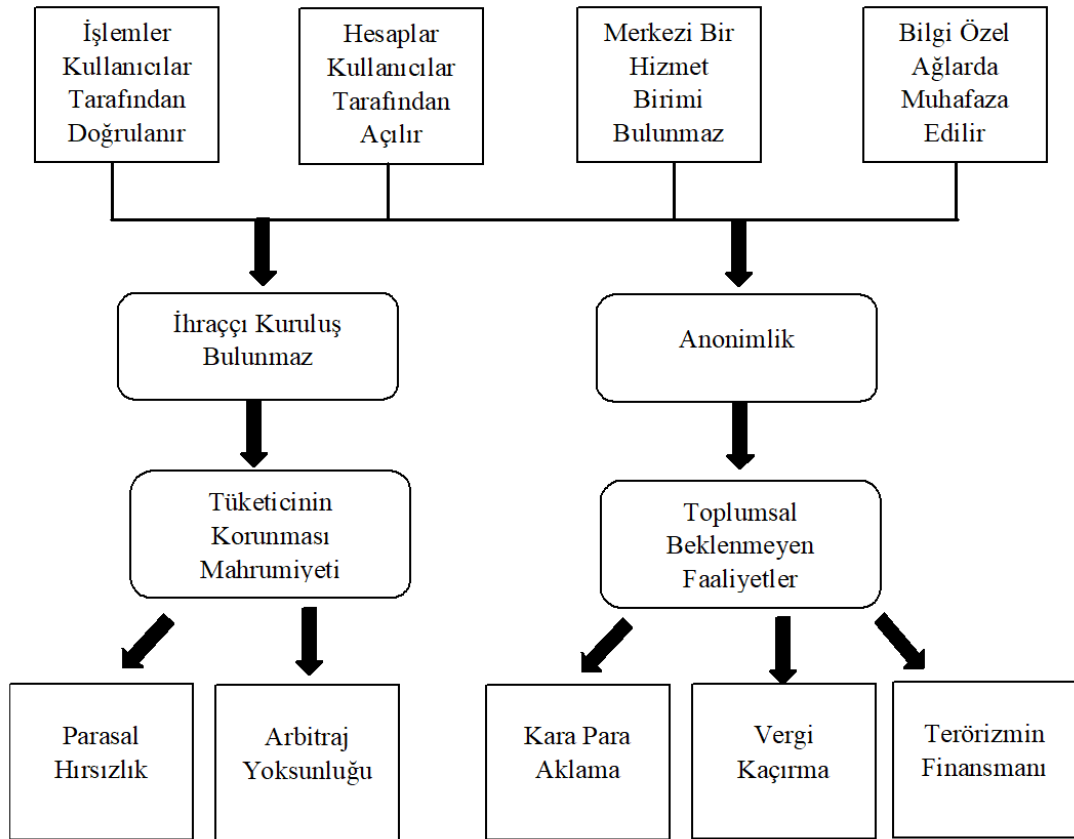
Küresel değişikliklerin ulusal güvenlik kavramına yeni bir kavramsal yaklaşım getirdiği belirtilmektedir. Ulusal güvenliğin kesin bir tanımını vermenin zorunlu olmadığı, zaman zaman kapsamının daraltılabileceği zaman zaman da genişletilebileceği ifade edilmektedir. Bazı yazarların ulusal güvenliğin içeriğini zihinsel felsefi olarak belirtirken diğerlerinin de teknolojik veya hukuki siyasi algı olarak ortaya koyduğu belirtilmektedir. Küresel ekonomi ve teknolojik gelişmelerin her ülkenin güvenliği konusunda birtakım yeni baş edilmesi gereken zorlukları da

³³⁸ Zoran Jović ve Goran Kunjadac, "Economic, Security And Information Aspects Of The Application Of Cryptocurrency And Their Impact On The South East European Countries", December 2018,

³³⁹ T. Limba ve diğerleri, "Cryptocurrency and National Security: Peculiarities of Interaction", Transformations in Business & Economics, Vol. 19, No 2 (50), 2020, s.43-44.

beraberinde getirdiği ifade edilmektedir. ABD Eski Başkanı Donald Trump'ın görev yaptığı dönemde Çin Bilişim devinin ABD'nin ulusal güvenliğini tehdit ettiğini duyurduğu zaman Huawei şirketine karşı aldığı siyasi pozisyonun, dijitalleşme ve ulusal güvenlik arasındaki ilişkinin önemini vurguladığı belirtilmektedir. Limba ve diğerlerinin kripto para birimlerinin parasal hırsızlık, arbitraj mahrumiyeti, kara para aklama, vergi kaçakçılığı ve Terörün finansmanı potansiyel risklerini beraberinde getirdiği ifade edilmektedir. Kripto paranın dijital platformlar üzerinde var olduğu ve doğal olarak da hukuk sistemini ihlal etmek için internet platformları oluşturarak yeni altyapılar ortaya çıkardığı ifade edilmektedir.

Şekil 3.1: Kripto Paraların Finansal Sistem Üzerindeki Potansiyel Tehditleri



i. Kripto paranın suç faaliyetleri için altyapı oluşturduğu alanlar:

1. Kripto paranın suç faaliyetleri için bir araç olarak kullanılması:
 - 1.1. Uyuşturucu satıcıları için bir internet platformu
 - 1.2. Geniş kapsamda yasa dışı ticaret (darknet ve diğer faaliyetler)
 - 1.3. Vergi kaçakçılığı
 - 1.3.1. Kara para aklama

- 1.3.2. Para tabakalama yöntemi (yasa dışı finansal bankacılık faaliyetlerinde olabilir)
 - 1.3.3. Para transferi
 - 2. Kripto paranın suç faaliyetleri için bir amaç olarak kullanılması
 - 2.1. Para hırsızlığı (makro veya mikro düzeyde)
 - 2.2. Suç teşkil eden dolandırıcılık faaliyetlerinde
 - 2.3. Yolsuzluk
- ii. Ekonomi güvenliğini tehdit ettiği durumlar:**
- 1. Doğrudan formlar:
 - 1.1. Yasa dışı ticaret faaliyetleri
 - 1.2. Vergi kaçakçılığı
 - 1.2.1. Yasa dışı finans bankacılık faaliyetleri (tabakalama, kredi verme)
 - 1.2.2. Vergi dolandırıcılığı
 - 1.2.3. Para transferleri
 - 1.2.4. Yolsuzluk
 - 2. Dolaylı formlar:
 - 2.1. Rekabet gücü
 - 2.2. Sosyal dışlanmışlık
 - 2.3. Şeffaf olmayan lobi faaliyetleri
 - 2.4. Devlete güven
- iii. Kamu güvenliğini tehdit ettiği durumlar:**
- 1. Doğrudan formlar:
 - 1.1. Organize suçlar
 - 1.1.1. Uyuşturucu kaçakçılığı
 - 1.1.2. Yasa dışı suç faaliyetleri
 - 1.1.3. Para hırsızlığı
 - 1.1.4. Dolandırıcılık
 - 1.1.5. Vergi kaçakçılığı ve vergi dolandırıcılığı
 - 2. Dolaylı formlar:
 - 2.1. Terörün finansmanı
 - 2.2. Hibrit tehditler (siberetik ve bilgisel tehditler)

2.3. Kritik altyapı nesnelere yönelik tehditler

Yukarıda yer alan sınıflandırma, kripto paranın ulusal güvenlik ile çok düzeyli etkileşimine dayandığını ifade etmektedir. Kripto paranın ekonomi güvenliğine veya ulusal güvenliğe bir tehdit olarak suç faaliyetleri için bir altyapı oluşturduğu tanımının yapılabileceği belirtilmektedir.

Kripto para birimlerinin doğrudan ve dolaylı olarak farklı vektörlerde ulusal güvenlik bağlamında ortaya çıktığı ifade edilmektedir. Doğrudan formların ekonomik güvenlik ve toplum güvenliği üzerinde etkisi olduğu belirtilmektedir. Kara para aklama, yasa dışı para transferi veya yasa dışı finansal bankacılık faaliyetleri ekonomi güvenliğini tehdit ettiği belirtilmektedir. Kamu güvenliğine yönelik tehditlerin uyuşturucu kaçakçılığı, dolandırıcılık suçu faaliyetleri, para hırsızlığı ve yasa dışı e-ticaret şeklinde organize suç faaliyetleri olarak ortaya çıktığı ifade edilmektedir. Tehditlerin ulusal güvenlik üzerindeki dolaylı etkisinin ulusal güvenliğin hem ekonomi hem de kamusal temel unsurlarından türetildiği belirtilmektedir. Ulusal güvenliğe yönelik dolaylı tehdit unsurları şu şekilde ifade edilmektedir; rekabet gücü, şeffaf bir yasama süreci, sosyal güvenlik, devlete güven, Terörün finansmanı ve hibrit tehditler ve kritik alt yapı nesnelere yönelik tehditler.³⁴⁰

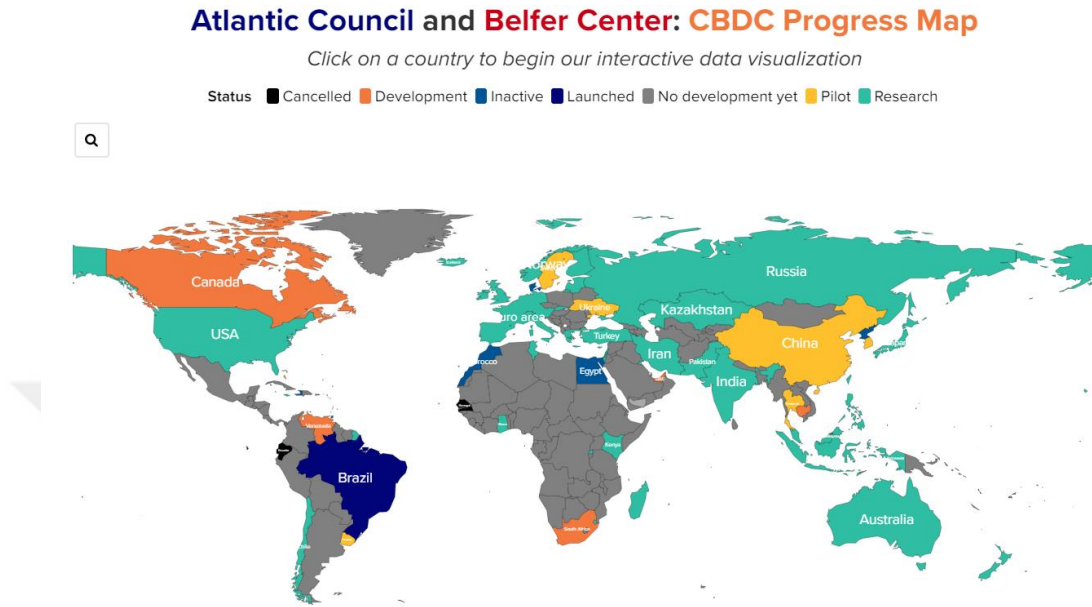
Para ve maliye politikaları bir ülkenin ekonomi politikasını oluşturan temel bileşenler olarak belirtilmektedir. Hükümetler büyümeyi ve istihdamı sağlayabilmek amacıyla vergilendirme (gelir toplama) ve harcama yapma şeklinde bir yol izleyerek maliye politikasını oluşturmaktadır. Para politikası, merkez bankaları tarafından farklı araçların kullanılması ile fiyat ve finansal istikrarın sağlanması olarak ifade edilmektedir. Merkez Bankaları ayrıca bir ulus devletin önde gelen güçlerinden olan para basma faaliyetini de yürütmekle sorumlu kurumlardır. Kripto paraların paranın üretilmesinden topluma arzına kadar ki sürecin tek elden yürütülmesinde rol üstlenen merkez bankalarına karşı bir mekanizma olduğu değerlendirilmektedir. Bu noktada merkez bankalarının kendi kripto paralarını geliştirmeleri konusunun gündeme geldiği de ifade edilmektedir.³⁴¹

³⁴⁰ T. Limba ve diğerleri, "Cryptocurrency and National Security: Peculiarities of Interaction", Transformations in Business & Economics, Vol. 19, No 2 (50), 2020, s.56-58.

³⁴¹ Mustafa Çalışır ve Cahit Şanver, "Kripto Paralar ve Para & Maliye Politikalarına Muhtemel Yansımaları", IBANESS Conference Series, Tekirdağ, 2018, s.160.

Aşağıdaki şekil ülkelerin merkez bankalarının kendi dijital para birimlerini çıkarmaları ile ilgili hangi aşamada olduklarını göstermektedir.

Şekil 3.2: Merkez Bankası Dijital Para Birimi Gelişim Haritası³⁴²



Basit bir niyet açıklaması ile gelecekteki kaderi için de neredeyse minimum düzeyde bir sorumluluk üstlenilen çoğunlukla da bir internet sitesi üzerinden ortaya çıkan yeni girişimlerin dakikalar içerisinde milyonlarca Doları keline çektiği ifade edilmektedir. İktisat teorisinden bilindiği üzere büyük gelirlerin, yüksek risklere dayandığı belirtilmektedir. Kripto paraların sahip olduğu durumun da bu kuralın bir istisnası olmadığı ifade edilmektedir. Büyük heyecan ile çeşitli blok zincir projelerindeki devasa nakit akışları sebebiyle bu alanın dijital para ekosistemi içinde spekülasyon yapan dolandırıcılar arasında en popüler kazançlardan biri haline geldiği belirtilmektedir. Bu kapsamda 2018 yılında Rusya’da Ethereum kripto parası ile gerçekleştirilen finansal dolandırıcılık tutarının 225 milyon ABD Dolarına ulaştığı ve yaklaşık 30 bin insanın da bu durumda mağdur olduğu ifade edilmektedir. Her bir kişinin kripto para dolandırıcılarına kripto para yatırımı amacıyla 7.500 ABD Doları

³⁴² The rise of Central Bank digital currencies, 01.02.2021, <https://www.atlanticcouncil.org/blogs/econographics/the-rise-of-central-bank-digital-currencies/>, Erişim: 13.02.2021.

gönderdiği belirtilmektedir. Bu durumun suç gelirlerinin aklanması ve Terörün finansmanı için büyük risk oluşturduğu belirtilmektedir.³⁴³

3.1.6. Milli Güvenlik ve Kripto Para

Ekonomi sisteminin gelişmelere açık, dinamik bir yapıya sahip olduğu ve yeni teknolojik fırsatların kullanımını içerdiği ifade edilmektedir. Ekonomi sisteminin bu yönünün yakın ilişkide olduğu milli güvenlik önlemlerinin sürekli kendini yenileyerek gelişmelere ayak uydurmak zorunda olmasına neden olduğu belirtilmektedir. Kripto paraların ortaya çıkışının küresel boyutta aktif bir şekilde tartışılmakta olduğu ve bunun en yaygın bilinen örneğinin de daha önceki bölümlerde de anlatıldığı üzere şüphesiz Bitcoin olduğu ifade edilmektedir. Bitcoin'in yaygınlığı ve bilinirliğinin dünya üzerindeki birçok ülkeye yayıldığı ve Avro ve Dolar gibi milli para birimleri ile de yarıştığı belirtilmektedir. Bitcoin'in herhangi bir fiziksel varlıklarla desteklenmediği ve herhangi bir dünya para birimine de bağlı olmadığı ifade edilmektedir. Arz ve talep dengesi ile değerinin belirlendiği ve bu durumun da fiyat dalgalanmasına neden olduğu belirtilmektedir. Tüm Bitcoin işlemlerinin kayıtlarının gerçek katılımcıların bilgilerinin ifşa edilmeden halka açık tutulduğu ifade edilmektedir. Bu özelliğin bu yenilikçi ödeme sisteminin suç faaliyetlerinde kullanılmasını kolaylaştıran bir araca dönüştürdüğü belirtilmektedir. Bitcoin'in döviz kurunun istikrarsız olduğu da ifade edilmektedir. İnternetin dünya genelindeki yaygınlığı ve kullanımına rağmen kripto para biriminin yasal olarak güvenli olmadığı belirtilmekte olup sadece hukukçular ve ekonomistler tarafından değil her şeyden önce yazılım mühendisleri tarafından da ayrıntılı bir şekilde ele alınması gerektiği vurgulanmaktadır. Daha önceki bölümlerde de ayrıntılı bir şekilde ele alınan kripto paraların ayırt edici özelliklerini şu şekilde sıralamak mümkündür:

1. Gerçek satın alma gücü
2. Güvenlik eksikliği

³⁴³ Vorobyev A. V., "ICO as Economic Security Threat. Possible Risks Analysis. Experience of Foreign States" in III Network AML/CFT Institute International Scientific and Research Conference "FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies", KnE Social Sciences, pages 208–214. DOI 10.18502/kss.v3i2.1544, 2018.

3. Başlıca dünya para birimleri ile resmi döviz kuru
4. Dağıtık yapısı (ihraç yönetimi ve kontrolünün tek bir kişi tarafından yürütülmemesi)
5. Operasyonların anonim olması
6. Algoritmik sınırlamalar nedeniyle enflasyonun olmaması
7. Değerinin arz ve talebe göre belirlenmesi

Elektronik para ile kripto para arasındaki ayrımı elektronik paranın sahip olduğu birtakım temel özellikleri bakımından yapmanın önemli olduğu vurgulanmaktadır. Geleneksel para biriminin elektronik transferi için yasal mübadele aracı olarak kullanılan elektronik para depolanabilmektedir. Bu bağlamda en büyük önem şudur ki yasa dışı eylemlerin uygulanmasına izin veren kripto paraların herhangi bir denetim mekanizmasının kontrolünde gerçekleşmeyen yetkisiz transferinin yasal çerçevenin dışında olduğu belirtilmektedir. Elektronik paranın ekonomik açıdan en önemli özelliğinin ise değerini koruması olarak ifade edilmektedir. Yukarıda bahsedilen kripto paranın sahip olduğu bu özelliklerin milli güvenliğe bir tehdit oluşturduğu belirtilmektedir. Kripto paraların doğrudan veya dolaylı olasılık yaratan bir dizi koşul ve faktörlerinin kendi varlıklarını korumaları ve sürdürülebilir gelişimlerini sağlamak için bireylerin toplumun ve devletin objektif olarak önemli ihtiyaçlarına zarar verdiği ifade edilmektedir. Sanal para birimlerinde gerçekleştirilen işlemlerin riski ile ilgili benzer bir görüşün Avrupa Birliği tarafından yayınlanan bir uyarı ile ortaya konulduğu da belirtilmektedir. Bu uyarıya göre sanal paraların yasal düzenlemeden yoksun oldukları ve bu nedenle tüketicilerin devlet tarafından korumasının mümkün olmadığı ve para kaybetme riskinin yüksek olduğu ifade edilmektedir. Avrupa Birliği Kara Para Aklama Önleme Direktifi'ne (Anti Money Laundering Directive – AMLD) göre ise sanal para birimlerinin yasal kullanım seçeneklerine sahip olmalarının yanı sıra cirosunun, finansal sistemler için yasal riskler içerdiği de belirtilmektedir.

Yasal kripto para işlemlerinin işlem maliyetlerini azaltarak ödemelerin verimliliğini artırma potansiyeline sahip olduğu belirtilmektedir. Bitcoin'in mevcut çevrimiçi ödeme sistemlerinin geliştirilmesine katkı sağlayacak bir özellik olan borsa alım satım işlem ücretleri olmadan küresel para birimi olarak işlev görebileceği de ifade edilmektedir. Bununla birlikte Bitcoin gibi kripto paraların yatırım aracı olarak

kullanıldığı durumlarında mevcut olduğu belirtilmektedir. Fakat Bitcoin'in ve türevlerinin milli güvenlik için en büyük risk sergilediğine dikkat çekilmesi gerektiği ifade edilmektedir. Özellikle Bitcoin sisteminin ağ katılımcılarını tam anonimlikle karakterize etmesinin aşırıcılık ve terörün finansmanı ile ilişkili yasa dışı faaliyetlerin gelişimine bir temel oluşturduğu belirtilmektedir. Ayrıca sanal para birimlerinin sahip olduğu potansiyel güvenlik açığının yasa dışı operasyonlarda sıklıkla kullanıldığı kara para aklama ile mücadelede görev yapan finans uzmanları tarafından işaret edildiği ifade edilmektedir. Bunun nedeni olarak da sanal para birimlerinin geleneksel nakitsiz ödeme yöntemleri ile karşılaştırıldığında sanal para birimi altyapısının müşterilerle doğrudan etkileşimin olmadığı durumlarda anonim finansmana izin verdiği sahip olduğu yüksek derecede anonimlik olduğu belirtilmektedir. Kripto para işlemlerinin finansman kaynağının tanımlamasının düzgün olarak yapılmadığı kripto para borsaları üzerinden yürütüldüğü ifade edilmektedir. Bu durumun sistemin şüpheli işlem gerçekleştirenlerin izini sürebilecek bir yazılımın kullanamamasından dolayı ciddi sorunlara neden olabileceği de belirtilmektedir. Diğer bir sorunun ise kripto para birimi içeren hizmetlerin çok yaygın bir coğrafyaya dağılması olduğu ifade edilmektedir. Bu yüzden kripto para birimlerinin dünyanın farklı coğrafyalarında farklı yargı sistemlerine maruz kalan karmaşık altyapı operasyonları sistemi içinde faaliyet gösterdiği belirtilmektedir. Bu nedenle denetleme ve yürütme yetkilerinin yanı sıra kara paranın aklanmasına karşı mücadele sistemine uymak için getirilecek birtakım sorumlulukların oluşturulmasının çok zor olduğu vurgulanmaktadır. Birçok devletin dünyanın herhangi bir yerindeki terörist organizasyonları kendi çıkarları doğrultusunda gizlice desteklediğinin bilindiği ifade edilmektedir. Bu kapsamda Bitcoin ve türevleri olarak geliştirilen kripto paraların işlemler üzerindeki kontrol mekanizması eksikliği göz önüne alındığında terörü finanse eden kuruluşlar ile arasında gerçekleşen anonim işlemlerin riskinin son derece yüksek olduğu ve milli güvenliğe tehdit oluşturabilecek bir unsur olduğu düşünülmektedir.³⁴⁴

³⁴⁴ Natalia G. Vovchenko, Evgeniy N. Tishchenko, Tatiana V. Epifanova, Mark B. Gontmacher, "Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them", European Research Studies Volume XX, Issue 1, 2017, s.37-38-39.

SONUÇ

Kripto anarşist felsefenin ürünü olarak hükümetlerden ve merkez bankalarından bağımsız bir şekilde resmi otoriteyi yok sayarak, dağıtık ağ üzerinden işlemlerini gerçekleştirmek amacıyla geliştirilen kripto paraların doğası gereği sahip olduğu teknolojik avantajlar, terörün finansmanında potansiyel bir araç olarak kullanılmakta, kara para aklama sistemleri için işlevsellik oluşturmakta ve bu durum ciddi bir milli güvenlik sorunu oluşturmaktadır.

Kripto para, işlemlerini gerçekleştirebilmek için teknolojinin dolayısıyla internetin gücünü kullanmaktadır. İnternet, P2P ve açık kaynak kodlu yazılımlar gibi bilgi teknolojilerinde meydana gelen gelişmeler Bitcoin ve benzeri kripto paraların ortaya çıkmasını, yaygınlaşmasını ve kullanımının artmasını sağlamaktadır. Kripto paraların doğası gereği sahip olduğu kaynağının ve hedefinin anonimlik özelliği, yani ortada sahibi belli olmayan sanal dijital bir cüzdanın varlığı, fidye taleplerinde, kara para aklama işlemlerinde, dolandırıcılık, vergi kaçırma, siber saldırılar, uyuşturucu kaçakçılığı ve terörün finansmanı gibi yasa dışı faaliyetlerde rahat kullanımı suç teşkil ederek ve suça teşvik etmektedir.

Kripto paralar işlemlerini gerçekleştirebilmek için teknolojinin dolayısıyla internetin gücünü kullanmaktadır. Kripto paraların kökeninin aslında 1992 yılında Timothy May tarafından bir manifesto olarak yayınlanan kripto anarşiye dayandırıldığı ifade edilmektedir. Kripto anarşinin temel felsefesi şifreleme yöntemi ile iletişimin otonom bir şekilde bireyler arasında gerçekleşmesi ve devletin müdahalesini ortadan kaldırması esasına dayanmaktadır. Baskı teknolojilerinin icadı nasıl ki ortaçağ loncalarının gücünü azaltıp değiştirdiyse, kriptolojik veya diğer bir ifadeyle şifreleme yöntemlerinin de şirketlerin, kurumların doğasını ve devletlerin ekonomik işlemlere müdahalesini değiştireceği görüşü savunulmaktadır. Teknolojinin de gelişmesi ile birlikte kripto anarşinin yeni sözcüklere ve resimlere de aktarılmasının likit bir piyasa oluşturacağı görüşü hakimdir. Küçük bir icat olarak görülen dikenli telin icadının batıdaki büyük çiftliklerin çitlerinin kaldırması ve böylelikle yer ve mülkiyet haklarını sonsuza kadar değiştirmesi gibi, matematiğin gizli bir dalı olan ve

önemsiz bir keşfi olarak görülen şifrelemenin de, fikri mülkiyetin etrafındaki dikenli teli kesen bir makas olacağı ifade edilmiştir.³⁴⁵

Bu bilgilerden yola çıkarak kripto paraların aslında ortaya çıkışının tesadüf olmadığı, doğuracağı sonucun da milli güvenliğe bir tehdit oluşturduğu ulus devlet yapısına zarar verdiği ve yakın bir gelecekte olmasa da belki bir nesil veya iki nesil sonra ortaya çıkma ihtimali olan ulus devlet yapısının ortadan kaldırılması için toplumun dönüştürülmesi şeklinde ortamı hazırladığıdır. Toprak parçası, halk ve egemenlik kavramları klasik devlet anlayışının zeminini teşkil eden unsurlardır. Meşrutiyet, şiddet araçlarının denetimi, anayasallık, iktidar, kamu bürokrasisi ve vergilendirme kavramlarının da eklenmesiyle ulus devletin unsurları ortaya çıkmaktadır.³⁴⁶ Bitcoin kripto para örneğinde, benzer etkileşim içerisinde yaşayan ve geliştiricileri tarafından ortaya konulan belli kuralları kabul etmiş insanların, devlet olmaya çalıştığı görülmektedir. Diğer taraftan kripto paranın sahip olduğu 915 milyar ABD Dolarını aşkın bugünkü piyasa değerinin dünyadaki birçok ülkenin ekonomisinden büyük olmasının ileride bu ülkelerin egemenlikleri konusunda çok hayati bir sonuç doğurabileceği ihtimalinin de göz ardı edilmemesi gerektiği de düşünülmektedir. Önce bilgisayar ağlarının; internetin ve sonrasında kişisel bilgisayarların, akıllı telefonların bilinçli olarak veya olmayarak hayatımızda önemli bir yer teşkil etmesi aslında milli güvenliğin tahrip edilerek devletin saf dışı bırakılmasıyla, verdiğimiz veya gönderdiğimiz verinin kaynağının bizi yönetmeye çalıştığının belirtileri şeklinde yorumlamak mümkündür.

Bir diğer önemli hususun da devlet yapısının ortadan kaldırıldığı an yeni terör tanımının ne olacağıdır. Devlet yapısı ortadan kaldırıldığında, terör yapıları da dönüşüme uğrayacaktır. Nasıl ki terör örgütleri teknolojiyi kendi amaçları doğrultusunda kullandıkça finansman araçlarında değişikliğe gidiliyorsa aynı şekilde kripto para egemen bir dünyada terörün şekil değiştireceği yorumu yapılabilmektedir.

Uluslararası güvenlik topluluğunun, kripto paranın mevcut ulusal finansal düzenleyici sistemin çok ötesinde olan ve tabiatını oluşturan izlenememe ve

³⁴⁵ Timothy C. May, “Kripto Anarşist Manifesto”, 22.11.2017, <https://www.activism.net/cypherpunk/crypto-anarchy.html>, (Erişim: 15.12.2017).

³⁴⁶ İbrahim Uğur Erkiş, “Ulus Devletin Tarihsel Gelişimi”, İİBF Sosyal ve Ekonomik Araştırmalar Dergisi, Yıl:13, Sayı:26, Konya 2013, s.69.

gözetiminin yapılamaması gibi özelliklerin üstesinden gelebilecek bir sistem geliştirerek terörist finansmanını engelleyip, suç tespitinin yapılana kadar, kripto paranın gelişmesinin endişe verici bir durum olmaya devam edeceğini ifade etmektedir. Kripto paralar, kullanıcının kimlik bilgisini gizli tutarak, yüksek miktarlarda ve çok hızlı bir şekilde dünyanın herhangi bir yerine işlem transferlerinin yapılabilmesine imkân sağlamasının DAESH, PKK ve diğer küresel terör örgütlerinin kullanımı için cazip bir alternatif oluşturduğu belirtilmektedir. Kripto para, başta terör örgütleri olmak üzere, kara para aklayıcıların ve diğer suç örgütlerinin fonlarını küresel olarak kolaylıkla hareket ettirebilmelerine imkân sağladığı belirtilmektedir. Bitcoin kripto parası kullanılarak gerçekleştirilen işlemler sırasında taraflar arasında standart işlem muhasebesi yöntemi kullanılmadığı için bu işlemlerin ayrıntılı olarak ulaşılabilir işlem defterinin bir parçası da olmayacağı ifade edilmektedir. Gerçek dünyadaki üçüncü kişi ve kurumlara açıkça bağlı olmayan Bitcoin işlemlerinin bu tek ve önemli istisnası dışında tamamen şeffaf olduğu betimlenmesi yapılmaktadır. Ama suç ögelerinin bu istisnayı kendi çıkarları doğrultusunda kullanabilme kabiliyetinin gözden kaçırılmaması gereken önemli bir unsur olarak belirtildiği ifade edilmektedir.³⁴⁷

Kripto para kullanımının yasa dışı faaliyetlerde artarak devam etmesi yasal bir düzenlemenin gerekliliğini ortaya koymaktadır. Ödemeyi gerçekleştiren ve alacaklı kişinin bilgilerinin açıkça belirtildiği izlenebilirlik sistemi geliştirilerek kripto para işlemlerinin gizliliği ortadan kaldırılmalıdır. Ayrıca kara parayı önlemek ve kara parayla mücadele etmek için sanal para düzenleme otoritesinin kurulması da küçük çapta bir çözüm oluşturabilmektedir.³⁴⁸

Kripto paraların düzenlemeye tabi tutulmasının yanı sıra Rusya ve Çin'de olduğu gibi tamamen yasaklanması da söz konusu olabilmektedir. Bu görüşün savunucuları anonimlik ve sistemin dağıtık yapısının kara para aklama işlemlerinde kolaylık sağlaması nedeniyle endişe duymaktadır. Bununla birlikte birçok kanun koyucu ise kâğıt paranın da Bitcoin gibi yasa dışı işlemlerde kullanılabileceğini ayrıca Bitcoin sisteminin dağıtık ağ yapısının yasa dışı olarak ilan edilse bile tamamen

³⁴⁷ Brill ve Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?", s.16-24.

³⁴⁸ Carata, "Modern Methods Of Financing Terrorism In A Global And Intercultural Society: Crypto-Currency", s.197.

kapatılmasının imkânsız olduğunu belirtmektedir. Bitcoin piyasasında yasa dışılığın nelerden kaynaklandığı üzerine yoğunlaşmak ve bu noktalarda düzenleyici tedbirler almak daha dengeli ve mantıklı bir yaklaşım olabilir. Bitcoin ve türevleri kripto paraların alım satımına aracılık eden borsalara yönelik bir düzenlemenin yapılması bir parça çözüm oluşturabilmektedir. Eğer kripto para borsaları “para verici” bir kurum olarak tanımlanırsa, örneğin hükümet kurumlarının Bitcoin’lerini 10 bin Dolara çeviren kişilerin kimliğini tespit etme imkânı sağlayabilir. Bu durum anonimlik özelliğini ortadan kaldırdığı için potansiyel suç aktivitelerinde bir azalma meydana getirecektir. Gerçek ve sanal para birimleri arasında aracılık eden borsalar bu durumdan etkilenirken, Bitcoin karşılığında Bitcoin türevlerinin alım satımını yapan borsalar maalesef dokunulmaz olarak kalacaktır ve hızlı ve ucuz bir değişim yöntemi olarak gelişmeye de devam edecektir.³⁴⁹

Bazı kripto paraların tam anonim özelliğe sahip olmasından dolayı, büyük bir çaba sarf edildiği takdirde bazı karmaşık tekniklerin de kullanılmasıyla yetkililerin kripto para kullanıcılarını bulmasının mümkün olabileceği ifade edilmektedir. Bu durumun kara para aklama ve terör finansmanı ile mücadelede yardımcı olmasına rağmen bazı durumlarda kara para aklama ve terör finansmanı ile mücadelede standart bir yaklaşıma izin vermediği de ifade edilmektedir.³⁵⁰

Kripto para düzenlemeye tabi olmayan dünyadaki en büyük pazarlardan birisidir. Yapılan bazı çalışmalara göre Bitcoin kullanıcılarının yaklaşık olarak dörtte biri ve Bitcoin işlemlerinin yarısının yasa dışı faaliyetlerle ilişkili olduğu ifade edilmektedir. ABD ve Avrupa yasa dışı uyuşturucu pazarının ölçeğine yakın olarak her yıl Bitcoin’i içeren yaklaşık 2 milyar ABD Doları yasa dışı faaliyet gerçekleştirildiği belirtilmektedir. Bitcoin faaliyetlerinin yasa dışı payının Bitcoin’e olan yoğun ilgiyle birlikte daha opak kripto paraların ortaya çıkmasıyla azaldığı ifade edilmektedir. Yapılan çalışmalar kripto paraların “kara e-ticaret” sağlayarak karaborsaların çalışma şeklini değiştirdiğini gösterdiği belirtilmektedir. Kripto paralar yasa dışı ticareti kolaylaştırmakla kalmayıp, blok zincir teknolojisinin doğası gereği sahip olduğu yapısından dolayı da yasa dışı faaliyetlerin tespitinde de etkili olduğunu

³⁴⁹ *Bitcoin and Money Laundering*, 2016-2017, s.171-172.

³⁵⁰ European Parliament, *Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion*, s.53.

kanıtladığı ifade edilmektedir. Bitcoin yasa dışı faaliyetlerde yoğun olarak kullanılsada, blok zincir teknolojisinin kripto paranın anonimliğine rağmen kolluk kuvvetlerinin yasa dışı faaliyetleri tespit etmesini gerçekten kolaylaştırdığı da ayrıca iddia edilmektedir. Koshy ve McDaniel'in 2014 yılında bilgisayardan blok zincirine iletilen işlemleri izleyerek gerçekleştirdikleri çalışma bireysel işlemlerle göndericinin IP adresi arasında bir bağlantının olduğunu göstermektedir. Kolluk kuvvetleri darknet üzerinde gerçekleştirilen yasa dışı faaliyetleri tespit etmek için siber gözetlemeden adli analize kadar posta hizmetleri yoluyla geçen şüpheli paketleri izlemek gibi birçok strateji kullanmaktadır. Bunun yanı sıra paket üzerindeki iade adreslerini araştırmak için de darknet pazarlarından uyuşturucu siparişi de verdikleri bilinmektedir. Bunun en güzel örneği büyük bir Avustralya'lı uyuşturucu satıcısından alışılmadık miktarda giden postalar, otoritelerin çok çeşitli uyuşturucu ve nakit ile birlikte 24 binden fazla Bitcoin'i ele geçirmesini sağlamıştır. Araştırmacılar bazen müşterilerin ve kimliklerini açığa çıkartmak için de tedarikçi olarak darknet üzerinde işlem yapabilmektedirler. Kolluk kuvvetleri tarafından yasa dışı pazara yönelik gerçekleştirilen 17 ülkeden 17 tutuklamanın yapıldığı Onymus Operasyonu gibi geniş çaplı girişimlerin, tespitlerin artmasını sağlayarak çevrimiçi yasa dışı gerçekleştirilen bu faaliyetleri engelleyebileceği ifade edilmektedir.³⁵¹

Dünyada ortak para birimi fikri, Harvard Üniversitesinde görevli Richard Cooper tarafından "Gelecek için Para Sistemi" (A Monetary System For The Future) isimli makale ile ilk defa 1984 yılında ortaya atılmıştır. Richard Cooper, yazdığı makalede yakın gelecek için 25 yıl içerisinde dünyanın daha elektronik bir hal alacağını belirterek radikal alternatif bir öneride bulunmuştur. Dünyadaki tüm endüstriyel demokrasiler için ortak bir para politikası ve bu para politikasını belirleyen ortak bir otorite ile ortak bir para biriminin oluşturulması tezini ortaya atmıştır. Her ülkenin kendi maliye politikasını belirlemekte bireysel özgürlüğe sahip olabileceğini fakat uluslararası sermaye piyasasında borçlanma gereği nedeniyle sınırlandırılabilirliğini ifade etmiştir. Richard Cooper'ın 1984 yılında yazmış olduğu makaleden³⁵² dört yıl sonra, The Economist dergisinin 9 Ocak 1988 tarihinde

³⁵¹ Sean Foley, Jonathan R. Karlsen ve Talis J. Putmins, "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?", Sydney 2018, s.8-9.

³⁵² Richard Cooper, "A Monetary System for the Future." Foreign Affairs, Fall 1984, 63(1), s.166-84.

yayınladığı kapak sayfasında “Dünya para birimine hazır olun” başlığı ile boynunda bir zincir ile altın renginde üzerinde 8026 yazan yeni bir para birimini taşıyan Anka kuşunun ayakları altında yanan dünya para birimleri resmedilmiştir.

Bu gelişmelere baktığımızda dünya ortak para birimi ile ilgili çalışmaların bundan yaklaşık 50 yıl önce başladığı söylenebilmektedir. Gerekli şartlar oluştuğunda da yapılan bu çalışmalar kendini göstermiştir. Bunun için dünya çapında para birimlerine olan güvenin azalması gerekiyordu ki 2008 yılında gerçekleşen finansal krizle birlikte, tasarlanan bu çalışma uygulamaya konulmuş oldu. 15 Eylül 2008 tarihinde Amerika Birleşik Devletlerinin en büyük finans kuruluşu olan Lehman Brothers’ın iflas etmesinden sonra dünyada geniş çapta bir ekonomik kriz patlak verdi. Temeli 90’lı yıllarda ortaya atılan blok zincir teknolojisi temeline dayanan Bitcoin 2008 yılında meydana gelen ve tüm dünyayı etkisi altına alan ekonomik krizi fırsat bilerek bu güven ortamının kaybolmasının ardından sadece birkaç ay sonra ortaya çıktı ve finansal dünyadaki tüm dengeleri altüst etmeye başladı. Bankaların para transferlerinde ve alışverişlerinde müşterilerinden aldığı işlem ücretleri ve komisyonların sebep gösterilerek, devletlerin ve bankaların finansal politikalarına tepki oluşturmak amacıyla piyasadaki güvensizlik ortamından yararlanan blok zincir teknolojisinin finans sektöründe kullanımı dünyada finansal piyasada bir dönüm noktası olarak kabul edilmektedir. Blok zincir teknolojisi kullanılarak geliştirilen kripto para Bitcoin ve türevleri blok zincir teknolojisinin dünyaya duyurulması aşamasında uygulamaya konulan bir oyun yaklaşımı olarak da değerlendirilebilir. Yeni finansal sistem faaliyete geçmeden önce mevcut finansal sistemle paralel çalışacaktır. Bitcoin ve benzeri kripto paralarının geliştirilmesi, dünyanın ortak dünya para birimine geçişte kullanıldığı geçiş argümanları olarak da nitelendirilebilir. Bitcoin ile blok zincir teknolojisinin pazarlandığını ve tarihte meydana gelen finans balonları gibi Bitcoin’in patlayabileceğini ama blok zincir teknolojisinin devam edeceği de açık bir gerçek olarak değerlendirilebilir. Şu an Bitcoin dışında yaklaşık 8.481 civarında alt coin bulunmaktadır. Bu alt coinlerin belki küçük bir kısmı gerçekten ciddi olarak bir teknoloji geliştirmek için ortaya çıkmış olabileceği düşünülebilir fakat geri kalan büyük çoğunluğunun tembel ve üretmeyen ülkelerin parasını sömürmek için ortaya çıkmış olma ihtimalinin yüksek olduğu yorumunu yapmak mümkündür.

Kripto para ve türevlerinde meydana gelen hızlı ve baş döndürücü gelişmeler dünya genelinde hükümetleri zaman zaman zor durumda bırakabilmektedir. Kripto paraların kara para aklama ve terörizm finansmanında yaygın kullanılması dışında, kripto paralar Mt. Gox Bitcoin borsasının 2014 yılında iflası ve milyonlarca Doların yok olması örneğinde olduğu gibi bazı çevrelerce çok riskli bir yatırım aracı olarak da değerlendirilmektedir.

İnsanoğlu tarih boyunca birkaç kere finans balonlarıyla karşı karşıya kalmıştır. Japonya'nın 1980'lerde hızlı büyümesinin ardından ABD'ye olan dış ticaret fazlasının oluşturduğu sorun ve ABD'nin de duruma el koyarak, Japon yeninin ABD Doları karşısında değerinin bilinçli olarak artırılmasından kaynaklanan ve aşırı fiyat enflasyonu olarak tabir edilen 1991 yılında patlayan balonun, Japonya'da 11 yıl ekonomik durgunluğa neden olduğu belirtilmektedir.³⁵³ 2000 yılında ABD'de internet tabanlı şirketlerin NASDAQ borsasındaki hisselerinin büyük değer kaybı yaşaması ile ortaya çıkan "Dotcom Balonunun"³⁵⁴ ve 2008 yılında emlak piyasasında ortaya çıkan "Housing Balonunun" küresel çapta tüm dünyayı etkileyerek finansal krizlere neden olduğu ifade edilmektedir.

Emtia fiyatlarının patlaması ve çökmesi örneklerinin tarih kadar eski olduğu söylenebilir. Lale Soğanı Balonu veya diğer bir ifadeyle "lale çılgınlığı" Hollanda'da 400 yıl önce meydana gelen hadise olarak bilinmektedir. 160 farklı çeşidi olan lalenin ilk defa 16. yüzyılda Türkiye'yi ziyarete gelen bir seyyah tarafından keşfedilip, İstanbul'dan alınıp Viyana'ya getirilmiştir. İlk defa 1554 yılında Hollanda'ya ithal edilen lale soğanı, birkaç yıl içerisinde çok değerli bir varlık haline gelip Almanya ve Belçika'ya yayılmıştır. Botanik bilimci Carolus Clusius'un Hollanda da bulunan Leiden Üniversitesinde 1593 yılında yetiştirdiği laleler çiçekler arasında egzotik bir çiçek olarak insanlar tarafından çok fazla rağbet görüp, dikkat çekmesi soylu ve asil aileler arasında bir çeşit statü sembolü haline gelmesi sonucu doğurdu ve lale soğanı spekülasyon nesnesi haline geldi.³⁵⁵ Lale 17. yüzyılın başlarında önce Fransa'da sonra

³⁵³ K. Ali Akkemik, "Japonya (1991) Ve Abd (2007-2009) Finans Krizlerinin Politik İktisat Perspektifinden Bir Değerlendirmesi", Doğu Üniversitesi Dergisi, 12 (2) İstanbul 2011, s.173.

³⁵⁴ Berk Bolat, "Dotcom Balonu: Yüksek Değerlemeli Halka Arzlar, Milyon Dolarlık Reklamlar Ve Çöp Olan Hisseler" 22.12.2017, <https://ekonomist.co/yatirim/borsa/dotcom-balonu-12896/>, (Erişim: 22.12.2017)

³⁵⁵ Nishibe, *The Enigma of Money, Gold, Central Banknotes and Bitcoin*, s.63.

Hollanda’da popüler olmaya başladı ve akabinde Amsterdam’da lale soğanı borsası kuruldu ve halka açıldı. Lale soğanı ticaretinin insanlar arasında yaygınlaşması için de Amsterdam’ı Rotterdam ve Leiden şehirleri takip etti ve lale soğanı için sürekli bir pazar oluşturuldu. Lale soğanlarının fiyatı 500 – 700 Hollanda guldeni³⁵⁶ arasında değişiyordu. Hollanda’da lale ticareti kaydi işlem olarak ifade edilmekteydi. Almanya’da 30 yıl savaşları sürerken 1630’lu yılların ortasında lale sadece soylu ailelerin değil çiftçilerin, zanaatkârların ve toplumdan herkesin ilgilendiği bir nesne haline geldi ve bu durum balonun oluşmasına zemin hazırladı. Lale soğanı balonun oluşmasındaki ana sebeplerden birisi sıradan insanların bu ticarete katılması olmuştur. Bu durum geçmişten günümüze kadar bu şekilde devam etmiştir. Japonya’daki ve Amerika Birleşik Devletleri’nde meydana gelen finans balonlarında sadece yatırımcılar ve ticari şirketler değil aynı zamanda sıradan insanlar da önemli miktarda para yatırmışlardır. Günümüz dünyasında kolay yoldan hızlı para elde etmek isteyen yatırımcılar finans balonlarına rağbet etmektedir. Birçok yatırımcı, lale çılgınlığına bu nedenle katılmışlardır. Bunun sonucunda Hollanda’ya akan para, sıradan ürünlerin, atların, mülklerin ve diğer tüm lüks tüketim ürünlerinin fiyatını artmasına sebep olmuştur. Lale soğanı fiyatları öyle artmaya devam etmiştir ki bu durum insanları evlerini teminat göstererek borç para ile lale soğanı almaya teşvik etmiştir. 1636’ya kadar tek bir lale soğanı bir araba ve tüm ekipmanları ile iki at almaya eşdeğerdi. Spekülasyonlarla pik noktasına ulaştıktan sonra 1636 yılında bir grup yatırımcı satış yapmaya başlayınca bu durum daha fazla yatırımcının satışı yapmasına neden olmuştur ve lale soğanı piyasasında bir panik havası meydana gelmiştir. Fiyatlar çok hızlı bir şekilde düşmeye başlamıştır. Evlerini arabalarını satarak lale soğanı çılgınlığına katılan insanlar iflas etmeye başlamıştır. O dönemde ticaretin merkezi olan Hollanda ekonomisi çok sert bir şekilde dibe vurmuştur. Finans balonları tarihte tekrarlanan olaylar olarak karşımıza çıkmaktadır.³⁵⁷ Şu an dünya genelinde lale soğanı çılgınlığı gibi kripto para Bitcoin ile yeni bir finans balonunu tecrübe ediyor olabiliriz. Dünyada küresel çapta yeni bir finansal sisteme geçme aşamasında olduğumuz söylenebilir. Kurulmaya çalışılan bu sistem, kendisini büyütmek için de “lale çılgınlığı” gibi davranış sergileyebilir bu nedenle tarihte yaşanan bu tecrübelerden

³⁵⁶ Hollanda’nın Euro para birimine geçmeden önce kullandığı para birimi

³⁵⁷ Nishibe, *The Enigma of Money, Gold, Central Banknotes and Bitcoin*, s.66.

ders çıkarmamız ve olası bir küresel çapta finansal krizle karşılaşılmması için gerekli tedbirlerin alınması gerekmektedir.

Dünyada en yaygın bilinen ve kullanıma sahip Bitcoin'i bir para birimi olarak değerlendirmek doğru olmayabilir, Bitcoin ona güvenen ve değer veren kullanıcıları tarafından kabul edilen bir ödeme aracı olarak nitelendirilebilir. Bitcoin, altında yatan teknolojinin mevcut finans sistemlerinin yeniden dizayn edilmesi gerekliliğini ortaya çıkaran bir araç olarak düşünülebilir. Bitcoin'in değerinin günden güne artması, dijital ekonomiye geçişte ileride hayatımıza yerleşecek olan kripto paraların toplumda yer bulması, itibar görmesi, güvenilir izlenimi vermesi ve tüm dünyaca benimsenmesi için kurgulanmış bir teori olabilir. Buradaki amaç; halkı, toplumları ve ülkeleri ortak dünya para birimine hazırlamak olarak ifade edilebilmektedir.

Son zamanlarda politik olarak, devlet onayı olsun ya da olmasın egemen bir ülkede mevcut fiziksel para biriminin yerini alması için sanal paraların yaygınlaştırılması gibi durumların yaşandığı belirtilmektedir. Auroracoin, Mart 2014 yılında İzlanda'da hükümet düzenlemelerine tabi olmayan enflasyona karşı daha az duyarlı para birimi sağlayıcısı olarak bilinmeyen bir kaynaktan ortaya çıktığı ifade edilmektedir. Bunun dışında Derek Nisbet, Scotcoin'i yeni bağımsız İskoç para birimi olarak tanıtmıştır. Ekvator, fiziksel para birimine alternatif olarak sanal paraların potansiyel kullanımı ile ilgili araştırmalar yapmaktadır. Şunu da vurgulamak gerekir ki İskoçya ve İzlanda örneklerinde yasal hükümet, sanal paraların kullanımı ve yaygınlaştırılmasını onaylamadığı fakat Ekvador hükümeti sanal paralarla ilgili bu çabaları desteklediği belirtilmektedir. Bir devlet dışı aktörün sanal para birimi yerine daha standart olan kâğıt para birimini seçebilirken, geçekte sanal paralara yönelik algı değişimlerinin sanal paraların daha güvenli, esnek ve ulaşılabilir para birimi olmasından kaynaklandığı ve bu özelliklerin sanal paraların sahiplenilmesini büyük oranda artırabileceği ifade edilmektedir. Özellikle siber anlamda karmaşıklığa sahip olan müttefik ulus devlet tarafından desteklenen devlet dışı aktörün sanal para kullanımını büyük ölçüde etkileyebileceği belirtilmektedir.³⁵⁸

³⁵⁸ Baron, ve diğerleri, "National Security Implications of Virtual Currency Examining the Potential for Non-state Actor Deployment", s.19-21.

Avusturyalı ekonomist Friedrich Hayek 1976 yılında paranın milli unsurlardan çıkarılması için para birimlerinin rekabet etmesine izin vererek para basımının serbestleşmesini öneren “*Paranın Devlet Kontrolünden Çıkarılması*” isimli bir kitap yayınlamıştır. Devletlerin bastığı para ile özel olarak çıkarılan paranın arasındaki rekabetin kötü parayı düşen değeri nedeniyle ortadan kaldıracağını bunun sonucunda da sabit bir değere sahip iyi paranın da gelişeceğini ifade etmiştir. Hayek, devletlerin paralarının sosyal refahı genişleterek enflasyona neden olduğunu ve devletlerin ulusal borçlanmalara neden olduğu bütçe açıklarını kapatmak için savaflara yöneldiğini belirtmiştir. İnternet, P2P ve açık kaynak kodlu yazılımlar gibi bilgi teknolojilerinde meydana gelen gelişmeler para birimlerinin rekabetini mümkün kılarken aynı zamanda kişiye de daha iyi para birimini seçme özgürlüğü tanımaktadır. Bu çerçevede Bitcoin’in devletlerin para birimlerinin neden olduğu ekonomik krizlere tepki olarak yayılma ihtimali söz konusu olabilmektedir.³⁵⁹

Kripto paralar birçokları tarafından sadece bir ödeme aracı veya bir yatırım nesnesi olarak değil aynı zamanda yeni dijital ekonomide bir değişim aracı niteliğinde kripto para birimi ekonomisine girmenin ön koşullarından biri olarak görülmektedir. Bu durumun da ekonomi güvenliğinin yöntem ve araçlarının daha ayrıntılı bir şekilde geliştirilmesi ihtiyacını doğurmaktadır. Kripto paraların geliştirilmesinin altında yatan ve çığır açıcı bir teknoloji olarak nitelendirilen blok zinciri teknolojisi yasa dışı işlemler için bir cazibe ve işlevsellik oluşturmaktadır. Kripto para birimleri ile gerçekleştirilen işlemlerin yasal olarak yasaklanması kripto para kullanımının gölge ekonomide kullanımını teşvik edebileceği için devletlerin ekonomi güvenliği üzerinde negatif sonuçlara yol açabileceği değerlendirilmektedir.

Ekonomi güvenliği bireylerin, hane halkının ve toplulukların gıda, barınma, giyim, korunma ve bakım gibi temel ihtiyaçlarını sürdürülebilir ve onurlu bir şekilde karşılama yeteneği olarak karakterize edilmektedir. Ekonomi güvenliği milletin ve toplum bölgesinin risk yönetimi ve ekonomik strese dayanan sistemin geliştirilmesini içeren temel yaşam standardına sahip olmayı sağlama olarak ifade edilmektedir. Bu kapsamdan bakıldığında kripto paralarla ekonomi arasında yakın ilişki dikkat çekmektedir. Devlet yapıları tarafından kontrol edilemeyen fonların devletlerin

³⁵⁹ Age, s.55.

ekonomi güvenliğinde; devlet bütçe sisteminin bütçe gelirlerini azaltması, kontrol edilemeyen fonların yasal ekonomi dışında kullanılma olasılığı, enflasyonun artması, yasal yatırımcıların ekonomi faaliyetlerinde azalma ve yolsuzluğun artması gibi negatif sonuçlara yol açması muhtemeldir.

Milli ekonominin dijital gelişimi temelde ülkenin ekonomi güvenliğine yeni risk ve tehditler oluşturmaktadır. Son yıllarda ortaya çıkan blok zinciri teknolojisinin her zaman toplum yararına kullanılmadığını söylemek mümkündür. Devrim niteliğindeki bu sistemin de sahip olduğu karanlık tarafları bulunmaktadır. Bu teknoloji herhangi bir finansal aracın bir işlevi olmayan, kripto para işlemleri kullanılarak kazanılan Bitcoin, Ethereum ve Ripple gibi spekülative bir gelir elde etmek için kullanılmasının yanı sıra kripto para birimi işlemlerinde “kişisizleştirme” için de kullanılmaktadır. Bu nedenle ekonomi güvenliği konularının kripto para gerçeği koşullarında güncellendiğini söylemek mümkündür. Kontrolsüz sınır ötesi fon transferlerinin gerçekleştirilmesi ve ardından nakde çevrilme olasılığı kripto para biriminin, suçtan elde edilen gelirlerin yasallaştırılması ve terörün finansmanı gibi hedeflenen şemalara potansiyel dahil olma riskinin yüksek olması için bir ön koşul olarak hizmet etmektedir.³⁶⁰

Kripto paraların bir araç olarak kullanılması durumunu teşkil eden kara para aklama ve terörizm finansmanı gibi ekonomi güvenliğine doğrudan veya dolaylı etkileri bulunan neticesinde milli güvenliğe ise tehdit oluşturan küresel boyutlu çok önemli bir risk oluşturduğu değerlendirilmektedir. Bu durum tüm dünya ülkelerin güvenliğine ve finansal sektörünün istikrarına zarar vermektedir. Ekonomi sisteminin dinamikliği, gelişime bağlı olması ve yeni teknolojik fırsatların kullanımını içermesi ulusal güvenlik kapsamındaki önlemlerin sürekli iyileştirilmesi gerekliliğini ortaya koymaktadır. Ülkelerin; piyasaların, küresel finans sisteminin ve neticesinde devletin bütünlüğünü korumak için kripto para kullanımının neden olduğu bu türdeki finansal istismarların önlenmesine yönelik dünya çapında süratle ortaklaşa gerekli düzenlemeleri yapılması ihtiyacını doğurmaktadır.

³⁶⁰ Khadzhiev Marat Ramzanovich ve Tsakaev Alkhozur Kharonovich, “Economic Security of Russia In The Cryptocurrency Reality Conditions: Problems And Solutions”, International Scientific Conference «Social and Cultural Transformations in the Context of Modern Globalism, eISSN: 2357-1330, 2020.

Kripto para kullanımının yasa dışı ürün ve hizmetlerin satışında kullanılması ve suç faaliyetini ve terörist finansmanını desteklemek için işlemlerin gizlilikle yapılıyor olması suç araştırmacılarının karşı karşıya kaldığı bir konudur. Ancak uluslararası düzenleyici kuruluşlar ve uluslararası hukuk uygulayıcıları bu yeni teknoloji ile ilgili önlem almak zorundadır. Güçlü kara para aklama yükümlülükleri ve güçlü mali düzenleyici sistemler suç ve terör örgütlerinin faaliyetlerini finanse etme veya gelirlerini aklamalarını zora sokacaktır. Sanal dünyaya bu hükümlerin uygulanmaması için bir sebep bulunmamaktadır.



KAYNAKÇA

- Accenture Consulting, *The (R)evolution of Money Blockchain Empowered Digital Currencies*, 2017.
- Akkemik, K. Ali, *Japonya (1991) Ve ABD (2007-2009) Finans Krizlerinin Politik İktisat Perspektifinden Bir Değerlendirmesi*, Doğu Üniversitesi Dergisi, 12 (2), İstanbul 2011.
- Ali, Robleh; Barrdear, John; Clews, Roger ve Southgate, James, *The Economics of Digital Currencies*, Bank of England Quarterly Bulletin, England, 2014.
- An Introduction to Electronic Money Issues Toward Electronic Money and Banking: The Role of Government, Washington DC 1996.
- Aren, Sadun, *100 Soruda Para ve Para Politikası*, İstanbul 1991.
- Armaoğlu Fahir, 20. Yüzyıl Siyasi Tarihi, 18. bs., İstanbul, Alkım Yayınevi, Nisan 2012.
- Armknicht, Frederic; Karame, O. Ghassan; Mandal, Avikarsha; Youssef, Franck ve Zenner, Eric, *Ripple: Overview and Outlook*, 2015.
- Aschmann, MJ; Leenen, L ve Vuuren, JC Jansen van, “The Utilisation of The Deep Web For Military Counter Terrorist Operations”, South African National Defence Force, South Africa
- Atkins, Jordan, “ Crypto Crime Cartel: The end is nigh for Tether”, 15 Ocak 2021, <https://coingeek.com/crypto-crime-cartel-the-end-is-nigh-for-tether/> , (E.T: 19.01.2021).
- Australian Government Australian Transaction Reports and Analysis Center, *Introduction to Money Laundering*, Avustralya 2008.
- Aybar, Rona “Milli Güvenlik Kavramı ve Milli Güvenlik Kurulu”
- Aykın, Hasan, “Jeopolitikten Jeoekonomiye: Ekonomik, Güvenliğin Yükselişi”.
- Baldwin, David A., “The Concept of Security”, Review of International Studies (1997), 23.

Bank Secrecy Act, “Anti-Money Laundering, and Office of Foreign Assets Control”, 1970.

Baqer, Khaled; Huang, Yuxing, Danny ve McCoy, Damon, “Stressing Out: Bitcoin Stress Testing”, Financial Cryptography and Data Security, Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner ve Kurt Rohloff (Ed.), 2016.

Baron, Joshua; O’Mahony, Angela; Manheim, David ve Dion-Schwarz, Cynthia, “National Security Implications of Virtual Currency Examining the Potential for Non-state Actor Deployment”, Rand Corporation, Santa Monica, 2015.

Barski, Conrad ve Wilmer, Chris, *Bitcoin For The Befuddled*, San Francisco 2015.

Bellany, Ian, “Towards a Theory of International Security” Political Studies. (29/1), 1981.

Binance USD, <https://crypto.com/price/binance-usd> , (E.T: 20 Ocak 2021).

Birdiřli, Fikret, “Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri”, Kahramanmarař Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakóltesi, Sosyal Bilimler Enstitüsü Dergisi Sayı: 31 Yıl:2011/2.

Bitcoin and Money Laundering, Developments In Banking Law. Boston University, 2016-2017,

https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjE4MGrwdnYAhVREVAKHScGAtsQFgg_nMAA&url=https%3A%2F%2Fwww.bu.edu%2Frbfl%2Ffiles%2F2017%2F03%2FDA-13.pdf&usg=AOvVaw1cHZOX80URnsw9maXFICtQ (E.T: 05 November 2017).

Bitcoin ATMs by Country, <https://coinatmradar.com/countries> , E.T: 21 Ocak 2021).

Bitcoin Price, www.bitcoin.com, (Eriřim: 01.02.2021).

Bolat, Berk, “Dotcom Balonu: Yüksek Deęerlemeli Halka Arzlar, Milyon Dolarlık Reklamlar Ve Çöp Olan Hisseler”, 22 Aralık 2017, <https://ekonomist.co/yatirim/borsa/dotcom-balonu-12896/>, (E.T: 22 Aralık 2017).

- Bourgi, Sam, “Polish city becomes first to adopt Ethereum blockchain for emergency services”, (27 Kasım 2020), <https://cointelegraph.com/news/polish-city-becomes-first-to-adopt-ethereum-blockchain-for-emergency-services> , (E.T: 20 Ocak 2021).
- Brill, Alan ve Keene, Lonnie, *Cryptocurrencies: The Next Generation of Terrorist Financing?*, New York 2014.
- Brito, Jerry ve Castillo, Andrea, “Bitcoin: A Primer For Policymakers”, George Mason University, Arlington 2013.
- Brown, Benjamin, “Threat Advisory: 2016 State of the Dark Web”, Akamai, Threat Advisory.
- Browne, Ryan, “\$10 billion crypto firm Ripple considers relocating to London over U.S. regulation”, 23 Ekim 2020, <https://www.cnbc.com/2020/10/23/crypto-firm-ripple-considers-relocating-to-london-over-us-regulation.html> , (E.T: 20 Ocak 2021).
- Bunjaku, Flamur; Gjorgieva-Trajkovska, Olivera ve Miteva-Kacarski, Emilija, “Cryptocurrencies – Advantages and Disadvantages”,
- Burks, Christopher, *Bitcoin: Breaking Bad Or Breaking Barriers?* North Carolina Journal Of Law & Technology Vol.18, U.S. 2017.
- Carata, Cristina, *Modern Methods Of Financing Terrorism in A Global and Intercultural Society: Crypto-Currency*, International Conference RCIC’17, Bari 2017.
- Chainalysis, “The 2020 Geography of Cryptocurrency Report, Analysis of Geographic Trend in Cryptocurrency Adoption, Usage, and Regulation”, September 2020, (E.T: 21 Ocak 2021).
- Chapkanovska, Evangelina, “Bitcoin Regulation: Where is Bitcoin Legal in 2020?” (30 Kasım 2020), <https://spendmenot.com/blog/bitcoin-regulation/> (E.T: 31 Aralık 2020).
- Cheng, Jonathan, “China Envisions Its Digital-Currency Future, With Lotteries and a Year’s Worth of Laundry”, 27 Aralık 2020,

- <https://www.wsj.com/articles/china-envisions-its-digital-currency-future-with-lotteries-and-a-years-worth-of-laundry-11609066819> , (E.T: 29 Aralık 2020).
- China Coin No More: Bitcoin Mining Shifting to Sweden and Norway, 27.12.2020, <https://u.today/china-coin-no-more-bitcoin-mining-shifting-to-sweden-and-norway> (E.T: 28 Aralık 2020)
- Committee on Payments and Market Infrastructures, “Digital currencies”, November 2015, <https://www.bis.org/cpmi/publ/d137.pdf> , (E.T: 05 Ağustos 2019).
- Congressional Research Service, “Dark Web”, Mart 2017. <https://fas.org/sgp/crs/misc/R44101.pdf> , (Erişim: 10 Kasım 2019).
- Consulting Technology Outsourcing, “The Growing Threat of Money Laundering”,
- Cooper, Richard, *A Monetary System for the Future*, Foreign Affairs, U.S. 1984, 63 (1).
- Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018”, <https://powercompare.co.uk/bitcoin-mining-electricity-map/> (E.T: 29 Aralık 2020).
- Crime and Misconduct Commission, “Background Intelligence Brief, Money Laundering”
- Cryptocurrencies: Potential For Terror Financing?, Ahmad Helmi Hasbi and Remy Mahzam.
- Cryptocurrency Market Capitalization, <https://coinmarketcap.com/>, (E.T: 15 January 2018).
- Çalışır, Mustafa ve Şanver, Cahit “Kripto Paralar ve Para & Maliye Politikalarına Muhtemel Yansımaları”, IBANESS Conference Series, Tekirdağ, 2018.
- Çelik, Kayahan, Kara Para Aklama Suçuyla Ulusal Ve Uluslararası Düzeyde Mücadele Ve Türkiye Örneği, Atatürk Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisan Tezi, Erzurum 2011.
- Çelikpala, Mitat “Geçmişten Günümüze Vazgeçilmeyen Kavram: Ulusal Çıkar”, H.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi, Cilt 23, Sayı 1, 2005.

- Çomaklı, Şafak Ertan ve Uzun, Murat, “Hawala Method in Terrorism Financing and Money Laundering”, *International Congress On Political, Economic and Social Studies*, Pesa Publications, 2018.
- Dedeoğlu, Beril, “Uluslararası Güvenlik ve Strateji”, *Yeniyüzyıl Yayınları*, İstanbul 2008.
- Demir, Sertif, “Avrupa Güvenlik Mimarisinin Tarihsel Gelişimi ve Türkiye’nin Bu Güvenlik Mimarisindeki Yeri”, *Güvenlik Stratejileri Dergisi*. (S. 9), 2009.
- Department of Finance, “Virtual Currencies and Blockchain Technology”, Dublin, March 2018.
- Digital Currencies vs. Cryptocurrencies, Explained, 13.12.2017, <https://cointelegraph.com/explained/digital-currencies-vs-cryptocurrencies-explained> (E.T: 05 Ağustos 2019).
- Dimers, Daniel; Arslanian, Henri; McNamara, Grainne; Dobrauz, Günther ve Wohlgemuth, Lukas, “Initial Coin Offerings A Strategic Perspective”, pwc, June 2018.
- Dion-Schwarz, Cynthia; Manheim, David ve Johnston, B. Patrick, “Terrorist Use Of Cryptocurrencies: Technical and Organizational Barriers and Future Threats”, *RAND Coporation*, Santa Monica 2019.
- Double Spending Explained, <https://academy.binance.com/en/articles/double-spending-explained> , (E.T:15.02.2021).
- Dunleavy Jerry, “Trump spy chief seeks SEC scrutiny of Chinese dominance in cryptocurrency”, 24 Kasım 2020 <https://www.washingtonexaminer.com/news/trump-spy-chief-seeks-sec-scrutiny-of-chinese-dominance-in-cryptocurrency>, (E.T: 28 Aralık 2020).
- Dyntu, Valeria ve Dykyi, Oleh, “Cryptocurrency In The System of Money Laundering”, *Baltic Journal of Economic Studies*, Vol. 4, No. 5, 2018.
- Eğilmez, Mahfi, *Örneklerle Kolay Ekonomi*, İstanbul 2014.
- Eğilmez, Mahfi, *Makroekonomik Denge*, İstanbul 2009.

- Ergüven, Nasih Sarp, “Uluslararası Hukuk Açısından Güvenlik Kavramının Teorik Temelleri”, Ankara Üniversitesi Hukuk Fakültesi Doktora Tezi, 2016.
- Erkış, İbrahim Uğur, *Ulus Devletin Tarihsel Gelişimi*, İİBF Sosyal ve Ekonomik Araştırmalar Dergisi, Yıl:13, Sayı:26, Konya 2013.
- Eskicioğlu, Osman, *İslam ve Ekonomi*, İzmir 1999.
- ESMA, EBA & EIOPA, “Warning on the risks of Virtual Currencies https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf”, (E.T: 05 Ağustos 2019).
- Ethereum Nedir?, 10 Ekim 2017, <http://blockchain.org.tr/ethereum-nedir/>, (E.T: 15 Aralık 2017).
- European Banking Authority, *Designing a Regulatory and Supervisory Roadmap for FinTech*, Mart 2018.
- European Central Bank, *Virtual Currency Schemes*, 2012.
- European Parliament, *Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion*, 2018.
- European Parliament, *Offshore Activities And Money Laundering: Recent Findings and Challenges*, Brussels 2017.
- European Parliament, *Virtual Currencies and Terrorist Financing: Assessing The Risks and Evaluating Responses*, Mayıs 2018.
- European Parliament, *Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead*, Temmuz 2018.
- Fanusie, Yaya, J., “Cryptocurrency Laundering Is a National Security Risk”, 27 Mart 2020, <https://www.lawfareblog.com/cryptocurrency-laundering-national-security-risk>, (E.T: 02 Ocak 2021).
- Fidan, Hakan, *Intelligence and Foreign Policy: A Comparison Of British, American and Turkish Intelligence Systems*, Yüksek Lisans Tezi, 1999.
- Financial Action Task Force (FATF), *Guidance For a Guidance For a Risk-Based Approach to Virtual Currencies*, 2015.

Financial Action Task Force (FATF), *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation – The FATF Recommendations*, 2017.

Financial Action Task Force (FATF), *Report on Emerging Terrorist Financing Risks*, October 2015.

Financial Action Task Force (FATF), *Virtual Currency Key Definition and Potential AML/CFT Risks*, 2014.

Foley, Sean; Karlsen, R. Jonathan ve Putmins, J. Talis, “Sex, Drugs, and Bitcoin:., How Much Illegal Activity is Financed Through Cryptocurrencies?”, Sydney 2018.

Frankenfield, Ake, “Verge XVG (Cryptocurrency)”, 05 Ocak 2020, <https://www.investopedia.com/terms/v/verge-xvg-cryptocurrency.asp> (E.T:19 Ocak 2021).

Frankenfield, Ake, “Tether (USDT)”, 25 Haziran 2019, <https://www.investopedia.com/terms/t/tether-usdt.asp#:~:text=Tether%20is%20a%20blockchain%2Dbased,trade%20under%20the%20USDT%20symbol> , (E.T: 19 Ocak 2021).

Greenberg, Andy, “FBI Says It's Seized \$28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road” www.forbes.com, 25 October 2013, (E.T: 05 November 2017).

Grigoreva Ekaterina ve Garifova Liliya, “The economic security of the state: the institutional aspect”, *Procedia Economics and Finance* 24, July 2015, Russia.

Hakkımızda, <https://www.btcturk.com/btcturk/hakkimizda> (Erişim: 21.01.2021).

Halaburda, Hanna ve Sarvary, Miklos, *Beyond Bitcoin The Economics of Digital Currencies*, New York 2016.

Hardy, Augustus, Robert ve Norgaard, R. Julia, “Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web, *Journal of Institutional Economics*, 2015.

Harm, Julianne; Obregon, Josh ve Stubbendick, John, *Ethereum vs. Bitcoin*, California.

Hazine ve Maliye Bakanlığı, *Yeni Ekonomi Programı Dengeleme-Disiplin-Değişim 2019-2021*, Eylül 2018, <https://ms.hmb.gov.tr/uploads/2018/10/yeni-ekonomi-programi.pdf> , (E.T: 20 Ocak 2021).

Hileman, Garrick ve Rauchs Michel, *Global Cryptocurrency Benchmarking Study*, University of Cambridge, Cambridge 2017.

History of Anti-Money Laundering Laws, <https://www.fincen.gov/history-anti-money-laundering-laws> (E.T: 01 Ocak 2018).

Howell, T Sabrina; Niessner, Marina ve Yermack, David, “Financing Growth with Cryptocurrency Token Sales”, Finance Working Paper N° 564/2018, U.S. 2018.

IntelBrief: Terrorists’ Use of Cryptocurrency, 10 Aralık 2020, <https://thesoufancenter.org/intelbrief-2020-december-10/> , (E.T: 29 Aralık 2020).

International Monetary Fund (IMF), *IMF Workin Paper: Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*, November 2020.

International Monetary Fund, *The IMF and the Fight Against Money Laundering and the Financing of Terrorism*, Factsheet, Washington 2017.

International Monetary Fund (IMF), *Virtual Currencies and Beyond: Initial Considerations*, January 2016.

İskenderoğlu, Lerzan, *Uluslararası Para Sisteminin Sorunları ve İyileştirme Çalışmaları*, Türkiye Cumhuriyet Merkez Bankası Araştırma Planlama ve Eğitim Genel Müdürlüğü, Tartışma Tebliği No: 8807, Ankara 1998.

“İş Bankası R3 Blockchain Birliği’ne katılan ilk Türk bankası oldu”, 29 Nisan 2020, <https://www.isbank.com.tr/bankamizi-taniyin/is-bankasi-r3-blockchain-birligine-katilan-ilk-turk-bankasi-oldu> , (E.T: 19 Ocak 2021).

“İş Bankası, blockchain teknolojisiyle dış ticarete ödeme garantisi veren ilk Türk Bankası oldu”, 03 Haziran 2020, <https://www.isbank.com.tr/bankamizi-taniyin/is-bankasi-blockchain-teknolojisiyle-dis-ticarete-odeme-garantisi-veren-ilk-turk-bankasi-oldu> , (E.T: 19 Ocak 2021).

- Jost, M. Patrick ve Sandhu, Singh, Harjit, “The Hawala Alternative Remittance System and its Role in Money Laundering”, Financial Crimes Enforcement Network Report, U.S..
- Jović Zoran; Kunjadic, Goran, “Economic, Security And Information Aspects Of The Application Of Cryptocurrency And Their Impact On The South East European Countries”, December 2018.
- Kamnar-Popovska, Neda, The Use Of Electronic Money And Its Impact On Monetary Policy, JCEBI, Vol. 1, No. 2, 2014.
- Karakaya, Oğuzhan, “Cloud Mining Nedir? Bulut Madenciliği Nasıl Yapılır?”, 28 Şubat 2017, <https://oguzhankarakaya.com/cloud-mining-nedir-bulut-madenciligi>, (E.T: 15 Aralık 2017).
- Karishnan, Hari; Saketh, Sai ve Vaibhav, Venkata Tej, *Cryptocurrency Mining – Transition to Cloud*, International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, India 2015.
- Keleş, Ali, *İslam’a Göre Para Kavramı*, Doktora Tezi, Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Bursa 1998.
- Klennan, John, *When Were Credit Cards Invented? A Complete History*, 2015.
- Kocaaslan, Nihat Emre, “Türkiye’deki En İyi 6 Bitcoin Borsası”, 28.Kasım 2020, <https://beincrypto.com.tr/ogren/turkiyedeki-en-iyi-5-bitcoin-borsasi/>, (E.T: 30 Aralık 2020).
- Köing Susanne, “The Evolution of Money From Commodity Money to E-Money”, UNICERT IV Program, 6 Haziran 2001.
- Krakov, Mesjasz, “Ekonomik Güvenlik”, Uluslararası İlişkiler, Cilt 5, Sayı 18 (2008).
- Kumar, Krishna, “Functioning of anti money laundering legislation in India a critical study”, Tamil Nadu Dr. Ambedkar Law University Doktora Tezi, 2015, https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0ahUKEwiPp9zIo9DYAhVkYZoKHV_nBUUQFghSMAU&url=http%3A%2F%2Fshodhganga.inflibnet.ac.in%2Fbitstream%2F10

[603%2F76711%2F7%2F07_chapter%25201.pdf&usg=AOvVaw0SIC6fUan454RKXEdeujyV](#) (E.T: 05.01.2018).

Lee, David ve Chuen, Kuo, *Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments and Big Data*, U.S. 2015.

Lee, Seunghyeon; Yoon, Changhoon; Kang, Heedo; Kim, Yeonkeun; Kim, Yongdae; Han, Dongsu; Son, Sooel ve Shin; Seungwon, “Cybercriminal Minds: An Investigative Study of Cryptocurrency Abuses in The Dark Web”, Network and Distributed Systems Security (NDSS) Symposium 2019, San Diego 2019.

Limba T.; Driaunys K.; Stankevicius A.; Andrulevicius A., “Cryptocurrency and National Security: Peculiarities of Interaction”, *Transformations in Business & Economics*, Vol. 19, No 2 (50), 2020.

Limer, Eric, “The World’s Most Powerful Computer Network Is Being Wasted on Bitcoin”, 13 May 2013, <https://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-504503726>, (E.T: 15 Aralık 2017).

Lindeberg, Rafaela ve Ummelas, Ott, “Sweden Explores Moving to a Digital Currency”, 11 Aralık 2020, <https://www.bloomberg.com/news/articles/2020-12-11/sweden-explores-the-feasibility-of-moving-to-a-digital-currency> , (E.T: 20 Ocak 2021).

Luciani, Giacomo, “The Economic Content Of Security”, *Journal of Public Policy*, (S.8). 1989.

M, Laura, “ Kapsamlı Jaxx vs Exodus İncelemesi”, 11 Eylül 2020, <https://tr.bitdegree.org/crypto/tutorial/jaxx-vs-exodus> (E.T: 01 Ocak 2021).

Mabunda, Sagwadi, “Cryptocurrency: The New Face of Cyber Money Laundering”, *2018 International Conference on Advances in Big Data, Computing and Data Communication*, Durban, South Africa 2018.

Manjee, Tera, “Bitcoin, its Legal Classification and its Regulatory Framework”, *Journal of Business & Securities Law*, Vol. 15, Issue, 2015.

Marian, Omri, *Are Cryptocurrencies Super Tax Havens?*. *Law Review First Impressions*, Vol. 112:38, Michigan 2013.

Market Cap, www.bitcoin.com, (Eriřim: 01.02.2021).

MASAK, “Aklama Yöntemleri”, <http://www.masak.gov.tr/tr/content/aklama-yontemleri/59> (E.T: 30 Aralık 2017).

Menezes, A., Oorschot P. Van, ve Vanstone S., *Handbook of Applied Cryptography*, Overview of Cryptography, 1996.

Merkez Bankası Başkanı Ağbal’dankripto para açıklaması1, 25 Aralık 2020, <https://www.cnnturk.com/ekonomi/son-dakika-merkez-bankasi-baskani-agbal-enflasyon-hedefini-acikladi> , (E.T: 20 Ocak 2021).

Meyer, David, “Google Ventures Invests In Opencoin, The Firm Behind Bitcoin Exchange Ripple”, 14 May 2013, <https://gigaom.com/2013/05/14/google-ventures-invests-in-opencoin-the-firm-behind-Bitcoin-exchange-ripple/>, (E.T: 15 Aralık 2017).

Moeller, Max, “Turkey’s Regulatory Board CMB Moves Against Bitcoin”, 07 Ocak 2020, <https://beincrypto.com/turkeys-regulatory-board-cmb-moves-against-bitcoin/> , (E.T: 20 Ocak 2021).

Money Supply, www.bitcoin.com, (Eriřim: 01.02.2021).

Most traded National Currencies for Bitcoin, <https://www.coinhills.com/market/currency/> , (E.T: 21 Ocak 2021).

Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

Nedelcu, Constantin, “Money Laundering Techniques Commonly Used. General Approaches”, Bucharest.

Nishibe, Makoto, *The Enigma of Money Gold*, Central Banknotes and Bitcoin, Japan 2016.

OECD, *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*, 2009.

Oğuzlu, H. Tarık, “Dünya Düzenleri ve Güvenlik”: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu? Güvenlik Stratejileri Dergisi. (S.6), 2007.

Osborne, Charlie, “UK ban on cryptocurrency derivatives, ETNs comes into force today”, 06 Ocak 2021, <https://www.zdnet.com/article/uk-ban-on->

cryptocurrency-derivatives-comes-into-force-
today/#:~:text=The%20ban%20has%20now%20become,crypto%20assets%20to%20retail%20consumers.%22&text=The%20value%20of%20these%20products,%20or%20Ethereum%20(ETH) , (E.T: 20 Ocak 2021).

Otieno, Nicholas, “U.S. Financial Regulators Warn Crypto Firms to Tighten Stablecoin AML Risk Controls”, 21 Kasım 2020, <https://blockchain.news/news/u.s.-financial-regulators-warn-crypto-companies-on-stablecoins-risks> (E.T: 28 Aralık 2020).

Özçoban, Cuma “21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü”, Harp Akademileri Stratejik Araştırmalar Enstitüsü Yüksek Lisans Tezi, İstanbul 2014.

Özdemir, Doğaç, “Bretton Woods Düzeni (1944-71)”, 15.08.2015, <http://www.gazetebilkent.com/2015/08/15/bretton-woods-duzeni-1944-71/> (E.T: 25 Aralık 2017).

Paribu Nedir?, <https://destek.paribu.com/hc/tr/articles/115005841469-Paribu-Nedir-> , (E.T:21 Ocak 2021).

Peer to peer nedir?, www.paribu.com, (E.T: 15.02.2021).

Petre, Marius, Economic Security, Organic Dimension of National Security, MPRA Paper No. 17936, 18 Oct 2009.

Quantum Computers Pose Imminent Threat to Bitcoin Security, 08 November 201, <http://www.comp.nus.edu.sg/news/news-media/2176-2017-quantum-computers/>, (E.T: 15 Aralık.2017).

Ramzanovich, Khadzhiev Marat ve Kharonovich, Tsakaev Alkhozur, “Economic Security of Russia In The Cryptocurrency Reality Conditions: Problems And Solutions”, International Scientific Conference «Social and Cultural Transformations in the Context of Modern Globalism, eISSN: 2357-1330, 2020.

Rankl, Wolfgang ve Effing, Wolfgang, Giesecke & Devrient GmbH, *Smart Card Handbook*, Germany 2010.

Regulation of Cryptocurrency Around the World, Egypt,
<https://www.loc.gov/law/help/cryptocurrency/world-survey> (E.T:15.02.2021).

Resmi Gazete, *On Birinci Kalkınma Planı (2019-2023)*, (23 Temmuz 2019),
<https://www.resmigazete.gov.tr/eskiler/2019/07/20190723M1-1-1.pdf> , Karar
No: 12252020 *Yılı Cumhurbaşkanlığı Yıllık Programı'nın Uygulanmasına*
Dair Karar, (04 Kasım 2019),
<https://www.resmigazete.gov.tr/eskiler/2019/11/20191104M1-1.pdf> , Karar
No: 1733, (E.T: 31 Aralık 2020).

Retter Lucia; Frinking, Erik J.; Hoorens, Stijn; Lynch, Alice; Nederveen Fook;
Phillips, William D., “Relationships between the economy and national
security Analysis and considerations for economic security policy in the
Netherlands”, RAND Corporation”, 2020.

Revoredo, Tatiana, “A comparative analysis between money, currency, digital money,
fiat money, electronic money and cryptocurrencies” 15 Eylül 2018,
[https://medium.com/@tatianarevored/a-comparative-analysis-between-](https://medium.com/@tatianarevored/a-comparative-analysis-between-money-currency-digital-money-fiat-money-electronic-money-and-36bbcfacea9b)
[money-currency-digital-money-fiat-money-electronic-money-and-](https://medium.com/@tatianarevored/a-comparative-analysis-between-money-currency-digital-money-fiat-money-electronic-money-and-36bbcfacea9b)
36bbcfacea9b (Erişim: 30 Ekim 2018).

Roberts, Jeff John, “Ripple says it will be sued by the SEC, in what the company calls
a parting shot at the crypto industry”, 22 Aralık 2020,
<https://fortune.com/2020/12/21/ripple-to-be-sued-by-sec-cryptocurrency-xrp/>
(E.T: 27 Aralık 2020).

Ronis, Sheila R., *Economic Security Neglected Dimension of National Security?*,
Center for Strategic Conferencing Institute for National Strategic Studies by
National Defense University Press Washington, D.C., 2011.

Ryan, *İnternetin Geçmişi ve Dijital Gelecek*, (Çev. Birsen Keleş), TÜBİTAK Popüler
Bilim Kitapları, Ankara 2019.

S., Aaron “Verge Cryptocurrency: What is Verge Coin?” 04 Ocak 2021,
<https://www.bitdegree.org/crypto/verge-coin> , (E.T: 19 Ocak 2021).

Sahoo, Pradipta Kumar, “Bitcoin as digital money: Its growth and future
sustainability”, Vol. XXIV, No. 4(613), India 2017.

- Sanal Para Bitcoin’le Uyuşturucu Siparişi Verdiler, 12 Kasım 2017, <http://www.haberturk.com/Bitcoinle-uyusturucu-siparisi-verdiler-1710096>, (E.T: 17 Aralık 2017).
- Sancak, Kadir, “Güvenlik Kavramı Etrafındaki Tartışmalar Ve Uluslararası Güvenliğin Dönüşümü, Sosyal Bilimler Dergisi.
- Sander, Oral Siyasi Tarih: 1918-1994, 24. bs., Ankara, İmge Kitabevi, Ekim 2014.
- Serin, Vildan, *Para Politikası (Tarihi – Teorik Gelişmeler ve Türkiye Uygulaması)*, Marmara Üniversitesi Yayın No:440, Hukuk Fakültesi Yayın No:4, İstanbul 1987.
- Sermaye Piyasası Kurulu Bülteni, 27 Eylül 2018, <https://spk.gov.tr/Bulten/Goster?year=2018&no=42> , s.4. (E.T: 20 Ocak 2021).
- Simanaviciene, Zaneta, “Economic Security and National Competitiveness”, Public Security and Public Orde 2015 (15).
- SPK’dan Bitcoin Açıklaması, 01 Aralık 2017, <https://uzmanpara.milliyet.com.tr/haber-detay/gundem2/spkdan-bitcoin-aciklamasi/76000/76545/> , (E.T: 20 Ocak 2021).
- Sterry, David R., *Introduction to Bitcoin Mining, A Guide Gamers, Geeks, and Everyone Else*, 2012
- Sui, Daniel; Caverlee, James ve Rudesill, Dakota, “The Deep Web And The Darknet: A Look Inside the Internet’s Massive Black Box”, *Wilson Center*, Washington DC 2015.
- Sundararajan, Sujha, “ECB President: Bitcoin Not 'Mature' Enough to Be Regulated”, 20 October 2017, <https://www.coindesk.com/ecb-president-Bitcoin-not-mature-enough-to-be-regulated/>, (E.T: 15 Aralık 2017).
- Şahin, Eser, “Borsa İstanbul, BISTcoin Adında Kendi Kripto Para Birimi Üzerinde Çalıştıklarını Duyurdu!”, 14 Aralık 2017, <http://www.webtekno.com/bistcoin-nedir-h37894.html>, (E.T: 17 Aralık 2017).
- Şengöz, Murat Türkiye Cumhuriyeti’nin Ulusal Güvenlik Paradigması Üzerine Bir Değerlendirme, Takvim-i Vekayi ISSN: 2148-0087, 2020.

Tar, Andrew, “Digital Currencies vs. Cryptocurrencies, Explained”, (13.12.2017), <https://cointelegraph.com/explained/digital-currencies-vs-cryptocurrencies-explained> (E.T: 05 Ağustos 2019).

Terörün Finans Kaynakları, <http://www.masak.gov.tr/tr/content/terorun-finans-kaynaklari/72>, (E.T: 15 Aralık 2017).

“The Nature of Money Laundering Activities”, Money Laundering Activities: *Explaining the Nature and Emerging Trends*, s.17-18, <https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjB8rnY6NDYAhUCdCwKHRTkCdUQFgg-oMAA&url=https%3A%2F%2Frepub.eur.nl%2Fpub%2F37747%2FD-%2520Chapter%25201-%2520Money%2520Laundering%2520Activities.pdf&usg=AOvVaw1VNeD9WcHisRB2dBPlkdT2> (E.T: 05 Ocak 2018).

The World Bank, Paul Allan Schott, “Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism”, Washington 2006.

Thornton, Grant, “Digital, Virtual And Crypto Currencies: Issues and Accounting Risks”, 2016.

Timothy, C. May, “*Kripto Anarşist Manifesto*”, 22 November 1992, <https://www.activism.net/cypherpunk/crypto-anarchy.html>, (E.T: 15 Aralık 2017).

Top Cryptocurrency Spot Exchanges, <https://coinmarketcap.com/tr/rankings/exchanges/> (Erişim:28.01.2021).

Trappe, Wade ve Washington, Lawrence C.. *Introduction to Cryptography with Coding Theory*, Overview of Cryptography and Its Applications, U.S. 2006.

Tsukerman, Misha, *The Block Is Hot: A Survey Of The State Of Bitcoin Regulation And Suggestions For The Future*, Berkeley Technology Law Journal, Vol. 30:385.

Tunç Hasan ve Döner, Ayhan “MGK ve Milli Güvenlik Kavramı”

- Turban, Efraim ve McElroy, Debbie, *Using Smart Cards in Electronic Commerce*, California 1998.
- Turpin, Jonathan B., *Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework*, Indiana Journal of Global Legal Studies Vol. 21 #1.
- Türk Bitcoin Borsaları, <https://coin-turk.com/piyasalar> (Erişim:28.01.2021).
- Türkiye Cumhuriyet Merkez Bankası, *Kâğıt Paranın Tarihçesi*.
- Türkiye Cumhuriyeti Ticaret Bakanlığı Resmi Twitter Sayfası.
- Türkiye'de kripto para günlük işlem hacmi 1 milyar Doları aştı, 4 Ocak 2021, <https://www.bloomberght.com/turkiye-de-kripto-para-gunluk-islem-hacmi-1-milyar-Dolari-asti-2271922> (E.T:21 Ocak 2021).
- Ulaştırma ve Altyapı Bakanlığı, *Ulusal Siber Güvenlik ve Stratejisi Eylem Planı 2020-2023*, 2020.
- UNICEF Türkiye, Paribu üzerinden Türkiye’de ilk kez kripto parayla bağış kabulüne başladı, <https://www.paribu.com/blog/haberler/unicef-turkiye-paribu-uzerinden-turkiyede-ilk-kez-kripto-parayla-bagis-kabulune-basladi/> (E.T: 21Ocak 2021).
- UNODC, Article 6: “Criminalization of the Laundering Of Proceeds Of Crime”, UN Convention Against Transnational Organized Crime, Vienna 2000.
- USD Coin (USDC), <https://cryptonews.com/coins/usd-coin/> , (E.T: 20 Ocak 2021).
- Usta, Ahmet ve Doğantekin, Serkan, *Blockchain 101*, İstanbul 2017.
- Üstün, Oktay, “Kara para Aklama ve Terörün Finansmanı ile Mücadelede Uluslararası Girişimler ve Araçlara Toplu Bakış”, *Bankacılar Dergisi*, Sayı 65, 2008.
- Üstünel, B.; Ekonominin Temelleri, Ankara 1975.
- Vigna, Paul ve Casey, J. Michael, *Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması; Kriptopara Çağı*, (Çev. Ali Atav), Buzdağı Yayınları, Ankara 2017.
- Virtual Currencies Mining the Possibilities, Allen&Overy, 2015.

- Vorobyev A. V., “ICO as Economic Security Threat. Possible Risks Analysis. Experience of Foreign States” in III Network AML/CFT Institute International Scientific and Research Conference “FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies”, KnE Social Sciences, pages 208–214. DOI 10.18502/kss.v3i2.1544, 2018.
- Vovchenko, Natalia G.; Tishchenko, Evgeniy N.; Epifanova, Tatiana V.; Gontmacher, Mark B., “Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them”, European Research Studies Volume XX, Issue 1, 2017.
- Wadsworth, Amber, “What Is Digital Currency”, *Reserve Bank*, Vol. 81, No.3, 2018.
- Weinmann, Gabriel, “Terrorist Migration to the Dark Web, Perspectives on Terrorism”, Vol. 10, Issue 3.
- What is Binance USD (BUSD)?, <https://www.paxos.com/busd/> , (Erişim:20.01.2021).
- What is Blockchain Technology? A Step-by-Step Guide For Beginners, 15.11.2017, <https://blockgeeks.com/guides/what-is-blockchain-technology/>, (E.T: 15 Aralık 2017).
- What is Ethereum 2.0? Overview, Features and Price Implications, 27 Kasım 2020, <https://www.diginex.com/insights/what-is-ethereum-2-0-overview-features-and-price-implications/> , (E.T:19 Ocak 2021).
- Wisniewska, Anna, “Bitcoin As An Example of Virtual Currency”, Institute of Economic Research Working Papers, Poland 2016.
- World Bank Group, *Distributed Ledger Technology (DLT) and Blockchain*, Fin Tech note, S. 1., Washington D.C. 2017
- Yablon, Benjamin, “Why London Is Becoming a Global Blockchain Hub”, 28 Ağustos 2018, <https://www.entrepreneur.com/article/318570> , (E.T:19 Ocak 2021).
- Yılmaz, Sait, “21. Yüzyılda Güvenlik ve İstihbarat”, Milenyum Yayınları, İstanbul, 2007.
- Zeytinoğlu, E.; Ekonomik Sistemler, M.Ü. Yayını, No: 429, İstanbul 1985.

Zug, “SEBA adds Bitcoin Cash and USD Coin to its Digital Ecosystem”, 19 Kasım 2020, <https://www.seba.swiss/media-and-investors/bitcoin-cash-and-usd-coin-added-to-digital-ecosystem/> , (E.T: 20 Ocak 2021).

6 Ways To Guarantee Anonymity When Making Bitcoin Transactions, 16 Temmuz 2019, <https://coinsutra.com/anonymous-Bitcoin-transactions/>, (E.T: 20 Temmuz 2019).

6493 Sayılı Kanun: Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun





