BLOK ZİNCİR TEKNOLOJİSİ BAĞLAMINDA KRİPTO PARALARIN SINIRAŞAN SUÇLAR VE TERÖRİZMİN FİNANSMANINDA KULLANIMI

Orhan KEMİKSİZ

Küreselleşme ve Uluslararası İlişkiler Anabilim Dalı

Danışman: Prof. Dr. Ensar NİŞANCI

2020

T.C.
TEKİRDAĞ NAMIK KEMAL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KÜRESELLEŞME VE ULUSLARARASI İLİŞKİLER
ANABİLİM DALI

BLOK ZİNCİR TEKNOLOJİSİ BAĞLAMINDA KRİPTO PARALARIN SINIRAŞAN SUÇLAR VE TERÖRİZMİN FİNANSMANINDA KULLANIMI

Orhan KEMİKSİZ

KÜRESELLEŞME VE ULUSLARARASI İLİŞKİLER
ANABİLİM DALI

Danışman: Prof. Dr. Ensar NİŞANCI

Tekirdağ – 2020

BİLİMSEL ETİK BİLDİRİMİ

Hazırladığım Yüksek Lisans Tezinin bütün aşamalarında bilimsel etiğe ve akademik kurallara riayet ettiğimi, çalışmada doğrudan veya dolaylı olarak kullandığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, yazımda enstitü yazım kılavuzuna uygun davranıldığını taahhüt ederim.

Orhan KEMİKSİZ

01.09.2020

T.C.
TEKİRDAĞ NAMIK KEMAL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KÜRESELLEŞME VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

Orhan KEMİKSİZ tarafından hazırlanan "Blok Zincir Teknolojisi Bağlamında Kripto Paraların Sınıraşan Suçlar ve Terörizmin Finansmanında Kullanımı" konulu YÜKSEK LİSANS Tezinin Sınavı, Tekirdağ Namık Kemal Üniversitesi Lisansüstü Eğitim Öğretim Yönetmeliği uyarınca 01.09.2020 günü saat 12:00'da yapılmış olup, tezin ……. OYBİRLİĞİ / OYÇOKLUĞU ile karar verilmiştir.

Jüri Başkanı:		Kanaat:	İmza:
Üye:		Kanaat:	İmza:
Üye:		Kanaat:	İmza:

Sosyal Bilimler Enstitüsü Yönetim Kurulu adına
...../...../20.....
Dr. Öğr. Üyesi Ali Faruk AÇIKGÖZ
Enstitü Müdür V.

ÖZET

Kurum, Enstitü : Tekirdağ Namık Kemal Üniversitesi, Sosyal Bilimler Enstitüsü
ABD : Küreselleşme ve Uluslararası İlişkiler Anabilim Dalı
Tez Başlığı : Blok Zincir Teknolojisi Bağlamında Kripto Paraların Sınıraşan Suçlar ve Terörizmin Finansmanında Kullanımı
Tez Yazarı : Orhan KEMİKSİZ
Tez Danışmanı : Prof. Dr. Ensar NİŞANCI
Tez Türü, Yılı : Yüksek Lisans Tezi, 2020
Sayfa Sayısı : 148

Teknolojik gelişmelerin insanı ve dahil olduğu her süreci yeniden şekillendirdiği günümüzde, kimi yenilikler görece daha büyük kapasiteli etkiler barındırmaktadır. Çağımızda eğitimden sağlığa, hukuktan güvenliğe, ekonomiden sosyal hayata, kişiler ve uluslararası ilişkiler düzleminde iddialı bir teknolojik yenilik adından sıkça söz ettirmeye başlamıştır. Blockchain. Bu çalışma, çok yönlü bir paradigma değişimini bünyesinde barındıran Blok zincir teknolojisini ve onun en popüler çıktılarından biri olan kripto kara kavramının sınıraşan suçlar nezdinde anlamlandırılmasını ve özellikle de siber suçlar, kara paranın aklanması ve terörün finansmanına konu olması bağlamında literatüre katkı sağlamak amacıyla hazırlanmıştır. Yapılan çalışma neticesinde her ne kadar kimi kripto paraların bu suçlara konu ve kayak teşkil ettiği görülse de global ölçekte bu paraların söz konusu suçlarda araçsal rolünün son derece kısıtlı olduğu görülmüştür. Bununla birlikte gelişmiş ülkelerin merkezi otoriteleri tarafından bu teknolojik yenilik bir tehdit olarak algılanırken bazı gelişmemiş ve gelişmekte olan ülkeler açısından küresel eşitsiz koşullarının aşılması bağlamında yeni bir sosyal ve iktisadi fırsat olarak görülmektedir.

Anahtar Kelimeler: Blok Zincir, Kripto Para, Sınıraşan Suçlar, Terörizm, Terörizmin Finansmanı, Siber Suçlar, Bitcoin, Karapara Aklama

ABSTRACT

Institution, Institute : Tekirdağ Namık Kemal University, Institute Of Social Sciences
Department : Globalization And International Relations
Thesis Title : Crypto Coins In The Context Of Blockchain Technology, Its Use Of In Terrorism Financing And Transnational Crimes
Thesis Author : Orhan KEMİKSİZ
Thesis Adviser : Prof. Dr. Ensar NİŞANCI
Type of Thesis, Year : MA Thesis, 2020
Number of Pages : 148

In today's world, where technological developments are reshaping people and every process they are involved in, some innovations have relatively larger capacity impacts. Education, health, law, security, economy, social life in our age; started talking about the name of an ambitious technological innovation at the level of people and international relations. The Blockchain. This study has been prepared to contribute to the literature in terms of the meaning of Blockchain technology, which includes a multidimensional paradigm shift in terms of cybercrime, money laundering and financing of terrorism and one of its most popular outputs. As a result of the study, although some cryptocurrencies are exposed to these crimes and skis, it has been observed that these coins have a very limited instrument role in these crimes. However, while technological innovation is perceived as a threat by the central authorities of developed countries, it is seen as a new social and economic opportunity for some undeveloped and developing countries to overcome global unequal conditions.

Keywords: Blockchain, Crypto Money, Transnational Crimes, Terrorism, Financing of Terrorism, Cyber crime, Bitcoin, Money Laundering

ÖNSÖZ

Blockchain teknolojisi, doğası gereği merkezi olmayan dağıtık veri mantığına dayanan günümüze değin erişilmiş, en güvenli sanal altyapı mimarisini ortaya koymaktadır. Devletler ve diğer merkezi otoriteler bu teknolojinin felsefi arkaplanı ve beraberinde getirebileceği teknolojik dönüşümü kendi varlıklarına karşı bir tehdit olarak okumakta; dezavantajlarıyla birlikte avantajlarına da direnç geliştirmektedirler. Toplumsal dönüşümlere milat oluşturabilme potansiyeline sahip olan Blockchain teknolojisinin bir ürünü olan kripto paralar, salt iktisadi etkilerinin ötesinde suç ve uluslararası suçlarla ilişkisi bağlamında ele alınarak, özellikle siber suçlar, kara paranın aklanması ve suçtan elde edilen gelirin terörün finansmanında kullanımı özelinde incelenmiştir. Çalışılan konunun sahadaki yansımasına bakıldığında, evrenin dinamik ve sınırları sürekli genişleyen bir yapıda olması sebebiyle, çalışmanın anlamlandırılmasında örnek olaylar ve gelişmelerin incelenmesi bir yöntem olarak uygulanmıştır. Çalışma sonucunda, Blockchain ve kripto paralarla ilişkilendirilen özellikle siber mecradaki suç faaliyetleri ile suçlardan elde edilen kara paranın aklanması ve terörizmin finansmanına ilişkin bulgularda çelişkili sonuçlara ulaşılmıştır. Bu sonuçlar perspektifinde Blockchain ve kripto paralarla çeşitli uluslararası suçlar özelinde alan yazına katkı sağlamayı amaçladığım bu çalışmamda danışmanım sayın Prof. Dr. Ensar NİŞANCI hocama, sonsuz desteği ile her zaman yanımda olan sevgili eşim Rukiye CİVAN KEMİKSİZ'e, hayatı anlamlı kılan canım yavrularım Ayşe Hüma ve Ömer Akif'ime teşekkür ederim.

İÇİNDEKİLER

Sayfa

2. BÖLÜM
SINIRAŞAN SUÇLAR VE TERÖRİZM

ŞEKİLLER LİSTESİ

RESİMLER LİSTESİ

KISALTMALAR LİSTESİ

AGİT	: Avrupa Güvenlik ve İş birliği Teşkilatı
BCH	: Bitcoin Chash
BDDK	: Bankacılık Düzenleme Denetleme Kurumu
BTC	: Bitcoin
DLT	: Dağıtık Kayıt Teknolojisi
DNS	: Alan Adı Sunucusu
DOS	: Hizmet Engelleme Saldırısı
EMI	: Elektromanyetik Girişim
ETH	: Ethereum
FATF	: Mali Eylem Görev Gücü
GPS	: Küresel Konumlama Sistwmi
HTML	: Hiper Metin İşaretleme Dili
KDV	: Katma Değer Vergisi
MASAK	: Mali Suçları Araştırma Kurulu
NBC	: Nükleer, Biyolojik, Kimyasal
PKK	: Partiya Karkeren Kürdistan
P2P Protocol	: Eşler Arası Protokolü
SHA	: Güvenli Hash Algoritması
SPK	: Sermaye Piyasası Kurulu
TEMPEST	: Telecommunications Electronics Material Protected from Emanating Spurious Transmissions
TCK	: Türk Ceza kanunu
TCMB	: Türkiye Cumhuriyet Merkez Bankası
XRP	: Ripple
VUK	: Vergi Usul Kanunu

GİRİŞ

İnsanlık tarihi boyunca dünya, köklü değişimlerin ve dönüşümlerin sahnesi oldu. Tarih kimilerini kalın harflerle not ederken kimilerini ise kayıt altına bile almaya fırsat bulamadı. Üzerinde güneşin batmadığı, hükmü kıtalara sığmayan nice deneyim dahi dünyanın bu tekâmülü karşısında iktidarını sürdüremedi; Bugün dünyanın güncellenme katsayısı karşısında insan, her zamankinden daha mücadeleci, her zamankinden daha avantajlı bir konumda olsa da dünya artık çok daha hızlı dönüyor. Uzak Asya'dan Avrupa'ya, Afrika'nın en güneyinden Kuzey kutup dairesine kadar insan, artık her kelebeğin kanat çırpışını daha derin hissediyor. Dünya tarihinde birçok felaket, ardından köklü değişimleri getirmiştir. Bu değişimler doğası itibariyle hem fırsatlar hem de tehditler barındırmaktaydı. Yaşanan bu deneyimler gerçek zamanlı ve gözlemlenebilir nitelikte olması sebebiyle olabildiğince öngörülebilmekteydi. Nitekim son yüzyıldaki gelişmeler; başta insanın kendisi olmak üzere, savaşlardan uluslararası sisteme, hükümet politikalarından küreselleşme sürecine birçok köklü değişimlere sebep oldu. Büyük kırılma ise internet teknolojisi ile gerçekleşti. İnsanlar, şirketler, devletler ve bunların davranışları, alışkanlıkları, iş şekilleri farklı bir boyuta taşındı.

Dünyamız ilkel parametreleri ile organik sürecine sadakatle devam ederken, insanoğlu, tüm kavramları yeniden kurgulamaktadır. Tüm zamanların en konsantre zaman dilimini yaşadığımız bu günlerde yeni bir çağa taşınıyoruz. Sahip olduğumuz kavramların bu deneyimi açıklamaya yetemeyeceği; çoğu şeyi deneyimleyerek yeniden keşfedeceğimiz bir çağa. Artık duyularımızın ötesinde zamanın ve mekânın gerçekliği evirdiği yeni bir gerçeklikle karşı karşıyayız. Sahip olduğumuz varlıklara, paraya ya da bir fikre, kelimenin tam manasıyla bilgiye, müdahale edilemez ve susturulamaz bir form arayışımız sonunda büyük değişimin kapılarını araladı; Blockchain.

Blockchain teknolojisi, yakın bir gelecekte insanın doğuştan sahip olduğu kimliği ve onu kanıtlama yöntemi başta olmak üzere meslekler, iş modelleri, iktisadi sistemler ve hatta oy kullanma biçimlerimizi dahi değiştirebilecek bir potansiyele sahiptir. Üstelik bugüne kadarki en güvenli ve en düşük maliyetli şekliyle. Kaçınılmaz olarak birçok sektör, kurum, kuruluş ve tabiki devletler bu değişimden köklü şekilde etkilenecektir. İnsanın ve inşa ettiği kurumların mevcut hallerinde ve çalışma

alışkanlıklarında dramatik değişiklikler öngörülmektedir. Akıllı sözleşmeler, kripto paralar, akıllı varlıklar bu yansımanın en öne çıkan örnekleridir.

Blockchain ürünü olan kripto paralar, günlük hayatımızda geleneksel tecrübelerimizden farlı olarak çoktan yerini aldı bile. Kimi zaman tasarruf aracı, kimi zaman fon transfer aracı kimi zaman ise bir örgütlü suç çetesi ile anılan kripto paraların hacmi iktisadi hayatta her geçen gün artmaktadır. Blok zinciri teknolojisinin ürünleri oldukça hızlı bir şekilde çoğalırken, buna karşılık kurumların bu yeni deneyimleri konumlandırma çabaları çoğu zaman hantal kalmaktadır. Bu durum kimi çevreler için suç faaliyetlerini yürütürken yeni mecralar da yaratmaktadır. İnternet teknolojisi suç kavramı ve suçların uluslararasılaşmasında astronomik bir imkân yaratırken; çoğu ülkenin hukuki mevzuatlarında henüz tanımlanmayan çeşitli kripto para birimlerinin birçok tehdidi de beraberinde getirdiği iddia edilmektedir. Bu durumun nedeni kripto paraların güvensizliğinden mi, yoksa ilgili kurumların refleks kapasitesinden mi kaynaklanmaktadır? Öte yandan potansiyeli henüz yeni yeni gün ışığına çıkan bu yeni teknolojilerin varlığı bile çoğu devlet tarafından tehdit olarak görülmekte ve entegrasyonuna direnç gösterilmektedir. Bu bağlamda kripto paraların, özellikle siber suçlar, kara para aklama ve terörün finansmanı gibi çeşitli sınıraşan suçlarla ilişkisi aydınlatılmaya değerdir.

Bu çalışma amaçları bakımından tasviri, araçları bakımından ise kaynaklara dayalı bir çalışmadır. Bununla birlikte, blok zincir teknolojisi ile üretilen kripto paraların sınıraşan suçlar ve terörizmin finansmanında kapsamında kullanımının arttığı hipotezi çerçevesinde bilgilerin ve elde edilen verilerin tasnifi amaçlanmaktadır. Bu bağlamda ortaya konulmaya çalışılan temel problem ise kripto paraların suç eylemlerine konu olup olmadığı, oluyor ise hangi düzeyde kullanıldığı ve hangi suçlarda yoğunlaştığını ortaya koymayı amaçlamaktadır. Çalışmada yer verilmiş olan veri ve istatistikler belirli kuruluşların yayınlamış olduğu birincil kaynaklardan elde edilmekle birlikte konular ile ilintili bilgiler kitap ve makaleler gibi ikincil kaynaklardan yararlanılarak elde edilmiştir.

Çalışma, birinci ve ikinci bölümleri kavramsal çerçeve, üçüncü bölümü bulgu, veri ve istatistiki içerikler olmak üzere üç bölümden oluşmaktadır. Birinci bölümde büyük ölçekli toplumsal siyasi ve iktisadi dönüşümlere zemin oluşturabilme kapasitesi bakımından önemli bir yenilik olarak karşımıza çıkan blok zincir teknolojisi

ile bu altyapının en popüler çıktısı olan kripto para olgusu irdelenmektedir. Çalışmanın ikinci bölümüde teknolojiyle eş zamanlı değişen ve yeni formlar kazanan sınıraşan suçlar kavramı ve bu kapsamda değerlendirilen yasa dışı suç faaliyetleri incelenmiştir. Ayrıca kara para aklama suçu ve terörizm kavramı, ülkelerin sınırlarına sığmayan ve küresel ölçekte politik sonuçlar üretmesi bakımından yine bu bölümde ele alınmaktadır. Üçüncü bölümde ise kripto paraların; bilişim suçlarında, karapara aklama faaliyetlerinde ve terörizmin finansmanında kullanımına ilişkin bulgu veri ve istatistiklere yer verilmektedir.

Kripto paralara ilişkin Türkiye özelinde mühendislik, iktisat ve hukuk disiplinlerinde çeşitli lisansüstü çalışmalar bulunmaktadır. Bununla birlikte kripto para olgusunun kriminoloji ile ilişkisini ortaya koyan bir çalışma bulunmamaktadır. Bu çalışma, kripto para olgusunu multidisipliner ölçekte ele alarak özellikle kriminoloji ile ilişkisinin irdelemesi bakımından alan yazınına katkı sunmayı amaçlamaktadır.

1. BÖLÜM
BLOK ZİNCİRİ VE KRİPTO PARA TEKNOLOJİSİ

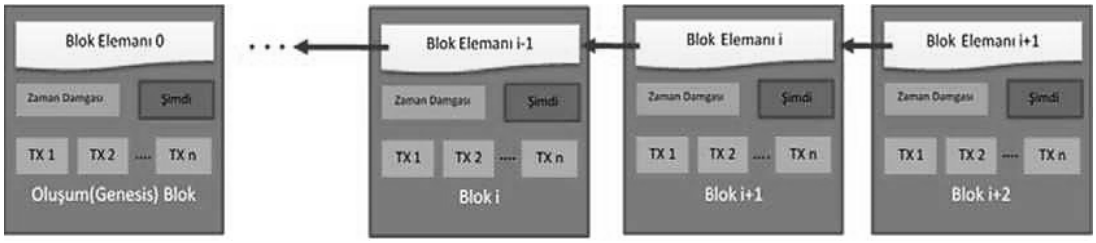
1.1. BLOK ZİNCİRİ TEKNOLOJİSİ

1.1.1. Blok Zinciri Tanımı

Blok zincir kavramı üzerinde araştırmacıların üzerinde ittifak edebildiği bir tanım ile karşılaşamamaktayız. Ortaya konulan tanımlar alt detayları özelinde farklılaşmakta ve birçok farklı tanım şeklinde ortaya konulmaktadır. Yapılan bu tanımlamalara bakıldığında Tian'a göre Blok Zincirini dağınık bir veritabanı modelinin kriptografik fonksiyonlar vasıtasıyla güvenli yöntemlerle inşa edilmiş bir veritabanı tekniği olarak ifade etmektedir (Tian, 2016, s. 9). Nakamoto' ya göre (2018) blok zinciri verilerin dağıtışmış bir şekilde depolandığı ve verilere ilişkin değişikliklerin ağda bulunan tüm kullanıcılar tarafından kaydedildiği bir veri ağı yapısıdır. Beck'e göre (2018) de, blok zinciri ağı üzerinde gerçekleştirilen işlemlerin tarafından sadece güvenli değil aynı zaman da doğrulanabilir şekilde yapılmasına imkân sunan bir veritabanıdır. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang (2017)'a göre blok zinciri, tüm kullanıcılar tarafından onaylanmış işlemlerin blok listeleri şeklinde saklandığı ve her yeni işlem bloğu ile büyüyen bir veri defteri olarak ifade edilmektedir. A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz (2018) blok zincirini ağ üzerindeki işlem güvenliğinin üçüncü taraflarca değil ağda konuşlu tüm kullanıcılara dağıtılmış doğrulama sorumluluğu ile gerçekleştirmektedir. Ağdaki tüm işlemler merkezi olmayan bir yapıda, herkese açık, silinemez ya da değiştirilemez nitelikte işlem yapabilme özelliklerini içeren bir veritabanı modelidir. Glaser (2017) ise blok zincirini, otoritesi kullanıcılarının tamamı tarafından paylaşılan herhangi bir aracıya ya da merkezi bir otoriteye ihtiyacı olmayan değerli varlıkların tüm kayıtlarının herkese açık ve anonim olarak adlandırıldığı bir veritabanı şeklinde tanımlamıştır. Kimi araştırmacılar ise blok zincirin detaylarını gözardı ederek sadece veri bütünlüğü fonksiyonu kabiliyetine odaklanmaktadır. Örneğin H. Halpin, M. Piekarska (2017) blokzincirinindeki veri listelerinin kriptografik yöntemlerle doğrulanabilme özelliği ile tanımlamaktadır. Teknolojik altyapısı itibariyle incelendiğinde blok zincirinin en temel özellikleri dağınık veritabanı, kriptografik algoritmalar ve merkezi olmayan mutabakat fonksiyonu ile tasvir etmek doğru olacaktır F. Hawlitschek, B. Notheisen,

T. Teubner, (2018). Blokzincirinde gerçekleştirilen tüm işlemlere ait veriler kriptografik yöntemlerle birbirine eklemlenen içerisinde de veri ve işlem bilgilerini depolayan sonsuz potansiyelde bloklar zincirinde saklanır. Veri bloklarının yaratılması, yapılan işlemlerin güvenilirliğinin ve geçerliliğinin kendine has algoritmalar ile katılımcılar tarafından yerine getirilen bir dizi işlem sonucu gerçekleştirilir şeklinde açıklar. J. L. Zhao, S. Fan, J. Yan, (2016) blok zincirin ayırt edici özelliği olarak işlemlerin güvenilirlik ve şeffaflığının bir insan organizasyonu ya da insan temelli bir denetleme mekanizmasıyla değil de zincir ağı üzerinde çalışan bir hesaplama algoritması ile yerine getirilmesi olarak ifade etmiştir. Blok zincirinde bugüne kadar tecrübe edilmiş veritabanlarından ayıran birtakım farklar bulunmaktadır. Bunlardan bazıları; blok zincirinde kayıtların veritabanından silinerek yerine yeni kayıt girilmesi yerine veri kaybı gerçekleşmeden bloğa yeni bir kayıt eklenmesi, kayıtlara ilişkin doğrulama ve bilgilerin dağıtılması işlemlerinde karşılıklı mutabakatı tesis eden bir takım P2P ağı kuralları ile çalışan geliştirilmiş bir veritabanı olarak ifade etmektedir (Lewis, 2018).

Şekil 1.1: Blok Zincir Mimarisi



Kaynak: Avunduk ve Aşçan, 2018, s. 373

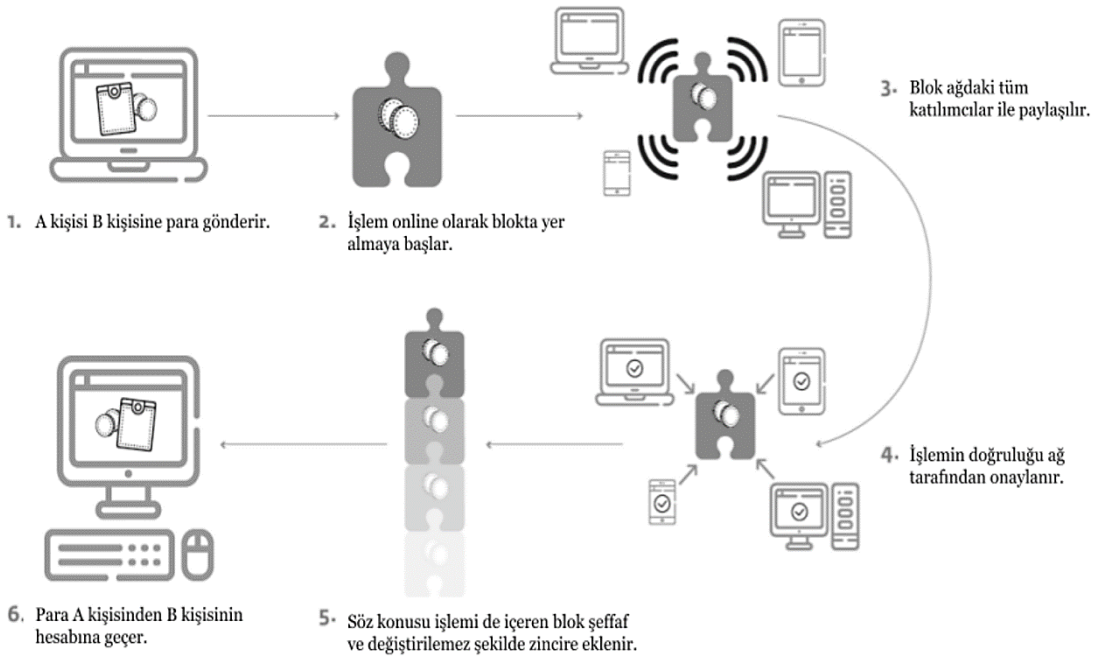
Blok zincir mimarisi Şekil 1.1 de gösterilen işlem mantığı üzerine kuruludur. Zincir oluşumu ilk genesis bloğu ile başlar. Her bir blok kendinden önceki bloğun değerine kendi değeriyle eklemlenir. Her yeni eklemlenen blok için bir sonraki blok üst blok olarak tanımlanır. Anılan bu yapı zincir şeklinde birbirine eklemlenerek sonsuz tane olabilecek şekilde uzanarak devam eder.

1.1.2. Blok Zincir Yapısı

Blok zinciri teknolojisinin felsefi arka planında insanlar için kıymetli olan kimlik bilgileri, kişisel verileri, dijital iktisadi varlıkları, fikri mülkiyete haiz varlıkları

ile sözleşmeler gibi maddi ve manevi varlıkların kayıt altına alınması ve doğrulanması gibi işlemlerin herhangi bir otoriteye bağlı kalmaksızın aracılık komisyonu olmadan sanal birtakım işlemler ile teyit edilmesi işlemlerine olanak yaratması düşüncesi yatmaktadır. Blokchain yapısı; sadece finansal işlemlerin yerine getirilmesinde değil, ticarete konu mal ve hizmetlerin alışverişinde, sigortacılık ve bankacılık hizmetleri gibi aracılık hizmetlerinde de hizmet sunumunu verilmi kılan maliyetleri düşüren dahası işlemlerin ve belgelerin doğrulanmasına olanak vermektedir (Mainelli, 2017, s. 3).

Şekil 1.2.: Blockchain Teknolojisinin Çalışma Prensibi



Kaynak: Financial Times retrieved Brookings, 2017

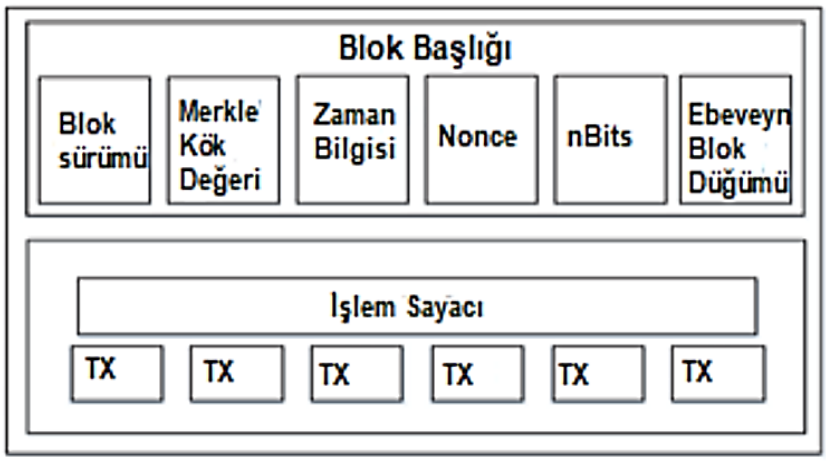
Bugün birçok aracılık hizmetleri, alışveriş işlemleri hergün daha da artan bir oranla internet kanalıyla gerçekleşmektedir. Bu işlemlere ilişkin oluşan kayıtların güvenilirliği ise ayrıca geliştirilen paket programlar tarafından sağlanmaktadır. Buna benzer işlemlerin kaydedilmesi ve onaylanması süreçleri tam manasıyla blokchain işlemlerini ifade etmektedir (Marvin, 2016, s. 2). Tüm bu açılardan değerlendirildiğinde blok zincir sistemi, çalışma mekanizması ve mutabakata varmak için hangi yöntemlerin kullanılacağı konusunda düzenlenebilmektedir. Bu sistem

küçük gruplar arasında ya da çok fazla üyesi olan yapılarda da kullanılabilmektedir. Bu yapıya en güzel örneklerden biri olarak milyonlarca üyesi olan Bitcoin verilebilir.

1.1.2.1.Blok

Herhangi bir değer ifade eden her çeşit verinin muhafaza edildiği yapılara blok denir. Blok; Blok zincirini onaylanmış ve güvenli bir ağ oluşturmuş bilgi bloklarından meydana gelmektedir. Blok zinciri işlem verilerinden oluşan blokların birbiri ardı sıra bir zincir halkası gibi eklemlenmesiyle oluşmaktadır. Blok zinciri dahilindeki her blok, başlık ve gövde olarak iki temel bölümden oluşmaktadır. Bloklarda herhangi bir değer içeren verilerden oluşmaktadır. Blok başlığında bir dizi genel bilgiler bulunmaktadır bunlar; tarih, bir önceki bloğa ait özet değeri, merkle kökü, işlem ispatı için gerekli verilerdir. Blok gövdesinde de özet değeri ve blok işlemleri bulunmaktadır.

Şekil 1.3. Blok Yapısı



Kaynak: Zheng vd., 2017 s. 558

1.1.2.2. İşlem / Hesap Hareketi

Veri bloklarının içinde tutulan veriler, hesap defterlerine ait girişleri ya da hesap hareketlerine ilişkin işlemleri temsil etmektedir. Tüm hesap işlemlerinin dijital bir imza ile imzalanarak güvenilirliğinin ve gerçekliğinin korunarak maksimum güvenlik amaçlamaktadır. Böylece blokların içerisindeki işlem kayıtlarına müdahale edilemez ve kimse tarafından değişiklik yapamaz ki bu, işlem kayıtlarının

güvenilirliğini mutlak hale getirir. Blok zincirinde terminaller arasındaki karşılıklı ya da tek taraflı varlık transferlerinin her birine işlem adı verilir. Tüm işlemler blokların gövdesine kayıt edilir. Esasında bir işlem; girdi-çıktı listesi, toplam miktar bilgisi, işlemin özet değeri bilgilerinden oluşmaktadır (Tikveşli, 2019, s. 7).

1.1.2.3. Hesap Adresleri

Blok zincirinde gerçekleşmiş her işlemde, gönderici ve alıcıların hesap adresleri kayıt altındadır. Blok zincire dahil olan tüm yeni kullanıcıların namına istemde yeni bir adres üretilir. Bu adresler sistem tarafından kullanıcıların kimlikleri olarak adlandırılabilir. Kullanıcılar da açık anahtarlarını kullanmak suretiyle adlarına hesap adresleri yaratırlar. Oluşturulan bu adreslerdeki her bir dijital varlık için sahiplik bilgisi yer alır. Hesaplara ait olan saklı anahtarların varlığı da kullanıcının dijital varlıkları üzerinde işlem yapabilmesi, tasarrufta bulunabilmesine imkân tanır. Söz konusu bu işlemler ancak kullanıcının saklı anahtarını kullanarak ilgili işlemi imzalaması/onaylaması ile gerçekleştirilebilir. Dijital varlıklar üzerindeki bu değişikliklerin doğrulanmasında da kullanıcının hesap adresi üzerinden üretilen açık anahtarlar kullanılmaktadır.

1.1.2.4. Kayıt Defteri / Hesap Defteri

Veriler, tüm terminalde yer alan ve herkese açık olan hesap defterlerinde yer almaktadır. Bu hesap defterlerinde blok zincir ağında yaratılan ve doğrulanan işlem kayıtları tutulmaktadır. Sistemin güvenliği, kullanıcıların dijital hesap defterlerinin eşzamanlı olarak zincir ağına dahil tüm kullanıcılara dağıtılmasıyla sağlanmaktadır. Altyapıdaki bir güvenlik katmanı, her bir hesap hareketine ilişkin durumu istenilen her an doğrulama sağlanabilmesi imkanına olanak vermektedir. Tüm katmanlarda, gerçekliği ve doğruluğu korunan işlemleri içeren hesap defterlerinin birer kopyası bulunmaktadır.

Sistem altyapısında sürekli aktif olan bir algoritma zincir üzerindeki her yeni hesap hareketini ya da mevcut hesaplardaki bir değişikliğin tüm kayıtlarını karşılaştırarak doğruluğunun kontrolünü sağlamaktadır. Hesap defterlerineki her bir kopya ya da çoğunluğu bu kayıt değişikliğinin doğruluğunu onayladığı takdirde ancak yeni bir blok ağa dahil edilmektedir. Nitekim sisteme dahil kopyaların çoğunluğu bu

yeni işlemi reddeder onaylamazsa, sözkonusu bu yeni hesap hareketi zincir sistemine kaydedilemeyecektir. İşte bu merkezi olmayan ağ sistemi sayesinde, odak bir yapı ile kontrol edilmeden ya da başka bir değişle tüm terminaller tarafından senkroize bir kontrol mekanizmasına imkân sağlayarak etkin ve sorunsuz bir şekilde işlemektedir.

1.1.2.5. Cüzdan

Kullanıcıların işlem hareketliliğine imkân sunan saklı anahtarları hayati önemdedir. Dijital varlıklar üzerindeki tasarruf hakkı ve bu tasarruflara ilişkin işlemlerin güvenliği bu anahtarın kullanıcısı tarafından saklanması ile mümkündür. Kullanıcıların bu anahtarları cüzdanlarında saklanır. Ayrıca cüzdanlarda kullanıcı anahtarına ek olarak cüzdan sahibinin dijital varlıklarına ilişkin bilgileri de bulunmakadır. Örneğin kullanıcıların bitcoin para birimi için paralarını saklayıp üzerinde işlem yapmalarına imkân sunan programlar bitcoin wallet olarak adlandırılır. Böylelikle kripto paralar sanal mecrada üretilebilen, muhafaza edilebilen ve alışveriş işlemleri gerçekleştirilebilen bir özellik taşır. Bu özellikleri sayesinde kripto para birimleri merkez bankaları gibi bir merkezi kuruma ihtiyaç duymazlar.

1.1.2.6. Kriptografik Hash Fonksiyonu

Kriptografi, matematiksel yöntemleri kullanarak verilerin gizliliği güvenliği ve denetlenebilmesine imkân sunan bir çeşit şifreleme olarak tanımlanabilir. Bu şifreleme süreci, karmaşık birçok yöntem ve gelişmiş birçok tekniği kullanan kapsamaktadır. Kriptografinin temelini oluşturan yine temel bir şifreleme işlemi olan hash fonksiyonudur. Hash kavramının dilimizdeki karşılığı özetleme olarak ifade edilmektedir. SHA-1, SHA-2, MD-5, BLAKE gibi çok çeşitli hash algoritmaları bulunmaktadır. Bir hash fonksiyonu, üç temel niteliğe sahip matematiksel yöntem içermektedir. Bunlar;

- Girdi verilerine ait boyut herhangi bir ölçekte olabilir ve veriler herhangi bir dize'de yer alabilir.
- Hash 64 bit, 128 bit, 256 bit gibi sabit boyutta çıktılar üretmektedir.
- Özetleme işlevi verimli olarak hesaplanmaya olanak sağlamaktadır.

Kriptografik bir işlemin hash fonksiyonun da H:{0,1}*-{0,1} istenilen herhangi uzunluktaki bir mesaj M için n bit'lik sabit uzunlukta özetleme değerini hesaplayan fonksiyondur. Kriptografik özetleme fonksiyonu birçok uygulamada kullanıma uygun temel bir şifreleme yöntemidir. Örnek vermek gerekirse parola işlem hash fonksiyonu, içerik adresli depolama, dijital imza şemaları, kimlik doğrulama kodları gibi uygulamalarda kullanılabilmektedir. Anılan uygulamaların çoğunun güvenliği ya da sorunsuz işleyişi, kırılmasının pratikte mümkün olmadığı görüşüne dayanmaktadır. Güvenli Hash Algoritması leteratürdeki tanımıyla SHA-Secure Hash Algorithm, bir dizi kriptografik özetleme fonksiyonu oluşmaktadır. Son Kısaca ifade etmek gerekirse kriptografik hash, şifrelenmek istenen veri dosyası için bir imza niteliği taşımaktadır. Bir örnekle hash işlevini açıklamak gerekirse; SHA-2 Hash Algoritmasının fonksiyonundan biri olan yüksek güvenlikli SHA-256 algoritması birçok farklı boyut ve ölçekteki metin, sayı ya da farklı formattaki dijital veriyi, tek yönlü ve standart büyüklükte, 256 bit boyutunda kriptolamakta ve böylelikle seçilen her veri için SHA-256 değeri hep aynı sonucu vermekte olup sadece söz konusu örneklenen veri içerisinde bir değişiklik olması halinde sonuç değer üzerinde orantılı değişiklik gözlenmektedir. SHA-256 hash algoritmasında, girdi olarak belirlenen verinin ne olduğu tespit edilemez. Bunun nedeni SHA1256 algoritmasının tek yönlü bir algoritma olmasından kaynaklanır. Bu da geriye dönük hash değerlerine bakılarak girdi verisinin kesin ve doğru bir şekilde elde edilebilmesine engel teşkil etmektedir. Söz konusu girdi verisi sadece tahmin edilebilir bu tahminin doğru sonuç verme oranı ise 2256 da 1 ihtimaldir. Blok zinciri altyapısında hash fonksiyonları sıklıkla kullanılmaktadır. Örneğin Bitcoin işlemlerinde yer alan adres oluşturma süreçlerinde ve PoW hesaplamalarında SHA-256 hash algoritmasından yararlanılmaktadır.

1.1.2.7.Merkle Ağacı

İngilizce ifadesiyle Merkle Tree, Merkle Root veya Root Hash, Türkçe ifadesiyle ise Merkle Ağacı, Merkle Kökü veya Kök Özet tanımları aynı anlamda kullanılmaktadır. Genel anlamda, Merkle Ağacı büyük veri yığınlarının bir araya getirilip özet olarak gösterilmesi ve bunun güvenli bir şekilde doğruluğunun sağlanabilmesidir. Çalışma prensibi açısından bir ağacın yapısına benzemektedir. Ağacın yaprakları veri bloklarını temsil etmekte, bu veri blokları özetleme

fonksiyonundan geçirilerek özet değerleri oluşmakta ve bunlar da ağacın dallarını temsil etmektedir. Oluşan özet değerlerde tekrar özetleme fonksiyonlarından geçirilerek yeni özet değerler elde edilir. Bu döngü aynı şekilde devam ederek en son kök özet değerine ulaşılır. Bu da ağacın köküne ulaşmak olarak yorumlanmaktadır. Merkle kökü ile blok zincirler arasında oldukça sıkı bir ilişki bulunmaktadır. Blok başlığı içerisindeki Merkle Kök Özeti, blok gövdesi içerisindeki işlemlere ait kök özet değerdir.

1.1.3. Blok Zincirinin Temel Bileşenleri

Blok zincirin tanımlamalarına bakıldığında çok farklı tür ve boyutta fonksiyonları yerine getirdiği görülmektedir. Genel olarak blok zincir altyapısı üzerine konuşlu işin niteliği, bu tanımlamaların perspektifini belirlemektedir. Örneğin, bu altyapı, bir finansal hizmet aracı olarak kurgulanmışsa dijital paralar-kripto paralar bağlamında tanımlanırken, teknik nitelikleri bakımından ele alındığında ise, onu diğer teknolojilerden ayıran yönleri bağlamında tanımlanmaktadır. Ancak genel olarak Blockchain, yüksek güvenlikli şifrelenmiş, müdahale edilemez, herhangi bir aracı veya otoriteye ihtiyaç duymaksızın taraflar arasındaki mutabakat ve anlaşmaların şeffaf bir şekilde dizinlendiği, bir tür kayıt ağacı olarak tanımlanabilir. Bu açıdan değerlendirildiğinde, oldukça yeni ve iddialı ve getirdiği yenilikler bakımında tsunamik bir potansiyeli barındırmaktadır (Bashir, 2017).

İktisadi araçların tanımlanmasında kullanılan özellikleri, her tanımlayan tarafından farklı ele alındığı gibi, blok zincir teknolojisinin özellikleri bağlamında da birbirinden farklı yaklaşımlar mevcuttur. Blok zincirin yerine getirdiği işlevler bakımından temel olarak üç ana unsurdan oluşmaktadır (Karaköse, 2017):

- Eşler Arası Protokol (P2P Protocol)
- Dağıtık Kayıt Teknolojisi (DLT)
- Mutabakat Birliği Protokolü (Consensus Protocol)

1.1.3.1. Eşler Arası Protokol

Katılımcıların sahip oldukları tüm kayıtlara erişim sağlayabileceği, herkese açık dijital kayıtlar olarak ifade edilebilmektedir. Açık blok zincirlerindeki kayıtlar herkese açıktır, kullanıcı tarafların sorumluluğu olmaksızın isteyen her kullanıcının

kullanımına sunulmuş bilgileri içerir. Dünyanın farklı yerlerinde tek bir kişi veya kuruluşun değil, dağıtık bir ağ ile sonsuz kullanıcının işlem gerçekleştirebileceği bir işlevi yerine getirmektedir. Özü itibariyle Blockchain altyapısı, her şeyi tek bir merkezi konumda tutmak yerine verileri birden fazla düğüm üzerinden paylaşmamaya başlayarak aracılık mekanizmasını ortadan kaldıran, şeffaflık temelinde sahtecilik ve verilerin işlenmesi olasılığını ortadan kaldıran, üçüncü tarafların müdahalesini azaltmak suretiyle her akıllı sözleşme işleminin daha ekonomik ve hızlı gerçekleştirilmesini sağlamaktadır. Ağ üzerindeki tüm katılımcıların bir yayıncı aynı zamanda da bir abone gibi konumlanması eşler arası bildirim işlevini ifade etmektedir. Tüm katılımcılar, diğer her bir katılımcıyla karşılıklı işlemler gerçekleştirebilirler ve bu işlemlere ilişkin kayıtlar, gerçek zamanlı olarak güncellenmektedir (Gupta, 2017).

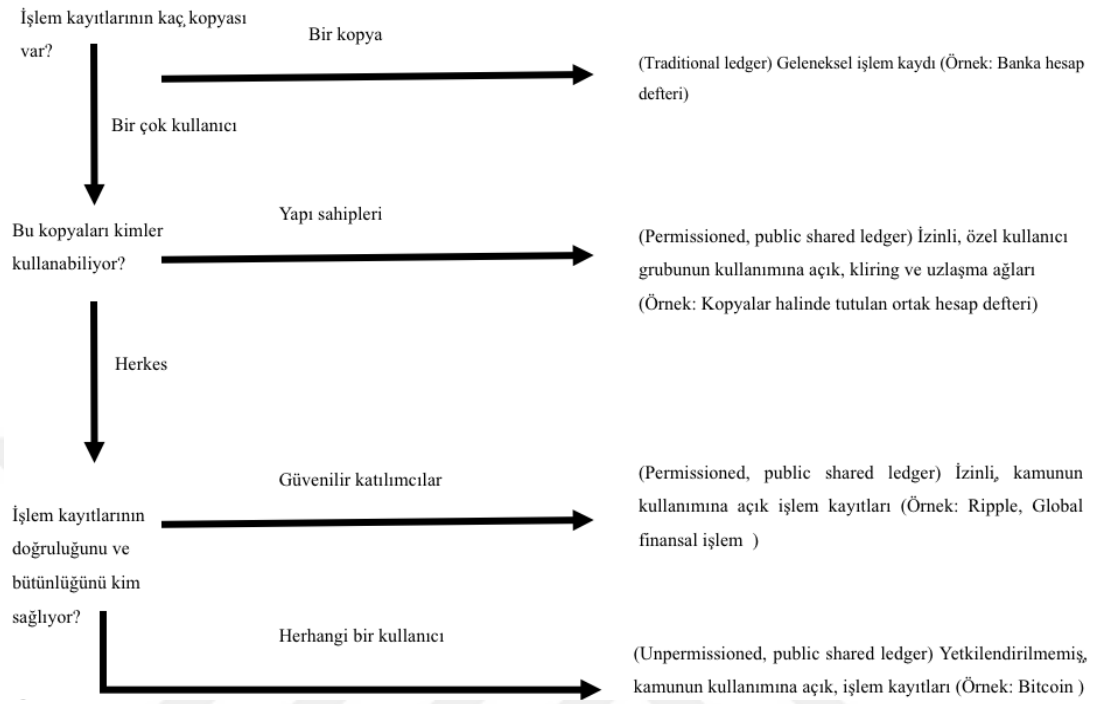
1.1.3.2. Dağıtık Kayıt Teknolojisi

Blok zincirinin günümüzde en popüler kullanım alanlarından birisi de ödeme sistemlerinde kullanılan dağıtık kayıt teknolojisi olarak karşımıza çıkmaktadır.

Merkezi olmayan bir sistem ve dağıtılmış sistem arasındaki temel fark, dağıtılmış bir sistemde hala tüm sistemi yöneten merkezi bir otoritenin bulunmasıdır. Buna karşılık merkezi olmayan bir sistemde böyle bir otoritenin varlığından söz edilememektedir. Merkezi olmayan bir sistem, düğümlerin tek bir ana düğüme bağlı olmadığı bir ağ türüdür. Bu yapı sayesinde, kontrol birçok düğüm arasında dağıtılmaktadır. Bu nitelikleri ile dağıtık kayıt fonksiyonu, üç ayrı işlevi yerine getirmektedir.

- Kayıt kümelerinin, şifreli işlem özetlerini hesaplamaktadır.
- Senkronize olamayan bir eşin ya da yakalaması istenilen bir kayıta ilişkin değişiklikleri iletmektedir.
- Toplam kayıt yükününün minimum seviyede tutulması.

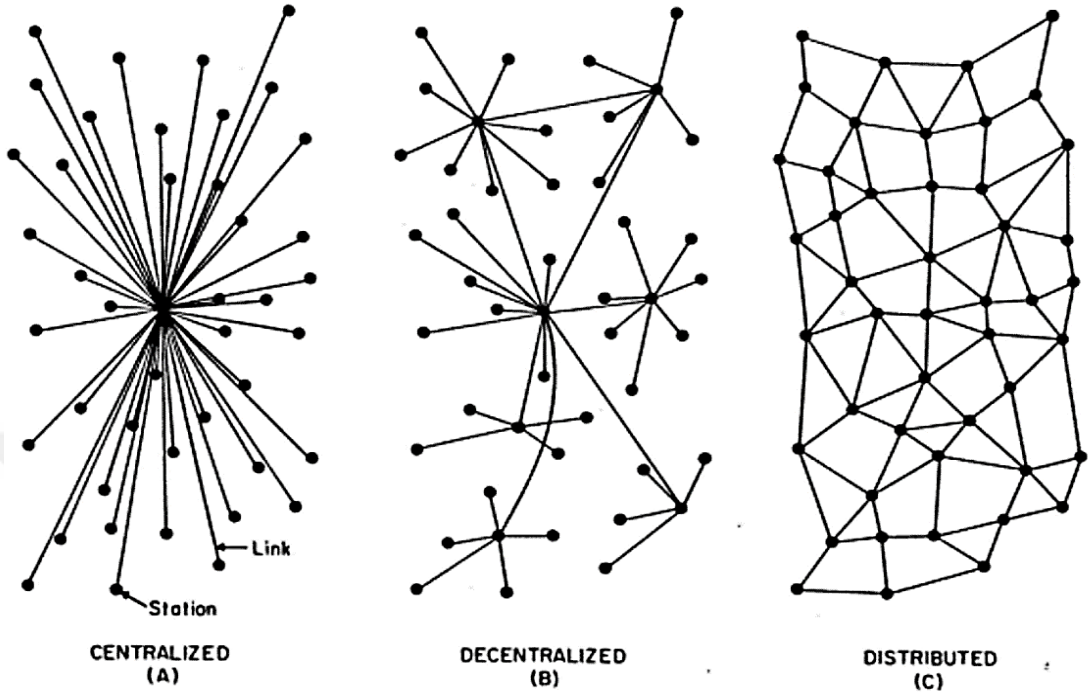
Şekil 1.4.: Dağıtık İşlem Kayıtları Sınıflandırması



Kaynak: Karaköse, 2017, s. 42

Özetle, dağıtık kayıt teknolojisi, hükümetin dolandırıcılık, yolsuzluk, hata ve kâğıt yoğun süreçlerinin maliyetini azaltma olanağı sağlamaktadır. Bilgi paylaşımı, şeffaflık ve güven açısından hükümet ve vatandaş arasındaki ilişkiyi yeniden düzenleme potansiyeline sahiptir. Özel sektör için de benzer imkanlar sunmaktadır Adından da anlaşılacağı gibi son derece yaygın biçimde tam kontrollü bir şekilde dağıtılırlar. Bunun için, hükümetin teknolojiyi uygulamak üzere uzman bir kullanıcı olarak hareket etmesi ve uygulanabilir olduğu yerde dağıtılmış kayıt çözümleri tedarik etmesi gerekmektedir. Dağınık kayıt uygulanmasının kullananımı için, uyumluluk, maliyet etkinliği ve hesap verebilirlik açısından önemli gelişmelere yol açması gerektiği kanısına varılmıştır. Bir dağıtık kayıt teknolojisi düzenlemesinin açık ya da kapalı olmasına bakılmaksızın, katılımcılar (dolayısıyla bulundukları düğümler) izin verilen roller ya da gerçekleştirmelerine izin verilen işlevler ile farklılıklar gösterebilmektedir (Karaköse, 2017, s. 42)

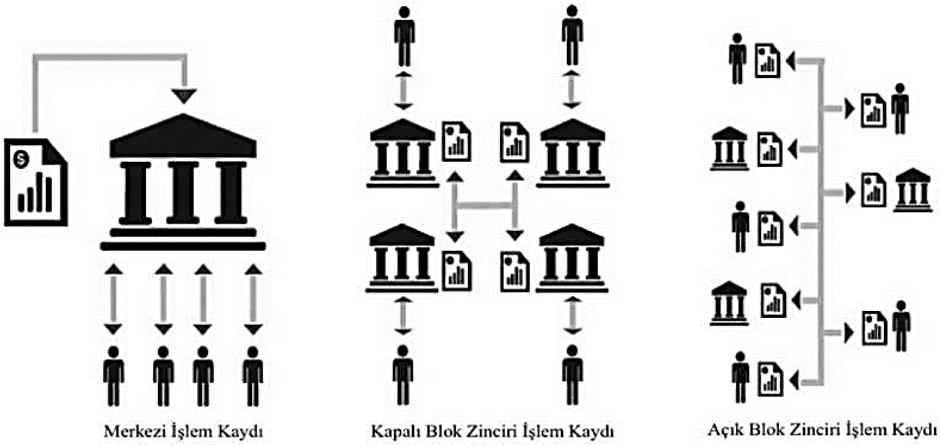
Şekil 1.5.: Ağ Tipleri



Kaynak: Baran, 1964, s. 1

Tekel hizmet sağlayıcısı (hükümetler, mahkemeler ve ticari tekeller gibi) ve alternatif sağlayıcılar (bankalar, çevrimiçi ödemeler veya bulut bilişim sağlayıcıları gibi) olmak üzere yaygın olarak iki çeşit merkezi kayıt sistemi bulunmaktadır. Alternatif sağlayıcıların bulunduğu yapılarda, tek bir servis sağlayıcısının başarısızlığı yalnızca kullanıcılarını etkiler. Kullanıcılar sağlayıcıları değiştirebilir veya birden fazla sağlayıcı kullanabilir. Diğer taraftan tamamen merkezi olmayan sistemler arasında Bitcoin ve Ethereum gibi izinsiz halka açık blok zincirleri bulunur. İzinsiz genel blok zincirleri tamamen açıktır: yeni kullanıcılar istedikleri zaman ağa katılabilir, işlemleri doğrulayabilmektedir. Buna karşın güncel finansal akış süreçleri merkezi bir gözetim ve onay mekanizması içerisinde varlığını sürdürmeyi benimsemektedirler. Bunun temel sebebi işlemler üzerinde kontrol imkânı sağlaması gösterilebilmektedir (Xu, Weber ve Staples, 2019).

Şekil 1.6.: Merkezi, Kapalı ve Açık Blok Zinciri İşlem Kayıtları



Kaynak: Karaköse, 2017, s. 43

Merkezi işlem kayıtlarında güven, mutabakat, doğrulama gibi fonksiyonel ve sistemsel konular merkezi yapılar aracılığıyla sağlanmaktadır. Kapalı veya özel blok zinciri uygulamaları işlemler için yetkilendirme gerektiren genelde izinli, yetkilendirilmiş ve düzenlemelere tabi yapılardır. Açık blok zinciri uygulamalarında blok zinciri ile ilgilenen her kullanıcı tarafından her kayıt görüntülenebilir ve protokol koşullarına uygun işlemler kullanıcılar tarafından gerçekleştirilebilmektedir. Merkezi işlem kayıtlarında bütün bilgiler ve işlemler merkez onayı ile doğrulanarak gerçekleştirilebilmektedir.

1.1.3.1.1. Açık Blok Zinciri

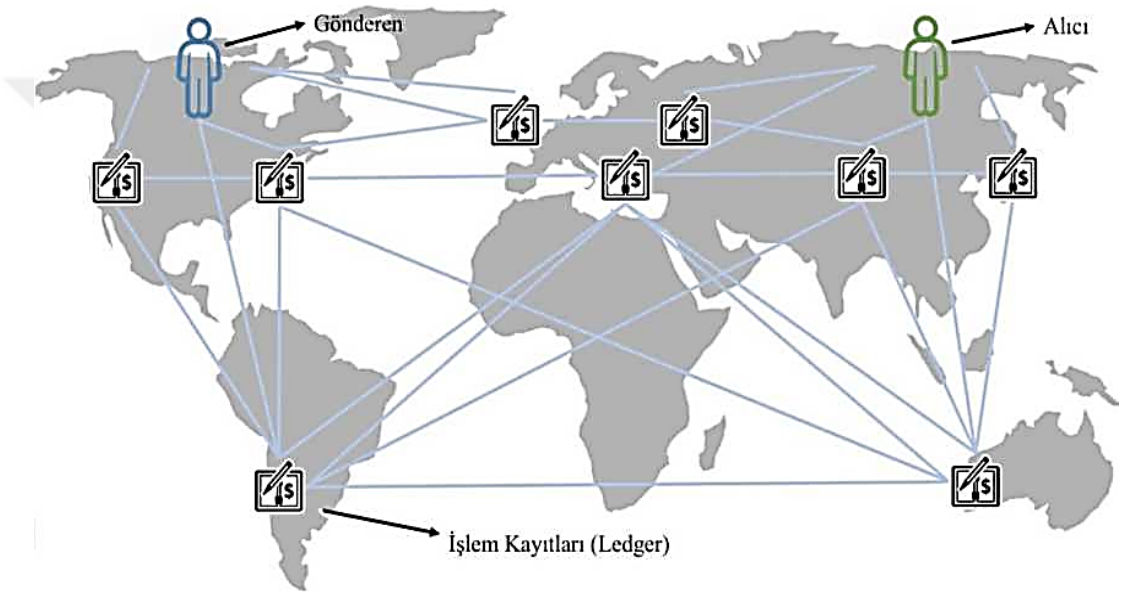
Herhangi bir otorite tarafından izne tabi olmaksızın tüm kullanıcıların verilere erişebildiği ve üzerinde değişiklik yaparak yeni kayıtlar oluşturabildiği sistemler açık blok zincirleri olarak tanımlanmaktadır.

Adından da anlaşılacağı gibi, bu blok zincirleri halka açıktır ve herkes karar verme sürecine bir düğüm olarak katılabilir. Kullanıcılar katılımlarından dolayı ödüllendirilebilir veya ödüllendirilemez. Bu defterler kimseye ait değildir ve ağa katılım herkese açıktır. İzinsiz defteri kullanan tüm kullanıcılar, yerel düğümlerde defterin bir kopyasını tutar ve nihai olay hakkında bir karara varmak için dağıtılmış bir konsensüs mekanizması kullanır. Bu blok zincirleri aynı zamanda "izinsiz

defterler" olarak da adlandırılmaktadır. Bu altyapı ile kurgulanmış blok zincirler bazı üstün nitelikler barındırmaktadır. Bunlar;

- Herkese açık olmalarına rağmen oldukça güvenlidir,
- Ekonomiktir,
- Olası kullanıcı hatalarını minimize etmektedir.

Şekil 1.7.: Dağıtık Kayıt Teknolojisi



Kaynak: IMF, 2016

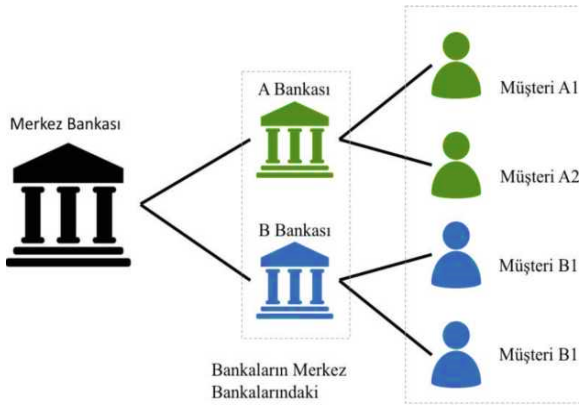
Açık blok zinciri işlemlerin basitleştirilmiş bir yaşam döngüsü Şekil 1.7'de gösterilmiştir. İşlem oluşturulduktan sonra, işlem parayı harcama, sözleşme oluşturma veya işlemlerle ilişkili veri parametrelerini geçirme yetkisi sağlayan işlem başlatıcısının imzasıyla imzalanır. İmzalı bir işlemin yürütülmesi için gereken tüm bilgileri içermesi gerekir. Önerilen bir işlem, işlemin geçerliliğini kontrol eden blok zincir ağına bağlı bir düğüme gönderilir. Geçersiz işlemler atılır. Daha önce düğüm tarafından bilinmeyen geçerli işlemler, diğer bağlı düğümlere yayılır. Bunlar da işlemler ağdaki her düğüme ulaşana kadar işlemleri daha fazla doğrulayacak ve eşlerine gönderecektir. Küresel bir ağda, geçerli bir işlemin genellikle birkaç saniye içinde tüm ağa ulaşmaktadır. İşlemin yayıldığından emin olmak için, gönderenlerin işlemi gönderdikleri herhangi bir düğüme, yeterli başka düğümlere gönderdikleri

sürece güvenmeleri gerekmez. Tüm işlemler imzalandığından ve herhangi bir düğüm tarafından bağımsız olarak doğrulanabildiğinden, alıcıların gönderenlere güvenmesi gerekmez. Bir işlem bir "madencilik" düğümüne ulaştığında doğrulanır ve bir bloğa dahil edilebilir. Madencilik, blok zincir veri yapısına yeni bloklar ekleme işlemidir. Bir blok zincir ağı, geçerli işlemleri bloklar halinde toplamak ve bunları blok zincire eklemek için madencilere dayanır. Yeni bloklar ağın tamamında yayınlanır, böylece her tam düğüm tüm deftere ait bir kopyaya sahip olamkatdır (Xu ve diğerleri, 2019).

1.1.3.1.2. Kapalı Blok Zinciri

Açık blok zincirleri, bazı uygulama bağlamlarında gereken gizlilik düzeyiyle çeliştiği için tartışmalara ve daha fazla gelişmeye konu olmuştur. Kapalı blok zincirleri okuma erişimini kısıtlar ve sonuç olarak artık işlem verilerinin geçmişine dayanan sahipliği açıklığa kavuşturmak için herkes tarafından kullanılamaz. Gizliliğin korunmasına yönelik alternatif yaklaşımlar, özel olarak gizliliğe odaklanan mevcut blok zincirleri veya dağıtılmış bilgi işlem platformları üzerindeki gizlilik katmanlarıdır. Başka bir ifadeyle kapalı blok zincirinde, verilere tam erişim yetkisine sahip olmadan kayıtlara ve doğruluğuna, erişmek mümkün değildir (Drescher, 2017).

Şekil 1.8.: Merkezi Ödeme Sistemi



Kaynak: IMF, 2016

Kullanım amaçları ile avantaj ve dezavantajlarından bakımından blok zincir türleri çeşitlilik arz etmektedir. Kapalı bir yapı görünümü sergileyen merkezi veri tabanı, blok zincirinin aksine yapılan tüm hareketleri merkezi bir sunucuda saklamaktadır.

1.1.3.1.3. Mutabakat Birliği Protokolü

Taraflar arasında herhangi bir menkul kıymet veya fon transferi işlemi esnasında yükümlülüklerin karşılıklı olarak yerine getirilmesi mutabakat olarak ifade edilmektedir (TCMB, 2014, s. 2). Mutabakat birliği ise oybirliği, fikir birliği anlamında kullanılmaktadır. Mutabakat mekanizmaları, dağıtık paylaşılan bir durumun güvenli bir şekilde güncellenmesine izin vermektedir ve son otuz yıldır aktif bir araştırma konusu haline gelmiştir. Dağıtık bir sistemde hata toleransını sağlamak için kullanılan ortak yöntem, paylaşılan durumu ağdaki katılımcılara dağıtmaktır. Yinelenmiş paylaşılan durumun güncellenmesi, tüm kopyalar üzerinde yürütülen "durum makinesi" tarafından, önceden belirtilmiş durum geçiş kurallarına göre gerçekleşmektedir. Bu teknik, durum makinesi replikasyonu olarak adlandırılmaktadır. Durum replikasyonu, bir veya daha fazla düğümün çökmesi ihtimaline karşı, durumun kaybolmamasını sağlamaktadır. Durum makinesi tüm düğümlerin aynı veriyi işlemesini sağlamaktadır. Aynı veriyi işleyen düğümler sonunda muhtemelen aynı çıktıyı üreteceklerdir. Bunun sonucu olarak mutabakat protokolü yoluyla durum değişimi konusunda nihai anlaşmaya varılması muhtemeldir. Replikalar da aynı zamanda bir fikir birliği oluşturmak ve bir durum değişikliği gerçekleştirildikten sonra durumu bütün olarak kabul etmek için birbirleriyle iletişim kurmaktadır. Blok zinciri tabanlı bir sistemde paylaşılan durum, blok zincirini oluşturmaktadır ve durum geçiş kuralları, blok zinciri protokolünün öngördüğü kurallardır. Prensip olarak dağıtık bir modelde katılımcıların her zaman hemfikir olması beklenemez. Mutabakat işlemleri için geliştirilen algoritmalar, işlem mesajlarındaki olası sorunlar ve gecikmeler ile düğümlere ve ağda gerçekleşebilecek problemlere karşı dayanıklı olmalıdır. Ayrıca kasten kötü amaçlı işlem gerçekleştirmeye çalışan düğümlerle mücadele etmek zorundadır. Her algoritma, senkronizasyon açısından gereklidir (Karaköse, 2017, s. 47).

Protokole bağlı olarak oluşabilecek risklerden biri çoğunluklu saldırıdır. Bitcoin örneğinde çoğunluklu saldırı, genellikle %51 atağı ya da > %50 atağı olarak da bilinmekte olup ağa yapılan bir saldırıyı ifade etmektedir (bitcoin.it, 2017). Bitcoin ağının yarısından fazlasının iyi niyetli olmayan madencilerin eline geçmesi durumunda ortaya çıkan bir risk olan çoğunluk atağının başarılı olma ihtimali %100'e yakındır (Çarkacıoğlu, 2016, s. 41).

Dağıtık kayıtlarda güvenilmez aktörlerin isleyişe zarar verme riski mevcuttur. Bir bilgisayar ağı üzerinde işlem gerçekleştirenler bu işlem esnasındaki karşılıklı veri akışı sırasında bir ağ protokolünü kabul ederler. Güvenilirliği sağlamak için, dağıtık kayıt teknolojileri Bizans generalleri problemi olarak bilinen bu sorunu çözecek şekilde tasarlanmalıdır. Merkezi bir düzenleyicinin olmadığı blok zinciri yapılarında bu durum daha da önem kazanmaktadır. Blok zincirini bu kadar güçlü kılan olguların başında, fikir birliğine dayalı işlemleri meşru kılma kabiliyeti gelmektedir.

Blok zincirinde mutabakatın verimli bir şekilde sağlanabilmesinin akraplanında üç ana parametre bulunmaktadır.

- Güvenlik: Sistemde konuşlu tüm düğümlerin senkronize ve tutarlı olması ile ancak güvenli işlemler gerçekleştirilebilir.
- Canlılık: İşlemler tüm düğümlerin dahil olduğu kabul edilen, prensip olarak dinamik süreçler ile yerine getirilmektedir.
- Hata Toleransı: kısıtlı da olsa yanlış gerçekleştirilmiş işlemlere ilişkin bir müdahale olanağı sunmaktadır.

Bir düğüm, kanıtını bulduktan sonra, kanıtı blokla birlikte yayınlamaktadır. Artık diğer tüm düğümlerin, yalnızca sağlanan kanıtın doğruluğunu, doğrulamak için bir işlem özeti hesaplaması yeterlidir. Doğrulamadan sonra blok, blok zincirine dahil edilir. Diğer her düğüm artık yaptıkları işi terk edebilir ve yeni işlemler yapmaya başlayabilirler. Bu şekilde protokol sayesinde mutabakat sağlanabilmektedir. Bir örnek ile Bitcoin sisteminin mutabakat protokolünde;

- Gerçekleştirilen tüm kayıtlar her düğüme yayınlanır.
- Bütün düğümler, gerçekleştirilen işlemleri ayrı bloklarda tutar.
- Periyotlarla rasgele belirlenen düğümler kayıtlarını paylaşmaktadır.
- Ancak doğruluğu ve güvenilirliği onaylanmış işlemler bloklara yazılır.
- İşlem bloklarının birbirine eklemlenmesinde önceki blok sonraki bloğa bir özet bilgi ile eklemlenir (Karaköse, 2017).

1.1.4. Blok Zincir Çeşitleri

Blok zinciri teknolojisinin altyapısını kullanan üç farklı türde blok zincir modeli bulunmaktadır. Bunlar; Genel, Özel ve Konsorsiyum Blok Zincirleridir.

1.1.4.1.Genel Blok Zincirleri

Bir genel blok zincirini, dünyadaki herhangi bir kişi okuyabilmekte, işlem yapabilmekte, yapılan işlemin geçerli olması durumunda sonuçlarını görebilmekte ve uzlaşma sürecine (mevcut durumun ne olduğu ve hangi blokların zincire ekleneceğinin belirlenmesi sürecine) katılabilmektedir. Kimseye erişim kısıtlaması yapılmamaktadır. En gelişmiş ve en çok bilinen genel blok zincirlerine örnek olarak Bitcoin ve Ethereum verilebilir (Tikveşli, 2019).

1.1.4.2.Özel Blok Zincirleri

Özel blok zincirinde ağa katılacak ve onay işlemi yapacak kişilere izin verilmesi gereklidir. Ağ yöneticileri tarafından davet edilmedikçe katılım sağlanamayacaktır. Hassas verileri, herkese açık olan bir yapıda riskle karşı karşıya bırakmamaktadırlar. Herhangi bir muhasebe mevzuat sistemine ve resmi kayıt işleme prosedürlerine bağlı olmadan kendi içerisinde kayıt tutmaya çalışmaktadırlar.

1.1.4.3.Konsorsiyum Blok Zincirleri

Bir konsorsiyum blok zincirinde ağa katılacak kişilere izin verilmesi gereklidir. Fakat bunu, özel blok zincirindeki gibi tek bir kuruluş kontrol etmez. Ortak yapıya dahil olan her şirket, ağ üzerinde bir düğüm işletebilmektedir. Konsorsiyum blok zincirinde, zincirin yöneticileri tarafından kullanıcıların okuma hakları kısıtlanmaktadır ve az sayıda güvenilir düğümlerin bir konsorsiyum protokolü işletmesine izin vermektedir (Tikveşli, 2019).

1.1.5. Blok Zincirinin Avantajları

Çalışma yapısı itibariyle blok zincirinin birçok avantajı bulunmaktadır. Tamamen dağıtık olması, yüksek erişilebilirlik imkânı sunmakta ve DDOS saldırılarına karşı sistemi dayanıklı kılmaktadır. Dağıtık ve şeffaf yapı, aynı zamanda, merkezi kontrol yapıları bulunmayan sistemler kurulmasına olanak sağlamakta, bu da sistemlerde kişi ve kurumlara güvenme gereğini ortadan kaldırmaktadır. Zincir yapısı sayesinde ise verinin bütünlüğü sağlanmaktadır. Eski bir veriyi değiştirmek, tüm zincirin yeniden oluşturulmasını gerektireceğinden, oldukça zordur. Bu durum sistemi oldukça güvenilir kılmaktadır. Bloklarda depolanan verilerin güvenilir ve tüm

katılımcılara açık olması kontrol edilebilirliği desteklemektedir. (Gültekin, 2019, s. 31).

1.1.6.Blok Zinciri Dezavantajları

Her altyapı ve sistemde olduğu gibi, blok zincirinin de bir akım dezavantajları bulunmaktadır. Dağıtık olması sebebiyle, her bir madenci doğrulama işlemlerini yapması gerekmekte ve bu da aynı işlemin farklı bilgisayarlarda tekrarı manasına gelmektedir. Bu tekrar, güç tüketimini arttırmaktadır. Farklı fikir birliği yöntemleri ile güç tüketimi azaltılsa da, doğrulamanın tekrar tekrar yapılmasının önüne geçecek bir yapı kurulamamıştır. Dağıtık olması aynı zamanda sistem oluşturulmasını ve kurulumunu, merkezi yapılara göre daha zor kılmaktadır. Bu durum, sistemde yapılacak güncellemeleri de zorlaştırmakta ve verinin çatallanmasına sebep olabilmektedir (Gültekin, 2019, s. 32).

1.2. KRİPTO PARA TEKNOLOJİSİ

1.2.1. Para Kavramı

Para, her türlü mal ya da kıymetin el değiştirmesine olanak sağlayan bir araçtır. Ayrıca öteden beri kullanılan, genel değişim aracıdır. Bu özelliği ile ekonomik ve ticari işlemlere taraf olanların çeşitli düzlemlerde buluşarak bu işlemleri gerçekleştirmelerine imkân sağlamaktadır. Paranın yaratılması devletlerin tekelindedir ve ülkelerin değer ölçüleri birbirinden çok farklı olabilmektedir. Paranın herkes tarafından kabul gören ortak bir değer ölçüsü olmasının en önemli nedenlerinden biri de merkezi bir otoritenin ürünü olmasından kaynaklanmaktadır. Para tüm bu özelliklerine ek olarak en çok tercih edilen yatırım ve tasarruf araçlarından biridir.

Sekmen,'e göre para, bir iktisadi varlığın el değiştirmesi esnasında herkes tarafından yaygın olarak kullanılan bir değer veya bir borcun ifasını yerine getiren bir araçtır (Sekmen, 2012, s. 15). Özbilen ise parayı, insanlar tarafından mal ve hizmetlerin değişim aracı olarak gördüğü ve güvenle bu işlemlerini gerçekleştirdiği her şeyi para kadul etmektedir (Özbilen, 2015, s. 1). Parasız 'a göre de para, mal ve hizmetlerin piyasa faaliyetlerinde ve borçların ifasında bir ödeme aracı olarak herkes tarafından kabul gören nesnelerdir (Parasız, 1996, s. 63). Bir şeyi para yapan, değişim aracı fonksiyonu katan özellik onun, herkes tarafından kabul görmesi ile ilgilidir. Bir

başka bir ifadeyle paranın bir birikim aracı olarak tercih edilmesinin, paranın likit bir varlık olması sebebiyledir (Aren, 2007, s. 244).

1.2.1.2. Paranın Türleri

Mal Para, Takas döneminde alışverişe konu olan varlıkların karşılıklı mübadele edilmesi sürecinde kullanılan paradır. Madenlerin yaygın olarak kullanıldığı dönemlerde sikke olarak kullanılmıştır.

Kıymetli madenlere dönüştürülebilen paralar temsili para olarak tanımlanır. İlk kullanıldığı dönemlerde temsili paralar, tam olarak altına çevrilebilme özelliğine göre sikkeler şeklinde kullanılsa da zamanla yerini kâğıt paralar almıştır. Bir başka ifade ile bir kıymetli madene oranla karşılık olarak üretilerek yeniden üretildiği madene geri çevrilebilen paralar olarak kullanılmıştır. Günümüzde hali hazırda sözü edilen kâğıt formlu paralar dolaşımdadır. Bu tanımlamalardan hareketle temsili para olarak ifade edilen değer ölçü birimlerini altı başlık altında açıklamak mümkündür.

Altın ve gümüşün doğrudan bir değer değişim aracı olarak tercih edildiği devirlerde bankerler, taşıma ve muhafaza sorunlarını bertaraf etmek için altın ve gümüşe karşılık olarak sertifikalar vermişlerdir. Bu sertifikalar temsil ettikleri para yerine değişim aracı olma işlevini yerine getirmişler, böylelikle ilk temsili para ortaya çıkmıştır. Sertifika olarak adlandırılan bu belgelerin en temel özelliği, bu kağıtları ihraç eden kurumun kasasında karşılık olarak %100 oranında değerli maden bulundurulmasıdır. Altın ve gümüş gibi değerli madenlere karşılık olarak sertifika veren bankalar, emanet edilen değerli madenlerin zamanla büyük bir bölümünün bir daha geri istenmediğini tecrübe ettiler. Sonrasında bankalar borç talep edenlere, para yerine sertifika verdiler. Böylelikle herhangi bir karşılığı olmayan, fakat istenildiği vakit değerli bir madene çevrilebilen belgeler icat edildi. Banka notu olarak adlandırılan bu belgeler başta tüm bankalar tarafından verilmekteydi. Ancak, sonrasında yaşanan birtakım olumsuzluklara çözüm olarak sadece merkez bankaları banknot çıkartma göreviyle yetkilendirildi. Devam eden süreçte merkez bankaları, banknotları altın veya gümüşe çevirmek yerine banknotla değiştirmişlerdir.

Küçük ve küsuratlı işlemlerin kolaylıkla gerçekleştirilebilmesi amacıyla bir miktar banknota denk bir değerde madeni paralar basılmıştır. Madeni paraların fiziki

değeri, nominal değerinin elli katı olarak belirlenmiştir. Ülkemizde madeni paraları Hazine, banknotları ise Türkiye Cumhuriyet Merkez Bankası basar.

Bir diğer para türü de ödeme işlemlerinde kullanılan kaydi veya banka parası şeklinde ifade edilen banka mevduatlarıdır. Bu paranın üretimi mudilerin parasal varlıklarını vadesiz mevduat hesaplarına yatırmasıyla gerçekleşmektedir. Nakit kullanımına göre daha kolay olan kaydi paralarda ödemeler; çek, virman ya da kredi kartıyla yapmaktadırlar.

Bunların dışında para yerine geçen ve finansal işlemlerin çeşitlenmesi sayesinde fiziki bir para olmaksızın bu işlemlerde kolaylıklar sağlamakla birlikte çokça da tercih edilen kredi kartları gibi ödeme araçları da bulunmaktadır.

1.2.1.3. Paranın Kısa Tarihçesi

Paranın icadına kadar, deniz kabuğu, kıymetli metaller gibi birçok nesne değişim aracı olarak kabul edilmiş ve kullanılmıştır. Bazı kaynaklarda, M.Ö. 118 yılında Çinlilerin deri para kullandıklarına dair tarihi kayıtlar mevcuttur. Tarihte yine kâğıt parayı ilk kullanan Çinliler olmuştur (TCMB, 2018, s. 2).

Öztürk'e göre para doğası itibariyle iktisadi, gündelik ilişkilere araç olması itibariyle Sosyal, üretimi ve merkezi otoritelerle olan organik bağı sebebiyle de siyasal bir olgu olarak değerlendirilmektedir (Öztürk, 2016, s. 5). Paranın ortaya çıkmasında yine insanların ihtiyaçlarını temin etme güdüleri etkili olmuştur. Geçmişte, bulundukları coğrafyaya ve şartlara göre toplayıcılık ya da avcılıkla geçimlerini sürdüren insanlar, ihtiyaçlarını kendi ürettikleri ihtiyaç fazlası ürünler ile takas yaparak temin etmekteydi. Bu yöntemin işlerliği alıcı ve satıcı tarafın sahip oldukları ürünlere karşılıklı ihtiyaç duymaları durumunda ancak geçerli oluyordu. Örneğin buğday üreten bir kimse kumaşa ihtiyacı olduğunda, kumaş üreten kişinin de buğdaya ihtiyacı olması durumunda mübadele gerçekleşebiliyordu. Takas sistemindeki bir diğer ve en önemli sorun ise takasa konu malların karşılıklı değer tespitlerinin yapılamıyor olması ayrıca takasına ihtiyaç duyulan malların her an elde hazır bulundurulamamasıdır. Tüm bu sorunlara çözüm olarak dünyanın farklı yerlerinde birçok farklı meta değişim aracı olarak kullanılmıştır. Örneğin, Hindistan'da denize kıyısı olan bölgelerinde deniz kabuğu, değer ölçüsü olarak kullanılmıştır (Ercan, 2005, s. 126). İlk başta uygulanan

malların başka bir mal ile takası tarihsel süreç içerisinde malların para ile alınıp satılmasına evirilmiştir (Berber ve Bocutoğlu, 2014, s. 221).

Tarihte ilk madeni paranın Anadolu'da yerleşik olan Lidya'lılar tarafından M.Ö VII. yüzyılda yapıldığı bilinmektedir. Lidya parası, bu manada bilinen en eski örnektir. Böylelikle insanlık tarihinde zengin ve köklü uygarlıklara ev sahipliği yapan Anadolu ilk paranın üretimine de şahitlik etmiştir. Anadolu medeniyetlerinin ulaştığı sosyo-kültürel seviye itibariyle önemli bir göstergedir. Ayrıca tarihte para basmak üzere kurulan ilk büyük darphane İstanbul'da Fatih Sultan Mehmet döneminde kurulmuştur ("Paranın tarihi", 2019).

Batıda kâğıt paraların günlük hayattaki yerini alması 1600'lü yılların sonlarına denk gelmektedir. Bu manada batıdaki ilk kâğıt paranın 1690'larda Massachusetts Hükümeti tarafından ABD'de çıkarıldığı bilinmektedir. İngiltere'de il başta kuyumculuk faaliyeti yürüten sarraflar tarafından basılarak tedavüle giren kâğıt paralar, 1694 yılında İngiliz Merkez Bankası tarafından basılmaya başlanmıştır. Bu tarihlerden sonra diğer ülkelerde de merkez bankalarının kurulması ile kâğıt paraların yaygınlaştığı görülmektedir.

1.2.1.4. Paranın Özellikleri

Bir nesnenin iktisadi olarak para sıfatıyla işlem görebilmesi için onun herkes tarafından genel bir kabul görmesinin yanı sıra bir değer ölçüsü ifade etmesi, değişim, değer biriktirme ve tasarruf aracı olması gerekir (Berber ve Bocutoğlu, 2014, s. 223). Bu bağlamda günümüzde devletlerin varoluş gücünün bir nevi simgesi olan geleneksel genel kabul görmekte ve kullanılmaktadır.

Para standart olarak üretilmez ise yaygın bir kullanım alanı bulamaz. Piyasadaki aynı miktarı ifade eden tüm paralar şekli ve özellikleri itibariyle standart nitelikte olmalıdır. (Günal, 2012, s. 9).

Paranın kullanılabilirliğini etkilen başka bir özellik de bölünebilir olmasıdır. Alışveriş işlemlerinde kullanılırken ya da alacak ve borç ödemelerinde işlemlerin eksiksiz ve kolay olarak yapılabilmesi bölünebilirlik mutlak gereklidir (Öztürk, 2016, s. 210). Mal paranın kullanıldığı zamanlarda paranın bölünememesi sorun yaratmaktaydı. Madeni ve kâğıt paraların günlük hayatta yer bulmasıyla birlikte bu

sorun çözüm bulmuştu. Alışveriş sonrası olası para üstü ya da büyük meblağlar problem olmaktan çıkmıştır. (Öçal, Çolak, Togay ve Eser, 1997, s. 8).

Paranın fiziki transferinin makul ve bir yerden bir yere taşınması kolay olmalıdır. Takas sistemlerinde, takasa konu olan malların taşınması zahmetli ve görece çok daha maliyetliydi. Sonraları kullanılan altın ve gümüş gibi paraların nakledilmesi farklı sorunlarla anılmaktaydı. Taşıma esnasında çalınma kaybolma gibi olumsuz durumlar oldukça yaygın ve büyük kayıplar meydana getirmekteydi. Tüm bu tecrübelerden hareketle günümüzde artık kâğıt paraların dahi yerini alan çek, kredi kartları gibi araçlar almıştır. Paranın daha kolay taşınmasında çokça tercih edilen bir yöntem haline gelen bu araçlar, taşınabilirlikle ilgili sorunları ortadan kaldırmışlardır (Öztürk, 2016, s. 27).

Para olabildiğince yıpranma ve aşınmalara karşı da dayanıklı olmalıdır. (Özbilen, 2016, s. 4).

Kâğıt ve madeni paralar, kolay ve basit yöntemlerle kopyalanamamalıdır. Parayı tedavüle hazırlayan kurumlar taklit edilmesini önlemek için birtakım önlemler geliştirmelidir (Öztürk, 2016, s. 27). Buna rağmen eski tarihlerden günümüze kalpazanlar parayı ve güvenlik önlemlerini taklit etmeye çalışmışlardır. (Özbilen, 2016, s. 5). Paranın taklit edilmesinin piyasaya olumsuz etkileri olmaktadır. Sahte paranın piyasadaki varlığı miktarıyla orantılı olarak parayı basan kuruluşun ekonomik kaybına ve enflasyonun tırmanmasına neden olmaktadır. Ekonomik sistemin sağlıklı çalışabilmesi için piyasanın işlem hacmi ile orantılı para bulunmalıdır. Ekonomilerdeki büyümeyle paralel piyasada bulunan paranın da artması olağan kabul edilmektedir. Diğer taraftan piyasa ihtiyacının üzerindeki paranın varlığı paranın değerini düşürerek, enflasyona sebep olmaktadır (Kesbiç, 2004, s. 28).

Paranın değişim fonksiyonunu yerine getirebilmesi değerinin çok fazla değişmemesiyle doğrudan ilgilidir. Paranın değerini koruması hatta değerinin uzun vadede artması arzu edilmektedir. Örneğin bugün 1 birim olan bir malın değeri gelecekte de 1 birim olması ya da paranın değerinin artması beklentisi ile daha ucuz bir fiyata erişilmesi ile açıklanmaktadır. (Berber ve Bocutoğlu, 2014, s. 223).

Para bir otoritenin bağımsızlık sembolüdür. Paranın yasal olarak kabul edilebilirliği bir kanuna dayalı olarak çıkarıldığında mümkün olmaktadır. Ancak yasal

şekilde çıkarılan para herkes tarafından kabul görür ve borç ödeme özelliğine sahip olur (Öztürk. 2017, s. 8).

1.2.2. Kripto Para Kavramı

1.2.2.1. Kripto Paranın Tanımı

Yeni bir teknolojik yenilik olarak bu paralara ait bir tanımlama yapmadan önce bu paraların yaratılmasındaki altyapı özelliği olan kriptoloji kavramının açıklanmasında yarar vardır. Küresel çapta hızına yetişmekte zorlandığımız bir şekilde gelişme gösteren iletişim teknolojileri birçok faydayı beraberinde getirmekle birlikte bazı sorunları da beraberinde getirmektedir. Dijital mecralarda gerçekleştirilen her bir işlemin güvenli bir şekilde yürütülememesi bu ortama olan güvenin azalmasına endişelerin artmasına neden olmaktadır. İşte tam da bu problemlere bir çözüm öneri olarak ortaya çıkan kriptoloji dijital mecralarda gerçekleştirilen işlemlerin güvenli bir şekilde yapılması için kullanıcısı haricinde erişimi engelleyen bir devrim olarak karşımıza çıkmaktadır (Yılmaz, 2007).

Brassard'a göre (1988), kriptoloji güven algısının olmadığı alanlarda güvenli iletişimi mümkün kılan bir bilim hatta sanat olarak tanımlamaktadır. Kriptoloji, bir mesajdan oluşan verilerin belirli bir sistematik içerisinde şifrelenerek, emniyetli bir ağ kanalıyla yollanması, iletinin sadece muhatabı tarafından çözümlenmesiyle neticelenen akıştır. Kriptoloji, en damıtılmış şekliyle bir şifreleme disiplini olarak da ifade edilebilmektedir. Sayın'a (2017) göre, kriptolojiyi; veriye ilişkin güvenliğinin ve bütünlüğünün sağlanması ile kimlik denetiminin gerçekleştirilmesi olmak üzere üç temel fonksiyonu içerdiğini belirtmektedir.

Kripto para güvenli işlem gerçekleştirmeyi garanti eden, fiziki niteliği olmayan, ancak bir ağ üzerinde kullanılabilen alternatif bir paradır. Burada bir noktanın altını çizmekte fayda vardır; dijital ya da sanal paralar sıklıkla Bitcoin ve altcoinlerle karıştırılmaktadır. Bitcoin ve altcoinler başlı başına ayrı birer para birimleridir. Bu özelliklerinden dolayı hiçbir devletin müdehalesi ya da denetimi altında değildirler. Kripto paraların haricinde dijital ve sanal paralar, müstakil birer birimi ifade etmemektedir (Çarkacıoğlu, 2016, s. 8).

Kripto paraların denetimi blokzinciri altyapısı ile sağlanmaktadır ve henüz tasarım aşamasındayken bir dizi şifreleme sistemleri yardımıyla bir kota dahilinde

kurgulanmaktadır. Daha en başında dolaşıma girecek olan para miktarı ve arz olma şekli ile buna ilişkin zamanlama belirlenmiştir. Fakat klasik paranın kontrolünü elinde bulunduran devletler ve onların uzantıları olan merkez bankaları ihtiyaç duymaları halinde piyasaya yeni para ihraç edebilirler. Ne var ki kripto para üretemedikleri gibi bunların sahiplerinin rızası olmadan kripto varlıklarına el dahi koyamazlar. Geleneksel para birimlerine bağlı olarak çıkarılan ve kriptografik bir fonksiyonu bulunmayan elektronik paralarda ise saklama, transfer vb. diğer işlemlerde merkezi nitelikte üçüncü bir kurum bulunmaktadır. Aslında ifade edilen bu üçüncü kurum, gerçekleştirilen işlemlerin güvenli bir şekilde devamında ve ihtiyaç halinde doğruluğunun ispatlanmasından sorumludur. Oysa ki kripto para sistemlerde aracı bir mekanizmaya ihtiyaç yoktur. (Ateş, 2016, s. 356).

1.2.2.2. Kripto Paraların Geleneksel Paradan Farkı

Geleneksel paranın basılması, dolaşımının sağlanması, dönem dönem sirkülasyonunun sağlanması gibi birçok mekanizmaya ihtiyaç duymaktadır. Ek olarak çoğu zaman gerçekleştirilmek istenilen varlık transferlerinde aksaklıklar yaşanmaktadır. Örneğin çok kısa zaman dilimlerinin hayati olduğu bazı fon transferlerinde gecikmeler yaşanabilmektedir. Ayrıca bu gibi işlemler için yüksek komisyonlar talep edilmektedir. Kripto para sistemlerinde katılımcılar gerçekleştirdiği işlemlerde herhangi bir üçüncül denetime ihtiyaç duyulmamaktadır. Bu fonksiyon P2P fonksiyonuyla yerine getirilmektedir. Diğer taraftan geleneksel finansal hizmet süreçlerinde yüksek aracılık ücretleri talep edilmektedir. Eğer bu fon transferi işlemi bir yurtdışı gönderimi ise fahiş komisyonlar söz konusu olabilmektedir. Buna karşılık olarak olarak, kripto paraların global transfer maliyeti kâğıt parayla kıyas bile edilemez oranda düşüktür.

Günümüz şartlarında kısa ya da uzun mesafeli seyahatlerde nakit bulundurmak hemen hemen bir zorunluluktur. Yurtdışı seyahatlerinde insanlar paralarını seyehat ettikleri ülkenin yerel para birimine dönüştürmek ihtiyacı hissetmektedirler. Bu durum bazen eşitli zorluklar yaşamalarına neden olmaktadır. Kripto paralar bir dizi şifreden ibaret oldukları için fiziksel olarak taşınmasını gerektirecek bir kütleye sahip değildir. Bu nedenle kripto paralarla işlem gerçekleştirmek için sadece internet bağlantısının olması yeterlidir. Kripto altyapılar

sağlamış oldukları yüksek güvenlik düzeyi ile gelecekte ödeme sistemlerinin temelini oluşturma konusunda benzersiz özellikler taşımaktadır. Birçoğuna göre dijital bir hesaba sahip olmak siber tehditler için yeterli bir neden olarak algılanmaktadır. Günümüzde bankalar ve mobil uygulamaları finansal işlemler için en güvenli seçenek olarak değerlendirilse de bankacılık sistemleri de kimi zaman siber saldırıların kurbanı olabilmektedir. Her ne kadar merkezi yapılar hatta devletler kripto para teknolojisini kendilerine bir tehdit olarak algılasalar da kripto paralar yüksek güvenlik gerektiren finansal işlemleri hızlı ve en uygun maliyetler ile gerçekleştirmeleri sebebiyle, geleceğin para birimleri olarak hızla varlıklarını kabul ettirmektedirler. Her geçen gün çok daha ilgi uyandıran bu kolaylıklar alışkanlığa dönüştükçe daha da fazla insan tarafından tercih edileceği gerçeği göz ardı edilmemelidir.

1.2.2.3. Kripto Paraların Doğuşu

Popüleritesini Bitcoin para biriminin ortaya çıkmasıyla yakalayan kripto paralar, Satoshi Nakamoto anonim adıyla bilinen yazarın 2008 yılında, "*Bitcoin: A Peer-to-Peer Electronic Cash System*" başlığı ile yayınladığı manifesto niteliğindeki çalışmasıyla ilk ortaya çıktı. Nakamoto, blok zinciri teknolojisinin altyapısını kullanılarak ürettiği Bitcoin para birimini dünya ile paylaştı. Bu gelişmeyi 2009 yılının hemen başında ilk açık kaynaklı Bitcoin işlemcisinin ve ağının kurulması seyretti. Teoride klasik 1'ler ve 0'lardan teşkil edilmiş ve kompleks problemlerin çözülmesiyle üretilen ilk Bitcoin bloğunu da yine Nakamoto üretmiştir. Bitcoin ile gerçekleşen ilk işlem ise Satoshi Nakamoto ile bir programcı olan Hal Finney arasında gerçekleşti. Devrim niteliğinde olan bu gelişme ile hiçbir aracı üçüncü kişi olmaksızın maddi bir değer ölçütü bir kullanıcıdan diğerine aktarılmıştı; üstelik bir devletin denetimi olmaksızın. Bütün bu gelişmeler kitleler tarafından ancak yıllar sonra kabul gördü ve Bitcoin ortak bir değer ölçütü olarak günlük yaşamdaki yerini aldı. Bitcoin para birimine süreç içerisinde gösterilen rağbet sonrasında Etherieum adından söz ettirmeye başladı. Bitcoin ve Etherieum'u takiben ar arda gelen kripto para birimleri, şifreli para sisteminin ardındaki blok zincir teknolojisini bir anda gündem haline getirdi. Geçmiş birkaç yıl içerinde de "*bitcoin çatallanması"* olarak da anılmakta olan "*fork*" fenomeni yeni bir trend oluşturdu. Bunun nedenini olarak madencilik

anlamında Bitcoin'in teknik açıdan kapasite sınırlarına ulaşması önemli bir rol oynadı ve sonucunda Bitcoin fork fonksiyonuyla ikiye ayrıldı (Şenel, 2019, s. 27).

Hard fork işlemi sonucu klasik Bitcoin (BTC) devam ederken, Soft fork işlevi ile birlikte Bitcoin Cash (BCH) adıyla yeni bir para birimi ortaya çıktı. 2015 yılına gelindiğinde Vitalik Buterin tarafından Etherium yaratıldı. Etherium birimi kripto para dünyasına "Akıllı Kontrat" olarak adlandırılan yeni bir kavramın gün yüzüne çıkmasıa sebep olmuştur. Etherium sahip olduğu teknik altyapı sayesinde farlı programlama dillerini kullanarak yeni kontrat, coin ve token üretimine imkân vermektedir (Şenel, 2019).

1.2.2.4. Kripto Paranın Sınıflandırılması

Bugün kullanılmakta olan ve her geçen gün yenileri eklenen çok sayıda kripto para bulunmaktadır. Kripto para kavramıyla özdeşleşen Bitcoin ve pek çok sayıda alternatifin ana özelliklerini ele alındığında, Bitcoin ve ona alternatif Altcoin'lerden her biri için ayrı ayrı bir değerlendirme gerekmektedir. Avrupa Parlamentosu Vergi Komitesinin hazırlamış olduğu "Cryptocurrencies and Blockchain" adlı çalışmasına göre, kripto paralar, Bitcoin ve Altcoin olmak üzere sınıflandırılmaktadır. Altcoinler de kaynak protokolü açısından ikiye ayrılmaktadır. Bunlardan ilki, Bitcoin'in orijinal açık kaynak protokolü kullanılarak oluşturulan ve altta yatan kodları farklı özelliklerle oluşturulan yeni bir para olan Litecoin'dir. İkinci tür ise, Bitcoin'in açık kaynak protokolüne dayanmayan, ancak kendi protokolüne sahip bir şekilde yayılmış defterlerin oluşturduğu yeni bir platform olan bu Altcoin'lerin iyi bilinen örnekleri Ethereum ve Ripple'dır (Houben ve Snyers, 2018).

1.2.2.5. Kripto Paraların Ortak Özellikleri

Değer aracı olarak birçok alternatifin bulunduğu günümüzde, kripto paraların öne çıkan özellikleri nedeniyle tercih edildikleri görülmektedir. Bu özelliklere yakından bakıldığında, onu diğer değer transfer araçlarından farklılaşan unsurları şu şekilde sıralanabilir:

- Taşınabilirlik

Geleneksel paralara göre, kripto para birimleri çok daha kolay ve ucuz maliyetlerle; bilgisayarlar, tabletler ve hatta akıllı telefonlar gibi çevrimiçi araçlar

kullanılarak bir hesaptan diğerine aktarılabilmektedir. Geleneksel para birimlerinde, bunu fiziksel olarak veya aynı banka aracılığıyla yapmak gerekmektedir. Ayrıca, kripto paralar fiziksel olarak taşımayı gerektirmemektedir. Çünkü bu paralar sanal ortamda saklanmaktadır. Bu sayede, bir İnternet bağlantısı ile her yere transfer edilebilir ve miktardan bağımsız olarak taşınabilmektedir.

- Daha İyi Değer Depolama

Bir değer aracı, ancak zaman içinde fayda veya memnuniyet seviyelerini koruyabiliyorsa, iyi bir değer depolama aracı olarak değerlendirilebilmektedir. Bunu finansal varlıklara uygulamak, zaman içinde satın alma gücünü koruyabilme anlamına gelir. Bir finansal varlığın değer tutma yeteneği, böyle bir varlığın hem nicel hem de nitel yönlerini dikkate alan temel analiz olarak adlandırılan yöntemle tahmin edilir. Değeri saklama yeteneği, Bitcoin, Ethereum ve diğerleri gibi kripto para yatırımları için temel işlev haline gelmiştir.

Kripto para birimlerinin kripto para birimlerinin uzun vadede değer saklama yeteneğini haklı çıkarırken değerli metallerle karşılaştırıldığında benzer metallere benzediği değerlendirilebilir. Bitcoin ve altcoin'ler uzun vadede değer muhafaza yeteneğine ilişkin genel bakış açısını etkileyebilecek çok güçlü bir faktör olabilir.

- Sınırlı Miktar

Tıpkı fiziksel formdaki altın gibi, Bitcoin gibi kripto para birimleri tipik olarak blok zinciri protokollerinde tanımlanan sınırlı miktarda birime sahiptir. Örneğin Bitcoin için, yaratılabilecek sadece 21 milyon birimlik bir kotaya sahiptir. Öte yandan Litecoin, çalışma protokolleri tarafından kontrol edilen 84 milyon adet üretilebilecektir. Kripto para birimlerini uzun vadede deflasyonist bir özelliğe sahiptir.

Kripto para birimlerinin, her geçen gün üretilebilecek üretilebilecek cevher kapasitesi daralmaktadır. Bu durumda kripto paraların uzun vadede satın alma gücünün artması anlamına gelmektedir. Bir diğer ifade ile mallar ve hizmetler üzerinde deflasyonist etkilere sahip olabileceği anlamına gelmektedir.

- Diğer Varlık Sınıflarından Bağımsızlık

Merkezi bankalar veya finansal kurum ve kuruluşlar tarafından yapılan açıklamalara veya spekülatif etkilere paralel, değerleri dalgalanan hisse senedi veya faiz oranları gibi diğer tüm finansal varlık sınıflarıyla karşılaştırıldığında, altın ve

gümüşün gerçek değeri, herhangi bir merkezi para otoritesi tarafından manipüle edilemez veya oldukça sınırlı oranda etki edilebilir. Herhangi bir para otoritesinden doğası gereği bağımsız olan, altın ve gümüş gibi değerli metaller zaman içinde fiyat şoklarına dayanabilir. Bu da onları uzun vadede çok iyi değer saklama araçları konumuna getirmektedir. Kripto paralarda da merkezi bir yapının olmaması onları benzer etkiler karşısında pozitif ayrıştırmaktadır. Ancak genel olarak, merkezi olmayan sistemlere sahip kripto para birimleri, değerlerinin düzenleyiciler tarafından etkilenmesi veya kurcalanması riskine karşı çok daha düşük risker barındırmaktadır.

- Temel veya İç Değerler

Gerçek değer depoları olarak kabul edilen varlıklar, değerleri için temel oluşturan kimi özelliklere sahiptir. Layman'ın terimleriyle, bu tür varlıkların içsel yarar değerleri vardır. Örneğin altın bazı yarı iletken elektronik parçaların üretiminde kullanılır. Arazi ya da gayrimenkulün temel değeri, üzerlerine yapılar inşa etme kapasiteleri gibi faydalarla da iliştilidir. Bu açıklamadan hareketle fayda değeri söz konusu olduğunda, kripto para birimlerinin potansiyeli çok yüksektir. Özellikle, kripto para birimleri, sözleşmelerin uygulanması, kayıtların tutulması ve ödemeleri içeren finansal işlemlerin çevrimiçi olarak yapılma şeklini değiştirme konusunda büyük bir vaatte bulunmaktadır. Bitcoin, Litecoin ve Ether gibi kripto para birimlerinin kullanımı giderek daha fazla pazarda kabul edildikçe, pratik fayda değerleri daha da arttıracaktır.

- Taklit Edilemezlik

Blockchain teknolojisi, çevrimiçi işlemleri gerçekleştirmek, verileri veya kayıtların depolanmasını kolaylaştırmak açısından devrim niteliğinde bir teknolojidir. Onu devim olarak tanımlamanın gerekçelerinden biri de, sahte versiyonlarını üretmenin neredeyse imkânsız olmasıdır. Blok zincirleri gelişmeye devam ettikçe, bir şey satın almak için kullanılabilecek sahte kripto para birimlerini üretmek çok daha imkânsız hale gelmektedir.

- Müdahale Edilemezlik

Özellikle Bitcoin ve Ether gibi kripto paraların piyasa değeri bugün milyarlarca dolar değere ulaşmıştır. Bu tür kripto para birimlerinin sadece fiyatlarını etkilemek veya manipüle etmek için devasa miktarda paraya ihtiyaç olacaktır.

Sözgelimi ortalama piyasa değeri yaklaşık 50 milyar ABD Doları olan Bitcoin arz-talebini manipüle edebilmek için, en az 10 milyar ABD Doları'na ihtiyaç vardır. Ortalama piyasa değeri 25 milyar ABD Doları düzeyinde seyreden Ether'i için, fiyatları lehe çevirebilmek için birkaç milyar dolar değerinde işleme ihtiyaç duyulmaktadır.

- Manipüle Edilemezlik

Hisse senetleri gibi nispeten yüksek miktarda yatırım sermayesi gerektiren diğer finansal varlıkların aksine, kripto para birimlerine giriş kısıtlılıkları düşüktür. Bu, yatırım yapmak için nispeten az miktarda paraya sahip olan kişilerin bile kolayca bu varlıklara sahip olabileceği anlamına gelmektedir. Bu nedenle, yatırımcıların kripto para birimleri piyasasını manipüle etmesi neredeyse imkansızdır.

- Göreli Güvenlik

Son olarak, kripto para birimlerinin çalınması neredeyse imkansızdır. Kripto para birimlerinini saldırılara karşı güvenli hale getirmek, ucuz ve çok kolaydır. Belli başlı yöntemlerin yanında biraz özen sayesinde bu varlıkların çalınması neredeyse imkânsız hale getirilebilmektedir.

1.2.2.5.1. Açık Kaynaklı Kodlama

Blockchain açık kaynaklı bir teknoloji olduğundan, yazılımı herkes tarafından çalıştırabilmektedir. Söz gelimi, herhangi bir kripto para birimini satın almak, yatırım yapmak istenildiğinde blockchain tabanlı bir yazılım çalıştırarak blockchain topluluğunun bir parçası olabilmek mümkündür. Yazılımın kendisini indirmek ve kullanmak da serbest olup herhangi bir kuruma karşı yükümlülük gerektirmemektedir. Yazılımın kullanılmasına karar verildiğinde, blockchain topluluğunun bir üyesi olarak cihazın da blok zincirinin bir parçası olması ve her yeni blok oluşturulduğunda cihazın da bu işlemin bir kopyasını alması söz konusudur (Söze, 2017).

1.2.2.5.2.Kriptografi

Kriptografi yani şifreleme, yalnızca amaçlanan alıcı tarafından okunabilen gizli mesajlar gönderilmesi anlamına gelmektedir. Şifreleme ve şifre çözme (mesajların kodlanması ve kodunun çözülmesi), hashing (verilerin parmak izi

özetlerine dönüştürülmesi) ve dijital imzalar (oluşturduğunuz bir mesaj veya onayladığınız kanıtlar) gibi teknikler kriptografinin başlıca temel fonksiyonlarıdır (Lewis, 2018). Kriptografi, üçüncü tarafların gözünde güvenli iletişim sanatıdır. Blok zincirler bu bağlamda, toplumun binlerce yıldır kullandığı birçok eski teknolojiyi yeni yöntemlerle harmanlamaktadır. Örneğin, kriptografi ve ödeme, kripto para birimini oluşturmak için birleştirilir. Değerleri temsil eden bir simge ile ödeme insanlık tarihinde çok uzun zamandır yapılagelmektedir ancak şifreleme ile birleştirildiğinde kripto para birimleri oluşturur ve tamamen yeni bir şey haline gelir. Kripto para birimleri, para birimlerinizi bir simge olarak alarak çevrimiçi hale dönüştürüp ticaret yapılabilir hale getirmeyi sağlamaktadır (Laurance, 2017).

1.2.2.5.3. Hash İşlevi

Hash fonksiyonları temel olarak bir mesajı sabit uzunluktaki bir özete sıkıştırmak için kullanılır. Bu modda, blok şifreler bir düz metin karması oluşturmak için bir sıkıştırma işlevi olarak kullanılır (Bashir, 2017).

Lewis (2018)'e göre, iyi bir hash fonksiyonu kriterleri karşılayan MD571 (İleti Özeti) veya SHA-256 (Güvenli Karma Algoritma) gibi bazı endüstri standardı kriptografik hash fonksiyonları vardır. Ona göre, bir kriptografik hash işlevi özeldir ve kriptografide ve kripto para birimlerinde yararlı kılan bazı özellikleri içerdiğini ve ideal kriptografik hash işlevinin beş ana özelliği olduğunu belirtir:

1. Aynı mesaj her zaman aynı hash ile sonuçlanır.

2.Herhangi bir mesajın hash değerini hesaplamak hızlıdır; kolayca ileri gidilebilir.

3.Tüm olası mesajları denemek dışında hash değerinden bir mesaj oluşturmak mümkün değildir dolayısıyla geriye gidilemez.

4.Mesajda yapılan küçük bir değişiklik, karma değerini o kadar büyük ölçüde değiştirmelidir ki, yeni karma değeri eski karma değeri ile ilişkilendirilmemiş görünecektir yani küçük bir değişiklik büyük bir fark yaratır

5.Aynı hash değerine sahip iki farklı mesaj bulmak mümkün değildir; bir hash çatışması oluşturmak zordur.

1.2.2.5.4. Simetrik Anahtar Şifreleme

Simetrik kriptografi, verileri şifrelemek için kullanılan anahtarın, verilerin şifresini çözmek için aynı olduğu ve bu nedenle aynı zamanda paylaşılan bir anahtar kriptografisi olarak da bilinen bir tür şifreleme türünü ifade eder. Anahtar, iletişim kuran taraflar arasındaki veri alışverişinden önce oluşturulmalı veya üzerinde anlaşmaya varılmalıdır. Gizli anahtar şifrelemesi olarak da adlandırılmasının nedeni budur (Bashir, 2017).

1.2.2.5.5. Açık Anahtar Şifreleme

Ortak anahtar şifrelemesini anlamak için, bakılması gereken ilk kavram, ortak ve özel anahtarlar fikridir. Özel bir anahtar, isminden de anlaşılacağı gibi, temelde kullanıcılar tarafından gizli tutulan ve gizli tutulan rastgele oluşturulmuş bir sayıdır. Özel anahtarın korunması gerekir ve bu anahtara yetkisiz erişim verilmemelidir; aksi takdirde, genel anahtar şifreleme şemasının tamamı tehlikeye girer, çünkü bu mesajların şifresini çözmek için kullanılan anahtardır. Özel anahtarlar, kullanılan algoritmaların türüne ve sınıfına bağlı olarak çeşitli uzunluklarda olabilir. Örneğin, RSA'da tipik olarak 1024 bit veya 2048 bitlik bir anahtar kullanılır. 1024 bit anahtar boyutu artık güvenli kabul edilmez ve pratikte en az 2048 bit kullanılması önerilir.
Ortak anahtar, özel-ortak anahtar çiftinin ortak parçasıdır. Genel bir anahtar herkese açıktır ve özel anahtar sahibi tarafından yayınlanır. Daha sonra ortak anahtarın yayıncısına şifreli bir mesaj göndermek isteyen herkes bunu, yayınlanan ortak anahtarı kullanarak mesajı şifreleyerek yapabilir (Bashir, 2017).

1.2.2.5.6. Dijital İmza

Yasal bir sözleşme söz konusu olduğunda, iş yapmanın geleneksel yolu, her iki tarafın, alıcının ve satıcının, yasallaştırma için diğer birçok belgenin yanı sıra sözleşmeyi imzalaması gerektiğidir. Sözleşmeleri imzalamanın bu geleneksel yolu kalem kullanılarak el yazısı ile gerçekleştirilir. Ancak, belirli belgelerin kimliğini doğrulamanın başka yolları bulunmaktadır ve en bilinenlerinden biri dijital imza kullanmaktır. Dijital imzalar standart geleneksel el yazısı imzalarına çok benzemektedir. Ancak, çok daha güvenlidirler. El yazısı imzaları söz konusu olduğunda, bir profesyonel veya biraz pratik yapan herkes tarafından kolayca taklit

edilen uzun bir geçmişi vardır. Dijital imzalar, bazı basit yöntemler kullanarak sahte imza sorunlarının üstesinden gelmiştir. Dijital imza alıcıya benzersiz bilgiler sağlar; bu nedenle özgünlük sağlar.

Dürüstlük: Mesaj aktarılırken herhangi bir değişiklik veya değişiklik yapılmamasını sağlamak içindir.

Kimlik Doğrulama: Gönderenin gerçekliğini sağlamak içindir.

Reddetme: Mesajı gönderenin, gönderdiğini inkâr edememesi (Söze, 2017).

1.2.2.5.7. Belli Bir Merkezin Olmaması

Ülkeler sahip oldukları para birimlerine dair politika ve işlemleri merkez bankaları ya da benzer nitelikte işlevler üstlenen kurumlar vasıtasıyla yürütmektedir. İyi niyetli üçüncü tarafların ya da aracıların yokluğu prensibi üzerine kurgulanarak üretilen kripto paralar, herhangi bir otoriteye ya da resmi yapıya dahil değillerdir. Bu sebeple herhangi bir denetim veya gözetimleri de söz konusu değildir. Merkezi bir bağlarının olmaması nedeniyle bu yapılar adem-i merkeziyetçi sistemler şeklinde anılmaktadır (Ceylan, 2019).

Merkezi olmayan özerk bir organizasyonun genel konsepti, kurumun fonlarını harcama ve kodunu değiştirme hakkına sahip olan belirli bir üye veya hissedar grubuna sahip sanal bir kuruluştur (Bambara ve Allen, 2018). Üyeler toplu olarak kuruluşun fonlarını nasıl tahsis etmesi gerektiğine karar vermektedirler. Merkezi olmayan bir oraganizasyon fonlarını tahsis etme yöntemleri, ödüller ve maaşlardan işi ödüllendirmek için iç para birimi gibi birçok alanda etkinlik göstermektedir. Uygulamada yalnızca kriptografik blockchain teknolojisini kullanan bu yapı, geleneksel bir şirketin veya kâr amacı gütmeyen kuruluşun yasal tuzaklarını çoğaltmaktadır.

1.2.2.5.8. Anonim Olmaları

Anonimlik, bir varlık grubunun başka bir varlık grubu tarafından tanımlanaması anlamına gelmektedir (Pfitzmann ve Hansen, 2010). Sanal uzamda kimlikle ilgili sıkça karşılaşılan anonimlik kavramı, kripto para birimi bağlamında ele alındığında, blok zincir teknolojisi tabanında fon ve tasarruf işlemleri esnasında gerçek kimliğini açıklamaksızın işlem yapabilmeyi sağlayarak ekonomik bir mahremiyet

alanı oluşturmaktadır. Sosyal medya mecralarında olduğu gibi kullanıcı isimleri, kripto para işlemlerinde kullanılan adresler, anonimlik için fırsat yaratmaktadır. (Ceylan, 2019).

1.2.2.6. Kripto Para Birimleri

1.2.2.6.1. Bitcoin

Satoshi Nakamoto 2008 yılında Bitcoin kripto birimini yaratırken, teknik bakımdan birtakım üstünlüklerini ön plana çıkararak halihazırdaki sanal ödeme sistemlerinin güvenlik sorunları ve bazı eksikliklerine odaklandı. Kaleme aldığı makalede, finansal sistemin yerleşik kurallarını gelişmiş şifreleme yöntemleri ile iktisadi ve teknolojik açıdan yeniden kurgulamaktadır. Nakamoto'nun bu kurgusu Bitcoin adını verdiği kripto para sisteminin mevcut uygulamalara ne katacağı, hangi yetersizliklere çözüm sağlayacağı, herhangi bir üçüncü taraf olmaksızın iki tarafın aralarındaki fon transferleri süreçlerinin hangi şekilde gerçekleşeceğini paylaşmaktadır. Böylelikle oluşturduğu yeni sistemin daha rasyonel çok daha verimli olduğunu savunmaktadır.

Şekil 1.9.: Bitcoin Ekosistemi

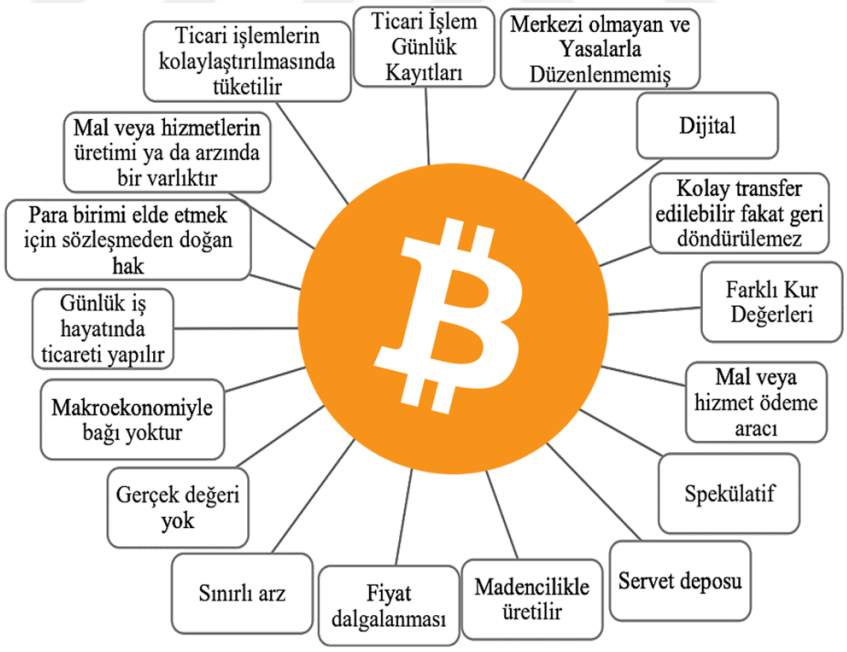
Kaynak: Gültekin ve Bulut, 2016

Bitcoin'in bilinen ilk merkezi olmayan blok zincir teknolojisi ürünü olan dijital para birimi olması bağlamında güvenli ve istikrarlı oluşunun kanıtlanması ile büyük bir devrime yol açmıştır. Akademik çalışmalara da bu yönüyle sıkça konu olmaya başlayan Bitcoin, 2008'deki tanıtımından bu yana, bitcoin çok popülerlik

kazandı ve şu anda milyarlarca dolarlık yatırımla dünyanın en başarılı dijital para birimi olarak görülmektedir (Bashir, 2017).

Satoshi Nakamoto 2008 yılında Bitcoin kripto birimini yaratırken, teknik bakımdan birtakım üstünlüklerini ön plana çıkararak halihazırdaki sanal ödeme sistemlerinin güvenlik sorunları ve bazı eksikliklerine odaklandı. Kaleme aldığı makalede, finansal sistemin yerleşik kurallarını gelişmiş şifreleme yöntemleri ile iktisadi ve teknolojik açıdan yeniden kurgulamaktadır. Nakamoto'nun bu kurgusu Bitcoin adını verdiği kripto para sisteminin mevcut uygulamalara ne katacağı, hangi yetersizliklere çözüm sağlayacağı, herhangi bir üçüncü taraf olmaksızın iki tarafın aralarındaki fon transferleri süreçlerinin hangi şekilde gerçekleşeceğini paylaşmaktadır. Böylelikle oluşturduğu yeni sistemin daha rasyonel çok daha verimli olduğunu savunmaktadır.

Şekil 1.10.: Bitcoin'in Karakteristikleri



Kaynak: Venter, 2016

Nakamoto'ya göre bitcoin iki kişi arasında ihtiyaç duyulan karşılıklı fon transferinin dijital kaynakları kullanarak herhangi bir aracı finans kuruluşu olmadan, bitcoin kripto para sistemi ile online bir şekilde gerçekleşmesine imkân tesis etmektedir. Aslında mevcut finansal araçlar üzerinde kullanılabilen dijital kimlik

doğrulama sistemleri (online imzalama yöntemleri gibi) bu ihtiyaca cevap veriyor gibi görünsede bitcoin sistemi herhangi bir üçüncü parti aracı tarafa ihtiyaç duymaması sebebiyle maliyet avantajı ile bu yöntemlerden pozitif ayrışmaktadır. (Nakamoto, 2007)

Küresel çapta kripto paralar içerisinde en popüler olan Bitcoin, mülkiyeti dünya çapında birbirine bağlanan ve yaklaşık 10.000 bağımsız çalışan bilgisayarda aynı anda güncellenen bir elektronik deftere kaydedilen dijital varlıklar olarak tanımlanmaktadır. Bitcoin'in blok zinciri denilen defter üzerine, bu madeni paraların mülkiyetinin transferini kaydeden işlemler, bir protokole (işlerin nasıl çalıştığını tanımlayan ve dolayısıyla deftere yapılan güncellemeleri yöneten kuralların bir listesi) göre oluşturulur ve doğrulanır. Protokol, katılımcıların bilgisayarlarında çalıştırdığı bir uygulama tarafından uygulanır. Tüm işlemleri bağımsız olarak doğrular ve defteri kebir kaydını kendi onaylanmış işlem bloklarıyla günceller. Herkes bitcoin satın alabilir, onlara sahip olabilir ve başkalarına gönderebilir. Her Bitcoin işlemi, Bitcoin'in blok zincirinde düz metin olarak kaydedilir ve halka açık olarak paylaşılır (Lewis, 2018).

1.2.2.6.2. Ethereum (ETH)

Blockchain, internet bağlantısı olan herkesin görüntüleyebileceği ve kullanabileceği çevrimiçi bir veritabanıdır. Bu veritabanı ağda bulunduğundan, merkezi olmayan olarak sınıflandırılmaktadır. Defter veya veritabanı yalnızca sınırlı erişime sahip belirli bir yerde depolanmakla kalmaz, dünyadaki her bilgisayar arasında paylaşılmaktadır. Bitcoin ve Ethereum gibi kripto para birimlerini bu kadar eşsiz yapan şey budur (Ozer, 2017).

En temel biçimde, Ethereum, geliştiricilere merkezi olmayan uygulamalar oluşturma ve bunları dağıtma fırsatı veren bir blockchain tabanlı açık kaynak platformudur. Bitcoin gibi, halka açık bir dağıtılmış blok zincir ağıdır, ancak ikisi arasında bazı önemli farklılıklar vardır. En önemli fark, iki ağın amacı ve kabiliyetidir. Bitcoin, Bitcoin'in çevrimiçi ödemelerine izin veren bir P2P dijital nakit sisteminin uyguladığı özel bir blockchain uygulaması sunuyor. Bu ağ, Bitcoin'in sahipliğini izlemek için kullanılır, ancak Ethereum, merkezi olmayan bir uygulamayı çalıştırmak için gereken program koduna odaklanmıştır. Ethereum, bir dijital para birimi olması

nedeniyle ticareti yapılabilir, ancak genellikle uygulama geliştiricileri tarafından Ethereum ağındaki hizmetler ve işlem ücretlerini ödemek için kullanılır (Ozer, 2017).

Ethereum, Merkezi Olmayan Otonom Organizasyonlar oluşturmak için de kullanabilmektedir. Bunlar, tek başına otorite olmayan, tamamen özerk olan ademi merkeziyetçi yapılardır. Sadece programlama kodu, Ethereum'la üretilen akıllı sözleşmeler en başarılı örnekleri arasında gösterilebilmektedir. Ethereum, en hızlı ilerleyen ve gelecek vadeden bir kripto para birimidir. Platform kullanıcı dostudur ve insanlara blockchain'in gücünü kullanma fırsatı vermektedir.

1.2.2.6.3. Ripple (XRP)

Bitcoin ve diğer kripto paraların aksine, Ripple blok zinciri, şirketin topluluğa ne zaman ve ne kadar para dağıtacağını belirlemesine izin veren kontrollerle oluşturulduğundan, kripto topluluğu bir değişikliği zorlayana kadar para birimi içinde benzersiz bir özellik yaratması, eleştirmenler tarafından, para arzını kontrol eden Federal Rezerv'e benzetilmesine neden olmaktadır (Derousseau, 2019). Merkezi olmayan para birimlerinin bu yeni dünyasında, para birimlerinin şirketten bağımsız olarak çalışması gerektiğine inanan birçok kripto para meraklısını kendinden uzaklaştırırken özel endüstriler ve onlara ait teknolojiler, bu yenilikçi stratejiyi desteklemektedir. Bu perspektif fdoğrultusunda özellikle dolandırıcılıkların yaygın olduğu bu evrende, bu meşruiyet düzeyini görmek güven verici unsuru, şirketlerin ödeme yapma şekillerini değiştirmek bakımından özel bir amaca da hizmet etmektedir. Zira internetin ortaya çıkmasından önce, sınırlar arasındaki ödeme sistemleri hem yavaş hem de pahalı sistemler olarak karşımıza çıkmaktadır. Bu amaç kapsamında, Ripple; Santander, Kanada Kraliyet Bankası, American Express ve MoneyGram dahil olmak üzere "RippleNet"i test eden bir dizi banka ve finans kurumuna sahiptir. Bu da Ripple'a büyük organizasyonların bu üst düzey ilgisini göstermesi bakımından önemlidir.

1.2.2.6.4. Alt Coinler

Kripto para kavramı her ne kadar popüleritesini Bitcoin'e borçlu olsa da bunun dışında da her geçen gün yeni dijital para birimleri piyasaya çıkmaya devam etmektedir. Bu yeni çıkan kripto para birimleri altcoin olarak anılmaktadır. Örnek

vermek gerekirse Ethereum, Dash, Bitcoin Cash, Litecoin, Monero, Neo, Zcash, Iota, Nem, Ripple vb. gibi birçok altcoin birimi bulunmaktadır. Aşağıda bu altoinlerden popüler olanlara ilişkin güncel piyasa verileri paylaşılmaktadır.

Şekil 1.11: Kripto Paraların Piyasa Değeri Ve Üretim Limitleri

Name	Symbol		Market Cap[122]	Supply limit[123]
Bitcoin		BTC	$124.969.093.161	21 million
Ethereum		ETH	$57.462.517.858	TBD[124]
Ripple		XRP	$23.790.387.789	100 billion
Bitcoin Cash		BCH	$17.159.025.225	21 million
Litecoin		LTC	$6.704.709.572	84 million
Stellar		XLM	$5.128.373.973	100 billion
Cardano		ADA	$5.034.129.651	45 billion
IOTA		MIOTA	$4.038.240.572	2,779,530,283,277,761
NEO		NEO	$3.386.383.000	100 million
Monero		XMR	$2.626.586.260	18,4 million
Dash		DASH	$2.592.894.544	17.74 – 18.92 million[125]

Kaynak: (Houben ve Snyers, 2018)

1.2.2.7. Kripto Paranın Avantajları ve Dezavantajları

Blockchain tabanlı üretilmekte olan kripto paraların bugüne kadar ki para deneyimlerinden çok üstün bazı avantajlarından söz edilebileceği gibi birtakım dezavantajlarından da bahsetmek mümkündür.

Öncelikle kripto paralar blockchain tabanlı özgün bir platform üzerinde inşaa edildiği için manipülasyonu veya müdehalesi çok zordur. Yine kullandığı altyapı iibariyle bu paralar dijial cüzdanlarda tutulduğu için fiziki bir hacme sahip değildir ve

bu yüzden fiziki olarak çalınması da mümkün değildir. Bu özelliği ile kripto paralar üstün bir taşıma avantajı da sunmaktadır. Kripto paralar kullanılarak gerçekleştirilen işlemlerde, kimlik unsurunun önemli olmaması bağlamında *anonimlik*, ekonomik bir otoritenin etkisinde olmaksızın *müdahale edilemezlik*, tüm kullanıcılara açık kaynaklı işlem imkânı sunması bakımından *şeffaflık, güvenilirlik* ve işlemlerin *hızlı ve ekonomik* olması gibi birçok avantajı kullanıcılara sunmaktadır (Clohessy, Acton ve Rogers, 2019). Bunların yanısıra yine herhangi bir resmi otoriteye bağlı olmaması nedeniyle vergilendirmeye tabi değildir. Kullanıcılar dinedikleri an diledikleri yerde ve diledikleri miktarda hiçbir bürokratik sınırlama olmaksızın işlem gerçekleştirebilmektetir.

Şekil 1.12.: Kripto paraların Swot analizi

FIRSATLAR Sırdaş hesap olma özelliği Arz artışının yapılamaması	**TEHDİTLER** Dağıtık sistemle takip edilmesi Merkezi Yönetimin olmaması Hesapların isme kaydedilememesi
GÜÇLÜ YANLARI -Yüksek güvenlikli şifreleme -İsteğe göre yönlendirilememe -Miktarın değiştirilememesi	**ZAYIF YANLARI** -Kabul görme sorunu -Hesap güvenliğinin olmaması -Vergilendirilememesi -Kara para aklamada kullanılması

Kaynak: (Çetinkaya, 2018)

Kripto paraların kullanımında sözü edilen avantajları yanında birtakım dezavantajlarından da sözetmek mümkündür. Bunların başında sosyal ve iktisadi yaşama tam manasıyla entegrasyonu gerçekleşmediğinden kullanım alanları henüz yeterince geniş değildir. Yatırım amacıyla tercih edilen kimi para birimlerin piyasa büyüklüklerinin çok kısıtlı olmusı sebebiyle istikrarlı bir seyre sahip değillerdir. Bunun yanında hemen hemen tüm devletler tarafından mesafeyle yaklaşılmakta hatta yok sayılmaktadır. Para birimleri arasında küçük farklılıklar arzetse de gerçekleştirilen

işlemler hata kabul etmemekte ve düzeltme yapılamamaktadır. Başka bir değişle herhangi bir başvuru mercii bulunmamaktadır. Ek olarak teze bir yenilik olması sebebiyle yetersiz bilgi kaynaklı bazı kötü niyetli olaylarda kullanılabilmektedir (Ömrüuzun, 2019).

1.2.2.8. Kripto Para Birimlerinin Türkiye'deki Hukuki Durumu

Henüz yeni bir teknolojik gelişme olarak sosyal ve iktisadi alandaki yerini alan kripto paraların Türkiye Cumhuriyeti hukuk mevzuatındaki karşılığı şu başlıklar altında toplanabilmektedir.

Kripto paraların her geçen gün yaygınlaşması, yeni eklenen altcoinler ve kullanıcıların bu konuya olan ilgisi neticesinde birçok olumlu gelişme yaşandığı gibi bu para birimleri ile yasadışı bir takım olumsuz deneyimler de görünmeye başlamıştır. Özellikle bu paraların vergi kaçırma, narkotik madde satışı, sanal ortamda işlenen bahis ve kumar oyunlarına konu olmakla birlikte adı suçtan elde edilen gelirlerin aklanması ile sıkça anılır hale gelmiştir. Tüm bu tespitlerle birlikte ülkemizdeki mevcut yasal hükümler bağlamında kripto paralarla yapılan ödeme, fon transferi gibi finansal işlemlerde ilişkin herhangi bir kısıtlayıcı hüküm bulunmamaktadır. Diğer taraftan, TCK-282. maddesinin, "*suçtan kaynaklanan malvarlığı değerlerini aklama*" bendi suç gelirlerinin, kripto para birimlerine dönüştürülerek işlem yapılması olasılığını beraberinde getirmektedir. Yine mevcut mevzuat hükümleri bağlamında kripto paraların suç geliri olarak kabul edilmemesinin önünde engel bir hüküm bulunmamaktadır. Bu açıdan değerlendirildiğinde kripto para cinsinden malvarlıkların, suçtan elde edilmiş gelirlerinin ceza kanunlarında düzenlenmiş suçlara konu olması durumunda sorumluluk doğuracağı açıktır.

MASAK (Mali Suçları Araştırma Kurulu), kripto para varlıklarının alım satım ticaretini yapan aracı kuruluşlara gerçekleştirdikleri finansal transferlere yönelik bildirim sorumluluğu getirmektedir.

BDDK (Bankacılık Düzenleme ve Denetleme Kurulu) en popüler kipto para olan Bitcoin için *"...Herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen Bitcoin, mevcut yapısı ve işleyişi itibarıyla Kanun kapsamında elektronik para olarak değerlendirilmemekte, bu nedenle de söz konusu Kanun çerçevesinde gözetim ve*

denetimi mümkün görülmemektedir (BDDK, 2018)." değerlendirmesi bulunmaktadır. Diğer taraftan kimi kurumların kripto para birimlerine yönelik tutumu daha olumlu seyretmektedir. Örneğin SPK Aralık 2016 tarihli araştırma raporunda kripto para birimi Bitcoin hakkındaki pozitif endişeli yaklaşılması ve teşvik edici mevzuat çalışmaları tavsiye etmektedir.

Vergi kanunları çerçevesinde bakıldığında ise, her ne kadar kripto paralar bir ekonomik değer ifade etseler de işletme bilançolarında hangi hesap kodu ile aktiflere kayıt edileceğine yönelik net bir bilgi bulunmamaktadır. Bunun sebebi halihazırda bu varlıklara yönelik mevzuat düzenlemesinin yapılmamış olmasıdır. Bir diğer ihtilaf konusu da kimilerince bir ödeme aracı olarak kullanılırken kimileri tarafından bir tasarruf aracı olarak tercih edilmesi hususudur. Lakin Türkiye Cumhuriyet Merkez Bankası kripto paraları bir döviz cinsi olarak görmemektedir. Yatırım aracı olarak değerlendirildiğinde de Sermaye Piyasası Kanununda bu varlıklar bir menkul kıymet aracı olarak anılmamaktadır. Halihazırda kripto varlıklar mevcut mevzuat hükümleri bağlamında değerlendirildiğinde, menkul kıymet olarak değerlendirilmediği gibi, nakit, döviz ve emtia olarak da tanımlanmamıştır. VUK (Vergi Usul Kanunu)'da da değerleme referansları verilen hiçbir iktisadi varlık içerisinde tanımlama imkânı bulunmamaktadır.

2. BÖLÜM
SINIRAŞAN SUÇLAR ve TERÖRİZM

2.1. SINIRAŞAN SUÇLAR

2.1.1. Sınıraşan Suç Kavramı

İlk bakışta sınıraşan suç kavramı 90'lı yılların sonlarına doğru kavramsal açıdan gündeme gelmeye başlasa da litaratürde kökeni "*transnasyonalizm*" kavramına yani 1970'li yıllara dayanmaktadır. Müstakil bir kavram olmaktan ziyade daha çok kriminoloji çalışmalarının içerisinde yer bulmuştur (Sazak, 2018).

Felsen ve Kalaitzidis'e göre; kriminolojinin de ötesinde küreselleşme sürecine atıfla uluslararası bir terim olarak değerlendirilmiştir. Yine bu kavram aynı zamanda terörün uluslararası bayutunu anlamlandırma çabaları içerisinde de kullanılmıştır (Sazak, 2018).

Ortaya atıldığı günden günümüze suç olgusunun içerisinde uluslararası düzeyde ifade etmeye çalışan bu kavram yarım asırdan bu yana çeşitli çalışmalara konu olmaktadır. Bu bağlamdaki öncül çalışmalar 1970li yıllara rastlamakta ve *"faillerden en az birinin hükümet dışı olması halinde; bilginin, paranın, fiziksel eşyaların, somut veya soyut nesnelerin ülke sınırlarını aşan hareketi"* şeklinde ifade edilmiştir. Bu bağlamda sınıraşan suçlar birtakım özellikler ihtiva etmektedir. Bunlar;

- Suçlular, suç eylemi esnasında başka bir devletin sınırlarını ihlal ederler.
- Sınıraşan suçlar birbirinden farklı özelliklere sahip birçok suç çeşidinde gerçekleşebilir. Örneğin illegal bir suç olan akaryakıt kaçakçılığı olabileceği gibi legal olan bir sanat eserinin yasadışı yollarla başka bir ülkeye kaçırılması gibi.
- Suçtan zarar gören taraf gerçek şahıslar da olabilir. Örneğin insan ticareti.
- Teknolojik teknikler vasıtasıyla gerçekleştirilebilir. Örneğin siber suçlar.
- Suç faaliyeti neticesi haksız bir kazanç sağlanmaktadır (Değirmenci, 2013, s. 61)

BM'nin 1975 tarihli raporunda ulusal ve uluslararası nitelikteki yasadışı faaliyetlerin iktisadi gelişimi olumsuz etkilediği ve bu duruma karşı alınabilecek önlem ve denetimlere ilişkin çalışmalara yer verilmiştir. Bu çerçevede 70 li yıllara kadar yasadışı faaliyetler ulusların sınırları dahilinde olan eylemlerdi. 80'li yıllara

gelindiğinde uluslararasılaşan suçlar "sınıraşan suç" şekinde tanımlanarak suçbiliminde yerleşik bir kavram niteliği kazanmıştır. 90'lara gelindiğinde ise teoride de uygulamada da popüler bir kavram olarak karşımıza çıkmaktadır. Organize olmadan kişisel nitelikte gerçekleştirilebilecek olan sınıraşan suçlar, ekseriyetle bir suç organizasyon olarak karşımıza çıkmaktadır. Bu sebepten ötürü ceza kanunları dahilinde bir kategorizasyonu bulunmamakla birlikte kriminolojik bir kavram olarak değerlendirilmektedir.

2.1.2. Organize ve Örgütlü Suç Kavramı

Soğuk Savaşın ardından seyreden süreçte dünyanın global olarak ele alınmasına yönelik yaklaşım ağırlık kazanmıştır. Küreselleşme beraberinte insanların her boyuttaki birbirleriyle etkileşimine büyük yenilikler getirmiştir. Bu süreçteki sermaye birikimindeki yükselişler ve bu sermayelerin transferini mümkün kılan yöntemlerin hayata geçmesi, yasadışı faaliyetler için de kuşkusuz yeni fırsatlar yaratmıştır. Suç amaçlı kurulan organizasyonların faaliyet alanlarını yerleşik alanlarının dışına taşıyarak diğer ülkelerde de suç faaliyetlerini yürütür büyüklüğe ulaşlamaları organize suç kavramını çok uluslu bir ölçeğe çıkarmıştır.

Görece eski olarak anılabilecem mazisi olan organize suç terimi, çoğunlukla dar boyutlu ulusal bir sorun olarak değerlendirilmiştir. 1990'lı yıllarla birlikte suç organizasyonları; kaçakçılık suçları başta olmak üzere, yolsuzluk ve kara para aklama suçları ile küresel bir probleme dönüşmüştür (Ütük, 2010).

Organize suçları ele alırken kavram karmaşalarını önlemek için en başta organize ve örgütlü suç kavramlarını çerçevelendirmek gerekmektedir. Örgüt, önceden belirlenmiş hedefe ulaşmak için gerçek kişi ya da kurum organizasyonlarıdır (Canak, 2005).

Bir suç fiilini icra etmek için eylem ve fikir birliği içerisinde toplanılması, bir organizasyon teşkil edilmesi ise *"örgütlü suç"* kavramı ile açıklanmaktadır. Bu bağlamda güncel tanımlara bakıldığında *"organize suç", "örgütlü suç"* gibi tanımlamalar yapılmaktadır.

Örgütlü suç terim olarak ilk 1920'de, iktisadi, toplumsal, politik bir takım yeni gelişmeleri açıklamak maksadıyla ABD'de kullanılmıştır. Ayrıca örgütlü suç

işleyen yapılara 1960'1ardan sonra illegal faaliyetler yürüten mafya olgusu açıklanırken benzer bir anlam atfedilmiştir (Baltacı, 2004, s. 54).

Suç örgütlerine katılan kişiler, az veya çok ama sürekli olarak, suç faaliyetlerinin içinde yer almak amacıyla biraraya gelen kişiler olarak düşünülmektedir. Bunlar çoğunlukla, yasadışı mal ve hizmetlerin veya hırsızlık veya dolandırıcılık gibi yasadışı yollardan elde edilmiş malların tedarik edilmesi olarak adlandırılan yatırım suçlan ile uğraşmaktadır. Örgütlü suç, yasal ekonomik dünyanın bir uzantısı olarak, hemen hemen her konuda yasaklanmış alanlarda kendisini göstermektedir. Suç örgütleri arasındaki çeşitlilik, meşru piyasa içindeki iş dünyasını hakimiyet altında tutma temel düşüncesinden kaynaklanmaktadır. Bu ise pazar payını koruma ve genişletme ihtiyacından ortaya çıkmaktadır. Günümüzde örgütlü suçlara yenileri eklenirken birçoğu için de yeni yeni yöntemler geliştirilmektedir. Hal böyleyken ittifak edilmiş net bir çerçeve çizilememiştir. Bu tanımlama çabaları içerisinde sözü edilen suç organizasyonlarının faaliyetlerini devam ettirebilmek için, kimi kurum ve kuruluşları istismar edebilme potansiyelleri üzerinde bir fikir birliği gözlemlenmektedir (Baltacı, 2004, s. 55).

2.1.3. Sınıraşan Suç Türleri

2.1.3.1. Uyuşturucu Kaçakçılığı

Uluslararası suça konusu olan alanlardan en önemlilerden birisi uyuşturucu maddelerin ticareti ve bunların uluslararası ticaretinin yapılış şekilleridir. Gerçekten uluslararası ilişkilere çeşitli etkileri olan uyuşturucu maddeler dünya üzerindeki güzergahları ve büyük çaplı ekonomik getirisi ile tartışma ve inceleme konusu olmaktadırlar. İnsanlık geçmişten günümüze birçok sağlık sorunu ve bunlara yönelik şifa amacıyla sayısız yöntem denemiştir. İlkel deneyimler süreç içerisinde çoğalarak modern tıp ve ilaç çalışmalarını geliştirmiştir. Geliştirilen bu yöntemler her zaman amacına yönelik kullanılmamış ve bazı saptırılmış amaçlar uğruna da kullanılmıştır.
Uyuşturucu maddelerin genel olarak tanımının yapılmasından sonra, türlerine bağlı olarak sınıflandırılması ve buna bağlı olarak tanımlanması gerekmektedir. Çünkü uyuşturucu maddelerin yetiştirildikleri bölgeler, sevk edildikleri güzergahlar, kullanıcı hedef kitlenin bulundukları ülkeler, uluslararası ilişkilere etkisi olan parametrelerdir.

Doğal, yarı yapay ve yapay uyuşturucu maddelerin tümü narkotik maddeler olarak tanımlanmaktadır. Yunanca uyku anlamında ki "narke"den oluşan, "*Narkotikos*" kelimesi uyuşukluk, rehavet, miskinlik durumunu ifade eder. Uyuşturucunun tanımlaması yapılırken eşanlamlısı olarak kullanılan narkotik uyuşturucu hissizleştiren, uyuşturan anlamına gelmektedir. Her ne kadar bu kavram uyuşturma özelliği ile niteleniyor olsa da haz, uyarma, sakinleştirme ve odaklanma kabiliyetini artıran maddeler için de kullanılmaktadır. Bu maddeler doğrudan insan metabolizmasında sinir sistemi faaliyetlerine müdehale ederek ruhsal ve fiziksel açıdan geri dönüşü olmayan etkiler meydana getirmektedir. Etkileri sadece kullananlar ile sınırlı kalmamakta büyük çapta toplumsal sorunlara yol açmaktadır. Bazı uyuşturucu maddelerin etkileri kullananlarda, pisikolojik bağımlılık belirtisiyle karakterize iken bazı maddeler ise artan oranlı bir fizyolojik bağımlılık geliştirirleri. İlaç-bilim uzmanları uyuşturucu maddeleri yoksunluk duyguusunu bastıran, yatıştıran ve uyku düzenleyici maddeler olarak kategorize etmektedirler.

Değişik kaynaklarda uyuşturucu maddelerin sınıflandırılması ve tanımlamaları farklı şekillerde yapılmaktadır. Elde edikleri hammaddelerin türlerine göre uyuşturucular;

- *Afyon ve türevleri*: Haşhaş bitkisinin kozasının çizilmesinden elde edilen özsuyun farklı şekillerde sentezlenmesi sonucunda elde edilen uyuşturuculardır. En önemlisi eroin diye bilinen uyuşturucudur.

- *Koka ve türevleri:* Koka ağacının yapraklarından elde edilen koka isimli uyuşturucu maddenin farklı bileşimlerle kullanılması sonucu elde edilen uyuşturuculardır.

- *Hint keneviri ve türevleri*: Hint keneviri bitkisinin dişi olanının yapraklarından elde edilen uyuşturucunun farklı şekillerde işlenmesiyle elde edilen uyuşturucular.

- *Sentetik uyuşturucular:* Uyuşturucu özelliği tespit edilmiş çeşitli suni maddelerin hap haline getirilmiş çeşitli şekilleridir.

- *Kimyasallar*: Uyuşturucu yapımında kullanılan asetik anhidrit gibi çeşitli kimyasal maddeler ile doğrudan kullanılabilen, tiner yapıştırıcı gibi çeşitli maddeleri kapsamaktadır.

Sınıflandırma yapılırken, bazı maddelerin sınıflandırılmasında farklı yorumlamalar olabilmekte ve bazı maddeler, birden fazla türü ilgilendirilmektedir. Farklı sınıflandırmalar içinde kullanıcılarda yaptıkları etkiler ve kullanılma şekillerine göre aşağıda bir sınıflandırma derlenmiştir.

- Narkotikler: Afyon vb, Kenevir vb, mantarlar
- Uyarıcılar (Stimulantlar): Koka vb, Amfetaminler, sentetikler
- Depresanlar (Sakinleştiriciler)
- Kimyasallar: Uyuşturucu imalinde yardımcı malzeme olarak kullanılan maddeler ile koklamak suretiyle kullanılan maddelerdir (KOM, 2020).

Narkotiklerin sınıflandırılmasında elde edildikleri bitki ve maddelere göre sınıflandırılması tercih edilmektedir. Elde edildikleri bitkilerinin yetiştirildiği yerler, ülkeler ve bölgeler üretim bölgeleri olarak nitelendirilmelidir. Üretim bölgeleri ile bu bölgelerden hedef ülkelere doğru güzergahlar, uluslararası örgütlü suçluluğa etkileri açısından önem taşımaktadır. Örneğin afyon ve türevlerinin ana üretim bölgesi Güney Asya bölgesi iken koka ve türevleri Orta ve Güney Amerika' da üretilmekte, buralardan pazar ülkelere akmaktadır. Ama bunun yanında sentetik uyuşturucular ve kimyasalların kaynağı ise Avrupa olup, diğer ülkelere tersine bir güzergâh izlemektedir. Örneğin eroin imal etmek için en kritik madde olan asetik anhidrit maddesi de Batılı ülkelerde üretilip eroin imali için afyon üretim merkezi olan ülkelere doğru kaçakçılık güzergahı izlemektedir.

2.1.3.2. Bilişim Suçları

Günümüzde her an yeni teknolojik gelişmeler, buna bağlı olarak da birçok yenilik ortaya çıkmaktadır. Özellikle 2000 sonrası internet tabanlı hizmetler günlük hayatın rutini haline gelmiş, eğitimden sağlığa alışverişten birçok kamu hizmetine sanal ortam herkes tarafından maliyetleri düşürmesi ve işlemleri kolaylaştırması sebebiyle tercih edilmektedir. Bu bağlamda söz konusu yenilikleri ve araçları kullanarak sanal mecralarda gerçekleştirilen yasadışı faaliyetler siber suç ya da bilişim suçu şeklinde ifade edilmektedir. Siber suç faaliyetlerini; bilişim sistemlerine yönelik ve bu sistemler vasıtasıyla gerçekleştirilen yasadışı faaliyetler olarak iki başlık altında gruplandırılmaktadır. Siber altyapıya yönelik gerçekleştirilen suçlarda sistemin ve

içeriğinin gizliliği, erişimi ve veri bütünlüğü tehdit altındadır. Örneğin internet tabanlı sağlanan bir bulut hizmetinde veriler ya da doğrudan depolama birimleri hedef alınmaktadır. İkinci olarak kimi suçların sanal ortama taşınarak dijital platformlar üzerinde gerçekleştirilmesi şeklinde gerçekleşmektedir. Örneğin dolandırıcılık suçunun internet tabanlı hizmet veren bir call-center görünümü altında sanal ağlar üzerinden gerçekleştirilmesi, sanat eserlerinin telifsiz paylaşımı, illegal maddelerin internetten pazarlanması gibi. (Gönen, 2016, s. 230).

Tarihte ilk bilişim suçu 1966 yılında "Minneapolis Tribune" adlı gazetede banka hesaplarında illegal değişiklikler yapması içerikli haberle kamuoyuna yansımıştır (Aydın, 1992, s. 13).

Küresel maliyeti trilyonlarca dolarla ifade edilen bilişim suçları, ilk işlendiği günden bu yana ulusal ya da uluslararası hukuki düzenlemelerde tarif edilmemiş diğer suç tipleri ile birlikte ele alınmıştır. Nitekim bu bağlamdaki tanımlama çabalarında da bir ittifaktan da söz edilememektedir. Dönmezer (1989) bu fiilleri; *"bilgisayarın kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek ahlakına aykırı davranışlar"* olarak tanımlarken, Yazıcıoğlu (1997) ise, *"ceza kuralları uyarınca, bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç içeren fiiller"* şeklinde tanımlamaktadır. Dolayısıyla bilişim suçlarını tarif ederken yalnızca bilgisayarı veya bilişim sistemlerini suçta kullanılan bir araç olarak gören bir tanım geliştirmek ya da bilişim suçlarını bilgisayar veya bilişim sistemlerine karşı işlenen fiillere hapsetmek konuyu dar alanda ele almamıza yol açacaktır. GPS (Küresel Konumlandırma Servisi) sistemleri, taşınabilir bellek, CD gibi bilişim teknolojilerinin teknik manada bilgisayar veya bilişim sistemi vasfı bulunmamaktadır. Ancak bu araçların bilişim teknolojileri içinde yer alan ve en azından veri depolayan ya da ileten birer araç olduğu kabul edilmektedir.

Bilişim teknolojilerine karşı işlenen tüm suçların bilişim suçu olduğunun kabulü de yanlış bir yaklaşım olarak karşımıza çıkmaktadır. Örneğin, failin mağdura ait tablet bilgisayarı hırsızlık amacıyla girdiği evden alarak daha sonra satması olayında hırsızlık suçu oluşmaktadır. Bu hâlde bilişim suçunun işlendiğinden bahsetmek mümkün olmamakla birlikte suçun konusunu bilgisayar oluşturmakta ve eylem neticesi mağdur bilgisayarda kayıtlı verilere ulaşamamaktadır.

Açıklananlardan hareketle bilişim suçlarının "*bilişim teknolojilerinin kendine özgü (sui generis) veri saklama, veri işleme ve veri iletme özelliklerinden bir veya birkaçının kullanılması suretiyle yine bu özelliklerin işleyişine, güvenliğine ya da bütünlüğüne yönelen suçlar"* olarak tanımlanması uygun olacaktır. Ayrıca bu tanımın bilişim teknolojilerinin kullanılması suretiyle işlenen klasik suçları dışladığı da hatırdan çıkarılmamalıdır.

Dünyada bilişim suçları yaygın olarak üç başlık altında sınıflandırılmaktadır.

- Veri ve sistemlere yönelik mahremiyet ve dokunulmazlığa ilişkin yasadışı girişimler,
- Bireysel veya iktisadi açıdan haksız menfaat sağlamaya yönelik yasadışı fiiller,
- Sanal ortamda üretilip yayılan içeriklere ilişkin konusu suç teşkil eden fiiller oluşturmaktadır (Turan, 2017, s. 46).

Deep web, Dark web ve Darknet gibi kavramlar genel olarak birbirinin yerine kullanılsa da esesan internetin farklı katmanlarını ifade etmektedir (Brown and Sirt, 2016 s. 2). Sınırlı erişim olanakları sunan bu katmanlar vasıtasıyla kimi kullanıcılar bazı kaynak veya hizmetlere illegal ve suç teşkil edecek şekillerde erişmesine imkân sağlamaktadır (Balduzzi ve Ciancaglini, 2015).

Kripto para birimleri günümüzde siber suçlar içerisinde çokça karşılaşılan bir metodtur. Teknolojik imkân kapasitesinin yaygın ve hızla kendini yükselten yapısı sayesinde büyük ölçekli siber suçlar, uyuşturucu kartelleri ile insan kaçakçılığı faaliyeti yürüten organizasyonlarla birlikte geleneksel yasadışı faaliyet yürüten örgütler incelendiğinde karşılaşılan tablo oldukça karmaşık bir görüntü vermektedir. İnternetin derin katmanlarında bir değer transfer aracı olarak anonimliği yüksek birçok kripto para birimi tercih edilmektedir. Birçok alternatif ve yüksek anonimlikleri ile kripto paralar yasal takip ve denetimleri oldukça zorlaştırmaktadır.

2.1.3.2.1. Bilişim Suçlarının Türleri

2.1.3.2.1.1. Bilgisayar Sabotajı

Tekil kullanıcılı bir sisteme ya da birçok bilgisayar sisteminden teşkil olmuş ağ sistemine izinsiz erişim ile sisteme müdehale ederek içeriğindeki verileri silmek ya da aslından farklı bir hale dönüştürmek olarak tanımlanabilmektedir. Saldırgan izinsiz eriştiği sistemin içeriğini görmekle kalmayıp sözkonusu verilerin kopyasını alabilir içeriği orijinalliğinden farklı hale getirebilir ya da bu içeriği üçüncü taraflara satabilmektedir. Bilgisayar sabotajlarında saldırganlar iki yöntem kullanmaktadırlar. Bunlardan ilki mantıksal ikincisi ise fiziksel sabotajlardır. Fiziksel sabotajı, fiziki şiddet uygulayarak sistemin zarar görmesi ve bilgilerin silinmesidir. Bunu yaparken amaç maddi zarara yol açmak değil sistemin çalışmasını engellemektir. Mantıksal sabotajda ise bilgisayar sistemleri aracılığıyla hedef sisteme ulaşarak, sistemi kullanılmaz hale getirmek amaçlanmaktadır (Bilek, 2012, s. 28).

2.1.3.2.1.2. Yetkisiz Erişim

Bir bilgisayar sistemine veya birden fazla sistemden meydana gelmiş bir ağa erişim izni olmaksızın giriş yapmak içeriğine erişmek olarak tanımlanabilmektedir. Bu suç faaliyetinde korsanın amacı saldırdığı sistem ya da ağda saklı olan veri ya da içeriğe izinsiz olarak sahip olmaktır. Bu eylemin icrası her zaman sistem veya ağa fiziksel bir yakınlık gerektirmemekte, uzak erişimler ile dünyanın herhangi bir yerinden söz konusu bağlantı gerçekleştirilebilmektedir Hizmete ilişkin gizlilik dereceli bilgi ve belgelerin şirket ve kurumların bilgisayar sistemlerinde muhafaza edildiğini düşündüğümüzde, bilgisayar sistemlerine erişen kişilerin bu kuruluşlara ciddi zararlar verebileceği ortadadır.

2.1.3.2.1.3. Bilgisayar Yoluyla Dolandırıcılık

Bilişim sistemlerindeki verilerin ve programların değiştirilmesi, sahte veriler girilmesi, mevcut verilerde tahribat yapılması gibi birtakım hileli hareketler sonucu haksız çıkar elde etmeğe yönelik eylemler, bilişim sistemlerinin aracı olarak kullanıldığı dolandırıcılık eylemleridir. Saldırılar çoğunlukla maddi bir değer elde etme arzusuyla gerçekleştirilmektedir. Buna ek olarak bazı saldırılarda amaç bir diğer tarafa mali bir zarar vermekte olabilmektedir. Bu yolla işlenen dolandırıcılık

suçlarının, suç işleme teknikleri açısından klasik dolandırıcılık tekniklerinden farklılıkları vardır. Bu suçlara örnek olarak sahte isimlerle e-postalar gönderilip cazip komisyonlar ve bedeller teklif edilerek, insanların tuzağa düşürülmesi gösterilebilir (Bilek, 2012, s. 29).

2.1.3.2.1.4. Bilgisayar Yoluyla Sahtecilik

Dijital ortamda tutulan bilgilerin üzerinde değişiklik yapmak sahteciliktir. Baskı teknolojilerinin gelişmesiyle birlikte evrak sahteciliğinde artış olmuştur. Yakalan zanlıların üzerinde çıkan sahte kimlikler alışılmış bir durumdur. Bugün itibar sahibi kişi ve kuruluşların unvan ya da isimlerini kullanmak suretiyle gönderilen bir elektronik posta içeriği veyahut benzer şekilde söz konusu itibarı çağrıştıracak bir internet sayfası kötü amaçlara hizmet edebilmekte sadece maddi kayıplar değil manevi itibar kayıplarına da sebep olabilmektedir. Ayrıca resmi evraklar üzerinde yapılan değişikliklerle söz konusu evraklar bir suç nesnesi haline dönüşmekte, adli bilişim safhasında yapılan incelemeler bu suç türünün aydınlatılmasına yeterince olanak vermemektedir (Akıncı, Alıç ve Er, 2003, s. 158).

2.1.3.2.1.5. Bilgisayar Yazılımının İzinsiz Kullanımı

Hukuki literatürde ‘eser’ olarak atfedilen yazılımlar lisanssız ya da eser sahibinin izni olmaksızın kullanılması çoğaltılması vb. yöntemlere hak ihlaline sebep fiillere konu olması durumundu gerçekleşmiş olmaktadır. Bu nevi yazılımların satış sözleşmeleri dâhilinde bulunan lisans sözleşmeleri gereği, söz konusu yazılımın aksi belirtilmediği sürece yalnızca tek kopya olarak kullanılabileceği ve üçüncü taraflara bu içeriğin kiralanamayacağı şeklinde hukuki bağlayıcılıklar içermektedir (Koç ve Kaynak, 2009, s. 28).

Korsan yazılımın ülkemizde gelişim göstermesinin sebebi orijinal yazılımların pahalılığı ve özellikle ticari amaçla kullanılan Office yazılımları ile görüntü ve grafik işleme yazılımları konusunda, işletmelerin istihdam girdi maliyetini düşürme çabasından kaynaklanmaktadır. Korsan yazılımların rahatlıkla elde edilebilir olması, her türlü yazılım ve materyalin tüketicilere ucuz ve kolay bir şekilde ulaşmasını sağlarken, her alanda yetkin ve kendini yetiştirmiş nitelikli elemanların

ortaya çıkması ve yazılım alanında daha fazla sayıda insanın yasal olamayan bu tip kaynaklara erişebilmesi imkânını doğurmuştur (Bilek, 2012, s. 30).

Korsan yazılım kullanılmasının neden olduğu vergi kayıpları, virüs ve solucanların yayılmasından ortaya çıkan güvenlik sorunları, yasal süreçleri uygulayan firmaların korsan yazılım kullanan firmalarla rekabet edememesi ve bilginin değersizleşip ucuzlaşması ve önemsizleşmesi kültürünün ortaya çıkmasına sebep olmaktadır (Bilek, 2012, s. 30).

2.1.3.2.1.6. Verilere Yönelik Suçlar

Avrupa Konseyi bünyesinde Türkiye'nin de imzaladığı, *"Siber Suçlar Sözleşmesine"* göre taraf ülkeler verilerin güvenliğini korumaya yönelik tedbirler almak zorundadır. Veri hırsızlığı, verilerin izinsiz olarak akışının engellenmesi, tahrif veya yok edilmesi veri suçu olarak değerlendirilmektedir. Bilişim sistemleri üzerinden yapılan bu suçlar mağdurun kişisel verilerinin elde edilip kötüye kullanılması ve maddi kazanç elde edilmesi şeklinde olur. İnternet ortamında kullanıcılar hakkında veri toplamaya veri korsanlığı denir. Bu uygulama reklam ve istatistik amacıyla yapılmakta çoğunlukla kişisel bilgisayarlarda ve internet servis sağlayıcılarındaki kişisel bilgiler kredi kartları ve banka hesaplarına ilişkin bilgilerin çalınmasını amaçlamaktadır (Demir, 2002, s. 481).

2.1.3.2.1.7. Yasadışı Yayınlar

Suç olarak nitelendirilecek içeriklerin sanal mecra ya da bilgisayarlar vasıtasıyla yayınlanması veya transfer edilmesi şeklinde ifade edilmektedir. Hukuki olarak yasaklamış dijital içerikler; web sayfaları, elektronik postalar ve bu amaçla kullanılan benzer tüm sistemleri kapsamaktadır. Suç teşkil eden yayınlar, web üzerinden belirli bir kişi veya zümreyi hedef alan ve hakaret niteliği taşıyan internet siteleri ve elektronik dokümanlar olabilir.

2.1.3.2.1.8. Terörist Faaliyetler

Bilgisayar sistemleri vasıtasıyla ulusal ölçakte ve bu hususdaki menfaatlerin zarara uğratılmasını hedef alan, bu amaç için kişisel motivasyonu yüksek ve bir

ideolojiden beslenen, maksatlı eylemler terörist faaliyet olarak tanımlanabilmektedir (Atıcı ve Gümüş, 2003, s. 57).

Ülkemizde internet üzerinden yapılan terörist faaliyetler kullanıcının tespiti zor olduğu için internet kafeler üzerinden yapılmaktadır. Aynı şekilde hakaret ve şantaj içerikli e-postalar ve sahte ihbarlar yine internet kafeler üzerinden yapılmakta, oturum ve kullanıcı takibi yapmayan ve güvenlik kamerası olmayan denetimsiz yerlerden yapılan bu saldırılarda failin tespiti güçleşmektedir (Bilek, 2012, s. 31).

2.1.3.2.1.9. Çocuk Pornografisi

Dijital teknolojilerdeki gelişmelerle paralel olarak üretilen dijital içeriklerin internet üzerinden dolaşımı ve yayılması çok daha basit ve hızlı gerçekleşmektedir. Teknolojideki bu değişim internetin zararlı yönlerinden biri olan pornografik içereklerin hazırlanmasına ve dağıtımına katkıda bulunmuştur. Bu istenmeyen gelişme toplumların ahlaki değerlerine yönelik önemli bir tehdittir. Çocuk pornografisi, genel anlamda 15 yaş altındaki çocukların cinsel istismarını içeren dijital içerikler olarak ifade edilmektedir. Bu bağlamda söz konusu içeriklerin üretimi ve dağıtımı yasaktır. 'Child porn (çocuk pornosu)' cümleciğini aratma konusunda Pakistan dünyada birinci sırada yer almaktadır (Bilek, 2012, s. 31).

2.1.3.2.1.10. Kartlı Ödeme Sistemlerinde Sahtecilik ve Dolandırıcılık

Bankacılık hizmetlerini ve en yaygın hizmetlerinden olan bankacılık kartlarının kullanımı her geçen gün artmaktadır. Buna paralel olarak bu araçların çeşitli suçlarla anılması da giderek yükselmektedir. Bu bağlamda çeşitli dolandırıcılık yöntemleri ile banka kartlarının kopyalanması çok yaygın suçlardan biridir. Dolandırıcılar ele geçirdikleri bu çalıntı kartlar ile altın ve mücevher, akaryakıt, teknolojik cihazlar gibi ürün ve hizmetleri satın almak suretiyle gelir sağlamaktadır.

Kredi ve banka kartları dolandırıcılığı interaktif yöntemlerle yapılabileceği gibi bilgisayar sitemleri ile klasik dolandırıcılık yöntemlerinin birleştirilmesi suretiyle de yapılabilir. Sözü edilen sahtecilik ve dolandırıcılık şekli incelendiğinde, gerçek dışı vatandaşlık bilgileri ve belgeleriyle başka tarafların banka hesaplarından finansal transferler gerçekleştirilmesi, banka ve finansal işlem yapan kurumlardan normal

şartlarda temin edilemeyecek bir kredinin gerçek dışı beyanlar, belgeler ya da bilgilerle kullanılmaya çalışılması şeklinde gerçekleşebilmektedir (Bayraktar, 2000, s. 72).

2.1.3.2.1.11. Ortam Dinlemesi ve Cep Telefonu Güvenliği

İletişim özgürlüğü ve gayrı resmi yollardan müdahale edilemezliği dünya üzerinde modern devlet sistemlerinin anayasalarında teminat altına alınmış olup, iletişim ve haberleşme süreçlerine ilişkin kısıtlamaların yalnızca ilgili yasal zorunluluk halleri dâhilinde ve mahkemelerin ilgili izni ile gerçekleştirilebilmektedir. Bu bağlamda hukuki çerçeveyi denetleyen ve uygulayan kurumlar görev yapmaktadır. Üçüncü tarafların illegal yol ve yöntemlerle iletişimi dinlemesi kayıt altına alması bunları yayması bir suç olarak tanımlanmaktadır. Ayrıca bu yolla elde edilen veriler yargı mercileri tarafından delil olarak da kabul görmemektedir.

Ortam dinlemesi, iletişimin ya da konuşmanın gerçekleştirildiği fiziki ortamın teknik kapasiteli sesi kaydetmeye imkân sunan aletler ile ya da ileri teknolojik araçları kullanmak suretiyle gerçekleştirilebilmektedir. Teknolojinin hızla ilerlemesi güvenlik ihlallerine ve bilgi güvenliğine büyük bir etki bırakmıştır. Bu etki ancak güvenlik prensiplerine tam ve kayıtsız bir şekilde uygulamakla bertaraf edilebilir. Öte yandan ortam dinlemesi yöntemi ile iletişimin dinlenmesi devletlerin en çok tedbir aldıkları bir istihbarat toplama şekli olarak da oldukça kullanılan bir yöntemdir. İletişimde kullanılan teknolojilerin sürekli tazelenmesi kablosuz ve mobil cihazların yaygın olarak tercih edilmesi onları bazı açılardan da güvenlik sorunlarıyla anılır hale getirmektedir (Sağıroğlu ve Bulut, 2009, s. 499).

Günümüzde mobil ya da analog telefonların haberleşme süreçlerine girilmesi, dinlenmesi, yasalarca yasaklanmış olmasına rağmen bu suçu işlemek için teknik altyapı sağlayan yazılımlar ve araçların temin edilmesi oldukça kolaydır. Diğer taraftan son kullanıcıların kişisel verilerini alışveriş tercihleri gibi istatistiki kayıtlarının operatör sağlayıcıları tarafından satılıyor olması bu süreci kolaylaştırmaktadır.

2.1.3.2.1.12. Dijital Aktivizm

Dijital aktivizm bireylerin sosyal medya ve internet aracılığıyla sosyal veya politik konularda kamuoyu oluşturarak eylemler tasarlayabilmek ve bu eylemlerle düşünce ve/veya siyaseti tasarlayabilmektir. Bu tanım ile masum bir amaca hizmet etse de otorite aleyhinde eylem yapmak, devleti yönetimini şeffaflaşmayı sağlamak için yasadışı yollarla devletin gizli bilgilerini ele geçirip internet ağları üzerinden yaymak suç oluşturmaktadır. Sansürden uzak ve özgür bir iletişim ideal olarak kabul edilse de özel hayatının gizliliğini ihlal eden ve ülkenin milli güvenliği ile uluslararası platformda saygınlığını sarsacak olan her türlü eylem engellenmelidir.

Amerika Birleşik Devletleri'nde diplomatik belge sızıntısı olarak kabul edilen Wikileaks olayı uzun süre dünya gündemini meşgul etmiştir. 25 Temmuz 2010'da Ocak 2004 ve Aralık 2009 tarihleri arasındaki Afganistan'daki savaşı anlatan 77 bin savaş günlüğü WikiLeaks.org tarafından açıklanmış ve birçok fikir ayrılığı ve tartışmaya yol açmıştır. Bu olay ülkelerin diplomatik yazışmalarına kadar da kolayca erişilip yayılabileceğini tüm dünyaya göstermiştir. Ayrıca sosyal medya Mısır, Tunus ve Libya gibi ülkelerde her türlü sansür ve engellemelere karşın internet üzerinden iletişimi sürdürmüş. Facebook üzerinde oluşturulan gruplarla birleşen insanlar sokaklara dökülmüş ve bu ülkelerde çok da barışçıl olmayan metotlarda sergilenerek ülke yönetiminde değişikliklere gidilmiştir (Bilek, 2012, s. 35).

2.1.3.2.2. Bilişim Suçlarının İşlenme Yöntemleri

2.1.3.2.2.1. Bilişim Korsanlığı (Hacking)

Hack, izinsiz olarak sisteme girilerek sistemin işleyişini kontrol etme ve sistemdeki verilerden bilgi sahibi olma ve sistemin işleyişini durdurma veya yönlendirmedir. Bu saldırıların çoğunluğu yazılım üreticiler tarafından gerekli durumlarda uzaktan müdahaleyle teknik destek sağlamak amacıyla kodlanan bu sistem açıklarını gerçekleştirilmektedir (Yılmaz, 2004, s. 381).

Bilişim korsanı ya da yaygın ifade şekliyle *"hacker"* niteliğine haiz kişiler, yasadışı yollarla elde ettikleri verileri nakte çevirmek isterler. Saldırı (hack) teknikleri konusunda yeterince bilgi sahibi olmayıp nasıl bilişim korsanlığı yapılacağını internet veya yazılı dokümanlardan öğrenerek saldırılarda bulunan kişilere de lamer denir. Lamerlerin alt seviye programlama bilgisi olmayıp genellikle HTML (Hiper Metin

İşaretleme Dili) kodlamasını öğrenip web sitelerine veya internet kullanıcılarına saldırıda bulunurlar. Web ve e-posta saldırıları dışında saldırı yöntemlerini genellikle tercih etmemektedirler (Bilek, 2012).

2.1.3.2.2.2. Gizli Kapılar (Trap Doors)

Trap Doors olarak ifade edilen gizli kapılar, yazılım geliştiriciler tarafından geliştirdikleri programa olası teknik destek taleplerine uzaktan erişmek ya da güncellemeler göndermek amacıyla bırakılan çeşitli erişim imkânlarını ifade etmektedir. Bu tür amaçlarla hazırlanan yazılımların henüz işletim sistemlerinin kurulumu aşamasında de aktif edilmesi veya tümüyle silinmesi olası riskleri minimuma indirmektedir.

2.1.3.2.2.3. Truva Atı

Yasal olarak lisanslanmış ve satın alınıp kullanılmakta olan bir yazılım üzerinde olağan çalışıyormuş izlenimi verip, gizli komutlar çalıştırarak kontrol dışı komutlar gerçekleştiren yazılımlardır. (Yılmaz, 2004, s.381).

Sinsi bir şekilde bulundukları sistem üzerinde çalışan truva atlarını bir çeşit virüs ya da solucan yazılım olarak tanımlamak da mümkündür. Bu zararlı yazılımlar illegal olarak internetten indirilen ses, veri ya da görüntü dosyalarının içerisine gizlenmiş şekilde bilgisayarlarımıza indirilmektedir. Bir diğer yöntem olarak da e-postalar vasıtasıyla gönderilmektedir. Bu yazılımlar sunucu ve istemci olmak üzere iki bileşenden teşkildir. Sunucu tarafı saldırı altındaki terminalde konuşlu yazılımı, istemci de sunucudaki solucanı kontrol eden ve saldırgan terminaldeki yazılımı ifade etmettedir (Bilek, 2012).

2.1.3.2.2.4. Ağ Solucanları ve Virüs

Virüsler ya da başka bir ifadeyle Ağ solucanları, yerleşip çalıştıkları bilgisayar sistemlerinde otomatik olarak aktifleşen, herhangi bir emare göstermeden gizlice çalışabilen ve genel olarak kendini sürekli kopyalamak üzerine kurgulanmış mini programlardır. Virüsler yerleştikleri sistemlerde farklı olumsuz etkiler meydana getirebilmektedir. Kendini kopma etmek üzere bir mantıkla kurgulandıklarından dolayı az zamanda sistemleri kullanılmaz duruma getirecek kadar çok

yayılabilmektedirler. Bu tür yazılımların ayırt edici unsurları, bilgisayar programları, dosyalar veya çok kullanıcılı ağlar arasında çok rahat kopyalanabilmeleridir. Zararlı yazılımların bu şekilde kopyalanması süreci *"virüs bulaşması"* olarak da ifade edilmektedir (Akbulut, 1999).

Sistem virüsleri bilgisayar kullanıcısının kontrolü dışında bilgisayarın olağan işleyişini bozan ve görünürde kendini belli etmeyerek arka planda çalışan bir çeşir yazılımdır. Virüs geniş manada zararlı programlar olarak tanımlansa da özgün karakteri gereği aktif olması ve kendini kopyalaması gerekmektedir (Önemli, 2004).

2.1.3.2.2.5. İstem Dışı Elektronik Postalar (Spam)

Sanal ortamda bir iletinin oldukça fazla kopya ile herhangi bir talep ya da evvelinde bir iletişim trafiği olmaksızın, tekil kullanıcılara bir tür zorbalıkla ulaştırılması spam olarak ifade edilmektedir. Spamlar daha çok bir ticari içeriğin tanıtımı niteliğinde olmakla birlikte güven uyandırmayan ürün ve hizmetlerin legalliği tartışmalı iddialı içerikler barındıran kampanyaların tanıtılması olarak karşımıza çıkmaktadır. Sanal mecrada sıklıkla karşılaşılan iki tip spam bulunmaktadır. Bunlardan ilki direkt olarak belirlenmiş bir hedef kitleye odaklanmış spamlardır. Bu hedef kitlenin belirlenmesindeki en büyük veri kaynakları forumlar ve arama motorları üzerinden sağlanan açık kaynak üyelik listeleri ve çeşitli yöntemlerle aynı listelerin yasadışı temin edilmesi ile gerçekleştirilmektedir. Bir diğer spam yöntemi de, temin edilen e posta adreslerine hiçbir kategori filtresi uygulanmaksızın kitlesel bir ileti gönderilmesi şeklinde yapılmaktadır. Bu yöntemde bir ürün veya ticari bir tanıtım amacından ziyade herhangi bir konuda olabildiğince çok kişiye içeriği iletmek amaçlanmaktadır. Daya çok soyut nitelikte olup bir propaganda, politik bir fikir ya da kitlesel bir algı oluşturmayı amaçlamaktadır.

Spam saldırılarına yönelik alınabilecek en kolay savunma, posta kutularının filtrelenmesiyle kolay bir şekilde sağlanabilmektedir. Bu sayede gönderilmiş spam içerikleri kullanıcıya erişememektedir.

2.1.3.2.2.6. Mantık Bombaları

Tekil kullanıcıların bilgisayar sistemlerinde ya da daha çok kullanıcı barındıran ağ sistemlerinde bir takım öncül gerekliliklerin sağlanmasıyla birlikte

olumsuz sonuçlara neden olabilen yazılımlardır. Bu yazılımlar sistem üzerinde henüz çalışmıyorken truva atlarına benzer özellikler göstermektedirler. Buna karşın çalışmaya başladığı andan itibaren sitem üzerinde yıkıcı etkiler meydana getirmektedir. Mantık bombalarının en bilinen örneklerden biri periyodik olarak her 26 nisanda aktifleşen Chernobil virüsüdür.

Mantık bombası gibi hareket eden bir diğer sistem de kendisini kopyalayarak kolonileşen ve bilişim sistemine gereksiz komutlar vererek yavaşlatan tavşan yazılımlarıdır. Bu yazılımların tek amacı belirli bir tarih ve saat ile başlayarak kendini sürekli kopyalayıp bellek işgal etmektir.

2.1.3.2.2.7. Phishing (Password Hacking- Şifre Saldırısı)

Kurbanlarının sosyal eğilimlerinin belirlenerek tıpkı onu tanıyormuş gibi psikolojik yöntem ve teknikleri de kullanarak, kişisel bilgilerinin yanı sıra, finansal kimlik ve şifreler gibi gizlilik ihtiva eden bilgilerin çalınması şeklinde ifade edilmektedir. Phishing kelime karşılığı olarak İngilizce'de balık tutmak fiiline karşılık gelen bir kelimedir. Bu yöntemde de kurban bir balık olarak tasvir edilmektedir. Saldırgan öncelikle bir elektronik posta hesabı üzerinden kurbana bir spam iletisi gönderir. Söz konusu bu ileti kurbanın bankasından gönderiliyormuş gibi görünen bir algı uyandıran, birtakım güncellemelerin girilmesini isteyen sahte bir link içermektedir. Bu sahte link önceden hazırlanmış ve ilgili finans kuruluşunun internet sayfasını taklit etmektedir. Kurban bu sayfada kendinden talep edilen bilgilerini güncellemek maksadıyla aldanarak kendisi paylaşmaktadır. Dolandırıcılar topladıkları tüm bu bilgileri kullanarak kurbanın aleyhine haksız çıkar elde etmektedirler. Bu yöntemle işlenen bilişim suçları Phishing olarak tanımlanmakta ve geniş bir mağdur kitlesi yaratmaktadır.

2.1.3.2.2.8. Sniffer (Koklayıcı)

Sniffer Türkçe karşılığı olarak koklayıcı manasında kullanılmaktadır. Yerel bilgisayar ağları üzerindeki veri trafiğinin ele geçirilmesi şeklinde ifade edilebilir. Bir yerel ağa konuşlanmış sniffer'in varlığından söz edildiğinde, bu sniffer'i kontrol eden saldırgan; örneğin bir internet tarayıcısı üzerinde girilen bir şifreyi kolaylıkla ele geçirebilmektedir (Bilek, 2012, s. 41).

2.1.3.2.2.9. Tuş kaydediciler

Bugün internet ağı üzerinden kullanıcılar tarafından sayısız içerik transferi gerçekleştirilmektedir. Kullanıcıların birbirlerine gönderdikleri ses, metin ve görüntü gibi dijital dosyalara saklanmış olarak karşı kullanıcının rızası dışında bilgisayarına konuşlanıp aktif olan özellikler barındıran yazılımlara tuş kaydediciler (keylogger) denir. Bu yazılımlar konuşlandığı bilgisayarda çalıştığı andan itibaren kullanıcının tüm klavye kaynaklı girişlerini veya fare hareketlerini kaydederek yazılımın yaratıcısına geri rapor etmektedir. Böylelikle kurbanların bilgisayarlarında bulunan kişisel veriler ile şifreler gibi kritik önem arz eden bilgiler çalınmaktadır.

2.1.3.2.2.10. ARP Zehirleme

Bilgisayar üzerinden saldırılar gerçekleştiren kişilerin, yerel ağlarda dilediği gibi yayın gerçekleştirmesi *"Adres Çözümleme Protokolü"* ARP zehirleme olarak tanımlanmaktadır. *"Man In The Middle"* yöntemi olarak da bilinen bu yöntem ile saldırganlar yerleşik sistemleri manipüle etmek suretiyle, ağ trafiğini by-pass ederek veri akışının kontrolünü ele geçirmektedir.

2.1.3.2.2.11. DNS Aldatmacası

Saldırıya uğrayan Alan Adı Sunucusularının ayarlarına müdehale edilerek kontrol dışı farklı bir sunucuya yönlendirilmesidir. Sözü edilen yönlendirme saldırısı DNS aldatmacası olarak tanımlanmaktadıruygulamada DNS aldatmacaları genellikle ARP zehirleme saldırılarıyla birlikte gerçekleştirilmektedir.

2.1.3.2.2.12. DOS (Hizmet Engelleme Saldırısı) Saldırısı

DDOS (Distrubuted Denial of Service) saldırıları, sistemleri çalışamaz hale getirmeyi amaçlayan siber saldırı türüdür. DDOS yöntemi DOS sistemlerine çok sayıda yabancı sistem üzerinden saldırılarak gerçekleştirilmektedir. Bu saldırılarda kullanılan yabancı sistem IP'leri çoğunlukla taklit adreslerden oluşmakta ya da köle terminaller tercih edilmektedir.

2.1.3.2.2.13. XSS ve XSRF

HTML tabanlı hazırlanmış kodlara istemci kodlar yerleştirilmesi ile saldırı gerçekleştirilecek taraftan talep edilen istemcinin aktifleştirilebilmesi XSS (Cross Site Scripting) olarak adlandırılır. Bu yöntemle oluşturulan açıklar çoğunlukla saldırganların bir olasılığı sınaması ile tesadüf eseri keşfedilmektedir. Saldırganlar keşfettikleri bu açıklar üzerinden saldırının gerçekleştirildiği kullanıcının bilgilerini ele geçirebilmektedirler. XSRF (Cross-Site Request Forgery) ise saldırganların, belirli internet alanlarına, alan yöneticilerinin tehdit beklemediği bir kullanıcı üzerinden geliyormuş gibi görünerek izinsiz komutlar yönlendirmesi olarak ifade edilebilmektedir. Bu şekilde gerçekleştirilen saldırılara *"session riding"* veya *"hostile linking"* denilmektedir.

2.1.3.2.2.14. İnternet Bankacılığı Dolandırıcılığı

Banka ve finans kuruluşlarının mobil ve internet tabanlı sundukları hizmetlerine erişirken kullandıkları ID ve giriş şifrelerinin çeşitli vasıta yazılımları kullanarak saldırganlarca çalınmasıdır. Bu yönten ile gerçekleştirilen saldırılarda amaca uygun casus programlar tercih edilmektedir. Çalınan hesaplara ilişkin bilgiler kullanılarak örgüt mensupları ya da sahte hesaplara transferler gerçekleştirilmektedir.

2.1.3.2.2.15. Kredi ve Banka Kartlarını Sahteciliği

Bankacılık hizmetlerini ve en yaygın hizmetlerinden olan bankacılık kartlarının kullanımı her geçen gün artmaktadır. Buna paralel olarak bu araçların çeşitli suçlarla anılması da giderek yükselmektedir. Bu bağlamda çeşitli dolandırıcılık yöntemleri ile banka kartlarının kopyalanması çok yaygın suçlardan biridir. Dolandırıcılar ele geçirdikleri bu çalıntı kartlar ile altın ve mücevher, akaryakıt, teknolojik cihazlar gibi ürün ve hizmetleri satın almak suretiyle gelir sağlamaktadır. Benzer şekilde belli işletlelere yerleştirilen pos cihazları ve atm makinalarına yerleştirilen aparatlar ile kart bilgileri çalınabilmektedir.

2.1.3.2.2.16. TEMPEST

TEMPEST kavramının bir kısaltma olup olmadığına dair günümüzde dahi tartışmalar yapılmaktadır. Fakat Amerikan Hava Kuvvetleri tarafından gizlilik

dereceli bir evrakının gizliliğini kaldırdıktan sonra yayımladığı belgeye göre TEMPEST kısaltmasının açılımı "Transient Elektromagnetic Pulse Emanation Standard" şeklinde yer almaktadır (USA Air Force, 1998).

TEMPEST güvenlik seviyesi yüksek verileri işleyen özel elektronik araçların neden olduğu istenmeyen elektromanyetik enerji yayılımları şeklinde gerçekleşen bilgi sızıntıların saptanması ve bunlara yönelik çözüm çabaları olarak tanımlanmaktadır. TEMPEST sızıntıları kontrol dışı gelişen, gizlilik içeren bilgiler içermektedir. Bu bilgiler bir frekans düzleminde ortama yayılmakta ve kablosuz ya da kablolu sondajlarla elde edilmektedir. İlk elde edildiğinde anlamlı olmayan verilerdir ve bunların anlamlı bilgilere dönüştürülebilmesi için bir dizi kod çözüm süreçlerinin işletilmesi gerekmektedir (Altıner ve Şaykol, 2013). TEMPEST kaçaklarına yönelik standartların sağlanması ve bu sızıntıların önüne geçebilmek için bu amaca yönelik geliştirilmiş yüksek teknolojili cihazların doğru yerde doğru şekilde kullanılması önem taşımaktadır.

2.1.3.2.2.17. Cep Telefonu Casus Yazılımları

Günümüz teknolojisinin kısa sürede geldiği nokta itibariyle cep telefonları artık her yere taşınan birer kişisel bilgisayara dönüşmüştür. Gerek teknik özellikleri gerek işletim sistemleri ve mobil uygulama kapasiteleri göz önüne alındığında, olumsuz amaçlara yönelik uygulamalar geliştirilebilmektedir. Mobil araçlar üzerinden gerçekleştirilen ses, görüntü ve her türlü dijital iletişim sürecine müdahale edilmesi ve mahremiyete yönelik saldırılar gerçekleşebilmektedir. Akıllı telefonların dijital mağazalarından erişilebilen kimi yazılımlar konusu suç teşkil edebilecek olumsuz amaçlara hizmet edebilmektedir. Örneğin ortam dinlemesi, görüşmelerin dinlenmesi ve kayda alınması, konum verilerinin izinsiz paylaşımı, sms mail ve arama kayıtlarının bilgisiz iletimi gösterilebilmektedir.

2.1.3.2.2.18. Gizlice Dinleme

Gelişen teknolojiyle birlikte kablosuz yeniliklerin hayatımıza girmesi birçok amaca hizmet eden ürünleri de hayatımıza dahil etmiştir. Bazı kablosuz cihazlar bulundukları alandaki sesleri dijital sinyallere dönüştürerek özelliklerinin desteklediği uzaklığa kadar alıcısına eriştirebilmektedir. Bu teknik ile alıcı, cihazın bulunduğu

ortamdaki sesleri dinleyebilmektedir. Özellikle devletler, gizlilik düzeyi yüksek işlerle ilgilenen kurum ve kuruluşlar ile kimi şirketler ortam dinlemesi tehdidine yönelik periyodik önlemler almaktadırlar.

Dinleme cihazları çok küçük boyutlarda araçlar olması sebebiyle bir bakışta görülebilmesi çok mümkün değildir. Kimi zaman da bir eşya ya da başka bir aracın içerisine yerleştirilebilmektedir. Bu amaca yönelik geliştirilen dinleme araçlarının en zayıf tarafı kapsama alanlarının düşük olması ve çok uzak olmayan mesafelere iletim yapabilmesidir. Mesafe konusundaki bu kısıtlayıcı problem, saldırganlar tarafından mobil telefonlar tercih edilerek aşılmaya çalışılmaktadır.

Cep telefonlarının da pil problemlerine yönelik olarak ise enerji ve mesafe sorunu olmaksızın geliştirilen GSM uzatmalı prizler kullanılmaktadır. Benzer biçimde bilgisayardan beslenen ve içine bir SIM kart yerleştirilen bilgisayar çevre birimleri üzerinden de dinleme yapılabilmektedir. Bu yöntemlere ek olarak dinleme amaçlı kullanılan, GSM Intercept A5.41 ChatterGuard cihazları, Kızılötesi Uzaktan Dinleme sistemleri, Paralel Telefon Vericileri ve birçok böcek cihaz da kullanılmaktadır.

2.1.3.3. İnsan Ticareti ve Göçmen Kaçakçılığı

Suç örgütlerinin yoğun faaliyet gösterdiği alanlarından birisini, yasadışı göçmen kaçakçılığı ve insan kaçakçılığı suçları oluşturmaktadır. Göçmen kaçakçılığının en önemli nedeni insanları bulundukları bölgelerdeki yaşadıkları çeşitli istikrarsız ortamlar ve daha iyi bir yaşama sahip olma arzusudur. Ekonomik yetersizlikler, savaş ve çatışma bölgeleri insanların daha huzurlu gördükleri bölge ve ülkelere göç etme heveslerini arttırmaktadır.

Göçlerin tarihinin çok eski olduğu açıktır. Göçmen ve mültecilik ile ilgili çalışmalar özellikle 20. yüzyılda şekillenmeye başlamıştır. Göç ve göçmenlik sorunları ve paralelinde suçlar ile en belirgin sorunlar 20. yüzyılda yaşanmaya başlamıştır. Göçmen kaçakçılığı ve insan ticareti aynı zamanda yasal olmayan ciddi bir kazanç kapısına dönüşmektedir. Yasadışı göçler nedeniyle sosyal yaşamda büyük değişiklikler meydana gelmekte, ülkelerin ve büyük şehirlerin görüntülerinde önemli değişiklikler oluşturmaktadır. Yasadışı göçler ve insan kaçakçılığı suçlarında en önemli artış; Sovyetler Birliği'nin dağılması sonrasında, iki kutuplu dünya düzeninin bozulduğu ve küreselleşmenin geliştiği doksanlı yıllardan sonra yaşanmaya

başlanmıştır. Göçmen ve insan kaçakçılığı ile insan ticareti suçlarını öncelikle iki başlık altında incelemek uygun olacaktır. Birincisi göçmenlere yasadışı sınır geçişi imkânı sağlayarak, gelişmiş ve istikrarlı ülkelere bu insanların nakledilmesi göçmen kaçakçılığı diye tanımlanan suçlar ikincisi ise fuhuş, yasadışı çalıştırma, yasadışı organ temini, insan kaçırarak ticaretinin yapılması şeklindeki insan kaçakçılığı suçlarıdır.

Göçmen ve insan kaçakçılığı suçunun genel olarak tanımı konusunda farklı yaklaşımlar mevcuttur. Çalışma yapan kişilerin, kendi disiplinlerine göre ele alarak tanımlar yapmaktadırlar. Genel bir tanımlamayla insan kaçakçılığı veya insan ticareti fuhuş yaptırmak, organ ve doku nakli, yasadışı işçi çalıştırılması gibi nedenlerle zorla insanları kaçırarak ve suça konu olacak şekilde insana iradesi dışındaki eylemlerin yaptırılması şeklinde ifade edilebilir.

2.1.3.4. Silah ve Mühimmat Kaçakçılığı

Silahlar çağlar boyunca insanın kendini koruması, doğadan istifade etmesinin bir aracı, kendini güvende hissetmesinin bir yolu, toplumsal ve sosyal hayatın ve kültürlerin bir parçası olmuştur. Bunun yanında insanoğlunun kendi kendine zarar verebilmesinin de en çok kullanılan araçlarından birisidir. Özellikle ateşli silahların icadı, bu silahların yirminci yüzyıldan itibaren insanın hayal gücünü zorlayacak gelişmesi insanlığı bambaşka tehlikelerin içine sokmuştur. Silah kaçakçılığı konusunun anlaşılması için silah kavramındaki tanımların sınıflandırılması faydalı olmaktadır. Genel olarak silahlar küçük silahlar, hafif silahlar, ağır silahlar ve kitle imha silahları şeklinde dört başlık altında tasnif edilmektedir.

Avrupa Güvenlik ve İş birliği Teşkilatı'na (AGİT) göre; Görevlerini silahlı olarak ifa eden güvenlik kuvvetlerince kullanılan tabanca, yivli tüfek, karabina (kısa tüfek) ve hafif makinalı tüfekler küçük silah olarak tanımlanmıştır. (AGİT) Hafif silahlar ise; ağır makinalı tüfekler ile bunlara takılan bomba atarlar elle taşınır uçaksavar ve tanksavarlar, geri tepmesiz tüfekler, tanksavar ve uçaksavar füze ve roketatarlar lançerleri, taşınabilir uçaksavar füze lançerleri ile 100 mm'den düşük kalibreli havanları kapsamaktadır" (Harp Araç ve Gereçleri ile Silah, 2007). Kitle imha silahları yirminci yüzyılda, uluslararası ilişkileri etkileyen önemli bir saha haline gelmiştir. Kitle imha silahları üç temel silah türü; nükleer, kimyasal ve biyolojik

terimlerinin baş harflerinin yan yana getirilmesinden oluşan NBK (İngilizce: NBC) terimi ile ifade edilmektedir. Atom çekirdeğinin bir dizi sürece tabi tutularak sonucunda gelişen zincirleme reaksiyon neticesinde büyük bir enerji açığa çıkaran düzeneklerden elde edilen silahlar nükleer silah olarak tanımlanmaktadır. Tahrip gücü yüksek bir patlama ile çevreye radyoaktif parçacıklar nedeniyle uzun süreli zararları olan silahlardır. Gözle görülmeyen boyutlardaki virüs ve bakteri gibi biyolojik varlıklar ile biyolojik reaksiyonlara neden olan maddelerin bilinçli şekilde hastalık yaymak ya da öldürmek kastıyla kullanılan silahlardır. Kimyasal Silahlar, Sonuçları itibarıyla maruz kalınması durumunda canlıların solunumları ve sistemini etkileyen, yakıcı ve zehirleyici sonuçları olan kimyasal içeriklerden sıvı ya da gaz şeklinde üretilmiş silahlardır.

Silah kaçakçılığı küresel silah ticaretinin yanında toplu silah kaçakçılığı ve bireysel silahlanma konularını da kapsamaktadır. Toplu silah kaçakçılığı terör ve suç örgütleri, çeşitli grupların silah ihtiyaçlarını karşılamakta, bireysel silahlanmayı beslemektedir. Bireysel silahlanma ise son yıllarda ön plana çıkmaya başlamıştır. Bireysel silahlanma toplum yaşamına olumsuz etkileri değerlendirilmesi gereken bir konudur. Yasadışı silah ticareti Silah mühimmat kaçakçılığı, özellikle sıcak savaş ve çatışmalar ile bu ihtimallerin yüksek seyrettiği, terör faaliyetlerinin işlendiği alanlarda yoğunlukla görünmektedir. Suç örgütlerinin birbirlerini tamamlayan en önemli saha silah kaçakçılığı olmakla birlikte, bu faaliyetler için en önemli finans kaynağı sağlama yöntemi uyuşturucu kaçakçılığıdır.

2.1.3.5. Yolsuzluk

Yolsuzluk kavramı son dönemlerde suç örgütlerinin faaliyet alanları içinde en önemlilerden birisi olarak değerlendirmektedir. Uluslararası suç örgütlerinin faaliyet alanlarından birisidir. Yolsuzluk kavramı son dönemde uluslararası güvenlik sorunları içinde ele alınmaya başlanmıştır. Uluslararası düzeyde yolsuzluk ile mücadele tedbirleri geliştirilmeye çalışılmaktadır. İlk olarak ABD de Clinton döneminde uluslararası faaliyet gösteren suç organizasyonları ile özellikli yolsuzluk ve kara para aklama suçlarıyla dünya genelinde mücadele edilmesine yönelik birtakım kararlar alınmıştır. Bu kararlar dünya devletleri arasında iş birliğini geliştirmeyi ve hukuki mevzuatın güçlendirilmesine yönelik amaçları içermekteydi. Öte taraftan

bakıldığında yolsuzluk kavramı çok geniş bir çerçevede değerlendirilebilir. Kanunlar ve yasal düzenlemelerde bulunan çeşitli boşlukların istismar edilmesi, bu düzenlemelerin uygulanmasından kaynaklanan istismarlar, eldeki imkân, yetki ve nüfuzun kötüye kullanılarak her alanda menfaat temin edilmesi gibi geniş bir alan ve kavramdır. Kısaca ifade etmek gerekirse yolsuzluk; Kamu gücünün kötü niyetle kullanılarak karar süreçlerine müdahale eden bunun sonucunda haksız menfaat sağlanan ve kurumların işleyiş süreçlerini bozan eylemlerdir.

Özbaran yolsuzluk olgusunu şöyle bir formülle açıklamıştır

"Yolsuzluk = Tekelci Güç + Takdir Yetkisi- Hesap verme Sorumluluğu" (Özbaran, 2019)

Yolsuzluk tanımının bugün artık sadece resmi sınırlar ile ile çerçevelendirilmesinden farklı olarak özel sektör içinde de yer bulduğu ifade edilmeye başlanmıştır.

2.1.3.6. Kara Para Aklama

Kara para aklama, bütünleşmiş ve disiplinlerarası bir tarzda ele alınması gereken, giderek daha karmaşık hale gelen bir olgudur. Kara para aklama, yasa dışı olarak elde edilen paranın kaynağını gizlemeyi amaçlayan bir faaliyettir. Kimliklerini gizlemek için, yasadışı menşeli fonlar ilk önce çeşitli yatırım şekillerinde yasal devreye girmeden önce finansal işlemlerde kullanılır. Kökeni şimdi keşfedilemeyen geçmişte biriken ve aklanan yasadışı yollardan temin edilen sermaye miktarı bilinmemekle birlikte azımsanamayacak oranda çoktur. Tipik olarak aklama (Dini, 2005), yasal olmayan piyasalar, bankalar ve genellikle farkında olmayan araçlar olarak kullanılan diğer finansal aracılar aracılığıyla gerçekleştirildiği ifade etmektedir. Bununla birlikte, bazı durumlarda, finansal aracıların yönetimi ile cezai menfaatler arasında tehlikeli bağlantılar bulunmaktadır.

Suç faaliyetlerinin mali tarafının karmaşıklığı, aklanacak meblağların büyüklüğü ve bunları oluşturan yasadışı faaliyetlerin yaygınlığı ile artar. Bazı durumlarda organize olarak işlenen bu suçlar kimi zaman devletlerin kendisine meydan okuyabilecek bir güce sahiptir. Günümüzde, organize suçlardan elde edilen suç gelirlerinin aklanması ile bu örgütler gelir kaynaklarını çeşitlendirir ve böylece hareket alanlarını da genişletmektedir. Başka bir ifade ile kara para aklamanın

toplumsal riski, suç örgütlerinin ekonomik gücünün pekiştirilmesi ve meşru ekonomiye nüfuz etmesi olarak fade edilebilir (Duyne, Harvey ve Gelemerova, 2018). Kara para aklama kavramı ile genellikle elde suç gelirlerine odaklanıldığından parasal olmayan çıktılar pek ilgi görmemektedir.

Somutlaştırmak gerekirse; bir parasal varlık gizleniyorsa, sadece o varlık değil, arkasındaki olası suç da gizlenmektedir. Bu, kanunlarda tanımlanmış bir suç olabileceği gibi dolaylı bir şekilde vergilerden kaçınma ya da bundan daha fazlası da olabilir. Parasal varlığın yasal yollardan şeffaf olarak kamuya açık bir şekilde kaynağının açıklananamaması, bu varlığın kara para olduğu anlamına gelmektedir. Sözü edilen paranın arkasındaki yasadışı faaliyetler, uyuşturucu ticareti, silah ticareti, hırsızlık, rüşvet, yasadışı madencilik gibi suçlar olabilmektedir.

Kara parayı uzun süre elde tutmak aklayıcılar açısında her zaman büyük bir risk oluşturmaktadır. Çünkü hükümetlerin bu durumu tespit etmesi halinde akalacılar açısından gelir ve zaman kaybı anlamına gelmektedir. Bu sebeple, kara parayı kazanmak kolay olsa da biriken parayı aklamak o kadar kolay değildir. Gelinen bu noktada aklayıcılar kara paralarının rengini veya kaynağını gizlemek için çeşitli yöntemler kullanmaktadırlar (Chandna, 2017). Bu bağlamda, suçtan elde edilen gelirlerin harcanması veya temizlenmesi amacıyla, kara paraya meşru bir kaynaktan elde edildiği görünümü verilmelidir. Böylece sorgulanmamalı veya araştırılmamalıdır. Araştırılsa bile, tüm işlem hareketleri açıklanabilir görünümde olacağından güvenlik otoritelerinin denetimlerine takılmayacaktır.

Türkiye, özellikle Orta Asya ve Kafkaslar ile Ortadoğu ve Doğu Avrupa için önemli bir bölgesel finans merkezidir. Kara para aklama ve finansal suçlarlara ilişkin ülke veritanlarının incelendiği rapora göre (INCSR, 2015), 2000'li yıllarla birlikte hızlı büyüyen Türkiye, coğrafi konumu ve ticari ilişkileri ile birleştiğinde, kara para aklama ve terörizmin finansmanı risklerine karşı daha riskli hale gelmektedir. Öte yandan Avrupa'ya taşınan Güneybatı Asya kökenli uyuşturucu maddeler için önemli bir geçiş yolu olmaya devam etmekle birlikte, uyuşturucu kaçakçılığı aklanan paranın sadece bir bölümünü oluşturmaktadır. Terörizmin finansmanı, özellikle son yıllarda Türkiye'nin Suriye'nin güney sınırından nakit akışları şeklinde gerçekleşmektedir. Türkiye'de uyuşturucu kaçakçılığı ve diğer yasadışı faaliyetlerle adı anılan belirli terör örgütleri bulunmaktadır. Kara para aklama bankalarda, banka dışı finansal

kuruluşlarda ve kayıt dışı ekonomide gerçekleşmektedir. Türkiye'de tercih edilen kara para aklama yöntemleri arasında sınır ötesi kaçakçılık faaliyetleri, yurtiçi – yurtdışı banka havaleleri, hayali ticaret ve değerli eşyaların ticareti gösterilebilir (INCSR, 2015).

2.1.3.6.1 Kara Paranın Tanımı

Karapara aklamak olarak Türkçe'ye geçen bu terimin İngilizce karşılığı "money laundring" olup, tam olarak, para yıkamak anlamına gelmektedir. Yıkamak deyiminin 1920'li yıllarda İtalyan mafyasınca kurulan çamaşırhaneler zincirleri üzerinde suçtan elde edilen gelirlerin yasal dolaşıma sokulması sırasında yapılan işlemlere ithafen kullanıldığı düşünülmektedir. Para aklama deyiminin kökeni 1920 li yıllarda İtalyan mafyası liderlerinden Al Capone'in sadece nakit parayla ödeme yapılan bir çamaşırhane zinciri kurarak, suçtan elde ettiği gelirleri küçük miktarlar olarak, bu çamaşırhanelerde gelir gibi gösterip dolaşıma sokmasında atfedilmektedir. Bu şekilde karapara yasal sisteme sokularak, kullanılmaya hazır hale getirilmektedir. 1980'lerde yoğunlaşan küreselleşme sürecinden dünya ekonomik sistemi de nasibini almış liberal ekonomiye geçişle konvertibilite ve fon transferlerinin sınırları ortadan kalkmıştır. İktisadi hayatın globalleşmesi birçok pozitif etki yaratırken buna paralel ortaya çıkan bazı organize suç türleri de ulusları tehdit etmeye başlamıştır (Küçüközyiğit, 2004).

Yasadışı yollardan elde edilen her türlü gelirlere, dar bir tanımla suçtan elde edilen gelirlere karapara denmektedir. Bir başka ifadeyle yasaların yasak kabul ettiği her türlü eylemden sağlanan haksız gelir ve kazançlardır (Altuğ, 2001, s. 118).

Karapara aynı zamanda kayıtdışı ekonominin ayrılmaz bir parçasıdır. Kayıtdışı ekonominin tanımında farklı düşünceler vardır. Vergilendirilmeyen kazanç ve suçtan elde edilen gelirlerin toplamı kayıtdışı ekonomi olarak tanımlanmakla birlikte kayıtdışı ekonomiyi tamamen kara para olarak nitelendirmekte mümkündür. Sadece vergi vermemek amacıyla hayali ihracat yapmak ya da sahte fatura tanzim etmek gibi suçlara yönelen örgütler olduğu düşünüldüğünde, ikinci tanımın uygun olduğu değerlendirilmektedir.

2000li yılların başlarında yalnızca birkaç ülkede karaparanın aklanması ile mücadele etmek için yürürlüğe giren hukuki tedbirler, günümüzde elliden fazla ulusta

yasal mevzuatta yer bulmaktadır. İnterpol kayaklarına göre küresel ölçekte işlenen aklama fiillerinin sadece %5'inin aydınlatılabildiği yönünde kanaat bildirilmektedir.

Günümüzde seç gelirlerinden elde edilen gelirlerin ekonomik tutarı devasa boyutlara erişmiştir. Bazı projeksiyonlar global çapta her yıl suç örgütlerince işlenen çeşitli bir trilyon dolar bir takım komplike yollarla aklanarak yasal sisteme dahil edilmektedir. Aklanan tuturın önemli bir bölümü yine suç fiillerinin işlenmesi sürecinde kaynak olarak kullanılmaktadır. Uluslararası Para Fonu (IMF)'nun bir raporuna göre dünyada aklanan paranın boyutu 2000 yılı itibariyle dünya GSMH'nın %2-%5'i olarak tahmin edilmektedir. Suç örgütleri işledikleri suçlardan sağladıkları kaynağı legalleştirebilmek için her geçen gün daha farklı yöntemlere başvurmaktadır. Elde ettikleri orantısız kaynak ile suç örgütleri siyasi ve iktisadi işleyişlere etki etmekte ulusların egemenlik haklarına ve hukuki süreçlere zarar vermektedir.

Sonuçları itibariyle birçok olumsuz etki doğuran kara para aklama suçu, öncül bir suç kaynaklı ekonomik varlıkların kanyağının saklanarak ekonomik dolaşıma sokulması sürecini ifade etmektedir (Yılmaz, 2011).

Kara aklamak için Bitcoin gibi kripto paraları kullanışlı hale getiren kendine has özellikleri bulunmakladır. Kısaca açıklamak gerekirse (Baath ve Zellhorn, 2016); Öncelikle, Bitcoin gibi kripto para birimlerinin merkezi olmayan teknolojik altyapısı, kullanıcıların gerçekleştirdikleri iş ve işlemlerde herhangi bir aracı kişi veya kuruma ihtiyaç duymaksızın, aralarında fon transferi gerçekleştirmelerine fırsat sunmaktadır. Klasik paralar üzerinden kara para aklama ile mücadele süreçlerinde temel kriter olarak kullanılan, fon transferi yapan suçluların hareket kabiliyetlerini sınırlandırmak için; fon gönderenler ve alıcıları arasındaki işlem trafiği kontrol edilmektedir. Kripto paralar klasik paradan ayrışan bu yönleriyle yapılacak denetimlere imkân vermemektedir. Yine kripto para işlemlerinde fiziki temasın olmaması açık kimlik tanımlamalarını engellemektedir. Bir diğeri, gerçekleştirilen işlemlerin her birinin blok zincirinde muhafaza edilmesi ve şeffaf bir şekilde takip edilebilmesine karşın, işlem sağlayan tarafların kişi veya kuruluşla ilişkisi tanımlanmamıştır. Blok zincir tabanlı kripto paralarla işlem gerçekleştirirken iki anahtara ihtiyaç vardır. Bu anahtarlardan biri gizli olan özel anahtar, diğeri genel anahtardır. Bu anahtarlar ile kullanıcılar çok sayıda elektronik cüzdan oluşturabilmektedirler. Çok sayıda cüzdan üzerinden yapılan işlemler de olası aklama eylemlerini takip etmeyi kısıtlamakta ve

oldukça karmaşıklaştırmaktadır. Son olarak, kripto paralar ile gerçekleştirilen işlemlerin, çok hızlı ve basitçe gerçekleştirilmesi, özellikle kara para aklamada kripto paraları klasik paralara göre avantajlı kılmaktadır. Klasik paranın fiziki olarak bir hacminin olması birtakım sınırlılıkları beraberinde getirmektedir. Diğer taraftan kripto paralarda ise küçük bir bellek kartına milyarlar sığdırılabilmektedir. Dahası çok kısa bir zaman diliminde, dakikalar içerisinde gezegenin herhangi bir konumuna aktarılabilmektedir.

2.1.3.6.2. Kara Para Aklamanın Evreleri

Kara paranın aklanması suç örgütlerinin ilgilendikleri özel bir suç alanı değildir. Suçtan elde edilen gelirlerin yasal dolaşıma sokulması için bütün örgütlerin kullanmak zorunda kaldıkları mecburi bir süreçtir. Suç örgütleri yasalar gereği suçtan elde ettikleri çeşitli gelirleri yasal sisteme açıkça dahil edememektedirler. Bunun için değişik yöntemler bulmak zorundadırlar. Turizm ve özelleştirme yatırımları, inşaat işleri, bu işler için özel bankalar kurulması, para akışının kontrolünün gevşek olduğu küçük ülke bankalarından istifade edilmesi gibi farklı birçok yöntem kullanılmaktadır. Kara para aklamanın şimdiye kadar tespit edilmiş olan yüzlerce yöntemi vardır. Bu bağlamda kara paranın aklanması üç adımda gerçekleştirilmektedir. Bunlar, yerleştirme, ayrıştırma ve bütünleştirme safhalarıdır.

Şekil 2.1.: Sanal Paraların Kara Para Aklama Riskleri

Her Aşamada Güvenlik Açıklarının Muhtemel Kullanımı			
Genel Risk Faktörleri	Yerleştirme	Ayrıştırma	Bütünleşme
Yarı Anonimlik	Sanal paralar suçlular ve dernekler tarafından kullanılabilir.	Şüpheli isimler, özellikle para kuryeleri belirlenemez.	Kişiler takip edilemediğinden isimsiz olarak işlenen suçların gelirlerinin nakde dönüştürülmesine izin verir.
Gerçek Zamanlı İşlemler	Suç gelirleri başka bir ülkedeki başka bir sanal paraya transfer edilebilir.	İşlemler gerçek zamanlı olarak gerçekleşir ve kara para aklamadan şüphelenilirse onları durdurmak için çok az zaman kalır.	Suç gelirleri sistem aracılığıyla hızlıca taşınabilir ve başka bir ülkeye aktarılabilir.

Kaynak: (Campbell-Verduyn, 2018)

2.1.3.6.2.1. Yerleştirme Evresi

Kara Para Aklama sürecinin ilk adımı yerleştirme aşamasıdır. Bu evrede paranın biçimi değiştirilir veya fizikselden fiziksel olmayan bir forma dönüştürülmektedir (Savona ve De Feo, 2005). Sadece nakit olarak yapılan büyük alımlar şüphe çektiğinden, banka hesaplarına kanalize edilmeleri gerekmektedir. Örneğin, nakit şekilde kara paraya sahip olan X, banka hesaplarına düzenli olarak çeşitli yol ve hesaplardan küçük miktarlar transfer etmeye başlar. X parasını bir banka hesabında toplamakla onu meşru ekonomik sistemin içerisine dahil etmiş olmaktadır ve bu fonu artık bu meşru hesap üzerinden başkaca işlemler gerçekleştirebilmek için kullanabilecektir. Fakat bu nokradan sonra artık paranın izi sürülebilecek ve tüm işlemler artık kayıt altına alınmaktadır.

Savona ve De Feo (2005), Büyük miktarlarda nakit dikkat çekebileceğinden ve sürekli hırsızlık veya el koyma riski taşıdığından, suçlular daha büyük aklama hacmi için küçük banknotlar alıp para yatırma ve finansal araçlar satın alma konusunda eğilim göstermekte olduğunu belirtmektedir. Bir başka ifadeyle toplu olarak nakit parayı derhal elden çıkarmak istemektedirler. Bu süreç, otoritelerin denetiminde olduğu için dikkat çekebilmektedir. Bu nedenle, suç örgütleri, bu gelirleri gizlice işlemek için yöntem ve mekanizmalar aramaya yönelmektedir. Böylece suç gelirleri gizlenir veya yanlış temsil edilerek sisteme dahil edilmektedir. Bu toplu nakit para, bankalar veya menkul kıymetler aracı kurumları gibi geleneksel finansal kuruluşları ile borsalar, kıymetli maden ticareti gibi alanlara aktarılmaktadır.

Kara para faaliyetlerinin önlenmesi noktasında önemli rol üstlenen Mali Eylem Görev Gücü (FATF), yasadışı faaliyetlerden kazanılan fonların saklanması veya temizlenmesi için üç temel yolu tercih etmektedir;

- Bankalar ve diğer finans kuruluşları ile "hawala" benzeri gayrıresmi finansal yöntemler
- Fiziki fon transferleri yöntemi Nakit kuryeleri ya da nakliyeciler)
- Sahte ticari işlemler ile hayali ihracat faaliyetleri (Aksoy, 2018, s. 13).

2.1.3.6.2.2. Ayrıştırma Evresi

Bu aşama, işlemleri daha karmaşık hale getirmek de dahil olmak üzere çeşitli yollarla gizleyerek yerleştirme aşamasının negatif tarafını ayıklamak için kullanılır.

Örneğin, X tarafından işe alınan bir ajan olan Y, parayı doğrudan Z'nin hesabına değil, onun bağlı kuruluşlarının veya bir şirketinin hesaplarına yatırır ve parayı birkaç kez tekrar ve tekrar dolaşıma sokar. Sonuçta kara para fonları X'in banka hesabına ulaşır ya da doğrudan fiziki olarak eline geçmektedir.

Biraraya getirilen paranın ilk yerleştirilmesinden sonra, bir sonraki adım ayrıştırma aşamasıdır. Bu aşamada herhangi bir denetime yakalanmamak üzere paranın izini kaybettirerek aklama sürecinin kesintiye uğramaması için tasarlanmış bir veya daha fazla finansal işlem ile katmanlanarak oluşturulan, yasadışı gelirlerin kaynaklarından ayrılmasını ifade etmektedir (Savona ve De Feo, 2005). Toplu nakitlerin yerleşimi tespit edilmezse, kara para aklayanların faaliyetlerinin yeniden yapılandırılması giderek zorlaşacaktır. İşlemlerin çok defa katmanlaştırılması kafa karıştırıcı ve karmaşık yolların kullanılması ile paranın izi kaybettirilmektedir.

2.1.3.6.2.3. Bütünleştirme Evresi

Bu aşamada kara para sahibinin kara parasının kaynağını, beyaz paraya dönüştürdüğünün gerekçelerini ortaya koyduğu son aşamadır. Bu adımı somutlaştırmak gerekirse, X, sahip olduğu fonlara ilişkin işlemlerin özgün olduğunu ve paranın gerçek işinden geldiğini göstermektedir. Bütünleştirme aşamalarının bilgisi, aklama işleminin çözülmesine yardımcı olur (Chandna, 2017).

Bütünleştirme, şüphe uyandırmadan ve görünüşte meşru bir kaynakla meşru ekonomiye suçtan türetilen servetin getirilmesidir. Katmanlama tamamlandıktan sonra, aklanan fonların, sahiplerinin yatırım veya tüketim hedeflerini gerçekleştirmek için yasal ekonomiye gizli bir şekilde dahil edilmesi gerekmektedir. Bütünleştirme sürecinde çeşitli yöntemler kullanılmaktadır. Bunlardan bazıları şunlardır (Savona ve De Feo, 2005);

i) Gayrimenkul İşlemleri

Aklanan parayı entegre etmek için gayrimenkul işlemleri kullanılabilir. Suç fonunnundan elde edilen gayrimenkulün mülkiyeti, yasadışı gelir kullanan bir paravan şirket tarafından satın alınabilir. Bu mülk daha sonra satılabilir ve gelirler aklanmış olur.

ii) Uzak Şirketler ve Sahte Krediler

Genellikle kurumsal gizlilik yasalarına sahip bir ülkede bulunan şirketler üzerinde toplanan kara para, yerel şirketlere borç olarak transfer edilir.

iii) Yabancı Bankalar

Suç ortağı yabancı bankalar kullanılarak yapılan kara para aklama faaliyetleri, çok daha komplike bir yöntemdir. Bu bankalar, suça ortak olan yönetici ve üst düzey yöneticileri vasıtasıyla kara para aklama işlemlerini yürütmektedir. Bu bankalar yine aklayıcılara sahte krediler sağlayarak, başka bir devletin bankacılık yasaları ve düzenlemeleri karşısında bağışıklığı garanti etmektedir.

iv) Hayali İthalat / İhracat

İthalat ve ihracat şirketleri tarafından sahte işlemlerin sahte belgeler düzenlenerek, yasadışı gelirleri yasal ekonomik sisteme entegre etmenin etkili bir yoludur.

2.1.3.6.3. Kara Para Aklamada Kullanılan Yöntemler

2.1.3.6.3.1. Klasik Kara Para Aklamada Klasik Yöntemler

Kara para aklamak için kullanılmış oldukça fazla yöntem olmakla birlikte klasik yöntemler arasındaki en yaygın olarak tercih edilen yöntemler şunlardır;

2.1.3.6.3.1.1. Suç Gelirlerinin Fiziksel Olarak Yurtdışına Çıkarılması

Bu yöntem ile elde edilen para taşıyıcı kişiler vasıtasıyla değişik ulaşım yolları ve yöntemleri kullanarak, ekonomik ve mali denetimi zayıf, finansal işlemlerin şeffaf olmadığı uluslara kaçırılmak suretiyle bu ülkelerin finansal sistemine dahil edilmektedir. Bu işlem ile nakit formdaki kara paranın, yeni yerleştiği ekonomik sistem içerisindeki finanasal kurum ve kuruluşlar aracılığı ile kaynak noktasına ya da başkaca yeni noktalara aktarılması mümkün olmaktadır. Böylelikle kirli paranın asıl yaratıldığı ilk yerle olan illiyeti koparılmaya çalışılmakta ve para aklanmaktadır. (Mavral, 2001, s. 62).

2.1.3.6.3.1.2. Şirinler Yöntemi

Aklayıcılar suç gelirlerini aklama süreçlerinde fonları bir araya getirmeden önce denetimlerden kaçınmak için birçok bankadaki suç gelirlerini şüphe

uyandırmayacak şekilde küçük parçalara bölmek için anonim yardımcılar kullanmaktadır (Savona ve De Feo, 2005). Şirinler yönteminde amaç, şüphe uyandırmayacak şekilde banka hesaplarına yasadışı nakit yatırmak olarak ifade edilebilmektedir. Böylece, nakit mevduatlar çok sayıda hesapta küçük miktarlarda toplanır. Böylece suç gelirleri küçük parçalar halinde sisteme dahil edilmiş olur (Chandna, 2017).

2.1.3.6.3.1.3. Paravan Firmalar

Paravan şirketler esasında aktif ticari faaliyetleri veya varlıkları olmayan bir şirkettir. Bu şirketler kâğıt üzerinde var olarak görünse da kuruluşarında beyan etmiş oldukları faaliyetlerinde aktif değildir. Fakat sahip olduğu varlıkları faaliyet büyüklüğüyle orantılı olmayabilir. Bu tür şirketler görünürde yasa dışı değildir, ancak ticari faaliyetleri ile varlıkları zaman içerisinde gizemli ve gayri meşru faaliyetlere dönüşebilmektedir. Paravan şirketler ile kara para aklama faaliyetleri arasındaki ilişki birbirine bağımlı bir ilişkiyi ifade etmektedir (Chandna, 2017).

Paravan şirketlerin kara para aklama süreçlerinde kullanılmasının en temel sebebi, aklamanın ayrıştırma adımında suç gelirlerinin transferine ihtiyaç duyulmasıdır. Suçtan sağlanan parasal menfaatin elde edildiği ilk nokta ile bağının gizlenmesi ancak komplike fon transferleriyle gerçekleştirilebilmektedir. Öte yandan bu transfer işlemlerinin takibini daha zorlaştırmak maksadıyla bu firmaların off-shore lokasyonlarda teşkil edilmesi aklayıcılar açısından bir avantaj sağlamaktadır.

2.1.3.6.3.1.4. Off-Shore Bankalar

Off-shore finans şirketleri, kara para aklama faaliyetlerinin temel mecraları niteliğindedir. Bu şirketler gerçek bir ticari faaliyet yapmak amacıyla değil, paranın bir yerden başka bir yere yönlendirilmesi amacıyla, yabancı bir ülkede kurulan şirketleri ifade etmektedir. Genellikle verginin sıfır veya asgari olduğu ülkelerde kurulmakla birlikte birçok küresel bankanın bu ülkelerde şubeleri de bulunmaktadır. Off-shore bankaları her zaman yasa dışı değildir, fakat bazen ülkeler arasındaki vergi yasaları ve vergi anlaşmalarındaki boşluklardan yararlanmaktadır (Chandna, 2017).

Off-shore bankalar, bankacılık sisteminin henüz kurumsallaşmadığı, finas sektörünün tabi olduğu mevzuatın ya olmadığı ya da önemli açıklarının bulunduğu

off-shore bölgeler olarak anılan deniz kıyısı bölgelerinde kurulmaktadır. Bu finans kurumları, anonim işlemler gerçekleştirmeleri ve işlem kayıtlarının tasnifi ve muhafazasına yönelik düzenlemelerin yeterli olmayışı buna ek olarak sağladıkları vergi avantajları sebebiyle aklama faaliyetlerinin çekim noktası olarak anılmaktadır (Gediz Oral ve Gökbunar, 2017)

2.1.3.6.3.1.5. Parçalama Yöntemi

Sahip olunan fonu daha küçük miktarlara parçalayarak birçok farklı kişi vasıtasıyla finans kuruluşuna aktarmak her zaman mümkün olmayabilir. Böyle bir durumda transferleri gerçekleştirecek taşıyıcıların adedini artırarak değil de transferlere ilişkin trafiği artırarak mevzuat hükümlerinden sıyrılmak mümkün olabilmektedir. Bu yöntem de kullanılan temel taktik, parçalama taktiğidir. Büyük ve dikkat çekici ve mevzuatın uygun gördüğü limitlerin üzerine çıkan işlemler parçalara ayrılarak birçok işlem üzerinden parça parça gerçekleştirilir. Örnek vermek gerekirse 50 milyon euro'luk bir işlemin 1000'er euro'luk işlemler üzerinden başka bir ülkeye gönderilerek aklanabilmektedir (TBB, 2013).

2.1.3.6.3.1.6. Döviz Büroları

Kara para aklama faaliyetleri sürecinde nakit yoğunluklu işlemler gerçekleştiren döviz ofisleri doğal olarak çekici olmaktadır. Fon transferlerine konu olan nakit paraların döviz cinsinden değiştirilmesi suç gelillerinin kaynağı ile bağının gizlenmesinde önemli bir işleve sahiptir. Bu nedenle fon varlık işlemlerinin taransfer işlemleri lisansına sahip döviz ofisleri, aklama faaliyetleri açısından risk faktörü yüksek bir niteliğe sahiptir. Döviz büroları sundukları döviz işlemlerine yönelik hizmetler bakımından çeşitli kolaylık ve avantajlar sunmanın yanı sıra bazı suistimallere sebep olabilecek yönleri de bulunmaktadır.

2.1.3.6.3.1.7. Oto Finansman Borç Yöntemi

Off-shore merkezlerindeki bankalar ve finansal işlem gerçekleştiren kuruluşlar üzerinden getirilen kara para, aynı kuruluşların sağladığı krediler şeklinde geri gönderilir. Oto finansman borç yöntemiyle gerçekleştirilen transferleri şu adımlarla uygulanmaktadır (TBB, 2013);

Kara para aklamak isteyen X kişisi Y ünvanlı off-shore aracı kuruma gider ve kara parasını bu bankaya yatırır. Ülkesine dönen X, ülkesindeki Z bankasına giderek Y bankasındaki parasını teminat göstererek kredi kullanmak ister. Kolaylıkla temin ettiği kredisini zaman içinde bankasına geri ödemeyen X, Y bankası tarafından takibe düşer ve Y bankasındaki mevduatı haczedilir. Sonucunda Y bankası parasını geri alır, X de kara parasını aklamış olur.

2.1.3.6.3.1.8. Kumarhane ve Gazinolar

Gayri meşru yollardan elde edilen paranın, kumarhanelerde ve egzotik eğlence ortamları ile bahis oyunları üzerinden aklama faaliyetleri sıkça tercih edilen aklama yöntemleri arasında yer almaktadır. Kumar oyunları, kazanılan paranın bir evrak ile ispat edebilme olanağı ve kazanılan paranın bir bankaya transferi ile sisteme dahil etme avantajını beraberinde getirmektedir. Tüm bu yasal nitelikleri ile kumar oynamak, para aklayanlar için büyük bir avantajdır. Kumarla ilgili açık düzenlemeler olmadıkça, kumardan kazanılanan bir paranın aklamasının tek şartı, devlete kazandığı kazançlar üzerinden vergi ödemekle sınırlıdır. Bununla birlikte kimi bölge veya ülkelerde kumara ve bahis olunlarına sıfır veya asgari vergi uygulaması şaşırtıcıdır (Chandna, 2017).

2.1.3.6.3.1.9. Hayali İhracat – İthalat Yöntemi

Bu yöntem, 1980'ler sonrası süreçte devletlerin küreselleşmeye entegrasyonunda gelişen ithalat – ihracat faaliyetleri neticesinde ortaya çıkmıştır. Amacı kısaca haksız vergi iadesi oluşturmaktır. Fiyatı çok ucuz bir mal, yüksek kaliteli bir malmış gibi ihraç edilir. Dış ticaret işlemlerine konu olan mal ve hizmetlerin gerçek dışı evraklar üzerinde yazılı değeri ile gerçek değerleri arasındaki ekonomik değer kara paranın aklanan kısmını ifade etmektedir. Bu yöntemde ayrıca soruşturma makamlarından kaçınmak amacıyla aklama faaliyetinin, vergi cennetlerinde kurulan bir paravan şirket tarafından gerçekleştirilmesi gerekmektedir (İpek, 2000, s. 27).

2.1.3.6.3.2. Karapara Aklamada Yeni Yöntemler

Sağlamış olduğu anonimlik ve aracısız işlem gerçekleştirmeye imkân sunan kripto para teknolojisinin çıkışı, kara para aklamak için de bu para birimlerinin

kullanılabileceği yönünde merak ve kaygılara neden olmuştur. Bugün milyarlarca kullanıcısı olan internet ağı mobil teknolojiler, mobil finansal hizmetler, online pazarlama kanalları gibi yenilikler suç gelirlerini aklamak isteyen suçlular için de çekici fırsatlar sunabilmektedir. Çünkü kripto paralar kendine has özellikleri ile kara para aklama işleminin temel sorunu olarak tanımlayabileceğimiz "büyük paraların fiziksel transferi" problemine çözüm olmaktadır. Öte yandan bu para birimlerinin dünya çapında yaygınlaşması, aklayıcıların ülkeden ülkeye farklılaşan ulusal güvenlik standartlarının açıkları fırsata çevirip illegal fonlarının hesap trafiklerini merkezi otoritelerden saklayabilme olanağı sağlamaktadır (Yazıcı, 2008, s. 158).

2.1.3.6.3.2.1. Akıllı Kartlar İle Aklama

Akıllı kartlar, E-cüzdan olarak da anılan ve klasik paraya alternatif olmak üzere oluşturulmuşlerdır. Akıllı kartlar üzerindeki elektronik yongaya tanımlanmış bir ekonomik değerin, elektronik olarak yüklenmesiyle kullanıcısına bir çeşit limitli kredi imkânı sağlamaktadır. Akıllı kart sistemleri, çalışma prensipleri açısından farklılıklar arz etmektedir. Bazı akıllı kartlar, gerçekleştirilen işlemlerde anonimlik sağlarken, kimi akıllı kartlar da özellikle şeffaflık sunmak maksadıyla tasarlanmıştır. (Dursun, 2008).

Akıllı kartların en temel özelliği; kişi veya kurumların kullandıkları kart vasıtasıyla kişisel ya da ticari bilgilerin sistem yetkilisinin kontrollü erişimine açık olmasıdır.

2.1.3.6.3.2.2. Elektronik Paralar İle Aklama

Elektronik paralarla gerçekleştirilen işlemler nakit paraya kıyasla kimlik gizliliği avantajı sağlamaktadır. Bunun nedeni en başta kâğıt paraların her birinin özgün bir seri numarasının olması nedeniyle basit bir şekilde denetlenebilir olmalarından kaynaklanmaktadır. Ek olarak kâğıt para işlemleri çoğunlukla fiziki bir yakınlık, yüz yüzelik gerektirmektedir. Buna karşılık elektronik paralar ise, elektronik şifreleme yöntemlerini kullanmaktadırlar ve mesafe sınırı olmaksızın transferlere olanak vermektedir. Ayrıca anonim işlem gerçekleştirmeyi de desteklemektedir (Ping, 2004).

Kısaca ifade edilen temel özellikleri nedeniyle elektronik paralar kara para aklayıcıları bazı avantajlar sunmaktadır. Bunlar; (Yazıcı, 2008);

- İşlem kısıtlaması veya limitler olmaksızın sınırsız elektronik para işlemi yapılabilmektedir.
- Kartlar arsında işlem gerçekleştirilebilmektedir.
- Elektronik paralar ile işlemler çok kısa sürede gerçekleştirilebilir.
- İşlemler kayıt altına alınmamaktadır.
- Elektronik paralar kimlik gizliliği sunmaktadır.

2.1.3.6.3.2.3. Borsa Yolu İle Aklama

Kara para, manipülasyon işlemleriyle veya finansal nitelikli bilgiler sızdırılarak borsa işlemleri vasıtasıyla da sisteme aktarılabilmektedir. Ayrıca hisse senetleri üzerinden yapılan spekülasyonlarla bu kağıtların piyasa değerleri yükseltebilir ya da düşürülebilmektedir. Bu şekilde taraflardan biri ekonomik olarak küçülürken diğeri ise aynı oranda ekonomik yönden büyümektedir (Ünlü, 2019).

Diğer yandan üçüncü taraflar da kara paranın aklanması için kullanılabilmektedir. Gizli anlaşmalı bir broker vasıtasıyla, kirli para hisse senedi ya da tahvile dönüştürülebilmektedir. Genelde bu işlemin gerçekleştirildiği kağıtlar paravan şirketlerin hisseleri olmaktadır. Hamiline yazılan bonolar için ise zaten kayıt gerekmemektedir. Finansal piyasalar ve bu piyasalarda çalışan profesyonellerin tabi oldukları hukuki mevzuatlar ülkeden ülkeye değişiklik göstermektedir. Bu sebeple kimi ülkelerde örneğin bir kambiyo görevlisi üzerinden fon işlemlerini gerçekleştirmek çok daha esnek olabilmektedir. Bununla birlikte daha katı kuralların uygulandığı ülkelerde bazı kuralları bilinçli esneten ya da gözden kaçıran görevliler nedeniyle kara paraların aklanması daha basit olabilmektedir (Ergül, 2001).

2.1.3.6.3.2.4. İnternet Aracılığı İle Aklama

Günümüzde internetin yaygın kullanımına bağlı olarak geliştirilen internet tabanlı finansal nitelikli ürün ve hizmetler artık daha çok tercih edilir bir hal almıştır. Durum böyle olunca internet üzerinden gerçekleştirilen mali işlemler ve alternatif yöntemleri de kara para aklamada bir yöntem olarak ilgi çekmektedir. Online sunulan

finansal hizmetler her geçen gün daha da artarak ticari bankalar ve yalnızca sanal şubeleri olan internet bankaları tarafından verilmektedir (Ergül, 2001).

Elektronik paralar, tedavülde bulunan en düşük maddi değeri temsil eden kâğıt ve madeni paradan bile daha düşük değerleri temsil etme konusunda olanak sunmaktadır. Bu özellik elektronik paraların mikro ödeme yöntemi aracı olarak ifade edilmesine neden olmaktadır. Bu özelliği ile bir söz gelimi dijital yayın yapan bir yayının yalnızca birkaç sayfasını satın alıp okumak mümkün olmaktadır (Dursun, 2008).

2.1.3.6.4. Kara Paranın Aklanmasında Uluslararası Mücadele

2.1.3.6.4.1. "Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı BM Sözleşmesi"

1990 yılında imzalanan sözleşme ile "uyuşturucu ve psikopat madde" olarak kabul edilen maddelerin kaçakçılığına karşı uluslararası iş birliğinin gerçekleştirilebilmesi için BM bünyesinde üye devletlerin mevzuatına dahil olmuştur. (MASAK, 2019). Sözleşmeye göre; Uyuşturucu ve psikotrop madde sınıfında değerlendirilen maddelerin ticareti ve tüm tedarik süreçlerinin, bu süreçlerden elde edilecek gelirlerin, bu amaca yönelik örgüt veya iş birliklerinin teşvik ve yardımların suç kapsamına alınması ve gerekli tedbirlerin uygulanması istenmektedir.

Sözleşmeye taraf devletlerin, anılan yasak fiillerin ülkelerinde işlenmesi durumunda hangi cezai yaptırımların yerine getirileceği öngörülmüştür. Viyana Konvansiyonu olarak da anılan bu sözleşmeye Türkiye 20.12.1988 tarihinde dahil olmuştur (MASAK, 2019).

2.1.3.6.4.2. "Sınıraşan Örgütlü Suçlara Karşı BM Sözleşmesi"

Organize olarak işlenen yasak fiillere yönelik düzenlenen ilk uluslararası sözleşme olmakla birlikte 2000 yılında imzalanarak BM nezdinde kabul edilmiştir. Palermo'da imzalanması sebebiyle Palermo Konvansiyonu olarak da bilinmektedir. Sınır aşan örgütlü suçların önlenmesine yönelik mücadelede iş birliğini etkinleştirmeyi ve geliştirmeyi amaçlayan sözleşmeye Türkiye 30.01.2003 tarihinde dahil olmuştur. Sözleşmenin kapsamında sınır aşan ve örgütlü olarak işenen suç olarak kara para aklama suçu, taraf devletler arasında en kapsamlı şekliyle öncül ve bağlantılı suçları

da ilgili hükümler de bulunmaktadır. Karapara aklama konusunda aracı işlem gerçekleştirebilecek finansal hizmetler gerçekleştiren kurumlara bildirim zorunluluğu öngörülmektedir. Karapara aklama suçu özelinde bilgi ve istatistikleri derleyecek mali istihbarat birimi kurulması, uluslararası fon trafiği amacıyla düzenlenen tüm işlemlere bildiriminde yükümlülüğü getirilmiştir. Ek olarak suç fiillerinin tespitinden sonra takip edilecek hukuki sürece ilişkin düzenlemeleri içermektedir (MASAK, 2019).

2.1.3.6.4.3 "141 Sayılı Avrupa Konseyi Sözleşmesi"

Suç gelirlerinin aklanmasıyla mücadele kapsamında, suç fiillerinden sağlanan gelirlere el konularak, aklamanın önüne geçilmesi amacıyla, Avrupa Konseyi tarafından 1990'da "Suç Gelirlerinin Aklanması, Aranması, Zapt Edilmesi ve Müsadere Edilmesi Hakkında Sözleşme" uluslararası mevzuata dahil edilmiştir. Bu çerçevede, günümüzde devletler için büyük tehditlere neden olan uluslararası ve örgütlü olarak işlenen hukuk dışı fiillerle mücadelede, en verimli neticeler suç örgütlerinin bu gelirlere erişiminin kesilmesiyle mümkün olmaktadır. Bu kapsamda küresel iş birliğinin de önemi oldukça büyüktür (MASAK, 2019).

Sözleşme, taraf devletler arasında yapılan taleplerin gereğinin yerine getirilmesine yönelik özellikle bilgi paylaşımı bağlamında bağlayıcı yükümlülükler getirmektedir. Bu yükümlülüklerle birlikte taraflar arasında formalitelerin aşılarak akıcı bir iş birliğinin tesis edilmesi amaçlanmaktadır. Strazburg Konvansiyonu olarak da anılan sözleşmeye Türkiye 27 Eylül 2001 tarihinde imzalayarak 16 Haziran 2004 tarihinde dahil olmuştur.

2.1.3.6.4.4. "198 Sayılı Avrupa Konseyi Sözleşmesi"

Suç örgütlerinin faaliyetlerinde ve dünya konjonktüründe meydana gelen gelişmelere paralel olarak Strazburg Konvansiyonu yeniden yorumlanarak yerine "Terörizmin Finansmanı ve Suçtan Elde Edilen Gelirlerin Aklanması, Aranması, Elkonması ve Müsaderesi Hakkındaki Avrupa Konseyi Sözleşmesi" 2005'te kabul edilerek yürürlüğe girmiştir. Yeni mevzuatın Strazburg Konvansiyonundan ayrıştığı norkta, kara para faaliyetlerine ek olarak terörizme aktarılan kaynaklarla mücadeleyi de kapsıyor olmasıdır. Varşova sözleşmesi olarakta bilinen sözleşmeyi Türkiye 28 Mart 2007 tarihinde mevzuatına dahil etmiştir (MASAK, 2019)

2.1.3.6.4.5. Mali Eylem Görev Gücü

Karaparanın aklanması suçuyla mücadelede etkin politikalar geliştirmek ve aklama suçunun önlenmesini teşvik etmek amacıyla kurulmuş uluslararası bir kuruluştur.

FATF, G-7 ülkeleri olan ABD, Almanya, Fransa Japonya, İngiltere, İtalya ve Kanada, tarafından uluslararası alanda karapara aklamanın önlenmesi amacıyla 1989'de kurulmuştur. Başlangıçta karaparanın önlenmesine yönelik bir amaçla kurulan FATF sonrası süreçte 2001'de mücadele alanını genişleterek amaçları arasına terörün finansal kaynaklarının kesilmeseni de eklemiktir. Bu kapsamda üye sayısını arttırmıştır. Türkiye ise organizasyona 1991'de katılmıştır. "ABD, Almanya, Arjantin, Avustralya, Avusturya, Belçika, Brezilya, Çin, Danimarka, Finlandiya, Fransa, Güney Afrika, Hollanda, Hong-Kong, İngiltere, İrlanda, İspanya, İsveç, İsviçre, İtalya, İzlanda, Japonya, Kanada, Lüksemburg, Meksika, Norveç, Portekiz, Rusya Federasyonu, Singapur, Türkiye, Yeni Zelanda, Yunanistan, Avrupa Komisyonu, Körfez İş birliği Konseyi FATF'in üyeleridir". Bunlara ek olarak aynı mücadeleyi lokal bazda yürüten organizasyonlar olan, "MENAFATF, MONEYVAL, APG, GAFISUD" da imtiyazlı üyelerdir (MASAK, 2019).

2.1.3.6.4.6. Avrupa Birliği Direktifleri

"91/308/EEC Sayılı Konsey Direktifi"; karaparanın aklanması suçu bağlamında Avrupa Konseyi kararıyla 1991'de kabul edilmiştir. Bu çerçevede konseyin yaptığı ilk düzenlemedir. Direktif; sermaye akış süreçleri ile mali hizmetlerin yerine getirilmesinde aksaklık ve sınırlandırmalara neden olmadan mali sistem içerisinde karapara aklanmasın engellenmesini amaçlamaktadır. Direktifin içeriği bu amaçla önceden yürürlüğe giren mevzuatlar ve tavsiyeleri esas alarak hazırlanmıştır. İçeriğinde aklama fiili, şüpheli işlem bildirimi, kimlik tespiti ve kayıtların saklanmasına ilişkin düzenlemeler bulunmaktadır.

İkinci olarak 14 Temmuz 1999'da 91/308/EEC sayılı Direktifte kapsamın genişletilmesi ve içeriğinin güncellenmesi amacıyla değişiklik önerisi verilmiştir. Bu öneride yer alan güncellemeler; özellikle sorumlu tarafların sorumluluk alanları artırılmış ve suç fiili ile bağlantılı fiiller suç kapsamına alınmıştır. Kapsamının genişletilmesi ile öncül suçlar ile ilgilidir. 1991 yılında yayınlanan direktifte öncül suç

olarak sadece uyuşturucu suçları bulunmakta iken yeni düzenleme ile bütün organize yasak fiiller ve kaçakçılık kaynaklı paranın aklanmasıyla mücadele de kapsama dahil edilmiştir. Ayrıca yeni hükümler ile, yalnızca finansal alanlarla çerçevelenmiş kapsam; belirli faaliyetler ve meslek gruplarının da eklenmesiyle genişletilmiştir. Bu şekliyle ile muhasebeci ve kontrolörler, mali işlem avukatları, kıymetli taş ve maden ticareti yapan satıcıları, emlak komisyoncuları, noterler, para transfer edenler ve kumarhanelere çeşitli yükümlülükler getirilmektedir.

Üçüncü olarak "2005/60/EC Sayılı Avrupa Parlementosu ve Konseyi Direktifi" ile "1991/308/EEC sayılı direktif" mevzuattan kalkmıştır. Yerine 2005 yılında kabul edilen yeni direktif ile Avrupa Birliğine üye ülkelerin Karapara Aklama suçu ile Mücadele kapsamında mevzuatlarında yapmaları gereken yeni düzenlemelere yer verilmektedir. Üçüncü direktif olarak da bilinen yeni düzenleme ile getirilen en temel yenilik direktifte önleyici tedbirler olarak sayılan bütün tedbirlerin terörizmin finansmanı kapsamına alınmasıdır. Ayrıca "müşterini tanı" prensibinin getirilmesi ile işlem gerçekleştiren müşterinin; kimlik tespiti, özen ilkesi ve risk takibi gibi konulara ilişkin yeni yükümlülükler getirilmektedir. Bu düzenlemelere ek olarak, aklama ve terörizme kaynak sağlanan yasadışı fiillere yönelik olarak hazırlanan analizlere göre CDD tedbirleri öngörülmüştür.

2.1.3.6.4.7. EGMONT Grubu

Egmont Grubu, 1995'de Brükselde 24 ulusun ve 8 uluslararası organizasyonun katılımıyla kurulmuştur. 2020 yılı itibariyle üye sayısı 139'a ulaşmıştır. Türkiye Mali Suçları Araştırma Kurulu (MASAK) ile 1998'de gruba dahil olmuştur. Organizasyonun genel amacı, üye ülkelerin mali denetim ve takip süreçlerinde kara para aklama ile mücadelelerinde yardım etmek, yol göstermek ve uygulamalarını geliştirmektedir. Bu sayede üye ülke kuruluşları ile oluşturulan iş birliği ağı sayesinde bilgi akışının kurumsallaşması, insan kaynakları faaliyetleri, teknik altyapı desteği ve tecrübe paylaşımını gibi destekler sağlanmaktadır. İlk başta sadece suçtan elde edilen paranın aklanması konusunda görev üstlenen grup ABD'deki 11 Eylül saldırılarının akabinde terörizmin mali kaynaklarının keselmesine yönelik çalışmalar daha hassas ve titizlikle takip ettiği konular olmuştur. Üyeler arasında veri akışı ve diğer konulardaki eşgüdüm ve paylaşımın sağlanabilmesi için "Egmont

Güvenlik Ağı" sistemi kurulmuştur. MASAK da bu ağa Mayıs 2001 de entegre olarak ESW ağının imkân verdiği fonksiyonlardan yararlanmaya başlamıştır.

2.2. TERÖR VE TERÖRİZM

2.2.1. Terör ve Terörizmin Tanımı

Terörizm terim olarak latince kökenli bir kelime olup "bilinmeyen ve öngörülemeyen bir tehlike karşısında duyulan aşırı korku, endişe ve dehşet" manasında kullanılan "terror" kelimesinden türemiştir. İlk olarak 1335 yılında Fransızca'da kullanıldığı tespit edilen terör ve terörizm kavramları bu tanımlamalarda kulanıldığı şekliyle; terör, korku ve dehşet, terörizm ise yıldırma, illegal politik ideolojik mücadelelerin şiddet yöntemleriyle gerçekleştirilmesi anlamında kullanılmıştır. Terör kavramının Türkçe'de anlamı korku yayma yıldırma fiillerine karşılık gelmektedir. Fakat terör kavramı Türkçe'de de yerleşik olarak, çoğu dildeki kullamın şekliyle aynı, müstakil bir kelime olarak kullanılmaktadır. Buradaki "korkutma", "yıldırma" ifadeleri yoğun bir şekilde büyük çaplı, bireylerin veya toplumun ruhsal yapısını aniden saran korku ve şiddet durumu anlamında kullanılmaktadır (Yıldırım, 2012).

Çakmak ve Kuruma göre de Terör, "belirli bir amaca ulaşmak için hukuk dışı yollarla yapılan eylemdir". Terörizm ise, "yapılan eylemleri savunan, stratejilerini anlatan, aktaran ve geliştiren bir düşünce disiplini veya akımı" olarak tanımlanmaktadır (Çakmak ve Kurum, 2008).

Bu manada değerlendirildiğinde terör kavramı için, şiddet fiili; terörizm kavramı için de ideolojik, politik vb bir hedefe erişmek amacıyla şiddeti araç edinen stratejik ve sistematik bir süreç olarak nitelendirilebilir. Yine bu bağlamda şiddeti, politik ve ideolojik amaçlı kullanımının dışında salt olarak terör faaliyeti şeklinde ifade etmek mümkün olmaktadır (Dilmaç, 2011).

BM; 1999 sayılı sözleşmenin 2'nci maddesinde terörizm tanımı; "silah kullanarak, bir amacın gerçekleşmesi ya da gerçekleşmemesi için, kişileri, halkı, karar vericileri veya ulusları sindirmek için doğrudan otoriteye veya sivillere yönelik gerçekleştirilen her türden eylem olarak tanımlanmaktadır (MASAK, 2015).

Terör tanımında ulusal ve uluslararası olarak da sınıflandırma yapılmaktadır. Ulusal terör hiçbir dış bağlantısı olmayan, kaynağını, nedenlerini ve sonuçlarını ülke

içinde bulan bir terör türüdür. Ulusal terörde adi suçların kolaylıkla işlenebilmesinden dolayı bu tür terörün amacı sadece toplumdaki korkuyu arttırmak iken, uluslararası terörizmde amaç somut bir siyasi hedefe ulaşmaktır (Çakmak ve Kurum, 2008).

Uluslararası terör yabancı bir devletin veya uluslararası bir örgütün politikalarını etkilemek üzere bir veya birkaç devletin desteğini alarak hedef aldığı bir veya birden fazla ülkeye karşı gerçekleştirilen ve uluslararası sonuç doğuran şiddet eylemleri şeklinde tanımlanmaktadır (Onay, 2009). Terörizm kavramını tanımlanmasındaki zorluk nedeniyle, genel olarak ittifak edilmiş bir tanımı yoktur. Bunun sebebi olarak ise terörizmin politik söylemlere karşıt gerçekleştirilen çelişkili fiillerden kaynaklanmasındandır (Yücebaş, 2011).

2.2.2.Terörizmin Amacı

Terörün temel gayesi siyasal anlamda zorbalıkla iktidara sahip olmak ya da bunu gerçekleştiremese bile bu anlamda onu güçsüz düşürmek zaafa uğratmak ve böylelikle devletin millet unsuru üzerinde korku ve çaresizliği şiddet unsuru ile yerleşik kılmaktır (Yücebaş, 2011, s.146).

Aykın ve Gümüşay'a göre ise terörizmin amacı; hedefindeki meşru düzene, onun iktisadi ve toplumsal yapısına, olumsuz tesir ederek, belirledikleri hedeflere uygun kararlar çıkarılmasını dayatmak, ya da meşru düzeni tümüyle ortadan kaldırarak kendi ideolojisine uygun gayrimeşru bir düzen inşa etmek olarak ifade edilebilir. (Aykın ve Gümüşay, 2008, s. 342).

Gerçekleştirdikleri veya gerçekleştirmeye çalıştıkları terörist eylemlerle, terör örgütleri; varlıklarını kitlelere duyurarak üyelerine ve yandaşlarına motivasyon sağlayıp onları şiddet eylemlerine yönlendirmeyi, kendi fikirlerini benimsemeyenlere korkutup sindirerek, meşru düzenin otoritesini sarsmayı böylelikle güç devşirerek üyeleri üzerinde hakimiyet kurmayı ve eylemlerini sürekli gerçekleştirerek sürekli kargaşa ortamını ve gündemde kalmayı amaçlamaktadır (Özkan, 2006, s. 8).

Uluslararası politika aracı olarak da kullanılan terörizm, var olan veya dışarıdan müdahalelerle oluşturulan ayrılıkçı, bölücü veya devrimci düşünce ve eylemlerin belirli bir yönde harekete geçirilmesi ile şekillenmektedir. Terör eylemlerinin temelinde örgütün propagandasını yapma ağırlık kazanmaktadır. Örneğin din motifli terör örgütleri belirli politik hedeflere ulaşmaktan çok dini hedeflere

yönelmektedir. Terör eylemleri sonucunda hedef alınan kitlenin veya kamuoyunun yıldırılması, sindirilmesi amaçlanmaktadır (Yıldırım, 2012, s. 13-14).

2.2.3.Terörizmin Özellikleri

Terör örgütlerinin kaynakları bulunduğu coğrafya eylem şekilleri üzerinden kendilerine özgü özellikleri bulunmakla birlikte genel hatlarıyla terörizmin özelleiklerini şu şekilde ifade etmek mümkündür;

- Terörizm bir stratejidir. Siyasi bir düşünce ya da ideoloji değildir.
- Şiddet eylemleri, örgüt tabanının rızasını kazanacak, haklılık düşüncesi yaratacak nitelikte bir kurgu ile tasarlanır.
- Uygulanan şiddet ve çekiler acılar büyük bir zafer ve mutluluk içindir.
- Uluslararası ilişkilerde bir argümandır. Her meşru gücün bir gayrı meşru uzantısı bu ilişkilerde oldukça fonksiyonel olmaktadır.
- Terörizm = Propagandadır.
- Terörizm profesyonel bir organizasyondur.
- Terörizmin olmazsa olmaz gereksinimi insan ve mali destektir. Bu nedenle silah, uyuşturucu kaçakçılığı ve soygun doğal faaliyetleridir.
- Hikâyenin başlangıcı bir hak mücadelesine, buna bağlı olarak bir sistem ya da devlet oluşturma fikrine dayanır.
- Terör faaliyetleri iradi ve planlı fiillerdir, bir gaye uğruna gerçekleştirilir.
- Şiddet unsuru varlık sebebidir ve bu uğurda hiçbir referansı ya da kuralı yoktur.
- Temel başarı kriteri toplam korku ve yılgınlık ile ölçülmektedir.
- Terör kimi zaman bir meşru gücün taşeronluğunu gerçekleştirebilir
- Terörün kendine has bir jargonu vardır ve bunun üzerinden iletişim kurar.
- Terör eylemleri, örgütlü bir şekilde icra edilir. (Alkan, 2002, s. 17-18).

2.2.4. Terörün Çeşitleri

2.2.4.1. Ulusal Terör

Bir ulusun sınırları içinde kanal, varlığı ve eylemleri tek bir ülke ile sınırlı herhangi bir dış kaynaktan beslenmeyen planlı ve devamlı terör çeşididir. Teröristler eylemlerini bir ulusun vatandaşlarına karşı yöneltirler (Taşdemir, 2006, s. 34). Bir

terör eyleminin iç ya da uluslararası olup olmadığını belirleyen bazı kriterler bulunmaktadır. Bunlar; eylemi gerçekleştiren kişi veya grupların eylemin yapıldığı ülkeden olup olmaması, hedefin saldırının yapıldığı ülkenin bir parçası ya da uyruğu olup olmaması, gerekli silah, eğitim, istihbarat desteklerinin nereden sağlandığı (Altuğ, 1995, s. 378).

Küreselleşme olgusuyla birlikte terörizm de artık yerelden globale doğru evrilen bir kavram olarak karşımıza çıkmaktadır. Dünyanın giderek küçüldüğü bir ortamda Uluslararası ilişkiler yoğunlaşmaya başlamış, mesafeler giderek kısalmıştır. Teknolojinin her geçen gün gelişme göstermesi terörizmin de küresel ölçüde değerlendirilmesi gereken bir olgu olarak karşımıza çıkarmaktadır. (Altuğ, 1995, s. 378). Dolayısıyla özellikle de küreselleşmeyle, bir terör örgütünün sadece ulusal terör olarak kalması mümkün değildir. Dünyada egemen güçlerin, sömürgeci ve işgalci zihniyetleri doğrultusunda da terör eylemleri bugün tek bir ulusla kalmamakta, aynı durum İslami ideolojiye sahip terör örgütlerinin de Batılı güçlere karşı birleşme ideali nedeniyle söz konusu olamamaktadır.

2.2.4.2. Uluslararası Terör

Uluslararası terör, geçmişle kıyaslandığında çok daha tehlikeli bir boyuta ulaşmıştır. Çünkü kullanılan amaçlar ve araçlar itibariyle gelişim göstermiştir. Ayrıca, sadece siyasal amaç güdülerek yapılan bir olay olmaktan da uzaklaşan uluslararası terörizm, gittikçe şekil değiştirmiştir. Dolayısıyla, giderek daha da 'Uluslararasılaşan' ve tüm dünyayı saran bir suç olarak karşımıza çıkan uluslararası terörizm, bir alanla çerçevelenmeyip coğrafya ya da millet ayırt etmeden faaliyet göstermektedir (Kaya, 2005, s. 31). Şüphesiz uluslararası terör örgütleri arkalarına bazı ülkelerin güçlerini de alarak ancak eylemlerini gerçekleştirebilmektedir. Günümüzde en ileri teknolojileri temin etme ve kullanma kapasitesi ile küresel çapta doğrudan insanı, iktisadi hayatı, ulusal ve uluslararası güven ve barışı ortamını tehdit eden uluslararası terörizm, yarattığı etkiler bakımından kimi zaman yerel kimi zaman ise küresel boyutta sonuçlar üretebilen ve tüm dünyayı ilgilendiren bir sorundur. (Topal, 2004, s. 78).

Eylül'e kadar terör olgusu için Fransız İhtilali dönüm noktası olarak kabul edilirken 11 Eylül şimdiye kadarki terörizm algısını değiştirmiştir. Dolayısıyla küreselleşen dünyada terörizmi tek bir unsura bağlı kalarak anlayabilmek ve

açıklayabilmek mümkün olmamakla beraber, yapısı ve işleyişi de olabildiğince değişen terör örgütlerinin eylemlerini tek bir terör çeşidine yerleştirebilmek de mümkün olamamaktadır.

Son 50 yılda dünyanın giderek daha küçük bir gezegen olması, başat legal güçlerin illegal amaçların hayata geçirilmesi bakımından fonksiyonel birer araç haline gelen devlet dışı aktörler, yeni ilişki ve düzen kurma noktasında giderek adından daha çok söz ettirmektedir. 1970'lerden sonra, söz konusu vekalet unsurlarının şiddet faaliyetleriyle anılmaya başlaması 'uluslar ötesi terörizm' kavramının ortaya çıkmasına neden olmuştur. Uluslar ötesi terörizm kavramı; görünürde bir legal gücün varlığından söz edemeyeceğimiz fakat etkisini devlet dışı aktörler üzerinden gösteren durumlarla ortaya koyan sistematik bir şiddet faaliyetini ifade etmektedir. Uluslar ötesi terörizmi muhteviyatı bakımından uluslararası terörizm kavramından ayrıştıran temel gösterge organizasyonun ve denetiminin organik olarak hiçbir şekilde legal bir ulusla anılmamasıdır (Saraçlı, 2007).

2.2.4.3. Devlet Terörü

Devlet tarafından bizatihi devletin bir kuruluşu veya devlet ile ilişkili olan kişi ve gruplarca, devletin kendi otoritesine karşı direnenlere karşı gerçekleştirilmektedir. Aynı zamanda mevcut rejime karşı tehdit oluşturduğu düşünülen kişi ve gruplara karşı terör uygulanması anlamına gelmektedir. Devlet terörü, direk olarak devletin bir kuruluşu tarafından yapılabileceği gibi, devletin görevlendirdiği fakat devlet dışında bulunan kişi veya gruplar tarafından da yapılabilmektedir. Kimi zaman devletle uzak veya yakın ilişkisi olmayan kişi ve gruplara devlet tarafından sağlanan birçok hizmetin söz konusu olması halinde de devlet teröründen söz edilebilmektedir (Yayla, 1990).

Devletlerin halkına yönelik olarak planlı ve sürekli olarak doğrudan insan canını hedef alan ya da çeşitli tehdit, yıldırma ya da bastırma şeklinde uyguladığı şiddet türüdür. Bu şiddetin karakteristik özelliği bir devlet politikası olarak uygularak uygulanmasıdır. Bu sebeple çok fazla terör kavramıyla birlikte anılmamaktadır. Öğreğin Lenin, Stalin, Mussolini ve Hitler gibi liderler halklarını sistematik bir devlet terörüne maruz bırakmışlardır. Bu liderlerin ülkelerinde birçok etnik grup ve azınlık gerek ırk gerek siyasi fikirlerinden ötürü baskı ve hatta soykırıma mahkûm

edilmişlerdir. (Topal, 2004). Bugün Suriye'de yaşananlar ve İsrail'in Filistin'de gerçekleştirdiği de devlet terörü niteliğindedir. Devlet terörü devletin sadece bizzat kendi halkına karşı uyguladığı bir terör değildir. ABD'nin Irak'ı işgalindeki gibi başka bir devlet tarafından da uygulanabilmektedir.

Devletin şiddete başvurmasının gözdağı vermek, baskı ile değiştirmek ve bir sınıf, etnik ya da dinsel grubun tümünü ideolojik gerekçelerle yok etmek şeklinde üç şekli vardır. Hükümetler, medya ve polis gücünü kullanarak, kendileri gibi düşünmeyenlerin cesaretini kırarlar, doğrudan ya da dolaylı tehdit edebilmektir. Özellikle Sovyetler Birliği ve İran'da olduğu gibi, devrim sonrası görülen baskı ile değişim, hükümetlerin bir ulusun hayat düzenini tümüyle değiştirme gayretlerini açıkça gözler önüne serilmektedir. Üçüncü şekildeki devlet terörüne soykırım denilmektedir. Nazi Almanya'sı, Stalin dönemi Rusya'sı, yakın dönemde Ruanda ve Bosna'da gerçekleştirilen kitlesel katliamlar, ayrıca Afrika ve Amerika'da Avrupalılar tarafından gerçekleştirilen sindirme hareketleri birer soykırım örneği olarak sunulmaktadır. Devlet terörü bir ülkenin tarihine geçen belki de en kara lekedir.

İnsan hakları ve uluslararası tüm referansları çiğneyerek 20. yüzyılda 70 milyonu aşkın insan devlet terörüne kurban edilmiştir. Bunu fırsat bilerek kaos ortamından faydalanan devlet dışı aktörler eliyle gerçekleşen şiddet olaylarında 100.000 insanın yaşamını yitirdiği bilinmektedir (Topal, 2004).

Devlet Teröründen bahsederken 1980'li yıllarda kullanılmaya başlanan bir kavram olan devlet destekli terörden de söz etmek gerekmektedir. Bu yıllarda kimi uluslar, husumet beslediği ya da menfaatlerinin çatıştığı ülkelere bir müdahale aracı olarak terörü bir ilişki kurma, düzen tesis etme yöntemi olarak benimsemiş ve kullanmıştır. Bu ve benzer nitelikte yaygınlaşan iletişim biçimi devlet destekli terörizm kavramını literatüre katmıştır (Yeniçeri, 2003). Bu bağlamda bir ülkenin direkt olarak terörist eylemde bulunması, diğer bir ülkeye yönelik sistematik tehditler yöneltmesi ya da bunu açıktan üçüncü bir taraf olarak terör örgütleri üzerinden yapması, finanse etmesi veya teşvik etmesi devlet destekli terör olarak tanımlanmaktadır (Aydın, 2009).

Devlet destekli terörün yanında devlete karşı terör de devlet terörü ile ilişkili bir başlık olarak karşımıza çıkmaktadır. Çoğunlukla mevcut düzeni yıkmaya yönelik devrimci, ayrılıkçı, bölücü ve etnik terör şeklinde karşılaşılmaktadır (Aydınalp, 2011).

Bölücü terör ise, belirli bir bölgeyi bağlı olduğu ülkeden ayırarak bağımsızlık kazandırmayı amaçlamaktadır. Burada ayrımı yapılması gereken önemli bir husus, bölücü terör ile sömürge karşıtı hareketler arasındaki farktır. Zira bölücü terör, meşruiyet sınırları içinde devletin mevcut otoritesini kabul etmeyerek muayyen bir bölgede bağımsızlık kazanma arzusuyla ilgilidir (Yayla, 1990).

2.2.5. Terörizmin Unsurları

Terörizm kavramının unsurlarını saptamak için terörizm tanımının iyi anlaşılması gerekir. Terörizmi; önceki kısımlardaki tanımlamalardan hareketle kısaca: İdeolojik temelli bir fikir çerçevesinde organize olan, iki ya da daha fazla üyeden oluşan ve şiddeti yöntem olarak kabul ederek, siyasal amaçlara yönelik olan faaliyetleri olarak ifade edebiliriz. Terörizmin hukuki açıdan kavranabilmesi için ve hangi oluşumların terörizm olduğunun saptanması için ideoloji, örgüt ve şiddet unsurlarının varlığının söz konusu olması gerekmektedir yoksa birkaç kişinin bir araya gelmesi terör örgütü olarak kabul görmemektedir. Bu sebeple terörden bir suç olarak bahsedebilmek için;

- Devletin ve halkının huzuruna bütünlüğüne kamu düzenine kast eden bir tehdidin varlığı (ideolojik boyut)
- Yasadışı bir organizasyonun varlığı (örgütsel boyut)
- Terörist eylem içeren şiddetin (Şiddet boyutu) varlığı şarttır (Fığlalı, 1998, s. 79-80).

Yukarıda sıralanan bu şartlardan ilki "amaç" ikincisi "fail" sonuncusu ise suçun "hareket" şartını yerine getirmektedir. Bu bağlamda amaç, ideolojik motivasyona; fail, terör örgütüne, hareket şartı da şiddet unsuruna karşılık gelmektedir (Şen, 2015, s.26).

2.2.5.1.İdeoloji Unsuru

Terör örgütlerinde ideoloji vazgeçilmez bir unsur olarak göze çarpmaktadır. İdeolojik unsur terör örgütlerinin hareketlerinin özünü oluşturur ve onun öteki şiddet eylemlerinden ayrılmasını sağlar. Şiddet barındıran ve organize olmuş suç şebekelerinden terör örgütlerini farklı kılan ideolojik yaklaşımdır. İdeolojiler terör örgütlerinin hareket noktalarının temelini oluşturduğundan; örgütünün yapıları,

eleman sağlamak, eylemlerin içerikleri ve biçimleri, uygulanacak program kesinlikle ideoloji kapsamında belirlenir. Genellikle örgüt, ideolojiyi benimseyen benzer amaca yönelmiş ve organize edilmiş kişilerden oluşur. Terör örgütü üyelerinin en önemli handikapı üyesi olduğu örgütün benimsediği ideolojileridir. Kişi ideoloji çerçevesinde düşüncesini, fikirlerini ve anlayışını şekillendirir.

Fikirlerin ve eylemlerin sistemli bir şekilde doğruluğunun ispatı ve kitlesel olarak yayılması böylece diğer fikir ve eylemleri etkilemeyi amaçlayan, söylem ve eylemlerdir. (Ergil, 1983, s. 69). Louis Althusser'e göre ise; sosyal yaşantıya özgün bir şekilde doğal olarak tesir eden bir süreçtir. Başka bir ifadeyle toplumsal pratik ile ideoloji ayrılmaz bir bütündür. Bütün düzene nüfuz etmiş ve sosyal varoluşun her noktasında bulunmaktadır (Kazancı 2002, s.57).

Bir ideolojiyi benimsemiş kişinin, o ideolojinin şekillendirdiği eylem ve söylemlere olan inanışı, bunları hayatına tatbik etmesi sonucunu doğurmaktadır. Düşüncelerin fiillerle hayat bulması gibi ideolojiler de onların uygulanmasıyla hayat bulmaktadır (Güngör, 2001, s. 226).

Şiddetin terör halinden bahsedebilmek için bir fikir çerçevesinde önceden saptanmış bir amaca doğru davranışlar sergileyen bir organizasyonun varlığı gerekmektedir. Zira her türlü yapılanma yıkıcı olsun ya da olmasın bir ideolojiye sahiptir. Dolayısıyla ideolojinin varlığı her durum için terörizm olarak nitelendirilmemektedir. Terörizm kavramı içerisinde değerlendireceğimiz ideoloji, şiddeti bir yöntem olarak kabul eden, düşünsel hedeflerini şiddet yoluyla hayata geçirmeyi amaçlayan siyasi temelli bir ideolojidir. İdeoloji terörün fikri açıdan en önemli motivasyonunu oluşturmaktadır. Nitekim bu saik ile örgüt üyeleri hayatlarını ortaya koymaktadırlar. Hayata dair çoğu güzel şeyden vazgeçip birçok sıkıntıyı da gönüllü kabul etmektedirler (Dilmaç 2004, s. 360).

Dünyada ve Türkiye'de terör örgütlerine birçok ideolojik akım kaynak teşkil etmektedir. Dini, milliyetçi, etnik, Marksist-Leninist-Maoist akımlar birçok örgütün ideolojik motivasyonunu şekillendirmektedir (Öztürk ve Çelik, 2009, s. 88).

2.2.5.2. Örgüt Unsuru

Örgüt, belli hedefe ulaşmak, bir gayeyi mümkün kılmak maksadıyla kurulmuş bir grup, organizasyon ya da teşkilat şeklinde ifade edilebilir. Bu ifade edilen örgüt yasal anlamdaki örgüttür. Bir de yasadışı oluşan örgütler vardır.

İllegal anlamda örgüt; kanunun suç saydığı eylemleri işlemek üzere aralarında teşriki mesai ve hiyerarşi ilişkisi bulunan iki veya daha fazla kişinin oluşturduğu birlik, teşekkül şeklinde ifade edilebilir. Ancak bir suç işlemek üzere bir araya gelmek örgüt kurma suçunu oluşturmaz. Örgüt suçunun oluşabilmesi için; amaç, yeterlilik, üye, süreklilik ve sempatizan gibi örgütün unsurlarının bulunması gerekir.

Terör örgütlerinin eylemlerinde hedeflerine ulaşabilmesi için örgütlenme önemli bir yere sahiptir. Çünkü örgüt teröristi suç üreten bir robot haline dönüştürerek onu belli bir eğitim ve şartlanma sürecine sokar. Böylece örgütünün varmak istediği sonucu eğitilen kişiyi kendiliğinden keşfeder (Bal, 2003, s. 278).

Örgütlenme üç ana unsur etrafında teşekkül etmektedir (Dilmaç, 2004, s. 360).

- Merkezi Yapı–Çekirdek–Lider Kadrosu
- Silahlı Eylem Grubu–Askeri Kanat
- Propaganda Birimi

Terör örgütlerini meydana getiren ana unsurların yanında bir de destek unsurları vardır. Destek unsurları iç ve dış kaynaklı destek unsurları olarak ikiye ayrılmaktadır. İç kaynaklı destekler; örgütün faaliyet yürüttüğü devlet içindeki belli bir halk kesiminden sağlanmaktadır. Dış desteklerde ise söz konusu faaliyetleri gerçekleştirebilmek için örgütler diğer devletlerden kaynak sağlamaktadır. Dış kaynaklı destekler çoğunlukla terörist faaliyet yürütülen ülkeye sınırı olan başka devletlerce sağlanmaktadır (Kuyaksil, 2014, s. 86).

Terörü bir yöntem olarak tercih eden örgütlerin amaçlarına erişebilmesinde yasadışı bir organizasyon şeklinde örgütlenmek kaçınılmaz bir gerekliliktir. Sadece yasadışı bir örgüt, şiddet eylemlerinde devamlılık sağlayabilir. Bu komplike sürecin en bariz tarafı da yüksek gizliliğe dayanmasıdır (Dilmaç, 2004, s. 360).

2.2.5.3. Eylem – Şiddet Unsuru

Eylem, belli bir ideoloji etrafında örgüt haline gelerek amaçlarını gerçekleştirmek isteyen grupların başka bir önemli unsurudur. Terörizm kavramlarında genellikle bir hareketin terörist eylemi sayılabilmesi için mutlaka şiddetin varlığı üzerinde vurgu yapılmıştır. Bir eylem terör eylemi olması için şiddet şarttır. Çünkü şiddet terörün aracıdır. Şiddet barındırmayan ideolojik örgütler terörizm olarak kabul görmemektedir. Şiddet hareketinin terörizm sayılabilmesi için bilinçli ve isteyerek, organize olmuş bir şekilde, hedef seçimi ve bu hedeflere uygun silah kullanarak ve örgüt haline gelerek gerçekleştirilmesi gerekir.

Şiddet, öteden beri ilişkilerin tesisinde, problemlerin sulha erdirilmesinde sürekli kullanılan metotlardan biridir. Terörde şiddet unsuru mutlaka vardır. Şiddetsiz terör olmaz. Terörü terör yapan hedefine ulaşmak için uyguladığı şiddet yöntemidir. Bu bağlamda yapılan tüm terör tanımlarında şiddet unsuruna atıf yapılarak terör açıklanmaya çalışılmıştır (Ceylan, 2012, s. 59).

Eylem, terörist veya bir örgüte bağlı teröristlerce örgütünün amaçları doğrultusunda seçilen hedeflere, amaçlanan etkiyi yapmak adına içinde hukuka aykırı şekilde ve haksız olarak şiddet barındıran faaliyetlerin bütününe verilen addır (Ceylan, 2012, s. 60).

Terörist yapılanmalar, kuruluş safhasının akabinde belli mesafe kat ettikten sonra örgütü, künyesini, amacını kamuoyunda ilan ederek ilgi uyandırmaya çalışırlar. Örgütler sonrasında deklere ettikleri amaçlara yönelik eylemler gerçekleştirirler. Bu aşama eylem aşaması olarak tanımlanmaktadır (Alkan, 2002, s. 73). Türkiye'de bölücü faaliyet yürüten PKK terör örgütünden de bilindiği şekliyle, ideolojik temelli kuruluş aşamasını tamamladıktan sonra 1984'de Eruh ve Şemdinli'de ilk eylemlerini gerçekleştirmiş bu sayede adını duyurmaya çalışmıştır (Dilmaç 2004, s. 360). Bu kapsamda değerlendirildiğinde terör örgütleri şiddete başvurarak bazı amaçlara ulaşmayı hedeflemektedir.

- Terör örgütleri, ses getirecek eylemler ile potansiyellerini kamuoyuna duyurmak ve taban genişletmek ve örgüt içindeki sadakati artırmak isterler.
- Örgütün faaliyet gösterdiği bölgede örgütle zıt düşen, maddi ve manevi katılım konusunda olumsuz tavır takınanlara gözdağı verirler.

• Terörist eylemler neticesinde bu durumu bertaraf etmek isteyen otorite ile savaş imajı yaratıp devamlı kaynak tedariki sağlamak (Şen, 2015, s. 32).

2.2.6. Terörizmin Finansal Kaynakları

2.2.6.1. Yasadışı Faaliyetlerden Elde Edilen Gelirler

Uyuşturucu kaçakçılığı, Terör örgütlerinin gelir elde etmede en çok başvurdukları yollardan birisidir. Bu tür maddeler, kazancının yüksek, nakliyesinin kolay, talep eden kitlenin geniş, talep elastikiyetinin sert, tedavüldeki her cins para ile takası mümkün, üretimi kolay ve pazarlama ağının yaygın bir mal olması nedeniyle pek çok terör örgütünün finans kaynakları arasında yer almaktadır (Caşın, 2008. s.533). Terör örgütlerinin uyuşturucu kaçakçılığı yapmalarındaki tek sebep mali kaynak sağlamak değildir. Günümüzde uyuşturucu kaçakçılığı ile terörizm arasındaki bağlantı ve bunun kapsamı öyle bir hâl almıştır ki tüm dünyada narko terörizm adı verilen yeni bir kavram ortaya çıkmıştır.

Interpol raporlarına göre PKK terör örgütünün 178 farklı yasadışı örgütle bağlantısının olduğu, Avrupa uyuşturucu pazarının %80'ini elinde tuttuğu dahası diğer uyuşturucu kaçakçısı örgütleri haraca bağladığı ve bu yolla da elde ettiği gelirle örgüt ve eylemlerini finanse ettiği belirtilmektedir. PKK'nın uyuşturucu kaçakçılığından yıllık 200-250 Milyon Avro elde ettiği tahmin edilmektedir. PKK terör örgütünün yıllık gelirinin tahmini 400 ila 500 milyon avro arasında olduğu düşünüldüğünde finansal desteğinin yarıdan fazlasını uyuşturucu kaçakçılığından sağladığı anlaşılmaktadır (Sever, 2008).

Silah ve mühimmat kaçakçılığı; *"sıcak savaş tehlikesi veya terör olaylarının tırmandığı dönemlerde ortaya çıkan ve artarak devam eden bir kaçakçılık şeklidir. Bu kaçakçılık türünde ana amaç maddi kazanç temin etmektir. Silah-mühimmat kaçakçılığında rota olarak özellikle otoritenin ve düzenin bulunmadığı karışıklığın devam ettiği bölgelerden, çeşitli yollarla kaçakçalık konusu malzemelerin hedef olarak seçilen ülkeye sokulduğu görülmektedir. Kaçakçılık faaliyetleri, hedef ülkenin ekonomik kaynaklarını zarara uğramakta ve güvenlik zaafiyetinin yaflanmasına yol açmaktadır"* (KOM, Faaliyet Raporu, 2005, s. 84).

Göçmen Kaçakçılığı ve İnsan Ticareti, günümüzde küresel bir problem olarak değerlendirilmektedir. Bu yaygın sorunlar da yine yaygın bazı yasadışı faaliyetlere

dönüşmektedir. Bu suç türü "yasadışı göç" olarak nitelendirilen, göçmen kaçakçılığı ve insan ticareti şeklinde ortaya çıkmaktadır. Savaş, iç karışıklıklar, daha iyi yaşam umudu, kötü ekonomi, insan hakları gibi nedenlerle ülkelerinden kaçanlar, kişi başına 5 ila 10 bin dolar arasında para ödemektedirler (Altunok ve Çakmak, 2009).

Haraç Toplama ve Fidye Alma; *"Terör örgütleri, kişilere koruma vaadinde bulunma, zarar vermeme garantisi sağlama, bir şekilde şahit olduğu veya öğrendiği bir suçu veya durumu yetkili mercilere bildirme tehdidinde bulunarak şantaj yapma veya adam kaçırma karşılığında kişi veya gruplardan zorla para toplamaktadır. Haraç vermeyi istemeyen kişileri kaçırmakta, işyerlerini bombalamakta veya suikastlar düzenlemektedirler"* (Aykın ve Sözmen, 2008, s. 31). Birçok terör örgütü finanasal kaynak sağlamak veya adlarını geniş kitlelere ulaştırabilmek maksadıyla daha çok varlıklı kişileri ve devlet görevlilerini kaçırma eylemlerinde bulunmuştur. Bu eylemler neticesinde elde etmiş oldukları fidyelerle kendilerine kaynak yaratmaktadırlar (Aykın ve Gümüşay, 2008, s. 358).

Sahtecilik; *"Günümüzün gelişen teknolojik imkânları dolayısıyla her türlü baskı, araç, gereç ve malzemesini kolaylıkla bulabilen ve sahtecilikte uzmanlaşan terör örgütleri, hem kendi mensuplarına sahte pasaport ve kimlik basmakta, hem de talep halinde organize suç örgütlerine sahte belge düzenlemek suretiyle gelir temin etmektedirler"* (Demirtaş, 2015, s. 21).

Taklit ve Kopya Ürün Ticareti; OECD'ye göre, küresel ticaretin %7'si taklit ürünlerin ticari faaliyetlerini kapsamaktadır. Kimi örgütler popüler ürünlerin taklitlerinin ticaretini yaparak örgüte gelir sağlamayı amaçlamaktadır.

Kredi Kartı Dolandırıcılığı; Terör örgütleri eylemlerini finanse edebilmek maksadıyla kredi kartı, çek dolandırıcılığı ve sigorta sahtekârlığı gibi yöntemlerle kaynak yaratmaktadır (Aykın ve Sözmen, 2008, s. 32).

Gasp ve Hırsızlık; Terör örgütlerinin, özellikle kuruluş yıllarında başlangıç finansmanını sağlamak ve örgütlerinin tanınması ve propagandasını yapmak için genellikle küçük çaplı örgütler tarafından bankalar, iş yerleri ve para nakil araçları gibi para bulunduran yerlere ve taşıyan araçlara yönelik eylemlerde bulundukları ve bu yolla önemli miktarlara ulaşan gelir elde ettikleri bilinmektedir (Yıldırım, 2012, s. 93).

Değerli Taş ve Maden Kaçakçılığı; Terör örgütlerini finansal açıdan destekleyen hayır kurumları ile vakıfların üzerindeki sıkı denetim ve bunların bazı

malvarlığı değerlerinin dondurulmasına sebebiyet veren işlemler bu kaynakların azalmasına neden olmuştur.

Değerli mücevherler, altın, gümüş benzeri değerli taş ve maden kaçakçılığı, muhafaza edilmesi ve bir yerden bir yere transfer edilebilme kolaylığı ile hemen hemen nakit paraya eşdeğer oranlı likiditeye sahip olması nedeniyle terör örgütleri tarafından büyük ölçüde tercih edilen ve hızla gelişen yeni yöntemlerden olarak karşımıza çıkmaktadır.

Akaryakıt, Sigara, Lüks Araç ve Diğer Kaçakçılık Yöntemleri; Terör örgütleri, lüks araçları sahte işlemlerle ve ucuz yollarla bazen de hırsızlık yapmak suretiyle elde edip bir ülkeden başka bir ülkeye götürüp satarak veya buna benzer yöntemlerle akaryakıt, sigara, elektronik eşya, canlı hayvan veya başkaca ekonomik değeri yüksek olan ticaret ürünlerini kaçakçılık yöntemi kullanılarak büyük ölçüde gelir elde etmektedirler. Irak'ta terör eylemleri yapan grupların en önemli gelir kaynağı akaryakıt kaçakçılığı ve hırsızlıktan elde edilmektedir. Irak yılda 4 ila 5 Milyar Dolar değerinde petrol ihraç etmekte olup, bunun %30'u çalınmakta ve ülke içinde ya da komşu ülkelere kaçak yollarla sokulmak suretiyle karaborsada tekrar satılmaktadır.

Terör örgütleri, her geçen gün teknolojinin ve çağın getirdiği olanaklar içerisinde yeni yöntemlerle yasadışı yollardan kolay gelir elde etme peşinde olduklarından yukarıda anılan yasadışı yollarla gelir elde etme yöntemleri de zamanla çeşitlenerek artmaktadır. Terör örgütleri kendilerine fon sağlama konusunda işlenebilecek ve işleyebileceği her suça iştirak edebilir ve kendisi için rant gördüğü her alanda kendisini gösterebilir ve o alanda kendini hissettirebilir (Yıldırım, 2012, s. 97).

2.2.6.2. Yasal Görünümlü Faaliyetlerden Elde Edilen Gelirler

Örgüte Yardım Adı Altında Aktarılan Paralar; Terör örgütlerine yapılan yardımlar genellikle aidat ve bağış adı altında sempatizanlar ya da örgütle bağlantısı bulunmayan kişiler tarafından para ya da eşya şeklinde gönüllü olarak ya da korku nedeniyle yapılan yardımlar şeklinde yapılmaktadır (Caşın, 2008). Kimi zaman bu yardım, gelirin belli bir oranının örgüte aktarılması şeklinde olabileceği gibi, kimi zaman örgütle organik bağları olan bir kuruluşa (vakıf, dernek gibi) yapılan yardım şeklinde de olabilir. Bunun yanında örgütle bağlantılı etkinlikler için bilet alımı, örgüte

ait televizyon kuruluşlarına yapılan reklamlar da bu yardımın farklı şekillerdeki tezahürüdür (Akın, 2009, s. 368).

Vakıf ve Derneklerin Kullanımı; *"Terör örgütleri hayır kurumu adı altındaki kuruluşlar aracılığı ile kişilerin dini, etnik veya coğrafik bağlarını kullanmak suretiyle önemli miktarda gelir elde etmektedir"* (Sözmen ve Aykın, 2008, s. 40). Genel olarak "kâr amacı gütmeyen kuruluşlar" şeklinde ifade edilen yapılar Türkiye'de daha çok dernek ve vakıf şeklinde ortaya tasnif edilmiştir. Vakıf ve derneklerin en önemli özelliği, terör örgütleri ile organik bir bağlantılarının olmaması nedeniyle, buralara çeşitli yardımlarda bulunan bazı kişilerin yaptıkları yardımların terör örgütlerine aktarıldığından bihaber olmalarıdır. Bu tür organizasyonlar, hukuk sistemleri tarafından desteklendikleri için, bunlara terör örgütlerinin sızma tehlikesi bulunmaktadır (Akın, 2009, s. 368).

Örgütsel Yayınlardan Elde Edilen Gelirler; Terör örgütleri, yazılı veya görsel araçlarla yayınladıkları televizyon programları ve basılı yayınlar ile eylemlerini duyurmak propaganda yapmak ve gelir sağlamayı amaçlamaktadır. Terör örgütleri basın ve yayın yoluyla propagandalarını yaptıkları gibi, bu organlar sayesinde önemli bir gelir kaynağı da yaratmaktadırlar (Yıldırım, 2012, s. 79).

Ticari Faaliyetler; Terör örgütlerinin de ticari faaliyetlerde bulunarak kendilerine fon sağlamaktadır. Elbette bu yapılırken daha ziyade sicili temiz kişilerin paravan olarak kullanıldığı tahmin edilmektedir. Aksi takdirde, söz konusu ticari işletme ile örgüt arasındaki bağlantıların kolaylıkla tespiti mümkün hale gelmektedir (Akın, 2009, s. 369). Terör örgütlerinin doğrudan kurduğu ve işlettiği ticari işletmeler kurulan ülkelerin kanunlarına göre yasaldır, fakat elde ettiği gelirleri aktardığı örgüt yasadışıdır ve terör örgütüdür (Çakmak ve Ünsal, 2009, s. 129).

Sosyal Etkinlikler; Terör örgütleri kendileri için organize edilen sosyal ve kültürel içerikli etkinlikler ile önemli miktarlarda gelir elde edebilmektedirler. Terör örgütlerinin yapılanma tarzları ve kadrolarının niteliği temelde suç örgütleri ile benzeşmektedir. Terör örgütleri hukuken nitelikli suç örgütü niteliğine haizdir. Bu nedenle terör örgütlerinin, tıpkı suç örgütleri gibi yasa dışı faaliyetler yürüterek, bazen de yürütülen yasa dışı faaliyetlerden pay almak suretiyle önemli bir yasa dışı gelir kaynağına sahiptir. Faaliyet alanları dar olan terör örgütleri daha çok basit suç faalyetlerini işlerken, büyük ölçekli terör örgütleri ise uyuşturucu kaçakçılığı, insan

ticareti, göçmen kaçakçılığı gibi uluslararası boyutlarda işlenen suçlardan gelir elde etmektedir. Bu kaynaklar aşağıdaki başlıklar altında açıklanmaya çalışılmıştır.

Yabancı Devletlerce Yapılan Yardımlar; Bir ülkede ortaya çıkan terör örgütünün dış devletlerin desteği olmadan varlığını devam ettirebilmesi imkânsızdır. Dış devlet desteklerinin birçok nedeni vardır; ekonomik ilişkiler, kültürel ve dini bağlar, stratejik iş ortaklığı, güvenlik, etnik bağ vb. nedenlerle dış devlet destekleri yapılmaktadır. Bu kapsamda yabancı devletlerin yapmış olduğu yardımlar 3 şekilde görülmektedir,

- Terörü Destekleyen Devletler; Bu devletler terör örgütlerini destekler ve terör örgütlerine ideolojik, finansal, askeri, operasyonel ve teknik yardımlarda bulunur.
- Terör Eylemlerini Yönlendiren Devletler; Bazı yabancı devletler amaçlarını gerçekleştirebilmek için kimi terör örgütlerini kullanabilmektedir.
- Terör Eylemi Yapan Devletler; Kimi devletler istihbarat görevlilerini kullanarak doğrudan terör eylemleri gerçekleştirirler. Bunun anlamı, devletlerin belli politikaları doğrultusunda savaş dışı yollarla müdehale etmesidir (Aykın ve Sözmen, 2008, s. 46).

2.2.7. Fon Transferinde Kullanılan Yöntemler

Terör örgütleri, legal ve illegal yollarla sağlamış oldukları gelirlerini ve bunlara ilişkin fon ve para hareketlerini saklama ihtiyacı duymaktadırlar. Zira terör örgütleri elde ettikleri fonları bir yerden başka bir yere güvenli bir şekilde fark ettirmeden nakletmek zorundadırlar. Bu nedenle para hareketlerini yasal ve yasal olmayan yollarla gerçekleştirmektedirler. Terör örgütleri, bazen üyeleri veya üyesi olmayan kişileri kurye olarak kullanarak veya yer altı bankacılığı denen "hawala ve/veya hundi" yöntemleriyle yasal olmayan yollardan, bazen de banka ve aracı mali kurumlar aracılığı ile yasal yollarla para transferini gerçekleştirmektedirler. 11 Eylül'den sonra resmi ve özel sektör mali kurumlarının terör örgütleri tarafından kullanılmasının sınırlandırılması yönündeki çalışmalar sonucunda terör örgütleri artan bir şekilde yasal işlemler dışına çıkmış ve yasadışı faaliyetlerin birçok türüne yönelmeye başlamıştır (Yıldırım, 2012). Bu yöntemler aşağıdaki başlıklar altında açıklanmaya çalışılmıştır.

2.2.7.1. Kuryeler Aracılığıyla Transfer

Terör örgütlerinin para transferleri için kullandığı yöntemlerden birisi, belki de en önemlilerinden olanı finansal ve aracı kurumlar kullanılmadan paranın veya değerli eşyanın fiziki olarak kuryeler aracılığıyla elden taşınarak transferi sistemidir. Bu yöntemde parayı taşıyacak kişi hem taşıdığı paranın kime ait olduğunu bilmez hem de parayı ulaştırdığı kişi hakkında ayrıntılı bilgiye sahip olmaz (Altunok ve Yenal, 2009, s. 140). Paranın kime ait olduğunun tespiti diğer metotlara göre çok daha zor olduğundan birçok terör örgütü para transferlerini kurye ile yapmaktadır. Örnek olarak, 2003 El-Kaide terör örgütünün İstanbul'da gerçekleştirdiği bombalı eylemlerinin masrafları kurye vasıtası ile Afganistan'dan gönderilen 160.000 dolar ile karşılanmıştır (Yayla, 2008, s. 437).

2.2.7.2. Mali Kuruluşlar Aracılığıyla Transfer

Mali kuruluşlar ulusal ve uluslararsı ölçekte ve buna bağlı olarak ithalat ve ihracat faaliyetleri ile yurtiçi ve yurtdışı ticaretine konu olan fon transferleri için büyük öneme sahiptir. 1980'lerden sonra yükselen küreselleşme trendi ve devletlerin bu sürece entegrasyon çabaları, teknolojinin de ilerlemesine paralel olarak, bankacılık ve fon transferi hizmetlerinin sunumunda önemli yeniliklerin ortaya çıkmasına sebep olmuştur. Bu sayede birçok fon kitlesel olarak dünyayı dolaşmaktadır (Aykın, 2008, s. 41). Finansal sistemin sağladığı bu kolaylıklar terör örgütlerinin ellerindeki fonları anonim olarak yurtiçine veya yurtdışına transferini mümkün kılmaktadır. Terör fonlarının transferi için banka, aracı kurumlar, yasal kumarhaneler, döviz şirketleri ve elektronik transfer hizmeti sunan diğer mali kuruluşlar aracı olarak terör örgütleri tarafından sıklıkla kullanılmaktadır. Bu bağlamda terör ve organize suç örgütleri, bankacılık sistemlerinde açıklar bulunan parasal varlıkların ve işlem yapan üyelerinin kullanıcı kimliklerinin saklanmasına olanak veren kuruluş ve ülkeleri daha çok tercih etmektedir (Aykın ve Sözmen, 2008, s. 52).

2.2.7.3. Bilişim Sistemleri Kullanılarak Yapılan Transfer

Terör örgütleri terörist fonların transferinde, mevcut küresel iktisadi sistemin ve teknolojik gelişmelerinin sunduğu tüm imkânlardan yararlanmaktadırlar. Özellikle bilişim sisteminin sunduğu tüm imkânlardan yararlanarak hem fon temin etmekte hem

de bu fonların transferini küresel düzeyde sağlamaktadırlar. ABD'de yapılan para transferlerinin parasal değer bakımından %90'ı; elektronik transfer yoluyla ve bankalararası takas ödeme sistemiyle gerçekleştirilmektedir. Giderek yaygınlaşan *e-cash* ve *smart card* gibi elektronik ödeme ve para transfer sistemleri; paranın transferinde kolaylıkla kullanılmaktadır. Bu durum karapara aklama ve terörist fon aktarımı için örgütlere ciddi bir potansiyel sağlamaktadır (Uyar, 2006).

İstatistiklere göre dünya üzerindeki internet kullanıcı sayısı Aralık 2009 itibariyle 1 Milyar 750.000'i geçmiştir (Internet World Stats, 2013). Bu rakamlar; bankacılık işlemleri, haberleşme, para transferleri, mal ve hizmet alımı gibi hayatın pek çok safhasına girmiş olan internetin organize suç ve terör örgütleri tarafından giderek daha fazla suistimal edileceğine işaret etmektedir. Terör örgütleri kendi web sayfaları veya gönderdikleri e-mailler aracılığıyla yardım talep etmekte, web sayfalarında satışlar yapmakta, internette paravan şirketlerini ve kendilerine fon sağlayan insani yardım kuruluşlarını kullanmak suretiyle veya internette kumar oynatarak, sahtekârlık yaparak çeşitli bilişim suçlarını işleyerek finansman ihtiyaçlarını karşılamaya çalışmaktadırlar (Uyar, 2006).

2.2.7.4. Yeraltı Bankacılık Yöntemleri Aracılığıyla Transfer

Yeraltı bankacılık sistemleri veya gayri resmi mali sistemler dünya çapında her devlette görülmektedir. Yer altı bankacılık sistemleri çeşitli adlarla anılmaktadır. Bunlar arasında *"Hawala"* ve/veya *"Hundi", "Karaborsa Döviz Mübadelesi"* gibi isimler sayılabilir. Birçok isim alan ama genelde *"Hawala"* adıyla bilinen ve yasadışı fonların yer değiştirilmesinde bir yöntem olarak kullanılan sistemin terörizmin finansmanında her geçen gün artan ilgi nedeniyle dünya çapında birçok örgüt tarafından tercih edilmektedir. Bu nedenle para hareketlerinin gerçekleştirilmesinde dünya çapında mükemmel bir ağa sahip önemli bir yöntemdir. Bu sistem aynı zamanda işçilerin evlerine para göndermesi bakımından önemli bir sosyal işlevi de görür. Çin'de, Hindistan'da ve Müslüman dünya da bu şekilde işleyen sistemin değişik türleri vardır ve dünyanın birçok yerinde kullanılan etkili bir yöntemdir (Biersteker 2008'den aktaran Yıldırım, 2012).

Hawala sistemi ile dünya da bir yıllık sürede aktarılan para miktarının 2 Trilyon ABD Doları olduğu tahmin edilmektedir. El-Kaide 11 Eylül öncesinde bu

sistemi para transferinde sıkça kullanmıştır. 11 Eylül saldırılarından akabinde El Kaide terör örgütünün 2001 yılında 30 Milyon dolar civarındaki bütçesini Ortadoğu merkezli hawala şebekesi aracılığıyla aktardığı şeklinde ciddi bulgular elde edilmiştir (Freedman, 2005).

2.2.7.5. Cep Telefonu Ödeme Sistemleri, Ticari Web Siteleri ve İnternet Üzerinden Ödeme Sistemlerinin Kullanılması

Cep telefonu ile ödeme sisteminin kullanılması oldukça kolay olup, bu sistemle havale işleminin gerçekleştirilmesi için belirli bir tutar karşılığında değer yüklenebilen bir kart ya da cep telefonu satın alınarak işlem gerçekleştirilmektedir. İnternetin dünya çapında kullanılan bir araç olmasıyla ticari web siteleri ve internet üzerinden ödeme sistemleri suç örgütleri ve terör örgütleri tarafından istismar edilmeye başlanmıştır. Günümüzde herkes tarafından kullanılan cep telefonu sayesinde tüm bankacılık ve diğer işlemlerin gerçekleştirildiği hususları göz önünde bulundurulduğunda suçlular ve terör örgütleri veya teröristler tarafından paranın transferinde yaygın olarak kullanıldığı bilinmektedir. Dünya bankasına göre; 175 milyon göçmen tarafından 2005 yılında en az 230 milyar ABD doları uluslararası havale işlemini cep telefonu aracılığıyla gerçekleştirmiştir (Aykın ve Sözmen, 2008).

2.2.7.6. Kripto Paralar Aracılığıyla Transfer

Terörizmin finansmanında nakit paranın dışında farklı yöntemlerin kullanılabilmesi mümkündür. Herhangi bir suçtan elde edilmeyip legal kaynaklı paralar somut olmayan para birimlerine dönüştürülerek online oynanan kimi video oyunlar üzerinden bir kurgu dahilinde suç örgütü üyelerine oyunun içerisinde "oyun içi alışveriş yöntemlerini kullanarak kolaylıkla transfer edilebilmektedir. Benzer şekilde doğrudan bir kripto para birimi transferi ile de gerçekleştirilebilmektedir. Bu işlemler neticesinde sanal ya da kripto kaynaklı paralar nakde çevrilerek terörist faaliyetlere kullanılabilir (Bozkurt Yüksel, 2015).

Kripto para denildiğinde ilk akla gelen Bitcoin para biriminin terörün finansmanını kolaylaştıran özelliklerinden bazıları şunlardır (Bains, 2015);

- Anonimlik: Paranın izi gizlenebilmektedir.

- Sınırlı Düzenleme: Bitcoin kullanmak herhangi bir Bitcoin işlemi için hiç kimsenin önceden izin alması gerekmemektedir,
- Uluslararası Niteliği: Bitcoin'in hukuki niteliğini çerçevelendirmek bir hayli zordur. Çoğu ülke mevzuatında henüz tanımlanmamıştır.
- Kolay Hareketlilik: Bir varlık/emtia olarak Bitcoin, fonların hareket etmesi için en kolay yoldur.

Suçlular uyuşturucuların teslimi ve bir suikastın gerçekleştirilmesi gibi herhangi bir yasa dışı faaliyetin tamamlanmasına ilişkin ödemeyi düzenlemek için akıllı sözleşmeler kullanabilirler. Fakat tüm endişelere rağmen, kamu kayıtlarında teröristlerin şifreli bir ödeme aracı olarak kripto para kullanmalarına dair somut bir gösterge bulunmamaktadır (Carlisle, 2017).

3. BÖLÜM
KRİPTO PARALARIN SINIRAŞAN SUÇLAR VE TERÖRİZMİN FİNANSMANI İLE İLİŞKİSİ

Günümüzde birçok ülkede hukuki olarak tartışmalı olan, merkezi otoriteler ve hükümetler tarafından tanınmayan kripto para birimleri, her geçen gün küresel fon transferlerinde önemli bir konuma gelmiştir. Bununla birlikte kripto paraların temel özelliklerinden olan anonimlik ve işlemlere müdahale edilemezliği birçok farklı suç faaliyetinde kullanımını cazip hale getirdiği düşünülmektedir. Bu nedenle kripto para birimleri genellikle teröristler için ideal bir araç olmakla suçlanır. Bitcoin ve benzeri alternatif para birimleri tamamen anonim olduğundan izlenmesi çok zor olsa da terörizmi finanse etmek için gerçekten uygun olup olmadıkları şüphelidir.

Geçtiğimiz yarım yüzyılda yaşanan gelişmelerle birlikte, pek çok gelişmekte olan ülke, ekonomik kalkınma, yaşam standartlarında iyileşme ve kişi başına düşen milli gelir seviyelerinde önemli iyileşmeler katetmiştir. Bununla birlikte, zayıf kurumsal kapasite, yüksek düzeyde yolsuzluk, iç savaşlar ve isyanlar yüzünden birçok ülke de negatif yönde ayrışmaktadır. Bazı bölgelerde isyancı güçler, yerel ve uluslararası terörist gruplar ile organize suç örgütleri, terörizm ve sınıraşan suçlar için bu türden otorite boşluklarından yararlanmaktadır.

Hükümetler, yasa dışı faaliyetlerden gelir elde etmek ve bankacılık sistemini istismar ederek bu varlıkların aklanmasını engellemek için mali sistemlerinde çeşitli regülasyonlar yapmaktadır. Kara paranın aklanmasına karşı küresel standartlar geliştirmek için kurulmuş hükümetler arası bir görev gücü olan Mali Eylem Görev Gücü, çoğu ülkenin aşamalı olarak benimsediği, giderek daha katı standartlar oluşturmuştur (Biswas, 2018). Bu önlemlere rağmen suç grupları, finansal sisteme erişmek için alternatif yenilikçi çözümlerini sürekli güncellemektedirler.

Teichmann (2018)'ın çalışmasında bitcoin ve benzeri kripto paraların terörizmin finansmanında büyük meblalar şeklinde kullanılmasının zor olduğu bununla birlikte darknet üzerinden terör faaliyetlerinde kullanılacak ekipmanların satın alınmasında e-cüzdanların ve kripto birikimlerin sınırlı kullanılmasının söz konusu olabileceğine dikkat çekilmiştir.

3.8. BULGULAR

3.1. Kripto Paraların Bilişim Suçlarında Kullanımına İlişkin Bulgular

Resim 3.1. : Bulgu 1

UZMANCOIN

Kripto para Monero, bir büyük borsadan daha çıkarıldı

Monero, kullanıcılarına gizlilik sağlayan özellikleri ve düşük işlem hacmi nedeniyle Huobi Kore'den liste dışı edildi.

Yazar Burak Köse 12 Nisan 2020

Gizlilik odaklı kripto para Monero'nun kolluk kuvvetlerine sorun çıkardığı biliniyor. Yakın zaman önce bir Europol görevlisi, Monero'nun soruşturmaların ilerlemesinde problem yarattığı ve Monero ile para hareketlerini izleyemediklerini kabul etmişti.

Hükümet organlarının baskıları, özellikle Asya borsalarında Monero'nun liste dışı edilmesine yol açmıştı. Monero, böylece birçok borsadan kaldırılırken şimdi, Huobi'nin Güney Kore kolu Huobi Kore de aynı kararı aldı.

Borsadan 8 Nisan'da yapılan açıklamada, 9 Nisan'dan itibaren Monero desteğinin sonlandırılacağı bildirildi. Şirket, bu kararı düşük işlem hacimleri ve kripto paranın anonimite özellikleri nedeniyle alındığını vurguladı.

Öte yandan açıklamada belirtilmese de bu karar, ülkede patlak veren cinsel saldırı skandalı Nth room olayının etkisiyle alınmış görünüyor. Nth room olarak bilinen olayda mesajlaşma uygulaması Telegram'da çeşitli sohbet kanalları oluşturulduğu ve binlerce üyeye sahip bu kanallarda genç kızlara şantaj ve tehditle yaptırılan cinsel görüntülerin yer aldığı ortaya çıkmıştı. İlgili kanallara girişin ücretli olduğu ve bu ücretin ise 200 ila 1200 dolar arasında değiştiği söyleniyordu. Kripto para Monero'nun buralardaki parasal işlemlerde kullanıldığı iddia ediliyor.

Bir başka Güney Kore borsası Bithumb, Monero'yu listelemeye devam ederken OKEx ve Upbit gibi diğer önde gelen borsalar bu kripto parayı daha önce liste dışı etmişti.

Kaynak: (Uzmancoin, 2020)

Resim 3.2. : Bulgu 2

webTekno

13 Milyon TL Değerinde Kripto Para Çalan Zanlılar, Otomobil Satışında Yakayı Ele Verdi

Beyazıt Kartal

Geçtiğimiz dönemde emniyet güçleri tarafından 24 kişinin gözaltına alınması ile başlayan kripto para operasyonunda 13 milyon TL değerinde kripto para hırsızlığı yapan dolandırıcılar, otomobil satın alırken yakalandılar.

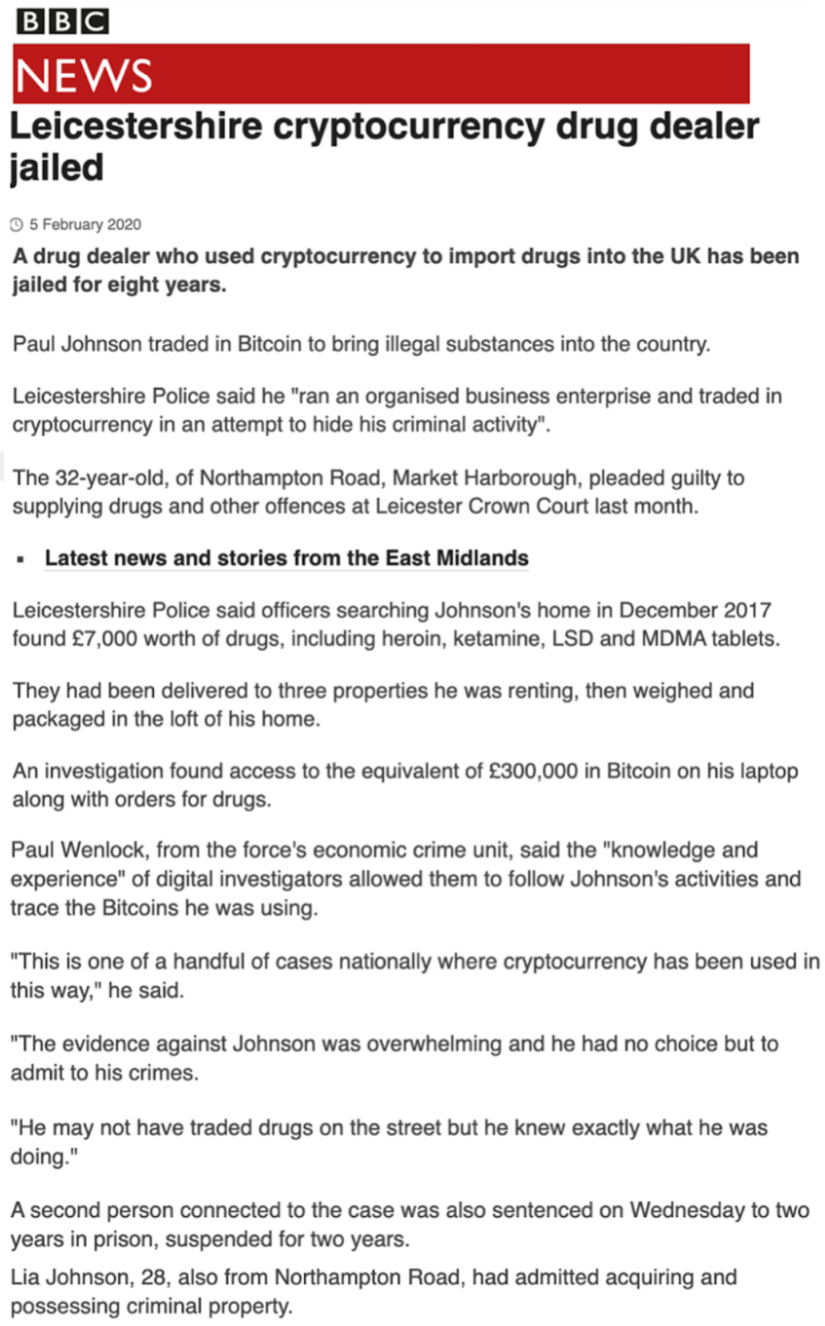
Geçtiğimiz hafta İstanbul Cumhuriyet Başsavcılığı Bilişim Suçları Soruşturma Bürosu'na bağlı ekipler tarafından ortaya çıkarılan 13 milyon TL'lik kripto para dolandırıcılığı ile ilgili yeni gelişmeler yaşandı. Çaldıkları Bitcoin, Etherium ve Ripple'lar ile otomobil alırken polis tarafından tespit edilen zanlılar kıskıvrak yakalandı.

Türkiye'nin en büyük kripto para şirketlerinden birinden 13 milyon TL değerinde kripto para çalan zanlılar, 1 milyon TL değerinde kripto para bozdurunca polisin dikkatini çektiler. Polislerin konuyla ilgili çalışmaları neticesinde paraları çalan ekibin, şirket çalışanı N.K. ile temasta olduğu ortaya çıktı.

İstanbul başta olmak üzere 7 ayrı ile operasyon gerçekleştiren ekipler, 24 kişiyi gözaltına aldı. Şüphelilerden 6'sı tutuklandı, 7'si hakkında adli kontrol hükmü uygulandı ve 9 kişiye yurtdışına çıkış yasağı getirildi. Çalınan kripto paralar ile ilgili çalışmalar ise sürüyor.

Kaynak: (Uzmancoin, 2020)

Resim 3.3. : Bulgu 3



BBC NEWS

Leicestershire cryptocurrency drug dealer jailed

5 February 2020

A drug dealer who used cryptocurrency to import drugs into the UK has been jailed for eight years.

Paul Johnson traded in Bitcoin to bring illegal substances into the country.

Leicestershire Police said he "ran an organised business enterprise and traded in cryptocurrency in an attempt to hide his criminal activity".

The 32-year-old, of Northampton Road, Market Harborough, pleaded guilty to supplying drugs and other offences at Leicester Crown Court last month.

- **Latest news and stories from the East Midlands**

Leicestershire Police said officers searching Johnson's home in December 2017 found £7,000 worth of drugs, including heroin, ketamine, LSD and MDMA tablets.

They had been delivered to three properties he was renting, then weighed and packaged in the loft of his home.

An investigation found access to the equivalent of £300,000 in Bitcoin on his laptop along with orders for drugs.

Paul Wenlock, from the force's economic crime unit, said the "knowledge and experience" of digital investigators allowed them to follow Johnson's activities and trace the Bitcoins he was using.

"This is one of a handful of cases nationally where cryptocurrency has been used in this way," he said.

"The evidence against Johnson was overwhelming and he had no choice but to admit to his crimes.

"He may not have traded drugs on the street but he knew exactly what he was doing."

A second person connected to the case was also sentenced on Wednesday to two years in prison, suspended for two years.

Lia Johnson, 28, also from Northampton Road, had admitted acquiring and possessing criminal property.

Kaynak: (BBCNEWS, 2020)

Resim 3.3.'de haber görüntüsü verilen, 5 Şubat 2020 tarihli BBC NEWS'in "Leicestershir'da kripto para ile uyuşturucu satan kişi hapse atıldı" başlıklı haberine göre özetle; bir İngiliz vatandaşının ülkesinde uyuşturucu sağlama suçunu kripto para birimi bitcoin ile ödeme yöntemiyle gerçekleştirdiği ve 8 yıl hüküm giydiği ifadeleri paylaşılmaktadır.

Resim 3.4. : Bulgu 4

COINTELEGRAPH
Türkçe

EMRE GÜNEN 04 MAR 2020

Rapor: Kripto Para ile Siber Suçlar Arasında Doğrudan İlişki Var mı?

Intsights ve Ciphertrace, siber suçlarda kripto para birimlerinin kullanımı hakkında detaylı bir rapor hazırladı.

Intsights ve Ciphertrace tarafından hazırlanan güvenlik raporunda, siber suçlar ile Bitcoin ve benzeri kripto para birimleri arasındaki ilişki masaya yatırıldı.

Örgütler, karteller ve siber suçlar üzerine hazırlanan raporda, kara para aklama ve terör finansmanı konuları özelinde Latin Amerika bölgesi mercek altına alındı.

Raporda, gelişmiş ülkelerde karşılaşılan devlet destekli bilgisayar ağı saldırılarının yaygın olmadığı Latin Amerika'da, evden bilgisayar korsanlığı yapan çok sayıda siber suçlu bulunduğu belirtildi.

Latin Amerika'da süregelen siyasi istikrarsızlık ve bu dönemde yaşanan hızlı dijitalleşme süreci siber suçların yaygınlaşmasına açık kapı bıraktı.

Son yıllarda yaşanan ekonomik kriz nedeniyle bilgisayar korsanlığı, dolandırıcılık, kara para aklama, fidye yazılımı ve benzeri siber suçlarda patlama gözlendi.

Raporda, tüm bu siber suç eylemlerinde kripto para birimlerinin aktif biçimde kullanıldığı ifade ediliyor.

P2P platformlarını ve yasa dışı borsaları kullanıyorlar

Kripto para birimleri ile gerçekleşen siber suçların çoğunda, eşler arası (Peer-to-Peer – P2P) platformlar veya düzenlemelere uygun olmayan yasa dışı borsalar tercih ediliyor. "Crypto mixing" ismi verilen kripto para işlemlerini karıştırma yöntemi ile işlemlerin takibi zorlaştırılıyor.

Raporda şu ifadeler yer alıyor:

> **"Organize suç örgütleri, dark web üzerinden siber suçluları kiralıyor ve yüklü meblağlardaki paralarını aklamak için kripto para birimlerini kullanıyorlar. [...] Yasa dışı ve düzenlemelere uygun olmayan borsaları kullanarak izlerini kaybettiriyorlar."**

Transfer işlemlerinin farklı altcoin'ler üzerinden gerçekleştirildiği ve takibinin iyice zorlaştırıldığı da raporda ayrıca belirtildi.

Kripto para birimleri ile ilişkili suçlar

Kripto para birimlerinin suç örgütleri tarafından tercih edilmesinin sebepleri arasında anonim yapıları yer alıyor. Yetkililer, uyuşturucu ve yasa dışı madde satılan çevrim içi pazaryerleriyle ilgili soruşturmalarında kripto para birimlerine daha sık rastlıyorlar.

Ağustos ayında konu hakkında görüş bildiren Birleşmiş Milletler Küresel Siber Suçlar Programı Başkanı Neil Wals, kripto paraların kara para aklamayla mücadeleyi zorlaştırdığını dile getirdi.

Cointelegraph'ın şubat ayında bildirdiği üzere, eski bir Microsoft çalışanı olan Volodymyr Kvashuk, kripto para birimlerini kullanarak zimmetine 10 milyon dolar geçirdiği iddiasıyla, 18 adet federal suçtan suçlu bulunmuştu.

Kaynak: (Cointelegraph, 2020)

Resim 3.5. : Bulgu 5

UZMANCOIN

Interpol'den kripto para takibi için iş birliği

Uluslararası polis teşkilatı Interpol, karanlık ağ üzerinde kripto para işlemlerini izlemek için Güney Koreli bir şirketle iş birliği yapmaya başladı.

Yazar Hakan Ateşler 23 Mart 2020

Uluslararası Kriminal Polis Teşkilatı (Interpol), kripto para işlemleri için "internetin karanlık bölgesi" olarak bilinen Dark Web'de (Karanlık Ağ) yapılan işlemleri takip edebilmek için Güney Koreli veri istihbarat firması S2W Lab ile ortaklık yaptığını duyurdu.

S2W Lab tarafından yapılan açıklamaya göre firma, kripto para kullanımı da dahil olmak üzere karanlık web etkinliğini analiz ve takip etmek için Interpol ile bir yıllık bir sözleşme imzaladı.

Açıklamada, yeterli izleme araçlarının bulunmamasından dolayı karanlık web portallarının, kredi kartı ve pasaport bilgilerinin yasa dışı ticaret de dahil olmak üzere siber suçların bir merkezi olarak ortaya çıktığı belirtildi.

2018'de kurulan girişim, benzersiz, yapay zeka tabanlı bir "çok alanlı analitik motor" kullanarak veri topluyor ve karanlık ağı analiz ediyor. S2W Labs şu anda, birden çok zaman dilimi ve birden çok etki alanı içinde bağlantıları bulan bir veritabanı oluşturma sürecinde.

S2W Labs CEO'su Suh Sangduk ortaklıkla ilgili olarak, "Dark Web'deki siber suçlara karşılık vermek, kripto para birimlerinin geniş kullanımı ve özellikleri nedeniyle çok zor. Uluslararası istihbarat kurumlarıyla teknolojimizi kullanarak iş birliği içinde olacağız ve iyiliğin yararına işler yapacağız" dedi.

Kaynak: (Uzmancoin, 2020)

Resim 3.6. : Bulgu 6

The New York Times

Dark Web Drug Sellers Dodge Police Crackdowns

The notorious Silk Road site was shut down in 2013. Others have followed. But the online trafficking of illegal narcotics hasn't abated.

By Nathaniel Popper

June 11, 2019

SAN FRANCISCO — Authorities in the United States and Europe recently staged a wide-ranging crackdown on online drug markets, taking down Wall Street Market and Valhalla, two of the largest drug markets on the so-called dark web.

Yet the desire to score drugs from the comfort of home and to make money from selling those drugs appears for many to be stronger than the fear of getting arrested.

Despite enforcement actions over the last six years that led to the shutdown of about half a dozen sites — including the most recent two — there are still close to 30 illegal online markets, according to DarknetLive, a news and information site for the dark web.

This week, customers could still score five grams of heroin — "first hand quality no mix" — for 0.021 Bitcoin (roughly $170), or a tenth of a gram of crack cocaine for 0.0017 Bitcoin (roughly $14) on the market known as Berlusconi.

Kaynak: (TheNewYorkTimes, 2019)

Resim 3.6.'da haber görüntüsü bulunan, 11 Haziran 2019 tarihli The New york Times gazetesinin haberine göre; İnternetin anonim işlemler gerçekleştirilebilen tarafı olarak nitelenen dark web portallarında çeşitli suçların kripto paralar kullanılarak gerçekleştirildiği, monero gibi bazı kripto birimlerin daha fazla anonimlik sağladığı için bu benzer faaliyetlerde tercih edildiği ifadeleri paylaşılmaktadır.

3.2. Kripto Paraların Kara Para Aklamada Kullanımına İlişkin Bulgular

Resim 3.7.: Bulgu 7

BitcoinSistemi

Terör Eylemi Ve Kara Para Aklamak İçin Bitcoin Kullananların Hesapları Kolay Tespit Edilebilir Mi?

Finansal Eylem Görev Gücü (FATF), başta kara para aklama ve para aklama olmak üzere, teröristler tarafından kripto paraların bir araç olarak kullanılmasına karşı hamlelerini sürdürüyor.

Murat Yıldırım • 05.03.2020 - 22:26 - Son Güncelleme 05.03.2020 - 22:26

IŞİD, PKK, YPG, PYD ve daha onlarcası... Her bir terör örgütünün ardında gerek devlet desteği, gerek ise dış finansman bulunuyor. Terör örgütleri bugün tüm dünyayı tehdit ediyor. ABD anakarası ve Rusya bu tehditten en az etkilenen ülkeler arasında yer alırken, yine İskandinav ülkeleri ve bazı Avrupa ülkeleri de Ortadoğu ülkelerine oranla tehditlerden daha az etkileniyor.

ABD anakarasının kısmen daha fazla güvende olmasının sebebi olarak ise okyanus ötesi bir konuma sahip olması, terör örgütleri konusunda istihbaratın çok güçlü olması ve olası saldırılar gerçekleşmeden önce Pentagon ve diğer ABD'li yetkililerin durumdan haberdar olması gösteriliyor. Tabii bu terör örgütlerine para ve silah yardımı yapan ülkenin, dolayısıyla "besleyen" ülkenin ABD olmadığını bugün söylemek imkansız. ABD Başkan'ı Donald Trump bile attığı Tweetler ile bunu defalarca kez doğruladı.

Aynı durum Rusya için geçerli olmasa bile, Rusya'nın gerek YPG gibi terör örgütlerini terör örgütü sınıfında barındırmaması ülkenin olası büyük terör örgütlerinin potansiyel saldırıları için yine kısmen güvende olduğunu gösteriyor.

Terör Örgütü Olarak Görülmeyen Örgütü Kim Durduracak?

Finansal Eylem Görev Gücü (FATF) ve diğer kurumlar teröristlerin kripto para birimleri ile başarılı olmasını engellemek için oldukça güçlü çalışıyor. Ancak bugün PKK, YPG gibi terör örgütleri ABD tarafından terör örgütleri listesinde görülmediği için bu örgütlerin kripto paralar yoluyla kendilerini güçlendirmesini diğer hiçbir ülke engelleyebilecek güçte değil.

Bir terör örgütünün başarılı bir şekilde engellenebilmesi için ABD'nin kesin ve eksiksiz tam desteğine ihtiyaç duyuluyor. IŞİD terör örgütünün finansal olarak çökertilmesinde ABD'nin rolünün çok büyük olduğundan söz edilirken, beraberinde kara para ve para aklama konusunda da terör örgütlerinin tespit edilmesi ve eylemlerinin önlenmesi eğer ki ABD tarafından terör örgütü olarak görülüyorsa kolay. Ancak ABD'nin terör örgütü olarak görmediği örgütlerin bu tür finansa eylemlerinin engellenmesi diğer ülkeler için hiç de kolay değil. En azından sınır ötesi olanlar için.

Kaynak: (Bitcoinsistemi, 2020)

Resim 3.8.: Bulgu 8

Ekonomi AA | Haber Giriş: 23.02.2018 - 11:01,Son Güncelleme:23.02.2018 - 11:24

Hürriyet com.tr

Milyarlarca Euro, kripto paralar üzerinden aklanıyor

Uluslararası yasa dışı faaliyetlerin finansmanında her yıl yaklaşık 3,4 ila 4,5 milyar Euro'luk kara paranın kripto para birimleri üzerinden aklandığı tahmin edilirken, Avrupa Polis Teşkilatı (Europol), söz konusu "karanlık trafiği" durdurmanın yollarını arıyor.

Kripto para birimleri içerisinde son dönemde en bilineni Bitcoin olsa da 2017 sonu itibarıyla bin 367 adet kripto para birimi dolaşımda bulunuyor. Söz konusu kripto paraların 7 bin 467'si piyasada işlem görüyor. İşlem gören 7 bin 467 kripto paranın toplam piyasa değerinin 613 milyar dolar olduğu tahmin ediliyor.
Kripto para birimlerinin transfer trafiğinin takibinin oldukça zor olması, özellikle kara para aklama faaliyetleri başta olmak üzere uyuşturucu ve silah ticareti gibi yaşa dışı işlerin finansmanını yürütenlerin ilgisini çekiyor. Kripto para birimleri, diğer bilinen para birimleri gibi herhangi bir merkez bankası tarafından kontrol edilmediği gibi, güvenlik güçlerinin bu para akışını takip edebilmesi de son derece güç...

Europol Direktörü Rob Wainwright, geçen hafta BBC'ye yaptığı değerlendirmede, her yıl yaklaşık 3,4 ila 4,5 milyar Euro'luk kara paranın kripto para birimleri üzerinden aklandığını söylemişti.

Söz konusu rakam, Euro cinsinden telaffuz edilse de her tür para cinsi, kripto para birimleri üzerinden kara para aklama faaliyetleri için kullanılabiliyor.
Europol'ün tahminlerine göre, her yıl Avrupa'daki 113 milyar Euro'luk kara para trafiğinin yaklaşık yüzde 3 ila 4'lük bölümü kripto para birimleri üzerinden aklanıyor.

UYUŞTURUCU KARTELLERİ DE KULLANIYOR

Merkezi Hollanda'da bulunan Europol'dan AA'ya yapılan açıklamada, sanal para birimlerinin, temel özelliklerinin para aklama faaliyetleri açısından cazip bulunması nedeniyle otoritelerin odak noktasında yer aldığı belirtilerek, "Bu paraların, küresel kullanıma elverişli, emniyetli ve geri çevrilemez transferlere izin veriyor olması, özellikle gerçek kimliklerini gizlemek isteyenlere düşük maliyetli, hızlı uluslararası transfer imkan tanıması, bu özelliklerin arasında yer alıyor." denildi.

Açıklamada, son dönemde kripto para birimlerinin kara para aklama faaliyetlerinde giderek daha fazla kullanılmaya başladığı, kripto para birimlerinin artık sadece siber suçlulara özel bir araç olmadığı, bunların sağladığı imkanlardan uyuşturucu kartellerinin de yararlandığı kaydedildi.

Europol, kara para trafiğinin kripto para birimleri üzerinden nasıl yürütüldüğüne ilişkin olarak da, kara paranın, sanal para veya nakit olmak üzere "Money mule" olarak adlandırılan aracı kuryelerin hesapları üzerinden çevriminin yapıldığı, sadece saniyeler içerisinde gerçekleşen bu detaylı "kripto" havale trafiğinin şifrelerini çözmenin ise oldukça zor olduğu vurgulandı.

YENİ TERCİH MONERO

Bu arada, Bitcoin'in giderek küçük yatırımcı tarafından tanınan ve takip edilen bir sanal para birimi halini alması, yasa dışı faaliyetlerde bulunanların alternatif sanal para birimlere yönelmesine neden oluyor. Bu konuda son dönemde en çok öne çıkan kripto para birimi ise Monero...

Ekonomist Adil Salem, konuya ilişkin AA muhabirine yaptığı değerlendirmede, "Monero protokolü, bir noktadan diğer noktaya üst düzeyde kripto işlem yapabilme imkanı tanıyor. Monero, yer altı faaliyetlerinde Bitcoin'e kıyasla şu anda daha çok tercih edilen bir birim." dedi.

Bloomberg International'de geçen ay yer alan haberde, hackerların saldırdıkları web sitelerinin sahiplerinden son dönemde özellikle Monero talep etmeye başladıkları öne sürüldü. Hackerların, 19 Aralık 2017'de, toplam 190 bin WordPress sitesini kilitleyerek site sahiplerinden Monero cinsinden fidye talep ettiği belirtiliyor.

MONERO, DİĞER SANAL PARA BİRİMLERİNE GÖRE DAHA KARMAŞIK BİR SİSTEME SAHİP

Monero, diğer sanal para birimlerine göre daha karmaşık bir sisteme sahip olmasıyla tanınıyor. İlk kez 2014 yılında ortaya çıkan Monero'nun temel özeliği; gönderilerde gönderen ve alıcının, adreslerini şifrelemesinin yanı sıra takibi daha da zorlaştırmak için sahte adresler üretebiliyor olması...
Dünyanın en büyük finans merkezi Londra'da kripto para birimleri konusunda denetim uygulamalarının sıkıştırılması için geçen yılın aralık ayında düğmeye basıldı.

İngiliz polisinden aralık ayında yapılan açıklamada, kripto para birimlerinin yasa dışı faaliyetlerin finansmanı için kullanıldığı belirtildi. Söz konusu açıklama, daha önce para transferlerinin takibinin zor olması nedeniyle iddia niteliğinde kalan "yasa dışı faaliyetlerin finansmanı" meselesinin resmi olarak doğrulanması anlamına geliyor.

İngiltere Başbakanı Theresa May, geçen ay İsviçre'nin Davos kasabasında düzenlenen Dünya Ekonomi Forumu sırasında Bloomberg'e yaptığı açıklamada, artık kripto para birimlerinin kullanım alanlarına daha ciddi yaklaşacağının sinyalini verirken, "Tam olarak kullanım şekillerine, özellikle suçlular tarafından kullanılmalarına ilişkin harekete geçilmesi gerekebilir." ifadesini kullanmıştı.

Ülkenin en büyük bankacılık gruplarından Lloyds, İngiltere Başbakanı May'in açıklamasından bir süre sonra, 5 Şubat'ta yaptığı açıklamada, kredi kartları yoluyla Bitcoin dahil olmak üzere tüm sanal para birimlerinin alımını yasakladığını duyurdu.

Kaynak: (Hürriyet, 2018)

Resim 3.9.: Bulgu 9

BLOCKCHAIN TÜRKİYE

İsviçreli düzenleyici: Blokzinciri kara para aklama riskini artırıyor

11 Aralık 2019

İsviçre'nin finansal düzenleyicilerinden FINMA, blokzinciri teknolojisinin kara para aklama riskleri oluşturabileceğine dair ülkeyi uyarıyor.

Düzenleyici, '2019 Risk Monitor' adlı raporunda, üzerindeki tüm işlemlerin dijital kaydını sağlayan blokzinciri teknolojisinin bankalara verimlilik kazanımları sağlayabileceğini kabul ediyor. Ancak anonimlik ve hız gibi özelliklerin kara para aklayanlara hitap edebileceği konusunda da uyarıyor.

FINMA kara para aklama olaylarının kripto benimsenmesini de yavaşlattığını iddia ediyor. Düzenleyici, blokzinciri teknolojisinin anonimlik potansiyelinin yüksek olduğunu ve bu tür finansal araçların hızı ve küresel niteliğinin onları cezai kullanım için çekici araçlar haline getirdiğine inanıyor. Dolayısıyla blokzinciri konusunda gerek devlet kurumları gerekse bireyler hılı bir şekilde ilerleme kaydedemiyor.

FINMA CEO'su Mark Branson konuyla ilgili olarak: "*Blokzinciri uygulamaları veya ödeme sistemleri hakkında konuşacak olursak, bu sistemin kara para aklama riskleri doğurduğu ve bu tür bir iş modeli için önemli bir risk kategorisi olduğu açıktır. Aynı riskler, aynı yoğunlukta denetlenmeli ve düzenlenmelidir.*" ifadelerini kullanıyor.

KAYNAK Bloomberg

Kaynak: (Blockchain, 2019)

3.3. Kripto Paraların Terörizmin Finansmanında Kullanımına İlişkin Bulgular

Resim 3.10.: Bulgu 10

CNN TÜRK .com

teknoloji haberleri

Mobil Donanım İnceleme İnternet Video

Haberler > Teknoloji Haberleri > Kripto para ile terör finansmanı ve yasa dışı faaliyet

Kripto para ile terör finansmanı ve yasa dışı faaliyet

15.10.2019 - 09:58
Ecevit Bıktım

Dijital paraların kara para aklamak için yoğun olarak kullanıldığını duyuran SEC'e, the Commodity Futures Trading Commission ve the Financial Crimes Enforcement Network de destek verdi.

ABD'deki finansal regulatör kurumların kripto paralara karşı birleşmiş tepkisi, ABD'nin kripto pazarını durdurmak için harekete geçeceği şüphesini doğurdu.

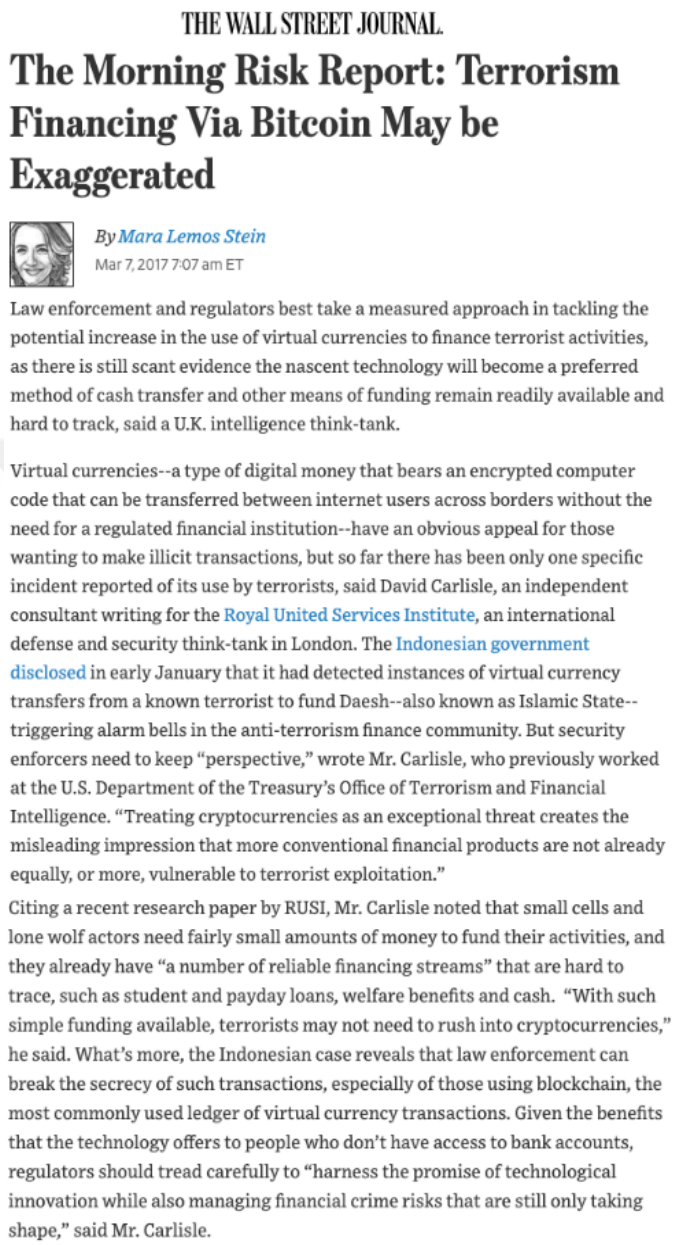
Finansal kuruluşları ve ticari **operasyon** yürüten kurumları uyaran SEC, dijital paralarla yapılan işlemlerin kara para aklama konusundaki şüpheleri yükselttiğini hatırlattı. yasal işlemler yapan şirketlerin **dijital para** gelirlerini belgelemesi gerektiğini de vurguladı.

ABD ayrıca terör finansmanı ve uyuşturucu ticareti konusunda da yükselen kripto pazarını suçluyor. Hatat dev şirketlerin vergi kaçırmak için bile kripto teknolojisini kullandığından şüpheleniyor. Bu suçlamaların şimdi ABD regülatör kurumları tarafından senkronize şekilde dile getirilmesi, pazara önemli sınırlamalar getirilebileceğin işareti kabul ediliyor.

ABD belki de, Ripple gibi kontrollü dijital varlıkların kullanımına izin verirken, Bitcoin gibi izlenmesi imkansız, kontrolsüz varlıkları yasaklama yoluna gidebilir mi? Bu şüphenin gerçekleşip gerçekleşmeyeceğini zaman içinde göreceğiz.

Kaynak: (CNNTÜRK, 2019)

Resim 3.11.: Bulgu 11



THE WALL STREET JOURNAL.

The Morning Risk Report: Terrorism Financing Via Bitcoin May be Exaggerated

By *Mara Lemos Stein*
Mar 7, 2017 7:07 am ET

Law enforcement and regulators best take a measured approach in tackling the potential increase in the use of virtual currencies to finance terrorist activities, as there is still scant evidence the nascent technology will become a preferred method of cash transfer and other means of funding remain readily available and hard to track, said a U.K. intelligence think-tank.

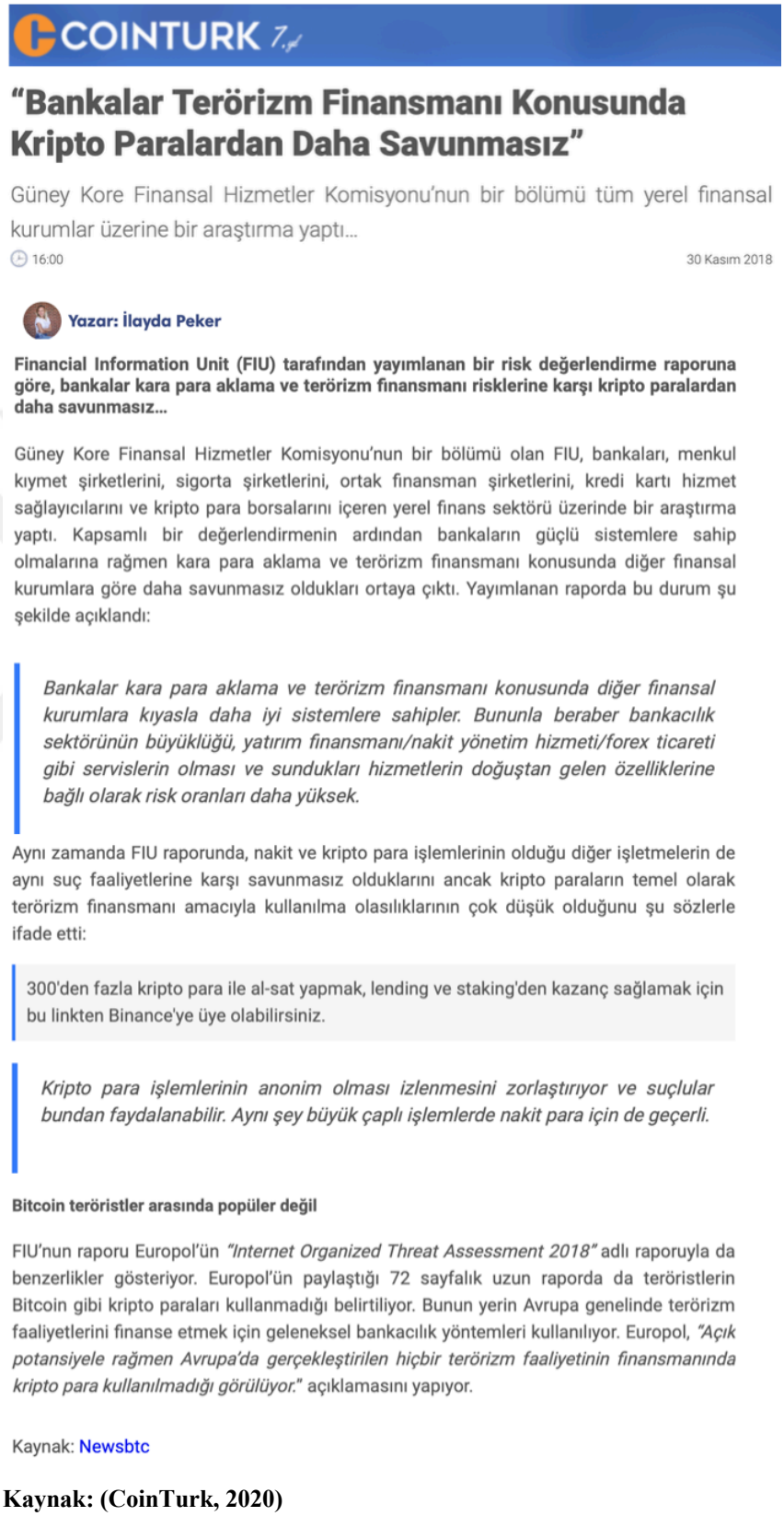
Virtual currencies--a type of digital money that bears an encrypted computer code that can be transferred between internet users across borders without the need for a regulated financial institution--have an obvious appeal for those wanting to make illicit transactions, but so far there has been only one specific incident reported of its use by terrorists, said David Carlisle, an independent consultant writing for the Royal United Services Institute, an international defense and security think-tank in London. The Indonesian government disclosed in early January that it had detected instances of virtual currency transfers from a known terrorist to fund Daesh--also known as Islamic State--triggering alarm bells in the anti-terrorism finance community. But security enforcers need to keep "perspective," wrote Mr. Carlisle, who previously worked at the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence. "Treating cryptocurrencies as an exceptional threat creates the misleading impression that more conventional financial products are not already equally, or more, vulnerable to terrorist exploitation."

Citing a recent research paper by RUSI, Mr. Carlisle noted that small cells and lone wolf actors need fairly small amounts of money to fund their activities, and they already have "a number of reliable financing streams" that are hard to trace, such as student and payday loans, welfare benefits and cash. "With such simple funding available, terrorists may not need to rush into cryptocurrencies," he said. What's more, the Indonesian case reveals that law enforcement can break the secrecy of such transactions, especially of those using blockchain, the most commonly used ledger of virtual currency transactions. Given the benefits that the technology offers to people who don't have access to bank accounts, regulators should tread carefully to "harness the promise of technological innovation while also managing financial crime risks that are still only taking shape," said Mr. Carlisle.

Kaynak: (TheWallStreetJournal, 2017)

Haber içeriğinde, ABD Hazine Bakanlığı, Terörizm ve İstihbarat Dairesine göre; Kripto para birimlerini istisnai bir tehdit olarak ele almak, daha geleneksel finansal ürünlerin zaten eşit derecede veya terörist sömürüye karşı daha savunmasız olmadığı konusunda yanıltıcı bir izlenim yaratıyor. Çünkü teröristlerin kripto para kullanımıyla ilgili yalnızca Endonezya hükümeti tarafından rapor edilen tek bir veri bulunduğu belirtilmektedir.

Resim 3.12.: Bulgu 12



COINTURK

"Bankalar Terörizm Finansmanı Konusunda Kripto Paralardan Daha Savunmasız"

Güney Kore Finansal Hizmetler Komisyonu'nun bir bölümü tüm yerel finansal kurumlar üzerine bir araştırma yaptı...

16:00 30 Kasım 2018

Yazar: İlayda Peker

Financial Information Unit (FIU) tarafından yayımlanan bir risk değerlendirme raporuna göre, bankalar kara para aklama ve terörizm finansmanı risklerine karşı kripto paralardan daha savunmasız...

Güney Kore Finansal Hizmetler Komisyonu'nun bir bölümü olan FIU, bankaları, menkul kıymet şirketlerini, sigorta şirketlerini, ortak finansman şirketlerini, kredi kartı hizmet sağlayıcılarını ve kripto para borsalarını içeren yerel finans sektörü üzerinde bir araştırma yaptı. Kapsamlı bir değerlendirmenin ardından bankaların güçlü sistemlere sahip olmalarına rağmen kara para aklama ve terörizm finansmanı konusunda diğer finansal kurumlara göre daha savunmasız oldukları ortaya çıktı. Yayımlanan raporda bu durum şu şekilde açıklandı:

> *Bankalar kara para aklama ve terörizm finansmanı konusunda diğer finansal kurumlara kıyasla daha iyi sistemlere sahipler. Bununla beraber bankacılık sektörünün büyüklüğü, yatırım finansmanı/nakit yönetim hizmeti/forex ticareti gibi servislerin olması ve sundukları hizmetlerin doğuştan gelen özelliklerine bağlı olarak risk oranları daha yüksek.*

Aynı zamanda FIU raporunda, nakit ve kripto para işlemlerinin olduğu diğer işletmelerin de aynı suç faaliyetlerine karşı savunmasız olduklarını ancak kripto paraların temel olarak terörizm finansmanı amacıyla kullanılma olasılıklarının çok düşük olduğunu şu sözlerle ifade etti:

> 300'den fazla kripto para ile al-sat yapmak, lending ve staking'den kazanç sağlamak için bu linkten Binance'ye üye olabilirsiniz.

> *Kripto para işlemlerinin anonim olması izlenmesini zorlaştırıyor ve suçlular bundan faydalanabilir. Aynı şey büyük çaplı işlemlerde nakit para için de geçerli.*

Bitcoin teröristler arasında popüler değil

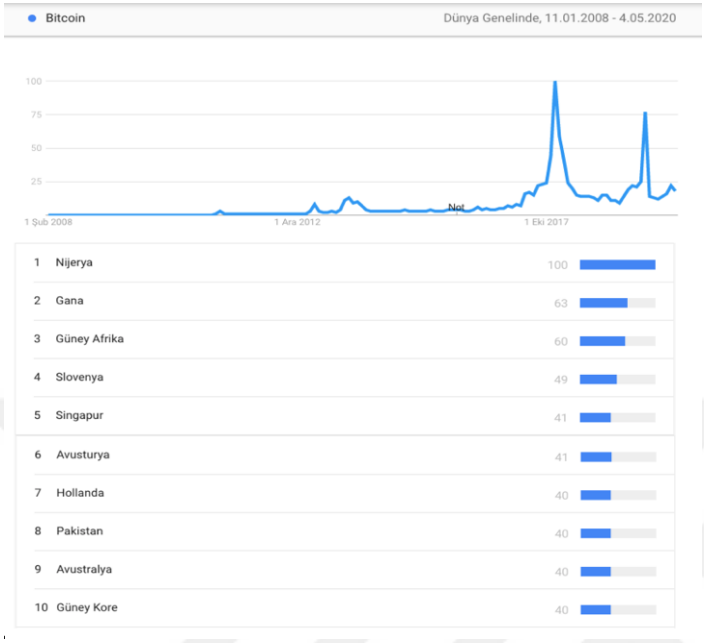
FIU'nun raporu Europol'ün *"Internet Organized Threat Assessment 2018"* adlı raporuyla da benzerlikler gösteriyor. Europol'ün paylaştığı 72 sayfalık uzun raporda da teröristlerin Bitcoin gibi kripto paraları kullanmadığı belirtiliyor. Bunun yerin Avrupa genelinde terörizm faaliyetlerini finanse etmek için geleneksel bankacılık yöntemleri kullanılıyor. Europol, *"Açık potansiyele rağmen Avrupa'da gerçekleştirilen hiçbir terörizm faaliyetinin finansmanında kripto para kullanılmadığı görülüyor."* açıklamasını yapıyor.

Kaynak: Newsbtc

Kaynak: (CoinTurk, 2020)

3.8.4. Diğer Bulgular

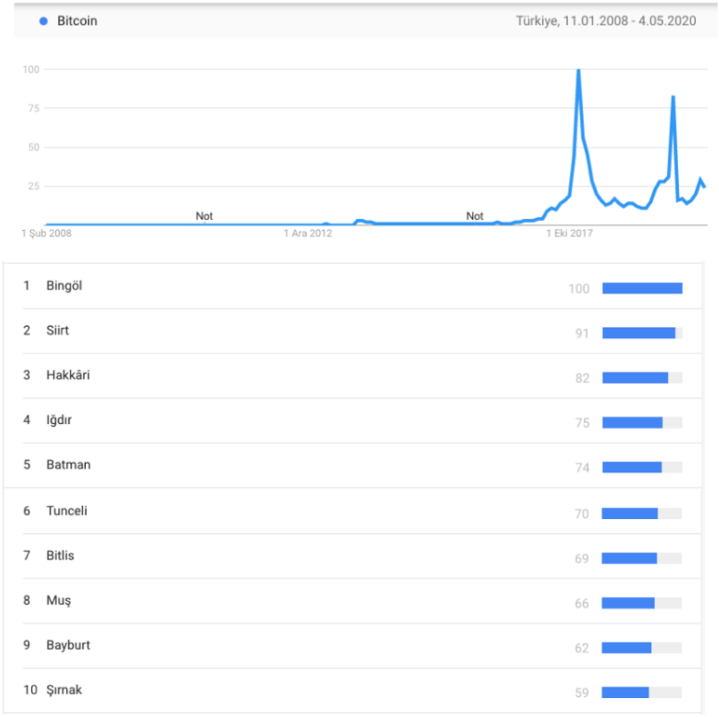
Resim 3.13.: Bulgu 13 (Dünya Genelinde Bitcoin Para birimine olan ilgi)



Kaynak: (GoogleTrends, 2020)

Bulgu 13'te Google Trends'ten elde edilen ve ortaya çıktığı 2008'den günümüze Bitcoin'e dünya ölçeğinde ilgiyi gösteren grafikten anlaşılacağı üzere, gelişmekte olan ülkelerde ilginin daha yüksek olduğu ve özellikle ilk üç sırayı Nijerya, Gana ve Güney Afrika ülkelerinin aldığı görülmektedir. Afrikalı tüketicilere ucuz ve verimli ticaret hizmetleri sunmak isteyen 10'dan fazla Bitcoin Borsası, Afrika Pazarında ortaya çıkmıştır. Afrika'da yeni pazara hizmet etmek ve birçok Afrika ülkesinde Bitcoin talebini gözlemlemek için bir ofis kurmuştur. Bu ilginin arka planında Nijerya'daki, yerel tüccarlar ve aktivistlerin geleneksel para ile başarısız olması ve aynı zamanda bu yeni paranın ekonomiyi demokratikleştirmek için bir fırsat sunduğuna inanması yatmaktadır. %14 enflasyon oranını denetleyen ve dünyanın en yüksek 6. enflasyon oranını yapan Nijerya Merkez Bankası, geçtiğimiz günlerde Bitcoin'i durduramayacaklarını açıklaması da bu ilginin varlığına işaret etmektedir. Gana'daki BTCGhana gibi bazı platformlar, zaman alıcı olan banka hesapları ve kredi kartları ile ilgili karmaşık para çekme ve para yatırma yöntemleriyle uğraşmak zorunda kalmadan Bitcoin alım ve satımı kolaylaştıran ve yerel para transfer noktalarında kolayca nakit çekmelerini sağlayan hizmetler sunmaktadır (Preiss, 2017).

Resim 3.14.: Bulgu 14 (Türkiye'de Bitcoin Para birimine olan ilgi)



Kaynak: (GoogleTrends, 2020)

Bulgu 14'te Google Trends'ten elde edilen ve Bitcoin'e Türkiye ölçeğinde ilgiyi gösteren grafikten anlaşılacağı üzere, ilk 10'da Doğu ve Güneydoğu Anadolu Bölgesi'ndeki iller yer almaktadır. Geçtiğimiz 40 yıl içinde özellikle terör, kaçakçılık gibi suç faaliyetlerinin yüksek olduğu bu illerdeki Bitcoin ilgisi dikkat çekicidir. Özellikle son yıllarda Bitcoin madenciliği için gerekli olan yüksek enerjinin kaçak yollardan temin edilmesi şeklinde çok sayıda yasadışı eylemin basına yansıdığı görülmektedir (Hürriyet, 2017). Buradan anlaşılacağı üzere yerel düzeyde bir enerji hırsızlığı olarak nitelenen bir suçun kripto para madenciliği ile uluslararası bir suça kaynaklık edebilme potansiyeli barındırmaktadır. Öte taraftan bu ilgi her ne kadar kripto para madenciliği olarak görünse de bir suçtan elde edilmesi bakımından, devamında bir aklama eylemini beraberinde getirmektedir. Suçtan elde edilen kripto paraların yasal zemine dahil edilmesinde tam olarak yerleşik bir mevzuat veya düzenleme bulunmaması sebebiyle bu türden eylemlerin net bir verisi bulunmamaktadır. Bu gerekçelerle elde edilen suç geliri kripto paralar yasal veya yasadışı eylemlerde kullanıma açık bir özellik sergilemektedir.

Resim 3.15.: Bulgu 15

euronews.

ALMANYA

Fransa'dan sonra Almanya da sanal paraya karşı savaş açtı

Sertaç Aktan • Son güncelleme: 18/09/2019

Almanya kapsamlı bir blok zinciri stratejisi uygulama kararı alarak özel şirketlerin devletlere ait para birimlerine paralel olarak oluşturdukları ve gelecekte oluşturacakları kripto paralara karşı savaş açtı.

Bu adımın arkasında özelikle Facebook tarafından açıklanan 'libra' kripto para birimi girişimi bulunuyor.

Daha öncekilerden farklı olarak büyük şirketlerin gerçek sermayelerine dayanan ve uluslararası organizasyonlarca denetim altında tutulması planlanan Libra'nın dolar ve euro gibi para birimlerine karşı ciddi bir tehdit oluşturduğu ve devletler tarafından kontrolünün son derece zor olacağı düşünülüyor.

Bitcoin ve diğer kripto paraların zayıf tarafı olan istikrarsızlığı ve volatiliteyi önleme amacıyla oluşturulan Libra'nın bir süre sonra gerçek para birimlerine rakip olması ve güvenlik riskleri doğurması söz konusu.

Blok zinciri teknolojisinin dijital gelecek için gerekli ve yararlı olduğuna inanan Alman hükümeti yetkilileri yeni teknolojilerin yaratabileceği risklere karşı ise şimdiden tedbirler alınması gerektiğini savunuyorlar.

Devletlerin hükümranlığı tehlikede mi?

Alman Finans Bakanı Olaf Scholz yaptığı açıklamada "Ülkemizi teknolojik ilerlemeler alanında lider konumda görmek istiyoruz ve blok zincir de geleceğin kaçınılmaz teknolojilerinden biri ancak aynı zamanda tüketicileri ve devletimizin hükümranlık alanlarını da korumamız gerekiyor" dedi.

Almanya'nın bu alanda uluslararası seviyede işbirliği geliştirmek istediği belirtilirken Alman Merkez Bankası ile de kripto para konusunda atılabilecek adımlara ilişkin yeni çalışmalar başlatıldığı kaydedildi.

Blok zincirli elektronik devlet tahvilleri planı

Buna göre Almanya bu yıl verilecek bir yasa teklifi ile blok zinciri ile işleyen yeni elektronik devlet tahvilleri çıkarmayı planlıyor.

Libra ve benzeri girişimler konusunda Fransa'dan da Berlin'e destek geldi ve Fransız hükümeti de özel şirket destekli kripto paralara Fransa'da ve Avrupa'da müsaade edilmeyeceğini duyurdu.

Sanal Euro oluşturulabilir

Bununla birlikte kıtada devletlerin desteklediği ortak bir kripto para oluşturulması fikrine sıcak bakılıyor. Bu olduğu takdirde Avrupa'da Libra ve benzeri sanal paraların kullanımının tamamen anlamsız hale getirilmesi hedefleniyor.

Kaynak: (Euronews, 2020)

Resim 3.16.: Bulgu 16

Fransa, Facebook'un kripto parası Libra'yı veto etti

AVRUPA 14:41 12.09.2019

Fransa, Facebook'un kripto parası 'Libra'yı hükümetlerin 'parasal egemenliklerini tehdit ettiği' gerekçesiyle engelleyeceğini duyurdu.

Ekonomik Kalkınma ve İşbirliği Örgütü'nün (OECD) sanal para birimleri hakkında düzenlediği konferansta konuşan Fransa Maliye Bakanı Bruno Le Maire, "Tümüyle açık olmak istiyorum: bu koşullar altında Libra'nın Avrupa topraklarında gelişmesine izin veremeyiz" dedi.

"Ülkelerin parasal egemenlikleri, paranın özelleştirilmesi ihtimali nedeniyle tehlikede" diyen Bakan, dünya çapında 2 milyardan fazla kullanıcı olabileceğine dikkat çekti.

DİĞER ÜLKELER TAKİP EDEBİLİR

Libra gibi kripto paralar için daha önce de "Bağımsız bir para birimi olması söz konusu bile değil" diyen Le Maire, G7 ülkelerinin merkez bankası yöneticilerini konuya dair inceleme yapmaya çağırmıştı.

Diğer Avrupa ülkelerinin de Fransa'nın bu tutumunu benimseyebileceği konuşuluyor.

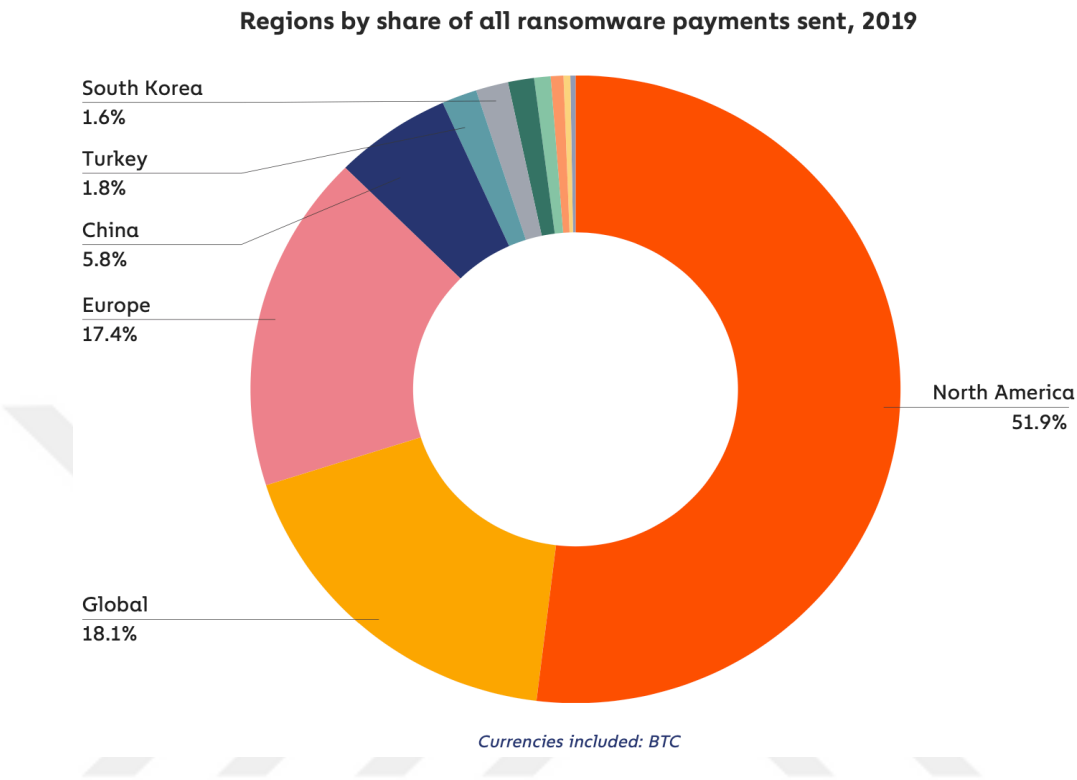
Facebook, kendi kripto para birimi Libra ve dijital cüzdan Calibra'yı 2020 yılında piyasaya sürmeyi planlıyor.

Sosyal medya devinin bu konuda Visa, Mastercard, Uber ve PayPal'in bulunduğu birçok şirketin desteğini aldığı belirtiliyor.

Ancak ABD dahil olmak üzere pek çok hükümet ve devlet bankaları kripto paralara temkinli yaklaşıyor. Yetkililer paranın işleyiş mekanizması konusunda endişelerini dile getiriyor, ayrıca kara para aklama ve terör finansmanında kullanılabileceği uyarısında bulunuyor.

Kaynak: (Sputnik, 2020)

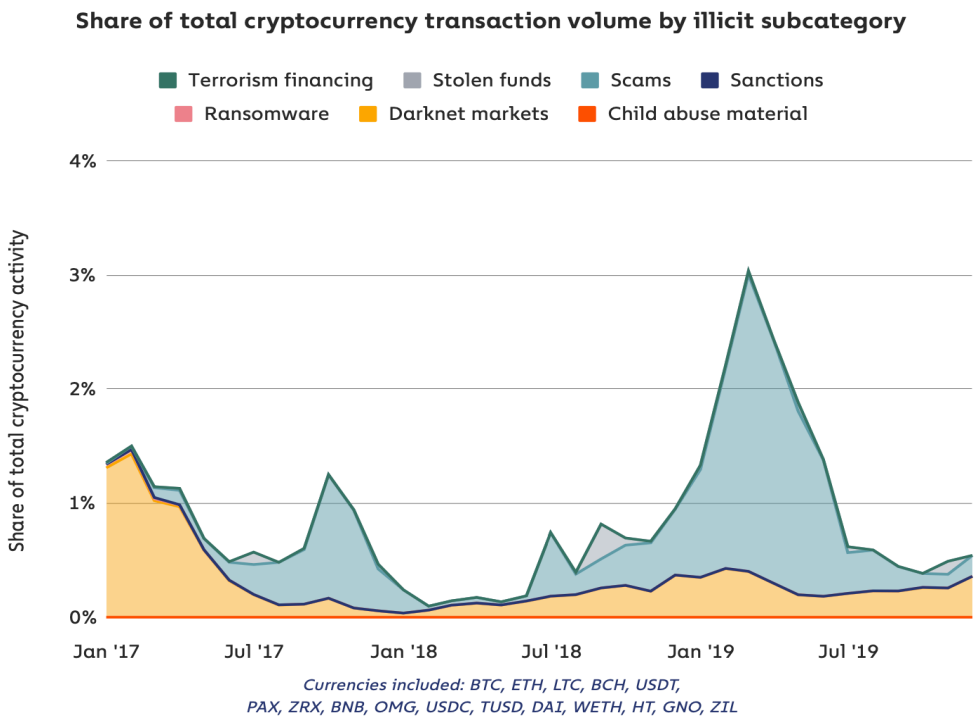
Resim 3.17.: Bulgu 17



Kaynak: (Chainalysis, 2020)

Bulgu 17'de 2020 tarihli Chainalysis Raporu'nda elde edilen Bitcoin'in fidye yazılımlar üzerinden gerçekleştirilen dolandırıcılık eylemlerinde kullanımına ilişkin dünyadaki bölgesel dağılımını gösteren grafikten anlaşılacağı üzere; söz konusu yasadışı fiilin Kuzey Amerika'da %51,9, Avrupa'da %17,4, Cin'de %5,8, Kuzey Kore'de %1,6 oranında dağıldığı görülmektedir. Ayrıca toplam işlenen suçların %1,8'i Türkiye'de, %18,1'i de küresel ölçekte gerçekleşmiştir.

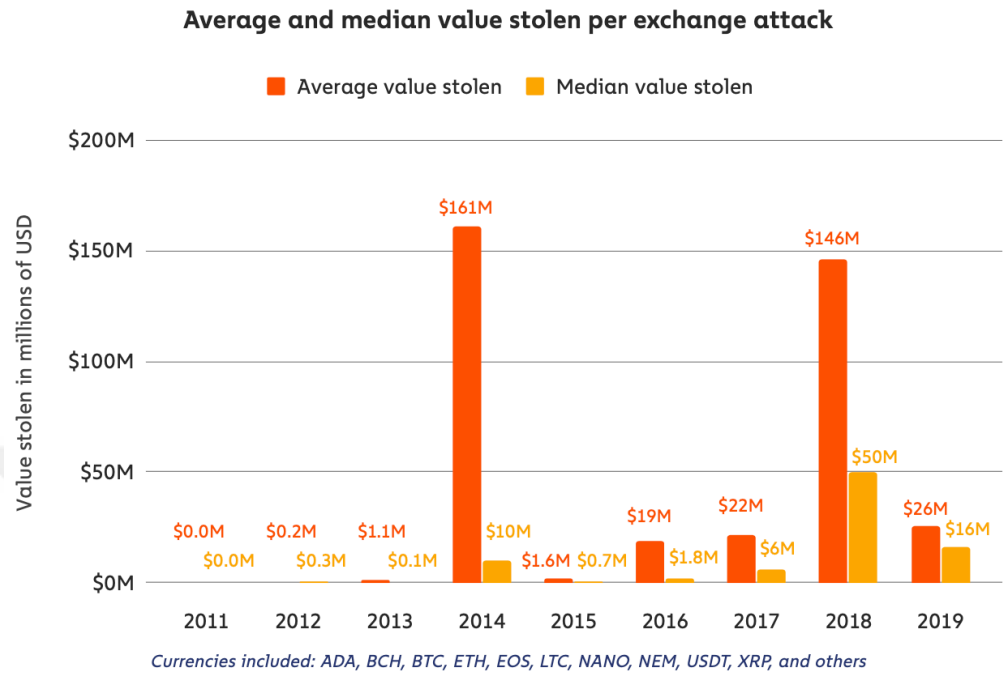
Resim 3.18.: Bulgu 18



Kaynak: (Chainalysis, 2020)

Bulgu 18'de Kripto paraların yasadışı faaliyetlerdeki kullanım alanlarına ilişkin dağılıma bakıldığında, Darknet pazarında en yüksek kullanımın 2017 yılında %1'in üzerinde, çalıntı hesaplarda %1'in altında kaldığı, dolandırıcılık ve terörizmin finansmanında ise en yüksek kullanımın 2019 yılında %3 civarında olduğu görülmektedir. Bu açıdan bakıldığında, yasadışı gelirler içerisinde oldukça düşük bir paya sahip olduğu görülmektedir. Söz konusu suçların gelir elde etme modellerinin klasik ve güvensiz yöntemlerle devam edegeldiği, görece güvenli bir teknoloji olan kripto paralarla suçlar arasında ilişkinin istatistiki olarak zayıf olduğu görülmektedir.

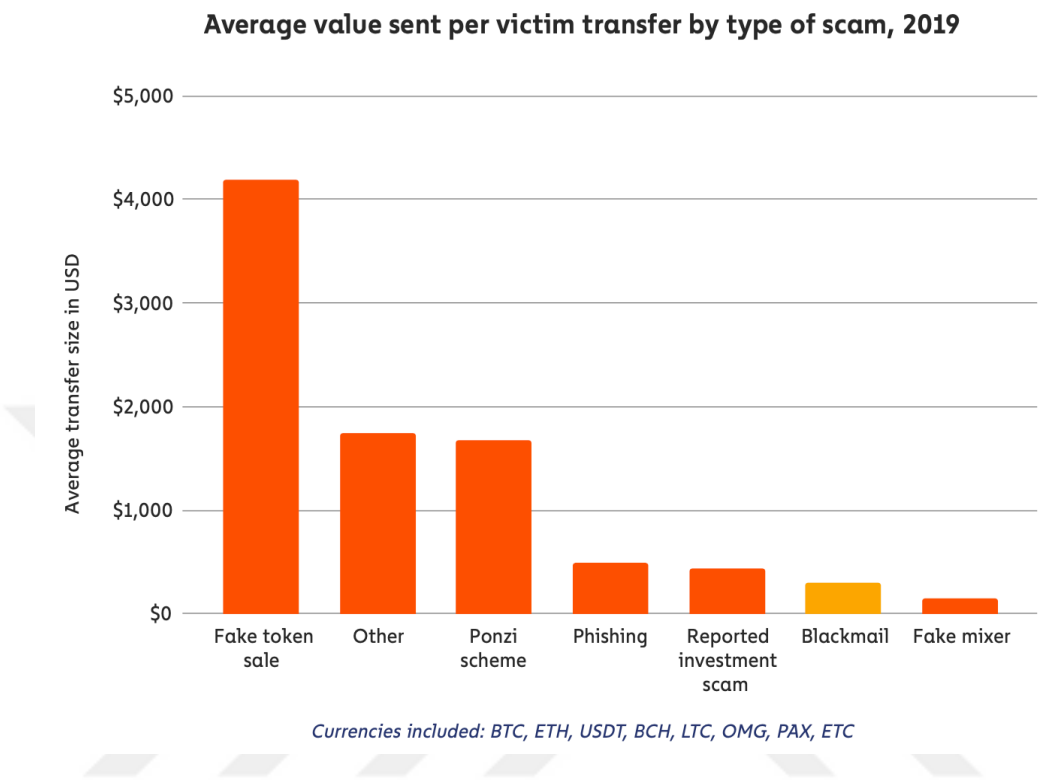
Resim 3.19.: Bulgu 19



Kaynak: (Chainalysis, 2020)

Bulgu 19'da yer alan grafikte yıllara göre kripto paraların çalınmasına ilişkin veriler bulunmaktadur. 2011 yılında rapor edilen vaka bulunmamakla birlikte, 2012 yılında 0.2M $, 2013 yılında 1.1.M $, 2014 yılında 161M $, 2015 yılında 1.6M $, 2016 yılında 19M $, 2017 yılında 22M $, 2018 yılında 146M $ ve 2019 yılında 26M $ tutarında bilişim suçları kapsamında kripto para hırsızlığı gerçekleştirilmiştir. Son 9 yılda en yüksek tutarlı hırsızlık faaliyeti 161M $ ile 2014 yılında kaydedilmiştir.

Resim 3.20.: Bulgu 20



Kaynak: (Chainalysis, 2020)

Bulgu 20'de yüksek piyasa değeri olan sekiz kripto para birimi üzerinden 2019 yılında gerçekleştirilen bilişim suçlarına ilişkin alt suç eylemlerine göre dağılımını gösteren veriler bulunmaktadır. Bu veriler ışığında, sahte para satışından eylem başına ortalama yaklaşık 4.000$, Ponzi zincirleri üzerinden ortalama yaklaşık 1750$, oltalama ile eylem başına yaklaşık 400$, dolandırıcılık fiillerinden işlem başına ortalama yaklaşık 350$, blackmail yöntemi ile eylem başına yaklaşık 250$ tutarında kripto paralar yasadışı suçlara konu olduğu görünmektedir.

Resim 3.21.: Bulgu 21

2019 Exchange attacks quantified

Exchange attacked	Type(s) of cryptocurrency stolen	USD value reportedly stolen (rounded)	Details
CoinBene	109 different types of ERC-20 tokens	$105,000,000	Exchange denied a hack had taken place soon after the attack, but blockchain analysis shows hackers drained funds from CoinBene's hot wallet.
Upbit	ETH	$49,000,000	Hackers removed funds from the exchange hot wallet, though according to the exchange the funds did not belong to users.
Binance	BTC	$40,000,000	Hackers reportedly gained access to the hot wallet using a combination of phishing and viruses, and structured their withdrawal to pass Binance security checks.
BITPoint	BCH, BTC, ETH, LTC, and XRP	$32,000,000	Hackers gained access to the exchange hot wallet.

Kaynak: (Chainalysis, 2020)

Bulgu 21'de yer alan tabloda 2019 yılı içerisinde çeşitili kripto paraların konu olduğu bazı bilişim saldırılarına ilişkin veriler bulummaktadır. Buna göre CoinBane platformuna yapılan saldırıda yaklaşık 105M $, Upbit platformuna yapılan saldırıda Ethereum üzerinden yaklaşık 49M $, Binance'e yapılan saldırıda Bitcoin üzerinden yaklaşık 40M $ ve BitPoint'e gerçekleştirilen saldırıda Bitcoin Csh, Bitcoin, Ethereum, Litcoin, ve Ripple kripto para birimleri cinsinden yaklaşık 32M $ çalınmıştır.

SONUÇ

Blok zincir teknolojisi günümüzde taban alanını hızla genişleten ve köklü değişikliklere kapı aralama kapasitesi ile popüler bir yenilik olarak karşımıza çıkmaktadır. Sağlamış olduğu altyapıyla birlikte özellikle arkaplanındaki felsefe oldukça ilgi uyandırıcı niteliktedir. Merkezi olmayan yapılar, hizmetler ya da fikirler üzerine şekillenen ve birbirine şeffaf, denetlenebilir bir mantıkla kenetlenmiş zincirler olarak ifade edebileceğimiz bu yapı, merkezi bir aygıta ihtiyaç duymamaktadır. Bu özelliği sayesinde günümüze değin geliştirilen teknolojiler bakımından ayrışmakta, son derece iddialı bir imkân sunmaktadır. Bu teknolojinin kullanılması ile geliştirilebilecek ürün ve hizmetlerin üretim ve sunumunda birçok karmaşık süreç, kişi ve kurumun ortadan kalkmasının yanı sıra son derece güvenli ve denetlenilebilir bir şeffaflık sağlaması, yakın gelecekte geniş kitleler tarafından yaygın kabulüne ilişkin bir öngörü sunmaktadır.

Bir paranın en temel özelliklerinden biri de genel kabul görme kabiliyetidir. Günümüzde birçok kripto para birimi merkezi otoritelerin olumsuz algısına rağmen adeta kendi hukukunu yaratarak varlığını kabul ettirmiştir. Yine çoğu ülke ulusal varlığına yönelik büyük riskler atfetse de doğası itibarıyla oldukça popüler olmuşlardır. Küresel çapta yaşanan krizler, çoğu ülke ekonomilerindeki faiz ve enflasyon baskısı, üretim faktörlerine erişimde yaşanan sorunlar, sermayenin dünyada belli bir azınlığın eline hapsolması insanları her zaman daha adil olana erişme arzusundan alıkoyamayacaktır. Bu sebeple daha adil olma iddiası ile ortaya çıkan kripto para sistemleri daha da rağbet görmeye devam edeceklerdir.

Yapılan araştırma ile elde edilen bulgular ışığında, kripto paraların sınıraşan suçlar kapsamında özellikle çeşitli bilişim suçlarına konu olduğu tespit edilmiştir. Bununla birlikte dünyanın çeşitli noktalarında bazı örgütlerinin suç faaliyetlerinden elde ettikleri gelirleri aklayarak finansal sisteme dahil ettikleri vakalara rastlanmıştır. Monero gibi gizlilik seviyeleri yüksek para birimlerinin suç eylemlerinde daha çok tercih edilmesi/edilebilme ihtimali nedeniyle Güney Kore gibi bazı ülkelerde yasaklandığı görülmüştür. Türkiye' kripto paralar ile gerçekleştirilen hırsızlık ve dolandırıcılık gibi suçların gerçekleştirildiği görülmüştür. Darknet üzerinden uyuşturucu satıcılarının çeşitli uyuşturucu maddelerin satışını gerçekleştirdiği ve

ödeme işlemlerini kripto para birimleri üzerinden sağladığı vakalar tespit edilmiştir. Latin Amerika ülkelerinde kripto paraların siber suçlar özelinde aktif biçimde kullanıldığı görülmüştür. Genel olarak işlenen yasadışı fiillerin darknet / dark web / deep web mecralarında anonimlikleri yüksek kripto para birimleri üzerinden gerçekleştirildiği tespit edilmiştir. Kripto paraların piyasa değeri en yüksek olan para birimine olan Bitcoin'e olan ilgi ilk çıkış tarihi 2008 yılından günümüze dünyada Afrika'da (Nijerya, Gana, Güney Afrika gibi) Türkiye'de Doğu ve Güney Doğu Anadolu bölgelerinde yoğunlaştığı sonucuna ulaşılmıştır. Bitcoin cinsinden fidye yazılımlar ile gerçekleştirilen eylemlerin %51,9'u Kuzey Amerika'da gerçekleşirken %1,8'i Türkiye'de gerçekleştiği görülmüştür. Kripto paralar 2017 Haziran 2019 temmuz tarihleri arasında toplam kripto para aktivitesinin %1'lik kısmının da altında bir oranda dolandırıcılık, terörizmin finansmanı, darknet markets, hesap hırsızlığı, fidye ve çocuk istismarı gibi suçlara konu olduğu görülmüştür. 2019 yılında bilişim suçlarında kripto paraların kullanımına ilişkin yöntem en yüksek ortalama tutar ile sahte kripto para satışı yöntemi ile gerçekleşmiştir. Avrupada Almanya Fransa başta olmak üzere Amerika gibi gelişmiş ülkelerde kripto para birimlerini yasal olarak reddetmenin ötesinde yüksek düzeyde bir karalama ve öcüleştirme politikası dikkat çekmektedir. Uluslararası kuruluşlar ve devletlerin kripto para birimlerini yoksayan yaklaşımlarının bu yeniliğe ilgiyi daha da artırdığı görülmüştür. Özellikle bazı kripto para birimlerindeki anonimlik oranının diğer birimlere göre daha yüksek olması ve işlem hareketliliğinin bi takım özellikleri sayesinde kısıtlanabilir olması onları suç örgütleri tarafından daha da çekici hale getirmektedir. Bu nedenle bu tür yasadışı faaliyetlerde bazı para birimleri belirgin olarak ayrışmaktadır. Öte taraftan sanılanın aksine kripto para birimlerinin suç faaliyetlerinde kullanımı söz konusu olmakla birlikte bu tarz faaliyetlerde çok fazla tercih edilmediği gözlemlenmiştir. Ulaşılabilen kaynaklar ışığında Bitcoin ve diğer altcoinleri suç örgütleri tarafından suça konu olacak şekilde kullanım oranının dünya genelinde oldukça düşük oranlarda kaldığı görülmüştür. Bu bağlamda bazı kripto para birimlerinin temel ortak özelliklerine ek bir takım gizlilik özellikleri onları suç faaliyetlerinde, uluslararası yasadışı fon transferlerinde klasik yöntemlere göre daha tercih edilir hale getirmiştir.

Kimi suçların günümüzde artık sınırlar içine hapsolamayacağı şüphe götürmez bir gerçektir. Suç örgütleri sanal mecradaki uzantılar sayesinde faaliyetlerini

küresel boyutlara taşıyabilmektedir. Bu sebeple onlarla mücadele eden hükümetlerin uygulamalarında daha yoğun bir uluslararası iş birliğine ve ortak çalışma anlayışına ihtiyaç olduğu görülmektedir.

Henüz yeni şekillenen, ya da son kullanıcıya yeni hitap eden bazı teknolojik yenilikler toplumun tüm kesimleri tarafından aynı oranda anlaşılamamakta bu durum da bazı olumsuzluklara sebep olmaktadır. Özellikle teknolojik yeniliklerin ne olup ne olmadığına dair temel bir farkındalık düzeyinin yakalanması, teknolojik bir yeniliğin fırsatlarının ve tehditlerinin kavranmasıyla mümkün olmaktadır. Bu bağlamda temel eğitim seviyesinde Teknoloji okur-yazarlığı eğitiminin teşvik edilerek hayata geçirilmesi son derece önem arz etmektedir. Öte taraftan sivil toplum kuruluşlarının halihazırda benzer eğitim, öğretim ve uygulama faaliyetleri son derece isabetli ve toplam faydaya etki eden çok önemli bir diğer inisiyatiftir. Türkiye toplumunun üretken, meraklı, teknolojik gelişmelere uyumu yüksek olması bu ihtiyacı daha da iştahlandırmaktadır. Başlı başına ayrı bir sorun olan ve sınırlara sığmayan terörizm uluslararası seyre yön verme konusundaki kararlılığını halen sürdürmektedir. Terörizmin finansmanı konusunda kripto paraların bu amaç için kullanılması çeşitli örgütlerce bir yöntem olarak tercih edilmektedir. Bununla birlikte birçok suç örgütünün yine birçok devletin çıkar devşirdiği bir enstrüman haline geldiği görülmektedir. Burada terör örgütlerinin kripto paralar ile kaynak transfer etmelerinden ziyade; neredeyse tamamı bir küresel gücün amacına hizmet eden söz konusu suç örgütlerinin gelinen zaman mekân ölçeğinde varlığının neden hala devam ettiği hususu başkaca birçok çalışmaya ilham vermelidir. Başka bir değişle terörizmin hala ortak bir tanımının yapılamamış olması bu örgütlerin amacına dolaylı olarak hizmet etmektedir.

Gerek Blok zincir teknolojisi gerekse kripto para birimleri olgusuna dair merkezi otoritelerin ve karar vericilerin-kurumların teknik adaptasyon sağlama ve hukuki önlemler geliştirmesi bakımından oldukça yetersiz ve yavaş kaldıkları gözlemlenmiştir. Bu sebepten hareketle her ne kadar kripto paraların çeşitli yasadışı eylemlere konu olması oranı oldukça düşük gibi görünse de bunun nedeninin merkezi kaynaklı verilere henüz ya da hiçbir zaman yansımamış-yansımayacak olmasından kaynaklanmaktadır. Diğer bir ifade ile suç örgütleri bu teknolojileri merkezi otoritelerin gözü önünde ve onların haberi olmaksızın geliştirip kullanabilmektedir.

Zira yasaların uyumlu hale getirilmesi uzun süreler almakta, teknik personelin yetiştirilmesi ve tutundurulmasının önündeki zaman ve maddi kaynak engelleri çoğu zaman baskın gelmektedir. Bir diğer ifadeyle merkezi otoriteler genellikle, yasadışı bir girişime yönelik refleks geliştirdiğinde çoktan o eylemin yerini daha güncel bir versiyon almış olmaktadır. Bu bağlamda proaktif yöntemlerin geliştirilmesi, hukuki nitelikli uyum süreçlerinin hızlandırılması ve teknik kapasitenin artırılması hayati önem arz etmektedir.

KAYNAKÇA

Akbulut, B. (1999). *Türk Ceza Hukukunda Bilişim Suçları*. (Yayımlanmamış Doktora Tezi), Selçuk Üniversitesi/Sosyal Bilimler Enstitüsü, Konya.

Akın, E. (2009). *Terör ve Terörizmin Finansmanı Suçu*. Ankara: Adalet Yayınevi.

Aksoy, M. (2018). *Kripto Para Birimleri ile Kara Para Aklama ve Terörizmin Finansman Riskinin Fatf Tavsiyeleri Çerçevesinde İncelenmesi*. İstanbul Ticaret Üniversitesi/ Finans Enstitüsü, İstanbul.

Alizade, R. (2015). Ermeni Terör Faaliyetlerine Dair. *Akademik Tarih ve Düşünce Dergisi, 2* (5), 107 -123.

Alkan, N. (2002). *Gençlik ve Terörizm*. Ankara: Temüh Yayınları.

Altıner H. ve Şaykol E. (2013). Veri Güvenliğinde Tempest Saldırı Türleri Üzerine Tarihsel Bir İnceleme. *Beykent Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi, 6*(2), 121-152.

Akıncı H., Alıç A.E ve Er C. (2004). *Türk Ceza Kanunu ve Bilişim Suçları, İnternet ve Hukuk*. İstanbul Bilgi Üniversitesi Yayınları.

Altuğ, Y. (1995). *Terörün Anatomisi*. İstanbul: Altın Kitaplar.

Altuğ, O. (2001). *Kayıtdışı Ekonomi*. Ankara: Türkmen.

Altunok, T. ve Çakmak H. (2009). *Terörizmin Yasal Olmayan Finans Kaynakları: Terörizmin Finansmanı ve Ekonomisi.* Ankara: Barış Platin Kitabevi.

Aren, S. (2007). *100 Soruda Para Ve Para Politikası.* Ankara: İmge.

Arıkan, R. (2007). *Araştırma Teknikleri ve Rapor Hazırlama*. Ankara: Asil

Aslan, A. (2018). *Kripto Para Olgusu Ve Blockchain Teknolojisi: Ekonomik Aktörlerin Tepkisi, Maliyet Analizi, VAR Modeli Ve Granger Nedensellik Testi*. (Yayımlanmamış Yüksek Lisans Tezi). Hacettepe Üniversitesi/Sosyal Bilimler Enstitüsü, Ankara.

Arslan, C. (2019, 14 Aralık). Kara para aklama kuralları, bitcoin ödeme platformunun sonunu getirdi. *Uzmancoin*. Erişim adresi: https://www.uzmancoin.com

Ateş, B. (2016). Kripto Para Birimleri, Bitcoin ve Muhasebesi. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,7* (1), 349- 366.

Atıcı, B. ve Gümüş Ç. (2003), Sanal Ortamda Gerçek Tehditler: Siber Terör. *Polis Dergisi*, 37, 57-66.

Avunduk, H. ve Aşçan, H. (2018). Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme, *Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *1*(33), 369-384.

Aydın, A. (1992). *Kürtler, PKK ve Abdullah Öcalan*. Ankara: Kitap Yayın Dağıtım.

Aydın, E.D. (1992). *Bilişim Suçları ve Hukukuna Giriş*, Ankara: Doruk Yayınları.

Aydın, N. (2009). *Küresel Terör ve Terörizm*. İstanbul: Kum Saati Yayınları.

Aydınalp, H. (2011). *İntihar Eylemleri Ekseninde Din ve Terör*. Ankara: Birleşik Dağıtım Kitabevi.

Aykın, H. ve Gümüşay, K. (2008). Terörle Mücadelede Yeni Boyut: Terörün Finansmanı ile Mücadele. S. Aydın (Ed.). *Karapara Aklama ve Terörizmin Finansmanı* içinde (ss. 341–346). Ankara: Adalet Yayınevi.

Aykın, H. ve Sözmen, H. K. (2008). *Terörizmin Finansmanı*. Ankara, MASAK Yayını.

Bains, T. (2015). "Bitcoin Digital Currency: A Portend for India's National Security", *CLAWS Journal.* Erişim Adresi: https://archive.claws.in/images/journals_doc/1620376481_BitcoinDigitalCurrency.pdf

Bal, M.A. (2003). *Savaş Stratejilerinde Terör*. İstanbul: IQ Kültür-Sanat Yayıncılık.

Bal, İ. (2006). *Alacakaranlıkta Terörle Mücadele ve Komplo Teorileri*. Ankara: USAK Yayınları.

Balduzzi, M. ve Ciancaglini, V. (2015). Cybercrime in the Deep Web. *Trend Micro*. Erişim Adresi: https://www.blackhat.com/docs/eu-15/materials/eu-15-Balduzzi-Cybercrmine-InThe-Deep-Web-wp.pdf

Baltacı, O. Y. (2004). *Küreselleşme ve Örgütlü Suçlar*. (Yayımlanmamış Yüksek Lisans Tezi), Kırıkkale Üniversitesi/Sosyal Bilimler Enstitüsü, Kırıkkale.

Baran, P. (1964). On Distributed Communications Networks. *IEEE Transactions on Communications Systems, 12*, (1), pp. 1-9.

Bashir, I. (2017). *Mastering Blokchain*. Birmingham: Packt Publishing.

Bayraktar K. (2000). *Banka Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları*. İstanbul: Beta Yayınevi.

Baath, D. ve Zellhorne, F. (2016). How to combat money laundering in Bitcoin? An institutional and game theoretic approach to anti-money laundering prevention measures aimed at Bitcoin. *Semantic Scholar.* https://www.semanticscholar.org/paper/How-to-combat-money-laundering-in-BitcoinAn-and-to-B%C3%A5%C3%A5th-Zellhorn/90366e86feeaaf57a5ad6c890aa7ee8b08b10a08#citing-papers

Berber, M. ve Bocutoğlu, E. (2014). *Genel İktisada Giriş*. Bursa: Ekin Yayınları.

BDDK, (2018). Bitcoin 6493 sayılı Kanun kapsamında olan elektronik para mıdır? *bddk.org.tr.* Erişim Adresi: https://www.bddk.org.tr/Sss-Kategori/Odeme-Sistemleri-ve-Elektronik-Para-Kuruluslari/3

Bilek, B. T. (2012). *Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri.* (Yayımlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi/Bilişim Enstitüsü, Ankara.

Bilgiç, M. Sadi (2014). PKK/KCK'nın Stratejisi Taktikleri ve Taktik Düzeyde Etnik Terörle Mücadele. *Bilge Strateji Dergisi, 6*(10), 85-114.

Biswas, R. (2018). *Emerging Markets Megatrends*. London: Palgrave Macmillan.

Bozkurt Yüksel, A. B. (2015). "Elektronik Para, Sanal Para, Bitcoin Ve Linden Doları'na Hukuki Bir Bakış", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 73(2): 173-220.

Brookings (2017, 15 December). Figures of week: Blockchain oppurtunities and challenges in Africa. *Brookings.edu.* Erişim adresi: https://www.brookings.edu/blog/africa-in-focus/2017/12/15/figures-of-the-week-blockchain-opportunities-and-challenges-in-africa/

Bulgu 1 (2020, 21 Mayıs) Erişim Adresi: https://uzmancoin.com/monero-kripto-para-huobi/

Bulgu 2 (2020, 21 Mayıs) Erişim Adresi: https://www.webtekno.com/13-milyon-tl-degerinde-kripto-para-calan-zanlilar-otomobil-satisinda-yakayi-ele-verdi-h63046.html

Bulgu 3 (2020, 21 Mayıs) Erişim Adresi: https://www.bbc.com/news/uk-englandleicestershire51393208?intlink_from_url=https://www.bbc.com/news/topics/cyd7z4rvdm3t/cryptocurrency&link_location=live-reporting-story

Bulgu 4 (2020, 21 Mayıs) Erişim Adresi: https://tr.cointelegraph.com/news/is-there-a-relationship-between-cryptocurrency-and-cyber-crime-new-report-says-yes

Bulgu 5 (2020, 21 Mayıs) Erişim Adresi: https://uzmancoin.com/kripto-para-interpol/

Bulgu 6 (2020, 21 Mayıs) Erişim Adresi: https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html

Bulgu 7 (2020, 21 Mayıs) Erişim Adresi: https://www.bitcoinsistemi.com/teror-eylemi-ve-kara-para-aklamak-icin-bitcoin-kullananlarin-hesaplari-kolay-tespit-edilebilir-mi/

Bulgu 8 (2020, 21 Mayıs) Erişim Adresi: http://bigpara.hurriyet.com.tr/haberler/bitcoin-haberleri/milyarlarca-euro-kripto-paralar-uzerinden-aklaniyor_ID1444232/

Bulgu 9 (2020, 21 Mayıs) Erişim Adresi: https://bctr.org/isvicreli-duzenleyici-blokzinciri-kara-para-aklama-riskini-artiriyor-12859/

Bulgu 10 (2020, 21 Mayıs) Erişim Adresi: https://www.cnnturk.com/teknoloji/kripto-para-ile-teror-finansmani-ve-yasa-disi-faaliyet

Bulgu 11 (2020, 21 Mayıs) Erişim Adresi: https://blogs.wsj.com/riskandcompliance/2017/03/07/the-morning-risk-report-terrorism-financing-via-bitcoin-may-be-exaggerated/

Bulgu 12 (2020, 10 Haziran) Erişim Adresi: https://coin-turk.com/bankalar-terorizm-finansmani-konusun da-kripto-paralardan-daha-savunmasiz

Bulgu 13 Türkiye Genelinde Bitcoin Para birimine olan ilgi, (2020, 3 Mayıs), Erişim Adresi: https://trends.google.com/trends/explore?date=2008-01-11%202020-05-04&geo=TR&q=%2Fm%2F05p0rrx

Bulgu 14 Dünya Genelinde Bitcoin Para birimine olan ilgi ((2020 3 mayıs) Erişim Adresi: https://trends.google.com/trends/explore?date=2008-01-11%202020-05-04&q=%2Fm%2F05p0rrx

Bulgu 15 (2020, 21 Mayıs) Erişim Adresi: https://tr.euronews.com/2019/09/18/fransa-dan-sonra-almanya-da-sanal-paraya-karsi-savas-acti-libra-blokchain

Bulgu 16 (2020, 29 Mayıs) Erişim Adresi: https://tr.sputniknews.com/avrupa/201909121040154379-fransa-facebookun-kripto-parasi-librayi-veto-etti/

Bulgu 17, 18, 19, 20, 21 (2020, January) Chainalysis. (2020). The 2020 State of Crypto Crime: Everything you need to know about darknet markets, exchange hacks, money laundering and more. Erişim Adresi: https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

Carlisle, D. (2017). *Virtual Currencies and Financial Crime Challenges and Opportunities.* United Kingdom: Royal United Services Institute for Defence and Security Studies.

Canak, E. (2005) *Suç İşlemek Amacıyla Örgüt Kurma ve Çıkar Amaçlı Örgütlenme Suçları.* İstanbul: Vedat Kitapçılık.

Campbell-Verduyn, M. (2018). Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance. Crime, *Law and Social Change, 69*(2), 283-305.

Caşın, M. H. (2008). *Uluslararası Terörizm*. Ankara: Nobel Yayın.

Ceylan, A. K. (2012). *Terör: Hiç Konuşmayanlar Konuşuyor Mücadele Edenlerin Dilinden.* İstanbul: Yeni Yüzyıl Yayınları.

Ceylan, M. E. (2019) *Bitcoin Ekonomisi: Kripto Para Bitcoin'in Finans Sektörü İçindeki Yeri*. (Yayımlanmamış Yüksek Lisans Tezi), Batman Üniversitesi/Sosyal Bilimler Enstitüsü, Batman.

Chandna, V. (2017). *The Curious Case of Black and White Money: Exposing the Dirty Game of Money Laundering.* Chennai: Nation Press.

Ciaian, P. ve Rajcaniova, M. (2016). The digital agenda of virtual currencies: Can BitCoin become a global currency?. *Information Systems and e-Business Management, 14*(4), 883-919.

Clohessy, T., Acton, T. ve Rogers, N. (2019). Blockchain Adoption: Technological, Organisational and Environmental Considerations. Treiblmaier, H. ve Beck, R. (Ed.) *Business Transformation through Blockchain Volume I* içinde 47-76. E- kitap: Palgrave MacMillan.

Çakmak, H. ve Kurum, M. (2008). Terörizmin Finansman Boyutu ve Terörizmle Mücadeledeki Yeri. Çakmak, H. ve Altunok, T. (Ed.) *Terörizmin Finansmanı ve Ekonomisi* içinde (7-50). Ankara: Barış Platin Kitap.

Çakmak H. ve Ünsal Z. (2009) Terörizmin Yasal Finans Kaynakları. Çakmak, H. ve Altunok, T. (Ed.) *Terörizmin Finansmanı ve Ekonomisi* içinde. Ankara: Barış Platin Kitap.

Çarkacıoğlu, A. (2016). Kripto-Para Bitcoin. Ankara: Sermaye Piyasası Kurulu Araştırma Dairesi Araştırma Raporu. Sermaye Piyasası Kurulu web sitesinden 14.12.2019 tarihinde erişildi: http://spk.gov.tr/yayingoster.aspx?yid=1130&ct=f&action=down-loadfile.

Çarkacıoğlu, A. (2016). Kripto- Para Bitcoin. *Sermaye Piyasası Kurulu Araştırma Raporu*. Aralık.

Çetinkaya, Ş. (2018). Kripto Paraların Gelişimi ve Para Piyasasındaki Yerinin Swot Analizi ile İncelenmesi. *Uluslararası Ekonomi ve Siyaset Bilimleri Akademik Araştırmalar Dergisi, 2*(5), 11-21.

Dandin, A. N. (2019) *Risk Toplumunda Bilişim Suçları ve Hukukun Etkinliği*. (Yayımlanmamış Yüksek Lisans Tezi). Afyon Kocatepe Üniversitesi/Sosyal Bilimler Enstitüsü , Afyonkarahisar.

Değirmenci, O. (2013). Çeşitli Görünümleriyle Uluslararası Suç Kavramı: Dar ve Geniş Anlamda Uluslararası Suçlar ve Türk Hukuku, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, *71*(1) , 229-266.

Demir, Ö. (2002). İnternet Servis Sağlayıcısının Hukuki Sorumluluğu. *Uluslararası İnternet Hukuku Sempozyumu*, 21-22 Mayıs, İzmir.

Demirtaş, İ. (2015). *6415 Sayılı Terörizmin Finansmanının Önlenmesi*

Hakkında Kanunda Gösterilen Terörizmin Finansmani Suçu. (Yayımlanmamış Yüksek Lisans Tezi). T.C. Kara Harp Okulu /Savunma Bilimleri Enstitüsü, Ankara.

Dilmaç, S. (2004). Global Tehdit: Terörizm ve Türkiye'ye Etkisi. *Polis Dergisi, 10* (40), 357-367.

Dilmaç, S. (2011). *Terörizmde Tanım Sorunu ve Yaklaşımlar*. (Yayımlanmış Doktora Tezi). Polis Akademisi/Güvenlik Bilimleri Enstitüsü, Ankara.

Dini, L. (2005). The Problem and its Diverse Dimensions. E. U. Savona (Ed.). *Responding to Money Laundering International Perspectives* içinde (pp. 3-8). University of Trento Italy: Harwood Academic Publishers.

Dönmezer, S. (1989). Yeni Türk Kanunu Öntasarısı. Akıncı, F. S. ve diğerleri (Ed.). *Ceza Hukuku El Kitabı* içinde, İstanbul: Beta.

Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* Frankfurt: Apress.

Dulupçu, M. A., Yiğit, M. ve Genç, A. G. (2017). Dijital Ekonominin Yükselen Yüzü: Bitcoin'in Değeri İle Bilinirliği Arasındaki İlişkinin Analizi. *Suleyman Demirel University Journal of Faculty of Economics & Administrative Sciences*, 22, 2241-2258.

Durdu, E. (2018). *Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku*. (Yayımlanmamış Yüksek Lisans Tezi). Galatasaray Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.

Dursun, H. (2008). Bankacılık Yoluyla Kara Para Aklanılması ve Alınması Gereken Karşı Önlemler. *Kamu-İş Dergisi, 10* (2).

Duyne, P. C, Harvey, J. H. ve Gelemerova, L. Y. (2018). *The Critical Handbook of Money Laundering: Policy, Analysis and Myths.* London: Palgrave McMillan.

Ercan, F. (2015). *Para ve Kapitalizm*. İstanbul: Devin Yayınları.

Ergil, D. (1991). Terörizmin Mantığı ve Hedefi. *Ankara Üniversitesi SBF Dergisi, 46*(1), 171-181.

Ergül, E. (2001). *Karapara Endüstrisi ve Aklama Suçu*. Ankara: Yargı Yayınevi.

Fığlalı, E. R. (1998). Din – Laiklik ve İstismarı. *Emniyet Genel Müdürlüğü Polis Dergisi, 17*, 68-87.

Fırat, A. (2019, 20 Aralık). Uluslararası Göçmen Kaçakçılığı ve İnsan Ticareti. www.taa.gov.tr/dersnotlari/GocmenKacakciligiveInsanTicareti.doc.

Freedman, M. (2005, October 16). The Invisible Bankers. *Forbes.* https://www.forbes.com/forbes/2005/1017/094/#11b090c2ed20

Glaser, F. (2017). Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabledsystem and Use Case Analysis. 50th Hawaii International Conference on System Sciences (HICSS 2017), 1-14.

Gediz Oral, B, Gökbunar, A. (2017). Karapara Aklamanın (Politik) Araçları: Yolsuzluk, Organize Suç ve Mücadelede Mali Önlemler. *Yönetim ve Ekonomi: Celal Bayar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 24* (1), 89-114.

Gupta, V. (2017,28 Şubat). A Brief History of Blockchain. *Brighton: Harvard Business School Publishing*. https://hbr.org/2017/02/a-brief-history-of-

blockchain

Gönen, S., Ulus, H.İ. ve Yılmaz, E.N. (2016). Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, *Bilişim Teknolojileri Dergisi*, *9*(3), 229-0.

Gül, İ.ve Yılmaz, S. (2017). Fethullahçı Terör Örgütü (FETÖ) ile Mücadele. *TURAN-SAM Uluslararası Bilimsel Hakemli Dergisi, 9*(35), 37-44.

Gül, T. (2012). *Terör ve Terörizm*. İstanbul: Ark Kitapları.

Gültekin, B. (2019). *Blok Zinciri Tabanli Elektronik Seçim Sistemi Tasarımı ve Kısmi Uygulaması.* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Teknik Üniversitesi/Bilişim Enstitüsü, İstanbul.

Gültekin, Y, Bulut, Y. (2016). Bitcoin Ekonomisi: Bitcoin Eko-Sisteminden Doğan Yeni Sektörler Ve Analizi. Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 3 (3), 82-92.

Günal, M. (2012). *Para ve Finansal Sistem*. Ankara: Berikan Yayınevi.

Güngör, S. (2001). Althusser'de İdeoloji Kavramı. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 6*(2), 221-231.

Gürbüz, S. ve Şahin, F. (2017). *Sosyal Bilimlerde Araştırma Yöntemleri: Felsefe- Yötem- Analiz*. Ankara: Seçkin.

Halpin, H. ve Piekarska, M. (2017). Introduction to Security and Privacy on the Blockchain, *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1–3.

Harm, J., Obregon, J., ve Stubbendick, ve J. (July 31, 2017). Ethereum vs. Bitcoin. *The Economist.* (Erişim Tarihi: 15.02.2020)

https://www.economist.com/sites/default/files/creighton_university_kraken_case_study.pdf

Harp Araç ve Gereçleri ile Silah, Mühimmat Ve Patlayıcı Madde Üreten Sanayi Kuruluşlarının Denetimi Hakkında Yönetmelik. (2007, 6 Mayıs). *Resmi Gazete* (Sayı:26514). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2007/05/20070506-1.htm

Hawlitschek, F., Notheisen, B., Teubner, T. (2018). The Limits Of Trust-Free Systems: A Literature Review On Blockchain Technology And Trust İn The Sharing Economy, *Electronic Commerce Research and Applications 29*, 50-63.

Houben, R. ve Snyers, A. (2018). Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Parliment. Erişim adresi : https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Hürriyet (2017, 26 Aralık). Bir evde fabrika kadar elektrik tüketildiği anlaşılınca... Diyarbakır'da Bitcoin operasyonu!. *Hürriyet*. Erişim adresi: https://www.hurriyet.com.tr/gundem/bir-evde-fabrika-kadar-elektrik-tuketildigi-anlasilinca-diyarbakirda-bitcoin-operasyonu-40690551

IMF. (2016). Virtual Curriencies and Beyond: InitiaI Consideration. *IMF Staff Dicussion Note,* 3. Erişim adresi: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

INCSR. (2015). Money Laundering and Financial Crimes Country Database. *United States Department of State Bureau for International Narcotics and Law Enforcement Affairs*, Volume II. Erişim adresi: http://iffoadatabase.trustafrica.org/iff/Money%20Laundering%20and.pdf

İpek, H. (2000). *Önemli Bir Sorun: Kara Para ve Kara Paranın Aklanması*. İstanbul: Beta Yayınları.

Kağıt Paranın Tarihçesi.. Erişim adresi: https://www.tcmb.gov.tr/wps/wcm/connect/d189b219-fe71-40bf-9754 6a5f7d0a65eb /KagitParaTarihce.pdf?MOD=AJPERES

Karaköse, İ.S. (2017). *Elektronik Ödemelerde Blok Zinciri Sistematiği ve Uygulamaları*. (Yayımlanmamış Yüksek Lisans Tezi) T.C. Erciyes Üniversitesi/Sosyal Bilimler Enstitüsü, Kayseri.

Kaya, M. (2017). Vergi Kayıp ve Kaçaklarıyla Mücadelede MASAK'ın Rolü-I, *Vergi Dünyası*, 363, 144-152.

Kaya, S. (2005). İnterpol, Europol ve Uluslararası Terörizm. *Stratejik Araştırmalar Enstitüsü Güvenlik Stratejileri Dergisi*, *1*(2), 31-49.

Kazancı, M. (2002). Althusser, İdeoloji ve İletişimin Dayanılmaz Ağırlığı. *Ankara Üniversitesi SBF Dergisi 57* (1), 55-87.

Kesbiç, C. Y., Baldemir, E., ve Bakımlı, E. (2004). Bütçe Açıkları İle Parasal Büyüme ve Enflasyon Arasındaki İlişki: Türkiye İçin Bir Model Denemesi. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, 19*(1), 81-98.

Kesebir, M. ve Günceler, B. (2019). Kripto Para Birimlerinin Parlak Geleceği. *Iğdır Üniversitesi Sosyal Bilimler Dergisi / Iğdır University Journal Social Science*. 17, 605-625.

Kocabaş, S. (2003). *Ermeni Meselesi Nedir, Ne Değildir ?*. (5. Baskı) İstanbul: Vatan Yayınları.

Koç, S. ve Kaynak, S. (2009). *Yeni Medya Olarak İnternet ve Hukuki Kişisel*

Güvenlik. XIV. Türkiye'de İnternet Konferansı Bildirileri, Bilgi Üniversitesi, İstanbul, (12-13 Aralık 2009).

KOM. (2005). Organize Suçlar: Silah ve Mühimmat Kaçakçılığı. *KOM Faaliyet Raporu 2005*. Erişim Adresi: https://www.egm.gov.tr/kurumlar/egm.gov.tr/IcSite/kom/YAYINLARIMIZ/T%C3%9CRK%C3%87E/2005%20RAPORU%20T%C3%9CRK%C3%87E.pdf

Kuyaksil, A. (2004). Türkiye'de Terör ve Terörün Kaynakları. *Polis Dergisi*, *10* (40), 89-108.

Küçüközyiğit, G. (2004). Karaparanın Aklanması Suçu ve Hukukumuzda Düzenlenmesi, *Vergi Dünyası*, http://www.vergidunyasi.com.tr/Makaleler/3320 .

Laurance, T. (2017). *Blockchain for Dummies*. New Jersey: Jonh Wiley& Sons.

Lewis, A. (2018, 9 Ekim). So, You Want to Use a Blockchain for That ?, https://www.coindesk. com/want-use-blockchain

Lewis, A. (2018a). *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurriencies and the Technology That Powers Them*. Florida: Mango Publishing Group.

Mainelli, M. (2017). Blockchain Will Help Us Prove Our Identities In A Digital World, *Harvard Business Review*. (Erişim Tarihi: 14.04.2018), https://hbr.org/2017/10/smart-ledgers-can-help-usreclaim-control-of-our-personal-data.

Mavral, Ü. (2001). *Kara Para; Kayıt Dışı Ekonomi İlişkisi ve Türkiye Yansımaları*, *Birinci Basım*. Ankara: Maliye Hukuk Yayınları.

Marvin, R. (2017). Blockchain: The Invisible Technology That's Changing the World. (Erişim Tarihi: 14.04.2018), https://software.org/wpcontent/uploads/Software_Beyond-Bitcoin.pdf

Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System. http://citeseerx.ist.psu.edu/viewdoc/summary? doi=10.1.1.221.9986

Nath, I. (2016). Data Exchange Platform to Fight Insurance Fraud on Blockchain. *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, 821–825.

Onay, Y. (2009). *Etki Odaklı Hareket Terör*. İstanbul: Yeni Yüzyıl Yayınları

Ozer, R. (2017). *Ethereum: The Insider Guide to Blockchain Technology, Cryptocurrency and Mining Ethereum.* E-Kitap: CreateSpace Independent Publishing.

Öçal, T., Çolak, Ö. F., Togay, S., ve Eser, K. (1997). *Para Banka Teori ve Politika*. Ankara: Gazi Kitabevi.

Ömrüuzun, B. (2019). *Yapay Sinir Ağları İle Kripto Paraların Fiyat Modellemesi*. (Yüksek Lisans Tezi).T.C. İstanbul Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.

Önemli, M. (2004). *İnternet Suçlarıyla Mücadele Yöntemleri*. (Yüksek Lisans Tezi). Türkiye ve Orta Doğu Amme İdaresi Enstitüsü (TODAİE), Ankara.

Özbaran, M. H. (2019, 20 Aralık.). Yolsuzluk ve Bu Alanda Mücadele Eden Uluslararası Örgütler. http://www.sayistay.gov.tr/yayin/dergi/icerik/der50m2.pdf.

Özbilen, Ş. (2015). *Para Teorisi*. Ankara: Gazi Kitabevi.

Özen Ü., Sarı. A. (2008). İnternet Reklamcılığı: İnternet Kullanıcılarının İnternet Reklamcılığı Konusundaki Tutum ve Davranışları. *Gazi Üniversitesi Bilişim*

Teknolojileri Dergisi,1(3).

Özortak, A. (2005). *Karapara ve Karapara Aklama ile Etkin Mücadele*. (Yayınlanmamış Yüksek Lisans Tezi), Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü, Kütahya.

Özkan, T. (2006). *Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi*. (Yayınlanmamış Yüksek Lisans Tezi). Anadolu Üniveristesi/Sosyal Bilimler Enstitüsü, Eskişehir.

Öztürk, N. (2016). *Para Banka Kredi*. Bursa: Ekin Yayınları.

Öztürk, S. ve Çelik K. (2009). Terörizmin Türkiye Ekonomisi Üzerine Etkileri. *Alanya İşletme Fakültesi Dergisi, 1* (2), 85-106.

Padem H., Göksu, A. ve Konaklı, Z. (2012). *Araştırma Yöntemleri SPSS Uygulamalı*. Sarajevo: IBU Publications

Paranın Tarihi. (2019, 30 Aralık). Erişim adresi: https://www.darphane.gov.tr/paranin-tarihi

Parasız, İ. (1996). *İktisada Giriş*. Bursa: Ezgi Kitabevi.

Parasız, İ. (2005). *Para Banka ve Finansal Piyasalar*. Bursa: Ezgi Kitabevi.

Pfitzmann, A. ve Hansen, M. (2010). A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectibility, Unobservability, Pseudonymity and Identitiy Manangement. Erişim Adresi: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Ping, H. (2004). New Trends In Money Laundering - From The Real World To Cyberspace. *Journal Of Money Laundering Control 8* (1), 48-55.

Preiss, M.R. (2017). Cryptocurrency is the Great African Opportunity. *NTU-SBF Centre for African Studies.* Erişim adresi: https://www.iabfm.org/download.php?id=433

Reyna, A., Martin, C., Chen, J. , Soler, E. ve Diaz, M.(2018). On blockchain and its integration with IoT Challenges and opportunities. *Future Generation Computer Sysems*, 88, 173–190.

Sağıroğlu Ş. ve Bulut H. (2009). Mobil Ortamlarda Bilgi ve Haberleşme Güvenliği Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,24*(3), 499-507.

Saraçlı, M. (2007). Uluslararası Hukukta Terörizm. *Gazi Üniversitesi Hukuk Fakültesi Dergisi, 11*(1-2), 1049-1078.

Sekmen, F. (2012). *Para Teorisi, Kavram-Kuramlar Modeller*. Ankara: Seçkin Yayınevi.

Seth, A. (2016). The Possibilities With Blockchains Explaning Software. (Erişim Tarihi: 14.08.2017), https://opensourceforu.com/

Savona, E. U. ve De Feo, M. A. (2005). International Money Laundering Trends and Prevention/Control Policies. E. U. Savona (Ed.). *Responding to Money Laundering International Perspectives* içinde (pp. 9-70). University of Trento Italy: Harwood Academic Publishers.

Sayın, N. (2017). *Dalgacık Dönüşümü Tabanlı Görsel Kriptoloji*. (Yüksek Lisans Tezi). Kocaeli Üniversitesi/Fen Bilimleri Enstitüsü, Kocaeli.

Sazak, S. (2018). *Sınıraşan Organize Suçlarla Mücadele de ABD ve Türkiye Kıyaslaması: Federal Soruşturma Bürosu (FBI) ve Emniyet Genel Müdürlüğü (EGM)*.

(Doktora Tezi) T.C. Polis Akademisi/Güvenlik Bilimleri Enstitüsü, Ankara.

Sever, M. (2008). Financial Sources of the PKK. Aydın, S. (Ed.) *Karapara Aklama ve Terörizmin Finansmanı* içinde, Ankara: Adalet Yayınevi.

Söze, K. (2017). Blockchain: Ultimate Step By Step Guide To Understanding Blockchain Technology, Bitcoin Creation, and the Future of Money (Novice to Expert). Apple Books Kindle Edition.

Şahin, H. (2017). *Kripto 15 Temmuz Darbe Gecesi*. İstanbul: Profil Kitap.

Şen, Y. F. (2015). Terörün Toplumlar Üzerindeki Sosyo-Ekonomik Etkilerine Bakış: PKK Terörü ve Ağrı Gerçeği. *Ağrı İbrahim Çeçen Üniversitesi Sosyal Bilimler Dergisi 1* (2), 17-70.

Şenel, M. M. (2019). *İslam İktisadında Kripto Paraların Yeri*. (Yüksek Lisans Tezi) T.C. İstanbul Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.

Tama, B. A., Kweka, B. J., Park, Y. ve Rhee, K.H. (2017). A critical review of blockchain and its current applications. International Conference on Electrical Engineering and Computer Science (ICECOS, 2017), 109–113.

Taşdemir, F. (2006). *Uluslararası Terörizme Karşı Devletlerin Kuvvete Başvurma Yetkisi*. Ankara: USAK Yayınları.

Teichmann, F.M.J. (2018). Financing terrorism through cryptocurrencies – a danger for Europe?. *Journal of Money Laundering Control, 21*(4), 513–519.

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. *Service Systems and Service Management (ICSSSM),* 13th International Conference on. IEEE.

Tikveşli, A. O. (2019). *Blok Zincir Teknolojisi ve %51 Sorunsalı*. (Yüksek Lisans Tezi). T.C. Beykent Üniversitesi/Fen Bilimleri Enstitüsü , İstanbul.

Topal, A. H. (2004). *Uluslararası Hukukta Devlet Destekli Terörizme Karşı Kuvvet Kullanma*. (Yayınlanmamış Doktora Tezi). Ankara Üniversitesi/Sosyal Bilimler Enstitüsü, Ankara.

Turan, M. (2017). *Bilişim Hukuku*. Ankara: Seçkin Yayıncılık.

Türk Ceza Kanunu(5237 S.K.), Resmi Gazete, 25611: 12/10/2004

Türkiye Bankalar Birliği, (TBB). (2013). *Kara Paranın Aklanması Suçu ile Mücadele ve Bankaların Yükümlülükleri*. Yayın No: 235.

Türkiye Cumhuriyeti Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu Başkanlığı. (MASAK) (2016). *Şüpheli İşlem Bildirim Rehberi (Bankalar).* Sürüm 1.4. Erişim adresi: https://ms.hmb.gov.tr/uploads/2019/09/MSK-RHB-%C5%9E%C4%B0B-001-1.4.pdf

Türkiye Cumhuriyeti Merkez Bankası. (2014). *Ödeme Sistemleri Türkiye'de Ödeme Sistemleri*. Ankara: Türkiye Cumhuriyet Merkez Bankası İdare Merkezi.

USA Air Force. (1998). Emission Security Countmeasures Reviews. *USA Air Force Systems Security Memorandum 7011*. Erişim adresi: https://cryptome.org/afssm-7011.htm

Uyar, T. (2006). Terörizmin Finansmanı ile Mücadele. *Polis Dergisi, 12* (50), 64−84.

Uyuşturucu Maddelerin Sınıflandırılması. (2019, 20 Aralık). Erişim adresi: http://www.kom.gov.tr/Tr/KonuDetay.asp?id=1&BKey=39, (20.12.2019)

Uyuşturucu Madde Türleri. (2019, 20 Aralık). Erişim adresi: http://www.kom.gov.tr/Tr/KonuDetay.asp?id=1&BKey=38

Uyuşturucu ve Uyarıcı Maddeler. (2019, 20 Aralık). Erişim adresi: http://www.genbilim.com/content/view/3468/33/

Ünlü, U. (2019). Kara Para Aklamada Yeni Yöntemler Ve Kara Paranın Ekonomi Üzerindeki Etkileri. *Sayıştay Dergisi*, 133.

Ütük, Ö. (2010) *Organize Suçlarla Mücadele Çerçevesinde Avrupa Birliğinde Suç Gelirlerinin Aklanmasinin Önlenmesine İlişkin Çalışmalar*. (Yayımlanmamış Uzmanlık Tezi) Avrupa Birliği ve Dış İlişkiler Dairesi Başkanlığı, Ankara

Ütük, Ö. (2009). Terörizmin Finansmanıyla Uluslararası Mücadele. *Bütçe Dünyası Dergisi, 3* (32).

Xu, X., Weber, I. ve Staples, M. (2019). *Architecture for Blockchain Applications.* Cham: Springer.

Venter, H. 2016. Digital currency – A case for standard setting activity. *A perspective by the Australian Accounting Standards Board (AASB)*, Principal ASAF meeting, December, ASAF Agenda ref: 5.

Yayla, A. (1990). Terörizm: Kavramsal Bir Çerçeve. *Ankara Üniversitesi S.B.F. Dergisi, 45*(1-4), 334-380.

Yayla, A. (2016). 15 Temmuz Direnişi ve Türkiye Demokrasisi. *Liberal Düşünce Dergisi*, 83, 5-49.

Yayla, A. S. (2008). Terörizmin Finansmanı ve Organize Suç Örgütleri İlişkileri. Aydın, S. (Ed.) *Karapara Aklama ve Terörizmin Finansmanı* içinde, Ankara: Adalet Yayınevi.

Yazıcı, A. (2008). Yeni Kara Para Aklama Yöntemleri Olarak Akıllı Kartlar ve İnternet. *Anadolu Üniversitesi Sosyal Bilimler Dergisi, 8* (2).

Yazıcıoğlu (1997) ise, *"ceza kuralları uyarınca, bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç içeren fiiller"* şeklinde tanımlamaktadır.

Yeniçeri, Ö. (2003). Terör ve ABD: Terörün Hegemonya Aracı Olarak Kullanılması Sorunu. *2023 Dergisi*, 32-41.

Yıldırım, Z. (2012). *Hukuksal Açıdan Terörizmin Finansmanının Önlenmesi*. Ankara: Adalet Yayınevi

Yılmaz D. (2004). Hacking Bilişim Korsanlığı ve Korunma Yöntemleri. İstanbul: Hayat Yayınları.

Yılmaz, O. G. (2007). Kriptoloji Uygulamalarında Hukuki Boyut. *Marmara Üniversitesi Hukuk Fakultesi Hukuk Araştırmaları Dergisi*, *13*(1-2), 137-147.

Yılmaz, S. (2011). Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu. *Ankara Barosu Dergisi*, *2*(71).

Yücebaş, Ö. (2011). *Suç Ekonomisi ve Terörün Finansmanı*. Ankara: Turhan Kitabevi.

Zhao, J. L. , Fan, S. ve Yan, J.(2016). Overview of Business Innovations and Research Opportunities in Blockchain and Introduction to the Special Issue. *Finance Innovation, 2*(1), 28.

Zheng, Z., Xie, S., Dai, H., Chen, X., ve Wang, H. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", In Big Data (BigData Congress), 2017 IEEE 6th International Congress Proceedings, 557–564.