TERÖRÜN FİNANSMANI VE KARA PARA AKLAMADA ELEKTRONİK PARA İLE BLOKZİNCİRİN ROLÜ

Kullanım Örüntüleri, Zincir Üstü Adli Analiz ve Takip Mekanizmaları

The Role of Electronic Money and Blockchain in Terrorist Financing and Money Laundering: Usage Patterns, On-Chain Forensics and Tracing Mechanisms

Derleme Makale / Review Article

Dr. Burak Olgun
burakolgun@solutionhome.net
Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Terörün finansmanı • Kara para aklama • Elektronik para • Blokzincir analizi • Stablecoin • Seyahat kuralı • MASAK

ÖZET

Terörün finansmanı ile suç gelirlerinin aklanması, yöntem bakımından birbirine yaklaşan ama amaç bakımından ters yönde işleyen iki süreçtir. Aklamada kirli bir kaynağa temiz görünüm kazandırılmaya çalışılır. Terörün finansmanında ise kaynak çoğu zaman yasaldır ve asıl gizlenen şey paranın varış noktasıdır. Son on yılda her iki süreç de bankacılık sisteminin kenarında gelişen iki altyapıya kaymıştır: ön ödemeli kartlar, e-cüzdanlar ve mobil para gibi elektronik para araçları ile blokzincir üzerinde çalışan kripto varlıklar. Chainalysis verilerine göre yasa dışı adreslere ulaşan kripto varlık hacmi 2025 yılında en az 154 milyar ABD dolarına çıkmış, bu hacmin %84'ü stablecoinlerle taşınmıştır. Terör örgütleri açısından bu tablo daha dar ama daha belirgin bir örüntüye işaret eder: TRON ağındaki USDT, her bağışçı için yeni üretilen adresler ve bölgesel borsalar ya da gayriresmî aracılar üzerinden nakde çıkış. Bu çalışma; elektronik paranın ve blokzincirin aklama ile terörün finansmanındaki işlevini, kullanılan gizleme tekniklerini ve bunlara karşı geliştirilen takip mekanizmalarını derlemektedir. Takip mekanizmaları iki düzeyde ele alınmıştır. Birinci düzey kümeleme, etiketleme ve akış analizine dayanan zincir üstü adli analizdir. İkinci düzey FATF seyahat kuralı, ihraççı düzeyinde varlık dondurma, kamu ile özel sektör arasındaki bilgi paylaşımı ve Türkiye'de MASAK, SPK ile TCMB tarafından kurulan kurumsal çerçevedir. Çalışmanın temel bulgusu, blokzincirin sanıldığı kadar anonim olmadığı, buna karşılık kimlik tespitinin hâlâ itibari paraya giriş ve çıkış kapılarında tutulan zincir dışı kayıtlara bağlı kaldığıdır. Çalışmada herhangi bir somut davaya ya da kişiye atıf yapılmamıştır.

Anahtar Kelimeler: *terörün finansmanı, kara para aklama, suç gelirlerinin aklanması, elektronik para, ön ödemeli kart, kripto varlık, blokzincir analizi, stablecoin, USDT, mikser, zincirler arası köprü, seyahat kuralı, FATF Tavsiye 15, MASAK, kripto varlık hizmet sağlayıcı, adli bilişim*

ABSTRACT

Terrorist financing and money laundering are two processes that converge in method but run in opposite directions in purpose. Laundering seeks to give illicit proceeds a clean appearance, whereas in terrorist financing the source is often legitimate and what is hidden is the destination of the funds. Over the past decade both processes have shifted towards two infrastructures on the margins of the banking system: electronic money instruments such as prepaid cards, e-wallets and mobile money, and crypto assets running on blockchains. According to Chainalysis, illicit addresses received at least 154 billion US dollars in 2025, with stablecoins accounting for 84% of that volume. For terrorist

burakolgun.com

organisations the picture is narrower but sharper: USDT on the TRON network, fresh deposit addresses for each donor, and cash-out through regional exchanges or informal brokers. This review examines the function of electronic money and blockchain in laundering and terrorist financing, the obfuscation techniques in use, and the tracing mechanisms developed in response. Tracing is discussed at two levels: on-chain forensics based on clustering, attribution and flow analysis, and the institutional layer formed by the FATF Travel Rule, issuer-level asset freezing, public-private information sharing and the Turkish framework built by MASAK, the Capital Markets Board and the Central Bank. The main finding is that blockchains are less anonymous than commonly assumed, yet identification still depends on off-chain records held at fiat on-ramps and off-ramps. No specific case or individual is referred to in this study.

Keywords: *terrorist financing, money laundering, electronic money, prepaid card, crypto asset, blockchain analytics, stablecoin, USDT, mixer, cross-chain bridge, Travel Rule, FATF Recommendation 15, MASAK, virtual asset service provider, digital forensics*

1. Giriş

11 Eylül 2001 saldırılarının toplam maliyeti yaklaşık 500 bin ABD doları olarak hesaplanmıştır (TRM Labs, 2026). Para, banka havaleleri, seyahat çekleri ve elden taşınan nakitle hareket etmişti. Aradan geçen yirmi beş yılda terörün finansmanıyla mücadele, bankacılık sistemini merkeze alan bir düzen kurdu: müşterini tanı ilkesi, şüpheli işlem bildirimi, yaptırım listeleri ve muhabir bankacılık denetimi. Bu düzen işe yaradıkça fon akışı sistemin kenarına kaydı. Bugün aynı işlev, bir mesajlaşma kanalında paylaşılan TRON adresine gönderilen birkaç yüz dolarlık USDT ile ya da başkası adına açılmış bir e-cüzdan hesabı üzerinden görülebilmektedir.

Bu kayma iki farklı altyapıda yaşanmıştır. Birincisi elektronik paradır: ön ödemeli kartlar, e-cüzdanlar, mobil para ve ödeme kuruluşlarının sunduğu hesaplar. Bu araçlar hukuken itibari paranın dijital temsilidir ve lisanslı bir ihraççıya bağlıdır. İkincisi blokzincir üzerinde çalışan kripto varlıklardır. Bunlar merkezî bir ihraççıya bağlı olmayabilir, sınır tanımaz ve aracısız el değiştirebilir. İki altyapı çoğu vakada birlikte kullanılır. Nakit bir e-cüzdana yüklenir, e-cüzdandan kripto borsasına geçer, oradan stablecoin olarak yurt dışına çıkar ve başka bir ülkede yeniden nakde döner.

Kamuoyunda kripto varlıkların izlenemez olduğu yönünde yaygın bir kanaat vardır. Teknik gerçeklik bunun tersine yakındır. Bitcoin ve Ethereum gibi açık blokzincirlerde her işlem kalıcı olarak kaydedilir ve herkes tarafından okunabilir. Sorun işlemin görülmesi değil, adresin arkasındaki kişinin belirlenmesidir. Bu nedenle kripto varlıklarla yürütülen bir soruşturmanın başarısı iki şeye bağlıdır: zincir üstü verinin doğru analiz edilmesi ve bu analizin, kimlik bilgisi tutan bir kuruma (borsa, elektronik para kuruluşu, OTC aracısı) bağlanabilmesi.

Ölçek de değişmiştir. Chainalysis (2026a), yasa dışı adreslere ulaşan kripto varlık hacmini 2025 için en az 154 milyar dolar olarak tahmin etmiştir. Bu rakamın büyük kısmı terör örgütlerinden değil, yaptırım altındaki devlet bağlantılı yapılardan gelmektedir. Terör örgütlerinin kripto kullanımı mutlak değer olarak çok daha küçüktür. Buna karşılık FATF (2025a), terörün finansmanı davalarında kripto varlıkların ve çevrim içi ödeme hizmetlerinin payının arttığını, değerlendirilen yetki alanlarının %69'unun terörün finansmanını soruşturma,

buralogun.com

kovuşturma ve mahkûmiyetle sonuçlandırmada büyük ya da yapısal eksiklik taşıdığını tespit etmiştir.

Türkiye bu tartışmanın kenarında değildir. Chainalysis (2025) verilerine göre Türkiye, Temmuz 2024 ile Temmuz 2025 arasında yaklaşık 200 milyar dolarlık kripto varlık girişiyle Orta Doğu ve Kuzey Afrika bölgesinin en büyük piyasasıdır. Türkiye Ekim 2021'de FATF'in artırılmış izleme listesine alınmış, Haziran 2024'te bu listeden çıkmıştır. 7518 sayılı Kanun ile kripto varlık hizmet sağlayıcıları Sermaye Piyasası Kurulu (SPK) izin ve denetimine bağlanmış, MASAK ise Şubat 2025'ten itibaren seyahat kuralını uygulamaya koymuştur. 2025 yılında büyük bir elektronik para kuruluşuna yönelik yasa dışı bahis ve aklama soruşturması, e-para altyapısının da aynı risk alanının parçası olduğunu açıkça göstermiştir.

Bu çalışmanın amacı, elektronik para ve blokzincirin aklama ile terörün finansmanındaki işlevini, bu işlevin dayandığı teknik ve kurumsal zayıflıkları ve bunlara karşı kullanılan takip mekanizmalarını tek bir çerçevede derlemektir. Makalenin geri kalanı şöyle düzenlenmiştir. İkinci bölüm kavramsal çerçeveyi kurar. Üçüncü bölüm elektronik paranın, dördüncü bölüm blokzincir ve kripto varlıkların rolünü inceler. Beşinci bölüm terör örgütlerinin dijital finansman örüntülerini vakalar üzerinden özetler. Altıncı bölüm zincir üstü adli analiz yöntemlerini, yedinci bölüm uluslararası düzenleyici takip mekanizmalarını ele alır. Sekizinci bölüm Türkiye'deki hukuki çerçeveyi ve uygulamayı değerlendirir. Dokuzuncu bölümde öneriler, onuncu bölümde sonuç yer almaktadır. Çalışma kamuya açık raporlara, mevzuata ve hakemli literatüre dayanmakta olup herhangi bir somut davaya ya da kişiye atıf yapılmamıştır.

2. Kavramsal Çerçeve

2.1. Kara Para Aklama ve Aşamaları

Kara para aklama (money laundering), suçtan elde edilen mal varlığının yasa dışı kaynağını gizlemek ve bu değere meşru bir görünüm kazandırmak amacıyla yapılan işlemlerin bütünüdür. Türk hukukunda karşılığı 5237 sayılı Türk Ceza Kanunu'nun 282. maddesinde düzenlenen "suçtan kaynaklanan malvarlığı değerlerini aklama" suçudur. Madde, alt sınırı altı ay veya daha fazla hapis cezasını gerektiren bir suçtan kaynaklanan değerin yurt dışına çıkarılmasını ya da gayrimeşru kaynağını gizlemek amacıyla çeşitli işlemlere tabi tutulmasını üç yıldan yedi yıla kadar hapis ve yirmi bin güne kadar adli para cezasıyla yaptırıma bağlar.

Literatürde aklama süreci geleneksel olarak üç aşamada tanımlanır. **Yerleştirme (placement)** aşamasında nakit ya da suç geliri finansal sisteme sokulur. **Ayrıştırma (layering)** aşamasında fon, izini kaybettirmek için çok sayıda işlem, hesap ve ülke üzerinden hareket ettirilir. **Bütünleştirme (integration)** aşamasında değer, meşru bir ekonomik faaliyetin getirisi gibi ekonomiye geri döner. Dijital araçlar her üç aşamanın maliyetini düşürmüştür. Nakdin bir e-cüzdana ya da P2P platformunda kripto alımına dönüştürülmesi yerleştirmeyi kolaylaştırır. Mikserler, zincirler arası köprüler ve otomatik adres üretimi ayrıştırmayı dakikalar içinde yüzlerce adıma çıkarabilir.

2.2. Terörün Finansmanı ve Aklamadan Farkı

burakolgun.com

Terörün finansmanı (terrorist financing), terör eylemi ya da terör örgütü için fon toplanması, sağlanması ve aktarılmasıdır. Türkiye'de 6415 sayılı Terörün Finansmanının Önlenmesi Hakkında Kanun'un 4. maddesi, bir terör örgütüne ya da terör suçlarının işlenmesinde kullanılacağı bilinerek fon sağlanmasını veya toplanmasını beş yıldan on yıla kadar hapis cezasıyla yaptırıma bağlar. Kanun, fonun eylemde fiilen kullanılmış olmasını aramaz. Literatürde ve bazı resmî çevirilerde "terörizmin finansmanı" ifadesi de kullanılmaktadır. Bunun en bilinen örneği, Birleşmiş Milletler'in 1999 tarihli International Convention for the Suppression of the Financing of Terrorism metninin Türkçe adı olan "Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme"dir. Türkiye bu Sözleşme'yi 4738 sayılı Kanun ile onaylamıştır (Birleşmiş Milletler, 1999). Bu çalışmada, 6415 ve 5549 sayılı Kanunlar ile MASAK uygulamasında yerleşmiş olan "terörün finansmanı" terimi tercih edilmiştir. Bu tercihin kavramsal bir gerekçesi de vardır. Terör, somut şiddet eylemini ve onu gerçekleştiren örgütü; terörizm ise bu eylemlere dayanak olan ideolojiyi ve stratejiyi ifade eder. Finanse edilen şey ideolojinin kendisi değil, eylemler, örgütler ve kişilerdir. FATF'in İngilizce metinlerinde "terrorism financing" yerine "terrorist financing" ifadesinin kullanılması da aynı yaklaşımı yansıtır.

Aklama ile terörün finansmanı arasındaki temel fark akışın yönüdür (Şekil 1). Aklamada kaynak kirlidir ve amaç onu temiz göstermektir. Terörün finansmanında kaynak çoğu zaman yasaldır: bireysel bağışlar, hayır kurumu kılığındaki kampanyalar, meşru bir işletmenin gelirinden ayrılan pay. Gizlenmesi gereken şey kaynaktan çok varış noktasıdır. İkinci fark tutarlardır. Aklama milyonlarca dolarlık akışlarla ilgilenirken tek bir eylemin maliyeti birkaç bin dolar olabilir. Bu nedenle eşik değerlere dayanan klasik izleme kuralları terörün finansmanında sık sık kör kalır. Üçüncü fark, iki sürecin giderek daha fazla aynı aracıları kullanmasıdır. FATF (2025a), terörün finansmanı şemaları ile örgütlü suç arasındaki yakınlaşmayı son dönemin belirgin eğilimlerinden biri olarak kaydetmiştir.



Kaynak: FATF (2015, 2025a) ve UNODC aklama aşamaları modeli temel alınarak yazar tarafından derlenmiştir.

Şekil 1. Kara para aklama ile terörün finansmanının aşamaları ve ortak zayıf nokta

Şekil 1'in alt kısmı, bu çalışmanın ana argümanlarından birini özetler. Her iki süreçte de dijital değer er ya da geç itibari paraya dönmek zorundadır. Silah, yakıt, kira ya da maaş büyük ölçüde hâlâ ulusal para birimiyle ödenir. Giriş ve çıkış kapıları (on-ramp ve off-ramp), yani kripto varlık hizmet sağlayıcıları, elektronik para kuruluşları ve OTC aracıları, hem failin en savunmasız olduğu hem de takip mekanizmalarının en etkili çalıştığı noktalardır.

2.3. Elektronik Para, Sanal Varlık ve Stablecoin Ayrımı

Kavramların karıştırılması hem hukuki nitelendirmede hem de delil değerlendirmesinde hata doğurur. **Elektronik para**, 6493 sayılı Kanun'un 3. maddesine göre elektronik para kuruluşunca kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, ödeme işlemlerini gerçekleştirmek için kullanılan ve ihraççı dışındaki gerçek ve tüzel kişilerce de ödeme aracı olarak kabul edilen parasal değerdir. Değeri itibari paraya birebir bağlıdır ve kuruluş, ihraç ettiği tutar kadar fonu korumakla yükümlüdür.

Kripto varlık ise 6362 sayılı Sermaye Piyasası Kanunu'na 7518 sayılı Kanun ile eklenen tanıma göre, dağıtık defter teknolojisi ya da benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan ve değer ya da hak ifade edebilen gayri maddi varlıktır. FATF terminolojisinde karşılığı "sanal varlık" (virtual asset), bu varlıklar üzerinde hizmet sunan kuruluşların karşılığı ise "sanal varlık hizmet sağlayıcısı" (VASP) kavramıdır. **Stablecoin** bu iki dünyanın arasında durur. Blokzincir üzerinde dolaşan bir kripto varlıktır, ancak değeri genellikle ABD doları gibi bir itibari paraya sabitlenmiştir ve merkezî bir ihraççı tarafından çıkarılır. USDT (Tether) ve USDC (Circle) en yaygın örneklerdir. Tablo 1, bu araçları aklama ve terörün finansmanı açısından önemli özellikleriyle karşılaştırmaktadır.

Tablo 1. Nakit, elektronik para ve kripto varlık türlerinin aklama/terör finansmanı açısından karşılaştırılması

Özellik	Nakit / Hawala	Elektronik para	Açık blokzincir (BTC, ETH)	Stablecoin (USDT, USDC)	Gizlilik coini (XMR)
Kimlik bağı	Yok / aracıya güven	İhraççıda KYC (anonim limit altı hariç)	Takma ad (adres)	Takma ad; ihraççıda KYC yok	Gizlenmiş
İşlem kaydı	Yok / defter	Kuruluş veritabanı	Herkese açık, kalıcı	Herkese açık, kalıcı	Şifreli, sınırlı
Sınır ötesi hız	Günler	Kuruluşa bağlı	Dakikalar	Saniyeler-dakikalar	Dakikalar
Değer oynaklığı	Yok	Yok	Yüksek	Düşük	Yüksek
Dondurulabilirlik	El koyma ile	Kuruluş talimatıyla	Yalnız borsada	İhraççı adres düzeyinde	Yalnız borsada
Adli izlenebilirlik	Çok düşük	Yüksek (kayıt talebiyle)	Yüksek (analizle)	Yüksek (analizle)	Düşük
Tipik suistimal	Kurye, hawala	Hesap kiralama, anonim kart	Fidye, darknet	Bağış, yaptırım kaçakçılığı	Aklama son aşaması

Not. Kaynak: FATF (2021, 2025b), 6493 ve 7518 sayılı Kanunlar ile Möser vd. (2018) temel alınarak yazar tarafından derlenmiştir.

Tablodan çıkan sonuç şudur: stablecoinler, failin istediği özelliklerin çoğunu bir araya getirir. Değeri sabittir, hızlıdır, ucuzdur ve ihraççı nezdinde kimlik tespiti gerektirmez. Tek zayıf noktası, merkezî ihraççının adres düzeyinde varlık dondurabilmesidir. Bu özellik yedinci bölümde ele alınan takip mekanizmalarının en etkililerinden birinin temelini oluşturur.

3. Elektronik Paranın Rolü

3.1. Ön Ödemeli Araçlar ve Anonim Kartlar

Ön ödemeli kartlar, terörün finansmanı gündemine 2015 Paris saldırılarından sonra yerleşmiştir. Saldırganların konaklama ve lojistik giderlerinde ön ödemeli kartlar kullandığının anlaşılması, Avrupa Komisyonu'nun 2016 tarihli terörün finansmanıyla mücadele eylem planında anonim ön ödemeli araçlara ilişkin eşiklerin düşürülmesini gündeme getirmiştir (Avrupa Komisyonu, 2016). Bu süreç, 2018/843 sayılı Beşinci Aklama Direktifi ile kimlik tespiti yapılmadan kullanılabilen ön ödemeli araçlar için eşiğin 150 avroya, uzaktan ödemelerde 50 avroya indirilmesiyle sonuçlanmıştır.

Anonim kartın riski tek bir kartın tutarında değil, çoğaltılabilirliğindedir. Aynı kişi farklı satış noktalarından çok sayıda kart alıp her birini eşik altında yükleyebilir. FATF (2015), ön ödemeli kartların fiziksel olarak sınır ötesine taşınmasının nakit beyan yükümlülüklerini aşmanın bir yolu olarak kullanılabildiğine dikkat çekmiştir. Türkiye'de bu risk, anonim ön ödemeli araçlar için aylık toplam yükleme ve harcama tavanı, ATM'den nakit çekimin durdurulması ve mobil ödemelerde tek işlem ile aylık işlem tavanları üzerinden yönetilmektedir. Kimlik doğrulaması tamamlanmamış anonim araçlarda aylık üst sınır 2.750 TL, mobil ödemelerde tek seferlik işlem sınırı 1.000 TL olarak uygulanmaktadır.

3.2. E-Cüzdanlar, Hesap Kiralama ve Yasa Dışı Bahis Ekonomisi

Kimlik tespiti yapılmış bir e-cüzdan hesabı, ilk bakışta aklama için elverişsiz görünür. Uygulamada sorun, hesabın gerçek kullanıcısının hesap sahibi olmamasıdır. Yasa dışı bahis ve dolandırıcılık ağları, küçük ücretler karşılığında başkalarının adına açılmış hesapları toplu hâlde kullanır. Bu "hesap kiralama" ya da "para katırı" (money mule) modelinde KYC kaydı doğrudur, ancak hesabı kullanan kişi başkasıdır. Kuruluşun elindeki kimlik bilgisi fiili kullanıcıya değil, çoğu zaman ekonomik güçlük içindeki bir aracıya çıkar.

Türkiye'de bu modelin ölçeği 2025 yılında görünür hâle gelmiştir. İstanbul Cumhuriyet Başsavcılığı'nın yasa dışı bahis, örgüt kurma ve suçtan kaynaklanan malvarlığı değerlerini aklama suçlarına ilişkin soruşturması kapsamında, 27 Mayıs 2025'te bir elektronik para kuruluşunun da aralarında bulunduğu şirketlere Tasarruf Mevduatı Sigorta Fonu kayyım olarak atanmıştır. Kamuoyuna yansıyan bilgilere göre MASAK raporlarında, kuruluş üzerinden açılan 26.012 hesabın 102 yasa dışı bahis sitesinde kullanıldığı ve bu hesaplarda yaklaşık 12,8 milyar TL tutarında işlem gerçekleştiği tespit edilmiştir. Elde edilen gelirin bir kısmının kripto varlık cüzdanlarına aktarıldığı ileri sürülmüştür (Euronews, 2025). TCMB, 30 Ekim 2025'te kuruluşun faaliyet iznini iptal etmiştir. Soruşturma sürmekte olup burada yalnızca kamuya açık bilgiler, e-para altyapısının aklama zincirindeki yerini göstermek amacıyla aktarılmıştır.

Bu örnek, elektronik para ile kripto varlık arasındaki geçişin önemini de gösterir. E-cüzdan, bahis ya da dolandırıcılık gelirinin toplandığı ilk havuzdur. Kripto varlık ise bu gelirin yurt dışına ve ulusal denetimin dışına taşındığı ikinci aşamadır. TCMB'nin 2025 yılı gözetim ve denetim sonuçları da sektördeki sorunun tekil olmadığını düşündürmektedir: yıl içinde 7 kuruluşun faaliyet izni iptal edilmiş, 14 kuruluşun izni geçici olarak durdurulmuş, 72

burakoguz.com

kuruluşa toplam yaklaşık 373,2 milyon TL idari para cezası uygulanmıştır (Anadolu Ajansı, 2026).

3.3. Mobil Para ve Hawala ile Melezleşme

Bankacılık hizmetlerinin sınırlı olduğu çatışma bölgelerinde mobil para ve hawala birlikte çalışır. Hawala, güvene dayalı ve kayıt tutmayan geleneksel bir değer transfer sistemidir. Hawaladar, bir ülkede aldığı parayı başka bir ülkedeki muhabirine iletir. Taraflar arasındaki hesap zamanla ticari mal, nakit ya da günümüzde giderek artan biçimde stablecoin ile kapatılır. FATF (2025a), para veya değer transfer hizmetlerini (MVTS) terörün finansmanı açısından yüksek risk alanları arasında saymakta ve dijital teknolojilerin geleneksel tekniklerle birleşerek analizi zorlaştırdığını belirtmektedir.

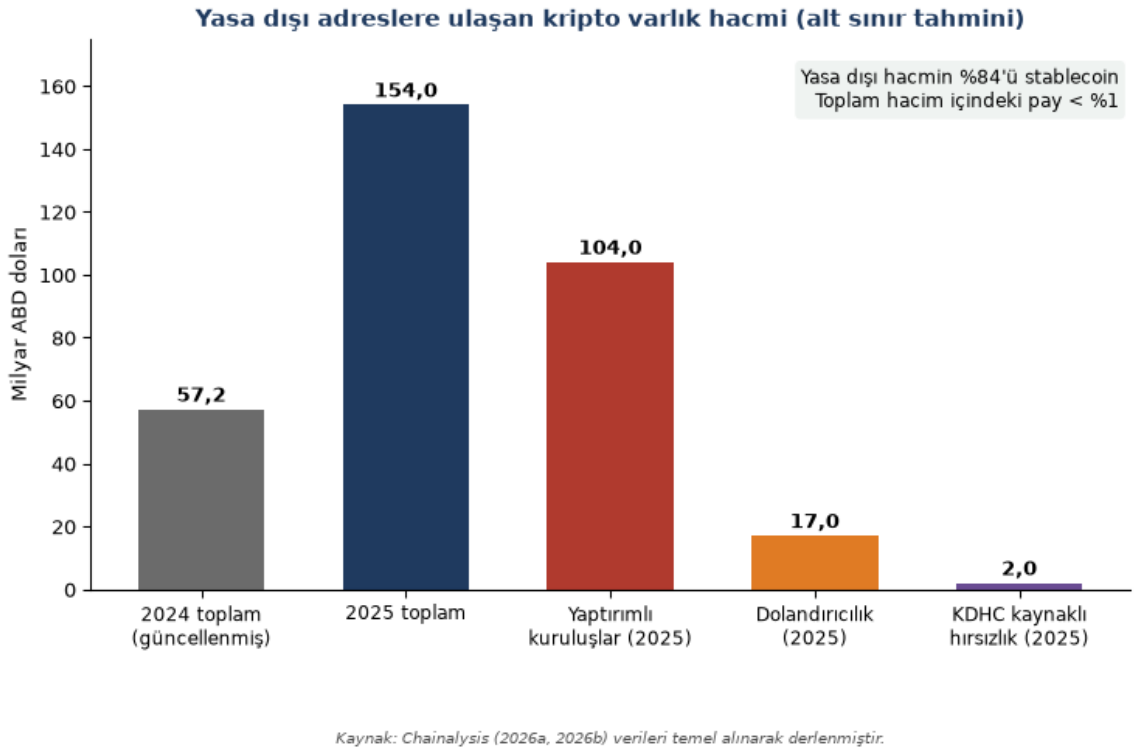
Bu melezleşme, takip açısından iki sonuç doğurur. Birincisi, zincir üstü analiz tek başına yetersiz kalır. Bir USDT transferi, hawala ağında kapanan bir borcun yalnızca bir ayağı olabilir. İkincisi, soruşturmanın finansal istihbarat, ticari kayıtlar ve iletişim verileriyle birlikte yürütülmesi gerekir. Bir hawaladarın cüzdanı, yüzlerce ilgisiz müşterinin işlemini de taşıdığından, bu cüzdana ulaşan her fonun terörle bağlantılı olduğunu varsaymak ciddi bir hatadır.

4. Blokzincir ve Kripto Varlıkların Rolü

4.1. Ölçek: 2024-2025 Verileri

Kripto varlıkların yasa dışı kullanımına ilişkin en sık başvurulan veri seti Chainalysis'in yıllık raporlarıdır. Bu verilerin iki özelliği bilinmelidir. Birincisi, tahminler o güne kadar yasa dışı olarak etiketlenmiş adreslere dayanır ve bu nedenle alt sınırdır. İkincisi, yeni adresler tespit edildikçe geçmiş yıllar yukarı doğru revize edilir. Nitekim 2024 yılı için ilk açıklanan 40,9 milyar dolarlık rakam, 2026 raporunda 57,2 milyar dolara güncellenmiştir (Chainalysis, 2026a).

burakolgun.com



Kaynak: Chainalysis (2026a, 2026b) verileri temel alınarak derlenmiştir.

Şekil 2. Yasa dışı adreslere ulaşan kripto varlık hacmi ve 2025 dağılımından seçilmiş kalemler (2026)

Şekil 2'de görüldüğü gibi 2025 yılında yasa dışı adreslere ulaşan hacim en az 154 milyar dolara çıkmıştır. Bu artışın temel kaynağı, yaptırım altındaki kuruluşların aldığı değerin %694 büyüyerek 104 milyar dolara ulaşmasıdır. Rusya bağlantılı, rubleye endeksli A7A5 token'ı bir yıldan kısa sürede 93,3 milyar dolarlık işlem hacmine ulaşmıştır. Kuzey Kore (KDHC) bağlantılı aktörler 2025'te yaklaşık 2 milyar dolar çalmış, bunun yaklaşık 1,5 milyar doları Şubat 2025'teki Bybit saldırısından gelmiştir. Dolandırıcılık kaynaklı kayıp yaklaşık 17 milyar dolardır (Chainalysis, 2026a, 2026b).

Bu rakamlar iki biçimde yanlış okunabilir. Yasa dışı hacmin toplam kripto hacmi içindeki payı %1'in altındadır. Dolayısıyla kripto varlıkların esas olarak suç amaçlı kullanıldığı iddiası verilerle desteklenmez. Öte yandan terörün finansmanına ayrılan pay bu toplam içinde çok küçüktür ve 154 milyar dolarlık rakam terör örgütlerinin kripto kullanımı için bir gösterge olarak kullanılmamalıdır. Terörün finansmanında önemli olan hacimden çok örüntüdür.

4.2. Stablecoin ve USDT-TRON Örüntüsü

Chainalysis (2026a) verilerine göre 2025 yılında yasa dışı işlem hacminin %84'ü stablecoinlerle gerçekleşmiştir. FATF (2025b) de aynı yıl yayımladığı hedefli güncellemede, KDHC bağlantılı aktörler, terörün finansmanı yapanlar ve uyuşturucu kaçakçıları dâhil olmak üzere yasa dışı zincir üstü faaliyetin büyük bölümünün artık stablecoinlerle yürütüldüğünü tespit etmiştir. FATF (2026) raporunda stablecoin piyasa değerinin 300 milyar doları aştığı belirtilmektedir.

Terör örgütleri açısından bu eğilim belirli bir ağ ve varlık üzerinde yoğunlaşmıştır. TRM Labs (2026), ideolojik olarak birbirinden farklı grupların aynı zincir üstü yönteme

Burakoğlu

yöneldiğini tespit etmiştir: TRON ağındaki USDT, her bağışçı için yeni bir yatırma adresi ve şifreli mesajlaşma kanalları üzerinden sürekli değiştirilen adresler. TRON'un tercih edilme nedeni teknik değil ekonomiktir. İşlem ücreti çok düşüktür, onay saniyeler içinde gerçekleşir ve USDT likiditesi Orta Doğu, Orta Asya ve Afrika'daki bölgesel borsalarda ve OTC aracılarında yaygındır. Nakde çıkış noktaları ise 2001'dekine benzer: bölgesel borsalar, gayriresmî aracılar ve nakit.

Bu örüntünün adli açıdan bir avantajı vardır. USDT ve USDC gibi merkezî stablecoinlerin akıllı sözleşmeleri, ihraççıya belirli adresleri kara listeye alma yetkisi verir. Yani tespit edilen bir adresteki bakiye, borsaya ulaşmadan zincir üzerinde dondurulabilir. Bitcoin'de böyle bir mekanizma yoktur.

4.3. Gizleme Teknikleri

Blokzincirin şeffaflığına karşı geliştirilen teknikler, zincir üstü bağlantıyı koparmaya ya da analizcinin sezgilerini yanıltmaya yöneliktir. Bu çalışmada teknikler, uygulanış ayrıntısına girilmeden ve yalnızca adli karşı yöntemleriyle birlikte ele alınmıştır (Tablo 2).

Tablo 2. Başlıca zincir üstü gizleme teknikleri ve adli karşı yöntemler

Teknik	İşleyiş (özet)	Adli karşı yöntem	Güncel durum
Merkezî mikser	Fonlar havuzda toplanıp farklı adreslerden geri ödenir	Giriş/çıkış tutar ve zaman eşleştirmesi; operatöre el koyma	Helix, Bitcoin Fog, ChipMixer kapatıldı
Akıllı sözleşme mikseri	Sıfır bilgi ispatıyla yatırma-çekme bağlantısı koparılır	Tutar, zaman, gaz ödemesi ve adres yeniden kullanımı analizi	Tornado Cash: yaptırım 2025'te kaldırıldı; ceza davası sürüyor
CoinJoin	Çok kullanıcılı ortak işlem; eşit çıktılar	Karışım sonrası harcama davranışı, para üstü çıktıları	Samourai kurucuları 2025'te hüküm giydi
Soyulma zinciri (peel chain)	Büyük bakiyeden her adımda küçük tutar ayrılır	Otomatik atlama takibi; ayrılan tutarların borsa girişleri	Fidye ve hırsızlık gelirlerinde yaygın
Zincir atlama / köprü	Varlık başka zincire taşınır ya da takas edilir	Köprü olaylarının eşleştirilmesi; zincirler arası grafik	Bybit sonrası aklamada yoğun kullanıldı
Stablecoin takası	Oynak varlık dolara sabit tokene çevrilir	İhraççı kara listesi; dondurma talebi	Yasa dışı hacmin %84'ü
Gizlilik coini	Halka imza, gizli adres, gizli tutar (Monero)	Borsa giriş-çıkışları, zamanlama, zincir dışı veri	AB'de KVHS'lere 2027'den itibaren yasak
P2P / OTC aracı	Kayıtsız aracılar üzerinden nakit takası	Aracı cüzdanlarının kümelenmesi; saha istihbaratı	Terör finansmanında başlıca çıkış noktası

Not. Kaynak: Möser vd. (2013, 2018), Chainalysis (2026a), TRM Labs (2025, 2026) ve ABD Adalet Bakanlığı açıklamaları temel alınarak yazar tarafından derlenmiştir.

Tablodaki tekniklerin hiçbiri tek başına mutlak gizlilik sağlamaz. Möser, Böhme ve Breuker (2013) daha 2013 yılında yaptıkları deneylerle bazı mikser hizmetlerinin giriş ve çıkış işlemlerinin eşleştirilebildiğini göstermiştir. Akıllı sözleşme tabanlı mikserlerde de kullanıcıların davranış hataları bağlantıyı çoğu zaman yeniden kurar: yatırılan ve çekilen tutarın aynı olması, çekimin kısa süre sonra yapılması ya da çekim adresinin işlem ücretinin yatırma adresiyle bağlantılı bir kaynaktan ödenmesi gibi. Gizleme teknikleri, analizcinin işini imkânsız kılmaktan çok pahalı hâle getirir.

4.4. Yaptırım Kaçakçılığı ve Devlet Bağlantılı Aktörler

2025 verilerindeki sıçramanın ardında bireysel suçlulardan çok devletler ve devlet bağlantılı ağlar vardır. Rusya merkezli Garantex borsası, Nisan 2019 ile Mart 2025 arasında en az 96

milyar dolarlık kripto varlık işlemine aracılık etmiştir. 6 Mart 2025'te çok uluslu bir operasyonla alan adına el konulmuş ve 26 milyon doları aşan varlık dondurulmuştur. Ancak Aralık 2024'te kurulan Grinex, Garantex'in faaliyetlerini kısa sürede devralmış ve kullanıcıların kayıpları rubleye endeksli A7A5 token'ı ile karşılanmıştır (TRM Labs, 2025).

Bu örnek terörün finansmanı açısından da önemlidir. Bir platformun kapatılması, altyapısı önceden hazırlanmış bir halefin devreye girmesine engel olmayabilir. Aynı yapı, terör örgütlerinin kullandığı bölgesel borsalar ve OTC ağları için de geçerlidir. Chainalysis (2026a) ayrıca İran'a bağlı vekil ağların doğrulanmış cüzdanlar üzerinden 2 milyar doları aşan fon aktardığını tespit etmiştir. Devlet destekli terör ile yaptırım kaçakçılığı arasındaki sınır, zincir üstü veride çoğu zaman aynı cüzdan kümeleri üzerinden kesişmektedir.

5. Terör Örgütlerinin Dijital Finansman Örüntüleri

5.1. Açık Bağış Kampanyaları ve Yöntem Değişikliği

Terör örgütlerinin kripto varlık kullanımına ilişkin ilk büyük kamuya açık operasyon, ABD Adalet Bakanlığı'nın Ağustos 2020'de duyurduğu ve Hamas'ın silahlı kanadı İzzeddin el-Kassam Tugayları, El Kaide ve IŞİD ile bağlantılı üç kampanyayı hedef alan operasyondur. Bakanlık bu operasyonu terör örgütlerine ait kripto hesaplarına yönelik bugüne kadarki en büyük el koyma olarak tanımlamış, 300'den fazla kripto varlık hesabına, dört internet sitesine ve dört sosyal medya sayfasına el konulmuştur (U.S. Department of Justice, 2020).

Bu kampanyaların ortak zaafı, bağış adreslerinin herkese açık yayımlanmasıydı. Sabit ve bilinen bir adres, analizciye bağışçıların borsa hesaplarına kadar uzanan bir harita sunuyordu. İsrail'in Terörün Finansmanıyla Mücadele Ulusal Bürosu (NBCTF), 2021'den itibaren Hamas bağlantılı çok sayıda adrese el koyma kararı yayımlamıştır. 27 Nisan 2023'te Kassam Tugayları, bağışçıların güvenliğini gerekçe göstererek Bitcoin bağışlarını durdurduğunu açıklamıştır (Chainalysis, 2023). Sonraki dönemde gruplar sabit adres yayımlamak yerine, gerçek cüzdanı gizleyen ödeme bağlantılarına ve her bağışçıya ayrı adres üretme yöntemine geçmiştir (Congressional Research Service, 2023).

Bu alandaki tahminler temkinle kullanılmalıdır. Ekim 2023 saldırısının ardından bazı basın haberlerinde Gazze merkezli grupların kripto yoluyla yüz milyonlarca dolar topladığı ileri sürülmüş, ancak veri sağlayıcı firmalar bu rakamların önemli bir bölümünün doğrudan örgüte değil, aynı adresleri kullanan borsa ve ödeme aracılarına ait olduğunu açıklamıştır (Congressional Research Service, 2023). Bu tartışma, zincir üstü analizde bir kümenin tamamını tek bir aktöre atfetmenin ne kadar kolay yanlış sonuç doğurabileceğini gösteren öğretici bir örnektir.

5.2. IŞİD ve Bölgesel Ağlar

IŞİD'in çöküşünden sonra örgütün finansmanı merkezî bir hazineden, bölgesel ofisler arasında dağılmış bir ağa dönüşmüştür. BM Yaptırımlar İzleme Ekibi'nin 2023 raporuna dayanarak TRM Labs (2026), Somali merkezli el-Karrar ofisinin Afganistan'daki IŞİD-Horasan vilayetine düzenli olarak ayda yaklaşık 25 bin dolar kripto aktardığını aktarmaktadır. Aynı kaynak, Mart 2024'te Moskova'daki Crocus City Hall saldırısının finansmanının bir kısmının

burakoguz.com

kripto varlıklarla sağlandığını belirtmektedir. Bu tespit, kripto varlıkların artık yalnızca örgütsel giderler için değil, doğrudan eylem finansmanı için de kullanıldığını göstermektedir.

Aynı dönemde sahte hayır kurumları ve kitle fonlaması platformları da öne çıkmıştır. ABD makamları, Mart 2025'ten itibaren Hamas bağlantılı kripto akışlarına yönelik beş ayrı işlemle yaklaşık 560 bin dolara el koymuştur. Bu vakalardan birinde sahte bir yardım kampanyasının 80 işlem üzerinden Filistin İslami Cihadı'na yaklaşık 30 bin dolar aktardığı tespit edilmiştir (TRM Labs, 2026). Tutarlar küçüktür, ancak terörün finansmanında küçük tutarların operasyonel etkisi büyüktür.

5.3. Seçilmiş Vakaların Kronolojisi

Tablo 3. Terörün finansmanında dijital araç kullanımına ilişkin seçilmiş vakalar

Tarih	Aktör / olay	Kullanılan araç	Sonuç / önemi
Kasım 2015	Paris saldırıları	Ön ödemeli kartlar	AB'de anonim kart eşiklerinin düşürülmesi (5. Direktif)
Ağustos 2020	Kassam Tugayları, El Kaide, IŞİD kampanyaları	BTC bağış adresleri, sahte KKD satışı	300+ hesaba el koyma; ABD'nin en büyük terör bağlantılı kripto el koyması
Temmuz 2021 ve sonrası	Hamas bağlantılı cüzdanlar (İsrail NBCTF)	BTC, USDT	Çok sayıda adres için el koyma kararı
Nisan 2023	Kassam Tugayları	BTC bağışları	Bağışların durdurulması; yöntem değişikliği
2023	IŞİD Somali (el-Karrar) → IŞİD-Horasan	Kripto transfer	Aylık ~25 bin dolar düzenli aktarım
Mart 2024	Crocus City Hall saldırısı (Moskova)	Kripto varlık	Eylem finansmanında kripto kullanımı
Mart 2025 ve sonrası	Hamas bağlantılı akışlar (ABD)	USDT, sahte yardım kampanyası	Beş işlemle ~560 bin dolar el koyma
2025-2026	T3 Mali Suçlar Birimi (Tether, TRON, TRM)	USDT-TRON	450 milyon doları aşan dondurma; terör finansmanı vakaları dâhil

Not. Kaynak: U.S. Department of Justice (2020), Avrupa Komisyonu (2016), Chainalysis (2023), Congressional Research Service (2023), CoinDesk (2025b) ve TRM Labs (2026) temel alınarak yazar tarafından derlenmiştir.

Kronoloji iki eğilimi açıkça göstermektedir. Birincisi, Bitcoin'den stablecoine ve özellikle TRON ağındaki USDT'ye geçiştir. İkincisi, herkese açık sabit adreslerden bağışçı başına üretilen tek kullanımlık adreslere geçiştir. Her iki değişiklik de takip mekanizmalarının etkisine verilmiş bir tepkidir ve analizcinin yöntemini de değiştirmektedir.

6. Takip Mekanizmaları I: Zincir Üstü Adli Analiz

Zincir üstü adli analiz (blockchain forensics), herkese açık defter verisinden hareketle adresleri kümelere ayırma, bu kümeleri gerçek dünyadaki hizmet ve kişilerle ilişkilendirme ve fon akışını izleme sürecidir. Şekil 3, bir terör finansmanı ya da aklama soruşturmasında bu sürecin adımlarını göstermektedir.



Şekil 3. Zincir üstü takipte başlangıç verisinden tedbire uzanan adli süreç

6.1. Kümeleme Sezgileri

Bitcoin gibi UTXO (harcanmamış işlem çıktısı) modeline dayanan zincirlerde en temel sezgi **ortak girdi sahipliği sezgisidir (common input ownership heuristic, CIOH)**. Bir işlemde birden fazla girdi harcanıyorsa, bu girdilerin hepsini imzalayabilen kişinin aynı olduğu varsayılır. Nakamoto (2008) bu bağlantıyı Bitcoin'in özgün makalesinde bir gizlilik sınırlaması olarak zaten belirtmiştir. Meiklejohn vd. (2013), bu sezgiyi **para üstü adresi (change address)** sezgisiyle birleştirerek Bitcoin ağındaki adreslerin önemli bir kısmını borsa, cüzdan ve hizmet sağlayıcılarına ait kümelere ayırabilmiş ve bilinen hırsızlıkların fonlarını borsalara kadar izlemiştir.

Sezgilerin bilinen istisnaları vardır. CoinJoin işlemleri, birden fazla kişinin girdisini bilerek aynı işlemde birleştirdiği için CIOH'u geçersiz kılar. Analiz yazılımları bu işlemleri tanıyıp kümelemeden hariç tutmalıdır. Aksi hâlde birbirinden bağımsız yüzlerce kullanıcı tek bir "süper kümede" birleşir. Beşinci bölümde değinilen Gazze kaynaklı hacim tartışması, bu tür aşırı kümelemenin sonuçlarını göstermektedir.

Ethereum ve TRON gibi hesap modeline dayanan zincirlerde CIOH uygulanamaz, çünkü her işlem tek bir gönderen hesaptan çıkar. Bu zincirlerde kümeleme daha çok davranışsal ipuçlarına dayanır: borsa yatırma adreslerinin fonları toplu olarak ana cüzdana aktarması, aynı hesaptan işlem ücreti (gaz) ödenmesi, token onay kalıpları ve zamanlama örüntüleri. Terör finansmanında sık görülen "her bağışçıya yeni adres" yöntemi, bu adreslerin daha sonra bir toplama adresinde birleşmesi nedeniyle genellikle toplama noktasında görünür hâle gelir.

burakoguz

6.2. Etiketleme ve Atfetme

Kümeleme adresleri gruplar, ama kimin olduklarını söylemez. **Etiketleme (attribution)**, kümeleri gerçek dünyadaki kimliklerle ilişkilendirir. Etiket kaynakları arasında borsalarla yapılan test işlemleri, kolluk kuvvetlerinin el koyduğu cihazlardan elde edilen adresler, OFAC ve BM yaptırım listelerindeki kripto adresleri, İsrail NBCTF gibi kurumların yayımladığı el koyma kararları ve açık kaynak istihbaratı (sosyal medyada paylaşılan bağış adresleri, forum gönderileri) bulunur. Ticari analiz platformlarının değeri büyük ölçüde bu etiket veritabanının kapsamından gelir.

Adli değerlendirme açısından etiketin kaynağı ve güven düzeyi raporda açıkça belirtilmelidir. Bir adresin "yüksek riskli" olarak işaretlenmesi, o adres sahibinin terörle bağlantılı olduğu anlamına gelmez. Özellikle bölgesel borsaların ya da ödeme aracılarının cüzdanları, binlerce masum kullanıcının işlemleriyle karışık hâldedir. Analiz raporunda doğrudan maruz kalma (bir yaptırımlı adresle doğrudan işlem) ile dolaylı maruz kalma (bir veya daha fazla ara adres üzerinden temas) ayrı gösterilmeli, atlama sayısı arttıkça çıkarımın gücünün azaldığı vurgulanmalıdır.

6.3. Akış Analizi ve Zincirler Arası Takip

Akış analizinde amaç, başlangıç adresinden çıkan fonu bir kimlik kaydının bulunduğu noktaya, yani bir KVHS'ye, elektronik para kuruluşuna ya da OTC aracısına kadar izlemektir. Soyulma zincirlerinde her adımda küçük bir tutar ayrılır. Bu ayrılan tutarların hangi borsalara girdiği, zincirin sonundaki bakiye kadar değerlidir. Otomatik atlama takibi yapan yazılımlar bu işi hızlandırır, ancak her dallanma noktasında analizcinin karar vermesi gerekir.

Zincirler arası köprüler ve merkeziyetsiz takas protokolleri, takibin en çok zorlaştığı noktalardır. Bir köprüde varlık bir zincirde kilitlenir ve diğer zincirde karşılığı basılır. Doğru eşleştirme için köprü sözleşmesinin olay kayıtları, tutarlar ve zaman damgaları iki zincirde birlikte okunmalıdır. Güncel analiz platformları bu eşleştirmeyi büyük ölçüde otomatikleştirmiştir. Bybit saldırısından sonra çalınan fonların hızla farklı zincirlere taşınması, bu yeteneğin hem ne kadar gerekli olduğunu hem de zaman baskısı altında ne kadar zorlandığını göstermiştir.

6.4. Gizlilik Coinleri ve Analizin Sınırları

Monero gibi gizlilik odaklı kripto varlıklar, gönderen, alıcı ve tutarı protokol düzeyinde gizler. Möser vd. (2018), Monero'nun ilk yıllarında karışımlı girdilerin %62'sinin "zincirleme çıkarım" yöntemiyle çözülebildiğini göstermiş, ancak sonraki protokol güncellemeleri bu açıkları büyük ölçüde kapatmıştır. Zcash'te ise Kappos vd. (2018), kullanıcıların çoğunluğunun gizli (shielded) havuzu kullanmadığını ve havuza giren ve çıkan tutarların eşleştirilmesiyle anonimlik kümesinin ciddi biçimde daraldığını göstermiştir.

Uygulamada gizlilik coinleri terörün finansmanında sınırlı kullanılmaktadır. Bunun nedeni teknik değil pratiktir: düzenlenmiş borsaların çoğu bu varlıkları listeden çıkarmıştır, likidite düşüktür ve bağışçıların bu varlıkları edinmesi zordur. Türkiye'de MASAK, gizlilik tabanlı kripto varlıkların alım-satımına veya saklanmasına aracılık eden KVHS'lerin uzaktan kimlik tespiti yapmasını yasaklamıştır. AB'de ise 2024/1624 sayılı Aklama Tüzüğü (AMLR),

burakolgun.com

KVHS'lerin anonimliği artıran kripto varlıklarla hizmet sunmasını 10 Temmuz 2027'den itibaren yasaklamaktadır. Bu nedenle gizlilik coinlerinin takibinde odak zincir üstü veriden çok borsa giriş ve çıkışları, zamanlama ve zincir dışı kayıtlardır.

6.5. Makine Öğrenmesi ile Risk Sınıflandırması

Kural tabanlı izleme sistemleri bilinen örüntüleri yakalar, ancak yeni örüntülere geç kalır. Weber vd. (2019), Elliptic ile birlikte yayımladıkları ve 203.769 Bitcoin işlemini içeren veri setinde işlemlerin yaklaşık %2'sini yasa dışı, %21'ini yasal olarak etiketlemiş, kalan işlemleri ise etiketsiz bırakmıştır. Çalışmada grafik evrişimli ağlar ile rastgele orman gibi yöntemler karşılaştırılmış, işlem grafiğinin yapısal özelliklerinin sınıflandırma başarısını artırdığı gösterilmiştir. Bu veri seti, sonraki yıllarda kripto aklama tespitine yönelik akademik çalışmaların ortak ölçüt setlerinden biri olmuştur.

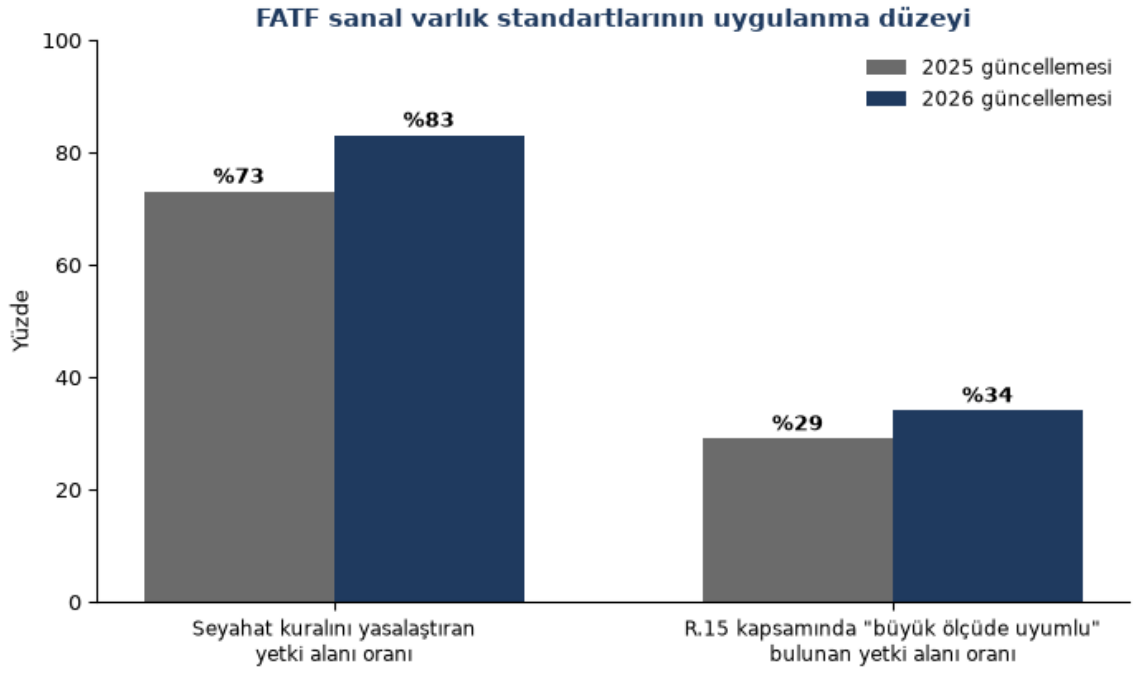
Makine öğrenmesi modellerinin adli süreçte kullanımı bir sınır taşır. Bir modelin bir işlemi "yüksek olasılıkla yasa dışı" olarak sınıflandırması, şüpheli işlem bildirimi ya da soruşturma başlatma için yeterli bir gerekçe olabilir, ancak ceza yargılamasında tek başına delil değeri taşımaz. Mahkeme önüne gelen bir raporda sınıflandırmanın hangi özelliklere dayandığı açıklanmalı ve sonuç, somut işlem zinciri ile zincir dışı kayıtlarla desteklenmelidir. TRM Labs (2026), üretken yapay zekânın belgelenmiş hiçbir terör finansmanı vakasında henüz ortaya çıkmadığını kaydetmektedir. Bu durum değişebilir, ancak bugün için risk, failin yapay zekâ kullanmasından çok analizcinin model çıktısına aşırı güvenmesindedir.

7. Takip Mekanizmaları II: Düzenleyici ve Kurumsal Çerçeve

7.1. FATF Tavsiye 15 ve Seyahat Kuralı

FATF, 2018-2019 yıllarında Tavsiye 15'i sanal varlıkları ve sanal varlık hizmet sağlayıcılarını kapsayacak biçimde genişletmiştir. Buna göre VASP'ler lisanslanmalı ya da kayıt altına alınmalı, müşterini tanı yükümlülüklerine tabi tutulmalı ve denetlenmelidir. Aynı çerçevenin en önemli bileşeni, Tavsiye 16'daki elektronik transfer kurallarının sanal varlıklara uygulanmasını öngören **seyahat kuralıdır (Travel Rule)**. Seyahat kuralı, bir VASP'den diğerine yapılan transferde gönderen ve alıcıya ilişkin bilgilerin transferle birlikte iletilmesini ve saklanmasını gerektirir. FATF bu kural için 1.000 ABD doları ya da avroluk bir eşik önermektedir (FATF, 2021).

burakolgun.com



Kaynak: FATF (2025b, 2026) hedefli güncelleme raporları temel alınarak derlenmiştir.

Şekil 4. FATF sanal varlık standartlarının yetki alanlarındaki uygulanma düzeyi (2026)

Şekil 4'te görüldüğü gibi seyahat kuralını yasalaştıran yetki alanlarının oranı 2025'te %73 iken (117 yetki alanından 85'i) 2026 güncellemesinde %83'e yükselmiştir. Buna karşılık Tavsiye 15 bakımından "büyük ölçüde uyumlu" bulunan yetki alanlarının oranı yalnızca %29'dan %34'e çıkmış, %43'lük bir kesim "kısmen uyumlu" düzeyde kalmıştır (FATF, 2025b, 2026). Yasanın varlığı ile uygulamanın etkinliği arasındaki bu fark, FATF'in en sık vurguladığı sorundur. Yasalaştırma olan yerlerde bile denetim ve sınır ötesi mesaj alışverişi tutarsız kalmakta, risk değerlendirmesi, lisanslama ve açık denizlerde (offshore) çalışan lisanssız sağlayıcılara yönelik işlem en zayıf alanlar olmayı sürdürmektedir.

Seyahat kuralının terörün finansmanı açısından bir zaafı vardır: kural VASP'ler arası transferlerde işler, kişinin kendi kontrolündeki (unhosted, self-hosted) cüzdanlar arasında yapılan eşten eşe transferlerde ise uygulanamaz. FATF (2026) bu nedenle barındırılmayan cüzdanlar üzerinden yapılan P2P işlemleri başlıca yeni riskler arasında saymaktadır. TRM Labs'ın (2026) tarif ettiği bağış örüntüsü tam da bu boşlukta çalışır: bağışçı kendi cüzdanından örgüt adresine gönderim yapar ve hiçbir VASP araya girmez. Kural ancak fon bir borsaya girdiğinde yeniden devreye girer.

7.2. Avrupa Birliği ve Amerika Birleşik Devletleri

Avrupa Birliği, 2023/1113 sayılı Fon Transferleri Tüzüğü (TFR) ile seyahat kuralını 30 Aralık 2024'ten itibaren kripto varlık transferlerine eşik uygulamadan genişletmiştir. KVHS'ler arasındaki her transferde gönderen ve alıcı bilgisi aktarılmak zorundadır. Kişisel cüzdanlarla yapılan ve 1.000 avroyu aşan transferlerde KVHS, cüzdanın müşteriye ait olup olmadığını doğrulamakla yükümlüdür. 2023/1114 sayılı MiCA Tüzüğü kripto varlık hizmet sağlayıcıları ve stablecoin ihraççıları için lisans rejimi kurmuş, 2024 aklama paketi ise doğrudan

uygulanan Aklama Tüzüğü (AMLR) ile Frankfurt merkezli yeni bir AB Aklamayla Mücadele Otoritesi (AMLA) oluşturmuştur.

ABD'de 18 Temmuz 2025'te yürürlüğe giren GENIUS Yasası, ödeme amaçlı stablecoin ihraççılarını Banka Gizliliği Yasası kapsamında finansal kuruluş olarak nitelendirmiş ve hukuka uygun taleplere uyum için varlık dondurma, el koyma ve işlemi engelleme yeteneğine sahip olmalarını şart koşmuştur. Böylece Tether ve Circle'ın fiilen uyguladığı dondurma kapasitesi yasal bir yükümlülüğe dönüşmüştür.

Aynı dönemde ABD'deki yargı pratiği, gizlilik araçlarının geliştiricilerinin sorumluluğu konusunda tartışmalı sonuçlar üretmiştir. Tornado Cash'e yönelik Hazine yaptırımları Mart 2025'te kaldırılmış, ancak kurucu ortak Roman Storm Ağustos 2025'te lisanssız para transferi işletme komplosundan suçlu bulunmuştur. Jüri, kara para aklama ve yaptırım ihlali suçlamalarında karara varamamış (CoinDesk, 2025a), savcılığın bu suçlamalar için talep ettiği yeniden yargılama Nisan 2027'ye ertelenmiştir (The Block, 2026). Samourai Wallet kurucuları ise suçlamayı kabul etmiş ve Kasım 2025'te beş ve dört yıl hapis cezasına çarptırılmıştır (CoinDesk, 2025c). Bu davalar, gözetimsiz (non-custodial) yazılım geliştiricisi ile para transfer hizmeti arasındaki sınırın henüz netleşmediğini göstermektedir.

7.3. İhraççı Düzeyinde Dondurma ve Kamu-Özel Sektör İşbirliği

Stablecoinlerin yasa dışı kullanımdaki payı artarken, aynı özellik takip mekanizması olarak da kullanılmaya başlanmıştır. Tether, TRON ve TRM Labs tarafından Eylül 2024'te kurulan T3 Mali Suçlar Birimi (T3 FCU), Ekim 2025 itibarıyla 300 milyon doları (CoinDesk, 2025b), 2026 itibarıyla ise 450 milyon doları aşan yasa dışı varlığı dondurmuştur. Birim, 2025'te engellenen yasa dışı gelirde %43,9 artış bildirmiş ve dondurmaların hırsızlık, KDHC bağlantılı faaliyet ve terörün finansmanı vakalarını kapsadığını açıklamıştır. Model basittir: analiz firması adresi tespit eder, kolluk kuvveti talebi iletir, ihraççı adresi kara listeye alır. Bitcoin'de ancak bir borsaya ulaşıldığında mümkün olan tedbir, stablecoinlerde fon hâlâ failin cüzdanındayken uygulanabilir.

Bu mekanizmanın bir bedeli de vardır. Özel bir şirketin, yargı kararı olmaksızın ya da farklı ülkelerin kolluk taleplerine dayanarak varlık dondurması, hukuki güvence ve orantılılık sorunları doğurur. Yanlış atfedilmiş bir adresin dondurulması masum bir kullanıcının varlığına fiilen el konulması anlamına gelir. Bu nedenle dondurma kararlarının gerekçesinin ve itiraz yolunun açık olması, mekanizmanın meşruiyeti için gereklidir.

burakisin.com

Tablo 4. Sanal varlık alanında seçilmiş düzenleyici çerçevelerin karşılaştırılması

Unsur	FATF standartları	Avrupa Birliği	ABD	Türkiye
Temel metin	Tavsiye 15 ve 16; 2021 rehberi	MiCA (2023/1114), TFR (2023/1113), AMLR (2024/1624)	BSA; GENIUS Yasası (2025)	5549, 6415, 6362 (7518 ile), MASAK tebliğleri
Lisans / izin	Lisans ya da kayıt	MiCA lisansı (KVHS)	FinCEN MSB kaydı + eyalet lisansı	SPK izni (KVHS)
Seyahat kuralı eşiği	1.000 USD/EUR önerisi	Eşiksiz (KVHS arası)	3.000 USD (mevcut kural)	15.000 TL üzerinde tam bilgi ve teyit
Kişisel cüzdan	Risk temelli yaklaşım	>1.000 EUR sahiplik doğrulaması	Risk temelli	Risk temelli; sıkılaştırılmış tedbirler
Gizlilik coinleri	Risk temelli	KVHS'ler için yasak (2027)	Açık yasak yok	Uzaktan kimlik tespiti yasağı
Stablecoin ihraççısı	2026 raporunda öncelikli risk	MiCA EMT/ART rejimi	Dondurma yeteneği zorunlu	Ayrı rejim yok
Denetim otoritesi	Ülke denetimleri	Ulusal otorite + AMLA	FinCEN, OFAC, eyaletler	SPK, MASAK; e-para için TCMB

Not. Kaynak: FATF (2021, 2025b, 2026), ilgili AB tüzükleri, GENIUS Yasası (2025), 7518 sayılı Kanun ve MASAK (2025) temel alınarak yazar tarafından derlenmiştir.

8. Türkiye'de Hukuki Çerçeve ve Uygulama

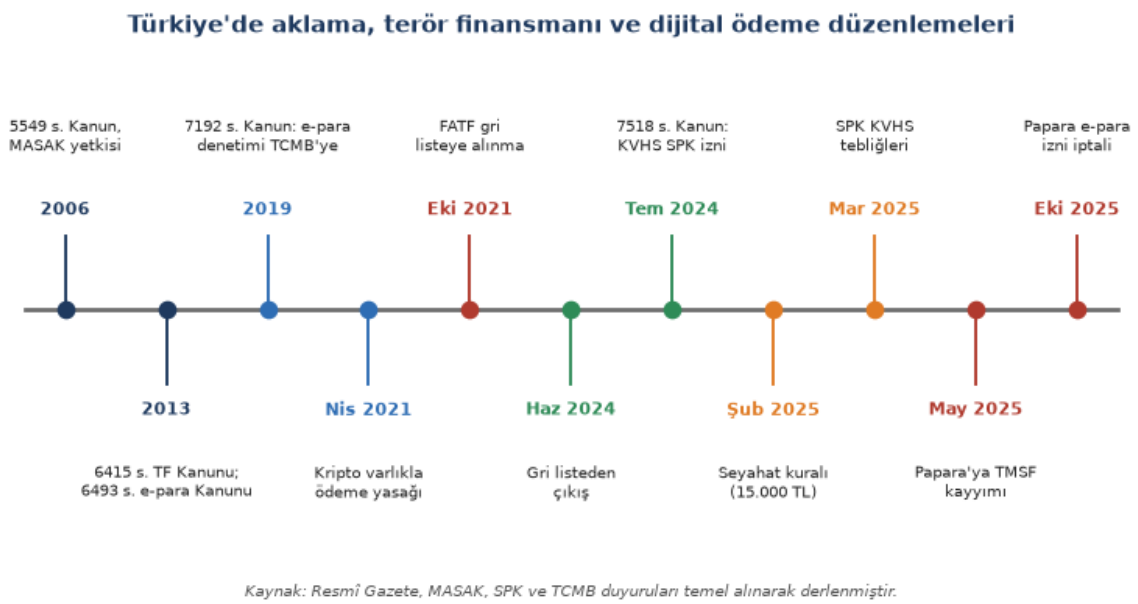
8.1. Mevzuat

Türkiye'de aklama ve terörün finansmanıyla mücadelenin temel metni, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'dur. Kanun, Mali Suçları Araştırma Kurulu'nu (MASAK) mali istihbarat birimi olarak yetkilendirmiş, yükümlülere müşterini tanıma, şüpheli işlem bildirimi, bilgi ve belge verme ile kayıt saklama yükümlülükleri getirmiştir. Yükümlülüklerin ayrıntısı, Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik'te düzenlenmiştir. 6415 sayılı Kanun terörün finansmanını ayrı bir suç olarak tanımlamış ve BM Güvenlik Konseyi kararları ile yabancı ülke talepleri doğrultusunda malvarlığının dondurulması usulünü kurmuştur. 7262 sayılı Kanun (2020) ise kitle imha silahlarının yayılmasının finansmanını ve bağış toplama faaliyetlerine ilişkin denetimi bu çerçeveye eklemiştir.

Elektronik para tarafında temel metin 6493 sayılı Kanun'dur. 7192 sayılı Kanun ile 2019'da ödeme ve elektronik para kuruluşlarının düzenleme ve denetim yetkisi BDDK'dan TCMB'ye devredilmiştir. Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik (2021), anonim ön ödemeli araçlara ve kimlik doğrulamasına ilişkin sınırları belirlemektedir. Elektronik para kuruluşları aynı zamanda 5549 sayılı Kanun kapsamında yükümlüdür.

Kripto varlıklar tarafında ilk düzenleme, TCMB'nin Nisan 2021'de yayımladığı ve kripto varlıkların ödemelerde doğrudan ya da dolaylı olarak kullanılmasını yasaklayan yönetmeliktir. Mayıs 2021'de kripto varlık alım satım platformları Tedbirler Yönetmeliği'ndeki yükümlüler arasına eklenmiştir. Asıl kapsamlı düzenleme, 2 Temmuz 2024 tarihli Resmî Gazete'de yayımlanan 7518 sayılı Kanun ile gelmiştir. Kanun, 6362 sayılı Sermaye Piyasası Kanunu'na kripto varlık, kripto varlık hizmet sağlayıcı ve cüzdan tanımlarını eklemiş, KVHS'lerin faaliyetini SPK iznine, platformların teknik altyapısını TÜBİTAK kriterlerine bağlamış ve izinsiz faaliyet için hapis cezası öngörmüştür. SPK'nın KVHS'lere ilişkin tebliğleri 13 Mart 2025'te yürürlüğe girmiştir.

bilgesam.com



Şekil 5. Türkiye'de aklama, terörün finansmanı ve dijital ödemelere ilişkin düzenleme ve uygulama kronolojisi (2026)

8.2. MASAK Düzenlemeleri ve Seyahat Kuralı

Aralık 2024'te Tedbirler Yönetmeliği'ne eklenen 24/A maddesi ile Türkiye, seyahat kuralını 25 Şubat 2025'ten itibaren uygulamaya koymuştur. Buna göre KVHS'ler, aracılık ettikleri kripto varlık transferlerinde gönderen ve alıcıya ilişkin bilgileri almak ve iletmekle yükümlüdür. 15.000 TL ve üzerindeki transferlerde gönderenin adı soyadı ya da unvanı, cüzdan adresi gibi bilgilerin mesajda yer alması ve doğruluğunun teyit edilmesi zorunludur. Aynı düzenleme, gizlilik tabanlı kripto varlıklara aracılık eden KVHS'lerin uzaktan kimlik tespiti yapmasını yasaklamıştır.

MASAK, Haziran 2025'te yayımladığı genel tebliğlerle KVHS'ler için sıkılaştırılmış tedbirleri ve uzaktan kimlik tespiti usullerini ayrıntılandırmış, 30 Eylül 2025'te ise Kripto Varlık Hizmet Sağlayıcılar Rehberi'ni güncellemiştir. Güncellenen rehbere göre 13 Mart 2025'ten itibaren yeni müşteri kabulü görüntülü görüşme yoluyla yapılmalıdır (MASAK, 2025). Bu düzenlemeler, Türkiye'deki lisanslı platformları uluslararası standartla büyük ölçüde uyumlu hâle getirmiştir. Asıl açık, yurt dışında yerleşik ve Türkiye'deki kullanıcılara hizmet veren lisanssız platformlar ile P2P piyasalarındadır.

8.3. Uygulamadan Gözlemler

Türkiye'deki kripto varlık piyasasının büyüklüğü, risk değerlendirmesinde belirleyici bir değişkendir. Chainalysis (2025), Türkiye'ye 2021 başından 2025 ortasına kadar 878 milyar doları aşan brüt kripto girişi olduğunu, son on iki aylık dönemde bu girişin yaklaşık 200 milyar dolar olduğunu ve bu hacmin önemli bir kısmının yatırım amaçlı ve spekülatif işlemlerden kaynaklandığını tespit etmiştir. Bu kadar büyük bir meşru hacim, yasa dışı akışların içinde saklanabileceği derin bir likidite havuzu anlamına gelir.

Adli bilişim uygulamasında karşılaşılan vakaların önemli bir bölümü, terörün finansmanından çok yasa dışı bahis, nitelikli dolandırıcılık ve bunların gelirlerinin aklanmasıyla ilgilidir. Bu vakalarda tipik zincir, kiralık banka ya da e-para hesaplarında

toplanan fonun bir KVHS'ye aktarılması, USDT'ye çevrilmesi ve yurt dışındaki bir platforma ya da kişisel cüzdana çekilmesidir. Terörün finansmanı vakaları ise sayıca az, tutarca küçük ve ağırlıklı olarak ağ analizine dayalıdır. Her iki durumda da soruşturmanın düğüm noktası yurt içindeki çıkış kapısıdır: KVHS'den alınan kimlik, IP ve cihaz kayıtları, elektronik para kuruluşundan alınan hesap hareketleri ve bu verilerin iletişim kayıtlarıyla karşılaştırılması.

8.4. Delil Değerlendirmesi

Kripto varlıklara ilişkin delil toplamada Ceza Muhakemesi Kanunu'nun 128. maddesindeki el koyma, 134. maddesindeki bilgisayar, bilgisayar programları ve kütüklerinde arama, kopyalama ve el koyma ile 332. maddesindeki bilgi isteme hükümleri birlikte uygulanır. Uygulamada dikkat edilmesi gereken birkaç husus öne çıkmaktadır.

- El konulan cihazda bulunan kurtarma ifadesi (seed phrase) ya da özel anahtar, varlığın kendisine erişim sağlar. Varlık, soruşturma makamının kontrolündeki bir cüzdana aktarılmadıkça fail ya da iş birlikçileri tarafından başka bir cihazdan boşaltılabilir. Aktarım işleminin karma değeri, saati ve tanıkları tutanağa geçirilmelidir.
- Zincir üstü veri kamuya açık olsa da analiz raporunda kullanılan blok gezgini ya da düğüm, sorgu tarihi, işlem kimlikleri (txid) ve adresler eksiksiz belirtilmelidir. Böylece rapor, bağımsız bir uzman tarafından aynı veriyle yeniden üretilebilir.
- Ticari analiz platformlarından alınan etiketler ve risk puanları, kaynağı ve güven düzeyi belirtilerek sunulmalıdır. Etiket, zincir dışı bir kayıtla (KVHS yanıtı, el konulan cihaz, yaptırım listesi) desteklenmedikçe kimlik tespiti olarak kullanılmamalıdır.
- Yurt dışında yerleşik KVHS'lerden bilgi alınması adli yardımlaşma (MLAT) sürecine bağlıdır ve aylar sürebilir. Stablecoin söz konusu olduğunda ihraççıya iletilecek bir dondurma talebi, adli yardımlaşma sonuçlanana kadar varlığın korunmasını sağlayabilir.

Son olarak, bir adresin terör bağlantılı bir kümeyle dolaylı teması, adres sahibinin kastını göstermez. Bölgesel borsa ve ödeme aracısı cüzdanları üzerinden kurulan dolaylı bağlantılar, özellikle suçun manevi unsurunun değerlendirilmesinde temkinle ele alınmalıdır.

9. Değerlendirme ve Öneriler

Derlenen veriler, takip mekanizmalarının etkisinin yöntem değişikliğiyle karşılandığı bir döngüye işaret etmektedir. Açık bağış adresleri el koymalarla sonuçlanınca bağışçı başına adres üretimine geçilmiş, Bitcoin'in izlenebilirliği anlaşılınca stablecoinlere yönelinmiş, stablecoin dondurmaları arttıkça P2P ve OTC aracılarının önemi büyümüştür. Bu döngüde kalıcı üstünlük sağlayan taraf, zincir üstü veriyi zincir dışı kayıtlarla en hızlı birleştirebilen taraftır. Bu tespitten hareketle aşağıdaki öneriler sunulmaktadır.

- **Giriş ve çıkış kapılarında veri kalitesi.** Elektronik para kuruluşları ile KVHS'ler arasındaki transferlerde, karşı tarafın kimliğine ilişkin bilgilerin yapılandırılmış ve makine tarafından okunabilir biçimde tutulması, hesap kiralama ağlarının tespitini hızlandırır. Aynı cihazdan ya da IP adresinden yönetilen çok sayıda hesap, KYC kaydı doğru olsa da ortak bir kullanıcıya işaret edebilir.

burakoguz.com

- **E-para ve kripto riskinin birlikte izlenmesi.** TCMB, SPK ve MASAK arasında, e-para hesaplarından KVHS'lere yönelen akışların ortak göstergelerle izlenmesini sağlayacak bir veri paylaşım protokolü, iki ayrı denetim alanına bölünmüş olan riskin tek bir resimde görülmesini sağlar.
- **Stablecoin dondurma sürecinin kurumsallaşması.** Türkiye'deki kolluk ve savcılık birimlerinin büyük stablecoin ihraççılarına doğrudan ve hızlı dondurma talebi iletebileceği bir usul, adli yardımlaşma süresince varlığın kaybolmasını önler. Talebin yargısal denetime tabi olması ve itiraz yolunun açık tutulması gerekir.
- **Adli analiz raporlarında standart.** Zincir üstü analiz raporları için kullanılan araç, etiket kaynağı, atlama sayısı, doğrudan ve dolaylı maruz kalma ayrımı ile yeniden üretilebilirlik bilgilerini içeren asgari bir şablon, bilirkişi raporları arasındaki kalite farkını azaltır.
- **Lisanssız yurt dışı platformlar ve P2P piyasalar.** 7518 sayılı Kanun lisanslı platformları düzenlemiştir. Türkiye'deki kullanıcılara hizmet veren yurt dışı platformlarla ilgili erişim, ödeme kuruluşu iş birliği ve kullanıcı bilgilendirmesi tedbirlerinin birlikte uygulanması, riskin bu alana kaymasını sınırlar.
- **Orantılılık.** Kripto varlık kullanıcılarının tamamını şüpheli sayan tedbirler, hacmi kayıt dışı P2P piyasalara iter ve izlenebilirliği azaltır. Hedef, meşru kullanıcıyı lisanslı ve izlenebilir kanallarda tutmak olmalıdır.

10. Sonuç

Elektronik para ve blokzincir, aklama ile terörün finansmanına yeni bir amaç kazandırmamış, mevcut amaçların maliyetini düşürmüştür. Elektronik para, özellikle hesap kiralama ve anonim ön ödemeli araçlar üzerinden, fonların toplanması ve yerleştirilmesi aşamasında kullanılmaktadır. Blokzincir ise sınır ötesi transferi hızlandırmakta ve ucuzlatmaktadır. Terör örgütleri söz konusu olduğunda bu kullanım belirgin bir örüntüye oturmuştur: TRON ağındaki USDT, her bağışçıya ayrı adres ve bölgesel aracılar üzerinden nakde çıkış. 2025 yılında yasa dışı kripto hacminin 154 milyar dolara ulaşması büyük ölçüde devlet bağlantılı yaptırım kaçakçılığından kaynaklanmaktadır. Terörün finansmanının payı küçük, ama operasyonel etkisi büyüktür.

Takip mekanizmaları açısından çalışmanın temel bulgusu, blokzincirin sanıldığı kadar anonim olmadığı, ancak zincir üstü verinin tek başına kimlik vermediğidir. Kümeleme, etiketleme ve akış analizi fonun nereye gittiğini gösterir. Kimin elinde olduğunu ise giriş ve çıkış kapılarındaki kayıtlar gösterir. Seyahat kuralı bu kapılar arasındaki bilgi akışını standartlaştırmış, stablecoin ihraççılarının dondurma yetkisi ise fon henüz failin cüzdanındayken tedbir almayı mümkün kılmıştır. Kişisel cüzdanlar arasındaki P2P transferler ve lisanssız yurt dışı platformlar ise bu mekanizmaların en zayıf kaldığı alanlardır.

Türkiye, 2021-2025 döneminde bu alanda hızlı bir düzenleme süreci geçirmiştir. FATF gri listesinden çıkış, 7518 sayılı Kanun, seyahat kuralı ve MASAK'ın KVHS rehberi, lisanslı platformları uluslararası standarda yaklaştırmıştır. 2025 yılındaki elektronik para soruşturması ise riskin yalnızca kripto varlık alanında olmadığını, e-para ile kripto arasındaki geçişin birlikte izlenmesi gerektiğini göstermiştir. Bundan sonraki aşamada belirleyici olacak konular,

burakolgun.com

kurumlar arası veri paylaşımı, stablecoin dondurma usulü ve adli analiz raporlarının niteliğidir.

Kaynakça

Anadolu Ajansı. (2026). TCMB, 2025 yılı ödeme ve elektronik para kuruluşlarının gözetim ve denetim sonuçlarını açıkladı. https://www.aa.com.tr/tr/ekonomi/tcmb-2025-yili-odeme-ve-elektronik-para-kuruluslarinin-gozetim-ve-denetim-sonuclarini-acikladi/3813862

Avrupa Komisyonu. (2016). Communication on an action plan for strengthening the fight against terrorist financing (COM(2016) 50 final). Brüksel.

Birleşmiş Milletler. (1999). International convention for the suppression of the financing of terrorism (BM Genel Kurulu, A/RES/54/109, 9 Aralık 1999). Türkçe adı: Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme; 4738 sayılı Kanun ile onaylanması uygun bulunmuştur (2002, 10 Ocak).

Chainalysis. (2023). Hamas' al-Qassam Brigades announces end of cryptocurrency donation efforts. https://www.chainalysis.com/blog/hamas-al-qassam-brigades-cryptocurrency-donations-shutdown/

Chainalysis. (2025). The 2025 geography of cryptocurrency report. https://www.chainalysis.com/reports/2025-geo-crypto-report/

Chainalysis. (2026a, 8 Ocak). 2026 crypto crime report: Introduction. https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/

Chainalysis. (2026b). Crypto sanctions: 2026 crypto crime report. https://www.chainalysis.com/blog/crypto-sanctions-2026/

CoinDesk. (2025a, 6 Ağustos). Roman Storm guilty of unlicensed money transmitting conspiracy in partial verdict. https://www.coindesk.com/policy/2025/08/06/roman-storm-guilty-of-unlicensed-money-transmitting-conspiracy-in-partial-verdict

CoinDesk. (2025b, 31 Ekim). T3 Financial Crime Unit, backed by Tron, Tether, TRM Labs, has now frozen $300M in assets. https://www.coindesk.com/policy/2025/10/31/t3-financial-crime-unit-backed-by-tron-tether-trm-labs-has-now-frozen-usd300m-in-assets

CoinDesk. (2025c, 6 Kasım). Samourai Wallet developer sentenced to 5 years in prison for unlicensed money transmitting. https://www.coindesk.com/policy/2025/11/06/samourai-wallet-developer-sentenced-to-5-years-in-prison-for-unlicensed-money-transmitting

Congressional Research Service. (2023). Terrorist financing: Hamas and cryptocurrency fundraising (IF12537). https://www.congress.gov/crs-product/IF12537

Euronews. (2025, 27 Mayıs). Papara'ya yasa dışı bahis operasyonu: Şirketlere TMSF kayyum olarak atandı. https://tr.euronews.com/2025/05/27/paparaya-yasa-disi-bahis-operasyonu-sekiz-sirkete-tmsf-kayyum-olarak-atandi

FATF. (2015). Emerging terrorist financing risks. FATF.

FATF. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF.

FATF. (2025a). Comprehensive update on terrorist financing risks. FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html

burakoguz.com

FATF. (2025b). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

FATF. (2026). Seventh targeted update on implementation of the FATF standards on virtual assets/VASPs. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

GENIUS Act. (2025). Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27.

Kappos, G., Yousaf, H., Maller, M., & Meiklejohn, S. (2018). An empirical analysis of anonymity in Zcash. 27th USENIX Security Symposium (s. 463-477). USENIX Association.

MASAK. (2025, 30 Eylül). Kripto varlık hizmet sağlayıcılar rehberi güncellendi ve yayımlandı. https://masak.hmb.gov.tr/duyuru/kripto-varlik-hizmet-saglayicilar-rehberi-guncellendi-ve-yayimlandi

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. Proceedings of the 2013 Internet Measurement Conference (s. 127-140). https://doi.org/10.1145/2504730.2504747

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. 2013 APWG eCrime Researchers Summit (s. 1-14). IEEE. https://doi.org/10.1109/eCRS.2013.6805780

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An empirical analysis of traceability in the Monero blockchain. Proceedings on Privacy Enhancing Technologies, 2018(3), 143-163. https://doi.org/10.1515/popets-2018-0025

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik. (2021, 1 Aralık). Resmî Gazete (Sayı: 31676).

Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik. (2021, 16 Nisan). Resmî Gazete (Sayı: 31456).

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets. Official Journal of the European Union, L 150, 1-42.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets. Official Journal of the European Union, L 150, 40-205.

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Official Journal of the European Union, L 2024/1624.

Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun, 7518 sayılı Kanun. (2024, 2 Temmuz). Resmî Gazete (Sayı: 32590).

Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun, 5549 sayılı Kanun. (2006, 18 Ekim). Resmî Gazete (Sayı: 26323).

burakogun.com

Terörün Finansmanının Önlenmesi Hakkında Kanun, 6415 sayılı Kanun. (2013, 16 Şubat). Resmî Gazete (Sayı: 28561).

The Block. (2026, 26 Ağustos). Tornado Cash developer Roman Storm's retrial pushed back to April 2027. https://www.theblock.co/news/regulation/2026-08-26-tornado-cash-roman-storm-retrial-april-2027-412761

TRM Labs. (2025). Garantex, Grinex, and the A7A5 token: A deep dive into sanctions evasion networks. https://www.trmlabs.com/resources/blog/garantex-grinex-and-the-a7a5-token-a-deep-dive-into-sanctions-evasion-networks

TRM Labs. (2026, 11 Eylül). The evolution of terrorist financing, 25 years after 9/11. https://www.trmlabs.com/resources/blog/evolution-of-terrorist-financing-25-years-after-9-11

U.S. Department of Justice. (2020, 13 Ağustos). Global disruption of three terror finance cyber-enabled campaigns. https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv. https://doi.org/10.48550/arXiv.1908.02591

burakolgun.com